Robustness and Performance Scaling of Large-Scale Quantum Computers with Faulty Gates

by

Yun Seong Nam

Faculty Advisor: Dr. Reinhold Blümel

A Dissertation submitted to the faculty of Wesleyan University in partial fulfillment of the requirements for the Degree of Doctor of Philosophy

Middletown, Connecticut

May, 2016
Abstract

This thesis presents an overview of my published work on streamlining and optimizing quantum processors. Complete, microscopic, quantum-gate–by–quantum-gate simulations of a variety of quantum circuits are implemented and executed on state-of-the-art multi-processor parallel computers. A host of analytical scaling formulas addressing the quality of quantum processors, e.g., in the presence of realistic gate errors and defects, are presented. These formulas reliably describe the practically interesting, large-number-of-qubit regime, inaccessible to simulations on classical computers.

Much of the technical details may be found in my published articles, which appear in the Appendix. This thesis also presents the generic and specific directions into which my current investigations are headed. In addition, several preliminary results are presented and discussed.
Acknowledgments

I would like to thank my research advisor, Professor Reinhold Blümel, for being a great mentor. Without your insight, knowledge, and understanding of physics, I wouldn’t have been able to write this thesis. It has been a great honor to be your student, and I look forward to future collaborations.

I would like also to thank the Wesleyan Physics Department. I am grateful for all the support I received from the department from the faculty and staff members as well as the students. My time at Wesleyan has been enjoyable thanks to your friendship and kindness.

Special thanks to my current and former colleagues in the research group, Daniel Weiss, Varun Ursekar, Max Silvester, Angus Kan, Jarrett Gorin, Dylan Courville, Guy Geyer, Dirk Miller, Jesse Tarnas, Eric Jones, and Philip Schmidt. It has been quite a journey working with you all, and I wish you the best in your future career.

I am grateful for the generous computing time allotted by the Wesleyan computing center and thank Henk Meij for all his technical support, which was vital to completing this thesis.
# Contents

1 History ........................................ 1  
  1.1 The Next Big Thing .......................... 1  
  1.2 Crisis and Recovery ......................... 2  
  1.3 Current State of the Art .................... 6  

2 Tapestry ....................................... 9  
  2.1 To Be AND Not To Be: Quantum Superposition 9  
  2.2 To Be OR Not To Be: Practical Quantum Computers 17  
  2.3 Robustness of Quantum Information Processors 24  
  2.4 Optimization and Performance Boost: Sensible Quantum Computing 32  

3 Discussion .................................... 37  

4 Remarks ....................................... 48  

5 A brief guide to my publications ............... 50  
  5.1 Quantum Computing ......................... 50  
  5.2 Ion Trapping .................................. 55  

A List of Publications .......................... 58
Chapter 1

History

1.1 The Next Big Thing

The timeline of quantum computing may be traced back to Landauer [1] who, in 1961, showed that only reversible computing is free of heating. Since heating must be countered by cooling for any physical machine to function properly, the feasibility of reversible computing became of both academic and practical interest. In 1973, Bennett showed that reversible computing is indeed possible [2], a fact that hints at the possibility of employing quantum mechanics, inherently unitary (hence reversible), in computations.

Meanwhile, in 1970, Wiesner discovered the so-called conjugate coding [3], where, for the first time, the fundamental concepts of quantum mechanics and their curious nature were applied to information technology. By introducing the bits of quantum information, now known as quantum bits or qubits [4], Wiesner showed that a secure cryptosystem may be constructed via exploiting the uncertainty principle [5]. This idea, sometimes referred to as quantum money, later led to the invention of quantum-key-distribution protocols [6], whose security is guaranteed by the No-Cloning Theorem [7, 8]. While Wiesner’s work was not well received by his contemporaries (the original manuscript was rejected by
IEEE Information Theory in 1970; eventually published in SIGACT News only in 1983 [9]), as it turned out, the emergence of the fields of quantum computing and quantum information was right around the corner.

The field of quantum computing finally emerged in the early 1980s. Some of the earliest founders include Benioff [10] and Feynman [11], who proposed the idea of quantum computing largely based on the idea of quantum simulators and the concept of universal reversible computing. The latter became a practical possibility via Toffoli’s inventions [12], such as classical, reversible, two-bit CONTROL-NOT (CNOT) gates and three-bit CONTROL-CONTROL-NOT (CCNOT) gates, that were proved to be universal for classical computing. When Deutsch introduced the quantum mechanical version of Turing’s principle to establish the notion of universal quantum computing [13] and realized it by introducing a three-qubit universal gate [14], quantum computing was ready to take center stage in scientific research.

1.2 Crisis and Recovery

Holevo, in 1973, provided and sharpened the upper bounds of the quantity of information that \( N \) qubits can contain (i.e., \( 2^N \) classical bits) and reveal (i.e., \( N \) bits) [15]. Useful for measuring the capacity of a quantum communication channel, the Holevo bound was later generalized to include quantum entanglement pairs [16–18] and the effect of noise [19].

The single-most interesting fact about the original Holevo bound [15] is that \( N \) qubits can only (directly) transfer at most \( N \) classical bits of information, which, at a first glance, is puzzling given the supposedly exponentially better information capacity of qubits compared with classical bits. Overcoming this bound was the use of quantum entanglement in communication. In this connection, Ekert first demonstrated that, via the use of an Einstein-Podolsky-Rosen (EPR) pair [20], one can establish a secure
quantum communication channel [21]. Culminating in what is now known as Superdense Coding, Bennett and Wiesner showed that with the help of an EPR pair, 2 bits of classical information may be transmitted in a single qubit [22] (see [23] for Bennett’s laws addressing the information capacity between qubits, EPR-pairs, and classical bits).

In the following year, Bennett et al. [24] discovered the possibility of teleporting arbitrary quantum information with the assistance of an EPR pair, starting the era of quantum communication.

At this time, an elephant in the room was the lack of useful quantum algorithms that are faster than their classical counterparts. The first-ever quantum algorithm, proved to be faster than any classical algorithm, was Deutsch’s algorithm [13]. This quantum algorithm, without revealing the exact action of $f$, can determine whether a function $f: \{0, 1\} \rightarrow \{0, 1\}$ is a non-constant function, i.e., $f(x) = x$ or $f(x) = x \oplus 1$, where $x$ may be 0 or 1 and $\oplus$ denotes the addition modulo 2 operation. While the algorithm has little merit in terms of practical applications (however, there has been a recent proposal to use this algorithm as a framework for MapReduce [25] in a quantum computer [26]), it was the conceptual leap that pointed the way to how quantum computers may be used for the purpose of outclassing classical counterparts. Followed by an extension of Deutsch’s algorithm from 1 to $n$ binary digits [27, 28], resulting in the so-called Deutsch-Jozsa algorithm [27], it set the standard of what quantum algorithms can efficiently compute.

Sparked by the pioneering works of Deutsch and Jozsa [13, 27], 1994 became a monumental year for quantum-algorithm development. In this year two of the most important quantum algorithms were developed: Simon’s algorithm [29] and Shor’s algorithm [30].

In the formal language of Computer Science, the Deutsch-Jozsa algorithm provided the distinction between the classical and quantum $\mathbf{P}$ complexity classes; $\mathbf{P}$ is the class of problems that a deterministic Turing machine can solve in polynomial time [31].
tinguishing between the probabilistic analogs, i.e., Bounded-error Probabilistic Poly-

omial time and Bounded-error Quantum Polynomial time, was Simon’s algorithm, where,

based on the works of Bernstein and Vazirani [32], Simon in 1994 demonstrated that

a quantum computer running this algorithm can probabilistically solve the following

problem exponentially faster than any probabilistic classical algorithm: For $f$ a function

from $n$-bit integers to $n$-bit integers, find $s$ such that $f(x) = f(y)$ implies $x = y \oplus s$ and

vice versa, where $x$, $y$, and $s$ are $n$-bit integers and $\oplus$ denotes a bit-wise addition [29].

Later Simon’s algorithm was developed into an exact algorithm [33], focusing further

attention on the complexity classes of quantum algorithms.

Shor’s algorithm was different and stirred much attention in the quantum computing

community since it showed, for the first time, that a quantum computer can be used

for solving a practically interesting problem, namely, factoring a semiprime number

$N = p \times q$ into its two prime factors $p$ and $q$ [30], exponentially faster than any known

classical algorithm (c.f. [34–41]). While at a first glance the problem does not seem to be

of much importance, the Rivest-Shamir-Adleman (RSA) cryptosystem [42], one of the

most widely used internet encryption methods, relies on just that, namely the extreme
difficulty of semiprime factorization. Thus, Shor’s demonstration of using a quantum

computer to factor a large semiprime in polynomial time, as opposed to exponential
time on a classical computer, immediately elevated quantum computing to the stage of

a serious and important subject to investigate.

Further generating interest in quantum computing by showing the practical potential of

quantum computing was Grover’s algorithm [43]. Boosting the performance of unsorted
database search from the classically optimal $O(N)$ to $O(N^{1/2})$, where $N$ is the size of the
database, Grover’s algorithm provides optimal quantum database search performance

[44]. While it is less dramatic in its performance boost (square-root advantage) compared
to that obtained from Shor’s algorithm (exponential advantage), Grover’s algorithm,
or “quantum googling”, and Shor’s algorithm, are currently considered the flagships of
practical applicability of quantum computing in real life.
At this point, with a proven record of the immense potential of quantum computing, the physical realizability of quantum hardware became an instant hot topic. Inspired by Lloyd’s introduction of a possible quantum computing architecture in the form of atoms addressed by electromagnetic pulses [45], in 1995, Cirac and Zoller proposed an ion-trap quantum computer hardware architecture [46], where a string of ions stored in a linear Paul trap [47] may be used to perform quantum computations. Together with the discovery by Sleator and Weinfurter [48] and Barenco et al. [49], of the smallest set of universal quantum gates, which consists of a two-qubit CNOT gate and a single-qubit rotation gate, the ion-trap quantum computer, employing a phonon mode as a bus qubit that allows for coupling between any two ion qubits, was shown to be capable of universal quantum computation. A physical realization of the ion-trap quantum computer in the form of a CNOT gate was then announced by Monroe et al. in the same year [50].

In addition to the ion-trap quantum computer, an early list of proposed quantum computer architectures included an NMR quantum computer [51, 52], a spin-based silicon-array quantum computer [53, 54], a one-dimensional heteropolymer Ising-system quantum computer [55], a quantum-dot quantum computer [56], a hyperfine-interaction-based nuclear-spin quantum computer [57], and a cavity electrodynamic quantum computer [58]. With so many possibilities at hand, it was quickly clear to many physicists and engineers that physically viable and practically interesting architectures will need to satisfy several realistic criteria. DiVincenzo was the first to compile a complete list of criteria [59]: A good quantum computer architecture must support (i) scalability, (ii) easy initializability, (iii) long coherence time, (iv) implementability of universal gates, and (v) addressability of individual qubits. Several modifications and improvements were made subsequently (see, for instance, [60] and references therein) and the five DiVincenzo criteria now serve as the foundation for realistic quantum hardware architecture viability.

As is thus evident from the above, the challenges of accurate quantum control were indeed recognized early in the history of quantum computing. Most notably, Landauer
Section 1.3. Current State of the Art

was the first to compile and clearly lay out the challenges that quantum computers will unavoidably face, and must be overcome, namely, manufacturing errors and decoherence [61, 62]. Since then many mathematicians, computer scientists, and physicists have invested much effort in fending off the adversary effects of defects and noise that naturally arise, in particular those of decoherence, and designed and implemented countermeasures in the form of quantum error correction codes. The first to specify explicitly a quantum error correction code was Shor [63], who proposed to encode one-qubit information into 9 physical qubits, attaining the capability of perfectly correcting a general, single-qubit error occurring on any one of the 9 qubits. Following this invention, scores of quantum error correction circuits have been developed to date, including the [7, 1, 3] Calderbank-Shor-Steane code [64, 65] and the perfect [5, 1, 3] code [66] (see [67, 68] for a more extensive list and details).

1.3 Current State of the Art

The pinnacle of quantum error correction codes, arguably, is the Threshold Theorem [68, 69]. This theorem states the following: The overall quantum-information-corruption rate is suppressed below the individual error rate of the components of the error-correction circuit when the error rate is below a certain threshold. Armed with fault-tolerance, i.e., a single-occurrence of an error on one part of the circuit does not proliferate to other parts of the circuit to result in a total corruption of the quantum information [66, 68, 70–73], assisted with the stabilizer formalism [66, 74], whose working principle resembles that of the quantum zeno effect [75], fault-tolerant quantum-error-correction codes bring about surprising resilience of quantum information processing against the undesirable effects of the surrounding environment on a quantum information processor.

The most robust types of quantum error correcting codes known to date, hence the current de-facto standard, is the so-called surface code [76], a type of toric code developed by Kitaev [77, 78] in pursuit of topological quantum computing via anyons [79]. Surface
codes make use of a two-dimensional square-lattice structure as their geometric configuration [80] and a topological braiding transformation over the lattice structure in the form of a CNOT gate [76, 81–84], while being equipped with quantum error detection circuitry with as small of a correction-circuitry overhead as possible [76]. Quantum computers equipped with surface codes are now being experimentally implemented at the basic geometric-configuration level, where a linear configuration of up to 9 qubits [85] and a square configuration of up to 4 qubits [86] have been reported. Other actively investigated architectures, such as an ion-trap simulator [87] or quantum-dot silicon-based quantum computers, have been demonstrated experimentally for up to 14 [88] and 2 qubits [89], respectively.

Modern-day advances in quantum computing are also based on advances in quantum software. Refining quantum-machine language was the invention of the sequence-approximation technique of a single-qubit rotation gate [90, 91] in 1997. According to this technique one decomposes an arbitrary-angle rotation gate into a series of gates drawn from a finite set of quantum gates. This allowed the implementation of more realistic fault-tolerant gate constructions, as only a finite number of gates needed to be fault tolerantly implemented. With the original sequence technique resulting in a sequence-size scaling of $O(\log^c(1/\epsilon))$ with $c > 3$, where $\epsilon$ is the accuracy of the sequence-approximated gate [92], a series of improvements of the technique over the past decade [92–98] culminated in a more favorable $O(\log(1/\epsilon))$ scaling (see, for instance, [92]).

On the assembly-language frontier, starting with the developments of the first architectures of arithmetic logic blocks such as (ripple-carry) adders in the late 20th century [99], a host of quantum arithmetic architectures have been proposed (see Table IV of Ref. [100] for an extensive list). For instance, Beauregard proposed quantum arithmetic units operating in Fourier space, accessed via the quantum Fourier transform [101], which is known to have the smallest required number of qubits for implementing Shor’s algorithm. Culminating in the development of the quantum ALU [102], the quantum software frontier, along with quantum algorithms [103–116], is an active and promising
area of current quantum information research.
Chapter 2

Tapestry

2.1 To Be AND Not To Be: Quantum Superposition

Quantum information devices make use of various quantum effects, among them quantum superposition, which means that a quantum state may be found in a superposition state of basis states. In other words, a quantum system may simultaneously occupy different states that are individually classically observable via measurement.

When one tries to take a look at the superposition state, the measurement device reveals only one of many possible outcomes, namely a single basis state. This is the so-called collapse of the wavefunction. The wavefunction that represents a superposition state can thus be characterized (partially) by the probabilities of collapsing onto certain basis states.

A tempting conclusion from this is to say that a superposition state is a mere mixture of probable classical states. However, this is incorrect. Consider the case of a two-level, spin one-half system. If the initial state is an equi-probabilistic mixture of the two exhaustive, orthogonal, observable states $|\uparrow\rangle$ and $|\downarrow\rangle$, the expected outcome, when measured in a different exhaustive, orthogonal, observable basis, say $|\rightarrow\rangle$ and $|\leftarrow\rangle$, is an
equi-probabilistic mixture, this time of $|\psi\rangle$ states. If, on the other hand, the initial state $|\psi\rangle$ is a linear superposition of the states $|\uparrow\rangle$ and $|\downarrow\rangle$ – whereby, when one subjects the system to a measurement that reveals the up-and-down-ness of the states, there is a 50/50 chance of observing $|\uparrow\rangle$ or $|\downarrow\rangle$ – measuring the state in an alternative basis, e.g., $|\rightarrow\rangle$ and $|\leftarrow\rangle$, would not in general result in a 50/50 chance of measuring $|\rightarrow\rangle$ or $|\leftarrow\rangle$. In fact, if $|\uparrow\rangle$ and $|\downarrow\rangle$ are the two eigenstates of the Pauli $z$ operator and $|\rightarrow\rangle$ and $|\leftarrow\rangle$ are the two eigenstates of the Pauli $x$ operator, such that $|\rightarrow\rangle \sim |\uparrow\rangle + |\downarrow\rangle$ and $|\leftarrow\rangle \sim |\uparrow\rangle - |\downarrow\rangle$, a superposition state that is prepared as $|\psi\rangle \sim |\uparrow\rangle + |\downarrow\rangle$, which would result in a 50/50 chance of observing $|\uparrow\rangle$ and $|\downarrow\rangle$ in the $z$-basis, would result in 100% $|\rightarrow\rangle$ in the $x$-basis. Therefore, we conclude that a superposition state is not a mixed state.

What this implies for quantum computing is powerful: Massively parallel computing. Because a superposition state is a true simultaneous realization of multiple basis states, the possibility of loading a quantum computer with an initial state that is a superposition of basis states that represent all possible input numbers, enables parallel processing of all input numbers simultaneously. Thus, the power of quantum computing stems from the possibility of parallel loading of quantum information, which is typically done in the following way.

Defining a Hadamard gate $\hat{H}$ as $\hat{H}|0\rangle \sim |0\rangle + |1\rangle$ and $\hat{H}|1\rangle \sim |0\rangle - |1\rangle$, where $|0\rangle$ and $|1\rangle$ are the basis states of a qubit, we see that $\hat{H}$ essentially acts to transform a classically observable state $|0\rangle$ or $|1\rangle$ to a superposition state. Initializing now $n$ qubits in the state of $|0\rangle$ for each individual qubit, then applying Hadamard gates to each, i.e., each component system is in the superposition state of $|0\rangle$ and $|1\rangle$, the composite, total system of $n$ qubits, according to a postulate of quantum mechanics [117], is then in the state of the tensor product of the $n$ individual component-system states. At this point, we realize that an $n$-fold tensor product of $|0\rangle + |1\rangle$ results in a superposition state, which contains the entire binary number spectrum ranging from 0 to $2^n - 1$. As a result, we find that we have successfully loaded all possible non-negative integer numbers into an
n-qubit quantum computer.

A natural question now rises: How do we parallel-process the input superposition state? In particular, can we perform a computational task that operates on multiple integer input states simultaneously and whose end result may be useful? For example, starting with a state that contains initially equally distributed number states, can we potentially coalesce and concentrate the probabilities in such a way that the final result contains, e.g., the zeroes of a certain function $f$?

To answer this question, we start by invoking a special kind of multi-qubit superposition state, such as the superposition of $|0\rangle_{I} \otimes |0\rangle_{II}$ and $|1\rangle_{I} \otimes |1\rangle_{II}$, where $|\ldots\rangle_{I}$ and $|\ldots\rangle_{II}$ denote the state of the component systems $I$ and $II$, respectively, and $\otimes$ denotes the tensor product. In this case, we may not factor the composite-system state into a product of the component-system states; rather the component systems are entangled with each other, resulting in an entangled, composite-system state. Quantum entanglement, therefore, allows for a physical representation of two coupled states, such as $|x\rangle$ and $|f(x)\rangle$, each contained in register $I$ and $II$, respectively. In particular, it allows for coupling of a superposition state to yet another superposition state on the basis-state level.

In order to appreciate the potential implication of quantum entanglement, consider a quantum operation which maps $|0\rangle_{I} |0\rangle_{II} \rightarrow |0\rangle_{I} |f(0)\rangle_{II}$ and $|1\rangle_{I} |0\rangle_{II} \rightarrow |1\rangle_{I} |f(1)\rangle_{II}$, where $f$, for the sake of conceptual clarity, is a one-to-one, single-bit to single-bit map, and from here on and in the following we omit the tensor-product notation $\otimes$. If we thus start with a superposition state of $|0\rangle$ and $|1\rangle$ in the first qubit, applying the quantum operation results in entanglement of the first qubit to the second qubit so that the composite system state is the superposition of $|0\rangle_{I} |f(0)\rangle_{II}$ and $|1\rangle_{I} |f(1)\rangle_{II}$. In this case, measuring the second qubit to be in a certain state, i.e., either $|f(0)\rangle_{II}$ or $|f(1)\rangle_{II}$, forces the state of the first qubit to be $|0\rangle_{I}$ or $|1\rangle_{I}$, respectively. What this implies is that, if the result in the second qubit is $|0\rangle$, we have successfully coalesced the probability, out of the possible, classically observable first qubit states $|0\rangle_{I}$ or $|1\rangle_{I}$, into the state that
corresponds to a zero of the map $f$. Should the result in the second qubit have been $|1\rangle$, we would have coalesced the probability spectrum of the first qubit state into the preimage of $f(1)$.

How can this possibly be useful, especially when we do not have any control over which state will be observed? Exploiting quantum superposition and quantum entanglement, together with a clever mathematical construction and tweaking of the problem, we now show that a quantum computer running a certain quantum algorithm can indeed crack the Rivet-Shamir-Adleman (RSA) cryptosystem (a widely-employed encryption technique used in today’s computer networks), exponentially faster than any classical algorithm known to date. Readers who are interested in a brief overview on where the power of RSA comes from are advised to refer to Section 3.1 of Ref. [118]. The description of this quantum algorithm, i.e., Shor’s algorithm, will then be linked to the broader context of quantum phase estimation algorithms (details to follow) and hidden subgroup problems, addressing further the proposition made in Chapter 10 of Ref. [118], i.e., “Any problem that can be turned into a period-finding problem can be (i) efficiently and (ii) reliably solved by a quantum computer”. We will focus on point (i) in this section. Point (ii) will be addressed in detail in the following sections. I discuss here the working principle of Shor’s algorithm, since Shor’s algorithm underlies a major portion of my published works [119–125].

We start with the fact that the RSA cryptosystem relies on the easiness of evaluating $p \times q$ and the difficulty of factoring $N$ into $p$ and $q$ on classical computers. Therefore, the goal of the quantum algorithm is to efficiently factor a semiprime $N = p \times q$ whose two factors $p$ and $q$ are prime. Taking a cue from the classical algorithm known as Robin-Miller’s algorithm [126, 127], we may show straightforwardly that for $x$ that is between 1 and $N$, and is relatively prime, we have $p = \gcd(x^{\omega/2} - 1, N)$ and $q = \gcd(x^{\omega/2} + 1, N)$, where $\omega$ is the minimal number that satisfies $x^\omega \mod N = 1$ and $\gcd$ denotes the greatest common divisor, provided that $\omega$ is even and $(x^{\omega/2} + 1) \mod N = 0$. Thus, given $x$ and $N$, the quantum algorithm would need to be able to efficiently determine $\omega$. For
this we observe that $f(r) = f(r + \omega)$, where $f(r) = x^r \mod N$ and $\omega$ is the period of $f$. We therefore conclude that the quantum algorithm must be capable of efficiently determining the periodicity $\omega$ of $f(r)$.

A straightforward way to determine $\omega$ is to evaluate $f(r)$ for many $r$, and then to look for the periodicity. Classically this is an inefficient task, since to first evaluate $f(r)$ for many different $r$ and then to extract the periodicity, e.g., via a Fourier transform, amounts to an exponentially demanding task in the bit-length $L$ of the semiprime $N$ to be factored [75, 128]. Quantum mechanically, on the other hand, such a task can be achieved efficiently, in polynomial time in $L$ [30].

A quantum computer, as discussed above, may load exponentially many numbers efficiently, using Hadamard gates, via quantum superposition. Then, using quantum entanglement, we may simultaneously process the input superposition state of exponentially many integer basis states in, say, register I to arrive at the composite state of the quantum computer that is the superposition of the states $|r\rangle_I|f(r)\rangle_{II}$, where $r = 0, 1, \ldots, 2^n_I - 1$, the subscripts I and II, as used before, denote registers I and II, respectively, and $n_I$, which scales linearly in $L$ [28], is the number of qubits in the first register. Since at this point we know that for a certain basis state in register II, e.g., $|f(s_0)\rangle_{II}$ for $0 \leq s_0 < \omega$, the coupled basis states of register I include $|s_0\rangle_1, |s_0 + \omega\rangle_1, |s_0 + 2\omega\rangle_1$, and so on, we see that the quantum version of the discrete Fourier transform, i.e., $|s\rangle \rightarrow (1/\sqrt{2^n_I}) \sum_{l=0}^{2^n_I-1} \exp(2\pi isl/2^n_I)|l\rangle$, applied to the first register – requiring only $\sim n_I^2$ quantum operations [118] – results in an output state that is a superposition state of integer basis states whose associated probabilities “peak” at integer multiples of $2^n_I/\omega$, in analogy to the discrete Fourier transform. Thus, the quantum computer can efficiently factor a semiprime $N$ via (i) the quantum modulo-exponentiation $f$ – requiring $\sim L^4$ quantum operations [122] – that entangles exponentially many basis states (in register I) to their individual $f$-mapped states (in register II), grouping the number states in register I that form the preimage of a particular-valued state of $|f(s_0)\rangle$ in register II and (ii) the quantum Fourier transform, which takes the input superposition
state whose exponentially many basis states are periodic, i.e., $|s_0\rangle, |s_0 + \omega\rangle, |s_0 + 2\omega\rangle, \ldots$ that are the fiber of $f(s_0)$ under $f$, and outputs the Fourier spectrum of the input state, useful for determining the periodicity $\omega$.

In short, we have shown that, by virtue of quantum superposition we can load exponentially many numbers, and by virtue of quantum entanglement we can process exponentially many numbers. In particular, with the latter, we have successfully established probabilistic inter-correlations between the zeroes of a function $f - f(s_0)$ for many different $s_0$. In the case of Shor’s algorithm, we found that all preimages of $f - f(s_0)$, regardless of $s_0$, have the period $\omega$ in their respective elements, a fact we exploited via the quantum Fourier transform in order to extract the periodicity.

Spoken now in the broader, algorithmic context, the algorithm at hand may be generalized as follows. We start by pointing out that the first step of modulo exponentiation may be understood as filling up the second register with the elements of a cyclic group $G$ with the generator $x$ in modulo $N$ space, where the associated powers (of the generator) are conditionally applied according to the basis states of the superposition state in register I. This means, essentially, the role of the quantum modulo exponentiation may be thought of as reducing the problem of factoring into finding the order of an element $x$ of the multiplicative group $\mathbb{Z}_N^\times$. Therefore, Shor’s algorithm may be thought of as a quantum algorithm solving a special hidden-subgroup problem, whereby, given a group homomorphism $f: \mathbb{Z}_{2^n} \rightarrow \mathbb{Z}_N^\times$ defined by $f(r) = x^r \mod N$, where $\gcd(x, N) = 1$, one is trying to solve for the order $\omega$ of a seed $x$, which would result in revealing “hidden” subgroups whose elements are for instance $s_0, s_0 + \omega, s_0 + 2\omega, \ldots$, as $f(s_0) = f(s_0 + \omega) = f(s_0 + 2\omega) = \ldots = x^{s_0} \mod N$, equivalent to finding the kernel of $f$.

In the case of Shor’s algorithm, it is important to realize that the overgroup of the hidden subgroups is cyclic. It has been proven that in the case of a cyclic overgroup, there exists an efficient quantum algorithm, such as Shor’s algorithm, solving the hidden
subgroup problem [129]. Furthermore, since any finite Abelian group is isomorphic to
the direct sums of a finite number of cyclic groups, the hidden subgroup problem for
a finite Abelian group can be decomposed into the hidden subgroup problems for its
smaller cyclic groups, thus resulting in (see [130] for detail) efficient quantum algorithms
for solving hidden subgroup problems for finite Abelian groups. This is consistent with
the aforementioned conjecture made in [118]. In fact, the method which the conjecture
refers to is known as the standard method for hidden subgroup problems. An open
question to date is whether efficient quantum algorithms exist for generic non-Abelian
cases, where no such proof is available yet. We note that there are several cases available
in the literature, where some non-Abelian hidden subgroup problems are known to be
efficiently solvable via quantum computing [130].

In any case, going back to the state of the register II after the modulo exponentiation,
this time, we notice that the state contains a superposition of the integer basis states
that correspond to each element of the group $G$, which is an eigenstate with eigenvalue
1 of an operation $g_{x,N}$, where $g_{x,N}(s) = s \times x \mod N$. Going further, inspired by the
eigenstate analysis, we may write down the following list of eigenstates of $g_{x,N}$, which are
characterized by $m$: $|\psi_m\rangle = \sum_{s_0=0}^{\omega-1} \exp(-2\pi is_0m/\omega)|x^{s_0} \mod N\rangle$, where the associated
eigenvalues are $\exp(2\pi im/\omega)$.

How does generalizing the algorithm entail this? Let us take a look at how one would indeed
realize Shor’s algorithm. Since a modulo exponentiation $x^r \mod N$ is nothing but a
series of modulo multiplications, i.e., $x^r = x^{2^0r_0}+2^1r_1+...+2^n r_n$, where $r_\nu$ denotes the
$\nu$th binary digit of $r$, we see that the corresponding quantum circuitry would involve first
the initialization of the register I to a superposition state of $|r\rangle$ for $r = 0, 1, ..., 2^n - 1$ and
the register II to $|1\rangle_{II}$, then the consecutive controlled-multiplication operations, which
apply $x^{2^\nu}$ on the register II if, in the controlling first register, $r_\nu = 1$. Now, if instead
register II were to be initialized to one of the eigenstates $|\psi_m\rangle_{II}$ (via whatever means,
which are not important for now for reasons to become clear later), the modulo exponen-
tiation circuitry would then result in a superposition state of $\exp(2\pi imr/\omega)|r\rangle_1|\psi_m\rangle_{II}$ for
The first register state, however, is nothing but a Fourier-transformed state of $|m2^n/\omega\rangle_1$ [if $\omega$ is a power of 2; if not, the first register is an approximate Fourier-transformed state of an integer state close to $|m2^n/\omega\rangle_1$ (see [28] for a detailed discussion)]. Thus, we realize that extraction of the phase angle is achieved when we take the inverse quantum Fourier transform. Now, this is relevant because the phase contains the information that we desire, namely the periodicity $\omega$. Most importantly, $\omega$ appears regardless of $m$. Therefore, a linear superposition of $|\psi_m\rangle_{\text{II}}$ as an initial input state of register II would work just as well when it comes to extracting $\omega$. Together now with the revelation that the original input state $|1\rangle_{\text{II}}$ in register II is in fact $\sim \sum_m |\psi_m\rangle_{\text{II}}$, to this end, we proved that a generalization of Shor’s algorithm leads to the phase-estimation algorithm.

So far, we primarily focused on the problem of quantum information processing. But what about quantum information extraction? In the end, one must take the resulting quantum information and use it for something, such as factoring.

The process of measurement is best described phenomenologically by the Born Rule [131], i.e., the state $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$ has probability $|a_0|^2$ and $|a_1|^2$ of collapsing onto $|0\rangle$ or $|1\rangle$, respectively. This may be well known and perhaps even be axiomatically trivial to many physicists. Nonetheless, this, in retrospect, in the context of quantum information processing, has tremendous importance: Sharpness.

Imagine that we try to implement the Fourier transform with $2^{300}$ input numbers with an analog device such as organ pipes. Sound waves can be superposed and can even be (classically) entangled. The only problem is that they are not quantum in nature, i.e., when we poke the apparatus, a collapse of the acoustic wave does not occur. This is extremely bad news for information handling since we would end up with too much data with insufficient accuracy; imagine a Fourier spectrum of sound with $2^{300}$ output amplitudes and we are trying to locate a single peak with $1$ in $2^{300}$ precision! Quantum mechanics does this job naturally and automatically, where the (absolute square of the)
amplitudes correspond to probabilities of observing a certain state. The importance of this quantum effect, therefore, cannot be overemphasized.

On the other hand, while, without the possibility of this curious extraction mechanism, we would not be able to use quantum computing, in the presence of unwanted measurements, quantum computing would be doomed. This is so, because we need to keep the quantum-ness of the quantum computation, namely superposition and entanglement, mostly intact throughout the entire duration of the quantum computation until the point where we actually want to measure. In light of the delicate nature of these quantum effects, an important question must now be answered: Can we build a practically useful quantum computer in the presence of these adverse effects that may induce unwanted measurements before the quantum computation is over?

2.2 To Be OR Not To Be: Practical Quantum Computers

In order for us to attack the problem of handling unwanted effects in a quantum computer, we take a step back to where we know what to do: Classical error correction. We will not delve into the details here since it is our aim to simply take the idea of error correction from the classical realm and to apply it in quantum computing in a rudimentary way to see whether error correction is indeed possible and, if so, what the limitations are. Readers who are interested in pursuing this direction as an active research direction may refer to the literature that is cited in this section. For those who are interested in the general area of quantum error correction, Ref. [68], for instance, is a good starting point.

Let us start with the most trivial example of an error-detection code, a parity-check code. In the most elementary case, each message (i.e., a bit string) is constructed in such a way that the sum of the message bits adds up to, say, 0 (mod 2). Hence, if
the receiver of the message finds that the sum of the message bits is 1, the receiver knows that there must have been some corruption of data that occurred on the way from the sender to the receiver, and may instruct the sender to re-send the message. Of course, in this particular case, the receiver does not know which bit(s) of the string are corrupted. In fact, the receiver is unable to detect an even number of bit-flip errors during transmission, since the parity of the received bit string would be even in this case. The point is that this method, as can also be shown to be true for other more complicated techniques, including error correction codes, relies on the fact that there is far less chance of, say, a two-bit error occurrence than a single-bit error occurrence, resulting in a mostly reliable channel.

The same principle applies to quantum information. Just as in the case of classical error correction, there does not exist a perfect quantum error correction code. Rather, the quantum error correction code, in analogy to the example discussed above, can correct only errors that have a higher chance of occurrence, while not being able to correct other errors that have a lower chance of occurrence.

What this means is the following. Obviously, if one wants to implement correction circuitry, the implementation will most definitely complicate the circuit, compared to a bare bones circuit. Thus, error correction circuitry introduces many more ways in which the desired circuitry may be perturbed and corrupted. Therefore, one has to weigh the benefits of the correction circuitry versus the consequences of the complications that it introduces. A straightforward analysis, assuming errors of a stochastic kind, such as the aforementioned bit-flip errors, when applied to a quantum computer, results in what is known as the Threshold Theorem, which states (roughly) that a quantum computer equipped with quantum error correction circuitry performs better than its bare-bones counterpart when the occurrence probability \( p \) of, say, a single-qubit error is less than a certain threshold \( p_{\text{threshold}} \).

Taking one step further, we know from classical error correction that the power of error
correction arises from redundancy. Now, for quantum computing, introducing redundancy is impossible because of the No-Cloning-Theorem, which states that it is impossible to clone an unknown, arbitrary quantum state \([7]\). This is a direct consequence of the unitarity of quantum mechanics and hence a circumventing method must be devised. To this end, we recall the action of a CNOT gate, defined as 
\[ |0\rangle_c |x\rangle_t \rightarrow |0\rangle_c |x\rangle_t \]
and 
\[ |1\rangle_c |x\rangle_t \rightarrow |1\rangle_c |x \oplus 1\rangle_t, \]
where \( |\ldots\rangle_c \) and \( |\ldots\rangle_t \) denote the control and target qubit states, respectively, \( x \in \{0,1\} \), and \( \oplus \) denotes addition modulo 2, i.e., the action of an XOR gate. In other words, a CNOT gate flips the state of the target qubit if the control qubit is in the state \( |1\rangle_c \). The significance of this is appreciated when we consider 
\[ |\psi\rangle_c = a_0 |0\rangle + a_1 |1\rangle \]
and 
\[ |\psi\rangle_t = |0\rangle \]
and operate with a CNOT gate. This results in the final state 
\[ a_0 |0\rangle_c |0\rangle_t + a_1 |1\rangle_c |1\rangle_t, \]
which is nothing but the entangled state between two qubits discussed earlier in Sec. 2.1. What we see here is that while we are not allowed to make a copy of the given arbitrary state, we are well allowed to entangle as many qubits with the given state as we want, which, in a (quantum) computational sense, can be exploited to detect and/or correct a potential error that may occur locally on, say, one of the many qubits via a mechanism that resembles a majority vote.

This means, that in order to realize quantum error correction circuitry, one needs multiple qubits to encode and protect one quantum bit of information. Therefore, we now make distinctions between a physical qubit, which is a bare-bones unit of quantum information and a logical qubit, which is the encoded unit of quantum information, represented by multiple entangled physical qubits. For a logical qubit to properly function, then, we would need to map out the correction-technique-specific encoding and decoding circuitry in addition to logical quantum gate operations on the physical qubit level.

This leads us to the topic of fault tolerance. Obviously, building circuitry that consists of many physical qubits and many gate operations to protect a logical qubit is costly. In fact, we would like to make the circuitry as streamlined as possible since, if the circuitry becomes overly complex, we would have too many ways that errors and defects can
channel in. In this spirit, we want to avoid infestation of the circuitry with errors across multiple qubits that may originate from a single, local error. This is best illustrated when we consider a bit-flip error on the control qubit of a CNOT gate. Compared to the desired error-free result without the bit-flip error, we end up with both control and target qubits that are now in the incorrect, flipped state. Building a quantum error-correcting circuit that can handle multiple errors requires much more demanding resource investments. Thus, we now introduce the notion of fault-tolerant quantum computing: “An operation is said to be fault-tolerant if the occurrence of a single gate error or storage error during the course of the operation produces no more than one error in each (code) block” [68].

This implies that within a logical qubit one should avoid using a two-(physical)-qubit gate, as this may create a new error from a potentially already corrupted physical qubit on the other. This motivates us to consider a logical-gate operation that consists of a parallel operation of a physical gate, applied to individual physical qubits that comprise the logical qubit. This way, should a single qubit out of many in a given logical qubit be compromised, the error will not corrupt other physical qubits in the logical qubit. This method of parallel operation is known as a transversal operation [132], and it epitomizes fault-tolerant design in quantum computing.

A two-qubit gate such as a CNOT gate may also be transversally applied between two logical qubits by means of applying physical CNOT gates across pairs of physical qubits that occupy the same place within each of the two logical qubits. The next question is then whether such a transversal operation will indeed lead to the desired logical operation. Unfortunately, not all quantum gates allow a straightforward, transversal implementation in quantum error correction circuitries. In fact, for different architectures of quantum-error corrections, transversally implementable gate sets are different. This leads to the idea of reducing the number of types of quantum gates that need to be realized, since the smaller the number of types the more the chance that we may be able to implement most, if not all, of the necessary quantum gates transversally. To this
end, we introduce the standard set \cite{133}, that consists of a CNOT gate, a Hadamard gate, and a T-gate, where a T-gate denotes a phase-rotation gate with phase-rotation angle $\pi/4$. Compared to the universal set of quantum gates, the standard set replaces the general phase-rotation gate $\theta$ with the $\pi/4$-gate, T. This may come as a warning sign that we may not be able to, for instance, realize a phase-rotation gate with a general phase-rotation angle (which, indeed, is a problem for some applications) but this is not the focus of the current investigation. There have been extensive studies regarding how the general phase-rotation gate may be built from the standard set \cite{92, 95–98, 134}, leading, most significantly, to the Solovay-Kitaev theorem \cite{90}. The important thing is that (approximate) universal quantum computing may be achieved with the standard set to an arbitrary precision (more details in Sec. 2.4).

Regrettably, in Refs. \cite{132, 135, 136}, it has been shown that no quantum error correction codes [of the kind known as stabilizer codes (see below for details)] supports the transversal implementation of all quantum gates necessary for universal quantum computing or even its approximate. This means that one has to devise custom-made fault-tolerant designs, if desired, of those quantum gates that cannot be implemented transversally under a certain quantum error correction circuitry. While this is not an impossible task to do, it does complicate the circuitry, adding to the concern that it may entail more harm than benefit in fending off quantum data corruption.

Summing up, we discussed how we can perform quantum computations fault-tolerantly in logical space. At this point, we recall the reason behind going to logical space: We want to take advantage of the possibility of correcting quantum information corruptions. To this end, we introduce a central idea in the current discussion of quantum error correction, i.e., the stabilizer formalism.

The source of inspiration is once again classical error correction. In analogy to classical linear codes, where one obtains distinct signals, namely, error syndromes, depending on the errors that may have occurred over the course of time (imagine some clever
parity-check codes, where one can actually determine in which locations bit-flip errors may have occurred via probing the encoded message in a variety of ways), quantum error correction codes may be constructed in such a way that error syndromes may be extracted from encoded quantum information, should certain errors occur. This is best and most straightforwardly achieved by exploiting the mathematical properties of Hilbert space spanned by multiple qubits, where one can find a group of operators known as stabilizers of a unique subspace of the Hilbert space. The stabilizers form a commutative (Abelian) group and all vectors in the corresponding, unique subspace are the eigenvectors of the stabilizers with eigenvalue 1. This is similar to classical linear codes, where the encoded messages or codewords form the kernel of the parity-check operator. In essence, the stabilizers, if operated on the ideal, uncorrupted, encoded quantum information, leave the information intact, while they would raise a flag, should there have been a certain error. Interestingly, if the encoded state vector becomes slightly off, the stabilizer would “stabilize” the state by virtue of realigning the tilted state back to the supposed, correct axis with high probability.

To better see this on a more quantitative level, consider the Bell states $|\uparrow\rangle_I|\uparrow\rangle_{II} + |\downarrow\rangle_I|\downarrow\rangle_{II}$, $|\uparrow\rangle_I|\downarrow\rangle_{II} - |\downarrow\rangle_I|\uparrow\rangle_{II}$, $|\downarrow\rangle_I|\uparrow\rangle_{II} + |\uparrow\rangle_I|\downarrow\rangle_{II}$, and $|\downarrow\rangle_I|\uparrow\rangle_{II} - |\uparrow\rangle_I|\downarrow\rangle_{II}$, where $|\uparrow\rangle$ and $|\downarrow\rangle$ are the eigenbases of $\hat{Z}$ and I and II denote the first and second qubits, respectively. The stabilizers are $\hat{Z}_I\hat{Z}_{II}$ and $\hat{X}_I\hat{X}_{II}$ and we can show that $\hat{Z}_I\hat{Z}_{II}$ operated on any one of the states returns the state itself (and the same holds true for $\hat{X}_I\hat{X}_{II}$). In this particular case, however, a flip-type error cannot be detected, since a flip would send a Bell state to another Bell state. In fact, one needs at least three qubits to correct a bit-flip error in a quantum circuit [69].

All is well, but for one thing: So far, we assumed stochastic errors. In particular, quantum error correction codes were built based on the assumption that, apart from the locally occurring errors, all the rest of the components of the circuitry work perfectly. However, in the real world, everything is flawed.
What happens to the quantum error correction circuitry when every single component is flawed? The answer is clear: Just as in the case of classical error correction, quantum error correction will have a non-zero chance of failing. We must readily admit that this will always be the case without any exception since in principle there does not exist perfectly accurate and precise hardware in nature.

In fact, there has been a growing concern recently within the quantum computing community that this issue of inherent hardware flaws must be taken much more seriously than previously thought. In anticipation of technological breakthroughs that would allow to conduct experiments with error rates close to the aforementioned threshold [137–147], many researchers in quantum computing are currently investigating ways in which we can reliably and efficiently characterize the quality of the quantum hardware. In particular, there has been a recent rise in the number of publications addressing the effect of coherent or unitary errors in quantum information processing [148–153]. Thus, at this time, one of the main topics of interest of the quantum computing community is focused on investigating quantum hardware defects, where experiments and numerical simulations can be directly compared, mostly at a single-qubit gate level.

Now, in order to shed light on this issue of coherent errors at a conceptual level, we consider the following simple example: A dial. The quality of a dial is characterized by its tunability. A good dial would then have the finest possible tunability. Consider now the chance we have to turn this dial by an exact, pre-specified angle, say $\theta = \pi$. The answer: The chance to hit $\pi$ is exactly zero.

One may ask, at this point, whether we can re-zero and/or re-calibrate our device to hit the mark better next time. While some improvements can indeed be made (see, e.g., [154]), the answer to the question of what the chance is to hit the mark exactly, is, once again, 0. This is so, because if we were to be able to measure and perfectly correct the errors, we would have to have a measuring device that is reliable down to infinite precision with infinite accuracy. This is impossible, even in principle. The conclusion
we draw from this is that the task of turning a dial by a specified angle is fatally flawed. It cannot be accomplished.

2.3 Robustness of Quantum Information Processors

So, is practical quantum computing impossible?

It may seem so, based on our observations delineated above. However, we did not consider one important thing: The whole is greater than the sum of its parts. Sure, it may be so that each individual component of the quantum computer may not be built to specification, ever, but what about the entire computer? Perhaps the whole quantum computer will function satisfactorily even with faulty parts?

In this section, following the line of arguments above, we tackle the issue of approximate quantum computing. As will be shown, quantum computers turn out to be exceptionally robust, to the surprise of many, against errors and defects.

The first thing to do is to identify which components will most likely be the bottlenecks. To this end, we take a look at the universal set of quantum gates that consists of a CNOT, gate, a Hadamard gate, and a single-qubit rotation gate. While none of these gates, as quantum gates, are “easy” to realize, the phase-rotation gates are the most difficult to realize (see below), in particular when the phase-rotation angle is very small.

Consider a phase-rotation angle $\theta$ that is of the order of $\pi/2^{300}$. This gate would need to be implemented on our quantum computer if we wish to realize, for instance, a 300-qubit quantum Fourier transform, a modestly-sized quantum circuit, given that we would need a quantum computer with thousands of qubits in order to use this quantum computer to factor a 2048-bit semiprime, for example. While needed in this context, realizing a $\pi/2^{300}$ gate is, unfortunately, impossible, even in principle. Therefore, the first thing we try is the following. Can we get away with removing those phase-rotation gates whose rotation angles are smaller than a certain threshold value? Can we still obtain
satisfactory results with such pruned circuitry?

Defining banding [119–122] as a systematic method to remove phase-rotation gates with rotation angles smaller than $\pi/2^b$, where $b$ is the bandwidth, we applied the banding operation to one of the most prominent quantum algorithms, namely, Shor’s algorithm. Shor’s algorithm consists of (i) modulo-exponentiation and (ii) period-finding parts, where banding may be applied to the two parts individually. Detailed derivations and analyses may be found in Refs. [119–122]. Below are the core results.

- **Period-Finding with Banding**: For this case, we assume that the modulo-exponentiation part of Shor’s algorithm, whose operation yields the $\omega$-periodic superposition state, $\sum_k |s_0 + k\omega\rangle$, where $0 \leq s_0 \leq \omega - 1$ and $k = 0, 1, \ldots$, operates perfectly. This way, the last part of Shor’s algorithm, namely, the period-finding part, is provided with an input state that is perfectly periodic. Provided with such an input state, analytically, we find that the period-finding bandwidth $b_{PF} = 8$ is sufficient for factoring a 2048-bit semiprime [120], posing a grave threat to cybersecurity (see Table 4 of the National Institute of Standard and Technology document [155]; a 2048-bit semiprime is the recommended standard until 2030). This choice of bandwidth also allows for saving more than 99.6% of the total number of phase-rotation gates in the period-finding part of Shor’s algorithm (or 8,353,828 gates) when factoring a 2048-bit semiprime, greatly assisting experimental realization.

- **Modulo-Exponentiation with Banding**: This time, we apply banding throughout the entire Shor’s algorithm. This is best achieved when we employ a Fourier-adder architecture [101] in the modulo-exponentiation circuitry, where the arithmetic circuits make use of quantum Fourier transforms, which consist mostly of phase-rotation gates, and quantum Fourier adders, which consist entirely of phase-rotation gates (see, for instance, Figs. 1 and 3 of Ref. [122]). Factoring integers of up to 57 [122], using numerical codes that honestly implement the entire algorithm, quantum-gate–by–quantum-gate, exactly as laid out in the quantum circuit
diagram of Shor’s algorithm, together with the evidence from the previous case of banded period-finding, we are able to deduce that the modulo-exponentiation bandwidth \( b_{\text{ME}} = 8 \) is sufficient for factoring the current security standard of 2048-bit semiprimes. This choice of bandwidth results in saving more than 99\% of the total number of phase-rotation gates, or 314,378,411,210,788 gates, when factoring a 2048-bit semiprime [122], a boon anticipated to be most definitely welcome by experimentalists who seriously consider implementing a practically interesting quantum computer. We also note that these quantum-computer simulations on a state-of-the-art cluster computer took us up to three months of computation time and 16 terabytes of memory per individual run. Thus, the banding operation is of tremendous importance to numerical methods as well, enabling the feasibility of numerical investigations, given limited computational resources.

We conclude, based on our findings above, that banding is an extremely efficient way of approximating quantum circuitry.

We now move on to imperfect phase-rotation gates. As has been argued before, there does not exist a perfect dial. This means that all of our phase-rotation gates should reflect such real limits. To this end we introduce two parameters that reflect inaccuracy and imprecision, respectively, in order to investigate the robustness of the quantum Fourier transform with respect to imperfectly realized gates. Below is a summary of the results of the investigation. Readers who are interested in additional technical material and a detailed account of the study may refer to Refs. [123, 124].

- **Inaccuracy.** While, ideally, one would hope to implement a phase-rotation gate with a realized phase-rotation angle that is as close as possible to the pre-specified amount, obviously, due to the limitations of any physical device, this is impossible. Therefore, to model incorrect zeroing of the device, we introduce an offset parameter \( \delta \), such that the ideal phase-rotation angle \( \theta_j = \pi/2^j \) is replaced by the non-ideal phase-rotation angle \( \tilde{\theta}_j = \delta/2^j \). This way, the ideal case corresponds to
$\delta = \pi$ and the inaccurate implementation of the phase-rotation gate is captured by $\delta \neq \pi$. When this inaccuracy model of the phase-rotation angle is introduced into the quantum Fourier transform, we find that the performance of the quantum processor, as expected, diminishes as $\delta$ moves away from $\pi$, resulting in a peak structure of the performance as a function of $\delta$ around $\delta = \pi$. The natural question to ask is then whether this peak will narrow as a function of increasing number of qubits, since, should this be the case, scaling up the quantum circuitry will require implementation of evermore accurate phase-rotation gates, ultimately prohibiting us from going toward a number of qubits that is of practical interest. Fortunately, we confirm numerically and analytically that the width of the peak is independent of the number of qubits, instilling us with the hope that a reasonably small offset in the phase-rotation angles of the phase-rotation gates, that may naturally arise, will not be a major hurdle for practical quantum computing.

- **Imprecision:** Having dealt with the incorrect zeroing part, we now address the precision issue of the phase-rotation gate. Following the main theme of the investigation, i.e., there exists no perfect hardware in nature, we model the imprecision of the phase-rotation gate with random perturbations imposed on the ideal phase-rotation angle. We are able to show in Refs. [123, 124] that the quantum Fourier transform, now reflecting the imprecision of the phase-rotation gates, performs satisfactorily in the presence of such random perturbations. In particular, the performance scales like $\sim \exp(-\gamma \epsilon^2)$, where $\gamma \sim \log(\omega)$ is a fit parameter that depends only on the periodicity $\omega$ of the input state of the quantum Fourier transform (recall the purpose of this quantum processor; we want to reveal the embedded periodicity $\omega$ of the input state $|\psi\rangle \sim |0\rangle + |\omega\rangle + |2\omega\rangle + \ldots$, for instance) and $\epsilon$ denotes the strength of the random perturbation (see Ref. [124] for technical details). Applied to the period finding part of Shor’s algorithm, since $\omega \sim N/5$ on average [120], where $N$ is the semiprime to be factored for code-breaking, Shor’s algorithm, equipped with imprecise phase-rotation gates in the period-finding part,
performs according to \( \sim \exp[-\eta(N, \epsilon)] \), where \( \eta(N, \epsilon) \sim \log(N)\epsilon^2 \). This is an encouraging result, since \( \log(N) \) is proportional to the bit-length of the semiprime \( N \) and thus the random perturbation strength \( \epsilon \) needs only be kept below an amount comparable to the square-root of the bit-length of the semiprime.

All together, we showed that the quantum Fourier transform, subjected to unavoidable, naturally occurring inaccuracy and imprecision of the phase-rotation gates, functions satisfactorily even when we scale up the number of qubits to the regime that is of practical interest. We also note that the case of both inaccurate and imprecise rotation gates is well approximated by considering the inaccuracy and imprecision separately, then combining the two resulting performances via products, an expectedly excellent approximation, given that the offset and the random perturbations are statistically independent.

So far, we investigated the sensitivity of quantum processors with respect to the shortfall of individual gates in meeting the standard specification. The results were striking in that the quantum processors are unexpectedly robust against these naturally present flaws. This motivates the investigation of the general, structural integrity of quantum processors (see below and Ref. [156] for details). The stability of the quantum Fourier transform under several structural perturbations was tested in the following way.

- **General Exponential Hierarchy** \( \theta_j = \pi/2^j \rightarrow \tilde{\theta}_j = \pi/(\alpha^j) \): The reason for why the quantum Fourier transform circuitry contains exclusively phase-rotation gates with rotation angles \( \pi/2^j \) is because of the binary nature of quantum computing, manifested by the presence of \( 2^j \) in the denominator of the angle. This is a logical, but artificial choice. Therefore, borrowing the term “structurally stable” from dynamical systems theory, which denotes the situation, in which one gets essentially the same dynamical behavior if one perturbs the functional form of the dynamical system, we perturb the binary-ness of our system by replacing the binary-based phase-rotation gates with real-number-system-based phase-rotation gates. To illustrate, consider the case \( \tilde{\theta}_j = \pi/3^j \); the resulting set of numbers forms
the number system $\nu = \sum_j \phi_j (1/3)^j$, where $\phi_j$ may be 0 or 1. It is isomorphic to the middle-thirds Cantor fractal [157] and, of course, is unusual in the context of binary computing. Therefore, this type of structural perturbation provides a significant test for the robustness of quantum processors. To this end, Fig. 3 (a) of Ref. [156] shows both numerical and analytical results, which point to the fact that, indeed, the quantum Fourier transform is structurally stable in the general exponential hierarchy.

- **Power-law Hierarchy** $[\theta_j = \pi/2^j \rightarrow \tilde{\theta}_j = \pi/(2j)^\beta]$: Continuing the structural stability test of the quantum Fourier transform, this time we consider a power-law hierarchy. The corresponding number system is far from a conventional one, such as the familiar base-2 system (exponential hierarchy), and thus forms a whole new subject of fundamental investigation from the number-theoretic point of view. Nevertheless, regardless of the exact mathematical nature of the corresponding number system, the phase-rotation gates in the quantum Fourier transform can be replaced with these power-law gates and may be investigated. The relevant numerical and analytical results appear in Fig. 3 (b) of Ref. [156]. Remarkably, the quantum Fourier transform, equipped with phase-rotation gates that follow this highly non-trivial hierarchical structure, still works at above $90\%$ performance, even when the circuit is of an appreciable size, say, 20 qubits.

- **Logarithmic Hierarchy** $[\theta_j = \pi/2^j \rightarrow \tilde{\theta}_j = \pi/\log_\gamma(j + 1)]$: In order to be sure that the observed structural stability of the quantum Fourier transform is not just some happy coincidence arising from accidental choices of the two aforementioned hierarchies, we tested yet another hierarchy, this time based on logarithms. Astonishingly, a 12-qubit logarithmically-modulated quantum Fourier transform processor functions at above $60\%$ performance. The full numerical results may be found in Fig. 4 of Ref. [156]. Based on this observation, we conclude that the quantum Fourier transform is structurally stable.
This astonishing result corroborates the very claim made at the beginning of this section, namely, the whole system of an entire quantum processor is more than just a collection of individual gates. However flawed, or altered, the gates may be (even when we perturb the structure of the hierarchy of the gates in the quantum circuit), the quantum computer, to a surprising degree, performs.

This is in stark contrast with a classical computer, where, for instance, removing a single logical gate from a billion-gate processor makes this processor useless. So, in order to test the ultimate resilience of the quantum computer, we subjected the quantum circuitry to a random hierarchy [158].

- **Uniformly Random Hierarchy**: Let us suppose, for some reason, perhaps due to some random spacings available between atomic transition lines, we have the ability to access random quantum gates. In particular, we assume that we have access to phase-rotation gates whose phase-rotation angles may be random. In this case, we may order the elements of the sample set of size $N$, drawn from the randomly distributed population, to best-match the pre-specified phase-rotation angles $\theta_j = \pi/2^j$, while allowing repetition. If the random distribution of the angles follows a uniform distribution in $(0, \pi)$, we refer to this case as the uniformly random hierarchy case. At first, this sounds too crude to work since, after all, we are dealing with a computer. How can a collection of gates drawn from a random set be used to result in reliable computation? The key lies in the rapid approximation of $\theta_j$ as a function of the size $N$ of the random sample, where the best-matching angle from the sample is, on average, only $\pi/N$ away from the ideal angle $\pi/2^j$. Analytical results, which are in excellent agreement with numerical results, show that, indeed, one only needs a size $N$ of the random set which is of the order of the size of the quantum circuitry $n$ to obtain satisfactory quantum processor performance. For instance, $N = n$ yields about $\sim 70\%$ quantum Fourier transform performance, and $N = 2n$ yields about $\sim 15\%$ quantum (Fourier-based) adder performance, for large $n$. 
• **Exponentially Random hierarchy:** We notice, however, that, in the case of the aforementioned uniformly random hierarchy, the best-matching angle from the sample would fare badly when trying to approximate a large \( j \), small \( \theta_j \) gate. This is so, because, as pointed out above, on average, the uniformly random hierarchy method can only approximate as close as \( \pi/N \) away on average from the ideal angle \( \pi/2^j \). Hence, for \( j \) that yields \( 2^j > N \) for a given \( N \), the uniformly random hierarchy method produces approximate gates that are more than 100% off on average. Circumventing this, we may employ, for instance, a random set in the exponent \( j \) of the phase-rotation angle \( \pi/2^j \), ensuring comparable percent differences in the approximate and exact gates for all \( j \). We refer to this method as the exponentially random hierarchy method. Interestingly, perhaps contrary to expectations, the exponentially random hierarchy case fares worse than the uniformly random hierarchy case in the limit of large \( n \) [see, for instance, Eqs. (3) and (41) of [158]], the practically interesting regime. In contrast to the uniformly random hierarchy case, where we only needed \( N \sim n \) for a satisfactory performance, in the exponentially random hierarchy case, we need \( N \sim n^{3/2} \) to result in a comparable performance.

The important insight we gain from this seemingly, purely-academic study of the random hierarchy is that it is far more important to focus on realizing large phase-rotation gates (small \( j \)) than putting much effort in realizing small phase-rotation gates (large \( j \)) while sacrificing the quality of the large phase-rotation gates. Motivated by this, we conducted banding on the uniformly random hierarchy case in [158], since banding removes the small phase-rotation gates that are not well-approximated by the uniformly random hierarchy method. A pleasant surprise: a boost of quantum processor performance is observed.
2.4 Optimization and Performance Boost: Sensible Quantum Computing

The performance boost by banding in the presence of imperfect gates may be understood in the following way. Let us once again consider a tiny phase-rotation gate whose phase-rotation angle is of the order of $\pi/2^{300}$, an impossibly small quantity. In this case, if an experimentalist nevertheless implements the gate as instructed by the blue prints of the quantum circuitry, the effect of the futile attempt will at best be some random phase rotation. Hence, we are better off simply not to implement the gate, should the difference between the random phase-rotation angle and the specified phase-rotation angle exceed the value of the phase-rotation angle of the gate itself that we are trying to implement.

This means that there exists a tug-of-war between banding away the proliferation of phase-rotation-gate errors that boosts the performance of the quantum processor and removing essential gates that would diminish the performance. Therefore, for a given error level, there exists an optimal bandwidth. The analytical formula of the optimal bandwidth as a function of the error level is reported in Ref. [158]. For a typical error level of $\sigma = 10^{-3}$ of Gaussian noise in the phase-rotation angle, the optimal bandwidth is 12.

Similar types of optimizations of quantum circuitry can be found in several other areas of quantum computing. Let us, for instance, consider the case of the Solovay-Kitaev Theorem, briefly discussed in Sec. 2.2, with respect to approximate quantum computing with the standard set of quantum gates. Since the standard set lacks a general phase-rotation gate as an element, and since universal quantum computing can only be achieved with the ability of implementing a general phase-rotation gate, a truly exact universal quantum computation cannot be achieved with a finite number of gates drawn from the standard set. This means, when it comes to universal quantum computing with
the standard set, one has to compromise between the inexactness of the computation and the additional effort one must spend in potentially better approximating the universal, exact quantum computation. This potential is typically realized by the so-called sequence approximation technique [92, 95–98, 134], where one decomposes a general phase-rotation gate into a sequence of standard gates that are cleverly assembled. It is here where optimization is once again important.

Even the standard gates, whilst taking full advantage of fault-tolerant error correction technology, are subject to errors and flaws, since they are part of nature. As is the case for any serial implementation of operations, repeatedly using uncontrollably flawed parts, yields accumulation of errors. Thus, the quality of the aforementioned sequence approximation technique, implemented with the necessarily flawed standard gates, deteriorates, as the length of the sequence becomes larger. This deterioration directly competes with the better approximation obtained from a longer sequence, once again resulting in a tug-of-war. Both analytical and numerical analyses indeed point to the existence of an optimal length of the sequence, detailed in Ref. [159].

Yet another area of quantum computing where optimization may arise is the rate at which one calls upon quantum error correction circuitry. Typically, the literature instructs us to apply quantum error corrections as often as possible, to make sure that no non-correctable error occurs from, say, accumulation of multiple errors. However, this assumes that the error correction circuitry is composed of perfect hardware. Since the circuitry itself is a source of errors, if the rate of the errors that the correction circuitry is trying to protect the quantum processor from is lower than the rate at which the correction circuitry itself introduces errors to the quantum computer, it makes sense not to apply the correction circuitry at every possible opportunity.

Basic steps toward this type of optimization have already been taken, mostly by Weinstein [160–163], where, in the presence of the aforementioned stochastic, flip-type errors, one may optimize a certain type of quantum error correction circuitry by investigat-
ing the response of the circuitry with respect to the frequency of correction [160, 161], the subcircuit structure regarding ancillary qubits [162], and the ordering of correction circuitries [163]. All of the studies, however, focus on stochastic errors, and, at present, the influence of hardware errors remain to be tested. In addition, the current state of the art remains at the single logical qubit level, and it remains to be seen how this type of optimization can also be employed in multiple-qubit environments. While many in the quantum computing community believe that the stochastic kind of errors are more detrimental to quantum computing than the unitary hardware errors, given the error-correction circuitry designed to fend off the stochastic errors, considering the majority-vote-like mechanism of the error correction, multiple-qubit, practically interesting quantum computers may paint a different picture. Preliminary results show that optimization at the quantum-Fourier-transform level is possible [164].

So far we discussed how optimization may be achieved at the hardware level, i.e., we addressed the problem of implementation of quantum gates on the basis of the individual-gate error rate. Hence, we now ask: Is there a way of optimization that may be performed at the software level? The answer is yes and in the following we demonstrate several mechanisms in the context of the familiar Shor algorithm (see Sec. 2.1).

We start by reiterating that Shor’s algorithm consists of the modulo-exponentiation part and the period-finding part. Since a modulo-exponentiation is nothing but a sequential application of modulo-multiplications, and since a modulo-multiplication is nothing but a sequential application of modulo-additions, we arrive at a quantum circuit of Shor’s algorithm that consists of multiple modulo-addition gates. Now, since we want our circuit to have a reasonable size – as we should, since we want to reduce the resource costs (given the bit-length $L$ of the semiprime to factor, we would like our circuit to have no more than, say, $\sim L$ in its number of qubits). This effort in keeping the number of qubits as small as possible in its scaling in $L$ is well justified, given that the coherent error channels will grow in the number of parameters that characterize a unitary operator of size $n^2$, where $n$ is the total number of qubits in the quantum processor.
In order to achieve this, however, we would need to reinitialize any work-space qubits used during our computational steps. Because of quantum entanglement, however, the reinitialization process is not as straightforward as simply perturbing the workspace qubits and then resetting the state to whatever is desired; we need to construct a more cleverly designed circuit.

To this end, we recall that a unitary design is, by definition, a reversible design. Therefore, if we have a unitary gate $U_{f_x}$ that performs $U_{f_x} |a\rangle|b\rangle \rightarrow |a\rangle|f_x(a,b)\rangle$, where $a$ and $b$ are integers and $f_x$ is a function that takes two integer inputs and generates an output integer, we have $U_{f_x^{-1}} |f_x(a,b)\rangle |a\rangle \rightarrow |c\rangle|d\rangle$, where the superscript $-1$ denotes the inverse, $c = f_x(a,b)$, and $f_x^{-1}(c,d) = a$. If we now consider a gate where $f_x(a,b) = ax + b$ (in modulo space), we see that $U_{f_x^{-1}} |f_x(a,b)\rangle |a\rangle \rightarrow |ax + b\rangle - bx^{-1})$. Thus, by setting $b = 0$, we obtain a modulo multiplication gate, which performs $|a\rangle \rightarrow |ax\rangle$, while restoring all workspace qubits to the initial state of $|0\rangle$ automatically. Using linearity of quantum mechanics, generalization to an input superposition state of any integer states is then immediate.

At this point, we imagine the following situation. While we may not be able to remove the inherent errors of hardware, we may, for instance, be able to undo the errors when we apply the inverse operation. This should not come as too big of a surprise, since spin-echos [165] provide an excellent example where we exploit this type of symmetry. Recalling now that Shor’s algorithm consists of these forward-backward pairs of gates throughout the modulo-exponentiation part of the circuitry, i.e., many back-to-back additions and subtractions for the aforementioned modulo multiplication, we see that potential cancellations of errors due to symmetry may help boost the performance of the quantum processor. In Ref. [166], we show our results and confirm that this is indeed the case.

Yet another way that we may optimize quantum computing is by choosing a proper adder architecture given a particular condition. In the case of Shor’s algorithm, one of
the two summands of an adder operation is always classically known. In this case, it may be advisable to choose, for instance, a Fourier-based architecture of the quantum adder [101] over a ripple-carry based architecture [99] – this is the way that humans add numbers; starting from the least significant digits, working our way up to the most significant digits while carrying all the carries – since the Fourier architecture only requires half the number of qubits than its ripple-carry counterpart. More technical details [99, 101] show that the Fourier architecture, if implemented exactly, requires $\sim n^2$ quantum gates as opposed to $\sim n$ for the ripple-carry architecture, where $n$ is the size of the circuit. However, we recall that banding is an extremely efficient method of approximating quantum circuitry. Therefore, applied to the Fourier-based adder, we obtain the same scaling $\sim n$ of the number of gates in both adder architectures, leaving room for optimization in the choice of adder architecture, depending on the coefficient in front of the number of gates in the performance scaling of the respective quantum adders. Preliminary results are encouraging [167], i.e., we may indeed optimize the quantum circuitry by choosing different architectures, and the results are expected to be available in the literature soon [167].
Chapter 3

Discussion

At this point in this thesis, having proved the stunning robustness of quantum computers, we need a reality check. Will we be able to control and preserve quantum superposition and entanglement, the two pillars of quantum information technology, on a scale relevant for quantum computing? The answer is yes on both accounts.

Neutrino oscillation [168–172], the 2015 Nobel Prize for Physics [173], is based on quantum superposition. Flavors and masses of neutrinos, two of the observable quantities, form two axes of measurement, in analogy to the $x$ and $z$ bases in Sec. 2.1. In other words, a flavor state of a neutrino is a superposition of distinct mass states of the neutrino and vice versa. Now, let us suppose a neutrino, initially in a distinct flavor state, travels through space. This makes its quantum state evolve on the basis of mass states. As a result, the composition of mass states change as the neutrino travels. Since, however, a flavor state is a superposition of mass states, a change in mass-state composition implies a change in the flavor state, leading to an oscillation of flavor states of the traveling neutrino.

Another system where we observe quantum superposition is the ammonia molecule (NH$_3$). Typically, the standard model of the ammonia molecule is depicted in many
textbooks (see for instance Fig. 3.19(a) of [174]) as a triangular pyramid, with three hydrogen atoms on the floor and a nitrogen atom on top. This, however, is misleading. There is no reason why the nitrogen atom should be on top; it can very well also be on the bottom. In fact, an ammonia molecule naturally exists in superposition state of these two configuration states, which may be exploited to result in a maser. The 1964 Nobel Prize in Physics [175] was given for this discovery.

Going further, a 60-carbon-atom buckyball and a 70-carbon-atom buckyball (a carbon soccer ball or a spherical fullerene - see the 1996 Nobel Prize in Chemistry [176]) have been reported to be in a superposition state via a double-slit experiment [177–179]. While we are still far from achieving a superposition state of a mol of atoms, i.e., the order of magnitude one would need in order to realize a true Schrödinger cat state, there is no doubt that we are making serious progress toward a macroscopic quantum superposition state.

The same can be said for quantum entanglement. A series of recent articles in the literature reports on the groundbreaking discovery that plants, during their photosynthesis process, make use of quantum entanglement to help boost the efficiency of harnessing energy from sunlight [180–182]. Given that plants are highly interactive, very complex organisms that function at room temperature, the future of quantum entanglement technology, perhaps, lies in taking some cues from nature.

On the information technology side, quantum entanglement is often used in quantum communication networks. Beyond the demonstration of entangling photons without any physical interaction [183], following the inception of the idea of teleportation of quantum information, devised in [21, 184], we are now able to experimentally realize teleportation up to 143 km [185]. In fact, several major quantum networks, that are already in place, support the entanglement-based quantum communication paradigm [186, 187].

In line with the novelty of quantum-entanglement technology, the physics behind quantum entanglement is still a subject of fundamental research. Evidenced as recently as
2015 [188–190], the scientific endeavor of verifying the way we understand or interpret the phenomenon of quantum entanglement, is still cutting-edge research. Closing many of the past experiments’ loopholes [191–193] (see also [194] and references therein) that demonstrated violations of local realism by quantum mechanics [195–204], the experimental realization of a loophole-free Bell test [188–190], devised by Bell himself [205], resulted in rejecting a host of local-realist theories by demonstrating superluminal “quantum” communication under space-like settings, a feature of quantum mechanics that is fundamental for establishing secure quantum networks.

Having revisited the foundations of quantum information technology from the empirical point of view, we now turn to the experimental state of the art of realizing a quantum computer. With particular emphasis on the number of qubits, we already discussed a number of different quantum-computer architectures in Chapter 1. In Chapter 2 we discussed how quantum hardware performance is approaching the error level that allows for large-scale quantum computation. Provided with these experimental breakthroughs, the evermore pressing question to answer has now become how one can characterize and verify the quality of quantum hardware. The importance of this step is evident when considering calibrating quantum hardware for its reliable performance. To this end, several facets of new research frontiers have emerged, some of which we lay out briefly in the following. Once we introduce the new frontiers, we will show how my works fit into the contemporary, cutting-edge quantum research.

To start, the most rudimentary method (i.e., quantum-process tomography) would be to directly probe the provided hardware, providing it with specially prepared initial states and recording corresponding final states to reconstruct and characterize the operation-dynamics of the hardware. This method, however, is costly, especially as the scale of the quantum computer becomes large consisting of millions of quantum gates. In addition, this method is sensitive to state preparation and measurement (SPAM) errors, as perfect preparation and measurements of peculiar states are crucial in this characterization method. Hence, for the purpose of characterizing the quality of quantum gates, we need
a better-suited method of characterization.

Circumventing this in the framework of tomography is the quantum gate-set tomography [206]. In this scenario, we assume the initialization and measurement procedures can be performed only as reliably as the quantum gates themselves allow, a reasonable assumption, given that the initialization and measurement processes are also bound by the associated quantum hardware limits. In essence, the underlying philosophy here is consistent with the central theme of my works (see also Sec. 2.2), namely, every single component of the quantum hardware is naturally and, therefore, necessarily flawed. Rather than trying to characterize individual gates as in the aforementioned case of quantum-process tomography, in the quantum gate-set tomography, one characterizes the entire quantum information processor as a whole, by means of considering a quantum processor in its entirety, which consists of both the SPAM part and certain quantum gates (hence the name quantum gate set) of interest. In other words, we treat a quantum processor as a single black-box unit and we attempt to characterize the quality of the entire black box all together, rather than by its individual components. This way, if there is an additional quantum gate to be characterized, it may be implemented inside the original black box to result, via comparison, in a posteriori knowledge of the additional gate’s quality. Initial steps in this direction have already been applied to ion-trap qubits [207].

Another way of characterization includes randomized benchmarking (RB). Via random sequences of quantum gates of sufficient length (see, for instance, [208–210] for technical details), comparison between the experimental and numerical results allows us to determine the characteristics of the operation dynamics of the experimental quantum hardware. This method is also cheaper than quantum-processor tomography, since RB is used to characterize only the computational aspect of the quantum gates, as opposed to a full description of the quantum process. Whether the full description is needed or not depends largely on the circumstances and the scope of the investigations concerning the effects of a variety of types of noise and errors present in the quantum processors. It
remains to be seen to what extent the RB protocol will be successful. For instance, the
technique of interleaved RB protocols has been devised in this regard, where interleaving
a particular choice of quantum gate (drawn from a Clifford group) between the random
gates, as prescribed in the standard RB protocol, results in the ability to characterize
the quality of the chosen quantum gate [211]. According to my work [159], estimation
of the quality of quantum gates via statistical analysis of gate sequences is expected
to yield an excellent approximation of the quality of quantum gates, and this method,
according to my experience in analytical estimation of the quality of quantum processors
with defective gates [123, 124, 158], is scalable in the number of qubits.

To sum up, and to put the above discussion into a more conceptual context, we note
that these characterization techniques may be visualized in the following way. Let us
consider, for the sake of conceptual clarity, a simple example of measuring the thickness
of a single page of a book. If we are given a crude measuring tool, say, a commonly-sold
ruler, and we try to directly measure the thickness of a single page, we will end up at
best with an error margin that is of the order of the precision limit of the ruler, orders
of magnitude larger than the page thickness itself. Typically, we avoid this issue by
ensuring that the object of interest is larger than the precision limit of the ruler, i.e.,
we measure the combined thickness of multiple pages, and thus indirectly obtain the
thickness of a single page by dividing the measured quantity by the number of pages,
assuming every page has about the same thickness.

Given the new variety of methods in estimating the quality of quantum hardware, it
is not surprising that there are several different measures that quantify the quality of
quantum hardware. The two most well-known ones are the fidelity and the diamond-
norm.

Fidelity is usually defined as $|\langle \psi_{\text{ideal}} | \psi_{\text{actual}} \rangle|^2$ (or sometimes without the square), where
$|\psi_{\text{ideal}}\rangle$ and $|\psi_{\text{actual}}\rangle$ are the ideal and actual quantum states after a pre-specified quan-
tum operation. In other words, fidelity is the trace norm of the product between the
density matrix of the ideal state and the density matrix of the actual state. The physical
intuition behind the measure is the overlap between the ideal result and the actual re-
sult, which can be understood straightforwardly, as long as the states are pure (coherent
quantum operations).

Trouble arises when there exists an interaction between the computational system and
the surrounding environment. Assuming that the environment is uncontrollable, un-
wanted entanglement between the computational system and the environment can de-
grade the coherence of the system. If we assume that our system is in the superposition
state $|0\rangle + |1\rangle$ and the environment couples to the system such that the composite
system state reads $|0\rangle |E(0)\rangle + |1\rangle |E(1)\rangle$, where $|E(x)\rangle$ denotes the state of the environ-
ment that couples to the system state $|x\rangle$, and $E(0) \neq E(1)$, observing the environment
in one of these distinct states will have collapsed the state of the system, destroying its
coherence. In this context, there may now be an associated probability of collapsing a
part or the entire state of qubits of a quantum computer, yielding an actual state that
is a mixed state (see Sec. 2.1). Therefore, in this case, the calculation of fidelity, which
requires a projection of the actual, mixed state to the ideal, coherent state, becomes
rather ill-defined and hence the trouble increases.

Thus, if we fully take these effects into account and still want to have some physical
intuition of what we are calculating as the quality of quantum hardware, it makes sense
to devise an alternative measure. Diamond-norm (the mathematical definition is rather
complicated; see [212]) is the recommended metric, tailor-made for this issue. Loosely
speaking, the diamond-norm allows us to measure the distance between two quantum
operators that act on the “universe”, which consists of the quantum computer and the
environment, in a way that the effect of the environment on the quantum computer is
taken into account. Among other advantages, the power of the diamond-norm lies in
the additive property of its maximum, an especially useful property when we consider
the difference between a series of approximate (real) operations versus a series of ideal
operations, yielding an upper bound on the difference between the two cases.
Now, throughout my published work, the performance of the quantum processor has been typically determined in two different ways: One is the aforementioned fidelity and the other is the algorithm-specific success probability, e.g., the success probability of factoring a semiprime in the case of Shor’s algorithm. The choice of fidelity has been made, because (i) so far in my research, I do not explicitly model in my simulations the quantum entanglement between the quantum computer and the surrounding environment, apart from measurements, and (ii) in this scenario, the fidelity can be shown to match the success probability [158], the ultimate, irrefutable measure of quantum processor quality. This way, the choice of fidelity as the proper metric for quantifying the quality of a quantum processor is well justified. On the other hand, since my simulations are capable of yielding the entire spectrum of the resulting states from a prescribed quantum process, extracting the diamond-norm, if necessary, can be done straightforwardly. In line with one of my current projects in fully modeling quantum-error-correction-code equipped quantum circuits in the presence of the effects of coupling to the environment [164], I expect my future research to include the diamond-norm metric as well for completeness.

Having discussed the tools to quantify the overall errors that may be present in the quantum hardware, we now address the issue of distinguishing the sources of errors. In particular, our goal is to devise a conceptually simple method that allows us to distinguish the effects of superposition-like errors (coherent) from probability-mixture-like errors (incoherent). This is desired, because, experimentally, if we wrongly identify the source of the errors, for instance, if a coherent error was mistakenly characterized as an incoherent one, it is conceivable that tweaking the quantum hardware to compensate for the supposedly incoherent error may make matters worse. As we shall see, as a result of the analysis to follow, this difficulty demonstrates how my research in modeling coherent errors in large-scale quantum processors, in retrospect, reflects and includes the effects of incoherent errors in the practically interesting regime of a large number of qubits.
On the conceptual level, the difference between the two sources of errors may be visualized with the help of a Bloch sphere [213, 214], which represents a single qubit. Let us first consider a Hadamard operation that sends the state $|0\rangle$ to $|0\rangle + |1\rangle$. This is illustrated on a Bloch sphere by rotating a Bloch vector [215] from its initial state of pointing into the direction of the north pole to pointing to the equator. In this illustration, a coherent error can be depicted as the inexact angle of rotation (see below for technical details). This is consistent with the dial argument in Sec. 2.2. On the other hand, an incoherent error, such as a bit-flip error (see, e.g., [68] for a depolarizing channel for more detail), is represented as both a contraction and imprecise rotation of the vector, forming a Bloch ellipsoid. Technically speaking, this is so, because a Bloch vector $\vec{a}$ is defined according to $\rho = (1 + \vec{a} \cdot \vec{\sigma})/2$ [68], where the density matrix $\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|$ is the sum of the outer products of the states $|\psi_i\rangle$ of the qubit that are associated with the mixture probabilities $p_i$, and $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ is the vector of Pauli matrices.

What this means in terms of quantum computing is the following. Let us consider once more the case of a single qubit, prepared in the state $|0\rangle$. Ideally, we would like to apply an identity operation, i.e., we would like to preserve and store the quantum state. However, because of some adverse effects of the environment, there may exist a nonzero but small probability $p$ that the qubit may flip (in the $z$-basis) to the state of $|1\rangle$, in analogy to a classical bit-flip error. In the case of the flip-channel model, we find that the corresponding Bloch vector reads $\vec{a} = 2p(1 - p)\hat{x} + 1 - 2p\hat{z}$, where $\hat{x}$ and $\hat{z}$ are the unit vectors in $x$ and $z$ directions, respectively. This means, to first order in $p$, we have the vector pointing in the direction $\theta \approx 2p$ away from the $z$-axis, tilted towards the $x$ axis, while the Euclidean norm of the vector is approximately $1 - 2p$. We notice that these operation dynamics are very similar to an approximate but fully coherent identity operation that tilts the Bloch vector, originally pointing toward the $+z$-direction, by an angle $2p$ towards the $x$-axis. The only difference is the resulting Euclidean norm of the vector.

Recalling the goal of these investigations, namely, practical quantum computing, we
would now require the Euclidean norm of the vector to remain as robust as possible. Otherwise, the flip-channel would have muddled the coherence of the quantum computer and practical quantum computing would be impossible. This means, $p$ needs to be kept relatively small. In this case, since the norm is considered to be robust, the remaining question is how, given the small $p$, the quantum computer would perform when running a useful algorithm. In other words, for the purpose of practical computing, the effect of incoherent errors is best captured by and thus indistinguishable from that of the coherent errors. My numerical and analytical studies [119–124, 156, 158, 159, 164, 166, 167] answer this very question. In fact, in retrospect, these studies may be considered a large-scale model that simulates the effects of depolarizing-channel-type noise since (i) according to the assumption of practical quantum computing, we need the norm to be robust, i.e., $p$ is small, and (ii) the remaining part of the depolarizing-kind of errors, namely the angular drifts, need to be indistinguishable from coherent, unitary errors.

Thus the encouraging results obtained in [119–124, 156, 158, 159, 164, 166, 167] demonstrate the viability of practical quantum computing. In these publications, contrary to the disbelief of many, it is shown that quantum computing with quantum computers consisting of hundreds of qubits is possible via already available technology [118, 216]. My results speak strongly for practical quantum computing without quantum information protection technology. While this may not be a widely accepted view just yet, there are signs that some physicists start to be on board with this [217].

Nevertheless, a very large-scale design of quantum computers may still need quantum error correction technology that is capable of correcting for flip errors, for instance, at least in its infancy stage. This is an expected path that quantum computing will most likely follow, just as classical computing has error correcting code (ECC) memory was the standard until the early 1990s for all personal computers ever since the first personal computer built by IBM [218]; most modern-day personal computers now, however, use Non-ECC memory, given the nowadays super-low error rate ranging from one in a thousand years [219] to one in a year [220]]. While, some day, we may consider ECC quantum
memory as superfluous for quantum computing, and the whole process of quantum error correction a Byzantine process, at present, while myopic perhaps, we consider quantum error correction a necessity.

Thus, assuming now that, for the time being, we are to use quantum error correction codes before a more suitable, new technology emerges to be used in very-large-scale quantum computers, we introduce a promising contemporary candidate of quantum error correction codes, namely, topological quantum error correction codes. The motivation behind this will become self-evident: The state-of-the-art topological code, namely the color code, will show properties that will make strong connections to many of my works addressing quantum computing and ion trapping.

Invented by Kitaev [221, 222] in the mid 1990s in the form of a toric code, together with subsequent developments [223–226], topological quantum error correction codes have now become one of the most promising contemporary candidates for the quantum error correction technique. A textbook introduction to, for instance, a 2-D realization of the original, toric codes, also known as surface codes, may be found in Ref. [76]. The most important aspect of the topological codes is the fact that the codes encode quantum information in the non-local degree of freedom, thereby being able to correct for local errors. In other words, in order to control (or perturb) the logical state, highly organized, coordinated quantum maneuvering needs to be executed.

The cutting-edge research in this direction has now culminated in what is known as the color code [227, 228], which, in its 3D form, can bypass the Eastin-Knill theorem [132], i.e., no quantum error correcting codes support transversal implementations of (approximately) universal quantum gates. So far, most, if not all, quantum error correction codes, including the aforementioned surface codes, trade off (i) the difficulty of the transversal implementation of quantum gates with (ii) the difficulty of preparing some “magic” states [229] that can be created with the help of many ancilla qubits that are not part of computational qubits. Color codes, cleverly, by virtue of making the
process of quantum error correction itself the magic-state preparation process [230], attain (approximate) universal quantum computing via transversal implementation of all standard gates (see Sec. 2.2) [231–233]. Following this discovery, a host of new quantum error correction techniques [234, 235] have been developed to circumvent the Eastin-Knill theorem [132].

Now, the color code, implemented on $D$ spatial-dimensions, allows us to realize the logical phase-rotation gate with phase-rotation angle $\pi/2^{D-1}$ transversally [233, 236]. For instance, the color code implemented in 3D, or higher, will support transversal implementation of the standard set of quantum gates, capable of achieving approximately universal quantum computing. This is of particular interest since, in Sec. 2.3 and Refs. [119–122], I showed $D = 8$ is sufficient for running Shor’s algorithm that threatens current cybersecurity. Provided that the hardware architecture applicable for high $D$-dimensional color codes relies heavily on the peculiar geometry of qubit networks [233, 236] then, my investigations on crystal formation [237] and morphology [238] may be of interest in developing and advancing trapped-ion, color-code-equipped quantum computers [147].
Chapter 4

Remarks

It is indeed an exciting time to be a quantum computer physicist. In the short term, taking a bottom-up approach, we will, for instance, need to verify the fault-tolerance of quantum error correction circuitry experimentally [239]. At the same time, we may also determine the sensitivity of quantum-computer performance with respect to the quality of quantum hardware, and, in this respect, we believe the recently proposed optical simulator of the quantum Fourier transform [125] will be of great interest to many in the quantum-computing community.

Once (February 21, 2013) I said in the physics colloquium at Wesleyan University on “[Super]symmetry and the quincunx nexus”, by Dr. Jim Gates, “... [S]ince you bring up classical error correction, I will bring up quantum error correction. I know, it sounds crazy, but have you considered applying quantum error correction [to model and understand the Universe]? ...” The following short discussion led to the difficulty of exact decomposition of the equations of supersymmetry into the units that can be dealt with at the quantum-error-correction level, but the approximate decomposition of it by virtue of the Solovay-Kitaev theorem has not been tried. Well, as it turns out, the idea of merging the field of quantum information and particle physics is not so crazy after all. There now is an active movement toward bridging the perceived gap between fundamental physics
and quantum information theory (see, for instance, Ref. [240], most notably by “It from Qubit” [241]).

The field of quantum computing is already helping us to understand, to an unprecedented degree, how the universe works. A recent experiment [242] already resulted in the confirmation that time is an emergent property of quantum entanglement for observers internal to the universe. Perhaps, in this case, it is entirely possible that the ways that nature does quantum computing will help and guide us on the road to robust quantum computing, going beyond many of the possible directions detailed in this thesis.
Chapter 5

A brief guide to my publications

My published work comprising my thesis consists of 12 papers.Thematically, these fall into two groups, (i) quantum computing and (ii) ion trapping. The link between these themes is established by noting that understanding the physics of ion trapping is essential for building an ion-trap quantum computer, currently one of the most promising quantum computer architectures.

In the following two sections, section 5.1 and section 5.2, I briefly guide the reader through my 9 published papers (1 recently accepted) on quantum computing and my 3 published papers on ion trapping, respectively.

5.1 Quantum Computing

My published work on quantum computing consists of 9 papers, which mainly focus on the effects of hardware errors on the performance of medium- and large-scale quantum computers.

I started my investigations of hardware errors with the paper [119] in which I subjected a quantum computer running the quantum Fourier transform to a class of static defects
known as banding, i.e., systematically removing all phase-rotation gates with phase-rotation angles less than a certain prescribed value $\pi/2^b$, where $b$ is the bandwidth. The choice of the quantum Fourier transform is made based on its universal utility in quantum computing. The removal of the phase-rotation gates whose phase-rotation angles are small is justified since one would need to realize phase-rotation gates with phase-rotation angles that are of the order of $\pi/2^n$, where $n \sim 1000$ is the number of qubits in the quantum Fourier transform circuitry that is of practical interest. By numerically investigating the performance of the quantum Fourier transform, measured via an objective criterion, namely, the success probability of extracting the embedded periodicity of the input quantum state, I showed in [119] that, based on numerical simulations that simulated up to nearly 40 qubits, 95% performance of a 1000-qubit quantum Fourier transform is expected when we keep only the phase-rotation gates with phase-rotation angles larger than $\pi/2^8$.

Motivated by this, I then investigated the banding technique further in [120], this time, analytically. This is necessary since a reliable extrapolation to a quantum computer with thousands of qubits can only be achieved using analytics. This is so, because, if we were to be able to simulate a large-scale quantum computer with thousands of qubits, this, in turn, means we do not need a quantum computer. Via the statistical analysis on the phase-rotation angles associated with the banded quantum Fourier transform, in [120], I showed analytically that the performance of the quantum Fourier transform, subjected to the banding operation, scales like $\sim \exp[-1.19 \times 2^{-2b}n]$ for large $n$, in excellent agreement with my numerical results $\sim \exp[-1.1 \times 2^{-2b}n]$ for large $n$. This striking accuracy demonstrates the power of statistical and analytical tools that may be employed in further investigating the performance of quantum hardware. Also pointed out in the paper was the discovery that the resulting Fourier peaks of the probability spectrum of the quantum Fourier transform respond in unison to the banding operation, a fact that is important for my subsequent publication on the optical simulator.

In [125], taking the unison-response discovery from [120], I proposed a classical analog-
device that simulates the quantum Fourier transform for up to tens of qubits, a medium-sized quantum computer. Now, one can straightforwardly show, according to Fourier optics, that a grating, equipped with a circular screen, exactly mimics the quantum Fourier transform operation. The unison response, moreover, allows us to focus on a single peak of the Fourier spectrum for the purpose of investigating the effect of defective gates in the quantum Fourier transform, making it feasible to meet the experimental resource requirements with currently already available technologies. Instead of being able to simulate just a few qubits using the apparatus running in the full-spectrum mode, with the single-peak mode, the apparatus, made with commercially available technologies, can experimentally explore, for instance, a 20-qubit quantum Fourier transform relatively easily. I further demonstrated in [125] that this optical simulator can be run in an exact mode, i.e., exactly reflecting the banding operation, for instance, but can also be run in the statistical mode, i.e., the apparatus can be tweaked in such a way that the Fourier output is statistically equivalent to that observed from running the apparatus in the exact mode.

In fact, in [125], in light of the optical grating, I established the statistical equivalence between banding and defective phase-rotations in the quantum Fourier transform. This is a conceptually consistent picture in that, after all, the missing phase-rotation gates, or the defective phase-rotation gates, will both result in some random perturbations in the mathematical exactness of the apparatus reflecting the mathematical framework of the Fourier optics. Based on the robustness of the quantum computer running the quantum Fourier transform with respect to banding, this hints at the robustness of a quantum computer with respect to defective phase-rotation gates. This was demonstrated in [123], where we investigated the effect of the defective rotation gates whose phase-rotation angles were perturbed according to relative and absolute errors. Both numerical and analytical results show that the quantum Fourier transform is indeed robust against these static errors, the case of relative errors yielding a performance-scaling relation of the form \( \sim \exp(-\gamma_r e^2 n) \) and the absolute-error case yielding a performance scaling
relation of the form $\sim \exp(-\gamma_r \epsilon^2 n^2)$, where $\gamma_r$ and $\gamma_a$ are constant coefficients in the exponent for relative and absolute errors, respectively, $\epsilon$ denotes the strength of the perturbation and $n$ denotes the number of qubits of the quantum Fourier transform circuit. Thus, for instance, for the case of relative errors, a 1000-qubit quantum Fourier transform circuit, equipped with defective phase-rotation gates whose error level is of the order of 3%, will result in a satisfactory performance, a surprising result that shows the resilience of the quantum circuits against random perturbations.

In [124], extending the investigation to both inaccuracy and imprecision of the phase-rotation gates, I investigated the performance of the quantum Fourier transform with respect to both the drift (inaccuracy) and the random perturbation (imprecision) of the phase-rotation gates. In particular, using analytical tools, validated by numerical results, I was able to show that the quantum Fourier transform performs remarkably well with respect to an inaccurate implementation, even when we scale up to thousands of qubits. In particular, I demonstrated that the effect of the drift errors do not scale in the number of qubits, extremely welcome news since, should this not have been the case, we would require an evermore accurate implementation of the phase-rotation gates as we increase the number of qubits, prohibiting us from reaching the number of qubits that are of practical interest. Fortunately, the analytically confirmed independence of the performance scaling of the quantum Fourier transform with respect to drift errors in the number of qubits guarantees that an impossibly accurate implementation of the quantum gates is not necessary.

Having shown the robustness of the quantum Fourier transform, I then investigated in [156] the structural stability of the circuit by altering the hierarchical structure of the phase-rotation angles from a binary base, i.e., $\pi/2^j$, where $j$ is an integer, to, for instance, a real-exponential base, i.e., $\pi/\alpha^j$, where $\alpha$ is a real number or a power-law base, i.e., $\pi/(2j)^\beta$, where $\beta$ is a real number. Both cases showed that the quantum Fourier transform, irrespective of the particular choice of hierarchy $\alpha$ or $\beta$, results in a satisfactory performance, as long as the assumed, altered hierarchy is reasonably close.
enough to the ideal hierarchy of $\pi/2^j$. In fact, the observed performance is so robust, that even when we alter the hierarchy to an inverse-logarithmic hierarchy, i.e., $\pi/\log_\gamma(j + 1)$, where $\gamma$ is a real number, a satisfactory performance of the quantum Fourier transform is obtained. The insight we gain from the work shown in [156] is then the importance of maintaining hierarchy and the secondary importance of the exact form of the hierarchy when it comes to the performance of the quantum computer.

Motivated by this observation, in [158], I investigated the so-called random hierarchy, where the phase rotation gates to be used in the quantum circuit are drawn from a pool of random phase-rotation gates whose phase-rotation angles are uniformly distributed between 0 and $\pi/2$. By sampling the phase-rotation gates from the pool, then using the gates that best match rotation-angle specifications in the quantum circuit, I demonstrated that a random hierarchical approach works remarkably well, yielding, for instance, above 30% performance of a 17-qubit quantum Fourier transform when merely 60 gates were drawn from a random set. In fact, my analytical results show that we only need to draw about the same number of gates from a random set as the number of qubits of the quantum Fourier transform to obtain a satisfactory performance of the quantum Fourier transform. Moreover, a boost of performance was observed when banding was superimposed on the random-hierarchy approach. In [158], I pointed out that this makes perfect sense since banding away erroneous gates gives rise to a performance boost. In fact, since the pruning of the erroneous gates increases the quantum Fourier transform performance, while banding away too many gates would result in the decrease of quantum Fourier transform performance, there must exist, given some error level, an optimal level of banding, which maximizes the performance of the quantum Fourier transform. I present an explicit formula of this optimal bandwidth in [158], which will come as a welcome boon for quantum computing experimentalists.

Additionally shown in [158] was the equally impressive robustness of the quantum adder whose architecture is based on the Fourier basis. This implies that a quantum processor running the entire Shor’s algorithm, if Fourier-based arithmetic units are used, will be
robust against defects and errors of the phase-rotation gates. This is indeed the case as shown in [121], where banding, whose effect is equivalent to that of the defective rotation angles of the phase-rotation gates, was imposed on the entire Shor algorithm circuitry. Factoring the semiprime 21 into its prime factors 3 and 7 on a complete, quantum-gate–by–quantum-gate implemented Shor algorithm code, to the best of my knowledge, was the first time ever that an entire Shor’s algorithm was shown to be robust against banding [121].

In [122], I extended the world record in quantum factoring by factoring semiprimes of up to 57 using a complete, basis-quantum-gate implementation of Shor’s algorithm, investigating the effects of banding, thus also the defective rotation gates, on the performance of Shor’s algorithm. Also breaking the previous record was the gate-by-gate simulation of the banded quantum Fourier transform using 40 qubits on a conventional, single-core PC, which, to the best of my knowledge, is the largest scale quantum calculation of its kind that has ever been simulated to date. My results show that inexact, approximate quantum arithmetic units are acceptable for a large-scale quantum processors, as opposed to a classical processor whose results would be horribly corrupted if approximate classical arithmetic units were to be used. Thus, in [122], I successfully delineated the fundamental difference between a quantum computer versus a classical computer.

### 5.2 Ion Trapping

My published work on ion trapping consists of 3 papers, which mainly focus on the heating and cooling of ions contained in the Paul trap.

First to investigate was how much heating of the ions is produced when the ions in the Paul trap are driven by the trap field. Conceptually and phenomenologically, the origin of the heating itself is well understood if one considers kneading of a dough, for instance, where a series of deformations leads to heating of a deformation-undergoing object. In
[121], with my collaborators I quantified and investigated the heating rate of the ion clouds in the Paul trap and announced the discovery of a single, universal heating curve that describes the (scaled) heating rate of ion clouds in the Paul trap as a function of the (scaled) size of the cloud. This allows us to immediately determine the heating rate of the cloud as soon as the trap control parameters and the number of particles are known, a critical knowledge that may come in handy when preparing the ion qubits for an ion-trap quantum computer.

In order to pin down the universality observed in [121], in [243] my collaborators and I showed analytically that the universal behavior is expected, and can thus be applied to any combinations of reasonable trap parameters and the number of ions. Also demonstrated was the power of mean-field theory employed in [243] that the description of the heating power of the Paul trap system can be well characterized by considering a guiding motion of the particles only in contrast to a jittery motion of the particles. Demonstrating the technique of dividing the motion into a slowly-varying, stroboscopic, macro-motion and a fast-fluctuating, trap-field-induced, micro-motion is useful in describing our system, and the fact that the heating rate was captured by the macro-coordinates instilled us with the hope that, perhaps, conventional thermodynamics may be applicable to our driven system if we only consider the macro-coordinates.

In [237], we took a first stab in this direction, namely, establishing the thermodynamics of a driven system. In particular, we focused on the cloud → crystal transition, a critical step in realizing an ion-trap quantum computer as we ought to cool the ion qubits into a spatially ordered, crystalline phase. With collaborators, I was able to show that this phase-transition phenomenon can be put into a critical phenomena context, where we observe a power-law behavior of the lifetime of the pre-phase-transition state as a function of the extra strength of cooling above the necessary critical cooling power, below which the cloud → crystal transition never occurs. This is expected to be of particular interest to the experimentalists who are interested in knowing how long a certain amount of cooling (by, say, laser cooling) needs to be applied to ensure the
production of a crystalline state of the ions in the Paul trap.
Appendix A

List of Publications

In this appendix, we present our peer-reviewed journal publications to date. The following is the list of publications including titles and abstracts, sorted according to chronological order, as shall appear in the subsequent sections of this chapter. All papers included in this chapter have self-contained references and citations.


Performance-Scaling of Shor’s Algorithm with Banded Quantum Fourier Transform

In excellent agreement with our numerical simulations of Shor’s algorithm, equipped with a truncated quantum Fourier transform of bandwidth $b$, we find that its performance scales $\sim 2^{-\xi_b n}$, where $n$ is the number of qubits, $\xi_b = 1.1 \times 2^{-2b}$, and the bandwidth $b$ is the number of quantum states coupled by the quantum Fourier transform. Non-exponential behavior is observed for small $n$ and explained analytically. The large-$n$ exponential scaling implies that $b = 7$ is sufficient to operate a 1,000-qubit quantum computer running Shor’s algorithm on the 95% performance level and implies hardware savings on the order of half a million rotation gates.
Scaling laws for Shor's algorithm
with a banded quantum Fourier transform

We investigate the performance of a streamlined version of Shor’s algorithm in which the quantum Fourier transform is replaced by a banded version that for each qubit retains only coupling to its $b$ nearest neighbors. Defining the performance $P(n, b)$ of the $n$-qubit algorithm for bandwidth $b$ as the ratio of the success rates of Shor’s algorithm equipped with the banded and the full bandwidth ($b = n - 1$) versions of the quantum Fourier transform, our numerical simulations show that $P(n, b) \approx \exp[-\phi_{\text{max}}^2(n, b)/100]$ for $n < nt(b)$ (non-exponential regime) and $P(n, b) \approx 2^{-\xi_b(n-b)}$ for $n > nt(b)$ (exponential regime), where $nt(b)$, the location of the transition, is approximately given by $nt(b) \approx b + 5.9 + \sqrt{7.7(b+2) - 47}$ for $b \geq 8$, $\phi_{\text{max}}(n, b) = 2\pi[2^{-b-1}(n - b - 2) + 2^{-n}]$, and $\xi_b \approx 1.1 \times 2^{-2b}$. Analytically we obtain $P(n, b) \approx \exp[-\phi_{\text{max}}^2(n, b)/64]$ for $n < nt(b)$ and $P(n, b) \approx 2^{-\xi_b(n-b)}$ for $n > nt(b)$, where $\xi_b^{(a)} \approx \frac{n^2}{12\ln(2)} \times 2^{-2b} \approx 1.19 \times 2^{-2b}$. Thus, our analytical results predict the $\phi_{\text{max}}^2$ scaling ($n < nt$) and the $2^{-2b}$ scaling ($n > nt$) of the data perfectly. In addition, in the large-$n$ regime, the prefactor in $\xi_b^{(a)}$ is close to the results of our numerical simulations and, in the low-$n$ regime, the numerical scaling factor in our analytical result is within a factor 2 of its numerical value. As an example we show that $b = 8$ is sufficient for factoring RSA-2048 with a 95% success rate.

Streamlining Shor’s Algorithm for Potential Hardware Savings

We constructed a virtual quantum computer by running a complete, scaling, quantum-gate by quantum-gate implementation of Shor’s algorithm on a 128-core classical cluster computer. In mode A [quantum period-finding (PF) only, supplied with classical results for the modular exponentiation (ME) part of Shor’s algorithm], factoring semiprimes up to $N = 557,993$ with up to $n = 39$ qubits, we confirm earlier, smaller-$n$ results concerning the performance scaling of Shor’s algorithm equipped with a truncated (banded) quantum Fourier transform.
Fourier transform. Running our virtual quantum computer in mode B (full quantum implementation of ME and PF), we find that a large number of gates may be discarded in a scalable way in both the ME and PF parts of Shor’s algorithm in exchange for only a small reduction in performance. We explicitly state the associated scaling laws. Implying significant savings in quantum gates, we suggest that these results are of importance for future experimental and technical large-$n$ implementations of quantum computers.


**Universal heating curve of damped Coulomb plasmas in a Paul trap**

A charged-particle cloud in a Paul trap is a nonlinear system that exhibits deterministic heating, i.e. conversion of energy provided by the radio-frequency (rf) drive of the trap into the disordered, gas-like motions of the trapped particles. In the presence of weak damping clouds reach an equilibrium state in which heating and cooling balance. For large damping, a cloud may collapse into a crystal. While the rf heating power of a given cloud depends sensitively on its particle number, its equilibrium size, the damping, and the control parameters of the trap, we find that scaling the heating power of the cloud with respect to its associated Coulomb-decoupled, non-interacting-gas state, and its equilibrium size with respect to its crystal size, results in a single, universal heating curve, independent of particle number and trap control parameters.


**Robustness and performance scaling of a quantum computer with respect to a class of static defects**

Competing computationally with experimental groups for the construction of scaling quantum computers, we simulate a complete quantum-gate by quantum-gate implementation of Shor’s algorithm on a classical 128-core cluster computer. The resulting virtual quan-
tum computer serves as a convenient quantum laboratory for the investigation of the effect of defects in the quantum circuitry. The class of defects studied here is the removal of all rotation gates with rotation angles $\theta < \pi/2^b$. Factoring semiprimes $N = 21, 33, 35, 39, 55, 57$, we find that the quantum computer still operates with acceptable performance (success probability of factoring) down to $b = 2$. This is surprising since deletion of rotation gates results in large errors in the arithmetic circuitry of the quantum computer. Extrapolating on the basis of these results we conclude that for quantum computers of practical interest more than 99% of rotation gates may be discarded with acceptable consequences in quantum computer performance. This result may be of interest to experimental physicists and quantum engineers currently embarked on designing efficient circuitry for scaling quantum computers.


**Surprising robustness of the quantum Fourier transform with respect to static gate defects**

The quantum Fourier transform (QFT) is one of the most widely used quantum algorithms, ranging from its primary role in finding the periodicity hidden in a quantum state to its use in constructing a quantum adder. Testing how the QFT performs under more realistic conditions, we find that the QFT, when used for period finding, shows extraordinary robustness with respect to static gate defects. For instance, replacing all rotation angles $\pi/2^j$ of the controlled rotation gates in the QFT circuit by $\pi r/2^j$, where $r$ is a uniformly distributed random variable taking values in the range $[-1, 1]$, effectively resulting in a QFT with random gates, the QFT performs well above the expected random result. However, it is important to keep the $2^j$ terms in the denominators of the rotation angles, resulting in random, but *hierarchically random*, gates. Relaxing this hierarchical structure of the QFT circuit, we find that the performance of the QFT deteriorates significantly. This observation indicates that the hierarchical structure of the quantum circuit of the QFT is more important for the observed robustness in performance than the precise actions of individual gates. In addition to the specific example of the QFT circuit studied here, this observation
also corroborates our experience with more general and more complex quantum circuits. Thus, backed by our detailed numerical and analytical results, we may condense the results of our research into the following general principle: The topology of a quantum circuit is more important than the precise actions of its gates.


**Analytical mean-field scaling theory of radio-frequency heating in a Paul trap**

While the microscopic origins of radio-frequency (rf) heating of simultaneously stored, charged particles in a Paul trap are not yet understood in detail, a universal heating curve [J. D. Tarnas, Y. S. Nam, and R. Blümel, Phys. Rev. A 88, 041401 (2013)] was recently discovered that collapses scaled rf heating data onto a single universal curve. Based on a simple analytical mean-field theory, we derive an analytical expression for the universal heating curve, which is in excellent agreement with numerical data. We find that for spherical clouds the universal curve depends only on a single scaling parameter, \( \lambda = [q(N - 1)]^{2/3}/T \), where \( N \) is the number of trapped particles, \( q \) is the Paul-trap control parameter, and \( T \) is the temperature.


**Structural stability of the quantum Fourier transform**

While it is important to investigate the negative effects of decoherence on the performance of quantum information processors, Landauer was one of the first to point out that an equally basic problem, i.e. the effects of unavoidable hardware flaws in the real-world implementations of quantum gates, needs to be investigated as well. Following Landauer’s suggestion, we investigated the structural stability of the quantum Fourier transform (QFT) via significantly changing the analytical form of its controlled rotation gates, thus modeling structural flaws in the Hamiltonian of the QFT. Three types of modified rotation gates were investigated, numerically and analytically, changing the exact QFT rotation angles \( \pi/2^j \) to
Appendix A. List of Publications

(1) $\pi/\alpha^j$, (2) $\pi/2j^\beta$, and (3) $\pi/\log((j + 1))$, where $\alpha$, $\beta$, and $\gamma$ are constants, and $j$ is the integer distance between QFT qubits. Surprisingly good performance is observed in all three cases for a wide range of $\alpha$, $\beta$, and $\gamma$. This demonstrates the structural stability of the QFT Hamiltonian. Our results also demonstrate that the precise implementation of QFT rotation angles is not critical as long as the angles (roughly) observe a monotonic decrease in $j$ (hierarchy). This result is important since it indicates that stringent tolerances do not need to be imposed in the actual manufacturing process of quantum information hardware components.


Performance scaling of the quantum Fourier transform

Addressing Landauer's question concerning the influence of static gate defects on quantum information processor performance, we investigate analytically and numerically the case of the quantum Fourier transform (QFT) with defective controlled rotation (CROT) gates. Two types of defects are studied, separately and in combination: systematic and random. Analytical scaling laws of QFT performance are derived with respect to the number of qubits $n$, the size $\delta$ of systematic defects, and the size $\epsilon$ of random defects. The analytical results are in excellent agreement with numerical simulations. In addition, we present an unexpected result: The performance of the defective QFT does not deteriorate with increasing $n$, but approaches a constant that scales in $\epsilon$. We derive an analytical formula that accurately reproduces the $\epsilon$ scaling of the performance plateaus. Overall, we observe that the CROT gates may exhibit static and random defects of the order of 30% and larger, and still result in satisfactory QFT performance. Thus we answer Landauer's question in the case of the QFT: far from being lethal, the QFT can tolerate tremendous static gate defects and still perform its function. The extraordinary robustness of the QFT with respect to static gate defects displayed in our numerical and analytical calculations should be a welcome boon for laboratory and industrial realizations of quantum circuitry.

Analytical formulas for the performance scaling of quantum processors with a large number of defective gates

Removing a single logical gate from a classical information processor renders this processor useless. Not so for a quantum information processor. A large number of quantum gates may be removed without significantly affecting the processor’s performance. In this paper, focusing on the quantum Fourier transform (QFT) and quantum adder, we show even more: Even if most of its gates are eliminated and the remaining gates are selected from a randomly generated set, the QFT, one of the most useful quantum processors, and the quantum adder, one of the most basic building blocks of a universal quantum computer, still operate with satisfactory success probability, comparable to that of a quantum computer constructed with perfect gates. We support these conclusions by first laying out a general analytical framework, then deriving analytical scaling relations, which are in excellent agreement with our numerical simulations. The demonstrated robustness of the QFT and quantum adder, to the point where randomly generated quantum gates take the place of the exact gates, is an important boon for the construction of quantum computers, since it shows that stringent gate error tolerances do not have to be met to obtain satisfactory performance of the corresponding quantum processors. Our analytical techniques are powerful enough to generate asymptotic scaling laws for any gate defect model of quantum information processors, and we illustrate this point by explicitly computing asymptotic analytical scaling formulas for several other defect models as well.


Lifetimes of metastable ion clouds in a Paul trap: Power-law scaling

It is well known that ions stored in a Paul trap, one of the most versatile tools in atomic, molecular, and optical (AMO) physics, may undergo a transition from a disordered cloud state to a geometrically well-ordered crystalline state, the Wigner crystal. In this paper we predict that close to the transition, the average lifetime $\bar{\tau}_m$ of the metastable cloud follows a power law, $\bar{\tau}_m \sim (\gamma - \gamma_c)^{-\beta}$, where $\gamma_c$ is the value of the damping constant.
at which the transition occurs. The exponent $\beta$ depends on the trap control parameter $q$, but is independent of both the number of particles $N$ stored in the trap and the trap control parameter $a$, which determines the shape (oblate, prolate, or spherical) of the ion cloud. In addition, we find that for given $a$ and $q$, $\gamma_c$ scales approximately like $\gamma_c = C \ln[\ln(N)] + D$ as a function of $N$, where $C$ and $D$ are constants. Our predictions may be tested experimentally with equipment already available at many AMO laboratories. In addition to their importance in AMO trap physics, we also discuss possible applications of our results to other periodically driven many-particle systems, such as, e.g., particle accelerator beams, and, based on our trap results, conjecture that power laws characterize the phase transition to the Wigner crystal in all such systems.
Performance scaling of Shor’s algorithm with a banded quantum Fourier transform

Y. S. Nam* and R. Blümel
Department of Physics, Wesleyan University, Middletown, Connecticut 06459-0155, USA
(Received 1 August 2012; published 23 October 2012)

In excellent agreement with our numerical simulations of Shor’s algorithm, equipped with a truncated quantum Fourier transform of bandwidth $b$, we find that its performance scales $\sim 2^{-\alpha_b}$, where $\alpha_b$ is the number of qubits, $\xi_b = 1.1 \times 2^{-9\alpha_b}$, and the bandwidth $b$ is the number of quantum states coupled by the quantum Fourier transform. Nonexponential behavior is observed for small $n$ and explained analytically. The large-$n$ exponential scaling implies that $b = 7$ is sufficient to operate a 1000-qubit quantum computer running Shor’s algorithm on the 95% performance level and implies hardware savings of the order of half a million rotation gates.

DOI: 10.1103/PhysRevA.86.044303 PACS number(s): 03.67.Lx

Together with Grover’s database search algorithm [1,2], Shor’s algorithm [3] is one of the most powerful quantum algorithms. Implemented on a quantum computer, Shor’s algorithm is capable of cracking RSA encryption codes [4] that currently form the backbone of internet security [5,6]. No wonder, then, that Shor’s algorithm has been presented and investigated in detail in the literature (see, e.g., [7–10]). So far, RSA is safe from attacks via Shor’s algorithm, since quantum computers do not yet exist that could run Shor’s algorithm for the large semiprimes $N$ currently used in RSA encryption algorithms [4–6,8,9,11]. However, the more we simplify its hardware requirements, the sooner Shor’s algorithm will come online in a regime relevant for Internet security. In this context, Coppersmith [10] was the first to notice that substantial hardware savings may be realized by eliminating, with negligible performance penalty, most of the quantum gates of the quantum Fourier transform [8,9], the centerpiece of Shor’s algorithm. According to Coppersmith, this leaves an approximate quantum Fourier transform [10,12] that performs well when used in connection with Shor’s algorithm. Written in matrix form, this Fourier transform has a banded appearance of bandwidth $b$, coupling only the $b$ nearest neighbors of any given quantum state. Therefore, this type of Fourier transform is called a banded quantum Fourier transform. Testing the performance of the banded quantum Fourier transform in numerical experiments with semiprimes of up to 20 binary digits, we confirm that a banded quantum Fourier transform indeed leads to substantial hardware savings without seriously compromising the effectiveness of Shor’s algorithm. In addition, improving on previous results [9,10,12], we present analytical scaling functions that measure the performance of Shor’s algorithm as a function of the bandwidth and the number of qubits. Our analytical scaling functions agree well with our numerical results.

Shor’s algorithm is based on Miller’s algorithm [8,9,11] for factoring semiprime numbers $N = pq$, where $p \neq q$ are two prime numbers. Given a number $x < N$, relatively prime to $N$, the smallest power $\omega$ of $x$ is determined such that $x^\omega \equiv 1 \mod N$. $x$ is called the seed and $\omega$ is called the order of $x$. Now, define $A = x^{\omega/2} - 1$ and $B = x^{\omega/2} + 1$. Then, if (i) $\omega$ is even and (ii) $B \not\equiv 0 \mod N$, the two prime factors of $N$ are revealed as (up to ordering) $p = \gcd(A,N)$ and $q = \gcd(B,N)$, where $\gcd$ denotes the greatest common divisor. If condition i or ii is violated, we simply try another $x$. It is known [8,9] that finding a proper seed $x$ has a high probability of success and very few $x$ need to be tried before a suitable seed is found. Since determining $\omega$ on a classical computer is an algorithmically hard problem, it is impossible (with currently known classical factoring algorithms) to factor large semiprimes $N$ on a classical computer if the number of decimal digits of $N$ exceeds, say, 1000. To do so in a reasonable time (say, about a month) would require a classical computer exceeding the current size of the universe. This is where Shor’s quantum algorithm comes in. Shor noticed [3] that determining $\omega$ on a quantum computer is exponentially faster than performing the same task on a classical computer, thus opening the possibility of factoring large $N$ within reasonable run times.

The centerpiece of Shor’s algorithm is a quantum Fourier transform,

$$|\ell\rangle = \frac{1}{\sqrt{2^n}} \sum_{s=0}^{2^n-1} \exp(2\pi i s \ell/2^n)|s\rangle, \quad (1)$$

where $n$ is the number of qubits. A circuit diagram of (1), which also incorporates a measurement of the output state $|\ell\rangle$, is shown in Fig. 1(a). On a quantum computer, as shown in Fig. 1, the phases in (1) are realized by conditional phase rotation gates, which rotate the phase of the target qubit $k$ by an angle

$$\theta_{k-j} = \frac{\pi}{2^{k-j}}, \quad (2)$$

if the control qubit $j$ is measured to be in state $|1\rangle$. We notice immediately that for large $n = \sim 1000$, as required for factoring semiprimes $N$ of practical interest, a complete implementation of quantum Fourier transform (1) would require the quantum hardware to distinguish phase differences of the order of $1/2^{1000} \approx 10^{-300}$, an impossible task under any circumstances. Not even fault-tolerant encoding [8,9] would solve this problem, since hardware, present or future, capable of distinguishing such small phase differences does not exist and cannot be built in our universe. This begs the question: What happens if we ignore gates that cannot be implemented? Eliminating unrealizable gates leads to a banded quantum Fourier transform [see, e.g., Fig. 1(b)] in which only the coupling to $b$ nearest-neighbor qubits is retained [Fig. 1(b) illustrates the case $b = 1$]. Coppersmith [10] found

*ynam@wesleyan.edu

1050-2947/2012/86(4)/044303(4) 044303-1 ©2012 American Physical Society
Appendix A. List of Publications

FIG. 1. Logic circuit of a five-qubit quantum Fourier transform, illustrating the concept of bandwidth, defined as the number of off-diagonal quantum states coupled by the quantum Fourier transform. (a) Full implementation (bandwidth $b = 4$); (b) truncated implementation (bandwidth $b = 1$). $H$, $\theta$, and $M$ denote Hadamard, single-qubit conditional rotation, and measurement gates, respectively.

That truncation to a quantum Fourier transform of bandwidth $b$ misses at most the phase

$$\Delta \psi = 2\pi n 2^{-b-1},$$

(3)

where $n$ is the number of qubits. Coppersmith’s estimate is rigorous but pertains only to the total “missing phase” of the quantum Fourier transform, which Coppersmith then qualitatively relates to the performance of Shor’s algorithm [10]. An improvement of (3) was obtained by Fowler and Hollenberg [12], who directly investigated the performance of Shor’s algorithm when equipped with a banded quantum Fourier transform. For the probability of a successful factorization, Fowler and Hollenberg obtained [12]

$$P^{(FH)} \sim 2^{-n(2/\log_2 N)^{b-1}} = 2^{-n e^{b \log_2 n}},$$

(4)

where

$$s_b^{(FH)} = 2 \times 2^{-b}.$$  

(5)

Since they pertain to different quantities, (3) and (4) cannot be compared directly. However, Fowler and Hollenberg's result (4) confirms Coppersmith's suggestion of a rapid (exponential) convergence of Shor's algorithm in $b$. While Fowler and Hollenberg used a stochastic model to arrive at their scaling result, (4), we use direct factorization of actual semiprimes $N$. This allows us to test the scaling relation (4) and derive an improved scaling relation for the performance of Shor’s algorithm with a banded quantum Fourier transform.

Shor’s algorithm determines the order $\omega$ of a seed $x$ for a given semiprime $N$ as the period of the function $f(t) = x^t \mod N$, $\ell$ integer, via a quantum Fourier transform that produces an output state $|\psi_{out}\rangle$, consisting of a superposition of all $n$-qubit binary states $|l\rangle$. A measurement of $|\psi_{out}\rangle$, then, has a high probability of collapsing into a state $|l\rangle$, where

$$l_j = \frac{2\pi j + \beta_j}{\omega}, \quad j = 0, \ldots, \omega - 1,$$

(6)

and $-1/2 < \beta_j < 1/2$ guarantees that $l_j$ is an integer. If $\omega$ is a power of 2, all $\beta_j$ are 0 and Shor’s algorithm performs perfectly, no matter what the bandwidth. Since for large $N$ the probability of encountering this case is practically 0, we do not consider this special case any further. In the general case (the most probable case), where $\omega$ is not a power of 2, we write

$$\omega = 2^r \alpha,$$

(7)

where $r$ and $\alpha$ are integers and $r$ is odd. In this case most of the $\beta_j$ are nonzero.

The probability of collapse into one of states (6) is

$$P(n,b) = \frac{1}{\alpha K^2} \sum_{j=0}^{K-1} \left| \sum_{k=0}^{K-1} \exp \left(i \Phi(n,s_j,l) - \Phi(n,b,s_j,l) \right) \right|^2$$

(8)

where

$$s_k = s_0 + k \omega, \quad k = 0, \ldots, K - 1,$$

and $s_{\nu}$, $0 \leq s_0 \leq \omega - 1$. We found that our results are insensitive to the choice of $s_0$. We used $s_0 = 0$ ($s_0 = n - 1$) in our analytical (numerical) calculations. Denoting by $a_{\alpha i}$ the $i$th binary digit of an integer $a$,

$$\Phi(n,s,l) = \sum_{m=0}^{n-1} \sum_{\mu=0}^{s_m-1} \frac{\Theta(n-1-m) \mu}{2^{m-\mu}}$$

(10)

in (8) is the total phase angle experienced by a state $|s\rangle$ mapped into a state $|l\rangle$ by a full, $n$-qubit quantum Fourier transform ($b = n - 1$), and

$$\Phi(n,b,s,l) = \sum_{m=0}^{n-b-1} \sum_{\mu=0}^{s_m-1} \frac{\Theta(n-b-1-m) \mu}{2^{m-\mu}}$$

(11)

is the “missing phase” due to the restriction of the bandwidth of the quantum Fourier transform to $b$ off-diagonal couplings [see Fig. 1(b)]. The exact maximum value of $\Phi$, consistent with Coppersmith’s bound (3), is

$$\Phi_{\text{max}}(n,b) = 2\pi \left[ 2^{b-1} (n-b) + 2^n - 2^b \right].$$

(12)

We evaluate $P(n,b)$ according to the following procedure. Given $n$ and $b$, we look for semiprimes $N = pq$ such that

$$n = [2 \log_2(N) + 1],$$

(13)

where $[\cdot]$ is the floor function, i.e., the largest integer smaller than $\cdot$. Then we randomly choose a seed $x$ of order $\omega$ and compute $P(n,b)$ according to (8). Since the $l_j$ values, (6), capture most (about 77%) but not all of the useful output of Shor’s algorithm [a measurement of $|\psi_{out}\rangle$ may collapse into an $|l\rangle$ state not contained in (6)] but equally useful for factoring], we normalize $P(n,b)$ to its maximal-bandwidth case $P(n,b = n - 1)$ to obtain the normalized probability,

$$P(n,b) = P(n,b)/P(n,b = n - 1).$$

(14)

We choose $P(n,b)$ in (14) as a quantitative measure for the performance of Shor’s algorithm as a function of $n$ and $b$.

Figure 2 shows $P(n,b)$ as a function of $n$ for four values of $b$, obtained by factoring up to 12 sample semiprimes for each $n = 9, \ldots, 39$. Already for $b = 4$, i.e., without implementing most of the rotation gates required by a full Fourier transform,
we observe excellent factoring performance in the 90% region over the entire range of \( n < 40 \). This observation has an immediate and important consequence for the construction of quantum computers: substantial hardware savings without significant sacrifice in performance. For fixed \( b \) and large \( n \), as predicted by (4), we observe exponential decay of \( P(n,b) \) as a function of \( n \). However, as extracted from Fig. 2 and discussed further below, our decay constants \( \xi_b \) are somewhat smaller than predicted by (5), resulting in an even better performance of Shor’s algorithm “in practice” than suggested by (5), based on a probabilistic model.

For small \( n \), not noticeable on the scale of Fig. 2, \( P(n,b) \) is not exponential. To analyze the small-\( n \) behavior, we start from (8) and note that for \( \beta_j = 0 \) the corresponding term in (8) contributes an amount \( 1/\omega \) to \( \tilde{P}(n,b) \). Since \( \beta_j = 0 \) occurs whenever \( j/r \) is an integer, there are \( \omega/r \) such cases, which contribute a total amount \( 1/r \) to \( \tilde{P}(n,b) \). Turning now to the \( j \) terms with \( \beta_j \neq 0 \), we found that \( \Phi(n,s_j,l_j) \) varies slowly with \( k \), while \( \varphi(n,b,s_j,l_j) \) is an erratic function of \( k \). Therefore, we write \( j \) terms with \( \beta_j \neq 0 \) in (8) approximately as

\[
\tilde{P}(n,b) \approx \frac{1}{\omega R^2} \left[ \sum_{k=0}^{K-1} \exp[i\Phi(n,s_k,l_j)](\exp[-i\varphi]) \right]^2, \tag{15}
\]

where \( \langle \ldots \rangle \) indicates a statistical average over the probability distribution of \( \varphi \). Numerically we found that, apart from isolated spikes, the distribution of \( \varphi \) is Gaussian in \( \varphi/\varphi_{\max} \) with a variance of about 1/200. Therefore, approximately,

\[
\langle \exp[-i\varphi(n,b)] \rangle \approx \exp[-\varphi^2_{\max}(n,b)/200]. \tag{16}
\]

The \( k \) sum in (15) can be evaluated analytically:

\[
\sum_{k=0}^{K-1} \exp[i\Phi(n,s_k,l_j)] = \frac{\sin(\pi \beta_j)}{\sin(\pi \beta_j/K)}. \tag{17}
\]

Since there are \((\omega - \omega/r)\) terms with \( \beta_j \neq 0 \), we obtain

\[
\tilde{P}(n,b) \approx \frac{1}{r} + \left( 1 - \frac{1}{r} \right) g \exp[-\varphi_{\max}(n,b)/100], \tag{18}
\]

where

\[
g = \frac{1}{\omega - \omega/r} \sum_{\beta_j \neq 0} \frac{\sin(\pi \beta_j)}{(\pi \beta_j)^2}. \tag{19}
\]

Defining

\[
f = \int_{-\frac{1}{2}}^{\frac{1}{2}} \frac{\sin(\pi \beta)}{(\pi \beta)^2} \, d\beta \approx 0.774, \tag{20}
\]

g can be expressed approximately as

\[
g \approx \frac{f - 1/r}{1 - 1/r^2}. \tag{21}
\]

and \( P(n,b) \), valid for small \( n \), as

\[
P(n,b) \approx \tilde{P}(n,b)/\tilde{f}. \tag{22}
\]

This fully analytical expression for (14) is shown as the solid lines in Fig. 3. We plot \( 1 - P(n,b) \) to increase our sensitivity in the small-\( n \) region. The analytical result captures the small-\( n \) behavior very well. Also shown are the crossover points (arrows) that mark the transition from the small-\( n \), nonexponential regime to the large-\( n \), exponential regime (dashed lines). The transition points move toward larger \( n \) for larger \( b \) so that the region of nonexponential behavior increases for increasing \( b \).

Returning to Fig. 2, we note that the slope of \( P(n,b) \) is a sensitive function of \( b \). Indeed, (4) predicts exponential scaling of the slope in \( b \). To test this prediction, we write \( P(n,b) \) in

\[
\text{FIG. 2. Probability for successful factorization of sample semiprimes } N \text{ of binary length } \log_2(N) \sim n/2 \text{ for details see (13)} \text{ using Shor's algorithm, supplied with a quantum Fourier transform of bandwidth } b. \text{ Shown are the data for up to } 12 \text{ randomly selected semiprimes } N \text{ per } n, \text{ factored with } b = 1 \text{ (triangles), } b = 2 \text{ (asterisks), } b = 3 \text{ (diamonds), and } b = 4 \text{ (squares). Solid lines are the scaling functions, (23), with decay constants, (24).}
\]

\[
\text{FIG. 3. Small-} n \text{ behavior of semiprimes } N \text{ for } b = 6 \text{ (squares), } b = 7 \text{ (crosses), and } b = 8 \text{ (circles). Solid lines are the analytical performance functions } P(n,b) \text{ in (22), with } \tilde{f} \rightarrow f \text{ according to (20). Dashed lines are their large-} n \text{, exponential behavior. Crossover points between the small-} n \text{, nonexponential and the large-} n \text{, exponential behavior are marked by arrows.}
\]
the form
\[ P(n,b) \approx 2^{-\xi_b (n-n_0)}, \]  
\[(23)\]
where \( \xi_b \) and \( n_0 \) are constants. We graphically extracted the decay constants \( \xi_b \) from Fig. 2 and found
\[ \xi_b = 1.1 \times 2^{-2b} \]
\[(24)\]
and \( n_b \approx 8 \). The quality of the scaling function, \( (23) \), is illustrated by the solid lines in Fig. 2, which are plotted using \( (23) \) with \( (24) \). Comparing \( (24) \) with \( (5) \), we find the same exponential dependence on \( b \). Our prefactor of 1.1, however, is smaller than the pre-factor predicted by \( (5) \), which, according to our results, implies a more optimistic performance scaling than predicted by \( (5) \).

As an additional test of performance scaling we plot
\[ \eta(n,b) = -\log_2 \left( \frac{P(n,b)}{\xi_b} \right) \]
versus \( n \) for all the data points in Fig. 2, where \( \xi_b \) is defined in \( (24) \). The result is shown in Fig. 4. The data points in Fig. 4 cluster around the straight line \( y = n - 8 \) (solid line in Fig. 4) as expected if the scaling in \( (23) \) were exact. The near-collapse of the data points in Fig. 4 confirms the approximate performance scaling of Shor’s algorithm with a banded quantum Fourier transform, as suggested in \( (23) \) and \( (24) \).

Extrapolating our results to \( n = 1000 \) qubits, \( P(n,b) \) reaches a performance level of 95% with a bandwidth of only seven qubits. Thus, without a substantial reduction of performance, of the order of half a million rotation gates can be saved when implementing a 1000-qubit quantum computer running Shor’s algorithm.

Scaling laws for Shor’s algorithm with a banded quantum Fourier transform

Y. S. Nam* and R. Blümel

Department of Physics, Wesleyan University, Middletown, Connecticut 06459-0155, USA

(Received 22 December 2012; revised manuscript received 19 February 2013; published 27 March 2013)

We investigate the performance of a streamlined version of Shor’s algorithm in which the quantum Fourier transform is replaced by a banded version that, for each qubit, retains only coupling to its b nearest neighbors. Defining the performance $P(n,b)$ of the n-qubit algorithm for bandwidth b as the ratio of the success rates of Shor’s algorithm equipped with the banded and the full-bandwidth ($b=n-1$) versions of the quantum Fourier transform, our numerical simulations show that $P(n,b) \approx 2^{-10n-20}$ for $n < n_c(b)$ (nonexponential regime) and $P(n,b) \approx 2^{-10n-30}$ for $n > n_c(b)$ (exponential regime), where $n_c(b)$, the location of the transition, is approximately given by $n_c(b) = b + 5.9 + \sqrt{7.7(b+2)-47}$ for $b \geq 8$, $\varphi_{\max}(n,b) = 2x(2-b)(n-b-2) + 2^{-b}$, and $n_c \approx 5.1 \times 2^{18}$. Analytically we obtain $P(n,b) \approx \exp[-\varphi_{\max}(n,b)/64]$ for $n < n_c(b)$ and $P(n,b) \approx 2^{-10n-30}$ for $n > n_c(b)$, where $\varphi_{\max} \approx x_{\max}^2 \times 2^{-b} \approx 1.19 \times 2^{-19}$. Thus, our analytical results predict the $\varphi_{\max}$ scaling ($n < n_c$) and the $2^{-b}$ scaling ($n > n_c$) of the data perfectly. In addition, in the large-$n$ regime, the prefactor in $\varphi_{\max}$ is close to the results of our numerical simulations, and in the low-$n$ regime, the numerical scaling factor in our analytical result is within a factor 2 of its numerical value. As an example we show that $b = 8$ is sufficient for factoring RSA-2048 with a 95% success rate.

DOI: 10.1103/PhysRevA.87.032333

PACS number(s): 03.67.Lx

I. INTRODUCTION

While the art of integer factoring lay dormant, literally for millennia, and not much progress beyond the crudest methods, such as trial division and looking for differences of squares, had been made [1], the advent of the widely used RSA cryptosystem [2] has recently propelled the factoring of large integers from the arcane recesses of an ancient mathematical discipline into the limelit of contemporary physics and mathematics. The reason is that a powerful factoring algorithm may be used in a frontal attack on the RSA cryptosystem, and, if successful, immediately reveals untold scores of government, military, and financial secrets [3,4]. No wonder, then, that the first substantial breakthrough in factoring in centuries, the quadratic number sieve [1,5], occurred shortly after the initial publication of the RSA method [2]. Using the quadratic number sieve, RSA keys with up to 100 decimal digits can now routinely be cracked [6] and are no longer safe. In 1993, the general number field sieve [7] added even more power to factoring attacks on RSA and was used successfully to factor the RSA challenge number RSA-768 (232 decimal digits) [8], which prompted the U.S. National Institute of Standards and Technology (NIST) to recommend retirement of all RSA keys with 1024 binary digits or less [9]. However, no matter how powerful these modern factoring algorithms are, they are based on classical computing algorithms, are executed on classical computers, and, without further improvements, will never be able to crack an RSA key consisting of 5000 decimal digits or more (see Sec. VIII). But not only classical computing profited from the advent of the RSA cryptosystem; so did quantum computing [10]. In 1994, Shor demonstrated that a certain quantum algorithm executed on a quantum computer is exponentially more powerful than any currently known classical factoring scheme and poses a real threat to RSA-encrypted data [11]. Since its inception in 1994, Shor’s algorithm has maintained its status as the gold standard in quantum computing, and progress in quantum computer implementation is frequently measured in terms of the size of semiprimes that a given quantum computer can factor [12,13]. While, compared with classical factoring algorithms, Shor’s algorithm is tremendously more powerful, it should not come as a surprise that, in order to break currently employed RSA keys, an enormous number of quantum operations still needs to be performed. Therefore, any advances in streamlining practical implementations of Shor’s algorithm that result in reducing the number of required quantum operations are welcome. A central component of Shor’s algorithm is the quantum Fourier transform (QFT) [10], and our paper focuses on how to perform this part of Shor’s algorithm with the least number of quantum gates and gate operations that still guarantee acceptable performance of the algorithm.

Our paper is organized in the following way. In Sec. II we present Shor’s algorithm. This section also serves to introduce the basic notation and explains the central position of the QFT in Shor’s algorithm. While the original version of Shor’s algorithm [11] is formulated with the help of a full implementation of the QFT, it turns out that a reduced, approximate version of the QFT, the banded QFT [14–16], yields surprisingly good results when used in conjunction with Shor’s algorithm. The banded QFT is introduced and discussed in Sec. III. In order to assess the influence of the banded QFT on the performance of Shor’s algorithm, we need an objective performance measure. Our performance measure is defined in Sec. IV. In Sec. V, based on the performance measure defined in Sec. IV, we investigate numerically the performance of a quantum computer for various bandwidths b as a function of the number of qubits n. We find that for fixed b the quantum computer exhibits two qualitatively different regimes, exponential for large n and nonexponential for small n. We also find that relatively small $b \lesssim 10$ are already
Appendix A. List of Publications

Y. S. NAM AND R. BLUMEL

PHYSICAL REVIEW A 87, 032333 (2013)

sufficient for excellent quantum computer performance, even for \( n \) so large as to be interesting for the factoring of semiprimes \( N \) of practical interest. These numerical findings are then investigated analytically in Sec. VI. In Sec. VIA, we show an important property of the performance measure, i.e., approximate separability, which allows us to analyze analytically the large-\( n \) behavior (Sec. VII) and the small-\( n \) behavior (Sec. VIIC) of the numerical data presented in Sec. V. In particular, we are able to predict analytically the scaling functions of the data in the large-\( n \) and small-\( n \) regimes. In Sec. VII we compare our work with the related pioneering work of Fowler and Hollenberg (henceforth, FH) [15]. While the final results are similar, our approach differs substantially from the approach in Ref. [15]. Factoring actual semiprimes, our approach is more realistic than the approach taken in Ref. [15] and may serve to check the results reported in Ref. [15]. We discuss our results in Sec. VIII and conclude the paper in Sec. IX. In order not to break the flow of exposition in the text, some technical material is relegated to three Appendixes. In Appendix A we prove the existence and uniqueness of an order 2 element for any semiprime \( N \). In Appendix B we compute an analytical bound for the maximal possible order \( \omega \) of a given semiprime \( N \). In Appendix C, we provide an auxiliary result on the distribution of an inverse factor of \( \omega \), needed for one of our analytical results reported in Sec. VI.

II. SHOR’S ALGORITHM

Progress in quantum computing happens in fits and starts. Periods of stagnation and pessimism are followed by unexpected breakthroughs and optimism. Shor’s algorithm is a case in point. Following a lull in quantum computing during which the only known quantum algorithms were of an “academic” nature, Shor’s algorithm, the first “useful” quantum algorithm, instantly revived the field when it burst on the scene, quite unexpectedly, in 1994 [11]. Shor’s algorithm is quantum mechanics’ answer to a task that is hard or impossible to perform on any classical computer: factoring large semiprimes \( N \). To accomplish this task, Shor’s algorithm makes use of the entire palette of quantum effects that result in an exponential speedup of the quantum algorithm with respect to any currently known classical factoring algorithm: superposition, interference, and entanglement. Shor’s algorithm is based on Miller’s algorithm [17], a classical factoring algorithm. Miller’s algorithm determines the factors of a semiprime \( N = pq \), where \( p \neq q \) are prime, according to the following procedure. First, we choose a positive integer \( 1 < x < N \), called the seed, relatively prime to \( N \), i.e., \( \gcd(x,N) = 1 \), where \( \gcd \) denotes the greatest common divisor. Then we determine the smallest positive integer \( \omega \), called the order of \( x \), such that

\[
x^\omega \mod N = 1.
\]

For Miller’s algorithm to work, we require (i) that \( \omega \) is even and (ii) that \( (x^{\omega/2} + 1) \mod N \neq 0 \). Both conditions need to be fulfilled. If either one is not, we need to choose another \( x \) and try again. There is a high probability that this will succeed after only a few trials [10,15,18]. Having found a seed \( x \) satisfying both conditions, we write (1) in the form

\[
[(x^{\omega/2} - 1)(x^{\omega/2} + 1)] \mod N = 0,
\]

which implies that \( N \) divides the product on the left-hand side of (2). This might be accomplished if \( N \) divides \( x^{\omega/2} - 1 \), which implies \( x^\omega \mod N = 1 \). This, however, is impossible, because \( \omega/2 < \omega \), and \( \omega \), according to (1), is the smallest such exponent. Another hypothetical possibility is that \( N \) divides the second factor in Eq. (2). This, however, is excluded according to condition (ii). The only remaining possibility is that \( p \) divides one of the factors in Eq. (2) and \( q \) divides the other. Appropriately naming the factors of \( N \), we have

\[
p = \gcd(x^{\omega/2} - 1, N), \quad q = \gcd(x^{\omega/2} + 1, N),
\]

and the factoring problem is solved. So, if Miller’s classical algorithm does the job, why do we need Shor’s quantum algorithm? The answer is that finding the order \( \omega \) on a classical computer is an algorithmically hard problem that, for a generic odd function, \( f \), need to report even periods may be found by a Fourier transform, the central idea of this idea [10,11,17,18], we work with a quantum computer consisting of two quantum registers, register I and register II. We assume that both registers consist of \( n \) qubits. In order to reliably determine \( \omega \) for a given \( N \), care must be taken to choose \( n \) at least twice as large as the number of binary digits of \( N \) [10,18]. We strictly observe this requirement in Sec. V (see Eq. (64)), where we present our numerical work. We start by initializing both registers to 0 such that the initial state of the quantum computer is

\[
|\psi\rangle = |0,\ldots,0\rangle_1 |0,\ldots,0\rangle_2.
\]

Next, we initialize register I with a superposition of all integers from 0 to \( 2^n - 1 \) by applying a single-qubit Hadamard transform [10] to each of the \( n \) qubits of register I, resulting in the state

\[
|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle_1 |0,\ldots,0\rangle_2.
\]

where we have introduced an intuitive equivalence, whereby an integer \( k \geq 0 \) is mapped onto the \( n \) qubits of a register according to the binary digits of \( k \). Now we make use of the function \( f \) defined in Eq. (4) to fill register II with the \( f \) images of register I. This results in the computer state

\[
|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle_1 |f(k)\rangle_2.
\]
This step entangles registers I and II. The function $f$ induces equivalence classes

$$[s_0] = \{s_0 + k\omega, 0 \leq k \leq K(s_0) - 1\} \quad (8)$$
on the $(0, \ldots, 2^n - 1)$ with representatives $0 \leq s_0 \leq \omega - 1$, where $K(s_0)$ is the smallest integer with $s_0 + K(s_0)\omega \geq 2^n$. In other words, $K(s_0)$ is the number of elements in the equivalence class $[s_0]$. Since the range of $s$ values is $2^n$ and the spacing is $\omega$, we obtain, approximately,

$$K(s_0) \approx \frac{2^n}{\omega}. \quad (9)$$

Because of the periodicity of $f$, each member of $[s_0]$ is mapped onto $f(s_0)$. Therefore, if a measurement of register II collapses this register into state $|f(s_0)\rangle$, the quantum computer is in the state

$$|\psi_i\rangle = \frac{1}{\sqrt{K(s_0)}} \sum_{k=0}^{K(s_0)-1} |s_0 + k\omega\rangle |f(s_0)\rangle. \quad (10)$$

We may now apply a QFT,

$$U^{(QFT)} = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |l\rangle \exp(2\pi i k/2^n) |k\rangle, \quad (11)$$
to register I of $|\psi_i\rangle$ to obtain

$$|\psi_f\rangle = \frac{1}{\sqrt{K(s_0)2^n}} \sum_{k=0}^{K(s_0)-1} \sum_{l=0}^{2^n-1} \exp(2\pi i l(s_0 + k\omega)/2^n) \times |l\rangle |f(s_0)s_0\rangle. \quad (12)$$

A measurement of register I then collapses $|\psi_f\rangle$ into $|l\rangle$ with probability

$$P(n, l, \omega) = \frac{1}{2^n} \sum_{k=0}^{K(s_0)-1} \left| \exp\left(2\pi i k\omega/2^n\right) \right|^2 = \frac{\sin^2(K\pi\omega/2^n)}{2^n K^2 \sin^2(\pi\omega/2^n)} \quad (13)$$

where here and in the following we have suppressed the argument $s_0$ of $K$. Apparently, $P(n, l, \omega)$ is sharply peaked at $l$ values for which $\omega l/2^n$ is close to an integer. As a consequence, these $l$ values will appear as a result of measurement with a high probability. Subsequent analysis of the measured peak location on a classical computer then reveals the factors of $N$ with a high probability [10]. This step is called classical postprocessing [10,18]. Equation (13) is the starting point of our analysis of the performance of Shor’s algorithm with a banded QFT in Sec. IV.

Several experimental demonstrations of Shor’s algorithm have been published [12,13,19–21]. Since it is exceedingly difficult to experimentally control more than a handful of qubits, the numbers $N$ factored in these experiments are very small, currently not exceeding $N = 21$ [13]. Therefore, reaching higher $N$ is facilitated by reducing the requirements to run Shor’s algorithm on a quantum computer. One such optimization is the use of an approximate, banded QFT [14] instead of the full QFT (11). Further optimization is possible by using a banded version of the semiclassical QFT [22] defined in the following section.

**III. BANDED QUANTUM FOURIER TRANSFORM**

A direct circuit implementation of the Fourier transform defined in Eq. (11) requires $n(n + 1)/2$ two-qubit quantum gates [10]. In Ref. [22], it was shown that, when followed by measurements, as required by Shor’s algorithm, an equivalent quantum circuit, consisting exclusively of single-qubit gates, is exactly equivalent to the two-qubit realization of the QFT.

Figure 1(a) illustrates this single-qubit realization of the quantum Fourier transform for the special case of five qubits (we classify the conditional rotation gates $\theta$ in Fig. 1 as single-qubit gates since they are controlled by classical input and act coherently only on a single qubit). This circuit still requires $\sim n^2$ gate operations, but since they are performed by single-qubit gates, experimental implementation of this single-qubit circuit is considerably simpler. In contrast to the full two-qubit implementation of the QFT, where the measurements may occur simultaneously at the end of the quantum computation, the measurements in the single-qubit version of the QFT [denoted by the M gates in Fig. 1(a)] occur sequentially and their (classical) measurement results are used to control the phase rotation gates $\theta$. As first pointed out by Coppersmith [14], even this quantum circuit may still be optimized by working with an approximate, banded QFT as illustrated in Fig. 1(b).

The banded QFT $U^{(QFT)}_b$ [see Fig. 1(b)] is obtained from the full implementation of the single-qubit QFT [see Fig. 1(a)] by retaining only the coupling to $b$ nearest neighbors of a given qubit. As illustrated in Fig. 1(b) for the case $b = 1$, this results in a banded structure of the corresponding quantum circuit [16]. The name is also justified on theoretical grounds since the unitary matrix representing the circuit shown in Fig. 1(b) has a banded structure [23]. The banded QFT of bandwidth $b$ is the basis of our work presented in the following sections.

**IV. PERFORMANCE MEASURE**

The key idea of Shor’s algorithm is to use superposition and entanglement to steer the quantum probability into qubits that
correspond to numbers encoded in binary form, which will then, as a result of classical postprocessing, reveal the factors of \( N \). Our first task, therefore, is to locate the useful peaks after the QFT is performed. In order to define our performance measure, we are interested in how sharp these peaks are in \( l \).

For this purpose, we note that \( P(n,l,\omega) \) [see Eq. (13)] (up to a factor) is of the form
\[
f(z) = \frac{\sin^n(Kz)}{\sin^n(z)},
\]
where \( K \) is a large integer, \( z \) is a real number, and \( f(z) \) is sharply peaked at integer multiples of \( \pi \). Since the shape of \( f(z) \) is the same for \( z \) in the vicinity of each peak, it suffices to investigate the peak at \( z = 0 \) to determine the width of all the other peaks of \( f(z) \). We define the half-width \( \Delta z \) of \( f(z) \) by requiring
\[
f(\Delta z) = \frac{1}{2}.
\]

Inspired by a second-order Taylor-series expansion of (15), we obtain the heuristic formula
\[
\Delta z \approx \frac{1.39}{K},
\]
which, for \( K > 10 \), satisfies (15) to better than \( 10^{-3} \). Applied to \( \tilde{P}(n,l,\omega) \) in Eq. (13), we have
\[
z = \frac{\pi\omega}{2n},
\]
and, therefore,
\[
\Delta z = \frac{\pi\omega}{2n} \Delta l \approx \frac{1.39}{K},
\]
from which we obtain
\[
\Delta l \approx \left( \frac{2}{\omega K} \right) \left( \frac{1.39}{\pi} \right) \approx 0.44,\]
where we have used (9). This result shows that the full width at half-maximum of the \( l \) peaks is only about one state and that this width is “universal” in the sense that it is independent of \( K, \omega, \) and \( n \).

Since a peak in \( \tilde{P}(n,l,\omega) \) occurs whenever \( \omega l/2n \) is close to an integer, we define the \( l \) integer closest to the peak number \( j \) according to
\[
l_j = \left( \frac{2n}{\omega} \right) j + \beta_j, \quad j = 0, 1, \ldots, \omega - 1.
\]
where \( \beta_j \), a rational number, ranges between \(-1/2\) and \(1/2\). Since the peaks in \( P(n,l,\omega) \) are universal in the sense and contain basically only a single state, namely, \( l \), defined in Eq. (20), we use
\[
P(n,l,\omega) \equiv \tilde{P}_j(n,\omega)
\]
as the basis for our performance measure.

Although the width of the peaks of \( P(n,l,\omega) \) is narrow—according to (19), of the order of a single state—and although \( |l_j| \) carries most of the probability in the peak number \( j \) of \( P(n,l,\omega) \) (approximately 77% on average), there are nevertheless several states \( |l| \) inside of peak number \( j \) that occur with a low but still appreciable probability in a measurement of \( |\psi_j\rangle \) in Eq. (12). These states are also useful for factoring during classical postprocessing (see Sec. II and [10,18]), and the question arises if these states should be included in the performance measure. Indeed, instead of determining the performance of Shor’s algorithm on the basis of the single state \( |l_j\rangle \), FH [15], e.g., base their performance measure on the two closest states to the peaks in \( P(n,l,\omega) \). We found that including more states in the performance measure is not necessary, since the width of the Fourier peaks in \( l \) is independent of the bandwidth \( b \). At first glance this is surprising since, intuitively, we would think that the quality of the QFT should deteriorate with decreasing bandwidth \( b \), possibly accompanied by a broadening of the Fourier peaks in \( l \). That this is not so, and that the widths of the Fourier peaks are indeed independent of \( b \), is demonstrated in Fig. 2 for the case \( N = 247 \) for \( b = 1, 2, 3, 10 \). Independent of \( b \), the vertical line in the figure cuts each Fourier peak at approximately its midpoint, thus demonstrating that the widths of the Fourier peaks in \( l \) are indeed independent of \( b \). Thus, upon a change in \( b \), all \( l \) states under a Fourier peak respond in unison to the change in \( b \). Therefore, a single \( l \) state, such as \( l_j \), is an excellent representative of all the \( l \) states in its immediate vicinity.

Defining \( \tilde{P}_j(n,b,\omega) = \tilde{P}(n,l,\omega) \) as the probability of obtaining \( |l_j\rangle \) in a measurement of \( |\psi_j\rangle \) if, instead of the full QFT, the banded QFT (see Sec. III) is used, and taking into account that the widths of the peaks in \( \tilde{P}(n,b,\omega) \) do not change as \( b \) is varied, we use the ratio of the total probability of collapse into one of the states \( |l_j\rangle \), given the bandwidth \( b \), to that of the full bandwidth \( b = n - 1 \), to capture the overall probability of obtaining the useful \( |l| \) states in the vicinity of \( |l_j\rangle \). Thus, the normalized ratio is of the form
\[
\frac{P(n,b,\omega)}{P(n,b,\omega)\tilde{P}(n,b,\omega)\tilde{P}(n,b,\omega)} = \prod_{j \neq 0} \tilde{P}_j(n,b,\omega)
\]
and \( \tilde{P}(n,b = n - 1,\omega) \) is the probability of collapsing into any one of the set of useful states \( |l_j\rangle \) as a result of measuring \( |\psi_j\rangle \),
where $|\psi_i\rangle$ is generated from $|\psi_i\rangle$ by application of the full QFT $\hat{U}^{(\text{QFT})}$ defined in Eq. (11). We use $P(n,b,\omega)$, defined in Eq. (22), as our performance measure throughout this paper.

Next, we derive an analytical expression for $\hat{P}_i(n,b,\omega)$, valid for any bandwidth $0 \leq b \leq n - 1$, that can be used in our performance measure, (22). In order to find $\hat{P}_i(n,b,\omega)$ we need to descend to the qubit-by-qubit level, since the bandwidth $b$ in $\hat{U}^{(\text{QFT})}_b$ refers to interqubit spacing on the qubit level in the circuit diagram of $\hat{U}^{(\text{QFT})}_b$ [see Fig. 1(b)]. We start with a representation of the QFT in bit notation,

\[
\hat{U}^{(\text{QFT})} |s, l\rangle = \frac{1}{\sqrt{2^m}} \sum_{j=0}^{2^m-1} e^{2\pi i s j} |j\rangle |0\rangle,
\]

where $s_j l_j$ indicates the $v$th binary digit of $s$ ($v$th binary digit of $l$) and

\[
(s_0 s_1 s_{n-1} \ldots s_0) = \sum_{v=0}^{n-1} s_v 2^{-(v+1)}.
\]

For bandwidth $b$, $\hat{U}^{(\text{QFT})}_b |s, l\rangle$ then becomes

\[
\hat{U}^{(\text{QFT})}_b |s, l\rangle = \frac{1}{\sqrt{2^m}} \prod_{v=0}^{n-1} \sum_{l_v} e^{2\pi i (s_v l_{v} + s_{v-1} l_{v-1}) \ldots (s_0 l_0)} |l_{n-1}\rangle |0\rangle,
\]

We may also write

\[
\hat{U}^{(\text{QFT})}_b |s, l\rangle = \sum_{j=0}^{2^m-1} B(s, l) |j\rangle |0\rangle,
\]

where

\[
B(s, l) = \frac{1}{\sqrt{2^m}} \exp \left\{ 2\pi i \sum_{m=0}^{n-1} [\lambda_m, l] - \lambda_{m,b+1} |s_{n-1}| + l_{n-1} \right\}
\]

and

\[
\lambda_m, l = (s_0 s_1 s_{n-1} \ldots s_0) |l_{n-1}| + l_{n-1}
\]

i.e., $\lambda$ zeros follow the binary point. Defining

\[
S_i(s, l) = \sum_{m=0}^{n-1} \lambda_m, |s_{n-1}| + l_{n-1}
\]

we may express $B(s, l)$ in the form

\[
B(s, l) = \frac{1}{2^{n+1}} \exp[2\pi i (S_0(s, l) - S_{b+1}(s, l))].
\]

Sorting indices, $S_i(s, l)$ may be written in the form

\[
S_i(s, l) = \frac{1}{2} \sum_{m=b+1}^{n} \sum_{j=0}^{2^{m-b}-1} S_{m-1, l} |j\rangle |2^{m-b}\rangle
\]

We are now ready to apply the banded QFT to register I of the initial state $|\psi_i\rangle$[see Eq. (10)] and obtain, with (27)

and (31),

\[
\hat{U}^{(\text{QFT})}_b |\psi_i\rangle = \hat{U}^{(\text{QFT})}_b \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} |s_k\rangle = \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} \sum_{l=0}^{2^n-1} B(s_k, l) |l\rangle
\]

\[
= \frac{1}{\sqrt{2^m K}} \sum_{k=0}^{K-1} \sum_{l=0}^{K-1} \exp[2\pi i (S_0(s_k, l) - S_{b+1}(s_k, l))] |l\rangle.
\]

From this we obtain

\[
\hat{P}_i(n,b,\omega) = \frac{1}{2^{n+1}} \sum_{k=0}^{K-1} \exp[2\pi i (S_0(s_k, l) - S_{b+1}(s_k, l))] |l\rangle
\]

which, using the expanded form, (32), of $S$, can be written in the form

\[
\hat{P}_i(n,b,\omega) = \frac{1}{2^{n+1}} \sum_{k=0}^{K-1} \exp[i \Phi(n, s_k, l) - i \omega(s_k, n, l)] |l\rangle
\]

where

\[
\Phi(n, s_k, l) = \pi \sum_{m=0}^{n-1} \sum_{j=0}^{2^m-n-1} S_{m-1, l} |j\rangle |2^{m-n}\rangle
\]

and

\[
\psi(n, s_k, l) = \pi \sum_{m=0}^{n-1} \sum_{j=0}^{2^m-n-1} \frac{S_{m-1, l} |j\rangle |2^{m-n}\rangle}{2^{m-n}}.
\]

While $\Phi$ in Eq. (36) is already in a form useful for numerical calculations, we now derive an expression for $\exp(\Phi)$, which is more convenient for the analytical calculations in Sec. VI. We start by summing (36) in reverse order over
Using the formula
\[ \exp(\frac{\pi i}{\kappa\Omega\delta}) = \exp\left(\frac{\pi i \omega \beta}{\kappa\Omega\delta}\right) \]
we obtain
\[ \exp(i\Phi(n,s,l)) = \exp\left(\frac{2\pi i}{K}\right) \]
Thus we obtained a closed-form, analytical expression for \( \exp(i\Phi) \).

Although [because of the presence of \( \psi(n,b,s,l) \)] in Eq. (35) not useful for the exact evaluation of (35), a well-justified approximation performed in Sec. VI allows us to compute
\[ \Omega(n,l,\omega) = \sum_{k=0}^{K-1} \left| \exp[i\Phi(n,s,l)] \right|^2 \]
separately. Using the formula for computing geometric sums, we obtain
\[ \Omega(n,l,\omega) = \sum_{k=0}^{K-1} \left( \exp(2\pi i\omega\beta_1/2^n) \right)^2 \]
\[ = \frac{1 - \exp(2\pi i\omega\beta_1/2^n)}{1 - \exp(2\pi i\omega\beta_1/2^n)} \]
With (9) we obtain
\[ \Omega(n,l,\omega) \approx \frac{1 - \exp(2\pi i\omega\beta_1)}{1 - \exp(2\pi i\omega\beta_1/2^n)} \]
\[ \approx e^{i\pi\omega\beta_1} K/\pi \]
Since \( \psi(n,b) = n - 1, \omega = 0 \), we note in passing that
\[ \hat{P}_{j}(n,b = n - 1, \omega) = \frac{1}{2^n} \left| \Omega(n,l,\omega) \right|^2 \]
We also need an analytical expression for the maximum value \( \psi_{\text{max}}(n,b) \) of \( \psi(n,b,s,l) \), defined as
\[ \psi_{\text{max}}(n,b) = \max_{k,j} \psi(n,b,s,l) \]
From (37) it is clear that \( \psi_{\text{max}} \) is obtained by setting all \( l_{[\alpha+1]} \) and \( l_{[\alpha]} \) values equal to 1. This procedure yields
\[ \psi_{\text{max}}(n,b) = \pi \sum_{m=0}^{n-1} \sum_{l=0}^{2^{m+1}-1} \frac{1}{2^{m+1} - n} \]
Only the formula for evaluating geometric sums is needed to compute the value of \( \psi_{\text{max}} \) in Eq. (53). We obtain
\[ \psi_{\text{max}}(n,b) = 2\pi[2^{b-1}((n-b) - 2^{-b} + 2^{-n})] \]
We now show that a quantum computer performs perfectly, no matter what \( b \) is, if \( \omega \) is a power of 2, i.e.,
\[ P(n,b,\omega) = 1 \quad \text{for} \quad \omega = 2^a, \quad a \geq 0 \text{ integer} \]
For such an \( \omega \), we note that (i) the \( a \)th binary digit of any \( l_j \) is 0 for \( k \leq n - a \) since, according to (20),
\[ l_j = 2^{a-k} j, \quad j = 0, 1, \ldots, \omega - 1 \]
is already an integer, which implies \( \beta_j = 0 \); and (ii) the \( a \)th binary digit of any equivalence class element in \( l_{[\alpha]} \) [see Eq. (8)] for \( 0 \leq i < \alpha \) is identical to that of \( s_0 \). Thus, we
write \( \psi(n,b,s,l) \) in Eq. (37) in the form
\[
\psi(n,b,s,l) = \pi \left( \sum_{m=0}^{n-1} \sum_{\mu=0}^{m-1} \frac{\theta_{[m-1]}[\theta_{\mu}]}{2^{m-\mu}} + \sum_{m=b+1}^{n} \sum_{\mu=0}^{m-1} \frac{\theta_{[m-1]}[\theta_{\mu}]}{2^{m-\mu}} \right)
\]

where the second equality was obtained using observation (i). Now, we observe that the \( n - m - 1 \)th digit of \( s \) is bounded between 0 and \( \alpha - b - 2 \) inclusively. Then, using observation (ii), we obtain
\[
\psi(n,b,s,l_j) = \pi \left( \sum_{m=0}^{n-1} \sum_{\mu=0}^{m-1} \frac{(s_j)\theta_{[m-1]}[\theta_{\mu}]}{2^{m-\mu}} \right) = \bar{\psi}_j,
\]

where \( \bar{\psi}_j \) is a constant for any \( s_j \) and a given \( l_j \). Inserting (58) in Eq. (55), \( \bar{P}(n,b,\omega) \) becomes
\[
\bar{P}(n,b,\omega) = \frac{1}{2^N K} \sum_{l=0}^{K} e^{i\sum_{k=0}^{n-1} \psi_k} \sum_{k=0}^{n-1} e^{i\sum_{k=0}^{n-1} \psi_k} = \frac{1}{2^N} \left( \frac{\Omega(n,l_j,\omega)}{\omega} \right)^2 \bar{P}(n,b = n - 1,\omega),
\]

where we have used (48) and (51). With (23) and (59) we obtain
\[
\bar{P}(n,b,\omega) = \sum_{j=0}^{n-1} \bar{P}(n,b = n - 1,\omega) = \bar{P}(n,b = n - 1,\omega).
\]

Therefore, with (22), the normalized probability (the performance measure) \( P(n,b,\omega) \) reads
\[
P(n,b,\omega) = \bar{P}(n,b = n - 1,\omega) \bar{P}(n,b = n - 1,\omega) = 1,
\]

which completes the proof.

Since \( \omega = 2 \) always exists (see Appendix A), this is an important observation, since the corresponding quantum computer works perfectly in this case for any \( n \) and any \( b \). The trick, of course, is to find the seed \( x \) that yields \( x^2 \mod N = 1 \). This, however, is an unsolved problem for large \( N \).

If \( \omega \) is not a power of 2, we write it in the form
\[
\omega = r^2 \alpha, \quad r, \alpha \text{ integer},
\]

where \( r \) is odd. For such an \( \omega \), according to (20), we may write \( l_j \) as
\[
l_j = \left( \frac{r^n}{r} \right) j + \beta_j,
\]

Therefore, if \( j \) is a multiple of \( r \), we have \( \beta_j = 0 \) and \( \bar{P}(n,b,\omega) = 1/\omega \), which is proved by following the corresponding steps for the case where \( \omega \) is a power of 2. This means that the contribution of these \( j \) values to \( \bar{P}(n,b,\omega) \) is \( 1/r \). This is a constant contribution, which does not depend on either \( n \) or \( b \). Therefore, if for large \( n \) the contributions to \( \bar{P}(n,b,\omega) \) tend to 0 for the \( l_j \) peaks for which \( j \) is not a multiple of \( r \), we expect \( \bar{P}(n,b,\omega) \) to approach \( 1/r \) for large \( n \). This is demonstrated in Fig. 3, which shows \( \bar{P}(n,b = 1,\omega = 6) \) as a function of \( n \). Since in this case \( \omega = 3 \times 2^1 \), we expect \( \bar{P}(n,b = 1,\omega = 6) \) to approach \( 1/3 \), which is clearly confirmed in Fig. 3.

V. NUMERICAL RESULTS

In this section we explore, numerically, the performance of Shor’s algorithm supplied with a banded QFT of bandwidth \( b \). The performance is measured objectively with the help of the quantitative performance measure \( P(n,b,\omega) \) defined in Eq. (22). In contrast to a similar investigation by FH [15], who use an effective \( \omega \) for the investigation of the performance of the banded Shor algorithm, we opted for a more realistic simulation of the performance of Shor’s algorithm using ensembles of semiprimes \( N \) together with their exact associated orders \( \omega \). Thus, our procedure for computing the performance measure is as follows. For a given \( n \) we choose an ensemble of semiprimes \( N = pq \) such that
\[
n = [2 \log_2(N) + 1].
\]

where \( \lfloor \cdots \rfloor \) is the floor function [24]. This ensures that \( n \) is at least twice as large as the number of binary digits of \( N \), as required to reliably determine the order \( \omega \) with an \( n \)-qubit quantum computer [18,25,26]. For each \( N \) we compute its set

FIG. 3. Probability \( \bar{P}(n,b = 1,\omega = 6) \) as a function of \( n \) for 14 semiprimes \( N \) with seeds chosen such that \( \omega = 6 \). As expected, the data clearly asymptote to the value 1/3.

032333-7
of orders \( \{a_1, \ldots, a_{d(N)}\} \), where \( a(N) \) is the number of orders for given \( N \). We also define the multiplicity of a given order \( \omega \) as the number \( v(\omega) \) of seeds \( x \) of order \( \omega \). Thus equipped, we compute the performance \( P_n(n,b) \) as the properly weighted average,

\[
P_n(n,b) = \frac{1}{\varphi_E(N)} \sum_{j=1}^{a(N)} v(\omega_j) P(n,b,\omega_j),
\]

where \( P(n,b,\omega) \) is defined in Eq. (22) and \( \varphi_E(N) \) is Euler’s totient function [27].

In Fig. 4(a) we show \( P_n(n,b) \) for various choices of \( N \) for \( b = 1, \ldots, 4 \) and \( n \) ranging from \( n = 9 \) to \( n = 33 \). Plot symbols correspond to particular \( N \) values and there are up to 7 semiprimes \( N \) per \( n \). Overall we see that the data exhibit exponential behavior on average, which is well represented by the fit lines,

\[
P_\sim(n,b) = 2^{-x_b(n-b)}, \quad \xi_b = 1.1 \times 2^{-2b}, \tag{66}
\]
drawn through the data points. In Sec. VI B we present an analytical model that explains the \( b \) scaling of (66) and, in addition, reproduces the prefactor in Eq. (66) within 10%. Figure 4(b) shows corresponding data for \( b = 5, \ldots, 8 \). Again, the data points behave exponentially and are well approximated by the fit lines defined in Eq. (66). This illustrates that the \( b \) and \( n \) scaling in Eq. (66) holds over a considerable range of \( b \) and \( n \) values.

While on the large scale of Fig. 4 the data show exponential behavior, looking more closely at the small-\( n \) regime, we see definite deviations from exponential behavior. Plotting \( 1 - P(n,b) \) magnifies the \( P(n,b) \) behavior in the small-\( n \) region and clearly brings out the deviations from exponential behavior. This is illustrated in Fig. 5, which shows the data in Fig. 4, plotted as \( 1 - P(n,b) \). The dashed lines in Fig. 5 are the exponential fit lines defined in Eq. (66). We see that, even on this magnified scale and in the large-\( n \) regime, the data are well represented by the exponentials, (66). For small \( n \), however, the data clearly deviate from exponential but are well fit by the solid lines representing the function [16]

\[
P_\sim(n,b) = \tilde{P}_\sim(n,b) / f, \tag{67}
\]

where

\[
f = \int_{-1/2}^{1/2} \frac{\sin^2(\pi \beta)}{(\pi \beta)^2} d\beta \approx 0.774 \tag{68}
\]
Appendix A. List of Publications

SCALING LAWS FOR SHOR’S ALGORITHM WITH A

and

\[ \hat{P}_n(n,b) = \left( \frac{1}{2} \right)^b + \left( 1 - \frac{1}{2} \right) \left( \frac{n}{2n - 1} \right) \left( \frac{1}{2} \right)^b \times \exp \left\{ -\psi_{\max}^2(n,b)/100 \right\}, \quad (69) \]

where \( \psi_{\max} \) is given in Eq. (54), \( r \) is defined in Eq. (62), and \( \left( \frac{1}{2} \right) \) is \( 2^4 \times 8/2^6 \) (see Appendix C). Based on our numerical evidence, we conclude that \( P(n,b) \) shows a clear transition from nonexponential behavior for small \( n \) to exponential behavior for large \( n \). The arrows in Fig. 5 point to the locations of the transition between the two regimes and are the intersection points between the functions defined in Eqs. (66) and (67).

Combining expressions (66) and (67), we derive an analytical expression, \( n_t(n,b) \), for the transition points between the two different regimes for given \( b \). The transition points \( n_t \) are defined as the \( n \) value at which (66) equals (67). A useful analytical formula, approximately valid for \( b \approx 8 \), is obtained in the following way. For \( b \approx 8 \), we noted numerically that the \( \frac{1}{\tau} \) terms in Eq. (69) may be neglected, resulting in only a small shift of \( n_t \), about 2 units in \( n \). Therefore, to lowest order, \( P_c(n,b) = P_r(n,b) \) results in

\[ \psi_{\max}^2(n,b)/100 = \xi_1 \ln(2)(n_t - 8), \quad (70) \]

which implies

\[ 1.1 \times 2^{-2b} \ln(2)(n_t - 8) = 4 \pi^2 \frac{\xi_1}{100} 2^{-b+1}(n_t - b + 2) + 2^{-n_t^2}/2. \quad (71) \]

At this point we note that the transitions \( n_t \) between the two regimes occur at \( n \) values for which

\[ 2^{-n_t} < 2^{-b}, \quad (72) \]

which implies that we can safely neglect the \( 2^{-n_t} \) term in Eq. (71). This turns (71) into the quadratic equation

\[ n_t^2 - 2n_t(C + b + 2) + 16C + (b + 2)^2 = 0, \quad (73) \]

where we have defined

\[ C = \frac{55 \ln(2)}{\pi^2}. \quad (74) \]

Solving (73) yields

\[ n_t = b + 5.9 + \sqrt{7.7(b + 2) - 47}. \quad (75) \]

Expression (75) for the transition points shows that the onset of exponential behavior is shifted toward larger \( n \) for larger \( b \). Formula (75) for the transition points \( n_t(n,b) \) is useful for extrapolating into the practically relevant qubit regime \( n \geq 4000 \), where classical computers cannot follow any more. In this classically inaccessible regime, we can then decide on the basis of (75), e.g., whether for given \( b \) and very large \( n \), formula (66) or formula (67) should be used to predict the performance of the quantum computer. For \( b = 1 \), ..., 4, as shown in Fig. 5(a), the transition is poorly defined, whereas, as shown in Fig. 5(b), the transition is progressively better defined as \( b \) increases. That this trend continues is shown in Fig. 6, which shows data for \( b = 10, 15, \) and 20. We also see that the quality of the fit of the data with (67) improves for increasing \( b \). The sharp cutoff displayed by \( P_c(n,b) \) in Fig. 6 at \( n = 11 (b = 10), n = 16 (b = 15), \) and \( n = 22 (b = 20) \) is also understood since, according to (54), \( \psi_{\max}(n,b) = 0 \) for \( n = b + 1 \).

VI. ANALYTICAL RESULTS

Our analytical investigation of the performance measure starts with (35). Analytically and numerically we found that \( \Phi(n,s,j) \) is a slow function of \( k \), whereas \( \psi(n,b,s,j) \) is a fast, erratic function of \( k \). Therefore, we can write, approximately,

\[ \hat{P}_f(n,b,\omega) \approx \frac{1}{2^f K} \left[ \sum_{j=0}^{K-1} |\Omega(n,s,j,\omega)|^2 |\langle e^{-i\omega}n_k, s, j,\omega \rangle|^2 \right] \]

\[ = \frac{1}{2^f K} \Omega(n,s,j,\omega)^2 |\langle e^{-i\omega}n_k, s, j,\omega \rangle|^2, \quad (76) \]

where \( \Omega(n,s,j,\omega) \) is defined in Eq. (48) and

\[ \langle e^{-i\omega}n_k, s, j,\omega \rangle = \frac{K^{-1}}{K} \sum_{j=0}^{K-1} e^{-i\omega n_k, s, j,\omega}. \quad (77) \]

With (22), (23), and (51) we now obtain

\[ P(n,b,\omega) = \frac{K^{-1}}{K} \sum_{j=0}^{K-1} |\Omega(n,s,j,\omega)|^2 |\langle e^{-i\omega}n_k, s, j,\omega \rangle|^2 \quad (78) \]

\[ \sum_{j=0}^{K-1} |\Omega(n,s,j,\omega)|^2 |\langle e^{-i\omega}n_k, s, j,\omega \rangle|^2. \]

We now proceed with a slightly less but still extremely accurate approximation by separating (78) in \( j \), which then yields

\[ P(n,b,\omega) = \frac{1}{omega} \sum_{j=0}^{omega} |\langle e^{-i\omega}n_k, s, j,\omega \rangle|^2 \quad (79) \]

where \( \langle \cdot \cdot \cdot | \langle \cdot \cdot \cdot \rangle \rangle_k \) and \( \langle \cdot \cdot \cdot | \langle \cdot \cdot \cdot \rangle \rangle_j \) are averages over \( k \) and \( j \), respectively. This expression for the performance measure \( P(n,b,\omega) \) is the basis of our analytical work.
Since (79) is based on the validity of the separation in $k$ and $j$, both are investigated in detail in Sec. VI A. A random model is used in Sec. VI B to evaluate (79) analytically in the large-$n$ regime. This yields an analytical explanation for the $b$ scaling in Eq. (66) and excellent agreement with the prefactor of the exponential term in Eq. (66). In Sec. VI C, again assuming separation in $k$ and $j$, we then arrive at an analytical formula describing the small-$n$ regime, which predicts the functional form and the $b$ scaling of (67) very well and, also, provides an estimate of the overall scaling factor.

A. Separability

In this section we investigate in detail the quality of the separations in $k$ and in $j$, which lead to our jump-off point, (79), for the analytical calculations reported in Sec. VI B and Sec. VI C. We start with justifying the separation in $k$. To this end we define

$$A^{(k)} = \sum_{j=0}^{n-1} \sum_{k=0}^{K-1} e^{i\Omega(n,k,j)} e^{-i\Omega(n,b,k,j)} \right|^2 \quad (80)$$

and

$$B^{(k)} = \sum_{j=0}^{n-1} \sum_{k=0}^{K-1} e^{i\Omega(n,k,j)} e^{-i\Omega(n,b,k,j)} \right|^2 \quad (81)$$

and compute the relative error

$$\Delta^{(k)} = \frac{|A^{(k)} - B^{(k)}|}{|A^{(k)}|} \quad (82)$$

incurred by the $k$ separation. Figure 7 shows $\Delta^{(k)}$ as a function of $b$ for various choices of $N$. We clearly see that $k$ separation is an excellent approximation, which produces negligible, exponentially small errors. We plotted the line $\Delta = 2^{-2.5b - 5.5}$ through the data to guide the eye. This line shows that the relative error of $k$ separation vanishes exponentially in $b$.

Turning now to the $j$ separation, we define

$$A^{(j)} = B^{(j)} \quad (83)$$

and

$$B^{(j)} = \sum_{j=0}^{n-1} |\Omega(n,j,\omega)|^2 \sum_{k=0}^{K-1} |e^{-i\Omega(n,b,k,j)}|^2 \quad (84)$$

and compute the relative error of $j$ separation

$$\Delta^{(j)} = \frac{|A^{(j)} - B^{(j)}|}{|A^{(j)}|} \quad (85)$$

Figure 8 shows $\Delta^{(j)}$ as a function of $b$ for various choices of $N$. Apparently, while a bit less accurate than $k$ separation, $j$ separation is still highly accurate, improving exponentially with $b$. This is seen from the fit line $\Delta = 2^{-2.5b - 1.5}$ through the data in Fig. 8, which also shows that $\Delta^{(k)}$ and $\Delta^{(j)}$ decay with the same exponential factor in $b$ and are offset by a constant only.

B. Large-$n$, exponential regime

In this section we evaluate (79) analytically in a model in which we treat $s_i$ and $l_i$ as independent random variables. This model, obviously, cannot capture the correlations between $s_i$ and $l_i$ introduced by $\omega$ and yields $P(n,b,\omega)$, which is independent of $\omega$. Therefore, the $\omega$ average in Eq. (65) is trivial and $P_\omega(n,b)$ does not depend on $N$ either. Therefore, we write $P_R(n,b) \rightarrow P(n,b)$ as the prediction of the random model. However, even in this model, where $\omega$ correlations are entirely neglected, it is hard to evaluate the expectation value of the exponential. Therefore, we proceed to evaluate (79) via its moment expansion,

$$\langle |(e^{-i\phi})_i|^2 \rangle_j = 1 - \left[ \langle |\phi_i|^2 \rangle_j - \langle |\psi_i|^2 \rangle_j \right] + \left[ \frac{1}{12} \langle |\psi_i|^4 \rangle_j \right] + \left[ \frac{1}{4} \langle |\psi_i|^2 \rangle_j - \frac{1}{3} \langle |\phi_i|^2 \rangle_j \right] \pm \cdots , \quad (86)$$

FIG. 7. Relative error $\Delta^{(k)}$ of $k$ separation as a function of $b$ for several semiprimes $N$. The data show that the error is negligible. The fit line, $\Delta = 2^{-2.5b - 5.5}$ (dashed line), shows that the relative error vanishes exponentially in $b$.

FIG. 8. Relative error $\Delta^{(j)}$ of $j$ separation as a function of $b$ for several semiprimes $N$. A fit line, $\Delta = 2^{-2.5b - 1.5}$ (dashed line), is also shown. Compared with $k$ separation (see Fig. 7), the error decays with the same exponent; only the overall scale factor is different.
where we have used $\langle \cdots \rangle = \langle \{ \cdots \} \rangle = \langle \{ \cdots \} \rangle$ in cases
where the averages commute. We start by computing
\[
\langle \psi^2 \rangle_k = \pi^2 \sum_{m,m'=0}^{n-1} \sum_{\mu=0}^{m-m'} (\langle \psi_{m-\mu} \psi_{m'-\mu} \rangle + \langle \psi_{m'-\mu} \psi_{m-\mu} \rangle),
\]
where we have made use of the assumed independence of $s$
and $l$. Taking into account that the binary digits of $s$ and $l$
can only take the values 0 and 1, we obtain
\[
\langle \psi_{m-\mu} \psi_{m'-\mu} \rangle = \frac{1}{2} \delta_{m,0} + \frac{1}{2}(1 - \delta_{m,0})
\]
and a similar expression for $\langle \psi_{m'} \psi_{m} \rangle$. Because of (88),
the evaluation of the quadruple sum, (87), is lengthy but can
be performed analytically. The result is
\[
\langle \psi^2 \rangle_k = \frac{\pi^2}{144} 2^{-2b} \left[ 9x^2 + 21x - 10 + 9(2 + x) 2^{-s} + 2^{-2s} \right],
\]
where $x = n - b - 2$. (90)

Next, we evaluate $\langle \psi^2 \rangle_k$. With (88) and following the same
procedures that lead to (89), we obtain
\[
\langle \psi^2 \rangle_k = \frac{\pi^2}{96} 2^{-2b} \left[ 6x^2 + 6x - 4 + 6(1 + x) 2^{-s} + 2^{-2s} \right],
\]
where $x$ is defined in Eq. (90). We define
\[
\delta^2 = \langle \psi^2 \rangle_k - \langle \psi^2 \rangle_k^2,
\]
which, on the basis of the results (89) and (91), is explicitly
given by
\[
\delta^2 = \frac{\pi^2}{288} 2^{-2b} (24x - 8 + 18 \times 2^{-s} - 2^{-2s}).
\]

With (90) and up to second order in the moment expansion
(86), the performance measure is now given by
\[
P(n,b) \approx 1 - \delta^2.
\]
Comparing (94) with the fit function (66) and using (90), we see that (94),
to leading order in $n$, is the first-order expansion of
\[
P^{(n)}(n,b) \sim 2^{-2b} \xi_b^{(a)},
\]
where
\[
\xi_b^{(a)} = \left[ \frac{\pi^2}{12 \ln(2)} \right] 2^{-2b} \approx 1.19 \times 2^{-2b}.
\]

This analytical result recovers the $2^{-2b}$ scaling of the fit line
(66) and is within 10% of the exponential prefactor in Eq. (66).

The analytical evaluation of the fourth-order terms in
Eq. (86) is technically straightforward, but tedious, and not
essential at this point. Our numerical calculations show that
the fourth-order terms are approximately given by $(\delta^2)^2/2$
and are, therefore, very small. This has two consequences: it
shows (i) that up to fourth order in $\psi$ the probability measure
$P(n,b)$ for fixed $b$ is consistent with exponential decay in $n$
and (ii) that, because of their smallness, it is currently not necessary
to evaluate the fourth-order terms analytically.

To conclude this section, we compute
\[
\langle \psi \rangle_k = \frac{\pi}{4} \sum_{n=0}^{n-1} \sum_{\mu=0}^{m-m'} \frac{1}{2^{m-m'}}
\]
which is needed in the following section. Using the summation
formula for the evaluation of geometric sums, we obtain
\[
\langle \psi \rangle_k = \frac{\pi}{4} \left( 2^{-b}(n-b-2) + 2^{1-n} \right) = \frac{1}{4} \psi_{\text{max}},
\]
where we have related $\langle \psi \rangle_k$ to $\psi_{\text{max}}$ via (54).

C. Small-$n$, nonexponential regime

Our starting point is again Eq. (79), but in this section we focus
on the small-$n$ regime, i.e., $n < n_{\text{cut}}(b)$ [see (75)].
We first derive some useful relations that can then be used to
evaluate (79) approximately in this regime. We start by inspecting $\psi(n,b,s,l)$ in Eq. (37). We note that
\[
\psi(n,b,s,l) = \pi \sum_{i=0}^{n-b-2} \left[ (2^s l) \mod 2^{n-b-1} \right].
\]

Since the modulus of the product of two numbers is smaller
than or equal to the product of the moduli of the two numbers, we obtain
\[
\psi(n,b,s,l) \leq \pi \sum_{i=0}^{n-b-2} \left[ (2^s l) \mod 2^{n-b-1} \right]
\]
\[
= \frac{\pi}{2^{n-b-1}} \left[ s \mod 2^{n-b-1} \right] \mod 2^{n-b-1},
\]
where the equality is obtained by using
\[
\left( \sum_{i=0}^{n-b-2} 2^s l \right) \mod 2^{n-b-1} = (s \mod 2^{n-b-1}) \mod 2^{n-b-1} = s \mod 2^{n-b-1}.
\]

In order to compensate for the difference between (99) and
(100), we introduce an effective parameter $l$ in Eq. (100) such that
\[
\psi = \frac{\pi}{2^{n-b-1}} (s \mod 2^{n-b-1}) \leq \psi_{\text{max}}.
\]
where the inequality is obtained from the definition of $\psi_{\text{max}}$
in Eq. (52). Since this inequality must hold for any $s$, inequality
(102) implies
\[
2^{-2b} l \leq \psi_{\text{max}}.
\]
where we have used $\max(s \mod 2^{n-b-1}) \approx 2^{n-b-1}$. Assuming
the random model used in Sec. VI B, in particular, its assumption
of statistical independence of $s$ and $l$, we compute the average
of (102). With (98) we obtain
\[
\langle \psi \rangle_k = \frac{\psi_{\text{max}}}{4} = \frac{\pi}{2^{n-b-1}} (s \mod 2^{n-b-1}) l = \frac{\pi}{2} 2^{-b} (l)\).
\]

032333-11
Appendix A. List of Publications

Hence, solving for $\langle l \rangle_j$, and dropping the small term $2^{-n}$ in Eq. (54), we expect
\begin{equation}
\langle l \rangle_j \approx \frac{n - b - 2}{2}.
\end{equation}
We note that $\langle l \rangle_j$ in Eq. (105) fulfills (103). Next, by writing the order of a seed as $\omega = 2^r$ [see Eq. (62)], and by using the form of an element $s_k$ of an equivalence class $[s_0]$ defined in Eq. (8), we obtain
\begin{equation}
s_k \text{ mod } 2^{n-b-1} = kr \text{ mod } 2^{n-b-1} = (kr \text{ mod } 2^{n-a-b-1})2^a,
\end{equation}
where we have assumed $s_0 = 0$ for analytical simplicity. We note that $(kr \text{ mod } 2^{n-a-b-1})$ is a random integer variable in $k$ for $k$ an integer, which spans the entire integer space $0 \leq k \leq 2^{n-a-b-1} - 1$. Now, we compute $\frac{\langle l \rangle_j}{\langle s \rangle_j}$, using (54), (102), and (106):
\begin{equation}
\frac{\langle l \rangle_j}{\langle s \rangle_j} \approx \frac{\pi^2}{2^{n-1} 2\pi [2^{n-b-1}(n-b) - 2b] + 2^n} \approx \frac{\pi}{n - b - 2} \frac{\langle l \rangle_j}{\langle s \rangle_j},
\end{equation}
where we have again dropped the small $2^{-n}$ term. Thus, we write
\begin{equation}
\langle l \rangle_j \approx \frac{n - b - 2}{\langle s \rangle_j} \langle l \rangle_j,
\end{equation}
where we have used
\begin{equation}
\langle s \rangle_j = |\frac{\eta}{\langle l \rangle_j} R_k|,
\end{equation}
which is a random variable in $k$ whose range is [0, 1]. We are now ready to evaluate (79). Inserting (108) in Eq. (79), we obtain
\begin{equation}
P(n,b) = \left| \left( \int \frac{\eta}{\langle l \rangle_j} R_k \right) \right|^2.
\end{equation}
Assuming that $R_k$ is uniformly distributed in [0, 1], we turn the $k$ average into an integral and obtain
\begin{equation}
P(n,b) \approx \left( \int_0^{\eta} e^{-\frac{1}{\eta} \frac{\eta}{\langle l \rangle_j} R_k} \right),
\end{equation}
where we have defined
\begin{equation}
\eta = \frac{\langle l \rangle_j}{n - b - 2}.
\end{equation}
Evaluation of (111) yields
\begin{equation}
P(n,b) \approx \left( \frac{1}{\eta} \right)^{1 - \cos(\eta)}.
\end{equation}
Since $\eta$ defined in Eq. (112) is small for $n < n_1$, we Taylor-expand (113), which results in
\begin{equation}
P(n,b) \approx \left( \frac{2}{\eta} \right) \left( 1 - \left( 1 - \frac{\eta^2}{2} \right) \frac{\eta^2}{24} \right) = 1 - \left( \frac{\eta^2}{12} \right).
\end{equation}
Inserting $\eta$ defined in Eq. (112) into (114), we obtain
\begin{equation}
P(n,b) \approx 1 - \frac{\langle l \rangle_j}{\langle s \rangle_j}.
\end{equation}
We compute $\langle l \rangle_j$ in the following way. Computing the average of the square of (102), we obtain
\begin{equation}
\langle l \rangle_j \approx \frac{\pi^2}{2^{n-1}} (s \text{ mod } 2^{n-b-1})^2 \langle l \rangle_j,
\end{equation}
where we have used the assumed independence of $x$ and $y$ of the random model. According to (89), and to leading order in $x$ [defined in Eq. (90)], we have
\begin{equation}
\langle l \rangle_j \approx \left( \frac{\pi^2}{16} \right) (2^{b-2}(n - b - 2))^2.
\end{equation}
Equating (116) and (117), we obtain
\begin{equation}
\langle l \rangle_j = \frac{1}{\pi} (n - b - 2)^2.
\end{equation}
Inserting (118) into (115), we obtain
\begin{equation}
P(n,b) \approx 1 - \frac{\eta_{\text{max}}}{64} \approx \exp \left[ - \frac{\eta_{\text{max}}}{64} n(b) / 64 \right].
\end{equation}
Compared with the numerical fit line, (67) [in particular, Eq. (69)], this analytical result predicts the functional form of the $b$ scaling exactly and the overall scaling factor within a factor of 2.

VII. COMPARISON WITH THE WORK OF Fowler and Hollenberg

Our work is closely related to the work of FH [15]. The purpose of this section is to discuss similarities and differences between the two approaches. The notation in Ref. [15] differs from ours. In order to avoid confusion, we translate the notation in Ref. [15] into our notation. As argued in Ref. [15] and here, because of the sensitivity of quantum gates to noise and decoherence, it is important to reduce the number of gates and gate operations as much as possible. This provides the motivation for studying the performance of Shor’s algorithm as a function of bandwidth $b$ of the QFT, since a small $b$ results in substantial savings in gates to be implemented and gate operations to be executed. Both works conclude that for large $n$ the period-finding part of Shor’s algorithm scales exponentially in $n$, $P(n,b) \sim 2^{-b \omega}$, where $\omega = \gamma 2^{-2b}$ and $\gamma$ is a constant. FH quote $\gamma = 2$; we find $\gamma = 1$. 1. Thus, while the research goals are the same, and the central results are similar, there are substantial differences in how the research programs are executed, and there are new findings in our work. Among the new findings is the existence of a nonexponential regime for small $n$ (see Sec. V), analytical results for the nonexponential and exponential regimes (see Sec. VI), and the existence of a provable bound for the maximal possible period $\omega$ of a given semiprime $N$ (see Appendix B).

The main difference between [15] and our work concerns the choice of $\omega$ in the simulations. While in our work we simulate the period-finding part of Shor’s algorithm for actual semiprimes $N$ and actual, associated $\omega$ values, FH use an effective $\omega = 2 + N/2$. Thus, our calculations are more realistic than those reported in Ref. [15] and check and complement the calculations in Ref. [15] under more realistic
Appendix A. List of Publications

SCALING LAWS FOR SHOR’S ALGORITHM WITH A...

PHYSICAL REVIEW A 87, 032333 (2013)

FIG. 9. Average ω as a function of N. (a) Scatterplot of ⟨ω⟩ defined according to (120); (b) double-averaged, binned ⟨⟨ω⟩⟩ defined according to (121).

conditions. Our first comment in this connection concerns the choice of FH’s effective ω value. It was chosen as a good representative of ω values in Fig. 5 of Ref. [15]. However, the ω values in that figure extend up to ω = N, which is more than 2 times larger than the maximal possible ω, which is smaller than N/2 (see Appendix B for the proof). Therefore, rather than being located in the middle of Fig. 5 in Ref. [15], FH’s effective ω actually lies beyond the allowed range of ω. However, this is not expected to make any difference in the conclusions in Ref. [15], since, as shown in Fig. 5 in Ref. [15], according to the simulations reported in Ref. [15], P(n,b) exhibits flat plateaus in ω.

In this connection it may be interesting to present more information on the distribution of allowed ω values. In Fig. 9(a) we show the properly averaged ω values,

\[ ⟨ω⟩ = \frac{1}{\psi(N)} \sum_{j=1}^{a(N)} v(ω_j) ω_j, \]  

(120)

defined as

\[ ⟨⟨ω⟩⟩ = \frac{1}{χ(N^{(i)+250}) - χ(N^{(i)-250})} \sum_{i=1}^{N^{(i)+250}} (ω_i), \]  

(121)

\[ N^{(i)} = 500 \left( i - \frac{1}{2} \right), \quad i = 1, \ldots, 20, \]

where χ(N) is the semiprime counting function and (ωi) is the average ω [see Eq. (120)] associated with the ith semiprime. Figure 9(b) shows that the twice-averaged ⟨⟨ω⟩⟩ are linear in N with

\[ ⟨⟨ω⟩⟩ \approx N/5. \]  

(122)

Therefore, according to Fig. 9(b), a representative ω value for a given N is an allowed ω value in the vicinity of N/5.

In contrast to our choice of a single l state representing a Fourier peak, FH choose two l states to represent a Fourier peak, one to the left and one to the right of the position of the peak’s maximum. This choice is more symmetrical than ours, but because of the uniform response of all states under a Fourier peak (see Fig. 2 and the discussion in Sec. IV), one representative is sufficient.

FH quote γFH = 2 as a safe estimate, which is about a factor of 2 larger than our, more optimistic, γ = 1.1. On the basis of the data in Fig. 6 of Ref. [15] we computed the actual γFH corresponding to the six panels in FH’s Fig. 6 and obtained γFH = 0.5 (b = 0), 1.85 (b = 1), 1.83 (b = 2), 1.79 (b = 3), 1.78 (b = 4), 1.77 (b = 5), 1.73 (b = 6), and 1.57 (b = 7). Discarding the γFH value for b = 0 (it is not generic, since it involves only H and M gates and no rotation gate) and the γFH values for b = 6 and b = 7 (given the numerical range of the data, the exponential regime displayed in Fig. 6 of Ref. [15] is very short, resulting in uncertainty in the decay constant of an exponential fit), the γFH values are well characterized by γFH ≈ 1.8, slightly more optimistic than the quoted γFH = 2. What is interesting to us is that γFH = 1.8 is already closer to our value of γ = 1.1.

Finally, what difference does it make for the performance of a quantum computer if γ = 2 or γ = 1.1? The answer depends on the performance level of the quantum computer. Since a factor 2 difference in γ is the difference between the performance and the square of the performance, a factor of 2 difference in γ has basically no effect if the quantum computer operates with close to 100% performance but has a large effect if the quantum computer operates, e.g., on the 10% level.

Because of the critical need for quantum error correction and fault-tolerant operation [28], FH also present an error-tolerant, approximate construction of rotation gates, consisting of more fundamental elementary gates. In fact, each single-qubit rotation gate, as written in the quantum algorithm, may result in thousands of gates when decomposed. Unlike FH, we do not discuss the actual realization of gates, since, in this paper, we focus on the algorithmic aspects of Shor’s algorithm, in particular, on the scaling of the performance with n and b. In any case, as shown by FH, the actual experimental realization of fault-tolerant gates may require large numbers of additional, ancillary gates and qubits, motivating and emphasizing the
critical need to reduce required quantum resources as much as possible by optimizing the quantum algorithms.

Given that error correction and fault-tolerant operation may introduce many additional auxiliary gates and qubits, what happens to our scaling laws in this case? Since our scaling laws depend on two parameters, \( b \) and \( n \), the answer has two parts. (i) Error correction will not affect the \( b \) scaling, since the possibility of reducing the full QFT to a narrow-band QFT with bandwidth \( b \) is an intrinsic property of the mathematical structure of the Fourier transform itself that has nothing to do with quantum error correction. In fact, under noisy conditions, it may not even be a good idea to increase the bandwidth of the QFT, because the algorithmic gain of the transform gained might be more than offset by the errors introduced by the additional gates that are now exposed to noise and decoherence. (ii) It is clear that each computational qubit in Shor’s algorithm has to be protected with quantum circuits that consist of additional qubits. However, since the scaling laws derived in this paper refer to the number \( n \) of computational qubits, our scaling laws remain unchanged.

Summarizing the discussion in this section, we see our work as complementary to the pioneering work of FH, adding new insights and confirming the major conclusions of FH, using an algorithm with \( 2000 \) qubits, our scaling laws remain unchanged. However, since the scaling laws derived in this paper refer to the number \( n \) of computational qubits, our scaling laws remain unchanged.

VIII. DISCUSSION

An absolute limit of classical computing is reached when the physical requirements exceed the resources of the universe. According to this definition we can safely say that a classical computer, no matter its precise architecture, using the best currently available factoring algorithms, will never be able to factor a semiprime with 5000 decimal digits or more. We see this in the following way. The best currently known algorithm for factoring large, “hard” semiprimes (more than \( \sim 130 \) decimal digits; no small factors) is the general number field sieve (GNFS) [1]. It was recently used by Kleinjung et al. [8] to factor the RSA challenge number RSA-768 (232 decimal digits). This factorization took the equivalent of 2000 years on a 2.2-GHz Opteron workstation [8]. The performance of the GNFS scales approximately as [1]

\[
P(N) \sim \exp[1.9\ln(N)^{1/3}\ln(\ln(N))^{2/3}],
\]

(123)

where \( N \) is the semiprime to be factored. If we take the Kleinjung et al. factorization as the current, best benchmark and estimate an Opteron processor to consist of roughly \( 10^{35} \) particles, then we can factor a 232-decimal-digit semiprime with \( 2000 \times 12 \times 10^{35} \approx 2 \times 10^{39} \) particles in the time span of a month. According to (123), then, in order to factor a 5000-decimal-digit number in the span of a month we need

\[
2 \times 10^{29} \times P(10^{5000})/P(10^{39}) \approx 10^{89}
\]

(124)

particles. This exceeds the number of particles in the universe (\( \approx 10^{80} \)) by several orders of magnitude. Clearly, the factorization of a 5000-decimal-digit semiprime is physically impossible to perform within a reasonable time (\( \sim 1 \) month) on a classical computer. Even if we allow substantial progress in computer development, for instance, replacing the current

MOSFET transistors [29] used in computer chips with single-electron transistors [30] and increasing the clock speed of a processor from 2.2 GHz to the optical regime of \( \sim 10^{15} \) Hz, we gain only insignificantly. Therefore, in the absence of a breakthrough in the design of classical factoring algorithms, if we want to make any progress in factoring large numbers, we need a different computing paradigm. This is provided by switching from classical computing to quantum computing, i.e., running Shor’s algorithm on a quantum computer. Instead of scaling (sub)exponentially, according to (123), Shor’s algorithm scales

\[
\sim O((\ln N)^2(\ln \ln N)/(\ln \ln \ln N))
\]

(11)

and thus provides an exponential speedup that allows us, in principle, to tackle semiprimes vastly in excess of \( N = 10^{5000} \). Obviously, for the practical implementation of powerful quantum computers, any optimization of quantum algorithms is welcome. Addressing this point, our paper shows that replacing the full QFT in Shor’s algorithm with a narrow-band version incurs only a negligible performance penalty. We also show how the performance of such a streamlined version of Shor’s algorithm scales with the number of qubits \( n \).

In order to objectively characterize the performance of a quantum computer with \( n \) qubits, equipped with a banded QFT of bandwidth \( b \), we define the performance measure \( P(n,b,\omega) \) in Sec. IV [see Eq. (22)]. This measure was carefully chosen to accurately reflect the performance of the quantum computer in terms of the probability of a successful factorization, yet not excessively expensive to compute numerically and, most importantly, a convenient starting point for analytical computations. As shown in Secs. V and VI, our performance measure fulfills both goals. Although any given peak in the QFT contains several \( l \) states with significant overlap with the Fourier peak, and useful for factorization in classical postprocessing [10,18], our performance measure defined in Eq. (22) is based only on a single \( l \) state, i.e., the state \( |j_1\rangle \) closest to the central maximum of the Fourier peak number \( j \) [see Eq. (20)]. This, no doubt, is convenient for analytical calculations, as successfully demonstrated in Sec. VI, and for the following reason it is also justified. Numerically investigating the response of the Fourier peaks to a reduction in the bandwidth \( b \), we found that the width of the Fourier peaks stays the same (about one state), while the height of the Fourier peaks is reduced. Thus, all \( l \) states under a Fourier peak respond in unison to a change in \( b \) (see Fig. 2), and since the width of the Fourier peaks stays the same, the number of significant states in a peak is conserved too. This means that a single state under the peak, for instance, the state with maximal overlap, accurately represents the response of any other state under the peak, in particular, the states useful for factorization. Thus, summarizing our choice of performance measure, we may say that, of course, choosing all those states under a Fourier peak that are useful for factorization would be best. However, this is computationally prohibitively expensive and not useful for analytical calculations. A proxy is necessary. Because of the uniform response of all states in a Fourier peak, this proxy is provided, e.g., by the state closest to the central peak, \( |j_1\rangle \), and leads directly to our performance measure \( P(n,b) \) defined in Eq. (22).

The exponential fit function in Eq. (66) is shifted by 8 units in \( n \). A possible explanation is the following. \( n = 8 \) corresponds to \( N = 15 \), the smallest odd semiprime. However,
for $N = 15$ all possible orders $\omega$ are powers of 2. Therefore, according to the discussion in Sec. IV, Shor’s algorithm performs perfectly in this case for all $b$. This means that $P(n = 8, b, \omega) = 1$ for all $b$, which is true independently of $b$ only if $\xi_b$ is multiplied with $n - 8$ in the exponent of (66).

The largest RSA challenge number [31] is RSA-2048. It has 2048 binary digits, which corresponds to 617 decimal digits. Factoring this number on a quantum computer requires a minimum of 4096 qubits. Since no numerical simulation data are available in this very-large-$n$ regime, we have to rely on our results, (66) and (67), to estimate the performance of the quantum computer. Which of the two formulas to use depends on which regime, exponential or nonexponential, we are in. For $b = 8$, and according to (75), the transition point $n_t$ for $b = 8$ occurs at $n_t = 20$. Therefore, since $n \gg n_t$ in this case, we are sure that we are not in the nonexponential regime. However, how certain can we be that the exponential law (66) is valid all the way up to $n = 4096$, when we checked it numerically only up to $n \approx 30$ (see Sec. V)?

We answer this question in the following way. The moment expansion (86) is certainly valid out to $n$ values for which our low-order Taylor expansion of $\exp(-i\xi)$ is valid, i.e., for $\xi < 1$. Since $\xi < \xi_{\text{max}}$, the safest estimate for the validity of (66) is $n \lesssim 2^{b+1}/(2\pi)$, which is obtained from (54) for $n \gg b$. For $b = 8$ this implies $n < 81$. This is already deeply in the $n$ regime where current numerical simulations cannot follow. However, we can do better than that. The moment expansion, (86), together with our numerical observation that the fourth-order terms are given by $(\delta^2)^2/2$, shows that the relevant expansion parameter of (86) is not $\xi$ but $\delta^2$, which is much smaller than $\xi_{\text{max}}$. Therefore, we can safely assume exponential decay out to $n$ values for which $\delta^2 < 1$. According to (93), then, this yields the estimate $n < 12 \times 2^{20}/\pi^2$, which amounts to $n < 79,682$ for $b = 8$, much larger than the $n = 4096$ required for the factorization of RSA-2048. We conclude that, for $b = 8$, we may safely use the exponential law, (66), to estimate the performance of the quantum computer. Therefore, using $n = 4096$ and $b = 8$ in Eq. (66), we obtain $P(n, b) = 0.954$; i.e., a quantum computer with a bandwidth of only $b = 8$ can factor the RSA challenge number RSA-2048 with a performance of better than 95%. If we increase $b = 8$ by only 1 unit, to $b = 9$, the performance increases to 98.5%.

Concluding this section, we briefly discuss the paper by Barenco et al. [32], which also investigates the effect of the banded QFT on the performance of the period-finding part of Shor’s algorithm. In fact, their performance measure $Q$, based on the probability of obtaining an $|l\rangle$ state closest to $2^l/\omega$, is, up to normalization, identical to our performance measure. However, the main focus of [32] is the effect of decoherence on $Q$, and similarly to the work of FH [15], Barenco et al. do not use factoring of actual semiprimes $N$ in their numerical simulations. Finally, the analytical performance estimates in Ref. [32] require $b > \log_2(n) + 2$, which, for $b = 8$, implies $n < 64$. Therefore, for small $b \leq 8$, the analytical formulas of [32] are not applicable to the performance of a quantum computer in the technically and commercially interesting small-$b$, large-$n$ regime with $n \gtrsim 4000$.

**IX. SUMMARY AND CONCLUSIONS**

Given that quantum computers are difficult to build, any advance in the optimization of quantum algorithms is welcome. Accordingly, in this paper, we have investigated the performance of Shor’s algorithm equipped with a banded QFT. Our predictions are based on the following five substantial advances.

1. Properly $\omega$-averaged numerical simulations of factoring actual semiprimes $N$ for qubit numbers ranging from $n = 9$ to $n = 33$, yielding the numerical performance estimates (66) in the large-$n$ regime and (67) in the small-$n$ regime.

2. Analytical and numerical justification of the separation of the $k$ and $j$ sums in the definition of the performance measure as the foundation of analytical computations of the performance measure in the large-$n$ and small-$n$ regimes. It is shown that both separations are exponentially accurate, with exponential improvement of accuracy for increasing bandwidth $b$ of the QFT.

3. Analytical computation of the performance measure in the exponential, high-$n$ regime, which predicts the $2^{-2b}$ scaling exactly and the prefactor in $\xi_b$ within 10% of the numerical result, (66).

4. Analytical computation of the performance measure in the small-$n$ regime, which predicts the functional form of the performance measure accurately and provides a reasonable estimate of a single, overall scaling factor.

5. Analytical formula (75) for the crossover points $n_t$, which mark the transition from the nonexponential regime to the exponential regime of quantum computer performance. For a given bandwidth $b$ and number of qubits $n$, this allows a quick, accurate, and convenient decision of whether the resulting finite-bandwidth quantum computer is working in the exponential or nonexponential regime.

In addition, in Appendix A, we prove the existence and uniqueness of an order 2 seed for any semiprime $N$, which, in Appendix B, is used to prove that the maximal possible order $\omega$ of a seed is less than $N/2$ (see Figs. 9 and 10). The maximally allowed $\omega$ is smaller than the effective, representative $\omega$ chosen in Ref. [15]. However, due to the insensitivity of the results in Ref. [15] with respect to the chosen $\omega$ (see Fig. 5 of Ref. [15]),

![FIG. 10. Maximal possible orders $\omega$ (maximum order) computed and displayed for each $N$ in the complete list of semiprimes in the interval $0 < N < 10^3$. Apparently, the maximal possible order never exceeds $N/2$, a fact proved in the text.](image-url)
Appendix A. List of Publications

Y. S. Nam and R. Blümel

PHYSICAL REVIEW A 87, 032333 (2013)

This fact is not expected to change the results predicted in Ref. [15]. Finally, we investigate the statistical properties of an inverse factor of \( \omega \) in Appendix C.

In our opinion, and based on the numerical and analytical results presented in this paper, we conclude that the period-finding part of Shor's algorithm equipped with a banded QFT of bandwidth \( b \) is now essentially understood. However, period finding is not the most demanding part of Shor's algorithm to implement. This distinction is reserved for the \( f \)-mapping part of Shor's algorithm (the modular exponentiation part), which feeds register II with \( f(x) \) values (see Sec. II) and, compared with the period-finding part of Shor's algorithm, requires vastly more quantum resources to implement [25,33–35]. Therefore, attention now has to be directed toward optimizing the \( f \)-mapping part of Shor's algorithm.

APPENDIX A: EXISTENCE AND UNIQUENESS OF AN ELEMENT OF ORDER 2

In support of the result that the probability of encountering a seed with a small order is small, we provide here a proof that there is one and only one seed \( x \) of order 2 for any semiprime \( N = pq \), where \( p \neq q \) primes larger than 2. A seed is any positive integer, larger than 1, that is relatively prime to \( N \). Let us collect all possible seeds \( s_j, j = 1, \ldots, L − 1 \), including the unit 1, into a set \( G_N = \{1, x_1, x_2, \ldots, x_{L−1}\} \). This way, \( G_N \) forms a multiplicative group modulo \( N \) containing \( L \) elements.

The computation of \( L \) is straightforward. There are at most \( N − 1 \) numbers that are relatively prime to \( N = pq \), (By definition, the unit element 1 is relatively prime to \( N = pq \), but \( N \) is not.) However, \( p − 1 \) of these numbers contain a factor \( q \) and \( q − 1 \) of these numbers contain a factor \( p \), and these numbers are all different. Therefore, there are \( L = (N − 1) − (p − 1) − (q − 1) = N − p − q + 1 \) group elements. Since \( N, p, q \) are odd, \( L \) is even. At this point we cite a well-known theorem of elementary algebra that states that each group with an even number of elements has at least one element that is different from the unit element and is of order 2 [27]. Applied to our group \( G_N \) this means that there exists at least one seed \( x \neq 1 \) with \( x^2 \equiv 1 \) modulo \( N \), i.e., a seed of order \( 2 \).

At this point it is important to observe that if there is a seed \( x \) with \( x^2 \mod N = 1 \), then there is also a seed \( z \equiv N − x \mod N \) which is also of order 2, since \( z \mod N = (N^2 − 2Nx + x^2) \mod N = x^2 \mod N = 1 \). Therefore, without restriction of generality, we restrict ourselves to the range of seeds smaller than \( N/2 \) and prove that there is only one \( x < N/2 \) with \( x^2 \mod N = 1 \), where \( N = pq \).

We already proved that there is at least one \( x \) with

\[
\begin{align*}
x^2 \mod N &= 1, \quad (A1)
\end{align*}
\]

Without restriction of generality, we can choose this \( x \) to be smaller than \( N/2 \), since, if it is larger than \( N/2 \), its mirror will be smaller than \( N/2 \). Assume that there exists another seed of order 2, \( y < N/2 \), with \( y > x \) (no restriction of generality) and

\[
\begin{align*}
y^2 \mod N &= 1, \quad (A2)
\end{align*}
\]

Since \( x^2 \mod N = 1 \) and \( y^2 \mod N = 1 \), we have

\[
\begin{align*}
(y^2 − x^2) \mod N &= (y − x)(y + x) \mod N = 0, \quad (A3)
\end{align*}
\]

This equation holds if either \( y \) at least one of the factors is divisible by \( N \) or \( y + x \) contains \( q \), or vice versa. However, case i is impossible: Since both \( x \) and \( y \) are smaller than \( N/2 \), \( y < N \) is, therefore, never divisible by \( N \). For the same reason \( y − x \) is divisible by \( N \) only if \( y − x = 0 \), which is excluded, since, according to assumption, \( y \neq x \). This leaves case ii.

Since \( x^2 \mod N = 1 \), we have \((x − 1)(x + 1) \mod N = 0 \). Since \((x − 1) < N \) and \((x + 1) < N \), for any \( N > 2 \), neither factor is divisible by \( N \) and the product is divisible by \( N \) only if \((x − 1) \) is a multiple of \( p \) and \((x + 1) \) is a multiple of \( q \).

There is no restriction of generality here, since which factor of the product is divisible by which factor of \( N \) is merely a matter of properly labeling the factors of \( N \). So, let us write

\[
\begin{align*}
x − 1 &= λp, \quad (A4)
x + 1 &= μq, \quad (A5)
\end{align*}
\]

where \( λ \) and \( μ \) are positive integers. We observe immediately that \( λ \) cannot contain a factor \( q \), since otherwise \((x − 1) \) would be divisible by \( N \). In the same way we reason that \( μ \) cannot contain a factor \( p \). We record this observation as

\[
\begin{align*}
λ \mod q &= 0, \quad (A6)
μ \mod p &= 0. \quad (A7)
\end{align*}
\]

We also have \( y^2 \mod N = 1 \), i.e., \((y − 1)(y + 1) \mod N = 0 \), which now implies two possibilities, since in Eqs. (A4) and (A5) we already chose the naming convention for the two factors, \( p \) and \( q \), of \( N \). The two cases are

\[
\begin{align*}
(A) \quad & (y − 1) \text{ is a multiple of } p, \quad (y + 1) \text{ is a multiple of } q; \quad (A8)
(B) \quad & (y − 1) \text{ is a multiple of } q, \quad (y + 1) \text{ is a multiple of } p. \quad (A9)
\end{align*}
\]

Let us look at case A first. Let us write

\[
\begin{align*}
(y − 1) &= ap, \quad (A10)
(y + 1) &= bq. \quad (A11)
\end{align*}
\]

In analogy with the reasoning that led us to (A6) and (A7) we have

\[
\begin{align*}
α \mod q &= 0, \quad (A12)
β \mod p &= 0. \quad (A13)
\end{align*}
\]

Then, because of \( x, y < N/2 \), (A3), and the discussion following (A3), we need to prove that either \((y − x) \) contains a factor \( p \) and \((y + x) \) a factor \( q \) or vice versa. We write

\[
\begin{align*}
y + x &= (y − 1) + (x + 1) = αp + μq. \quad (A14)
\end{align*}
\]

But since \( α \) is not divisible by \( q \) [see Eq. (A12)] and \( μ \) is not divisible by \( p \) [see Eq. (A7)], \((y + x) \) is divisible neither by \( p \) nor by \( q \). Therefore, case A leads to a contradiction, which implies that, according to case A, a second order 2 seed \( y \neq x \) does not exist.

Let us now look at case B. Let us write

\[
\begin{align*}
(y − 1) &= yq, \quad (A15)
(y + 1) &= qp. \quad (A16)
\end{align*}
\]

032333-16
Appendix A. List of Publications

where, again, in analogy with the reasoning that led us to (A6) and (A7), we have

\[ y \mod p \neq 0, \quad (A17) \]
\[ \nu \mod q \neq 0. \quad (A18) \]

Then

\[ y - x = (y - 1) - (x - 1) = \gamma q - \lambda p. \quad (A19) \]

which, because of (A17) and (A18), is divisible neither by \( p \) nor by \( q \). Therefore, case B, too, leads to a contradiction.

As a result, we obtain that the existence of an additional order 2 seed \( y \neq x, y < N/2 \) is impossible. Therefore, \( x \) is a unique order 2 seed with \( x < N/2 \). This means that for any given semiprime \( N = pq \), there are exactly two order 2 seeds, \( x < N/2 \) and its mirror \( N - x > N/2 \).

**Appendix B: Maximal Order**

In connection with Shor’s algorithm, for a given semiprime \( N \), we consider seeds \( x \) with an even order \( \omega = 2\Omega \), where \( \Omega \geq 1 \) is a positive integer. The purpose of this section is to show that the largest possible even \( \omega \) is smaller than \( N/2 \).

A seed \( x, 1 \leq x < N \) is a positive integer, relatively prime to \( N = pq \), where \( p \neq q \) are prime numbers larger than 2. As discussed in Appendix A, the set of seeds \( x \) forms a group \( G_N \) with

\[ |G_N| = N - p - q - 1 = (p - 1)(q - 1) \quad (B1) \]

elements. We note that, according to (B1), \( |G_N| \) is divisible by 4, a fact which becomes relevant below. If \( x \) is relatively prime to \( N \), so is \( N - x \). Therefore, if \( x \) is a seed, so is \( N - x \), which implies (i) a symmetry of seeds with respect to \( N/2 \) and (ii) that there is an even number of seeds. We use implication (i) to define a set \( \hat{G}_N \), consisting of elements \( \hat{x} = (x, N - x) \), where \( x \) and \( N - x \) are identified. The set \( \hat{G}_N \) forms a group.

This is so since \( \hat{G}_N \) contains the unit element \( 1 = (1, N - 1) \), the product \( \hat{x} \hat{y} \) of two elements of \( \hat{G}_N \) is again in \( \hat{G}_N \), and with each \( \hat{x} \), we also find its inverse \( (\hat{x})^{-1} \) in \( \hat{G}_N \). Because of implication (i) the group \( \hat{G}_N \) has

\[ |\hat{G}_N| = |G_N|/2 \quad (B2) \]

elements.

Let us form the set \( G_N^* \), which contains the squares of \( x \) modulo \( N \). Since \( G_N^* \) contains the unit element \( 1 \), and since with each \( x^2 \) and \( y^2 \) in \( G_N^* \), the product

\[ (x^2)(y^2) \mod N = (xy)^2 \mod N \quad (B3) \]

is also in \( G_N^* \), and since with each \( x^2 \) we also find its inverse

\[ (x^2)^{-1} \mod N = (x^{-1})^2 \mod N \quad (B4) \]

in \( G_N^* \), the set \( G_N^* \) is a group. In the same way we form the set \( \hat{G}_N^* \) from the squares of \( \hat{x} \) in \( \hat{G}_N \). Because of the definition of \( \hat{G}_N \), identifying \( x \) and \( N - x \), and because of

\[ (N - x)^2 \mod N = x^2 \mod N, \quad (B5) \]

which shows that the squares of \( x \) and \( N - x \) are identical, the groups \( G_N^* \) and \( \hat{G}_N^* \) have the same number of elements. In addition, as is easily verified, groups \( G_N^* \) and \( \hat{G}_N^* \) are isomorphic, which implies that the order of an element in \( \hat{G}_N^* \) is the same as the order of an element in \( G_N^* \). Let us denote the number of elements in these two groups

\[ |G_N^*| = |\hat{G}_N^*| = M. \quad (B6) \]

Then, because of (B2), and because \( \hat{G}_N^* \) is a subgroup of \( G_N^* \), we have that

\[ M = |\hat{G}_N^*| \text{ divides } |G_N^*| = |G_N|/2. \quad (B7) \]

One possibility is \( M = |G_N^*|/2 \). However, since the group \( G_N^* \) of squares is a subgroup of \( G_N^* \), \( M = |G_N^*|/2 \) is possible only if there are as many squares \( \hat{x}^2 \) in \( G_N^* \) as there are elements \( \hat{x} \) in \( G_N \). However, because of the existence of a nontrivial order 2 element \( \hat{a} \) (see Appendix A), this is impossible, since both \( \hat{a}^2 = 1 \) and \( \hat{a}^2 = 1 \), which immediately implies \( M < |G_N^*|/2 \). Therefore, the largest possible \( M \) that divides \( |G_N^*|/2 \) (an even number) is \( |G_N^*|/4 \), which implies

\[ M \leq |G_N^*|/4. \quad (B8) \]

According to Euler’s totient theorem [27], we have, for any \( \hat{x}^2 \) in \( \hat{G}_N^* \),

\[ (\hat{x}^2)^M = 1, \quad (B9) \]

which implies that the order of any element \( \hat{x}^2 \) in \( \hat{G}_N^* \) is at most \( M = |G_N^*|/4 \). Because of the isomorphism between \( G_N^* \) and \( \hat{G}_N^* \), this implies that the order of any \( \hat{x}^2 \) in \( \hat{G}_N^* \) is at most \( |G_N^*|/4 \). This, finally, implies that the order of any element \( x \) in \( G_N^* \) is at most \( |G_N^*|/2 \), i.e.,

\[ \omega \leq |G_N^*|/2 < N/2. \quad (B10) \]

We note that since an essential element of the proof is to consider the group of squares of \( x \), the proof indeed applies only to even \( \omega \). An illustration of (B10) is provided in Fig. 10, which shows the maximum even orders of all semiprimes \( N \) ranging up to \( N = 100,000 \). The figure illustrates (i) that the maximal order is indeed smaller than \( N/2 \) and (ii) that the maximal order of a given semiprime \( N \) is not always close to \( N/2 \) but still has to divide the group order. Therefore, in addition to the line \( N/2 \), we also see the lines corresponding to \( N/4, N/6, \) etc.

![FIG. 11. The fraction \( (\hat{x}/n) \) as a function of \( n \) for several semiprimes. The fit line (solid line) is the function \( (\hat{x}/n) = 2^{-\omega(n)^{1/2}} \).](032333-17)

032333-17
APPENDIX C: 1/r AVERAGE

For analytical formula (69), we need the average \( \frac{1}{r} \) of \( 1/r \) as a function of \( r \), where \( r \) is defined in Eq. (62). We computed it in the following way. First, we computed all possible orders, \( \alpha_j \), of a given semiprime \( N \) with their associated multiplicities, \( \nu(\alpha_j) \). Then we extracted the odd part of the obtained orders, \( r \), as defined in Eq. (62). Denoting the odd part of a specific order \( \alpha_j \) by \( r_j \), in analogy with (65) and (120), we obtain

\[
\left\langle \frac{1}{r} \right\rangle = \frac{1}{\psi(N)} \sum_{j=1}^{\nu(\alpha_j)} \frac{1}{r_j}, \quad (C1)
\]

where the symbols in Eq. (C1) share the same definition as shown in Eqs. (65) and (120), i.e., \( \psi(N) \) is Euler’s totient function and \( \nu(\alpha_j) \) is the number of orders for given \( N \). Figure 11 shows the computed \( \left\langle \frac{1}{r} \right\rangle \) according to (C1) as a function of \( n \), the number of qubits needed for a reliable determination of the order as described in connection with (64). By graphically extracting the \( n \) dependence of \( \left\langle \frac{1}{r} \right\rangle \) using the fit line in Fig. 11, we find

\[
\left\langle \frac{1}{r} \right\rangle = 2^{-(n-8)/2.6}, \quad (C2)
\]

---

[27] N. Jacobson, Basic Algebra I (Dover, Mineola, NY, 2009).
Streamlining Shor’s algorithm for potential hardware savings

Y. S. Nam and R. Blümel
Department of Physics, Wesleyan University, Middletown, Connecticut 06459-0155, USA
(Received 14 May 2013; published 26 June 2013)

We constructed a virtual quantum computer by running a complete, scaling, quantum-gate–by-quantum-gate implementation of Shor’s algorithm on a 128-core classical cluster computer. In mode A [quantum period finding (PF) only, supplied with classical results for the modular exponentiation (ME) part of Shor’s algorithm], factoring semiprimes up to \( N = 557 \cdot 993 \) with up to \( n = 39 \) qubits, we confirm earlier, smaller-\( n \) results concerning the performance scaling of Shor’s algorithm equipped with a truncated (banded) quantum Fourier transform. Running our virtual quantum computer in mode B (full quantum implementation of ME and PF), we find that a large number of gates may be discarded in a scalable way in both the ME and PF parts of Shor’s algorithm in exchange for only a small reduction in performance. We explicitly state the associated scaling laws. Imposing significant savings in quantum gates, we suggest that these results are of importance for future experimental and technical large-\( n \) implementations of quantum computers.

Most computations of practical interest cannot be performed on classical, digital computers because they exceed the capabilities of even the largest presently existing supercomputers. A well-known example of importance in cryptanalysis is the factorization of large semiprimes \( N = pq \), where \( p \) and \( q \) are prime numbers of about equal size [1]. Solution of the factorization problem would immediately break many popular encryption schemes, such as the RSA (Rivest, Shamir, and Adleman) encryption scheme [2], and would immediately reveal untold scores of government, military, and bank secrets. However, even if we build a classical supercomputer combining the resources of the entire known universe, we would still not be able to factor a relatively modest-sized semiprime with 5000 decimal digits [3]. Therefore, encryption codes that rely on the difficulty of integer factorization are considered secure—for now.

Classical digital computing, however, is not the only form of information processing. Since the early 1980s, we have known that a quantum computer [4–6], a qualitatively new form of information processor, is capable of solving problems that are strictly beyond the powers of any conceivable classical computer. In the world of integer factoring this is impressively demonstrated by Shor’s algorithm [7], which is exponentially more powerful than any currently known classical factoring algorithm. In particular, at least in principle, a quantum computer running Shor’s algorithm is powerful enough to break currently employed RSA-based encryption codes [8–10].

The quantum core of Shor’s algorithm may be broken down into two parts: (1) modular exponentiation (ME) and (2) period finding (PF). Given an integer \( x \), relatively prime to \( N \), the ME part of Shor’s algorithm determines the values \( f(r) = x^r \mod N \) for integer exponents \( r \). This is followed by the PF part of Shor’s algorithm, which, supplemented with an efficient classical algorithm (classical postprocessing [8–10]), performs a quantum Fourier transform (QFT) [8–10] to determine the period \( \omega \) of \( f \), i.e., \( f(r + \omega) = f(r) \). Given the period \( \omega \) and a few additional conditions that are straightforwardly accommodated in practice [8–10], the factors of \( N \) are then determined according to \( p = \gcd(x^{\omega/2} - 1, N) \) and \( q = \gcd(x^{\omega/2} + 1, N) \), where gcd is the greatest common divisor, efficiently computed via Euclid’s algorithm [1].

Because of its importance, several experimental groups have implemented demonstration models of quantum computers that are capable of factoring small semiprimes [11–15]. Although these experiments employ quantum circuits that implement both parts of Shor’s algorithm, i.e., ME and PF, the quantum circuits are tailor-made and optimized for a single semiprime \( N \). Thus, these quantum circuits do not scale; i.e., they are not capable of factoring any other \( N \) than the one they are designed for. The high degree of specialization in the experimental implementations of ME and PF is necessary since even with today’s standards of exquisite quantum control, it is still a daunting task to coherently control more than a handful of qubits. Therefore, experimental implementations of quantum computers are currently limited to \( N \leq 21 \) [11–15].

In order to overcome the current experimental limitations on \( N \) and to be able to study, theoretically, the performance of Shor’s algorithm under various conditions, we implemented a complete quantum-gate–by-quantum-gate simulation of a scaling, virtual quantum computer on a 128-core classical cluster computer. We designed our virtual quantum computer to run in two modes: (A) PF only, supplied with ME performed classically, and (B) both ME and PF executed quantum mechanically. With our currently available classical computing resources, running our virtual quantum computer in mode A, we are able to factor all semiprimes up to and including \( N = 557 \cdot 993 \). Running the quantum computer in mode B, we are able to factor all semiprimes up to and including \( N = 557 \cdot 993 \). We view our virtual quantum computer as a convenient virtual quantum laboratory that lets us investigate the effects of various (scaling) optimizations. One of these optimizations is the use of a banded QFT and its influence on the performance of Shor’s algorithm [3,16,17]. Running our virtual quantum computer in mode A, we report results that test our performance scaling laws [3,17] in the region of up to 39 qubits. Running our quantum computer in mode B, we report results on the effects of a scaling optimization of the adder and ME-QFT components [18] of ME.
Given the experimental challenges in achieving coherent quantum control of many qubits simultaneously, experimental implementations of Shor’s algorithm are facilitated if the algorithm itself can be simplified. We distinguish two types of simplifications: performance conserving and performance changing. One such simplification, a performance-conserving optimization, is the substitution of the fully coherent QFT [8–10] in Shor’s algorithm by a semiclassical version due to Griffiths and Niu [19]. A five-qubit circuit of the Griffiths-Niu QFT is shown in Fig. 1(a). Although the Griffiths-Niu version of the QFT replaces all two-qubit gates in the fully coherent QFT by (controlled) single-qubit gates and destroys phases as a result of measurement (see $M$ gates in Fig. 1), it is exact when used in conjunction with the PF part of Shor’s algorithm. Our virtual quantum computer is equipped with a banded version [3,16,17,20] of the Griffiths-Niu QFT [see Fig. 1(b)]. This means that in addition to using only single-qubit gates, as shown in Fig. 1(a), we also retain only coupling to $b$ nearest-neighbor qubits, which results in a banded structure of the quantum circuit [see Fig. 1(b)]. Of course, denoting by $n$ the number of qubits of our virtual quantum computer, the exact case is included for the choice $b = n - 1$. While the case $b = n - 1$ is performance conserving, $b < n - 1$ is not but leads to substantial savings in quantum gates. Therefore, for given $n$, our goal is to determine the optimal choice of $b$ that corresponds to maximal savings in gates for still acceptable quantum computer performance.

Quantifying our performance measure, we note that the probability of finding our quantum computer in state $|l\rangle$, where $l$ is in the vicinity of $\tilde{l}_j$, i.e., states useful for factoring [8–10], respond in unison to the reduction of $b$ [3]. Therefore, defining $\tilde{l}_j$ as the closest integer to $\tilde{l}_j$, we find it useful and convenient to measure the performance of the banded Shor algorithm using the normalized performance measure [3]

$$P_b(n) = \frac{\sum_{l=0}^{n-1} \tilde{P}_{b}(\tilde{l}_j)}{\sum_{l=0}^{n-1} \tilde{P}_{b=0}(\tilde{l}_j)},$$

(2)

where $\tilde{P}_{b}(\tilde{l}_j)$ is the probability of collapse into the state $|\tilde{l}_j\rangle$ if the full QFT is replaced by its banded version of bandwidth $b$ [see Fig. 1(b)]. Previously, we were able to compute $P_b(n)$ for quantum computers with up to 33 qubits [3] and found the scaling law

$$P_b(n) = \exp[-1.1 \times 2^{-2b}(n - 8)]$$

(3)

(solid, straight lines in Fig. 2). Testing our earlier results, we report here calculations of $P_b(n)$ that extend the range of qubits to $n = 39$. The plot symbols in Fig. 2 include our data for $P_b(n)$ in the range from $n = 34$ to 39. These data were obtained by running our virtual $n$-qubit quantum computer for various $N$, ranging from $N = 116\,939$ to $N = 557\,993$. These computations are extensive, so that in the range from $n = 34$ to 39 we can only afford to choose a single sample $N$ for each $n$. We chose $N = 116\,939 = 337 \times 347$ for $n = 34$, $N = 171\,371 = 409 \times 419$ for $n = 35$, $N = 239\,117 = 487 \times 491$ for $n = 36$, $N = 265\,189 = 509 \times 521$ for $n = 37$, $N = 378\,221 = 613 \times 617$ for $n = 38$, and $N = 557\,993 = 743 \times 751$ for $n = 39$. Our chosen $N$ values are products of consecutive primes. This is obviously not useful for cryptological applications but emulates the case $p \approx q$, known to be the most difficult case to factor [1]. For each chosen $N$, we determine all of its orders $\omega$ (each of these $N$ has up to 72 different orders, which all require quantum processing) and then compute the $\omega$-averaged $P_b$ [3], which then appears as a plot symbol in Fig. 2. These results confirm the scaling law (3), thus confirming the conclusion in [3] that a substantial number of quantum gates can be saved by pruning
the QFT down to bandwidths around \( b = 8 \) (although based on a slightly different scaling law, the same conclusion was reached by the authors of [16]). This is seen clearly in Fig. 2, which shows that for \( b = 8 \) the performance of the quantum computer is very close to 1 for all \( n \) ranging up to \( n = 39 \).

We now turn to our mode-B calculations. Supplementing the QFT with quantum circuitry as described in [18], we obtain a complete quantum-gate-by-quantum-gate implementation of a virtual quantum computer that currently runs on a 128-core classical cluster computer. Our gate-by-gate implementation gives us access to each individual quantum gate and allows us to investigate the effects of gate pruning on the performance of the quantum computer. Another advantage of our implementation is that it allows us to experiment with the factoring of actual semiprimes \( N \). We report here results for \( N = 21 \), although, given our classical hardware resources, \( N = 33, 35, 39, 51, 55, \) and 57 are within our reach [21]. Running test cases for \( N = 15 \) and \( N = 21 \) and comparing the computational results to the theoretically expected result (1), we verified that our virtual quantum computer is implemented correctly.

Relating to our experiments with a reduced bandwidth \( b \) in the PF part of Shor’s algorithm and making use of our access to each individual quantum gate of our virtual quantum computer, we introduced the bandwidth \( b_{\text{ME}} \) in the adder and ME-QFT parts [18] of Shor’s algorithm by removing all gates causing single-qubit phase shifts of less than \( \exp(i\pi/2b_{\text{ME}}) \).

For fixed \( b_{\text{ME}} \) we compute \( P_{b}(b_{\text{ME}}) \) as in (2) and define \( \Gamma_{b}(b_{\text{ME}}) = 1 - P_{b}(b_{\text{ME}}) \). We chose \( N = 21 \) with \( n = 10 \) to investigate the effects of this pruning operation. Figure 3 shows \( \Gamma_{b} \approx 1 - P_{b} \) for our test case \( N = 21 \) with \( b \) ranging from 1 to 7. We find that \( \Gamma_{b} \) depends only weakly on \( b_{\text{ME}} \) and decays exponentially for increasing \( b \). This implies that satisfactory performance of Shor’s algorithm can be achieved with relatively small \( b (b_{\text{ME}}) \), resulting in tremendous savings in quantum gates. Quantitatively, we find that

\[
\Gamma_{b} \approx 2^{-2b}, \quad (4)
\]

![FIG. 3. Complement \( \Gamma_{b}(b_{\text{ME}}) = 1 - P_{b}(b_{\text{ME}}) \) of quantum computer performance as a function of \( b \) for five different values of \( b_{\text{ME}} \). Triangles: \( b_{\text{ME}} = 1 \); asterisks: \( b_{\text{ME}} = 2 \); diamonds: \( b_{\text{ME}} = 3 \); squares: \( b_{\text{ME}} = 4 \); circles: \( b_{\text{ME}} = 5 \). The solid line is the scaling function (4).]

which is reminiscent of the \( b \) scaling in mode A [see (3)]. Because exponentially many quantum operations need to be simulated, our quantum computer currently runs at an accuracy of \( \approx 10^{-5} \). The point corresponding to \( b = 8 \) in Fig. 3 is not shown because it is at the limit of our accuracy and therefore unreliable.

Multiprocessor simulations of Shor’s algorithm on classical hardware are not new (see, e.g., [22–25]), and applications range from proofs of principle of the suitability of the multiprocessor architecture [22,23] and the creation of convenient parallel-computing environments [25] to massively parallel implementations on state-of-the-art supercomputer facilities [24]. While we cannot compete with supercomputer implementations of Shor’s algorithm as far as raw computing power is concerned, the results reported in this paper push the envelope in different ways. Our mode-A calculations allow us to confirm the scaling behavior of Shor’s algorithm equipped with a banded QFT for up to \( n = 39 \) qubits, which is substantially larger (the execution time essentially doubles with each unit increase in \( n \)) than the number of qubits used in earlier investigations of this type [3,16,17]. The results of our calculations confirm our analytical model of performance scaling [3,17], which predicts that the scaling (3) persists for quantum computers with several thousand qubits, relevant for factoring semiprimes of practical interest. However, our main result is the realization that the ME part of Shor’s algorithm may be banded in the same way as the PF part, resulting in the scaling law (4). This proves that the adder and ME-QFT components of ME may be considerably streamlined, resulting in substantial savings in quantum gates in exchange for only a negligible reduction in performance. Detailed circuit diagrams illustrating the ME pruning operation defined above will be published elsewhere [21].

We also mention the investigations by Garcia-Mata et al. [26,27]. These investigations are related to our mode-A calculations since in [26,27] the ME part of Shor’s algorithm is represented by the product of unitary matrices computed classically. However, the focus in [26,27] is not on the effects of bandedness but on the influence of noise on the performance of Shor’s algorithm. This motivates the question of whether in the presence of noise and decoherence a larger bandwidth \( b (b_{\text{ME}}) \) may be required than predicted by our noise-free model, possibly erasing the benefits that a small \( b (b_{\text{ME}}) \) entails. For the following simple reason this is highly unlikely. The gates pruning now are (classically controlled) single-qubit rotation gates with exponentially small rotation angles. Because the rotation angles are so small, these gates are easily drowned out by noise, and instead of performing their function, they would merely act as “antennas” to pick up noise and channel it into the quantum circuit. Therefore, in the presence of noise, it may actually be beneficial to prune even more gates, i.e., to work with an even smaller bandwidth than indicated by the noise-free model in order to avoid this “antenna effect.” Our preliminary calculations confirm these conclusions and will be reported elsewhere [21].

The computations reported in this paper are expensive. They took three months to execute on a 128-core cluster-computer and are thus at the limit of computer power that even a university computing center can provide for a single research group. Therefore, we need streamlined versions of Shor’s
algorithm not only for efficient practical implementations of Shor’s algorithm but also for quantum simulations performed on classical computers in order to be able to explore the high-$n$ regions of practical importance for meaningful quantum computations.

In summary, we presented some recent results on extending our mode-A calculations to 39 qubits, thereby testing and confirming our scaling laws for finite-bandwidth quantum computer performance [3, 17]. These calculations involved quantum factorization of actual semiprimes up to and including $N = 557,993$. Running our quantum computer in mode B, we showed that quantum adders and ME-QFTs may be banded without significant loss in factoring performance. We are sure that this will be of considerable interest for technological implementations of Shor’s algorithm.

The authors are grateful for a generous allotment of computer resources by the Wesleyan Scientific Computing Center. R.B. acknowledges financial support by Grant No. 216687 of the Research Council of Norway.

Appendix A. List of Publications

Universal heating curve of damped Coulomb plasmas in a Paul trap

J. D. Tarnas, Y. S. Nam, and R. Blümel
Department of Physics, Wesleyan University, Middletown, Connecticut 06459-0155, USA
(Received 18 August 2013; published 4 October 2013)

A charged-particle cloud in a Paul trap is a nonlinear system that exhibits deterministic heating, i.e., conversion of energy provided by the radio-frequency (rf) drive of the trap into the disordered, gaslike motions of the trapped particles. In the presence of weak damping clouds reach an equilibrium state in which heating and cooling balance. For large damping, a cloud may collapse into a crystal. While the rf heating power of a given cloud depends sensitively on its particle number, its equilibrium size, the damping, and the control parameters of the trap, we find that scaling the heating power of the cloud with respect to its associated Coulomb-decoupled, non-interacting-gas state, and its equilibrium size with respect to its crystal size, results in a single, universal heating curve, independent of particle number and trap control parameters.

DOI: 10.1103/PhysRevA.88.041401

Invented in the 1950s by Paul (Nobel Prize 1989) and collaborators [1], the Paul trap consists of two end-cap electrodes (hyperboloid of two sheets) and a ring electrode (hyperboloid of a single sheet). An x-z cross section of the trap is shown in Fig. 1. As one of the most versatile devices in atomic and molecular physics, the Paul trap is capable of storing just about any charged particle species ranging from charged leptons [2] to charged grains of dust [3]. Both the classical and quantum dynamics of a single particle in an ideal Paul trap are known analytically [1,4] and may be expressed exactly in closed form with the help of Mathieu functions [5]. However, already the dynamics of two simultaneously stored particles is nonintegrable and chaotic in general [6]. In this case we observe the phenomenon of radio-frequency (rf) heating [7]; i.e., simultaneously stored charged particles gain energy on average. While the single-particle dynamics in the Paul trap is understood completely, little is known about chaotic heating of charged-particle clouds in a Paul trap. As a first step toward a theory of deterministic rf heating in a Paul trap, we present here some recent results on the existence of a universal heating curve that describes rf heating in a Paul trap, we find that scaling the heating power of the cloud with respect to its associated Coulomb-decoupled, non-interacting-gas state, and its equilibrium size with respect to its crystal size, results in a single, universal heating curve, independent of particle number and trap control parameters.

where

\[ q = \frac{4QV_0}{m\Omega^2\Omega_0^2 + 2\zeta^2}, \quad a = \left(\frac{2U_0}{V_0}\right) q. \]  (2)

are the two control parameters of the Paul trap [1,6,8], \( y \) is the damping constant (generated, e.g., by laser cooling [6]), \( \gamma \) is measured in units of \( 2\Omega \), and distances are measured in units of \( (Q^2/\pi \epsilon_0 m \Omega^2)^{1/2} \), where \( Q \) is the charge and \( m \) is the mass of each of the trapped particles, and \( \epsilon_0 \) is the permittivity of the vacuum. Defining

\[ s_i^2 = \sum_{w=1}^{N} w_i^2, \quad w = x, y, z, \quad x^2 = \sum_{w=1}^{N} x_w^2, \]  (3)

the total instantaneous energy of an \( N \)-particle cloud is

\[ E(t) = E_{\text{kin}}(t) + E_{\text{trap}}(t) + E_{\text{Coul}}(t), \]  (4)

where

\[ E_{\text{kin}}(t) = \frac{1}{2} \sum_{i=1}^{N} \dot{s}_i^2, \]  (5)

\[ E_{\text{trap}}(t) = \frac{1}{2} \left[ a - 2q \sin(2\gamma) \right] \left( s_i^2 + x_i^2 - 2x_i^2 \right), \]  (6)

and

\[ E_{\text{Coul}}(t) = \frac{1}{2} \sum_{i,j=1}^{N} \frac{1}{|r_i - r_j|}. \]  (7)

With Eq. (1), the time rate of change of Eq. (4) is

\[ \frac{dE(t)}{dt} = G(t) + S(t), \]  (8)

where

\[ G(t) = -\gamma \sum_{i=1}^{N} \dot{s}_i^2 = -2\gamma E_{\text{kin}}(t), \]  (9)

and

\[ S(t) = -2\gamma \cos(2\gamma) \left( s_i^2 + x_i^2 - 2x_i^2 \right). \]  (10)

Since \( E_{\text{kin}}(t) > 0 \) for all \( t \), \( G(t) \) is the sink of energy and \( S(t) \) is the source of energy. Since \( G(t) \) and \( S(t) \) are energy rates of

1050-3947/2013/88(4)/041401(4) 041401-1 ©2013 American Physical Society
change, $G(t)$ is the cooling power and $S(t)$ is the heating power. In order to be able to define an equilibrium state, we introduce the time average over a cycle of the applied trap field, which yields cycle-averaged quantities. The cycle-averaged energy rate of change is

$$\frac{dE(t)}{dt} = (G(t)) + (S(t)).$$

In equilibrium we have $(dE(t)/dt) = 0$, which entails

$$H = (S(t)) = - (G(t)) = 2\gamma \bar{E}_{kin},$$

where we defined $\bar{E}_{kin} = (E_{kin}(t))$.

By solving Eq. (1) numerically with a standard fourth-order Runge-Kutta integrator [9], Eq. (12) allows us to compute $H$ for any given $N, a, q, \gamma$. In order to obtain statistically reliable results for $\bar{E}_{kin}$, we break the data-taking process into two steps: (i) Equilibration: We start with random initial conditions for positions and velocities of the $N$ particles and integrate Eq. (1) forward in time for $n_t$ trap cycles, where $n_t \gg 1/\gamma$. This ensures that the cloud has settled down into its dynamical equilibrium state. (ii) Data taking: Following step (i), we compute $n_s$ samples of $E_{kin}$ by averaging $E_{kin}(t)$ over $n_d$ cycles in $n_t$ consecutive time intervals. For each of these $n_s$ time intervals we also compute the average cloud size $\bar{s}$, defined as the mean of $n_d$ cloud sizes $s$ [see Eq. (3)], evaluated at the end of each of these $n_d$ trap cycles. Breaking the data-taking cycles into $n_t$ different sets gives us an idea of the statistical spread of $H$ for given $N, a, q,$ and $\gamma$. Figure 2 shows heating rates $H$ versus cloud sizes $\bar{s}$ calculated according to this procedure for $q = 0.2, a = q^2/2$ (approximately spherical clouds), for four different particle numbers ($N = 50, 100, 200, 500$), with $\gamma$ values ranging from $\gamma = 10^{-5}$ to $\gamma = 10^{-2}, n_t = 3,$ and $n_d$ chosen large enough to ensure a small statistical error of $\bar{s}$ and $H$. (The choice of $n_d$ is not critical since its only function is to determine the size of the statistical fluctuations of the data points. For the data displayed in Fig. 2, we chose $n_d$ ranging from $n_d = 1000$ for small clouds to $n_d = 10,000$ for large clouds.) Figure 2 illustrates several key features of the data: (a) The heating rates $H$ vary over several orders of magnitude. (b) Large clouds heat less; small clouds heat more. (c) For large enough $\gamma$, clouds collapse into crystals (plot symbols on the left of their respective heating curves in Fig. 2). (d) The statistical spread of the data is small.

Given the large variation of the heating rates with $N$ and $\gamma$ we look for a scaling transformation that collapses the data onto one single heating curve. To this end, we evaluate $E_{kin}$ in the pseudopotential model [1] of the Paul trap. This results in

$$\bar{E}_{kin} = \frac{1}{2} \sum_{i=1}^{N} \left[ \left( 1 + \frac{q^2}{8} \right) (\dot{X}_i^2) + \left( 1 + \frac{q^2}{2} \right) (\dot{Y}_i^2) \right] + \frac{q^2}{2} (\dot{X}_i^2 + \dot{Y}_i^2) + 2q^2 (\dot{Z}_i^2),$$

where $X, Y, Z$ are the components of the macromotion [1] and the $\dot{q}^2$ terms originate from the micromotion [1]. Since charged-particle clouds in a Paul trap are fully chaotic, we may safely replace time averages with ensemble averages. For small $\gamma$ the trapped clouds are large [see observation (b) above]. Therefore, by neglecting the Coulomb interaction, we may evaluate the ensemble averages approximately, using the statistical model of a noninteracting gas [10] confined in the pseudo-oscillator potential [1] of the trap. We obtain

$$\bar{E}_{kin} = \frac{1}{2} \left[ \left( 1 + \frac{q^2}{8} \right) \omega_x^2 + \frac{q^2}{2} \right] (\dot{x}_i^2) + \left[ \left( 1 + \frac{q^2}{8} \right) \omega_y^2 + \frac{q^2}{2} \right] (\dot{y}_i^2)$$

$$+ \left[ \left( 1 + \frac{q^2}{2} \right) \omega_z^2 + 2q^2 \right] (\dot{z}_i^2),$$

where $\omega_x, \omega_y,$ and $\omega_z$ are the pseudo-oscillator frequencies in $x, y,$ and $z$ directions, respectively. We now define the scaled heating rate according to

$$r = \frac{H}{2\gamma \bar{E}_{kin}}.$$
where $s_r$ is the size of the crystal evaluated according to Eq. (3) at the end of any rf cycle in the crystal phase. No averaging is necessary for the computation of $s_r$, since the constituent particles of the crystal occupy geometrically ordered positions that are exactly periodic with the frequency of the rf drive [6,8,11,12].

Figure 3 shows the result of plotting the data of Fig. 2 in the form of scaled heating rates $h$ versus scaled cloud sizes $\sigma$. The data points all collapse onto a single, universal curve.

Since the only length scale in the system is the size of the crystal, we also define the scaled cloud size

$$\sigma = \frac{s}{s_c}$$

(16)

where $s_c$ is the size of the crystal evaluated according to Eq. (3) at the end of any rf cycle in the crystal phase. No averaging is necessary for the computation of $s_c$, since the constituent particles of the crystal occupy geometrically ordered positions that are exactly periodic with the frequency of the rf drive [6,8,11,12].

Figure 3 shows the result of plotting the data of Fig. 2 in the form of scaled heating rates (15) versus scaled cloud sizes (16). The scaled data all collapse onto one universal curve within the size of the plot symbols. Given the wide range of the data in Fig. 2, this result is surprising. Analyzing the shape of the universal curve we understand and observe (see Fig. 3) that because of its definition (15) the universal heating curve is approximately 1 for large $\sigma$. Ignoring the discrete charge distribution in the crystal phase, and instead assuming a homogeneous charge distribution (an excellent assumption on average for a continuous charge distribution in a three-dimensional harmonic oscillator potential), we compute an estimate for $H$ in the crystal phase. The result is

$$H_c = \gamma E_{kin}$$

(17)

This explains $h \approx 1/2$ in the crystal phase (see data close to $\sigma = 1$ in Fig. 3).

Is $h$ universal for all spherical clouds? To answer this question, we repeated the calculations of Fig. 2 for $q = 0.3$, $a = q^2/2$, scaled them according to Eqs. (15) and (16), and displayed them together with the Fig. 3 data in Fig. 4. Not only do all the $q = 0.3$, $a = q^2/2$ data collapse onto one curve, so do the two curves for $q = 0.2$, $a = q^2/2$ and $q = 0.3$, $a = q^2/2$, approximately, within the width of a few plot symbols. Therefore, on the basis of these two sets of Paul-trap control parameters, the scaled heating curve is universal.

The universal heating curve has three regimes: (I) Coulomb decoupled (noninteracting gas, $\sigma \gtrsim 3$), (II) Coulomb coupled (interacting gas, $1 < \sigma \lesssim 3$), and (III) crystal ($\sigma = 1$). In the Coulomb-decoupled regime (I), as shown by the data in Figs. 2 and 3, a charged-particle cloud in a Paul trap is well described by the model of a noninteracting gas in the trap’s pseudo-oscillator potential. Since $q$ is small, one might be tempted to use the lowest-order approximation $a_0 = a_1 = a_2 = q$ for the pseudo-oscillator frequencies in the case $a = q^2/2$. However, we found that the universal heating curve reacts very sensitively to the pseudo-oscillator frequencies, and using this lowest-order approximation will not collapse the data onto one universal curve. Therefore, we used more accurate values for the pseudo-oscillator frequencies based on the expansion 20.3.18 in Ref. [5].

While the scaling transformation is constructed in such a way that the universal curve is “hooked up” at both ends ($h \to 1$ for $\sigma \gtrsim 3$ and $h = 1/2$ for $\sigma = 1$), there is no reason why the data should collapse in the intermediate regime (II) of strong Coulomb coupling. In the absence of a microscopic theory of heating in the strong coupling region this result is surprising and awaits an explanation. Replacing the Coulomb interaction in Eq. (1) with a harmonic two-body force $\beta(r - \bar{r})$, $\beta > 0$ constant, results in a set of equations that are completely integrable (even in the presence of the time-dependent drive) and contain no chaos [13]. We found that in this case clouds do not heat; they collapse into crystals for any $\gamma$. This shows that the chaos produced by the nonlinear Coulomb interaction in (1) is essential for explaining region (II).

While in this paper we focused on the case $a = q^2/2$ that results in clouds that are very close to spherical, we also computed some exploratory results for near-spherical ($a = 0.35q^2$) and nonspherical ($a = 0$) clouds. We find that the data collapse in close vicinity to the universal curve of Figs. 3 and 4. Therefore, the scaled heating curve $h$ may be universal for a wide range of $a$ and $q$ values.

The sensitivity of the collapse with respect to the precision in the pseudo-oscillator frequencies may explain (a) why the data in Figs. 3 and 4 do not approach 1 from below and (b) why there is a difference between the $q = 0.2$ and the $q = 0.3$ data in Fig. 4. The reason for both observations may be found in our neglecting the Coulomb space-charge effect present even for large clouds. The space charge, if included, will result in a small modification of the pseudo-oscillator frequencies.
that may explain these two discrepancies. The deviation from the expected asymptotic value \( h = 1 \) is largest for the \( q = 0.3 \) data, which correspond to smaller clouds, which, in turn, correspond to larger Coulomb forces. So, this appears to go in the right direction. In any case, we are currently working on including space-charge effects to obtain Coulomb-corrected pseudo-oscillator frequencies that may result in an even better data collapse.

We also noticed a phenomenon that is not directly connected to the existence of the universal heating curve, but worth mentioning. It is known [6] that, at least for small \( N \), a region of cloud sizes exists that corresponds to unstable clouds that either collapse into crystals or expand to larger clouds for any choice of damping constant \( \gamma \). This gap is clearly apparent in the data of Fig. 2. As shown in Fig. 2, the relative gap size (the ratio of the gap with respect to its corresponding crystal) seems to decrease with increasing \( N \), and appears to be absent for \( N = 500 \). This phenomenon is currently unexplained.

Exploring the consequences of adding noise to our system, we modeled the effect of stochastically emitted cooling photons on our calculations as described in Ref. [6]. While we definitely see an effect (as we have to, since the presence of chaos in the dynamics means exponential sensitivity to perturbations of the system), the resulting heating rates are within the statistical variations of Fig. 2 and again fall on the universal heating curves in Figs. 3 and 4.

Approximating the Coulomb interaction by a single-particle mean-field theory, we are able to explain the \( \sigma \) scaling of \( h \) in pseudopotential approximation. In this theory the thermodynamical quantities do not depend on the particle number \( N \) and the temperature \( T \) separately, but only on the ratio \( T/(N - 1)^{2/3} \). Combined with Eq. (13), this fact is sufficient to obtain the \( \sigma \) scaling (up to corrections of order \( 1/N \)) of \( h \), if we assume additionally that \( \sigma_c \sim N^{1/3} \). More details can be found in Ref. [14].

In summary, we showed that a universal heating curve describes scaled heating rates of charged particle clouds in a Paul trap for a wide range of particle numbers, trap control parameters, and damping constants. While a mean-field theory combined with the pseudopotential approximation is capable of explaining the observed \( \sigma \) scaling of the data, a completely satisfactory explanation of the observed phenomena reported in this paper can only be provided by a fully time-dependent, microscopic theory of rf heating that needs to be developed in future numerical and analytical work.

We thank Glenn Carlson, Bob Elsinger, and Scott Michael of the Wesleyan ITS computer workshop, who generously provided us with decommissioned PCs for building and expanding our research group’s Beowulf PC cluster on which the initial discovery of the universal heating curve was made. We also acknowledge a generous allotment of computer time by the Wesleyan Scientific Computing Center. R.B. acknowledges financial support by Grant No. 216687 of the Research Council of Norway.

Appendix A. List of Publications

Robustness and performance scaling of a quantum computer with respect to a class of static defects

Y. S. Nam and R. Blämel

Department of Physics, Wesleyan University, Middletown, Connecticut 06459-0155, USA

(Received 10 October 2013; published 10 December 2013)

Competing computationally with experimental groups for the construction of scaling quantum computers, we simulate a complete quantum-gate by quantum-gate implementation of Shor’s algorithm on a classical 128-core cluster computer. The resulting virtual quantum computer serves as a convenient quantum laboratory for the investigation of the effect of defects in the quantum circuitry. The class of defects studied here is the removal of all rotation gates with rotation angles \( \theta < \pi/2^b \). Factoring semiprimes \( N = 21, 33, 35, 39, 55, 57 \), we find that the quantum computer still operates with acceptable performance (success probability of factoring) down to \( b = 2 \). This is surprising since the deletion of rotation gates results in large errors in the arithmetic circuitry of the quantum computer. Extrapolating on the basis of these results we conclude that for quantum computers of practical interest more than 99% of rotation gates may be discarded with acceptable consequences in quantum computer performance. This result may be of interest to experimental physicists and quantum engineers currently embarked on designing efficient circuitry for scaling quantum computers.

DOI: 10.1103/PhysRevA.88.062310

PACS number(s): 03.67.Lx

I. INTRODUCTION

Although the power of modern supercomputers seems limitless, there are many unsolved problems of theoretical and practical interest that are squarely beyond the capabilities of any classical computer. One of these problems is the factorization of a large semiprime, where \( p \) and \( q \), the prime factors of \( N \), are about the same size. Several powerful methods have been developed, such as the quadratic number sieve [1] or the general number field sieve [2], to attack the factorization problem. However, even if we constructed a classical supercomputer the size of the universe, factoring a 5000 digit semiprime would still be impossible [3]. In fact, the security of many public-key cryptosystems [4], among them the Rivet-Shamir-Adleman (RSA) cryptosystem [5], depend precisely on this observation.

When it comes to quantum computing, however, the story is quite different. A quantum computer running Shor’s algorithm [6] is capable of factoring current RSA semiprimes in a reasonable amount of time and therefore poses a threat to RSA-encrypted documents. Quantum algorithms, such as Shor’s algorithm, make full use of quantum features, such as superposition and entanglement, that allow for types of information processing that are not available to classical computers.

The enormous potential of quantum computers notwithstanding, only a few “useful” quantum algorithms are known to date. One of them, and arguably the most important one, is Shor’s algorithm, which consequently has been under intense investigation both theoretically [3,7–23] and experimentally [24–28]. In 2001, e.g., Vandersypen et al. [24] successfully implemented Shor’s algorithm, factoring \( N = 15 \) on a liquid nuclear magnetic resonance (NMR) quantum computer. Subsequently, Lu et al. [25] and Lanyon et al. [26], again factoring \( N = 15 \), successfully demonstrated a quantum computer using a photonic system. This was followed by another successful demonstration by Politi et al. [27]. Recently, in 2012, Martín-López et al. [28] used a qubit recycling technique to factor \( N = 21 \), setting a new record for the largest semiprime factored on actual quantum computer hardware.

Despite the pioneering accomplishments of the authors of Refs. [24–28], all experiments to date use various compiled versions of Shor’s algorithm, i.e., tailor-made algorithms that take advantage of the preknowledge of the two prime factors of the semiprimes used in the experiments (\( N = 15 = 3 \times 5 \) and \( N = 21 = 3 \times 7 \)). These algorithms will not work for any other \( N \) than the one they are designed for, making the resulting quantum computers special purpose quantum computers. Defining a scaling quantum computer as one that accepts different values of \( N \), the current implementations of Shor’s algorithm are said to be nonscaling. However, considering that even for the small \( N \) currently used in the experiments (\( N = 15 \) and \( N = 21 \)), thousands of quantum-gate operations are needed to run a complete, scaling, experimental implementation of Shor’s algorithm, the use of compiled, highly optimized versions of Shor’s algorithm is currently unavoidable and complete, scaling experimental implementations of Shor’s algorithm remain elusive. Therefore, given the experimental situation, and for the time being, the behavior of the complete (scaling) version of Shor’s algorithm can only be studied via numerical simulations on classical computers [3,9–11,29–34].

The current experimental limitations provide the motivation for our numerical work. Running a complete implementation of Shor’s algorithm on a classical cluster computer, we report here the results on factoring semiprimes up to \( N = 57 \). In addition, with the help of a shortcut, i.e., executing the modular exponentiation part of Shor’s algorithm classically, we are able to factor semiprimes up to \( N = 1,034,273 \).

Being able to factor substantially larger \( N \) than are possible experimentally is not the only advantage of our numerical implementation. On a computer we have access to each individual quantum gate, which lets us enable or disable any individual quantum gate at will, something which is extremely difficult to accomplish experimentally. Making use of our free access to quantum gates, our main result is that an enormous number of quantum gates may be pruned from Shor’s algorithm without significantly compromising the performance of the resulting streamlined quantum computer.

We readily admit that our lead with respect to experiment will only be temporary. The (classical) computer resources
needed for our simulations grow exponentially in the number of qubits, which is unsustainable beyond even modest values of $N$. Therefore, sooner or later, the experiment will catch up to the simulations and then easily surpass them as far as $N$ is concerned. But for now, even if only temporarily, numerical simulation has the edge.

Our paper is organized in the following way. A detailed description of the gate-by-gate decomposition of Shor’s algorithm is presented in Sec. II. The banded Shor algorithm is presented in Sec. III. Our virtual quantum computer may be operated in two modes, A and B. In mode A, we perform the modular exponentiation part of Shor’s algorithm classically, which results in a significant speedup and memory savings that allow us to study factorization of semiprimes up to $N \sim 10^8$. In Sec. IV we present the theory and simulation results of our mode-A calculations. A new 40-qubit result that took about three months to compute is also presented. The theory and simulation results of mode B, a complete quantum-gate by quantum-gate implementation of Shor’s algorithm, is presented in Sec. V. Both our mode-A and mode-B calculations show that a substantial number of quantum gates may be saved in future experimental implementations of Shor’s algorithm following a pruning strategy, which we call banding (see Sec. III). In Sec. VI we discuss our results and in Sec. VII we summarize and conclude our paper.

II. SHOR’S ALGORITHM

Shor’s algorithm may be divided into two parts: (1) modular exponentiation (ME) and (2) period finding (PF). Given a semiprime $N = pq$ to be factored, the ME part of Shor’s algorithm, supplied with an integer seed $x$ between 1 and $N$ that is coprime to $N$, computes $x^r \mod N$ for an integer exponent $r$. Defining the mapping

$$f(r) = x^r \mod N,$$  (1)

the PF part of Shor’s algorithm, then, determines the period $\omega$ of $f$, i.e., the smallest integer $\omega > 0$ for which $f(\omega) = 1$, via a quantum Fourier transform (QFT). For a successful factoring, $\omega$ needs to meet the following two conditions: (i) $\omega$ needs to be even and (ii) $(x^{\omega/2} - 1) \mod N \neq 0$. If any one of these two conditions are not met, we try a different seed $x$. When both conditions are satisfied, the two factors $p$ and $q$ of $N$ are then obtained via

$$p = \gcd(x^{\omega/2} - 1, N), \quad q = \gcd(x^{\omega/2} + 1, N),$$  (2)

where $\gcd$ denotes the greatest common divisor.

To date, there have been multiple proposed methods of implementing Shor’s algorithm on a quantum computer; a list of several different architectures is available in Table IV of Ref. [35]. Notable ones include, but are not limited to, those proposed by Vedral et al. [12], Beckman et al. [13], Zalka et al. [14], Beauregard [15], Van Meter et al. [16,17], Takahashi et al. [18], and Kutin [19]. In this paper, from the numerous methods available, we focus on Beauregard’s representation of Shor’s algorithm, which is based on QFT operations. The reason behind this choice is due to the possibility of approximating part of the circuit using a particular method of circuit pruning (banding), which will be introduced in detail in Sec. III.

A. Period finding

The first step of the PF part of Shor’s algorithm is a QFT defined as

$$|s\rangle = U^{(\text{QFT})} |s\rangle = \frac{1}{\sqrt{2^n}} \sum_{l=0}^{2^n-1} e^{2\pi i s l / 2^n} |l\rangle,$$  (3)

where $n$ is the number of qubits, $|s\rangle$ and $|s\rangle$ indicate input and output states, respectively, and $|l\rangle$ are the basis states of the $2^n$-dimensional Hilbert space $\mathcal{H}^2$ spanned by the $n$ qubits. Since our quantum computer is based on qubits, it is natural to decompose $\mathcal{H}^2$ into the tensor product of $n$ two-dimensional Hilbert spaces according to

$$\mathcal{H}^2 = \mathcal{H}^2_{[0]} \otimes \mathcal{H}^2_{[1]} \otimes \mathcal{H}^2_{[2]},$$  (4)

where $\mathcal{H}^2_{[m]}$ denotes the $m$th Hilbert space. In this notation, for instance, with $t_{[m]}$ the $m$th binary digit of an integer $I$,

$$|l\rangle = |l_{(m-1)}\rangle |l_{(m-2)}\rangle \cdots |l_{(1)}\rangle |l_{(0)}\rangle |0\rangle,$$  (5)

This decomposition with its associated $\{\ldots\}$ notation has additional advantages since in our quantum circuits qubits and states do not always correspond. For example, the state $|0\rangle$ of the $j$th qubit may actually correspond to the $m$th Hilbert space $\mathcal{H}^2_{[m]}$, in which case we write $|a_{[m]}\rangle$. This notation is of particular convenience in connection with QFT circuits where the output has to be read in reverse order (see Ref. [36] and Fig. 1).

In the decomposed Hilbert space notation, with $|0\rangle_{[m]}$ and $|1\rangle_{[m]}$ as basis states of the $m$th Hilbert space, (3) may be written as

$$|s\rangle = \frac{1}{\sqrt{2^m}} \prod_{m=0}^{m-1} \sum_{j=0}^{2^m-1} e^{2\pi i s_j (2^m-1-j) / 2^m} |j\rangle_{[m-1]} |0\rangle_{[m]} |0\rangle_{[m-2]} |0\rangle_{[m-3]} \cdots |0\rangle_{[0]} |0\rangle,$$  (6)

where $s_j$ denotes the $j$th binary digit of $s$, and

$$s_{[m]} = s_{[m-1]} \cdots s_{[0]} = \sum_{j=0}^{m} s_j (2^{m-j} + 1).$$  (7)

Expanding the product in (6), we obtain explicitly [36]

$$|s\rangle = \frac{1}{\sqrt{2^m}} (|0\rangle_{[m]} + e^{2\pi i s_0 2^m} |1\rangle_{[m]} |0\rangle_{[m-1]} (|0\rangle_{[m-2]} + e^{2\pi i s_1 2^{m-1}} |1\rangle_{[m-2]}) \cdots (|0\rangle_{[0]} + e^{2\pi i s_{m-1} 2^0} |1\rangle_{[0]} |0\rangle_{[0]} |0\rangle_{[0]} ) |0\rangle_{[0]} |0\rangle_{[0]}$$  (8)

which demonstrates that the QFT may be realized with a series of Hadamard gates and phase rotation gates. A fully quantum mechanical realization of the QFT in (8) is shown in Fig. 1.
FIG. 2. Logic circuit of a five-qubit semiclassical QFT. The meaning of H and \( \hat{r} \) is the same as in Fig. 1. M denotes the measurement gate.

We emphasize that in the case of the PF part of Shor’s algorithm since the QFT is directly followed by measurements, we are allowed to interchange the orders of the controlled phase rotation gates with the measurements. This way, by replacing the coherently controlled two-qubit phase rotation gates in Fig. 1 with single-qubit phase rotation gates that are classically controlled by the results of measurements, we obtain the semiclassical QFT circuit shown in Fig. 2 [20]. We note that due to the presence of measurements, the semiclassical QFT cannot be used to construct the quantum ME, which, as shown in Sec. II.B, requires the coherent QFT.

B. Quantum modular exponentiation

In this section we show that ME may be broken down into modular multiplications (MM), which then may be expressed as a sequence of modular additions (MA). This shows that MA is the basic building block of ME. Then, we separate as a sequence of modular additions (MA). This shows that modular multiplications (MM), which then may be expressed as consecutive MMs according to

\[
\theta^N \equiv \left\{ \begin{array}{ll}
|b - a|, & \text{if } b \geq a, \\
2^{n' + 1} - (a - b), & \text{if } b < a,
\end{array} \right.
\]

which is equivalent to subtraction. Noticing that \((a + b) \mod N\) (MA of \(a\) and \(b\) with respect to \(N\)) is \((a + b - N)\) if \(a + b \geq N\) or \((a + b) \mod N\) for integers \(a, b < N\), adding \(a\) to \(b\) then subtracting \(N\) results in

\[
\theta^N \hat{u}_a \hat{u}_b = \begin{cases} \theta^N\hat{u}_a \hat{u}_b & \text{if } a + b \geq N, \\ 2^{n' + 1} - \left[N - (a + b)\right], & \text{if } a + b < N, \end{cases}
\]

which correctly yields case (i). Since \(a + b - N < 2^{n'}\) and \(2^{n' + 1} - N < 2^{n'}\), case (ii) may be captured correctly with the help of (a) an overflow and (b) an auxiliary (qu)bit in the following way. Defining \(\hat{e}(t); |c\rangle\) as a controlled-NOT operation, linear in its two arguments, according to

\[
\hat{e}(t); |c\rangle = |t\rangle |(t + 1) \mod 2\rangle, \quad \text{if } c = 1,
\]

for \(|t\rangle\) a target state and \(|c\rangle\) a control state, both of which may be \(|0\rangle\) or \(|1\rangle\), an initialized auxiliary state of \(|0\rangle\) as a target, controlled by an overflow state, differentiates the two different cases in (18), namely,

\[
\hat{e}(0); |\theta^N \hat{u}_a \hat{u}_b |\rangle = \begin{cases} |0\rangle, & \text{if } a + b \geq N, \\ |1\rangle, & \text{if } a + b < N, \end{cases}
\]

where \(|\theta^N \hat{u}_a \hat{u}_b |\rangle\) is the state of the \(n'\)th qubit, or the overflow state, of \(\theta^N \hat{u}_a \hat{u}_b |\rangle\). Since for case (ii) we would like \(a + b\) as our MA result that needs an addition of \(N\) to the current state in (18), whereas for case (i) we should not alter its current state, as we already have the correct MA output, we make use of a controlled addition defined as, for \(|c\rangle\) a binary state

\[
\hat{u}_a (b); |c\rangle = \begin{cases} |b\rangle, & \text{if } c = 0, \\ |a + b\rangle, & \text{if } c = 1, \end{cases}
\]

with the target state of (18) and the controlling state of (20) for the controlled addition of \(N\) to obtain

\[
\hat{u}_N (\theta^N \hat{u}_a \hat{u}_b |\rangle; \hat{e}(0); |\theta^N \hat{u}_a \hat{u}_b |\rangle) = \begin{cases} |a + b - N\rangle, & \text{if } a + b \geq N, \\ |a + b\rangle, & \text{if } a + b < N, \end{cases}
\]

which is the desired result of MA.

In practice, the auxiliary state needs to be restored to its initial state \(|0\rangle\) for recycling. This may also be achieved coherently with the help of an overflow and an auxiliary state. Since the auxiliary state after the MA operation in (22) is (20), we simply need to design a sequence of functions that
differentiate the two cases (i) and (ii), which can be used for the restoration process. One way is to subtract $a$ from (22), namely,
\[
\hat{a}_{a}^{-1} U_{a}^{-1} \hat{a}_{a} U_{a} \hat{a}_{a}^{-1} \hat{a}_{a} [\hat{u}(0); \{a^{-1}_{a} \hat{a}_{a}[b]; \hat{v}([a^{-1}_{a} \hat{a}_{a}[b])_{[\ell_{a}]}]\}]
\]
\[
= \begin{cases} 
|a + b - N>, & \text{if } a + b \geq N, \\
|a + b>, & \text{if } a + b < N, 
\end{cases}
\] 
(23)

which restores the auxiliary state to $|0\rangle$ for both cases (i) and (ii). Adding $a$ to (23) after the restoration in (25), we once more obtain
\[
\hat{a}_{a} U_{a}^{-1} \hat{a}_{a} [\hat{u}(0); \{a^{-1}_{a} \hat{a}_{a}[b]; \hat{v}([a^{-1}_{a} \hat{a}_{a}[b])_{[\ell_{a}]}]\}]
\]
\[
= \begin{cases} 
|a + b - N>, & \text{if } a + b \geq N, \\
|a + b>, & \text{if } a + b < N, 
\end{cases}
\] 
(26)

which completes a coherent and reusable MA architecture that has separate addition and modulo parts.

So far we have coherently broken ME down into adders. Hence, the last step required to complete the decomposition process, i.e., breaking ME into elemental coherent gates, is now to construct a coherent adder circuit. Executing the addition transform (16) in Fourier space, we would like to obtain
\[
\hat{a}_{a} U_{a}^{-1} \hat{a}_{a} [\hat{u}(0); \{a^{-1}_{a} \hat{a}_{a}[b]; \hat{v}([a^{-1}_{a} \hat{a}_{a}[b])_{[\ell_{a}]}]\}]
\]
\[
= \hat{U}^{(\text{QFT})}^{-1} \hat{a}_{a} \hat{v}^{(\text{QFT})}[b],
\] 
(27)

where $\hat{U}^{(\text{QFT})}$ denotes the unitary inverse of $\hat{a}_{a} \hat{v}^{(\text{QFT})}$ denotes the addition operation in Fourier space. Since we have $\hat{U}^{(\text{QFT})} \hat{a}_{a} \hat{v}^{(\text{QFT})}[b] = [a + b]$, multiplying $\hat{U}^{(\text{QFT})}$ on both sides results in
\[
\hat{U}^{(\text{QFT})} \hat{a}_{a} \hat{v}^{(\text{QFT})}[b] = \hat{U}^{(\text{QFT})}[a + b].
\] 
(28)

Using (6) in (28) and comparing phase factors, we have
\[
\hat{a}_{a} \hat{v}^{(\text{QFT})}[2\pi i (a + b)_{[\ell]} / [2\pi]]_{[m] - 1}
\]
\[
= e^{2\pi i (a + b)_{[\ell]} / [2\pi]} \hat{U}^{(\text{QFT})}[a + b]_{[m] - 1].
\] 
(29)

Since any integer multiple of $2\pi i$ in the exponents of (29) leaves the expression unchanged, replacing $(b_{[m] + b_{[m] - 1]} \cdots b_{[0]})$ with $(b_{[m] - 1] b_{[m] - 2} \cdots b_{[m + 1]} b_{[m] - 1} \cdots b_{[1]} b_{[0]})$, we obtain
\[
e^{2\pi i (a + b)_{[\ell]} / [2\pi]} = e^{2\pi i (\theta / 2^\ell) / [2\pi]}.
\] 
(30)

where we used
\[
b_{[m] - 1] b_{[m] - 2} \cdots b_{[m + 1]} b_{[m] - 1} \cdots b_{[1]} b_{[0]} = b / 2^{\ell}.\]
(31)

Similarly, for the right-hand side of (29), we obtain
\[
e^{2\pi i (a + b)_{[\ell]} / [2\pi]} = e^{2\pi i (\theta / 2^\ell) / [2\pi]}.
\] 
(32)

Inserting (30) and (32) into (29) and solving for $\hat{a}_{a} \hat{v}^{(\text{QFT})}$, we have
\[
\hat{a}_{a} \hat{v}^{(\text{QFT})}[j]_{[m] - 1} = |j^{(a)}⟩_{[m] - 1}
\] 
(33)

which yields $2^{n + 1} - (N - b) > 2^n$ and $b < 2^n$. Defining yet another operation $\hat{w}$ on a binary state $|c⟩$ as
\[
\hat{w}[c] = |(c + 1) \text{ mod } 2⟩,
\] 
(24)

we notice that
\[
\hat{w}[c] = \hat{w}[c + 2^n] = \hat{w}[c + 2^n - N] = \hat{w}[c] + N kinda)
\]

with
\[
|j^{(a)}⟩_{[m] - 1} = e^{2\pi i (\theta / 2^\ell) / [2\pi]} |j⟩_{[m] - 1}.
\] 
(34)

The circuit diagram for $\hat{a}_{a} \hat{v}^{(\text{QFT})}$ in (33), i.e., the quantum Fourier adder (QFA), is shown in Fig. 3.

III. BANDWIDTH

To break currently employed RSA codes, we would need to factor semiprimes $N$ whose bit lengths are of the order of several thousands. Constructing a quantum computer with thousands of qubits and running Shor’s algorithm with the exact QPT circuits as shown in Figs. 1 and 2, however, is strictly impossible since this would require a realization of phase rotation gates with angles $\leq \frac{\pi}{126}$. Given the finite precision and accuracy laboratory tools can provide, realizing even a relatively modest $\frac{\pi}{126}$ phase rotation gate is still unrealistic. Therefore, in this section, we present one way of relaxing such a stringent requirement, namely, banding [3,9–11,21].

Defining an integer $b$, which we call the bandwidth, we band a quantum circuit by removing all the phase rotation gates with an angle smaller than $\frac{\pi}{b}$. In the case of Shor’s algorithm, constructed with the method shown in Sec. II, we can band the following two main circuits: (i) QFT and (ii) QFA. It is, in fact, of the possibility of banding these two

![Fig. 3. Logic circuit of a five-qubit QFA. The number to be factorized is $N = 88$, $\theta$ and $\phi$ are the rotation angles of the phase gates $\hat{a}_{a} \hat{v}^{(\text{QFT})}$ and $\hat{w}$, respectively.](image-url)
circuits that are centrally used in both the ME and PF parts of Shor’s algorithm that provides us with the advantage of using the particular architecture in Ref. [15]. In this section, therefore, we will introduce the banded QFT (BQFT) and the banded QFA (BQFA).

We start by removing phase rotations that are smaller than
\[
\frac{\pi}{2^b} \quad \text{in} \quad (6), \quad \text{i.e.,}
\]
\[
|s_k⟩ = |\hat{U}^{(QFT)}_b|_{k}|0⟩
= \frac{1}{\sqrt{2^b}} \prod_{m=0}^{b-1} \sum_{j=0}^{2^b-1} e^{2\pi i s_m (n_{m-1} - n_{m-2})/2^m}|j⟩|_{n_{m-1}}.
\]
(35)

where \(|\hat{U}^{(QFT)}_b⟩\) denotes the unitary operator for the BQFT with bandwidth \(b\). Writing out the products in (35) in the basis of binary states of Hilbert space, we obtain
\[
|s_k⟩ = (0) + e^{2\pi i s_0/2}|1⟩|_{0-1} + e^{2\pi i s_1/4}|1⟩|_{1-2} + \ldots + e^{2\pi i s_{b-1}/2^{b-1}}|1⟩|_{n_{b-1}},
\]
(36)

which shows that the BQFT may be realized with Hadamard gates and phase rotation gates. A fully quantum mechanical circuit diagram of the BQFT is shown in Fig. 4.

From Sec. II A we recall that the QFT circuit may be constructed semiclassically if it is used for the PF part of Shor’s algorithm. In fact, the semiclassical QFT may also be banded to result in the banded semiclassical QFT as shown in Fig. 5. The only difference in the banding mechanism here from that of the fully quantum version in Fig. 4 is that the deleted gates are classically controlled single-qubit phase rotation gates instead of coherently controlled two-qubit phase rotation gates.

The BQFT as an approximation of the exact QFT has already been described and investigated in the literature [3,9,10,21]. Although the idea may be traced back to Ref. [22], banding other quantum circuits such as QFA has not yet been studied in detail. Therefore, studying the BQFA is a main focus of this paper. In analogy to the BQFT, we turn the QFA

FIG. 4. Logic circuit of a five-qubit BQFT for bandwidth \(b = 1\). In general, a BQFT of bandwidth \(b\) retains all rotation gates \(\theta_j\) with \(j \leq b\) and discards all rotation gates \(\theta_j\) with \(j > b\).

IV. MODE A: HYBRID IMPLEMENTATION OF SHOR’S ALGORITHM

So far in this paper we have demonstrated how Shor’s algorithm may be constructed with a series of coherent quantum circuits (see Sec. II) of which two, i.e., QFT and QFA, can be banded as an approximation method (see Sec. III). In this section we present one way of simulating Shor’s algorithm on a classical computer, a hybrid mode, called mode A, in which we simulate the PF part of Shor’s algorithm, using the semiclassical QFT supplied with the classical result of the ME part of Shor’s algorithm. The goal here is to compute the scaling laws of success probabilities of factoring as a function of \(n\) that allow us to extrapolate the number of gates needed for large \(n \sim 1000\).

Our virtual quantum computer running Shor’s algorithm has two registers: a control register (register I), which is used for the PF part of Shor’s algorithm and a computational register (register II) on which the ME part is executed. In mode A, since the ME part is performed classically, the periodicity \(\omega\) is implemented in register I directly and we need not simulate register II. Therefore, with \(n\) the number of qubits in register I, we define the success probability of factoring, or the absolute performance of the quantum computer, as the sum of probabilities of obtaining any one of the integers closest to integer multiples of \(2^j/\omega\) in register I (the expected peak locations in Fourier space given input with periodicity \(\omega\)), i.e.,

\[
P(n, \omega) = \sum_{j=0}^{n-1} P_j(n, \omega),
\]
(38)

where \(P_j(n, \omega)\) denotes the probability of obtaining an integer \(l_j\) in register I, where

\[
l_j = \left(\frac{2^j}{\omega}\right) j + \beta_j,
\]
(39)
and $\beta_j$, a rational number, ranging from $-1/2$ to $1/2$, ensures that $I_j$ is an integer. Introducing the bandwidth $b_{PF}$ in the PF part of Shor’s algorithm and defining $\tilde{P}(n,b_{PF},\omega)$ as the probability of obtaining $|I_j\rangle$ as a readout of register I when BQFT instead of the exact QFT is used, we define, with (38), the scaled performance as

$$P(n,b_{PF},\omega) = \frac{\tilde{P}(n,b_{PF},\omega)}{\tilde{P}(n,b_{PF}=n-1,\omega)}, \quad (40)$$

where

$$\tilde{P}(n,b_{PF},\omega) = \sum_{j=0}^{n-1} \tilde{P}(j,n,b_{PF},\omega). \quad (41)$$

The scaled and the absolute success probabilities (40) and (41), respectively, serve as the basis for our performance measure. We note that the choice of a single state around $|I_j\rangle$ as a proxy for the performance is well justified since all states under a Fourier peak respond in unison to a varying bandwidth $b_{PF}$ (see Ref. [3]).

Supplied with the exact ME part of Shor’s algorithm, the initial input state in register I of the PF part reads

$$|\psi_I\rangle_I = \frac{1}{\sqrt{K(s_0)}} \sum_{k=0}^{K(s_0)-1} |s_0 + kw\rangle_1, \quad (42)$$

where $K(s_0)$ is the number of elements in the equivalence class

$$[s_0] = \{s_0 + kw, 0 \leq k \leq K(s_0) - 1\}, \quad (43)$$

where the representative $s_0$ ranges between 0 and $\omega - 1$, inclusively. Since the number space in register I ranges from 0 to $2^n - 1$, where $n$ is the number of qubits in register I, which, for a semiprime $N = pq$, is defined as

$$n = \left\lfloor 2 \log_2(N) + 1 \right\rfloor, \quad (44)$$

where $\lfloor \cdot \rfloor$ is the floor function [37], we note that on average $K(s_0)$ is $2^n/\omega$.

Now applying the BQFT with bandwidth $b_{PF}$ defined in (35) on (42), we obtain the final output state

$$|\psi_f(b_{PF})\rangle_I = \frac{1}{\sqrt{2^n K(s_0)}} \sum_{k=0}^{K(s_0)-1} \prod_{m=0}^{n-1} e^{2\pi j s(k) k_m (k_m - 1)} |f\rangle_{(n-m-1)}, \quad (45)$$

where

$$s(k) = s_0 + kw. \quad (46)$$

Thus, with (40) and (41), the normalized success probability is

$$P(n,b_{PF},\omega) = \frac{\sum_{j=0}^{n-1} \langle I_j | \psi_f(b_{PF}) \rangle_I^2}{\sum_{j=0}^{n-1} \langle I_j | \psi_f(b_{PF}=n-1) \rangle_I^2}. \quad (47)$$

Since we are interested in the effect of bandwidth $b_{PF}$ on the performance of a quantum computer, specifically how it scales in $n$, we need to average out the remaining argument $\omega$ in $P(n,b_{PF},\omega)$ above. Defining the order-averaged scaled performance as

$$\tilde{P}_\nu(n,b_{PF}) = \frac{\sum_{s=0}^{\nu(n)} v(s) \tilde{P}(n,b_{PF},s)}{\sum_{s=0}^{\nu(N)} v(s)}, \quad (48)$$

where $v(N)$ is the number of useful orders for a given semiprime $N$ and $v(\omega)$ is the multiplicity of a given order $\omega$, i.e., the number of seeds $x$ of the order $\omega$, we present the order-averaged scaled performance (48) for $n$ ranging from 9 to 40 in Fig. 7. Testing our earlier results in Refs. [3,10,11] which imply that quantum computers follow the scaling law

$$P_{\nu}(n) = 2^{-1.1 \times 2^{3\log_2(n)}}, \quad (49)$$

we report here that the new results confirm the scaling law up to $n = 40$. This is at the limit of what can be achieved on our current computer facility, a 128-core cluster computer. To generate the additional $n = 40$ data point in Fig. 7, we chose

FIG. 7. Mode A scaled performance measure $P$ represented by the properly averaged success probability (48) for successful factorization of sample semiprimes $N$. With bit length of $N \sim n/2$, the normalized probability is shown as a function of $n$ for eight different PF-bandwidths. (a) $b_{PF} = 1$ (triangles), $b_{PF} = 2$ (asterisks), $b_{PF} = 3$ (diamonds), and $b_{PF} = 4$ (squares). (b) $b_{PF} = 5$ (triangles), $b_{PF} = 6$ (asterisks), $b_{PF} = 7$ (diamonds), and $b_{PF} = 8$ (squares). Solid lines through the data points are the fit functions (49).
Appendix A. List of Publications

ROBUSTNESS AND PERFORMANCE SCALING OF A . . .

PHYSICAL REVIEW A 88, 062310 (2013)

\( N = 1,034,273 = 1013 \times 1021 \) since its two prime factors are relatively close to each other, a case known to be hard to factor [38]. Concerning the data displayed in Fig. 7, we note that there are up to 72 different orders for a chosen \( N \), and only after averaging over all these different orders does the data corresponding to a given \( N \) appear as a single point in Fig. 7.

Absolute performance data may be obtained analytically from the scaled performance data in Fig. 7. First, noticing that the absolute performance of our virtual quantum computer running in mode A with bandwidth \( \nu_P \) is

\[
P(n, \nu_P, \omega) = P(n, \nu_P, \omega) \sum_{j=0}^{n-1} |\langle j | \psi \rangle (\nu_P = n - 1)|^2,
\]

where we used (40) and (47), we immediately see that the analytical expression of the sum in (50), which is the same as \( \hat{P}(n, \omega) \) in (38), will yield the desired absolute performance conversion right away. Applying a full bandwidth QFT to (42) and suppressing the argument \( \nu_P \) of \( K \), we obtain

\[
|\psi\rangle_I = \frac{1}{\sqrt{2^K}} \sum_{j=0}^{2^K-1} e^{2\pi i j \omega n / 2^K} |j\rangle,
\]

where \( |\psi\rangle_I \) indicates the final output state of register I. Evaluating the sum in (50) together with (39) and (51), we obtain the analytical absolute performance measure of the quantum computer as

\[
\hat{P}(n, \omega) = \sum_{j=0}^{n-1} |\langle j | \psi \rangle (\nu_P = n - 1)|^2
\]

\[
= \sum_{j=0}^{n-1} \frac{1}{2^K} \left| \sum_{k=0}^{K-1} e^{2\pi i j k \omega / 2^K} \right|^2
\]

\[
= \sum_{j=0}^{n-1} \sin^2(\pi K \omega n / 2^K)^2.
\]

Inserting (52) in (50), we obtain the desired conversion

\[
\hat{P}(n, \nu_P, \omega) = P(n, \nu_P, \omega) \sum_{j=0}^{n-1} \sin^2(\pi K \omega n / 2^K)^2
\]

Applying the order averaging in analogy to (48), we obtain

\[
\hat{P}_\delta(n, \nu_P) = \sum_{k=0}^{N/2-1} v(\nu_k) \hat{P}(n, \nu_P, \nu_k)
\]

where the solid lines are

\[
\hat{P}_\delta(n) = 0.774 \times 2^{-1.12 \times 2^{19} (n-8)}.
\]

We note that compared to the solid lines in Fig. 7 [see (49)], (55) is a factor 0.774 smaller, but is otherwise identical with (49).

The factor 0.774 arises due to the following reason. Previously, in Ref. [3], it has been demonstrated that the average order for a given odd, non-complete-square semiprime \( N \) scales like

\[
\langle \omega \rangle \approx N/5,
\]

where the inner average indicates order averaging, i.e.,

\[
\langle \omega \rangle = \frac{\sum_{k=0}^{N/2-1} v(\nu_k) \nu_k}{\sum_{k=0}^{N/2-1} v(\nu_k)}
\]

and the outer average denotes our binning process [3], i.e.,

\[
\langle \langle \omega \rangle \rangle(N^{(i)}) = \frac{1}{\chi(N^{(i)} + 250) - \chi(N^{(i)} - 250)} \sum_{k=0}^{N/2} \frac{1}{\nu_k} \langle \omega \rangle_k,
\]

\[
N^{(i)} = 500 \left( i - \frac{1}{2} \right), \quad i = 1, \ldots, 20,
\]

where \( \chi(N) \) is the odd, non-complete-square semiprime counting function and \( \langle \omega \rangle_k \) is the average \( \omega \) in (57) for the
Appendix A. List of Publications

Y. S. Nam and R. Blumel

PHYSICAL REVIEW A 88, 062310 (2013)

FIG. 9. Doubly-averaged \( \langle r \rangle \) defined according to (58) as a function of \( N \). The solid line through the data points is the fit function (63).

1st semiprime. Using (39) in (52), we obtain

\[
\sum_{j=0}^{\frac{\omega}{2}} \frac{\sin^2(\pi j \omega)}{2 \pi j^2} = \sum_{j=0}^{\frac{\omega}{2}} \sin^2(\pi j \omega) / 2^{\alpha} \sin(\pi j \omega) / 2^{\alpha} \approx \sum_{j=0}^{\frac{\omega}{2}} \frac{\sin^2(\pi j \omega)}{2^{\alpha}} / 2^{\alpha} \sin^2(\pi j \omega) / 2^{\alpha} \approx \sum_{j=0}^{\frac{\omega}{2}} \frac{\sin^2(\pi j \omega)}{2^{\alpha}} / 2^{\alpha} \sin(\pi j \omega) / 2^{\alpha}
\]

(59)

where we used the \( \pi \) periodicity of the square of the sine function. Motivated by an increasing \( \langle \omega \rangle \) in \( N \), we would like to transform the sum into an integral ranging between \( -\pi \) and \( \pi \) with the same double average as used in (63). This inspires us to investigate how \( \langle \omega \rangle \) scales in \( N \) since an increase in \( N \) will allow us to employ the integral approximation we would like to use in (61). Numerical results for \( \langle \langle r \rangle \rangle \) with the same double average as used in (56) are shown in Fig. 9. The fit line has an \( N \)-dependence of

\[
\langle \langle r \rangle \rangle = \frac{\gamma}{100} N
\]

(63)

which implies that we may indeed use the integral transform to approximate the sum in (61). Using (i) \( K \approx 2^i / \omega \) and (ii) \( \omega < N \ll 2^i \) in (61) and turning the sum into an integral ranging from \(-\frac{1}{2}\) to \( \frac{1}{2} \) with \( \beta \) now a continuous variable, we obtain

\[
\sum_{j=0}^{\frac{\omega}{2}} \frac{\sin^2(\pi j \omega) / 2^{\alpha}}{2 \pi j^2} \approx \frac{1}{\omega} \int_{-\frac{1}{2}}^{\frac{1}{2}} \sin^2(\pi j \omega) / 2^{\alpha} \sin(\pi j \omega) / 2^{\alpha} \, d\beta
\]

(64)

where

\[
\int_{-\frac{1}{2}}^{\frac{1}{2}} \frac{\sin^2(\pi \beta)}{(\pi \beta)^2} \, d\beta \approx 0.774
\]

(65)

This completes the explanation of the origin of the factor 0.774 in (55).

As an aside we note a typo in Eqs. (65) and (120) in Ref. [3]: \( \varphi_{\pi \omega}(N) \) in these two equations needs to be replaced by the proper normalization \( \sum_{n=1}^{N} \psi(\omega_n) \), where the sum is over all \( \psi \) functions \( \omega_n \), as in Eqs. (48) and (57) in this paper. However, since the computations in Ref. [3] had been done with the correct normalization, the results and conclusions in Ref. [3] remain unchanged.

In Fig. 8 we observe that the performance scaling in the low \( n \) region is not as well represented by the fit line (55) as in the higher \( n \) region, especially for the larger bandwidth cases. This is no surprise since the integral approximation holds well for the large \( n \) region only. We also expect this deviation for the following reason. In case \( \omega \) is a power of 2, i.e.,

\[
\omega = 2^r
\]

(66)

we note that

\[
K = 2^r / \omega = 2^{r-\alpha}
\]

(67)

for any \( \omega \), and in (39)

\[
\beta_j = 0
\]

(68)

since \( \beta_j = j K \). Inserting (67) and (68) into (52), we obtain

\[
\hat{P}(n, \omega = 2^r) = 1
\]

(69)

Combined with the result proved in Sec. IV of Ref. [3], i.e., that for \( \omega = 2^r \) the scaled performance of the quantum computer is 100% for any bandwidth \( \beta_{PP} \), we have

\[
\hat{P}(n, \beta_{PP}, \omega = 2^r) = \hat{P}(n, \beta_{PP} = n - 1, \omega = 2^r)
\]

(70)

We conclude that, together with (69),

\[
\hat{P}(n, \beta_{PP}, \omega = 2^r) = 1
\]

(71)

This means that we can decompose the fit line (55) into two parts: (i) power 2 orders that result in perfect performance and (ii) nonpower 2 orders that result in an imperfect performance.

Defining the weight \( \mu_N \) for a given semiprime \( N \) in terms of the multiplicity of power 2 orders according to

\[
\mu_N = \frac{\sum_{n=1}^{N} \psi(\omega_n) \theta(\omega_n)}{\sum_{n=1}^{N} \psi(\omega_n)}
\]

(72)

where \( \theta(\omega) \) is a binary function defined as

\[
\theta(\omega = 2^r \rho) = 0, \quad \text{if} \quad \rho \neq 1,
\]

\[
1, \quad \text{if} \quad \rho = 1,
\]

(73)

we observe that \( \mu_N \) shows a power-law behavior in \( N \). To extract the power, we bin \( \mu_N \) in (72) logarithmically, i.e.,

\[
\mu(\mathcal{N}_i) = \frac{1}{x(10^{\log_{10}(\mathcal{N}_i)}) - x(10^{\log_{10}(\mathcal{N}_i - 1)})} \times \sum_{\substack{j=1 \atop j=x(10^{\log_{10}(\mathcal{N}_i - 1)})}}^{j=x(10^{\log_{10}(\mathcal{N}_i)})} \mu_j
\]

(74)

\[
\mathcal{N}_i = 10^{2.2i}, \quad i = 1, \ldots, 6
\]
Appendix A. List of Publications

where \( \mu \) is the \( L \)th semiprime. Figure 10 shows \( \mu \) as a function of \( N \) as a log-log plot with \( N \) ranging up to \( 10^4 \). We find numerically

\[
\mu \approx \frac{8}{N^{0.81}},
\]

which is the solid line shown in Fig. 10. Together with

\[
N \approx 2^{\nu/2},
\]

implied by our choice of \( n \) in (44), we obtain

\[
\mu \approx 2^{-0.415n+1}.
\]

Decomposing the \( \tilde{P}_{\text{bn}}(n) \) fit line (55) into the two parts (i) and (ii), we obtain with (77)

\[
\tilde{P}_{\text{bn}}(n) = \mu + (1 - \mu) \times 0.774 \times 2^{-1.1n} \times 2^{-0.3(\nu(n-8))}.
\]

As shown in Fig. 11, we find that the new fit line (78) with the power 2 order correction is in better agreement with the absolute performance data than the original fit line (55). We note that even the new line does not fit the data perfectly, however, since the scaling in the low \( n \) region, especially for large \( b_{\text{PF}} \), is not exponential to start with (see Ref. [3]). In addition, the poor quality of the integral approximation [see (64)] in this regime results in the scattering and the deviation of data points from the fit line (78), which becomes more prominent as \( N \) becomes smaller since the smaller \( N \), the fewer the number of orders of \( N \) that are present. To see this better, we plot our data with extended range in \( \tilde{P} \) in Fig. 12. We observe that in the low \( n \) regime the new line (78), as it should, fits the data much better than the old line (55) with some remaining, but noticeable, scattering of the plot symbols around the improved fit line.

V. MODE B: COMPLETE IMPLEMENTATION OF SHOR’S ALGORITHM

In Sec. IV we investigated a hybrid implementation of Shor’s algorithm, providing the quantum computer with the classically computed ME result. In this section we study a complete implementation of Shor’s algorithm where both ME and PF are performed quantum mechanically. We show that a quantum computer running Shor’s algorithm, when

constructed according to Beauregard’s method [15] (see Sec. II), is robust against QFT and QFA banding defined in Sec. III. Specifically, we report here the scaling law of its performance and compare it to numerical results.

Our mode-B implementation is based on the circuits presented in Ref. [15]: we build ME from MMs that can be decomposed into consecutive MAs, which we construct by combining adders that are executed in Fourier space and modular parts that are executed using qubit recycling (see Sec. II B for the explicit construction). Assessing the number of qubits needed for running our simulation in mode B, we note that the number of qubits used in the simulation is, for \( L \) the bit length of the semiprime \( N \) to be factored, (i) \( 2L+2 \) for the ME part and (ii) \( 2L \) for the PF part, making the total number of qubits in the simulated quantum computer \( 4L+2 \). This is so because QFA, for instance, requires \( L+1 \) qubits for adding two \( L \)-bit integers, where the additional qubit arises from the need to have an overflow qubit. Since the modulo part demands an auxiliary qubit to be used, the computational register, which is capable of executing the quantum MA, then, consists of \( L+2 \) qubits. Since MM now is constructed via consecutive applications of MA, requiring \( L+2 \) qubits, and since the MM

\[
\begin{align*}
\text{FIG. 10.} & \quad \text{Power 2 order multiplicity } \mu \text{ as a function of } N, \text{ binned according to (74). The solid line is the fit function (75).} \\
\text{FIG. 11.} & \quad \text{Mode A absolute performance measure } \tilde{P} \text{ for sample semiprimes } N \text{ (as a function of } n \text{ as in Fig. 8) with improved fit functions (78) (solid lines). The PF bandwidth } b_{\text{PF}} \text{ ranges from } b_{\text{PF}} = 1 \text{ to } b_{\text{PF}} = 8. \text{ (a) } b_{\text{PF}} = 1 \text{ (triangles), } b_{\text{PF}} = 2 \text{ (asterisks), } b_{\text{PF}} = 3 \text{ (diamonds), and } b_{\text{PF}} = 4 \text{ (squares). (b) } b_{\text{PF}} = 5 \text{ (triangles), } b_{\text{PF}} = 6 \text{ (asterisks), } b_{\text{PF}} = 7 \text{ (diamonds), and } b_{\text{PF}} = 8 \text{ (squares).}}
\end{align*}
\]
operation needs a quantum register that stores the intermediate L-bit computational results from the previous MM operation. Since no extra qubits are required to obtain ME from MM as shown in (11), we conclude that 2L + 2 qubits are required to realize ME. Counting 2L qubits used for the PF part of Shor’s algorithm [6], we obtain 4L + 2 as the total number of physical qubits. We remark that, in principle, a bus qubit is necessary for running a quantum computer. Hence, the effective total number of qubits that are simulated on our virtual quantum computer is 4L + 3.

Implementing the quantum circuit presented in Ref. [15], this time, we build the ME part of Shor’s algorithm equipped with BQFT and BQFA as it would be used on an actual quantum computer. We choose, as mentioned previously, the number of qubits in register I that is to be used for the PF part of Shor’s algorithm to be

$$n = 2L$$  \hspace{1cm} (79)

and the number of qubits that contain the result of ME to be

$$n' = L.$$  \hspace{1cm} (80)

Unlike in mode A (see Sec. IV), this time, the PF part of Shor’s algorithm is not fed with input states that are periodic in \(\omega\) [see (43)]. Rather it is provided with the result of the banded ME. In general, with \(b_{PF}\) the bandwidth imposed on the BQFT and the BQFA in the ME part, the initial state reads

$$|\psi_i\rangle = \frac{1}{\sqrt{2^b}} \sum_{r=0}^{2^b-1} \left[ |r\rangle_I \sum_{y=0}^{2^b-1} |y\rangle_{\Pi A} \left( \sum_{y'=0}^{2^b-1} |y'\rangle_{\Pi B} \times \left[ \frac{1}{c} \sum_{\beta=0}^{1} \Lambda_{r,y',y',\beta}^{(b_{PF})} \right] \right) \right].$$  \hspace{1cm} (81)

where \(|r\rangle_I\) represents register I states, \(|y\rangle_{\Pi A}\) contains the ME results, \(|y\rangle_{\Pi B}\) indicates the states of the quantum register employed in MA, including the overflow qubit, \(|c\rangle\) is the auxiliary qubit used in MA, and \(|\beta\rangle\) is the bus qubit state of the quantum computer with the associated amplitudes \(\Lambda_{r,y',y,y',\beta}^{(b_{PF})}\), whose normalization is

$$\sum_{y=0}^{2^b-1} \sum_{y'=0}^{2^b-1} \sum_{\beta=0}^{1} \left( \Lambda_{r,y',y',\beta}^{(b_{PF})} \right)^2 = 1.$$  \hspace{1cm} (82)

We note that since each elementary quantum gate is executed exactly, introducing bandwidth to our circuit does not alter the bus state. Hence, we write

$$|\psi_i\rangle = \frac{1}{\sqrt{2^b}} \sum_{r=0}^{2^b-1} \left[ |r\rangle_I \sum_{y=0}^{2^b-1} |y\rangle_{\Pi A} \sum_{\beta=0}^{1} \Lambda_{r,y',y',\beta}^{(b_{PF})} \right].$$  \hspace{1cm} (83)

where we suppressed the bus state \(|\beta\rangle = |0\rangle\) here and in the following, and used

$$\Lambda_{r,y',y',\beta}^{(b_{PF})} = \delta_{y,0} \delta_{\beta,0} \Lambda_{r,y,y',\beta}^{(b_{PF})},$$  \hspace{1cm} (84)

where \(\delta_{m,m'}\) is 1 if \(m = m'\) and 0 if \(m \neq m'\).

Applying the BQFT with bandwidth \(b_{PF}\) in the PF part of Shor’s algorithm, and recalling that the performance of the quantum computer is defined as the probability of obtaining any one of \(I_f\) in (39), we obtain the absolute performance of the quantum computer running Shor’s algorithm in mode B with seed \(x\) and its associated order \(\omega_0\) as

$$\hat{P}(n,b_{ME},b_{PF},\omega_0; x) = \sum_{j=0}^{\omega_0-1} \sum_{y=0}^{2^b-1} \sum_{y'=0}^{2^b-1} \sum_{\mu=0}^{1} \sum_{\nu=0}^{1} \frac{1}{\sqrt{2^b}} \sum_{r=0}^{2^b-1} \prod_{n=0}^{b-1} \Lambda_{r,y,y',\mu}^{(b_{PF})} \times e^{2\pi i \delta_{\mu,1} j (\mu' y_0 + \nu' y' n_0) |\beta\rangle_\omega |\beta\rangle_\omega + i}.$$  \hspace{1cm} (85)
Since a semiprime $N$ has multiple seeds that can be used to factor, we employ a seed averaging scheme to measure the average performance of the quantum computer

$$\bar{P}(n, b_{ME}, b_{PF}) = \frac{\sum_{\upsilon=1}^{r(N)} \hat{P}(n, b_{ME}, b_{PF}, \omega_{\upsilon}; x(\upsilon))}{\Upsilon(N)},$$  \hspace{1cm} (86)$$

where $x(\upsilon)$ is the $\upsilon$th seed of $N$ that is useful for factoring (see Sec. II) and $\Upsilon(N)$ is the useful seed counting function. In Fig. 13, we show the results of computing (86) for semiprimes $N = 21, 33, 39, 55$, and 57. We note that each semiprime has up to 30 useful seeds that need to be computed individually for different $b_{PF}$ for the ME part of Shor's algorithm, then for different $b_{PF}$ for the PF part of Shor's algorithm. The data for $N = 51$ are not shown due to the fact that all of its orders are powers of 2, leading to a nonscaling behavior in $b_{PF}$.

Normalizing the absolute performance given a seed $x$ in (86) for each different bandwidth in the ME part of Shor's algorithm with that of the full bandwidth in the PF part of Shor’s algorithm, we plot $1 - P$ in Fig. 14, where $P$ is the scaled performance as defined in (40) together with seed averaging in (86), namely,

$$P_{N, b_{PF}} = \sum_{\upsilon=1}^{r(N)} \frac{\hat{P}(n, b_{ME}, b_{PF}, \omega_{\upsilon}; x(\upsilon))}{\Upsilon(N)}.$$

We find quantitatively that

$$1 - P_{N, b_{PF}}(b_{PF}) \approx 2^{-2b_{PF}}$$

(88) (see solid lines in Fig. 14). While for our current simulations ($L = 6$) the number of gates is relatively modest (of the order of 30 000), the number of quantum states that need to be processed by these gates is exponentially large. Therefore, the accuracy of our virtual quantum computer is currently $\approx 10^{-5}$. 

FIG. 13. Mode B absolute performance measure $\bar{P}$ represented by the properly averaged success probabilities (86) for successful factorization of semiprimes $N = 21, 33, 39, 55$, and 57 as a function of PF bandwidth $b_{PF}$ for several ME bandwidths. $b_{ME} = 2$ (asterisks), $b_{ME} = 4$ (squares), and $b_{ME} = 6$ (crosses).
FIG. 14. Mode B PF bandwidth $b_{PF}$ scaling of $1 - P$ [see Eq. (87)] for semiprimes $N = 21, 33, 35, 39, 55,$ and 57 with a proper seed average over $\{x(\nu)\}$. The ME bandwidth ranges from $b_{ME} = 1$ to $b_{ME} = 6$; $b_{ME} = 1$ (triangles), $b_{ME} = 2$ (asterisks), $b_{ME} = 3$ (diamonds), $b_{ME} = 4$ (squares), $b_{ME} = 5$ (circles), and $b_{ME} = 6$ (pentagons). Solid lines are the fit functions (88).

Some of the data for $b_{PF} \geq 8$ are, therefore, omitted as they are at the limit of our accuracy.

VI. DISCUSSION

When it comes to factoring a large semiprime, currently available analytical and numerical techniques fail. However powerful the breakthroughs made in the past century, such as the quadratic number sieve [1] that routinely factors a 100-decimal-digit semiprime, or the more advanced general number field sieve (GNFS) [2] that was used to factor the RSA challenge number RSA-768 [39], they cannot factor even a moderate-sized semiprime of, say, 5000 decimal digits [3].

Quantum computation, a new paradigm of computing, changes the story entirely. Taking advantage of classically impossible logic operations (such as, e.g., the “square root of NOT”), a quantum computer, running Shor’s algorithm, allows us to factor a large semiprime with exponential speedup when compared to its classical counterpart. Of course, even with today’s quantum control techniques, we are far from realizing an actual quantum computer that can factor any meaningful semiprime that might lead to a security breach. This point is driven home by the fact that to date the record largest semiprime factored experimentally using a quantum computer is $N = 21$ [28]. In addition, no experimental demonstration of quantum semiprime factoring has implemented a complete, scaling Shor algorithm. Instead, compiled, highly optimized versions of Shor’s algorithm are used. Hence, any streamlining of quantum algorithms will help realize a scaling quantum computer. Precisely such a simplification of Shor’s algorithm is suggested in our paper: The replacement of the full QFT and QFA with their banded versions. That such a replacement of the quantum circuitry works at all is not obvious. This is illustrated by the following example. Let us look at the result of a banded adder with the bandwidth $b = 2$ that performs the addition $19 + 37$ modulo 64. The expected result is 56. However, as shown in Fig. 15, the adder performs far from ideally, producing the correct result, 56, in only 62% of the
cases. The adder also produces the manifestly wrong results 24, 40, and 48 with each more than 10% probability, in addition to the wrong results 0, 8, and 32 with \( \sim 1\% \) probability. That such an erroneous adder, which, for factoring \( N = 57 \), is applied more than 700 times, still allows us to factor semiprimes with acceptable probability is nothing short of astonishing. This points to a general principle of robustness of quantum computers with respect to static defects. Thus, without sacrificing performance, large numbers of quantum gates may be pruned, resulting in a streamlined architecture that is much more conducive to experimental implementation. In addition, we show how the banded Shor algorithm scales. Simulations of Shor’s algorithm themselves have been performed before, most of which have focused on parallel implementation on a multiprocessor classical computer. Notable ones include the following. (i) Obenland et al. [29] simulated Shor’s algorithm with the adder shown in Ref. [13] and focused on the scaling of the speedup and the execution time in the number of classical processors. (ii) Niwa et al. [30] simulated Shor’s algorithm with the adder in Ref. [23], which is very close to the one presented in Ref. [12]. They investigated the effects of decoherence and operational errors, using the classical ME results (akin to our mode A) for semiprimes \( N > 15 \). (iii) De Raedt et al. [31] illustrated the use of a portable software package simulating quantum computers on massively parallel classical supercomputers, implementing Shor’s algorithm as a test case. The ME part of Shor’s algorithm was simulated without the auxiliary qubit array. (iv) Tabakin et al. [32] created a convenient parallel computing environment. Other works more closely related to our work include (v) Fowler and Hollenberg [9], addressing the effect of bandwidth introduction to the PF part of Shor’s algorithm and (vi) García-Mata et al. [33,34] focusing on the influence of noise on the performance of the quantum computer running Shor’s algorithm using the classical ME results. The pioneering investigations described in (i) to (vi) all differ from our implementation in various ways, from different adder architectures to the presence or the absence of the auxiliary qubit array, with the ME or the PF parts of Shor’s algorithm simulated fully coherently or not. Most importantly, however, our implementation focuses on the influence of simultaneous banded of the PF part and the QFT-based ME part of Shor’s algorithm running on a virtual, scalable, fully coherent quantum computer including auxiliary qubits that are executed at an elementary quantum gate level.

We note that even though we use 128 classical computing cores simultaneously in our simulations, we are at the limit of our computing resources: Running our virtual quantum computer in its hybrid mode, it took us three months of CPU time to compute the data, as each semiprime needs to be factored with different orders individually, each with up to 72 different orders. This means that not only do we suggest barding for the purpose of practical implementation of quantum computers but also as a way to simulate larger virtual quantum computers with more qubits. Running our virtual quantum computer in its complete mode due to its memory requirement scaling exponentially in the number of qubits \( 4L + 3 \), where \( L \) is the bit length of the semiprime to be factored, we are currently limited to \( L \leq 6 \). Nonetheless, this is enough to break the current experimental record of \( N = 21 \). Increasing \( L \) to 7, however, is within our reach and will be explored in future work.

For now it is interesting to explore how many rotation gate operations may be saved by barding the quantum computer. We start by counting the total number of rotation gates \( n_s \) of the ideal, nonbanded quantum computer of \( n = 4L + 3 \) qubits.

We obtain

\[
\begin{align*}
n_s &= 18L^4 + 42L^3 + 26L^2 - L. 
\end{align*}
\]

Introducing barding with bandwidth \( b_{PF} \) in the period finding part of Shor’s algorithm, we save

\[
\begin{align*}
n_{s,PF} &= \frac{(2L - b_{PF})(2L - b_{PF} - 1)}{2} 
\end{align*}
\]

rotation gates. Introducing barding with bandwidth \( b_{ME} \) in the modular exponentiation part of Shor’s algorithm, we save

\[
\begin{align*}
n_{s,ME} &= (L - b_{ME})(L - b_{ME} + 1)(18L^2 + 4L) 
\end{align*}
\]

rotation gates. Adding \( n_{s,PF} \) and \( n_{s,ME} \), we obtain the total number of saved rotation gates

\[
\begin{align*}
n_s &= \frac{(2L - b_{PF})(2L - b_{PF} - 1)}{2} 
+ (L - b_{ME})(L - b_{ME} + 1)(18L^2 + 4L). 
\end{align*}
\]

Although we factored semiprimes up to \( N = 57 \) and found that \( b_{PF} = 4 \) and \( b_{ME} = 5 \) is sufficient to factor these semiprimes with a 70% success rate, it is too early to extrapolate these results to the \( n \sim 1000 \) regime. This requires more statistics to be accumulated by running our virtual quantum computer for larger \( n \). However, if the mode-A results are any indication, it is perhaps possible to factor large semiprimes on \( n \sim 1000 \) qubit quantum computers with \( b_{PF} = b_{ME} = 8 \). In this case, for \( L = 2048 \), according to (92), 314 378 411 210 788 rotation gates, or 99.167% of the total number of rotation gates, may be discarded, resulting in a substantial simplification of the required quantum circuitry.

Gate pruning, as suggested in this paper, does not reduce circuit depth. As a consequence, gate pruning will not affect the run time of Shor’s algorithm as implemented in this paper. In the same vein, gate pruning does not affect the total number of qubits required in our implementation of Shor’s algorithm.
The reduction of run time and number of qubits is a challenge for quantum algorithm development, a topic beyond the scope of our present paper. In the present paper, we take an existing quantum algorithm, i.e., Shor’s algorithm, and investigate how it can be “trimmed” in a scalable way to actually have a chance to be implemented in practice. However, while not shortening execution time, or reducing the total number of required qubits, the possibility of gate pruning has profound advantages in terms of the actual realization of a scaling quantum computer. Since quantum gates are prone to error, any reduction in the number of quantum gates is an advantage when it comes to actually building a working quantum computer. Since according to our estimates, for a computer of contemporary interest, more than 99% of rotation gates may be trimmed from the quantum circuit with acceptable consequences for the performance, only 1% of rotation gates actually need to be realized. In our opinion, this is an important step forward toward the actual realization of scaling quantum computers.

VII. SUMMARY AND CONCLUSION

Using banding as a special way of optimizing Shor’s algorithm, we investigated the performance of a quantum computer running Shor’s algorithm in two different modes, a hybrid mode, called mode A, with classical ME and quantum mechanically executed PF, and a complete mode, called mode B, with quantum mechanically executed ME and PF. Mode A allows us to study the effects of BQFT, while mode B allows us to study the effects of BQFT and BQFA combined. Our contributions can be summarized in the following advances.

1. Constructing a virtual 128-core quantum computer running Shor’s algorithm based on the QFT as suggested in Ref. [15], fully decomposed into elementary quantum gates.
2. Confirming an earlier result of exponential scaling of the normalized performance $P$ in hybrid implementation (classical ME; quantum PF) up to and including $N = 1,034,273$, using $n = 40$ qubits, the largest virtual quantum computer simulated so far.
3. An improved scaling law for the absolute performance $P$ in the hybrid mode of a virtual quantum computer using the doubly averaged $(\langle r \rangle)$ and the weight of the power 2 orders $\mu$.
4. Absolute performance results of the complete implementation of Shor’s algorithm when the QFA and the QFT in the ME part of Shor’s algorithm are pruned via banding.
5. Confirmation of the previously found $2^{-20}$ scaling of $1 - P$ of a virtual quantum computer running in its complete mode for additional semiprimes other than $N = 21$ such as $N = 33, 35, 39, 55, \text{and} 57$. The data shown in this paper are seed-averaged (with up to 30 different seeds per semiprime) according to [86], whereas in Ref. [11] $N = 21$ was factored with the single seed $s = 2$. In addition the case $N = 21$ was run with $n = 12$ in this paper, whereas it was run with the lower $n = 10$ in Ref. [11]. This demonstrates the scalable nature of the quantum computer.

We believe that based on the numerical and the analytical work presented in this paper, in conjunction with Refs. [3,10,11], the PF part of Shor’s algorithm, equipped with a BQFT, is well understood. This includes the absolute performance, an absolute lower bound on the factoring success of the banded Shor’s algorithm running in hybrid mode. We have also simulated a more demanding part of Shor’s algorithm, the ME part, fully coherently, keeping the exact quantum entanglement during the entire simulation, including the auxiliary qubits, factoring up to and including $N = 57$. Numerically confirming the scalability of our virtual quantum computer, we see a surprising robustness of the quantum computer when pruned with banding, resulting in substantial savings in required quantum circuitry.

ACKNOWLEDGMENTS

The authors are grateful for a generous allotment of computer resources by the Wesleyan Scientific Computing Center. R.B. acknowledges financial support by Grant No. 216687 of the Research Council of Norway.

Appendix A. List of Publications

Robustness of the quantum Fourier transform with respect to static gate defects

Y. S. Nam and R. Blümel
Department of Physics, Wesleyan University, Middletown, Connecticut 06459-0155, USA
(Received 18 February 2014; published 30 April 2014)

The quantum Fourier transform (QFT) is one of the most widely used quantum algorithms, ranging from its primary role in finding the periodicity hidden in a quantum state to its use in constructing a quantum adder. Testing how the QFT performs under more realistic conditions, we find that the QFT, when used for period finding, shows extraordinary robustness with respect to static gate defects. For instance, replacing all rotation angles $\pi/2^j$ of the controlled rotation gates in the QFT circuit by $\pi(1+r)/2^j$, where $r$ is a uniformly distributed random variable taking values in the range $[-1,1]$, effectively resulting in a QFT with random gates, the QFT performs well above the expected random result. However, it is important to keep the $2^j$ terms in the denominators of the rotation angles, resulting in random, but hierarchically random, gates. Relaxing this hierarchical structure of the QFT circuit, we find that the performance of the QFT deteriorates significantly. This observation indicates that the hierarchical structure of the quantum circuit of the QFT is more important for the observed robustness in performance than the precise actions of individual gates. In addition to the specific example of the QFT circuit studied here, this observation also corroborates our experience with more general and more complex quantum circuits. Thus, backed by our detailed numerical and analytical results, we may condense the results of our research into the following general principle: The topology of a quantum circuit is more important than the precise actions of its gates.

DOI: 10.1103/PhysRevA.89.042337
PACS number(s): 03.67.Lx

I. INTRODUCTION

Many quantum algorithms are known that use the quantum Fourier transform (QFT) [1] as their core ingredient. Examples range from the proof-of-concept Deutsch-Jozsa algorithm [2,3] to the more “practical” Shor algorithm [1,4], perhaps the most well-known and most powerful quantum algorithm to date. Considering additional algorithms that make use of the QFT, such as Simon’s algorithm [5] and the Gaussian summation algorithm [6], an interesting fact emerges: Quantum algorithms that use the QFT generally display exponential speed-up when compared to their classical counterparts. It is this characteristic feature of the QFT that motivates us to investigate QFT circuits under realistic conditions.

Numerous studies of the performance of the QFT under various conditions have already been performed and can readily be found in the literature [7–11]. Despite these pioneering works, however, the performance of the QFT subjected to a wider class of static defects introduced at the gate level has not yet been explored in sufficient analytical detail to result in explicit, analytical scaling formulas as a function of the size of the defects and the number of qubits. Therefore, the goal of this paper is to close this gap. We do this by systematically introducing different types of static defects into the QFT circuit and subsequently investigate analytically and numerically the performance of the resulting, altered QFT circuits. As one of the most surprising results of our investigation we find that the QFT circuit is astonishingly tolerant of static gate defects. For instance, in the case of the controlled rotation (CROT) gates of the QFT circuit we find that using “small but otherwise random” rotation angles instead of the exact angles is sufficient to guarantee satisfactory performance of the QFT circuit.

Since in this paper we focus on the QFT, the controlled phase rotation gate (CROT) and the Hadamard gate (H) take center stage. Since, depending on the state of some control qubit, the role of the CROT gate is to rotate the phase angle of a target qubit by a specified amount, we study the effect of altered, “defective” CROT gates whose rotation angles deviate significantly from their respective ideal values. Given that an ideal H gate is supposed to turn the two computational states $|0\rangle$ and $|1\rangle$ into even and odd superpositions of each other, the defective H gates to be studied will produce superpositions that deviate considerably from the ideal, equiweighted superposition produced by the ideal H gate. Thus, our investigations in this paper may be summarized as follows: Replacing the ideal CROT and H gates in the ideal QFT circuit by defective CROT and H gates results in a defective QFT circuit whose performance scaling is studied as a function of the strength of the defects and the number of qubits of the QFT circuit. As a recurring theme of this paper we find that the QFT circuit still operates satisfactorily under conditions in which the individual gates have been distorted so much from their specified functions as to act nearly, or actually, as random gates. Therefore, as our central result, we find that the operation of a QFT circuit depends to a lesser degree on the actions of individual gates in the circuit than on the hierarchical structure of the circuit. We prove this point by showing that the QFT circuit is much more sensitive to a breakdown of its hierarchical structure than to the precise operation of its gates. This observed robustness of the QFT circuit with respect to “manufacturing defects” of the quantum gates may be welcome news for experimental physicists and quantum engineers, since it means that manufacturing tolerances may be relatively relaxed when it comes to producing or implementing the gates for an actual hardware realization of the QFT circuit.

Our paper is organized as follows. In Sec. II we present a numerical study of the effects of static defects in the CROT and H gates of the QFT circuit. We start this section by defining the four different types of static defects studied in this paper, and then systematically explore three cases: (i) ideal H gates and defective CROT gates (Sec. II A), (ii) ideal CROT gates...
Appendix A. List of Publications

Y. S. Nam and R. Blumel

PHYSICAL REVIEW A 89, 042337 (2014)

FIG. 1. Circuit diagram of an exact five-qubit QFT. While all numerical simulations in this paper are performed for \( n \geq 10 \) qubits, we chose the five-qubit case here for illustrative and graphical reasons only. The QFT shown transforms an integer input state \(|a\rangle\) into a superposition of integer output states \(|b\rangle\). The square brackets in the subscripts denote the positions of the binary digits.

and defective H gates (Sec. II B), and (iii) a case in which both CROT and H gates are defective (Sec. II C). We find that although the defects introduced are large, going so far as to introduce random gates in place of the required ideal gates, the QFT circuit still operates with surprisingly high performance. In Sec. III we support our numerical results with detailed analytical calculations. We discuss our results in Sec. IV and summarize and conclude our paper in Sec. V. All numerical results presented in Secs. II and III are for QFTs with \( n = 10 \) qubits. We verify that our \( n \)-scaling predictions, we simulate QFTs with a variable number of qubits, ranging from \( n = 10 \) to \( n = 20 \).

II. NUMERICAL RESULTS

The QFT employs two types of quantum gates: The Hadamard gate (H) and the controlled phase rotation gate (CROT). For an \( n \)-qubit QFT circuit (see Fig. I for an illustration of a QFT circuit with \( n = 5 \) qubits) there are \( n \) Hadamard gates and \( n(n - 1)/2 \) CROT gates. Thus, in the large \( n \) limit, the CROT gates are by far the most numerous quantum gates in the QFT circuit. Therefore, it is natural to first study the case in which we treat the H gates as ideal and introduce static gate defects only in the CROT gates (Sec. II A). This is followed by the case in which we treat the CROT gates as ideal, introducing static gate defects only in the H gates (Sec. II B), and then conclude (Sec. II C) with a representative case in which we introduce static defects in both the CROT and the H gates. As a measure of the performance of the QFT, we use the success probability of obtaining the correct periodicity of an input state from the measured output state via the nearest real-valued, correct Fourier peaks (see Ref. [12]). We exclude, however, those trivial peaks that correspond to the powers-of-2 factor of the given periodicity, since it can be shown analytically [12] that they do not respond to any of the CROT defects we introduce in this paper. In all the cases studied, we find that despite the CROT gate being defective, the QFT still determines the periodicity of the input state with reasonable probability. Thus, if used in Shor’s algorithm, e.g., a QFT realized with defective quantum gates, even if the defects are “large” by some measure (to be quantified below), we will still be able to factor large semiprimes with large enough probability to be acceptable for code breaking [1,13].

A. H gates exact; CROT gates defective

An exact CROT gate performs the following quantum operation:

\[
\hat{\theta}_j|c\rangle|t\rangle = \begin{cases} |c\rangle e^{i\theta_j} |t\rangle, & \text{if } |c\rangle = |1\rangle = |t\rangle, \\ |c\rangle |t\rangle, & \text{otherwise}, \end{cases}
\]

where

\[
\theta_j = \frac{\pi}{2^j}
\]

is the exact rotation angle. We call a CROT gate with nominal phase-rotation angle \( \theta_j \), a CROT gate of type \( j \). In practice, of course, it is impossible to realize \( \theta_j \) exactly. In an NMR quantum computer [1], e.g., the magnetic fields may be slightly off, resulting in a small modification of \( \theta_j \); in an ion-trap quantum computer [7,14], e.g., a stray, static electric field may be present, again resulting in a modified \( \theta_j \). All these imperfections, however, have one thing in common: They are likely to stay fixed during the time it takes to perform a quantum computation. We therefore call these imperfections static defects. In the presence of a static defect, \( \theta_j \) is altered to a modified CROT gate \( \hat{\theta}_j \) that performs the operation

\[
\hat{\theta}_j|c\rangle|t\rangle = \begin{cases} |c\rangle e^{i\tilde{\theta}_j} |t\rangle, & \text{if } |c\rangle = |1\rangle = |t\rangle, \\ |c\rangle |t\rangle, & \text{otherwise}, \end{cases}
\]

where

\[
\tilde{\theta}_j = \theta_j + \epsilon_j
\]

and \( \epsilon_j \) is the size of the static defect caused by the imperfections of the gate. In this paper we study four different kinds of CROT defects, depending on whether the defects introduce relative or absolute phase errors, and whether the defects are correlated with the type \( j \) of the CROT gates or not. Correlated defects are natural if we think of solid-state implementations [15] of quantum computers in which CROT gates of a certain type are mass produced by a process specific to the type \( j \) of a gate. Thus we may assume that as a result of this manufacturing process all gates of type \( j \) have the same relative error, i.e., in this case,

\[
(\text{RC}) \quad \tilde{\theta}_j = \theta_j(1 + \epsilon_j),
\]

where \( \epsilon > 0 \) is the size of the defect, and \( \epsilon_j \) is a random variable, the same for all gates of type \( j \). As indicated in (5), we refer to this case as (RC) (relative error; gate-correlated). Of course, we may also imagine manufacturing processes in which the relative error of the CROT gates is controlled, but the error happens randomly, not correlated with a specific type of gate. In this case we have

\[
(\text{RU}) \quad \tilde{\theta}_j = \theta_j(1 + \epsilon),
\]

where, as before, \( \epsilon > 0 \) controls the size of the defect, but \( \epsilon \) is a random variable, uncorrelated with the specific type of the CROT gates. As indicated in (6), we denote this case by RU (relative error; uncorrelated with gate type). To complete the types of static defects that the CROT gates in the QFT
Appendix A. List of Publications

ROBUSTNESS OF THE QUANTUM FOURIER TRANSFORM . . .

PHYSICAL REVIEW A 89, 042337 (2014)

FIG. 2. Normalized success probability $P$ of period finding as a function of $\epsilon$ for RC type (triangles) and RU type (crosses) static defects in the $\text{CROT}$ gates of the QFT. (b) Shows (a) on a logarithmic scale, expanding the tail of (a). The numerical fit function (11) is shown as the dotted lines in (a) and (b). The horizontal dashed line in (b) is the approximate, large-$\epsilon$, asymptotic performance (13). The numerical calculations were performed for QFTs with $n = 10$ qubits.

In this section, keeping the $\text{H}$ gates exact, we investigate the performance of the ten-qubit QFT circuit as a function of $\epsilon$ for the four different types of static defects listed in (9). The procedure is as follows. We choose an input state with periodicity 30, apply a QFT with defective gates on this input state, and attempt to obtain the periodicity of the input state from the output state of the defective QFT via the nearest nontrivial peak criterion. The probability of obtaining the correct periodicity of the input state according to this procedure is denoted by $P^{(\lambda)}(\epsilon)$, where $\lambda$ stands for the label of the corresponding type of static defect, i.e., RC, RU, AC, or AU. From $P^{(\lambda)}(\epsilon)$ we construct our performance measure $P^{(\lambda)}(\epsilon)$ as the normalized probability

$$
P^{(\lambda)}(\epsilon) = \frac{P^{(\lambda)}(\epsilon)}{P^{(\lambda)}(\epsilon = 0)}.
$$

(10)

Numerical results for static defects of types RC and RU are shown in Fig. 2. As expected, the performance $P$ of the QFT starts at $P = 1$ for $\epsilon = 0$ and decreases as $\epsilon$, i.e., the strength of the defects, increases. However, surprisingly, in both cases, RC and RU, the QFT still performs well above the 30% level even at $\epsilon = 1$.

For $\epsilon < 0.5$ there is hardly any difference between $P^{(\text{RC})}(\epsilon)$ and $P^{(\text{RU})}(\epsilon)$. Fitting a Gaussian to $P^{(\text{RC, RU})}(\epsilon)$ in this region, we obtain

$$
P^{(\text{RC, RU})}(\epsilon) \approx e^{-\epsilon^2},
$$

(11)

which is accurate to within 4% up to $\epsilon \approx 0.7$ for RC and up to $\epsilon \approx 1.1$ for RU [see Fig. 2(a)]. As shown in Fig. 3, a similar behavior is observed for AC and AU types of static defects, although the Gaussian fitted to the performance data is now a little narrower than in the RC and RU cases, indicating larger sensitivity to defects. Explicitly, we obtain

$$
P^{(\text{AC, AU})}(\epsilon) \approx e^{-\epsilon^2/0.65},
$$

(12)

which, for $\epsilon$ up to $\epsilon \approx 0.7$, is accurate to within 5% for AC and 3% for AU [see Fig. 3(a)].

In order to better present the asymptotic behavior of the performance scaling in $\epsilon$, we show log-log plots of the performance of the four types of defects in Figs. 2(b) and 3(b) for the relative and the absolute defect types, respectively. We observe that all four types of defects result in

$$
P \approx 0.039,
$$

(13)

shown as the horizontal dashed lines in Figs. 2(b) and 3(b). The explanation for the asymptotic behavior and the specific numerical quantity will be provided in detail (analytically) in Sec. III A.

The QFT is more susceptible to absolute-type defects because the accumulated defect phase angle is much larger for the absolute type of defects than the corresponding ones...
were performed for QFTs with the \( H_{\text{CROT}} \) introduced according to (9). Still, the robustness of the QFT circuit is apparent in that, reminiscent of RC and RU, the performance level is above 25% for both AC and AU up to \( \epsilon \lesssim 1 \).

### B. \texttt{CROT} gates exact; \texttt{H} gates defective

So far we have investigated the effects of various kinds of static defects in the \texttt{CROT} gates, keeping the \texttt{H} gates exact. In this section we investigate how static defects in the Hadamard gates influence the performance of the QFT while keeping the \texttt{CROT} gates exact.

An exact Hadamard gate performs the following quantum operation:

\[
\hat{H}(t) = \begin{cases} 
\frac{|0\rangle + |1\rangle}{\sqrt{2}}, & \text{if } |t\rangle = |0\rangle, \\
\frac{|0\rangle - |1\rangle}{\sqrt{2}}, & \text{if } |t\rangle = |1\rangle.
\end{cases}
\]

(14)

A modified Hadamard gate \( \hat{H}_\alpha \) is obtained by introducing static defects into the Hadamard gate in the following way:

\[
\hat{H}_\alpha(t) = \begin{cases} 
\sin \left( \frac{\pi}{4} + \alpha \right) |0\rangle + \cos \left( \frac{\pi}{4} + \alpha \right) |1\rangle, & \text{if } |t\rangle = |0\rangle, \\
\cos \left( \frac{\pi}{4} + \alpha \right) |0\rangle - \sin \left( \frac{\pi}{4} + \alpha \right) |1\rangle, & \text{if } |t\rangle = |1\rangle,
\end{cases}
\]

(15)

where, for a given \( \texttt{H} \) gate,

\[
\alpha = \epsilon r.
\]

(16)

Here, as in Sec. II A, \( \epsilon > 0 \) controls the size of the defect and \( r \) is uniformly distributed in \([-1, 1]\).

As in the case of the \texttt{CROT} gates, the modified Hadamard gates may also have correlated and uncorrelated defects. If all Hadamard gates in the QFT circuit have the same static defect throughout the entire circuit, we call this a correlated defect (HC), whereas if each given Hadamard gate in the QFT circuit has its own specific defect, independent of all the other \( \texttt{H} \) gates, we call this an uncorrelated defect (HU). Figure 4 shows the numerical results of the normalized performance \( P \) of the ten-qubit QFT as a function of \( \epsilon \) for both HC (triangles) and HU (crosses) type defects.

As in the case of \texttt{CROT} defects (see Sec. II A), the case of defective Hadamard gates also demonstrates extraordinary robustness of the QFT circuit: as seen in Fig. 4, the performance level is above 40% (25%) for correlated (uncorrelated) Hadamard defects for \( \epsilon \) as large as \( \epsilon = 0.7 \). Fitting the data in Fig. 4 for \( \epsilon \lesssim 1 \), we obtain

\[
P^{(\text{HC})} \approx e^{-\epsilon^2/0.33}.
\]

(17)

The fit is accurate within 6% for HC and 2% for HU for \( \epsilon \) up to \( \epsilon \lesssim 0.4 \). In the large-\( \epsilon \) limit, we obtain two different tail behaviors. In the correlated case the performance converges to

\[
P \approx 0.22,
\]

(18)

while in the uncorrelated case we obtain

\[
P \approx 0.039.
\]

(19)

The two lines (18) and (19) are shown in Fig. 4(b) as horizontal dashed lines. The explanation for the two asymptotic behaviors will be provided in detail (analytically) in Sec. III B.

### C. Both \texttt{H} gates and \texttt{CROT} gates defective

While Secs. II A and II B focus on cases in which only one type of gates (\texttt{CROT} or \texttt{H}, but not both) are defective and the other is treated exactly, we study, in this section, a case in which both types of gates are defective simultaneously. Obviously an enormous number of combinations of different types of defects may be imagined, too numerous to study them all. Instead, we make our point by presenting a case in which the QFT, despite the fact that both the \texttt{CROT} defects and the \texttt{H} defects are large, nevertheless performs surprisingly well. Selecting the “worst case scenario” for each type of gates, i.e., AU-type defects for the \texttt{CROT} gates and HU defects for the Hadamard gates, we see that, surprisingly, even with \( \epsilon \approx 0.4 \), the QFT still performs above the 50% level (see Fig. 5). The fit curve in this case is

\[
P(\epsilon) \approx e^{-\epsilon^2/0.22}.
\]

(20)
QFTs with large-dashed line in (b) are the approximate, large-$\epsilon$, asymptotic performance of the QFT with HC type of defects (18). The bottom dashed line in (b) is the approximate, large-$\epsilon$, asymptotic performance of the QFT with HU type of defects (19). The numerical calculations were performed for QFTs with $n = 10$ qubits.

III. ANALYTICAL ANALYSIS SUPPORTING THE NUMERICAL RESULTS

In the previous section we showed numerically that the QFT is robust with respect to static defects introduced in the $H$ and CROT gates. Despite the promising robustness we found throughout Sec. II, however, these results were obtained for a relatively small number of qubits and, while these results are a strong indication, it is not clear whether the robustness persists if we increase the number of qubits, say to a few thousand, the simulation of which is far beyond any classical computer, present or future [12,16], but is a number of qubits of practical interest, e.g., for code breaking [19,13]. Furthermore, at this point, we do not know whether the heuristic Gaussian $\epsilon$ scaling found in (11), (12), and (17) is indeed universal or how the numerically determined constants in (11), (12), and (17) scale in $n$. To answer these questions, we derive, in this section, analytical expressions for the performance scaling of the QFT circuit as a function of the number of qubits $n$ and the strength $\epsilon$ of the static defects. The analytical work in this section supports, and is consistent with, the numerical results obtained in Sec. II. The analytical results also allow us to extrapolate into the large-$n$ regime, inaccessible to numerical simulation. But most importantly, the analytical results confirm the trend discovered numerically at low $n$, i.e., that the QFT tolerates surprisingly large static defects and still performs satisfactorily.

A. CROT defects

In this section we focus on the analytical calculation of the effects of static defects introduced in the CROT gates on the performance of the QFT. First, we investigate how static defects in the CROT gates affect the performance of the QFT in general. Then, we derive the defect-specific analytical expressions that show the effects of the four different types of static defects (RC, RU, AC, AU) introduced in the CROT gates. Finally, we statistically analyze our analytical expressions to obtain the performance scaling of the QFT circuits subjected to the four types of static defects in the CROT gates.

The $n$-qubit QFT $|a\rangle$ of an $n$-qubit integer state $|a\rangle$ is defined as the sum

$$|a\rangle = \frac{1}{\sqrt{2^n}} \sum_{b=0}^{2^n-1} \Phi(a,b)|b\rangle$$

over all $n$-qubit integer states $|b\rangle$, where

$$\Phi(a,b) = \exp(2\pi i a b/2^n).$$

Defining $a_{\nu,1}$ and $b_{\mu,1}$ as the $\nu$th and $\mu$th binary digit of $a$ and $b$, respectively, we may write (22) in the form

$$\Phi(a,b) = \prod_{\nu=0}^{n-1} \prod_{\mu=0}^{\nu-1} \exp\left(i\pi a_{\nu-\nu-j-1} b_{\mu}/2^n\right).$$
Instead of using a pure integer state $|a\rangle$ as the input of the QFT, we now consider input states $|\psi_j\rangle$, which have a period $\omega$. If $2^n > \omega$, there are $\omega$ different $\omega$-periodic $n$-qubit input states $|\psi_j\rangle$. We write them in the form

$$|\psi_{s0}(i)\rangle = \sum_{k=0}^{K(s0) - 1} \frac{1}{\sqrt{K(s0)}} |s0 + k\omega\rangle,$$  \hspace{1cm} (24)

where $0 \leq s0 \leq \omega - 1$ labels a particular input state $|\psi_j\rangle$ in the set of $\omega$ possibilities, and $K(s0)$ is the number of full periods $k\omega$ contained in $[0, 2^n - 1]$. We see that $|\psi_{s0}(i)\rangle$ defined in (24) is a superposition of integer input states. Therefore, if we compute the QFT of (24), the phase $\Phi_{s0,a}(b)$ of a selected output state $|b\rangle$ of the QFT is a superposition of phases $\Phi(s0 + k\omega, b)$ (see (21) and (22)), given explicitly by

$$\Phi_{s0,a}(b) = \sum_{k=0}^{K(s0) - 1} \frac{1}{\sqrt{K(s0)}} \Phi(s0 + k\omega, b).$$  \hspace{1cm} (25)

If now the selected output state $|b\rangle$ is to have a large amplitude, i.e., $b$ is one of the likely outputs after applying the QFT to an $\omega$-periodic input state, the terms in the sum in (25) should cluster, i.e., the possible $\Phi(s0 + k\omega, b)$ for different $k$ values should effectively form a set whose elements’ phase angles are close to one another. In fact, if $\omega$ is a power of 2, for any $b$ that is an integer multiple of $2^n/\omega$, $\Phi$ becomes single valued, i.e., the number of elements in the set is 1. Therefore, the probability density of the phase angles $\Phi(s0 + k\omega, b)$ may be written with the help of a sum over Dirac $\delta$ peaks, i.e.,

$$\Phi_{s0,a}(b) = \sum_{\kappa=0}^{N-1} \sum_{\kappa=0}^{N-1} v(\kappa) v(\kappa') \frac{1}{\sum_{\kappa=0}^{N-1} v(\kappa')} d\theta d\theta' \sum_{\kappa=0}^{N-1} v(\kappa'),$$  \hspace{1cm} (26)

where $\theta(\kappa)$ is the phase angle of the $\kappa$th element of the set of possible values $\Phi(s0 + k\omega, b)$, $v(\kappa)$ is the multiplicity of the $\kappa$th element, i.e., the number of different $\kappa$ values that corresponds to the $\kappa$th element of the set, and $N$ is the number of elements of the set. In other words, those output states $|b\rangle$ with large amplitudes tend to have a relatively small $\kappa$ value or at least $\theta(\kappa)$ are closely distributed. In this view, the effect of the static defects in the CROT gates becomes apparent: the static defects deform the phase-angle distribution.

Now, introducing the four types of static defects [see (9)] into the QFT circuit, the ideal phase (23) turns into the modified phases

$$\Phi^{(RC)}(a,b) = \prod_{l=0}^{n-2} \prod_{j=1}^{n-1} \exp \left\{ j(a_{n-l-1,j}b_l - \beta\Delta^{(RC)}(l,j)) \right\};$$

$$\Phi^{(RU)}(a,b) = \prod_{l=0}^{n-2} \prod_{j=1}^{n-1} \exp \left\{ j(a_{n-l-1,j}b_l - \beta\Delta^{(RU)}(l,j)) \right\};$$

$$\Phi^{(AC)}(a,b) = \prod_{l=0}^{n-2} \prod_{j=1}^{n-1} \exp \left\{ j(a_{n-l-1,j}b_l - \beta\Delta^{(AC)}(l,j)) \right\};$$

$$\Phi^{(AU)}(a,b) = \prod_{l=0}^{n-2} \prod_{j=1}^{n-1} \exp \left\{ j(a_{n-l-1,j}b_l - \beta\Delta^{(AU)}(l,j)) \right\};$$  \hspace{1cm} (27)

where the notation $R_j$ for the correlated defects denotes the different (random) defects for the different $j$ values and the notation $R_{ij}$ for the uncorrelated defects denotes the different (random) defects for different $l$ and $j$ pairs. We note that any $R_j$ or $R_{ij}$ with $j = 0$ since such a term would correspond to a Hadamard operation, and not a CROT operation. Denoting by $\Delta$ the offset of the phase angle in (27) with respect to (23) and reversing the $l$ and $j$ sums in (27), we obtain with (5)-(8)

$$\Delta^{(RC)}(a,b) = \sum_{j=1}^{n-1} \sum_{l=0}^{n-2} a_{l} |b_{n-l-1,j} - \frac{\pi}{2} \epsilon_{l,j}^{(RC)}|;$$

$$\Delta^{(RU)}(a,b) = \sum_{j=1}^{n-1} \sum_{l=0}^{n-2} a_{l} |b_{n-l-1,j} - \frac{\pi}{2} \epsilon_{l,j}^{(RU)}|,$$  \hspace{1cm} (28)

$$\Delta^{(AC)}(a,b) = \sum_{j=1}^{n-1} \sum_{l=0}^{n-2} a_{l} |b_{n-l-1,j} - \frac{\pi}{2} \epsilon_{l,j}^{(AC)}|;$$

$$\Delta^{(AU)}(a,b) = \sum_{j=1}^{n-1} \sum_{l=0}^{n-2} a_{l} |b_{n-l-1,j} - \frac{\pi}{2} \epsilon_{l,j}^{(AU)}|,$$

which shows the cumulative effect of the four types of static defects in the CROT gates on the QFT circuit.

We now recall that the phase $\Phi^{(def)}(a,b)$ of an integer output state $|b\rangle$, after providing the $n$-qubit defective QFT with an input state in which integer states $|a\rangle$ of the form $|s0 + k\omega\rangle$ are superposed, is obtained to be [see (25) and (27)]

$$\Phi^{(def)}(b) = \frac{1}{\sqrt{K(s0)}} \sum_{a \in [s0]} \Phi^{(def)}(a,b),$$  \hspace{1cm} (29)

where the superscript (def) can be any of the four defect types, RC, RU, AC, or AU, and $[s0]$ is the equivalence class whose elements are $s0 + k\omega$ for $k = 0, 1, \ldots, K(s0) - 1$. We also note that we no longer explicitly write $s0$ and $\omega$ in the subscript of $\Phi^{(def)}(b)$. Dividing $\Phi^{(def)}(a,b)$ in (29) into two parts, the exact part from the exact part of the QFT and the random part from the defective part of the QFT, with the help of $\Delta^{(def)}$ in (28), we write

$$\Phi^{(def)}(b) = \frac{1}{\sqrt{K(s0)}} \sum_{a \in [s0]} \Phi(a,b) \Delta \Phi^{(def)}(a,b),$$  \hspace{1cm} (30)

where

$$\Delta \Phi^{(def)}(a,b) = \exp \left\{ \Delta^{(def)}(a,b) \right\},$$  \hspace{1cm} (31)

Since $\Phi(a,b)$ for the selected output state $|b\rangle$ with a large amplitude are closely distributed in its phase angle space, whereas $\Delta \Phi^{(def)}(a,b)$, the random term, fluctuates fast, we can now approximate (30) as

$$\Phi^{(def)}(b) \approx \left[ \frac{1}{\sqrt{K(s0)}} \sum_{a \in [s0]} \Phi(a,b) \right] \times \left[ \frac{1}{K(s0)} \sum_{a \in [s0]} \Delta \Phi^{(def)}(a,b) \right].$$  \hspace{1cm} (32)

Normalizing (32) with the analogous phase with the exact QFT, i.e., the first sum in (32), we obtain the figure of merit $P$.
to be approximated as
\[ P \approx \left| \frac{1}{K(s_0)} \sum_{a \in [a]} \Delta \Phi^{\text{def}}(a,b)_b \right|^2, \] (33)
where \( \langle \ldots \rangle_b \) denotes the averaging over the desired output states.

At this point, we gain an important insight from (33): the core term responsible for the performance decay is \( \langle \Delta \Phi^{\text{def}}(a,b) \rangle_b \). More specifically, since we are to add complex numbers, we are interested in how the phase angles \( \beta_{\Delta 1} \) are distributed in \( a \) around its mean phase angle \( \mu_b \). Defining
\[ \mu_b = \frac{1}{K(s_0)} \sum_{a \in [a]} \Delta^{\text{def}}(a,b), \] (34)
together with (28), we obtain the objects of our statistical analysis,
\[ \langle \Delta^{(RC)}(a,b) - \mu_b \rangle_b \]
\[ = \left( \sum_{j=1}^{n-1} \sum_{l=0}^{j-1} \left( a_{jl} - \frac{1}{K(s_0)} \sum_{a \in [a]} a_{jl} \right) b_{l,j-1} e^{\frac{\pi}{2} i \rho_{l,j}} \right)_b, \]
\[ \langle \Delta^{(RU)}(a,b) - \mu_b \rangle_b \]
\[ = \left( \sum_{j=1}^{n-1} \sum_{l=0}^{j-1} \left( a_{jl} - \frac{1}{K(s_0)} \sum_{a \in [a]} a_{jl} \right) b_{l,j-1} e^{\frac{\pi}{2} i \rho_{l,j}} \right)_b, \]
\[ \langle \Delta^{(AC)}(a,b) - \mu_b \rangle_b \]
\[ = \left( \sum_{j=1}^{n-1} \sum_{l=0}^{j-1} \left( a_{jl} - \frac{1}{K(s_0)} \sum_{a \in [a]} a_{jl} \right) b_{l,j-1} e^{\frac{\pi}{2} i \rho_{l,j}} \right)_b, \]
\[ \langle \Delta^{(AL)}(a,b) - \mu_b \rangle_b \]
\[ = \left( \sum_{j=1}^{n-1} \sum_{l=0}^{j-1} \left( a_{jl} - \frac{1}{K(s_0)} \sum_{a \in [a]} a_{jl} \right) b_{l,j-1} e^{\frac{\pi}{2} i \rho_{l,j}} \right)_b. \] (35)

We define
\[ x_l = a_{jl} - \frac{1}{K(s_0)} \sum_{a \in [a]} a_{jl}. \] (36)
Since \( a_{jl} \) reads either 0 or 1 and \( \sum_{a \in [a]} a_{jl}/K(s_0) \) is approximately 0.5 for most \( l \) values, \( x_l \) may be thought of as a random variable in \( l \) that returns either \(-0.5\) or \(0.5\). Its probability density distribution can be written as
\[ f_\sigma(x_l) = \frac{1}{2} \delta[x_l - 0.5] + \delta(x_l + 0.5)], \] (37)
where \( \delta(y) \) is the Dirac \( \delta \) function. Inserting (36) in (35), we see immediately that the terms responsible for random behavior \( \rho_{l,j}^{(\text{def})} \) are
\[ \rho_{l,j}^{(C)} = x_l \rho_{l,j}, \quad \rho_{l,j}^{(U)} = x_l \rho_{l,j}, \] (38)
where the superscripts (C) and (U) stand for correlated and uncorrelated defects. Since the random number \( r \), whether it is correlated with \( j \) only or with both \( j \) and \( l \), has the probability density distribution of
\[ f_r(v) = \begin{cases} \frac{1}{2} & \text{if } |v| \leq 1, \\ 0 & \text{otherwise,} \end{cases} \] (39)
we can now compute the probability density function of \( l_r^{(\text{def})} \),
\[ f_r(t) = \int_{-\infty}^{\infty} f_r(v) f_r(t) \frac{1}{\sqrt{2 \pi}} e^{-v^2/2} dv, \] (40)
which can be evaluated with (38) and (39) and results in
\[ f_r(t) = \begin{cases} 1 & \text{if } |t| < 1, \\ 0 & \text{otherwise.} \end{cases} \] (41)

This provides an important piece of information: there is no statistical difference between the correlated and the uncorrelated defects.

With this information in hand, we may now collapse \( \langle \Delta \Phi^{\text{def}}(a,b) \rangle_b \) expressions in (35) into
\[ \langle \Delta^{(RC)}(a,b) - \mu_b \rangle_b \]
\[ = \left( \sum_{j=1}^{n-1} \sum_{l=0}^{j-1} \left( a_{jl} - \frac{1}{K(s_0)} \sum_{a \in [a]} a_{jl} \right) b_{l,j-1} e^{\frac{\pi}{2} i \rho_{l,j}} \right)_b, \]
\[ \langle \Delta^{(RU)}(a,b) - \mu_b \rangle_b \]
\[ = \left( \sum_{j=1}^{n-1} \sum_{l=0}^{j-1} \left( a_{jl} - \frac{1}{K(s_0)} \sum_{a \in [a]} a_{jl} \right) b_{l,j-1} e^{\frac{\pi}{2} i \rho_{l,j}} \right)_b, \]
\[ \langle \Delta^{(AC)}(a,b) - \mu_b \rangle_b \]
\[ = \left( \sum_{j=1}^{n-1} \sum_{l=0}^{j-1} \left( a_{jl} - \frac{1}{K(s_0)} \sum_{a \in [a]} a_{jl} \right) b_{l,j-1} e^{\frac{\pi}{2} i \rho_{l,j}} \right)_b, \]
\[ \langle \Delta^{(AL)}(a,b) - \mu_b \rangle_b \]
\[ = \left( \sum_{j=1}^{n-1} \sum_{l=0}^{j-1} \left( a_{jl} - \frac{1}{K(s_0)} \sum_{a \in [a]} a_{jl} \right) b_{l,j-1} e^{\frac{\pi}{2} i \rho_{l,j}} \right)_b. \] (42)
Now, \( b_{l,j-1} \), averaged over many different \( b \) values, to a good approximation, is \( 1/2 \). In addition, we see that \( \rho_{l,j} \) is nothing but \( r_{l,j} \), i.e., a flat distributed random variable with the only difference being the range [see (41) and (39) for \( r_{l,j} \) and \( \rho_{l,j} \), respectively]. Hence, we may replace \( \rho_{l,j} \) in (42) with \( r_{l,j} \). Implementing the two findings in (42), we obtain
\[ \langle \Delta^{(RC)}(a,b) - \mu_b \rangle_b = \sum_{j=1}^{n-1} \sum_{l=0}^{j-1} \pi \rho_{l,j}^2 / 4, \]
\[ \langle \Delta^{(RU)}(a,b) - \mu_b \rangle_b = \sum_{j=1}^{n-1} \sum_{l=0}^{j-1} \pi \rho_{l,j}^2 / 4, \]
\[ \langle \Delta^{(AC)}(a,b) - \mu_b \rangle_b = \sum_{j=1}^{n-1} \sum_{l=0}^{j-1} \pi \rho_{l,j}^2 / 4, \]
\[ \langle \Delta^{(AL)}(a,b) - \mu_b \rangle_b = \sum_{j=1}^{n-1} \sum_{l=0}^{j-1} \pi \rho_{l,j}^2 / 4, \] (43)
which are now solely dependent on the random variable \( r_{l,j} \). At this point, we analyze the two cases in (43) individually. We start with the simpler case, absolute defects. Here, since all \( r_{l,j} \) random variables are statistically independent, the central limit theorem [17] applies. Hence, for the absolute defects, the limiting distribution function for large \( n \) converges toward a normal distribution, and, therefore, the only quantity we need to compute is its variance, since the mean, according to our construction of (43), is 0. Computing the variance for the absolute type of defects, we obtain
\[ \langle \sigma^2 \rangle^{(A)} = \frac{n(n-1)\pi^2}{96}, \] (44)
which, in the large-\( n \) limit, becomes
\[ \langle \sigma^2 \rangle^{(A)} = \frac{n^2 \pi^2}{96}. \] (45)
Replacing first the \( a \) sum in (33) with the integral over the discrete \( \delta \) function in (26) then replacing \( \langle \Delta \Phi^{(\text{def})}(a,b) \rangle_b \)
in (33) with a single complex variable $e^{\theta}$ whose phase angle distribution is now Gaussian (replacing the discrete $\delta$ functions) with the variance $\sigma^2$, we obtain, with the additional approximation of extending the integral limits to infinity, which holds whenever the variance of the Gaussian is small compared to $\pi$,

$$P^{(A)} \approx \int_{-\infty}^{+\infty} e^{\theta} G_{(a \mu_b)}(\theta) d\theta)^2,$$

where

$$G_{a \mu_b}(\theta) = \frac{1}{\sqrt{2\pi \sigma}} e^{-\theta^2/2\sigma^2}\tag{47}$$

denotes the normalized Gaussian distribution function with variance $\sigma^2$. Evaluating the integral in (46), we obtain the performance scaling of the QFT with absolute defects

$$P^{(A)} \approx \exp \left(-\frac{\pi^2 \sigma^2}{96}\right).$$

(48)

where we used $(\sigma^2)^{(A)}$ in (45).

For the relative type of defects [see (43)], we can again use the central limit theorem. The difference from the absolute case, however, is that, in the relative case, the random variables $\epsilon_{l,j}$ with the same $j$ are scaled with a factor $1/2^j$. This means we ought to use the central limit theorem for the $l$ sum only, unlike in the case of absolute defects, where we used the theorem for both the $j$ and $l$ sums, thus approximating the relative defects distribution function as a sum (over $j$) of Gaussian functions with different variances. We note that, for large $j$, the $l$ sum may not have enough terms for the central limit theorem to be applicable. However, this is not really a problem since in this case the contribution of the $l$ sum to the distribution function will be exponentially suppressed in $j$. Rewriting the relative defect $\langle \Delta^{(R)}(a, \mu_b) \rangle$ in (43) with the help of Gaussian distributed random variables $X_j$, we obtain

$$\langle \Delta^{(R)}(a, \mu_b) \rangle \approx \sum_{j=1}^{n-1} X_j,$$

(49)

where $X_j$, with mean 0, has the variance

$$\langle \sigma^2 \rangle^{(R)} = \left( \frac{n-j}{48} \right) \left( \frac{\pi \epsilon}{2} \right)^2.$$

(50)

Since the sum of Gaussian distributed random variables results in yet another Gaussian distributed random variable with variance whose value is the sum of the variances of the individual, constituent random variables [17], we write the variance of the relative type of defects, $(\Delta^{(R)}(a, b) - \mu_b)_b$, as

$$(\sigma^2)^{(R)} = \sum_{j=1}^{n-1} (\sigma_j)^{(R)} = \frac{\pi^2 \epsilon^2}{432} (3n - 4 + 2^{n-2}).$$

(51)

Again, replacing first the $a$ sum in (33) with the integral over the discrete $\delta$ functions in (26), then replacing $(\Delta \Phi^{(R)}(a, b))_b$ in (33) with a single complex variable $e^{\theta}$ whose phase angle $\theta$ is distributed according to a Gaussian (no longer the discrete $\delta$ functions) with the variance $(\sigma^2)^{(R)}$ in (51), together with the additional approximation of extending the limits of the integral, we obtain

$$P^{(R)} \approx \int_{-\infty}^{+\infty} e^{\theta} G_{(a \mu_b)}(\theta) d\theta)^2.$$ 

(52)

Evaluating the integral (52), we obtain the performance scaling of the QFT with relative defects

$$P^{(R)} \approx \exp \left(-\frac{\pi^2 \sigma^2}{144}\right).$$

(53)

where we used $(\sigma^2)^{(R)}$ in (51) and took the large-$n$ limit, keeping the leading order in $n$ only.

The two analytical performance-scaling functions in (53) and (48) for relative (RC and RU) and absolute (AC and AU) defects, respectively, are shown in Fig. 6 as solid lines, together with the numerical data (plot symbols) and the dashed numerical fit lines imported from Figs. 2 and 3. Our analytical results are accurate up to 6%, 8%, 8%, and 9% for $\epsilon$ up to 0.5 for RC, RU, AC, and AU types, respectively.

Since the Fourier transform approximation, i.e., extending the integral limits from $-\infty$ to $+\infty$, taken to obtain (53) and
(48) are better in the small-$\epsilon$ limit, the large-$\epsilon$ limit behavior is expected to deviate from the analytical performance scaling results. In order to get a better estimate for the large-$\epsilon$ limit, we follow a different strategy. Provided with a large $\epsilon$, we expect that the probability distribution of the output states of the QFT becomes completely randomized, i.e., on average, the likelihood of obtaining any state, except for the trivial Fourier peaks that correspond to the pure power 2 factor of the periodicity, is equiprobable. Using the condition that the sum of the probabilities equals 1, assuming that the trivial Fourier peaks that correspond to the pure power 2 factor of the likelihood of obtaining any state, except for the trivial Fourier peaks, is expected to deviate from the analytical performance scaling results. In order to get a better estimate for the large-$\epsilon$ limit, we follow a different strategy. Provided with a large $\epsilon$, we expect that the probability distribution of the output states of the QFT becomes completely randomized, i.e., on average, the likelihood of obtaining any state, except for the trivial Fourier peaks that correspond to the pure power 2 factor of the periodicity, is equiprobable. Using the condition that the sum of the probabilities equals 1, assuming that the trivial Fourier peaks that correspond to the pure power 2 factor of the periodicity, is equiprobable. Using the condition that the sum of the probabilities equals 1, assuming that the trivial Fourier peaks that correspond to the pure power 2 factor of the periodicity, is equiprobable.

\[ \tilde{P} = C(n, \omega) \times \frac{1}{2^n} \]

where $C(n, \omega)$ is the number of useful states in determining the periodicity of the input states, given $n$, the number of qubits, and $\omega$, the periodicity of the input states. Since the criterion of success in this paper is to include those states that are nearest to the supposed Fourier peaks apart from the trivial ones (power 2 corresponding peaks), with $n = 10$ and $\omega = 30$, the expected absolute success probability $\tilde{P}$ becomes

\[ \tilde{P}(n = 10, \omega = 30) = C(n = 10, \omega = 30) \times \frac{1}{2^{30}} \approx 0.0273, \]

which perfectly matches the horizontal dashed lines in Figs. 2(b) and 3(b).

### B. Hadamard defects

Unlike the defects in the CNOT gates, the defects in the Hadamard gates [see (15)] do not change the phase-angle distribution. In fact, the phase angle $\theta$ of $\Phi(s_0 + k_0, b, 0)$ remains fixed for any input state $|s_0 + k_0, b\rangle$ when the QFT is subjected to the static defects in the Hadamard gates. Upon introduction of the defects $\alpha$ [see (15)], only the amplitude of $\Phi(s_0 + k_0, b, 0)$, i.e., the modulus of $\Phi(s_0 + k_0, b, 0)$, is changing. With (15), the modified phase $\Phi^{(H)}(a, b)$ of the Hadamard gates is

\[ \Phi^{(H)}(a, b) = \prod_{k=0}^{n-1} A_k(a) \prod_{j=0}^{n-1} \exp \left( i \alpha a_{[n-1-i]j} b_{[j]} \right), \]

where

\[ A_k(a) = \begin{cases} 
\sqrt{2} \sin \left( \frac{\pi}{4} + a \right) & \text{if } a_{[n-1-i]} = b_{[j]}, \\
\sqrt{2} \cos \left( \frac{\pi}{4} + a \right) & \text{if } a_{[n-1-i]} \neq b_{[j]}, \end{cases} \]

Since the second product in (58) is over $j$ for fixed $i$, we may assume that this product is approximately statistically independent of each of the $A_i(a)$ in (58). In this case we can compute the state average over $A_i(a)$ and the product separately, and arrive at

\[ \hat{A} = \sum_{A=1}^{n-1} A \left( A(a), n, b \right) \prod_{i=0}^{n-1} \exp \left( i \alpha a_{[n-1-i]} b_{[j]} \right). \]

(60)

We now evaluate $\sum_{A=1}^{n-1} A \left( A(a), n, b \right)$ in the case of correlated defects, i.e., the case in which $\alpha$ is fixed for all $l$ values in (59). Assuming that $0's$ and $1's$ occur with equal probability in $a_{[n-1]}$ and $b_{[j]}$, we obtain

\[ \langle A^C \rangle_{a,b} = \left[ \sqrt{2} \sin \left( \frac{\pi}{4} + a \right) \right] \left[ \sqrt{2} \cos \left( \frac{\pi}{4} + a \right) \right]^{n/2}, \]

(61)

where, in order to avoid complications with signs, we have also assumed $|a| < \pi/4$. For $|a| > \pi/4$ will be discussed later. Turning now to the case of uncorrelated defects, i.e., the case in which we have a random $\alpha$ for each $l$ as in (60), we obtain

\[ \langle A^C \rangle_{a,b} = \sum_{A=1}^{n-1} \prod_{l=0}^{n-1} \left( \sqrt{2} \sin \left( \frac{\pi}{4} + a_l \right) \right), \]

(62)

Here, the subscript $l$ of $\alpha$ denotes the different $\alpha$ values for the different $l$ values. We note that because of the statistically identical nature of the two cases $\sin \left( \frac{\pi}{4} + a \right)$ and $\cos \left( \frac{\pi}{4} + a \right)$ in (60), which arises from the evenness of the $\alpha$ distribution [see (16)], we chose $\sin \left( \frac{\pi}{4} + a \right)$ to represent both the sine and cosine factors. We also note that, here [see (61) and (62)] and in the following, we suppress the argument(s) $\alpha (a_l)$ of $A^C(\alpha) \left[ A^C(\alpha) \right]$. Evaluating the product in terms of a sum over logarithms, we obtain

\[ \langle A^C \rangle_{a,b} \approx \exp \left( \sum_{l=0}^{n-1} \ln \left( \sin \left( \frac{\pi}{4} + 2a_l \right) \right) \right), \]

(63)

\[ \langle A^U \rangle_{a,b} \approx \exp \left( \sum_{l=0}^{n-1} \ln \left( \sqrt{2} \sin \left( \frac{\pi}{4} + a_l \right) \right) \right), \]

which, together with the ensemble average over $\alpha$, may be approximated with the help of an integral approximation of the sum as

\[ \langle A^C \rangle_{a,b} \approx \exp \left( \frac{n}{2\pi} \int_{-\pi}^{\pi} \ln \left( \sin \left( \frac{\pi}{4} + 2a \right) \right) da \right), \]

(64)

\[ \langle A^U \rangle_{a,b} \approx \exp \left( \frac{n}{2\pi} \int_{-\pi}^{\pi} \ln \left( \sqrt{2} \sin \left( \frac{\pi}{4} + a \right) \right) da \right). \]

Although the integrals in (64) may be performed exactly, in the limit where $\epsilon$ is small, we can replace the integrands with their leading Taylor expansion terms. The replacement results in

\[ A^C \approx A^U \approx \exp \left( \frac{n}{2\pi} \int_{-\pi}^{\pi} (-\alpha^2) da \right). \]

(65)
where both $A^{(C)}$ and $A^{(U)}$ now have the same integrand. Solving the integral in the exponent of (65) and using the result in (58), we obtain the ratio of the modified phase (58) to the ideal phase (23) in the form

$$\frac{\phi^{(H)}}{\phi^{(M)}} = \exp \left( -\frac{ne^2}{2} \right).$$

Taking the absolute square, we obtain the desired performance scaling result

$$P^{(H)} \approx \exp \left( -\frac{2ne^2}{3} \right).$$

This result is shown as the solid line in Fig. 7, which also shows the numerical performance results as a function of $\epsilon$ for both HC (triangles) and HU (crosses). For the convenience of the reader the numerical results were imported into Fig. 7 from Fig. 4 and are identical to the numerical results in Fig. 4. We see that, as predicted by the analytical result (65), the HC data and the HU data are indeed nearly identical in the small-$\epsilon$ regime. While (65) successfully predicts this feature of the performance data, the performance according to the numerical simulation is actually better than the expected analytical prediction (67). In more quantitative terms, the prefactor of the $e^2$ term in the exponent of (67) is $\approx 20/3 \approx 6.7$, while the prefactor of the $e^2$ term in the numerical fit function (17) is $\approx 3$, i.e., about a factor 2 difference, accounting for the better than expected performance of the QFT with HC or HU defects.

We now turn to the case $|\alpha| > \pi/4$, which is the regime of large $\epsilon$, and first focus on the HU case, i.e., the case where the defect size $\alpha$ is different for each of the $n$ Hadamard gates in the QFT circuit. In this case and in the large-$\epsilon$ limit, we expect well-mixing of amplitudes, a situation similar to that of the QFT circuit subjected to static defects in the CROT gates. Therefore, in this case, $P^{(H)} \approx 0.039$ in the large-$\epsilon$ limit, as predicted by (57). $P^{(H)} \approx 0.039$ is shown as the lower dashed line in Fig. 4. We see that it is an excellent fit to the numerical data in the large-$\epsilon$ regime. Incidentally we note that in this case the analytical prediction (57) and the numerical fit (19) agree perfectly.

Turning now to the HC case, we note that in the large-$\epsilon$ regime the HC case behaves quite differently from the HU case and any of the CROT cases. This is so since in the HC case the defects of the Hadamard gates are the same across the entire QFT circuit, which does not result in well-mixing of amplitudes, but instead, according to (65), results in a periodic structure of the probability spectrum in $\alpha$ with periodicity $\pi$. Approximating the shape of the unit cell of the periodic structure in the probability spectrum with a Gaussian, as found in (67), we now expect the large-$\epsilon$ limit performance of the QFT circuit subjected to correlated static defects in the Hadamard gates to be the average value of the performance of the unit cell. Evaluating the normalized average value, we obtain the expected performance in the large-$\epsilon$ limit as

$$P \approx \frac{1}{\pi} \int_{-\pi/2}^{\pi/2} e^{-2n\epsilon^2/3} d\epsilon \approx \frac{1}{\pi} \int_{-\infty}^{\infty} e^{-2n\epsilon^2/3} d\epsilon = \sqrt{\frac{3}{2n\pi}}.$$  

For our sample case $n = 10$, the limit in (68) evaluates to

$$P(n = 10) \approx 0.22,$$

which, together with the large-$\epsilon$ limit 0.039 in the uncorrelated case [see (57)], match the fit lines (18) and (19) perfectly (see Fig. 4). The reasons for why the analytical fit (67) is not as good as the corresponding analytical fits in the case of the CROT defects may be the following. First of all, the ensemble averages taken in (61) and (62) are not exact when compared to the actual numerical values. The averages assume the occurrence of the same number of sines and cosines in (59), i.e., a 50-50 chance of obtaining either the same or a different input digit $a_j$, and output digit $h_j$. However, the numerical investigation shows that this is not the case. This observed imbalance results in fluctuations in the exponent of the performance formula (67), which are significant. Another reason may be the use of the integral approximation. Since the approximation is taken in the exponent part of the performance, the difference between the summations in (63) and the integrals in (64) has a noticeable effect and results in a significant difference between the numerical data and the analytical approximation. In the large-$n$ limit, however, this deviation becomes relatively small. Yet another source of discrepancy may be the second-order Taylor series approximation (65). However, the numerical evaluation of the integrals in the exponents of (64) shows that it deviates from that of (65) by only 4%.

IV. DISCUSSION

Even a single gate error is potentially fatal in a conventional, digital information processor. This is the reason for the stringent quality controls in the semiconductor industry, which accepts only perfect chips. In 1998, challenging this paradigm, scientists at Hewlett-Packard Laboratories built Teramac, an experimental, classical computer, consisting of a mixture of working and defective semiconductor chips [18]. Although Teramac’s chips contained about 220 000 hardware defects, the
Appendix A. List of Publications

ROBUSTNESS OF THE QUANTUM FOURIER TRANSFORM . . . PHYSICAL REVIEW A 89, 042337 (2014)

machine performed perfectly, and for some tasks outclassed then high-end workstations by a factor of 100 [18]. Teramac achieved this degree of defect tolerance based on its novel hardware architecture, together with special software that allowed the computer, after an initial self-diagnosis step, to circumvent defective components. While this is an important step forward in classical computing, and may come in handy in future, error-prone, chemically self-assembled molecular computers [18,19], a specific quantum circuit, the QFT, as shown in this paper, works quite differently. Instead of the need to circumvent defective gates, perhaps making use of some specialized quantum compensation software, the QFT can literally tolerate defective gates, working with acceptable performance even if the gates operate well off specifications, or are even missing [9,12,20,21]. This is explained qualitatively by the fact that quantum information processors are hybrids achieved this degree of defect tolerance based on its novel hardware architecture, together with special software that needs to circumvent defective gates, perhaps making use of some specialized quantum compensation software, the QFT can literally tolerate defective gates, working with acceptable performance even if the gates operate well off specifications, or are even missing [9,12,20,21]. This is explained qualitatively by the fact quantum information processors are hybrids.

CROT

We turn now to focus on four types of static defects for the CROT gates and H gates actually present in a quantum circuit. As an especially important sample circuit we focus on the QFT, since it is the core quantum subroutine of many important quantum algorithms, such as Shor’s algorithm [1,4,13], and others [2,3,5,6]. Globally, we find a surprising robustness of the QFT with respect to gate defects, defects that may be so random that the respective gate operation is effectively random. More specifically, we obtained the following results.

Of the enormous number and combinations of static defects that may arise in the manufacturing process and/or the operation of the CROT and H gates of the QFT circuit, we chose to focus on four types of static defects for the CROT gates [RC, RU, AC, and AU (see Sec. II A)] and two types of static defects for the H gates [HC and HU (see Sec. II B)]. There are also any number of ways the performance of the QFT circuit subjected to static defects can be characterized. We chose as our performance measure the success probability of running the QFT supplemented with the nearest nontrivial peak banding. This provides us with the ability to check our analytical predictions. The most interesting feature revealed by our analytical results is that in all cases studied (RC, RU, AC, AU, HC, and HU), the performance $P$ has the form

\[ P \sim \exp(-\gamma n^\beta \epsilon^2), \]

where $\gamma$ is a constant and $\beta$ is either 1 or 2. This result has an immediate consequence: It means that even if we need $n \sim 1000$, as required for code breaking applications [1,13], in the worst case, i.e., for $\beta = 2$, we need only to keep $\epsilon$ below $\epsilon \sim 1/n \sim 10^{-3}$, to achieve acceptable QFT performance. This condition does not seem too stringent and seems manageable technologically.

However, the situation is even more promising than that. This is so, since $\beta = 2$ corresponds to the absolute case, the case in which we assume the presence of an absolute error for all gates in the circuit. In this case, the absolute error $\epsilon$ needs to be compared with the nominal gate rotation angle $\pi/2^j$. As soon as, for increasing $j$, we have $\epsilon = \pi/2^j$ for some $j_0$, i.e., $j_0 = \ln(\pi/\epsilon) / \ln(2)$, then, for all $j > j_0$, the respective $j$ gates will be completely swamped by the absolute error $\epsilon$, turning all $j$ gates with $j > j_0$ into random gates. Astonishingly, although in this case we are running the QFT circuit in a mode where most of the gates operate as completely random gates (the number of swamped gates scales like $n^2$, while there is only a total of $\sim n^2$ gates), the QFT circuit still performs well if $\epsilon \lesssim 1/n$. This insight also suggests a course of action: It seems that eliminating the swamped gates entirely from the QFT circuit might result in better performance of the QFT circuit than in the presence of these gates. This is actually true. It is so, since the large exponent $\beta = 2$, in both cases with absolute defects, is generated by summing over the swamped gates. Therefore, cutting these gates will actually lower the $\beta$ exponent, resulting in more favorable $n$-scaling behavior. In fact, cutting the swamped gates is equivalent to banding the QFT circuit [12,20]. This implies that for satisfactory QFT performance, even in the defect-free case, these gates do not have to be present in the first place, and adding them into the circuit in the presence of absolute-type defects will just turn them into conduits, whose only purpose would be to downgrade the performance of the circuit by channelling errors into it. So, eliminating these gates from the circuit right from the start is by far the better choice.

An actual manufacturing process will most likely introduce defects not according to the two models of absolute defects (AC and AU), but will again like in results in relative type defects, modeled by our cases RC and RU. In these cases, e.g., we have $P^{\text{RU}} \propto \exp(-\pi^2 n^2 \epsilon^2/144)$ [see (53)], which implies that even at $n = 1000$, we can afford defects as large as $\epsilon \sim [144/(\pi^2 \times 1000)]^{1/2} \sim 0.12$, i.e., gate defects of the order of 10% still yield acceptable QFT performance.

The situation is similar for the H gates, whose performance is $P^{\text{HU}} \propto \exp(-2n\epsilon^2/3)$ [see (67)], which has a $\epsilon \sim 1/n^{3/2}$ scaling. In particular, for $n = 1000$, $\epsilon \sim (3/2000)^{1/2} \sim 0.04$, i.e., defects on the order of 4% may be tolerated in this case.

Although we can never simulate a $n \sim 1000$ qubit quantum computer on a classical computer, we can still simulate up to $n \sim 20$ on a classical computer with modern hardware. This provides us with the ability to check our analytical $n$-scaling predictions. In Fig. 8 we plot the performance of the QFT subjected to the four defects (RC, RU, AC, and AU) as a function of $n$, while fixing the defect size at $\epsilon = 0.2$. As predicted by our analytical calculations, the RC and RU cases [Fig. 8(a)] scale in $n$ with $\beta = 1$ [see (53) and (70)], while the AC and AU cases [Fig. 8(b)] scale in $n$ with $\beta = 2$ [see (48) and (70)]. The dashed lines in Figs. 8(a) and 8(b) are our analytical results (53) and (48), respectively.

Since the specific way of plotting our data in Fig. 8 is much more sensitive to the details of our analytical predictions than the plots in Figs. 2 and 3, we also show the solid lines in Fig. 8, which are obtained in the following way. In Sec. III A, we have shown analytically that the performance scaling functions are of the form

\[ P \sim e^{-\gamma}, \]
where $\sigma^2$ are the variances of the defective phase angles $\Delta$ in (27). To compensate for residual correlations responsible for the deviations between the analytical performance scaling functions and the simulation data (correlations are suppressed in our analytical calculations), we compute the variances numerically. Since we have shown analytically that the variances $\sigma^2$ scale linearly or quadratically in $n$ for relative or absolute defects, respectively, we may compute the coefficients $\gamma$ of the $n$-dependent terms in the variances $\sigma^2$ [see (70) and (71)] from the numerically obtained variances with a fixed defect strength $\epsilon = 0.2$. Although different $n$ values result in slightly different $\gamma$ values, we choose $n = 10$ as our proxy number of qubits, since, according to our analytical calculations, these $\gamma$ values are supposed to be independent of $n$. In addition, since both relative and absolute defects contain the cases of correlated and uncorrelated defects, to take the differences in numerically obtained $\gamma$ values for the correlated and uncorrelated cases into account, we take the average of the two corresponding $\gamma$ values, i.e., one from the correlated and the other from the uncorrelated defects, as the representative $\gamma$ value, for both relative and absolute defects. The solid lines in Figs. 8(a) and 8(b) are then $\gamma e^{\epsilon n^2}$ with the representative $\gamma$ obtained as described above, $\epsilon = 0.2$, and $\beta = 1$ or 2 for relative or absolute defects, respectively. We observe that, with the residual correlations taken into account, the fit between the solid lines and the simulation data is nearly perfect. The purpose of the dotted lines in Figs. 8(a) and 8(b) with slopes $\beta = 1$ and $\beta = 2$, respectively, is to guide the eye and to prove that the numerical data indeed follow the analytical $n$-scaling predictions.

If the performance of the QFT circuit is so insensitive to the precise actions of individual gates, what are the essential features of the QFT circuit that determine its function? We found that while precise gate operation is a secondary issue, the most important features of the QFT circuit are control and hierarchy. Removing the control from the QFT circuit (see Fig. 1), i.e., turning all CROT gates into single-qubit RY gates, turns the QFT circuit into a random-number generator, since any input state $|\alpha\rangle$, irrespective of the value of the integer $a$, produces a superposition state $|b\rangle$ as an output state that contains any integer state between 0 and $2^n - 1$ with equal probability. It is exactly this control element in the QFT circuit that channels the massively parallel quantum computation into the desired output state by making essential use of quantum interference. Thus, removing the control results in nothing more than an illustration of how massive parallelism without interference results in randomness [1,13].

While for large defect size $\epsilon$ some, or even most, of the CROT gates are turned into random gates, there are always some gates left that preserve the hierarchy of the CROT gates, i.e., their respective rotation angles are $\rho/2^j$, where $\rho > 0$ is random, but smaller than $2\pi 2^j$. We checked that if $\rho > 2\pi 2^j$, i.e., all CROT angles are random modulo $2\pi$, the QFT ceases to work. This means that it is permitted to replace $\pi$ in $\pi/2^j$ by a random number, but it needs to be small enough to preserve the hierarchical ordering of rotation angles for $j < b$, where $b \approx 8$ is the banding cutoff [12,20]. Therefore, we conclude that the hierarchical ordering of the QFT circuit is more important than the precise values of its rotation angles.

V. SUMMARY AND CONCLUSION

Answering Landauer’s question concerning the importance of manufacturing defects in the production of quantum hardware on quantum circuit performance [22,23], the central result of this work is that the QFT circuit, e.g., does not have to be implemented precisely in order to work. This is supported by a related result shown previously [9,12,20,21]: Some gates may be pruned from the QFT circuit entirely without significantly impairing the functioning of the circuit. We showed in this paper that not even the remaining gates have to be implemented precisely in order to work. This is demonstrated this by explicit quantum simulations of the QFT circuit supplemented with analytical results—how large the gate defects may actually be that still allow the QFT circuit to work with acceptable performance. However, different parts of
the circuit react with different sensitivity to changes (defects) in the circuit. We find that it is most important to preserve the hierarchy and the control nodes of the circuit. Both the hierarchy and the control act as the “steering elements” of the circuit, which ensure that the quantum flow of the QFT circuit is steered toward the desired results. The QFT circuit reacts least sensitively to changes in the rotation angles of the CROT gates and changes of the population transfer ratios of the H gates. In fact, we demonstrated that, preserving the hierarchy of the QFT circuit, the majority of the rotation angles of the CROT gates may be random, and the QFT circuit still works. These statements are corroborated with detailed numerical simulations backed by analytical calculations. In summary, therefore, our results motivate the following general conclusion: In the QFT circuit the structure (topology) of the circuit is more important than the precise operation of its elements, sometimes to the extent that “small, but otherwise random,” which, e.g., applies to the CROT gates in the QFT circuit, is sufficient to ensure acceptable results. This may come as good news for experimentalists and quantum engineers, who are currently embarked on manufacturing and implementing hardware components for quantum circuits.

Analytical mean-field scaling theory of radio-frequency heating in a Paul trap

Y. S. Nam, E. B. Jones, and R. Blümel
Department of Physics, Wesleyan University, Middletown, Connecticut 06459-0155, USA
(Received 2 April 2014; revised manuscript received 28 May 2014; published 2 July 2014)

While the microscopic origins of radio-frequency (rf) heating of simultaneously stored, charged particles in a Paul trap are not yet understood in detail, a universal heating curve [J. D. Tarnas, Y. S. Nam, and R. Blümel, Phys. Rev. A 88, 041401 (2013)] was recently discovered that collapses scaled rf heating data onto a single universal curve. Based on a simple analytical mean-field theory, we derive an analytical expression for the universal heating curve, which is in excellent agreement with numerical data. We find that for spherical clouds the universal curve depends only on a single scaling parameter, \( \lambda = [q(N - 1)]^{2/3}/T \), where \( N \) is the number of trapped particles, \( q \) is the Paul-trap control parameter, and \( T \) is the temperature.

DOI: 10.1103/PhysRevA.90.013402

I. INTRODUCTION

Ever since the invention of the Paul trap in the 1950s [1], now used worldwide in scores of laboratories for applications ranging from ultrahigh accuracy atomic clocks [2] to quantum computers [3], experimentalists observed a curious phenomenon of ensembles of charged particles simultaneously stored in a Paul trap: radio-frequency (rf) heating [4–6]. Cooling in various forms, e.g., laser cooling [7] or buffer-gas cooling [8], has to be applied to counteract this heating phenomenon. While at this point in time we cannot yet predict rf heating rates as a function of particle number and trap parameters, we are able to offer an ordering principle, a universal curve [9], onto which scaled rf heating rates of stable, trapped particle clouds collapse. While in [9], based on extensive numerical simulation data, the heating curve was discovered phenomenologically, the purpose of this paper is to reveal the physical origin of the universal curve and derive analytically the scaling relationships that underlie the near-exact collapse of heating data onto the universal curve. Thus derivation and analytical investigation of this universal curve is the main objective of this paper.

Our paper is structured in the following way. In Sec. II, we summarize the most important Paul-trap equations and introduce the notation. In Sec. III, based on an analytical mean-field theory, we derive the general form of the universal heating curve, further developing the general expression obtained in Sec. III, we derive, in Sec. IV, an explicit, analytical expression for the universal heating curve and compare it with numerical data. We find that the agreement is excellent. In Sec. V, we uncover an as yet hidden symmetry that explains why the universal curve is also universal in the Paul-trap \( q \) parameter. Thus we are able to show that for spherical clouds the universal curve depends only on a single scaling parameter, \( \lambda = [q(N - 1)]^{2/3}/T \), where \( N \) is the number of trapped particles, \( q \) is the Paul-trap control parameter, and \( T \) is the temperature of the cloud. This result is based on the mean-field theory developed in Sec. III, which rests on several assumptions and numerical observations, discussed and justified in detail in Sec. VI. In Sec. VII we summarize and conclude our paper.

II. PAUL-TRAP EQUATIONS

We start by briefly summarizing the most important Paul-trap equations [1,10,11], which also introduce and define the notation [9]. In dimensionless units, the coupled set of nonlinear Paul-trap equations is

\[
\ddot{r}_i + \gamma \dot{r}_i + \left[ a - 2q \sin(2\pi r) \right] \left( \frac{x_i}{r_i^3} - \frac{2y_i}{r_i^5} \right) = \sum_{j=1, j \neq i}^{N} \frac{\vec{r}_i - \vec{r}_j}{|\vec{r}_i - \vec{r}_j|^3}, \quad i = 1, \ldots, N,
\]

where \( \vec{r}_i = (x_i, y_i, z_i) \) is the position of the \( i \)th trapped particle, \( a \) and \( q \) are the dimensionless Paul-trap control parameters, and \( t \) is the dimensionless time. The set of equations (1) completely defines the damped dynamics of \( N \) particles in an ideal Paul trap and contains all the relevant physics of the heating problem. We also define the second moments \( s_2^2, s_3^2, \) and \( s_4^2 \), where \( s_2^2 \), e.g., is given by \( s_2^2 = \sum_{i=1}^{N} x_i^2 \), and analogously for the other two moments. In addition, we define \( s^2 = s_2^2 + s_3^2 + s_4^2 \). The total instantaneous energy of the set of particles described by (1) is

\[
E(t) = E_{\text{kin}}(t) + E_{\text{sup}}(t) + E_{\text{cool}}(t),
\]

where

\[
E_{\text{kin}}(t) = \frac{1}{2} \sum_{i=1}^{N} \dot{r}_i^2,
\]

\[
E_{\text{sup}}(t) = \frac{1}{2} [a - 2q \sin(2\pi r)] (s_2^2 + s_3^2 + s_4^2),
\]

and

\[
E_{\text{cool}}(t) = \frac{1}{2} \sum_{i,j=1, i \neq j}^{N} \frac{1}{|\vec{r}_i - \vec{r}_j|^3}.
\]

Heating and cooling of the particles governed by (1) is best described by changes in the total energy \( E(t) \) as a function of time \( t \). Therefore, we compute \( dE(t)/dt \) and write it in the form

\[
\frac{dE(t)}{dt} = G(t) + S(t),
\]

where \( G(t) \) and \( S(t) \) are the heating and cooling terms, respectively.
where

\[ G(t) = -\gamma \sum_{i=1}^{N} \dot{z}_i^2 = -2\gamma E_{kin}(t) \]  

(7)

is the dissipative term, describing energy irretrievably lost from the system [since \( E_{kin}(t) \) is positive definite], and

\[ S(t) = -2\gamma \cos(2t)(\dot{z}_i^2 + \dot{z}_j^2 - 2\dot{z}_i^2) \]

(8)

is the source of energy for the system. Since heating or cooling of the particles does not refer to the short-time fluctuations and oscillations of the energy on the scale of one trap cycle \((\Delta t = \pi)\), but is a systematic, macroscopic effect that emerges when \( E(t) \) is evaluated over many trap cycles, we introduce the cycle average \( \bar{f}(t) \) of an arbitrary function \( f(t) \) according to

\[ \bar{f}(t) = \frac{1}{\pi} \int_{t}^{t+\pi} f(t')dt'. \]

(9)

In a situation where heating and cooling balance on average, i.e., a steady state is reached, it makes sense to define the long-time average of a dynamical function \( f(t) \) as an average over many cycles according to

\[ \bar{f} = \lim_{M \to \infty} \frac{1}{M} \int_{t}^{t+Ms} f(t')dt', \]

(10)

where, in steady state, the zero of time \( t \) is arbitrary. In steady state, there is no net long-time gain or loss of system energy. Therefore, we have

\[ \frac{d\bar{E}}{dt} = \bar{G} + \bar{S} = 0, \]

(11)

from which it follows immediately that the average heating power \( \bar{S} \) may be expressed with the help of the cooling power \( \bar{G} \) via

\[ \bar{S} = -\bar{G} = 2\gamma \bar{E}_{kin}. \]

(12)

A consequence of (12) is that, given \( \gamma \), it allows us to compute the heating power \( \bar{S} \) as soon as we have an expression for \( \bar{E}_{kin} \). We derive it in pseudopotential approximation [1,4,12].

The advantage of the pseudopotential approximation is that it allows access to average properties of the particle dynamics, approximately keeping track of the time dependence of the particles’ motion during a trap cycle. Splitting the trajectory of particle number \( i \) into its macromotion part \( \bar{R}_i = (\bar{X}_i, \bar{Y}_i, \bar{Z}_i) \) and its micromotion part \( \bar{Y}_i \) [12], we may integrate analytically over the micromotion part of the trajectories when computing cycle averages and arrive at an expression for \( \bar{E}_{kin} \) that contains only the macromotion parts of the particle trajectories. We obtain [9]

\[ \bar{E}_{kin} = \frac{1}{2} \sum_{i=1}^{N} \left[ \left( 1 + \frac{\omega_i^2}{\kappa} \right) (\bar{X}_i^2 + \bar{Y}_i^2) + \left( 1 + \frac{\omega_i^2}{2} \right) \bar{Z}_i^2 \right] + \frac{\omega_i^2}{2} (\bar{X}_i^2 + \bar{Y}_i^2) + 2\bar{M}_i^2 \]

(13)

where the overlines indicate long-time averages according to (10), and the terms proportional to \( q^2 \) are due to the micromotion, thus taking the micromotion into account. Assuming ergodicity, we may replace the time averages by ensemble averages and obtain

\[ \bar{E}_{kin} = \frac{1}{2} \sum_{i=1}^{N} \left[ \left( 1 + \frac{\omega_i^2}{\kappa} \right) (\bar{X}_i^2 + \bar{Y}_i^2) + \left( 1 + \frac{\omega_i^2}{2} \right) \bar{Z}_i^2 \right] + \frac{\omega_i^2}{2} (\bar{X}_i^2 + \bar{Y}_i^2) + 2\bar{M}_i^2 \cdot \left( \sum_{i=1}^{N} \frac{1}{N} \right). \]

(14)

where ensemble averages are denoted by the angular brackets \( \langle \cdot \rangle \). Given the chaotic nature of the dynamics of a trapped Coulomb gas [10,11], replacing time averages with ensemble averages is expected to be an excellent approximation.

III. MEAN-FIELD THEORY

In order to evaluate the ensemble averages in (14), we need the distribution function \( f(\bar{V}_1, \ldots, \bar{V}_N; \bar{R}_1, \ldots, \bar{R}_N) \), where \( \bar{V}_i \) is the macromotion velocity of particle number \( i \), i.e.,

\[ \bar{V}_i = \bar{R}_i. \]

(15)

Since positions and velocities are not coupled in the \( N \)-particle Hamiltonian of the trap, the distribution function separates into a velocity-dependent part and a space-dependent part according to

\[ f(\bar{V}_1, \ldots, \bar{V}_N; \bar{R}_1, \ldots, \bar{R}_N) = f_v(\bar{V}_1, \ldots, \bar{V}_N) f_s(\bar{R}_1, \ldots, \bar{R}_N), \]

(16)

where

\[ f_v(\bar{V}_1, \ldots, \bar{V}_N) = (2\pi T)^{-3N/2} \exp \left( -\frac{1}{2T} \sum_{i=1}^{N} \bar{V}_i^2 \right). \]

(17)

In (17) we introduced the temperature \( T \) of the trapped particle clouds. This may look like a dangerous proposition given that the dynamics (1) of the trapped particles are explicitly time dependent. Indeed, the temperature of the cloud changes during a trap cycle and may even be different in the radial and the \( z \) directions. However, the concept of temperature is well defined if it refers to the temperature of the macromotion [13] and care is taken to evaluate \( T \) always at the same phase during a trap cycle, i.e., \( T \) has to be evaluated stroboscopically. Moreover, focusing, for now, on the case of spherical clouds eliminates the problem of different temperatures in different directions and a single temperature \( T \), as used in (17), is well defined.

The pseudo-oscillator energy of the macromotion is

\[ V_{osc}(\bar{R}_1, \ldots, \bar{R}_N) = \frac{1}{2} \sum_{i=1}^{N} \left( \omega_i^2 \bar{X}_i^2 + \omega_i^2 \bar{Y}_i^2 + \omega_i^2 \bar{Z}_i^2 \right). \]

(18)

where [11]

\[ \omega_i^2 = \omega_c^2 \approx a + q^2/2, \quad \omega_i^2 \approx 2(q^2 - a). \]

(19)

The Coulomb energy of the macromotion is

\[ V_{Coul}(\bar{R}_1, \ldots, \bar{R}_N) = \sum_{i,j=1 \atop i \neq j}^{N} \frac{1}{|\bar{R}_i - \bar{R}_j|}. \]

(20)
Appendix A. List of Publications

and the distribution function of the macromotion positions is

\[ f_s(\tilde{R}_1, \ldots, \tilde{R}_N) = N_s \exp \left\{ -\frac{1}{T} \left[ V_{\text{osc}}(\tilde{R}_1, \ldots, \tilde{R}_N) + V_{\text{Coul}}(\tilde{R}_1, \ldots, \tilde{R}_N) \right] \right\}, \]

where

\[ N_s = \left[ \int \exp \left\{ -\frac{1}{T} \left[ V_{\text{osc}}(\tilde{R}_1, \ldots, \tilde{R}_N) + V_{\text{Coul}}(\tilde{R}_1, \ldots, \tilde{R}_N) \right] \right\} d^{3N} \tilde{R} \right]^{-1}. \]

Instead of including all particle-particle correlations in our analytical analysis, we imagine that we focus on a single trapped particle at position \( \tilde{R} \) with velocity \( \tilde{V} = \tilde{R} \), moving in the mean field set up by the other \( N - 1 \) particles. This defines a mean-field picture in which all correlations are neglected and all particles are described by the single-particle distribution function

\[ f(\tilde{V}, \tilde{R}) = \beta(\tilde{V}) \rho(\tilde{R}), \]

where \( \beta(\tilde{V}) \) describes the probability distribution of velocity and \( \rho(\tilde{R}) \) is the space-distribution function of any one of the particles in the cloud. The velocity distribution function is the single-particle version of (17), i.e.,

\[ \beta(\tilde{V}) = \frac{1}{(2\pi T)^{l/2}} \exp \left( -\frac{1}{2T} \tilde{V}^2 \right) = \beta_i(V_i) \beta_j(V_j) \beta_k(V_k), \]

where

\[ \beta_i(V_i) = \frac{1}{(2\pi T)^{l/2}} \exp \left( -\frac{1}{2T} V_i^2 \right), \]

and \( l = x, y, \) or \( z \). The single particle space-distribution function is

\[ \rho(\tilde{R}) = N \exp \left\{ -\frac{1}{T} \left[ V_{\text{osc}}(\tilde{R}) + V_{\text{Coul}}(\tilde{R}) \right] \right\}, \]

where

\[ N = \left[ \int \exp \left\{ -\frac{1}{T} \left[ V_{\text{osc}}(\tilde{R}) + V_{\text{Coul}}(\tilde{R}) \right] \right\} d^{3N} \tilde{R} \right]^{-1}, \]

is the normalization factor,

\[ V_{\text{osc}}(\tilde{R}) = \frac{1}{2} \left( \omega_r^2 X^2 + \omega_y^2 Y^2 + \omega_z^2 Z^2 \right), \]

and

\[ V_{\text{Coul}}(\tilde{R}) = (N - 1) \int \frac{\rho(\tilde{R}) d^3 \tilde{R}}{|\tilde{R} - \tilde{R}'|}. \]

Using (29) in (26), we obtain an integral equation for \( \rho \) according to

\[ \rho(\tilde{R}) = N[\rho] \exp \left\{ -\frac{1}{T} \left[ V_{\text{osc}}(\tilde{R}) + (N - 1) \int \frac{\rho(\tilde{R}) d^3 \tilde{R}}{|\tilde{R} - \tilde{R}'|} \right] \right\}, \]

where the notation \( N[\rho] \) indicates that the normalization constant (27) via (29) is a functional of \( \rho \). We now notice that \( V_{\text{osc}} \) and \( V_{\text{Coul}} \) are homogeneous functions [12] of degrees 2 and \( -1 \), respectively. Therefore, scaling \( \tilde{R} \) according to

\[ \tilde{R} = (N - 1)^{1/3} \tilde{u}, \]

together with \( \rho(\tilde{R}) d^3 \tilde{R} = \rho(\tilde{u}) d^3 \tilde{u} \), allows us to write (30) in the form

\[ \rho(\tilde{u}) = \tilde{N}[\rho(\tilde{u})] \exp \left\{ -\frac{(N - 1)^{2/3}}{T} \left[ V_{\text{osc}}(\tilde{u}) \right. \right. \]

\[ \left. + \left( \int \rho(\tilde{u}) d^3 \tilde{u} \right) \frac{d^3 \tilde{u}}{|\tilde{u} - \tilde{u}'|} \right\}, \]

where

\[ \tilde{N}[\rho] = \left[ \int \exp \left\{ -\frac{(N - 1)^{2/3}}{T} \left[ V_{\text{osc}}(\tilde{u}) \right. \right. \]

\[ \left. \left. + \left( \int \rho(\tilde{u}) d^3 \tilde{u} \right) \frac{d^3 \tilde{u}}{|\tilde{u} - \tilde{u}'|} \right\} d^{3N} \tilde{u} \right]^{-1}, \]

is the new normalization constant. Equations (32) and (33) show clearly that \( \rho(\tilde{u}) \) is not a function of \( N \) and \( T \) separately, but depends only on the ratio

\[ \kappa = \frac{(N - 1)^{2/3}}{T}. \]

Therefore, we may write

\[ \rho(\tilde{u}) = \rho(\tilde{u}; a, q, \kappa). \]

In [9] we defined the scaled heating rate

\[ h = \frac{E_{\text{kin}}}{E_{\text{kin}}} \]

where

\[ E_{\text{kin}} = \frac{N}{2} \left\{ \left[ 1 + \frac{q^2}{8} \right] \omega_r^2 + \frac{q^2}{2} \right\} \langle X^2 \rangle \]

\[ + \left\{ \left[ 1 + \frac{q^2}{8} \right] \omega_y^2 + \frac{q^2}{2} \right\} \langle Y^2 \rangle \]

\[ + \left\{ \left[ 1 + \frac{q^2}{2} \right] \omega_z^2 + 2q^2 \right\} \langle Z^2 \rangle \]

is the cycle-averaged kinetic energy of the trapped particles with the Coulomb interaction switched off (noninteracting gas). We showed that for fixed \( a \) and \( q \) a universal curve results, independent of \( N \) and \( T \), when \( h \) is plotted against

\[ \sigma = \tilde{s}/s_c. \]

Here,

\[ \tilde{s} = \sqrt{\langle T^2 \rangle} = \left( \sum_{\text{atom}} \left[ \langle X^2 \rangle + \langle Y^2 \rangle + \langle Z^2 \rangle \right] \right)^{1/2}, \]

if \( \tilde{s} \) is evaluated at the end of each trap cycle, and \( s_c \) is the root-mean-square size of the crystal. Assuming spherical symmetry and a homogeneous charge distribution, we evaluate \( s_c \) in pseudo-oscillator approximation, where the confining field is a harmonic oscillator with oscillator frequencies \( \omega_r = \omega_y = \omega_z = \omega \), where, according to (19), \( \omega \approx q \). In this
Appendix A. List of Publications

Y. S. Nam, E. B. Jones, and R. Blumen

PHYSICAL REVIEW A 90, 013402 (2014)

case, the charge density $\rho_c$ of the crystal is a constant for $0 \leq R \leq R_c$ and $0$ for $R > R_c$, where $R_c$ is the radius of the crystal. To determine $R_c$, we need to equate the mechanical restoring force $F = \omega^2 R$ of the oscillator with the Coulomb force, $E$, at $R = R_c$. From $\nabla \cdot E = 4\pi \rho_c$, we obtain

$$\rho_c = \frac{3q^2}{4\pi}.$$  

(40)

and from $N = 4\pi \rho_c R_c^3/3$ we obtain

$$R_c = (N/q^3)^{1/3}.\quad(41)$$

This is all we need to compute $s_i = \left\{4\pi \rho_c \int_0^R r^4 \, dr \right\}^{1/2} = \left(\frac{3}{5q^3/3}\right)^{1/2} N^{5/6}.\quad(42)$

On the basis of (35) it is now straightforward to provide a theoretical underpinning for what in [9] was a purely heuristic procedure. Defining

$$\bar{M}^{(\alpha)} = \frac{1}{N} \sum_{i=1}^{N} (X_i^{(\alpha)} Y_i^{(\alpha)} Z_i^{(\alpha)}) = (X^{(\alpha)} Y^{(\alpha)} Z^{(\alpha)})\quad(43)$$

as the $\alpha$th moments of the macromotion coordinates and

$$\bar{\rho}^{(\alpha)} = \int (u^{(\alpha)} v^{(\alpha)} w^{(\alpha)}) \rho(u; a, q; \kappa) \, du^3\quad(44)$$

as the $\alpha$th moments of the scaled density $\rho(u; a, q; \kappa)$, we obtain with (31)

$$\bar{M}^{(2)} = (N-1)^{2/3} \bar{\rho}^{(2)}(a; q; \kappa).\quad(45)$$

With (43), (44), and (45), we may express $\delta$ in (39) in the form

$$\delta = \left[ N \left[ M^{(2)} + M^{(2)}_{\|} + M^{(2)}_{\perp} \right] \right]^{1/2}$$

$$= \left[ N \left[ (N-1)^{2/3} \bar{\rho}^{(2)}(a; q; \kappa) \right] \right]^{1/2}.\quad(46)$$

which, for large $N$, where $(N-1)/N \approx 1$, may also be written as

$$\delta = N^{5/6} \left[ \bar{\rho}^{(2)}(a; q; \kappa) \right]^{1/2}.\quad(47)$$

We now see that, when computing $\sigma$ defined in (38) as the ratio of $\delta$ defined in (47) and $s_i$ defined in (42), the factor $N^{5/6}$ cancels, and since the moments $\mu_i$ in (47) are functions of $a$, $q$, and $\kappa$ only, we obtain the result that

$$\sigma = \sigma(a, q; \kappa)\quad(48)$$

is a function of $a$, $q$, and $\kappa$ only, and is not dependent on $N$ and $T$ separately. We also note that

$$\frac{1}{T} \bar{M}^{(2)} = \kappa \bar{\rho}^{(2)}(a; q; \kappa)\quad(49)$$

is a function of $a$, $q$, and $\kappa$ only. Assuming the same temperature in all three directions, we have

$$\langle X^2 \rangle = \langle Y^2 \rangle = \langle Z^2 \rangle = T.\quad(50)$$

With this information in hand, we define and compute

$$\epsilon(a; q; \kappa) = \frac{1}{NT} \bar{E}_{\text{kin}}$$

$$= \frac{1}{2} \left[ 1 + \frac{3}{4} q^2 + \frac{\kappa q^2}{2} \left( \mu_2^{(2)} + \mu_4^{(2)} \right) + 2 \kappa q^2 \mu_2^{(2)} \right].\quad(51)$$

and

$$\epsilon_g(a; q; \kappa) = \frac{1}{NT} \bar{E}_{\text{kin}}^{\text{num}} = \frac{\kappa}{2} \left[ \left( 1 + \frac{q^2}{8} \right) \omega_0^2 + \frac{q^2}{2} \mu_2^{(2)} \right]$$

$$+ \left[ \left( 1 + \frac{q^2}{2} \right) \omega_0^2 + 2q^2 \right] \mu_2^{(2)} \right].\quad(52)$$

Therefore, we have

$$h(a, q; \kappa) = \frac{\epsilon(a; q; \kappa)}{\epsilon_g(a; q; \kappa)}\quad(53)$$

i.e., $h(a, q; \kappa)$ is a function of $a$, $q$, and $\kappa$ only. Thus, for fixed $a$ and $q$, as observed numerically in [9], a one-parameter manifold, i.e., the universal curve [9], results when $\alpha$ is plotted against $\sigma$.

IV. HEATING CURVE: EXPLICIT ANALYTICAL FORM AND COMPARISON WITH NUMERICAL DATA

At this point, because of $\kappa$ scaling, we explained why the heuristic scaling procedure outlined in [9] "works," i.e., why, for fixed $a$, $q$, the heating data of trapped, charged particle clouds all collapse onto one single, universal curve. What is missing is an explicit, analytical formula of the universal heating curve to be compared with the numerical heating data. Moreover, the numerical results in [9] indicate that the heating curves for different $q$ may also collapse onto each other. To find the analytical form of the heating curve and to check whether there is yet another scaling hidden in the particle dynamics that may account for the observed near degeneracy of heating curves for different $q$, we have to solve (32) analytically. To accomplish this, we restrict ourselves to the spherically symmetric case $\omega_0 = \omega_r = \omega_z$, which, according to (19), occurs for $a = q = 2/3$. In this case we have

$$\omega_i = \omega_0 = \omega_0 = q\quad(54)$$

and

$$\rho(u) = \tilde{N} \exp \left[ -\kappa \left( \frac{1}{2} \frac{q^2 u^2}{|u|^2} + \int \frac{\rho(u') |d^3 u'|}{|u|^2 - |u'|^2} \right) \right].\quad(55)$$

The integral term in (55) may be reduced to an expression containing only one-dimensional integrals according to

$$\int \rho(u') |d^3 u'| = 4\pi \left[ \int_0^\infty (u')^2 \rho(u') \, du' + \int_\infty^0 u' \rho(u') \, du' \right].\quad(56)$$

Even with the simplification of spherical symmetry, Eq. (32) is still a nonlinear integral equation. Therefore, we look for an
Appendix A. List of Publications

ANALYTICAL MEAN-FIELD SCALING THEORY OF . . .


According to construction, and for fixed \( N \), we expect that \( h \to 1 \) for \( T \to \infty \). This is indeed the case. Using (63), applicable in the case \( T \to \infty \), we obtain \( h = 1 \). In [9] we showed that \( h \approx \frac{1}{2} \) in the crystal state where \( T = 0 \) and \( \kappa \to \infty \). Since, according to (64), \( \alpha \) is a constant in this case, we obtain \( h = 1/[2(1 + \sqrt{2}/8)] \approx 1/2 \) in this limit. Thus our analytical result (66) reproduces both limits of the universal curve.

In order to compare our analytical universal curve with the numerical data of [9], we need an analytical expression for \( \sigma(q; \kappa) \). In [9] we normalized the size of the particle cloud to the size of the crystal. In our analytical model the consistent, analogous procedure is to normalize the size of the particle cloud at finite \( T \) to the size of the cloud at \( T = 0 \). Since

\[
\langle s^2 \rangle = N(X^2 + Y^2 + Z^2) = N(N - 1)^{2/3}(u^2)
\]

we have

\[
\sigma = \sqrt{\frac{\alpha(q; \kappa = \infty)}{\alpha(q; \kappa)}}
\]

where \( \alpha(q; \kappa = \infty) \) is stated in (64).

We are now ready to plot the universal curve and compare with the numerical data. The result is shown in Fig. 1. The smooth line is the universal heating curve (66); the data points are the scaled heating rates imported from Fig. 3 of [9]. We see that, especially for small \( \sigma \), i.e., in the low-temperature regime, the agreement of the analytical prediction with the numerical simulation data is near perfect. Deviations occur only for large \( \sigma \), i.e., in the high-temperature regime. This observation, in fact, is odd, since the agreement is expected to be better in the more “trivial” high-temperature regime where the interacting Coulomb gas is expected to become a noninteracting gas of isolated particles, perfectly described

\[
\text{FIG. 1. Scaled heating rate } h \text{ versus scaled cloud size } \sigma. \text{ Solid line: analytical scaled heating rate (66) versus analytical cloud size (68). Plot symbols: numerical data for scaled heating rates obtained by simulating the dynamics of } N = 50,100,200,500 \text{ particles simultaneously stored in an ideal Paul trap with } q = 0.2 \text{ and } \alpha = q^{7/2} \text{ (data transferred from Fig. 3 of [9]). The analytical curve is in excellent agreement with the numerical data.}
\]
Appendix A. List of Publications

V. UNCOVERING A HIDDEN, ADDITIONAL SCALING

In [9] we found that the heating data for $q = 0.3$ almost collapse onto the heating curve for $q = 0.2$, indicating that an additional, unexpected scaling might exist. This is indeed the case. Let us introduce the scaling $\alpha = q^{1/3}w$, which turns (61) into

$$w = \frac{1}{2} \lambda q^{1/3} - \frac{2\sqrt{n\pi}}{3\sqrt{\lambda}} q^{2/3} u^{1/2}, \quad (69)$$

Defining

$$\lambda = q^{-1/3} = \left(\frac{N - 1}{T} \right)^{1/3} q^{-2/3}, \quad (70)$$

we have

$$w = \frac{1}{2} \lambda - \frac{2\lambda}{3\sqrt{\pi}} u^{1/2}. \quad (71)$$

Unlike (61), which depends on $q$ and $k$ separately, Eq. (71) depends only on the single scaling parameter $\lambda$. Thus we may write the solution of (71) in the form $w(\lambda)$. Returning now to the evaluation of $\sigma$ in (68), we find

$$\sigma(\lambda) = \frac{3\sqrt{\pi}}{4} \left(\frac{u(q; \lambda)}{w(q; \lambda)}\right)^{1/2} \quad (72)$$

which scales in the single parameter $\lambda$. Similarly, expressing $\hbar$ in (66) in terms of $w(\lambda)$, we find

$$h(q; \lambda) = \frac{2\sqrt{n\pi} u(\lambda)(1 + q^2/4) + \kappa q^2}{2\kappa q^2(1 + q^2/8)} \quad (73)$$

For small $q$, we may neglect the terms quadratic in $q$ in (73). In this case, just like $\sigma$ in (72), $h$ depends on the single scaling parameter $\lambda$ only. In fact, for $q \leq 0.4$, the analytical curves $h(q; \lambda)$ collapse approximately onto one single curve and cannot be distinguished as separate curves on the scale of Fig. 1. Thus we explained the near degeneracy of heating curves for different $q$ values found in [9] as due to the fact that both $\hbar$ and $\sigma$ scale significantly only in the single parameter $\lambda$. Thus we showed that the heating data of spherical clouds confined in a spherical trap all collapse onto a single, universal heating curve.

VI. DISCUSSION

In order to predict absolute heating rates of charged-particle clouds in a Paul trap, our ultimate goal is to evaluate $S(t)$, the source term defined in (8), directly as a function of trap parameters. This, however, is extremely difficult and depends on both microscopic and macroscopic details of the trapped particles’ dynamics. Concerning the global characteristics of the dynamics, we found that it makes a substantial difference whether the particle dynamics are integrable or not. For instance, as reported in [9], replacing the two-body Coulomb interaction in (1) with an integrable, harmonic two-body force results in particle clouds that do not heat. This shows that the global properties of the dynamics are an essential ingredient for understanding rf heating. However, it has also been suggested in the literature that close particle-particle collisions are a source of rf heating [15–17]. This is corroborated by our numerical simulations with two-body Coulomb interactions, which show that large, sudden changes in $E(t)$ are always accompanied by close particle-particle collisions. However, in view of our experience with integrable two-body interactions, it is clear that close collisions are only a necessary condition for rf heating to occur, since close collisions certainly do occur in the case of the nonheating, harmonic two-body force, which does not exhibit rf heating [9]. Therefore, we are led to the conclusion that both close collisions and nonintegrable dynamics are necessary ingredients for understanding the rf heating phenomenon. Since both nonintegrability and nonlinear collisions are difficult to deal with analytically, this explains why it is so difficult to evaluate $S(t)$, and, by extension, $S$. Applied to the present case, for example, neglecting collisions, but taking the micromotion into account, it is straightforward to show that $S = 0$, a useless result that does not explain the rf heating phenomenon, but does point to the importance of two-body collisions as a necessary ingredient for the explanation of rf heating.

Side-stepping direct evaluation of $S(t)$, we took a different route, evaluating instead the dissipative term $G(t)$, which, according to (7) is simply connected with $E_{\text{kin}}(t)$ and is much more readily accessible. The price to pay is that $S(t)$ and $G(t)$ are directly connected only in steady state, i.e., when a balance exists between rf heating and dissipative cooling. Nevertheless, this allows us to determine the universal scaling behavior of trapped particle clouds in the form of a universal curve that all future rf heating theories have to satisfy and may be used to constrain these theories.

An important condition for our method to work is the existence of a steady-state solution of (1). In order to prove the existence of a steady state in the kinetic energy $E_{\text{kin}}(t)$, we show, in Fig. 2, $E_{\text{kin}}(n\pi)$ as a function of trap cycle number $n$ for the case $N = 20, a = 0.02, q = 0.2$, and $\gamma = 4 \times 10^{-4}$. Figure 2 shows that after an initial transient, lasting for about 3000 trap cycles (due to choosing a random initial condition for this cloud at $t = 0$), $E_{\text{kin}}(n\pi)$ settles down into a steady state, fluctuating around its long-time average $E$. We checked
explicitly, continuing to run this simulation for 10^3 cycles (not shown in Fig. 2), that (a) the upward spike at \( n \approx 50000 \) is only a local fluctuation and (b) the stationary pattern exhibited in Fig. 2 continues as shown in Fig. 2 without indication of any runaway heating, strongly suggesting that for \( n \gtrsim 3000 \), rf heating and cooling are always balanced on average. While Fig. 2 shows an isolated example of the existence of a steady state for a single \( N,a,q,\gamma \) combination, of the literally thousands of \( N,a,q,\gamma \) combinations for which we performed numerical heating simulations, spherical or not, we never found a single example that would have shown runaway heating.

At first glance, the eventual balance of heating and cooling, i.e., the existence of stationary states for any damping parameter \( \gamma > 0 \), may seem surprising. However, given the fact that numerical evidence firmly establishes that the rf heating rate of trapped particle clouds decreases with cloud size (see, e.g., [10]), this phenomenon is no longer surprising.

Figure 3, a schematic sketch for the purpose of increasing clarity, illustrates the connection between rf heating rate and cloud size, in the following referred to as the rate function. We see that the overall shape of the rate function, qualitatively, has the form of a tent. There exists a cloud size that produces a maximal heating rate (tip of the tent), and the heating rate decreases to both sides of the tip. Let us first focus on large clouds (right wing of the rate function). Let us also assume that cooling is switched on with a damping constant \( \gamma \) that results in the cooling power \( G(\gamma) \), indicated by the dashed line in Fig. 3. If in this situation, we start with a cloud whose size corresponds to point \( R \) on the rate function, the rf heating power produced by the cloud is insufficient to counteract the cooling power \( G \). Consequently, kinetic energy is drained from the cloud, and its size shrinks. Indicated by the arrow in Fig. 3, the cloud will move from point \( R \) toward point \( Q \). Conversely, if we start with a smaller cloud, corresponding to point \( P \), the rf heating power of the cloud will exceed the cooling power \( G \). As a consequence, the kinetic energy of the cloud will increase, the cloud will expand, and, as indicated by the arrow in Fig. 3, will move toward point \( Q \). Thus clouds larger than those corresponding to point \( Q \) will cool, shrink, and move toward \( Q \), and clouds smaller than those corresponding to point \( Q \) will heat, expand, and also move toward \( Q \). Thus, for given damping constant \( \gamma \), point \( Q \) is a stable stationary point. It is apparent that no matter how small \( \gamma \), a stable stationary point always exists on the right wing of the rate function.

A technical point is in order here. We did not extend the plot of the rate function toward very large cloud sizes, since, at this point in time, we do not know whether the rate function actually intersects the cloud-size axis, or approaches it asymptotically. Clearing up this question is computationally expensive, since the smaller the damping constant \( \gamma \), the longer the simulations have to run in order to establish the stationary point \( Q \). Luckily, for the statement that \( Q \) exists on the right wing of the rate function, independent of the size of \( \gamma \) (as long as \( \gamma \) is small enough so that \( G \) is below the tip of the rate function), it does not matter whether the rate function intersects the cloud-size axis, or whether it only approaches it asymptotically. Based on this discussion, and, in particular, based on the decreasing nature of the rate function for large cloud sizes (see Fig. 3), a runaway event, in which from some time \( t^* \) on the rf heating power beats the cooling power (on average) for all times \( t \gtrsim t^* \), leading to an ever-expanding cloud, is strictly impossible.

Let us now discuss what happens if we start the cloud in point \( R' \) on the left wing of the rate function. In this case the rf heating power of the cloud is smaller than the cooling power. Therefore, the cloud will lose kinetic energy, and become even smaller. In fact, indicated by the arrow in Fig. 3, the cloud will move away from point \( Q' \) and rapidly collapse into the crystal state. Conversely, a cloud started in point \( P' \) has more rf heating power than can be counteracted by the cooling.
where the pseudo-oscillator frequencies \( \omega_x, \omega_y, \) and \( \omega_z \) are defined in (19), and [12]

\[
\begin{align*}
\xi_i(t) &= \frac{-q}{2} X_i(t) \sin(2t), & \eta_i(t) &= \frac{-q}{2} Y_i(t) \sin(2t), \\
\zeta_i(t) &= q Z_i(t) \sin(2t).
\end{align*}
\]

 Apparently, the main effect of the pseudopotential approximation is to represent (not eliminate) the effect of the rapid micromotion in the equations of the macromotion \((77)\) by time-independent force terms, derived from an effective potential, the pseudopotential. In our experience this method is highly accurate as long as (i) \( q \) is small [see (18) and the fact that the ratios of the micromotion and macromotion amplitudes in \((78)\) are proportional to \( q \) and (ii) the trap frequency is large compared to the pseudo-oscillator frequencies \( \omega_x, \omega_y, \) and \( \omega_z \). In fact, in our experience, \( q < 1/2 \) and a ratio of 2:1 for the ratio of trap frequency and pseudo-oscillator frequencies are sufficient to guarantee acceptable accuracy. Since the set of equations \((1)\) is unstable for \( q \geq 0.45 \) (Mathieu stability limit), for stable three-dimensional trapping the condition \( q < 1/2 \) is automatically satisfied. Since for spherical clouds \( \omega \approx q \), and since in our units the trap frequency is equal to 2, the other condition is also fulfilled. The accuracy of the pseudopotential approximation improves quickly with decreasing \( q \) and increasing trap frequency. We conclude that, for the parameter sets used in this paper, the pseudopotential approximation is reliable.

The first time the pseudopotential approximation is used in this paper is in the derivation of \((13)\). It is important to emphasize that \((13)\) is not obtained by discarding the micromotion; it is derived taking full account of the micromotion by writing \( \tilde{x}_i(t) \) in the form \((74)\), with the components of \( \tilde{y}(t) \) given by \((78)\), and then processing the explicitly time-dependent terms originating from the micromotion \( \tilde{y}(t) \) explicitly and analytically.

In \((14)\) we replaced time averages by ensemble averages, and a few comments concerning this procedure are in order. To start the discussion, it is important to point out that in our numerical simulations we do not make this approximation. The numerical data points in Fig. 1, e.g., are computed via time averages, as required. The replacement of time averages by ensemble averages is necessary only for our analytical calculations. In Sec. II we argued that, because of the chaotic nature of the trapped particles’ dynamics [10], the replacement is most likely justified. While it is known that chaos does not necessarily imply ergodicity [19], it likely does so in the case of hard chaos [20], in which there are no regular islands in phase space. In our case, in the presence of weak damping, regular islands correspond to attractors. To the best of our knowledge, based on extensive experience with trapped-particle simulations, there is only a single attractor in phase space, the one that corresponds to the crystal state. Apart from this attractor, we never encountered any others (except for crystals with different geometric orderings that are close in phase space). In addition, the phase-space volume of the basin of attraction [20] of the crystal attractor is vanishingly small compared with the total accessible phase space. A rough upper bound for the ratio of the phase-space volume of the crystal basin, \( V_c \), to the total phase-space volume, \( V \), may be estimated in the following way. Let us assume that the ratio of the available spatial dimensions of a cloud to the spatial dimensions of the basin is 2:1 (a gross underestimate), and that the same is assumed for the velocities. Then, in the case of \( N = 20 \) particles, an upper bound for the ratio of the phase-space volumes is \( V_c/V \approx (1/2)^{10} \approx 10^{-30} \). This shows that, while in the cloud state, the presence of the crystal
Appendix A. List of Publications

**ANALYTICAL MEAN-FIELD SCALING THEORY OF . . .**

PHYSICAL REVIEW A 90, 013402 (2014)

![Graph](image)

**FIG. 4.** Velocity distribution $\tilde{P}_x(V_x)$ of $N = 20$ trapped particles (solid line) together with the theoretically expected Gaussian (dotted line), computed according to (25) with a temperature $\bar{T}$ extracted from the macromotion of the particles.

The attractor is irrelevant for the cloud dynamics and therefore, for clouds, an assumption of ergodicity, allowing the approximate replacement of time averages with ensemble averages, is likely justified.

A final point concerns the notion of temperature in our manifestly time-dependent system. It is clear that a constant temperature cannot be defined for the trapped cloud during all phases of a trap cycle. According to (78), during a trap cycle, the cloud is first compressed in the radial direction while expanding in the $z$ direction, and then it is compressed in the $z$ direction while expanding in the radial direction. This is a nonequilibrium situation in which a temperature seemingly has no place. However, in the stationary state of a cloud, in which rf heating and cooling balance, the temperature of the macromotion is well defined [13]. It is the macromotion temperature, i.e., the thermal motion of $\tilde{R}_i(t)$, that we refer to in our mean-field calculations. To test this picture, and to prove that the assumption of a Gaussian velocity distribution is valid, we computed, as an example, the distribution of the $x$ component of the velocity of $N = 20$ trapped particles in the stationary state for the case $a = 0.02$, $q = 0.2$, and $x = 4 \times 10^{-3}$. To improve the statistics we computed the combined ensemble and temporal average $\tilde{P}_x(V_x)$ of the $x$ component of the velocity distribution, defined as

$$\tilde{P}_x(V_x) = \frac{1}{N} \sum_{i=1}^{N} \tilde{P}_i(V_{x,i}),$$

(79)

where $\tilde{P}_i(V_{x,i})dV$ is the probability of finding particle number $i$ in the velocity volume element $dV$, and the time average, in the stationary state, was extended over 10 000 trap cycles. Since our simulations return $\tilde{x}_i(t)$, but not $\tilde{X}_i(t)$, as required for the computation of $\tilde{P}_x(V_x)$, we obtain $\tilde{X}_i(t)$ by compensating for the micromotion. With (78) we have

$$\tilde{V}_{x,i} = \tilde{x}_i(n\pi) + q\chi_i(n\pi).$$

(80)

The solid line in Fig. 4 shows $\tilde{P}_x(V_x)$, where the macromotion velocities $V_{x,i}$ were evaluated according to (80).

To compare with the theoretically expected Gaussian velocity distribution (25), we also computed the temperature

$$\bar{T} = \frac{1}{N} \sum_{i=1}^{N} \tilde{X}_i^2$$

(81)

as the temporal and ensemble average over all $N = 20$ particles and over 10 000 trap cycles, where the velocities $\tilde{X}_i$ were again evaluated according to (80). Using $\bar{T}$ computed according to (81) in (25) with $l = x$, we obtain the Gaussian plotted as the dotted line in Fig. 4. We see that $\tilde{P}_x$ and the Gaussian are reasonably close both in shape and in width. We note that there are no free parameters in this comparison, since the temperature, determining the width, is extracted from the numerical simulations as well. Thus the quantitative, parameter-free agreement between the two curves in Fig. 4 corroborates our assumption of (i) a Gaussian velocity distribution (agreement of shapes) and (ii) the notion of a temperature (agreement of widths).

**VII. SUMMARY AND CONCLUSIONS**

In this paper we provided the analytical underpinning of the scaling results found in [9]. We showed that a simple analytical mean-field theory is capable of explaining both existence and form of the universal heating curve [9]. The scaling we found is a consequence of the fact that both the pseudo-oscillator potential and the mean-field Coulomb potential are homogeneous functions of degrees 2 and $-1$, respectively. In addition we found an unexpected scaling that explains why the heating curve depends only on the single scaling parameter $\lambda = [q(N - 1)]^{2/3}/T$. We observe excellent agreement between our analytical mean-field theory and the available numerical data.

**ACKNOWLEDGMENT**

R.B. acknowledges financial support by Grant No. 216687 of the Research Council of Norway.

Appendix A. List of Publications

Structural stability of the quantum Fourier transform

Y. S. Nam · R. Blümel

Received: 16 July 2014 / Accepted: 9 January 2015

Abstract While it is important to investigate the negative effects of decoherence on the performance of quantum information processors, Landauer was one of the first to point out that an equally basic problem, i.e. the effects of unavoidable hardware flaws in the real-world implementations of quantum gates, needs to be investigated as well. Following Landauer’s suggestion, we investigated the structural stability of the quantum Fourier transform (QFT) via significantly changing the analytical form of its controlled rotation gates, thus modeling structural flaws in the Hamiltonian of the QFT. Three types of modified rotation gates were investigated, numerically and analytically, changing the exact QFT rotation angles $\pi/2^j$ to (1) $\pi/\alpha^j$, (2) $\pi/2j^\beta$, and (3) $\pi/\log_j(j + 1)$, where $\alpha$, $\beta$, and $\gamma$ are constants, and $j$ is the integer distance between QFT qubits. Surprisingly good performance is observed in all three cases for a wide range of $\alpha$, $\beta$, and $\gamma$. This demonstrates the structural stability of the QFT Hamiltonian. Our results also demonstrate that the precise implementation of QFT rotation angles is not critical as long as the angles (roughly) observe a monotonic decrease in $j$ (hierarchy). This result is important since it indicates that stringent tolerances do not need to be imposed in the actual manufacturing process of quantum information hardware components.

Keywords Quantum Fourier transform · structure · stability · robustness · hierarchy · topology

PACS 03.67.Lx

Y. S. Nam
Department of Physics, Wesleyan University, Middletown, Connecticut 06459-0155, USA
E-mail: ynam@wesleyan.edu

R. Blümel
Department of Physics, Wesleyan University, Middletown, Connecticut 06459-0155, USA
1 Introduction

There are many obstacles in the way of realizing a quantum computer. Prominent among them are gate defects [1,2] and decoherence [1,3,4]. Much work has been focused on decoherence, culminating in methods of quantum error correction [3–8] that, at least in principle, are capable of controlling the detrimental effects of decoherence. However, the problem of decoherence notwithstanding, when it comes to an actual implementation of a physical quantum computer, the adverse effects of gate defects on the performance of the quantum computer need to be addressed first. This is so, because no matter how well we protect our quantum computer from its environment, even if we eliminate decoherence effects completely, if the performance of our quantum computer reacts sensitively to flaws in the implementation of its components, a working, physical quantum computer may never be realized. Given the fact that it is strictly impossible to execute a quantum gate with 100% accuracy under any circumstances, we shall focus in this paper on the sensitivity of a quantum processor with respect to structural changes in its Hamiltonian.

As a testbed algorithm, we use the quantum Fourier transform (QFT) [3,4]. This choice is justified since the QFT is one of the core ingredients of many important quantum algorithms, such as Shor’s algorithm [9]. Accordingly, there have already been a number of studies investigating the performance of the QFT under a variety of conditions [2,10–15] and one of the findings is extraordinary robustness of the performance of the QFT with respect to static gate defects [15]. Adding to this result we show in this paper that the QFT is also insensitive to structural changes in the actions of its phase rotation gates. Supporting the idea of the primary importance of the hierarchy, or the topology, of the QFT circuit [15], we confirm here that even maintaining only a rough hierarchy in the phase rotation gates of the QFT still allows us to find a hidden periodicity in a quantum input state with acceptable probability.

Several quantitative measures of phase-angle hierarchy are proposed in this paper. First, we investigate an exponential hierarchy, i.e. the hierarchical type used in the exact QFT [3,4]. This is followed by a study of a power-law hierarchy, which is fundamentally different from its exponential counterpart, since there is no scale factor in a power-law. Structural insensitivity is found in both cases. Finally, further corroborating our results, we also present an inverse-log hierarchy, after which we discuss our results and conclude the paper.

We note that throughout this paper we use the banded QFT [14], keeping only those phase rotation gates that are within \( b \) nearest neighbors with respect to the control qubit, where \( b \) is the bandwidth [14]. In particular, we use \( b = 8 \). This choice is motivated by the fact that \( b = 8 \) is sufficient for the practical use of the QFT in the period-finding part of Shor’s algorithm [11,14]. The cases without banding, and how they relate to their banded counterparts, will be discussed briefly toward the end of this paper.
2 Numerical Results

2.1 Exponential Hierarchy

Operating between qubits number \( k \) and \( l \), we start by introducing the controlled phase rotation gate \( \hat{\theta}_j \) (CROT) [3,4] used in the QFT, where \( j = |k - l| \) is the integer distance between qubits number \( k \) and \( l \). If qubit number \( k \) acts as the control qubit \( |c_k\rangle \in \{0, 1\} \), and qubit number \( l \) acts as the target qubit \( |t_l\rangle \in \{0, 1\} \), the CROT gate \( \hat{\theta}_j \) is defined as

\[
\hat{\theta}_j |c_k\rangle |t_l\rangle = \begin{cases} |c_k\rangle e^{i\theta_j} |t_l\rangle, & \text{if } |c_k\rangle = |1\rangle \implies |t_l\rangle, \\ |c_k\rangle |t_l\rangle, & \text{otherwise,} \end{cases}
\]

(1)

where, in the case of the exact QFT,

\[ \theta_j = \frac{\pi}{2^j}. \]

(2)

The relation (2) defines an exponential hierarchical structure of phase rotation angles, where the rotation angle of the target qubit decreases exponentially with its distance from the control qubit. The base 2 of the exponential in (2) is not an accident. It relates directly to the base-2 arithmetic used in transcribing the abstract QFT unitary transformation into a realization with qubits that have two possible states. Only in this way, because of number-theoretic relationships, will the qubit-based QFT perform perfectly, since desired amplitude cancellations and reinforcements (quantum interference) will happen exactly [3,4]. One might think, then, that any change of the base 2 in (2), in conjunction with the continued use of qubits, will hopelessly muddle the inner workings of the QFT algorithm, effectively destroying its function. This seems especially critical in the case where the base 2 in (2) is changed to an irrational number, which does no longer correspond to a number system which is in a simple algebraic relationship to the base-2 number system induced by two-state qubits. However, in an actual, physical implementation of phase-rotation gates, the precise base-2 relationship of the exponential hierarchy of phase rotations cannot be guaranteed. Therefore, still keeping the exponential nature of the hierarchy in (2), our first test case of a structural change in the QFT consists of replacing the exact rotation angles (2) with modified rotation angles according to

\[ \theta_j \to \tilde{\theta}_j^{(E)} = \frac{\pi}{\alpha^j}. \]

(3)

As discussed above, this is a serious structural change of the QFT, since \( \alpha \) is allowed to be any real number.

The exact \( n \)-qubit QFT \( |s'\rangle \) of an \( n \)-qubit integer input state \( |s\rangle \) is defined as the sum

\[
|s'\rangle = \frac{1}{\sqrt{2^n}} \sum_{l=0}^{2^n-1} \Phi(s, l) |l\rangle
\]

(4)
over all \( n \)-qubit integer output states \(|\ell\rangle\), where
\[
\Phi(s, l) = \exp(2\pi i s l / 2^n). \tag{5}
\]
Defining \( s_{[m]} \) and \( l_{[m]} \) as the \( m \)th binary digits of \( s \) and \( l \), respectively, we may alternatively write (5) in the form
\[
\Phi(s, l) = \prod_{t=0}^{n-1} \prod_{j=0}^{l_t-1} \exp \left( i\pi s_{[n-t-j-1]} l_{[j]} / 2^n \right). \tag{6}
\]
Changing the base 2 in (6) to \( \alpha \) according to (3), introducing the bandwidth \( b \), and resumming, the phase (6) of the exact QFT is transformed into the phase of the general \( n \)-qubit exponentially hierarchical QFT according to
\[
\Phi_b^{(E)}(s, l; \alpha) = \exp \left[ ix_{\alpha}^{(E)}(s, l; \alpha) \right], \tag{7}
\]
where
\[
x_{\alpha}^{(E)}(s, l; \alpha) = x \left( \sum_{m=0}^{n-1} s_{[m]} l_{[n-1-m]} + \sum_{j=1}^b \frac{1}{2^j} \sum_{m=0}^{n-1} s_{[m]} l_{[n-j-1-m]} \right). \tag{8}
\]
Using the most-prominent-peak criterion [13, 14], i.e., choosing the nearest-integer peaks to the Fourier peaks of the QFT except for those trivial peaks that correspond to the powers-of-2 factor of a given periodicity [15] as our performance measure of the QFT (assumed here and throughout the paper), Fig. 1 shows the normalized performance \( P \) of the banded \((b = 8)\), exponentially hierarchical QFT as a function of \( \alpha \), where the normalization is performed with respect to the performance of the exact, exponentially hierarchical QFT with \( \alpha = 2 \) and \( b = 8 \). For the input state \(|s\rangle\) we used an \( \omega \)-periodic state, i.e. \(|\ell + \omega|s\rangle = \langle \ell |s\rangle\), with periodicity \( \omega = 30 \).

As expected, the best performance is achieved for \( \alpha = 2 \), which corresponds to the exact QFT. However, as shown in Fig. 1, even for deviations of up to 5% from \( \alpha = 2 \), we still obtain better than 90% performance for qubit numbers up to \( n = 20 \), and better than 50% performance for deviations up to 10% from \( \alpha = 2 \). This points to an extraordinary robustness of the QFT with respect to structural changes. However, we also observe a rapid decline in performance for decreasing \( \alpha \) (left wings of the performance curves in Fig. 1). A decreasing \( \alpha \) flattens the hierarchy, i.e. for decreasing \( \alpha \), \( \pi / \alpha \) takes longer to decline, erasing the hierarchy completely for \( \alpha \rightarrow 1 \), accompanied by zero performance. This shows that hierarchy in the rotation angles of the CROT gates is important. However, as the right wings of the performance curves in Fig. 1 show, it is not advisable to overemphasize the hierarchy. In fact, for \( \alpha > 2 \), we also see a decline in performance. The decline is not as fast as in the exponential case, since larger \( \alpha \) effectively correspond to cutting CROT gates, which corresponds to tighter banding [14]. This explains the slower decay of performance for \( \alpha > 2 \), since banding, in itself, is actually beneficial [14]. But only to a certain extent. For \( \alpha \gg 2 \), too many CROT gates are effectively cut,
again eliminating the hierarchy, since for $\alpha \gg 2$ there are too few effective CROT gates left to define a hierarchy in the first place. In the limit $\alpha \to \infty$, this results in a QFT where the hierarchy is eliminated completely and only Hadamard gates remain. Therefore, the limiting performance for $\alpha \to \infty$ is expected to be the one of a QFT equipped with Hadamard gates only. This point will be discussed further in more quantitative detail below.

2.2 Power-law Hierarchy

Next, we study a power-law hierarchy. Unlike in the exponential case, we can no longer vary a scale factor, since there is no scale factor in a power-law. Instead, we characterize our power-law QFT in the following way:

$$\theta_j \to \tilde{\theta}^j = \frac{\pi}{2^j \beta}, \quad (9)$$

where the form (9) was chosen such that for $j = 1$ both $\theta_j$ and $\tilde{\theta}^j$ are $\pi/2$. In this case the phase of the $n$-qubit power-law QFT with input state $|s\rangle$ and output states $|l\rangle$ reads

$$\Psi_b^P(s; l; \beta) = \exp \left[ i \omega_b^P(s; l; \beta) \right], \quad (10)$$

where

$$\omega_b^P(s; l; \beta) = \pi \left( \sum_{m' = 0}^{n-1} s_{m'} |l_{n-1-m'}\rangle + \sum_{j=1}^{b} \frac{1}{2^j \beta} \sum_{m=0}^{n-j-1} s_{m} |l_{n-j-1-m}\rangle \right), \quad (11)$$
Again using the most-prominent-peak criterion and computing the performance of the QFT on the basis of (10), we plot, in Fig. 2, the resulting normalized performance $P$ of the banded ($b = 8$) power-law hierarchical QFT for revealing the periodicity $\omega = 30$ as a function of $\beta$. As before, the normalization is performed with respect to the absolute performance of the exact QFT with $\alpha = 2$ and $b = 8$.

As shown in Fig. 2, the performance of the power-law hierarchical QFT is qualitatively similar to the performance of the exponentially hierarchical QFT shown in Fig. 1. This time, however, we do not have an intuitive prediction for the location of the maximum of the performance, which occurs at $\beta_0 \approx 1.4$. Surprisingly, although the hierarchy is changed from exponential to power-law, a significant qualitative change in the structure of CROT rotation angles, the peak performance of the power-law hierarchical QFT at $\beta_0$ is significantly larger than 90%. Even for variations of the order of 10% around $\beta_0$ we still obtain better than 90% performance, which drops below 50% only for deviations larger than 30% from $\beta_0$. Arguments similar to the exponentially hierarchical case apply to explain, qualitatively, the behavior of the performance on the left and right wings of the performance curves in Fig. 2.

3 Analytical Results

Analytical analysis of QFT performance on the basis of (7) or (10) is not straightforward. This is due to the intricate nature of the phases $\Phi$ and to the fact that the $s$ values for a given $l$ value in the vicinity of the most prominent Fourier peaks tend to cluster in modulo $2\pi$ space. Still, we can extract some useful information regarding the shape and the location of the maxima of the curves shown in Figs. 1 and 2. Assuming that we obtain the best performance with the banded, otherwise exact QFT ($\alpha = 2$), we see from
In the limit we obtain the minimum of the sum of Gaussian-distributed variables is the sum of their variances [16], change in hierarchy in unison in the statistical sense, and since the variance centered around (in (13) with a Gaussian-distributed variable, whose variance is $\frac{3}{16}$, that the central limit theorem [16] is applicable, we may replace the are random, (b) that $\varphi_b^E(s; t; \alpha = 2)$, respectively. Here, $\var{\ldots}$ denotes the variance in the argument $s$ and $\var{\ldots}$ denotes averaging over $l_{\text{mp}}$. the labels of those integer output states $l_{\text{mp}}$ that are closest to a Fourier peak. Minimizing (i) is straightforward and follows immediately from

$$\varphi_b^E(s; t; \alpha) - \varphi_b^E(s; t; \alpha = 2) = \pi \sum_{j=1}^{b} \left( \frac{1}{\alpha j} - \frac{1}{2 \beta} \right) \sum_{m=0}^{n-j} s_m l_{n-j-1-m}, \quad (12)$$

which shows that minimization is achieved for $\alpha = \alpha_c = 2$, for which the variance is zero. This is consistent with the peak location of the curves in Fig. 1.

Minimizing (ii) is not so straightforward and a more sophisticated approach is required. Let us first state the argument of the variance that is to be minimized:

$$\varphi_b^P(s; t, \beta) - \varphi_b^P(s; t, \alpha = 2) = \pi \sum_{j=1}^{b} \left( \frac{1}{2 \beta j} - \frac{1}{2 \beta j} \right) \sum_{m=0}^{n-j} s_m l_{n-j-1-m}. \quad (13)$$

Assuming (a) that the bits of the binary representations of both $s$ and $l_{\text{mp}}$ are random, (b) that $s_m$ and $l_{n-j-1-m}$ are statistically independent, and (c) that the central limit theorem [16] is applicable, we may replace the $n$-sum in (13) with a Gaussian-distributed variable, whose variance is $3(n - j)/64$, centered around $(n - j)/4$. Assuming further that all $l_{\text{mp}}$ respond to the change in hierarchy in unison in the statistical sense, and since the variance of the sum of Gaussian-distributed variables is the sum of their variances [16], we obtain the minimum of the $l_{\text{mp}}$-averaged variance of (13) for

$$\frac{d}{d \beta} \left[ \pi^2 \sum_{j=1}^{b} \frac{3(n - j)}{64} \left( \frac{1}{2 \beta} - \frac{1}{2 \beta} \right)^2 \right]_{\beta = \beta_c} = 0. \quad (14)$$

In the limit $n \gg b$, since $\min(n - j) = n - b \approx n$, (14) further simplifies to

$$\frac{d}{d \beta} \left[ \pi \sum_{j=1}^{b} \left( \frac{1}{2 \beta} - \frac{1}{2 \beta} \right)^2 \right]_{\beta = \beta_c} = 0. \quad (15)$$
Solving (15) in the case $h = 8$, we obtain $\beta = \beta_\sigma = 1.364$, which is close to $\beta_0 = 1.4$, and therefore consistent with the peak locations of the curves in Fig. 2.

Along the lines of the discussion above it is now straightforward to obtain the approximate shapes of the curves in Figs. 1 and 2. Since, to a good approximation, the $m$-sum in (12) and (13) is Gaussian distributed, together with the fact that the sum of Gaussian-distributed variables is yet another Gaussian-distributed variable [16], we expect the phase angles $\varphi_b^\beta(s; l; \alpha)$ and $\varphi_b^\beta(s; l; \beta)$ with respect to $\varphi_b^\beta(s; l; \alpha = 2)$ to be Gaussian distributed. Now, in order to compute the normalized performance $P$ of the QFT, we first need to sum over the probabilities of obtaining any one of the most-prominent peaks $l^\text{(np)}$ as a result of measurement after performing the QFT, which is computed by taking the absolute square of the sum of $\Phi(s, l^\text{(np)})$, where $\Phi(s, l^\text{(np)})$ may refer either to the exponential case or to the power-law case. Following this, we need to normalize these two results by the banded, otherwise exact, QFT. Denoting the absolute performance of the QFT by $\tilde{P}$, we obtain

$$P_h^{(\text{EP})} (\alpha|\beta) = \frac{\tilde{P}_h^{(\text{EP})} (\alpha|\beta)}{\tilde{P}_h^{(\text{EP})} (\alpha = 2)} = \frac{\sum_{l^\text{(np)}} |\sum_s \Phi_h^{(\text{EP})} (s; l^\text{(np)}; \alpha|\beta)|^2}{\sum_{l^\text{(np)}} |\sum_s \Phi_h^{(\text{EP})} (s'; l^\text{(np)}; \alpha = 2)|^2} ,$$

(16)

where $\text{EP}$ and $\alpha|\beta$ refer to the exponential and power-law cases, respectively.

Invoking the previous assumption that all $l^\text{(np)}$ respond in unison to a change in hierarchical structure in a statistical sense, we may approximate $P_h^{(\text{EP})}$ by dropping the sums over $l^\text{(np)}$ and $l^\text{(np)}$ in (16). Writing $\Phi_h^{(\text{EP})}$ in the form

$$\Phi_h^{(\text{EP})} (\alpha|\beta) = \exp \left[ i \varphi_b^\beta (\alpha = 2) \right] \exp \left\{ i \left[ \varphi_b^\beta (\alpha|\beta) - \varphi_b^\beta (\alpha = 2) \right] \right\},$$

(17)

we find that the first exponential term on the right-hand side of (17) is a slowly varying function of $s$, while the second exponential term on the right-hand side of (17) is a rapidly fluctuating function of $s$. Therefore, assuming statistical independence of the slowly and rapidly fluctuating terms (separation ansatz), we may cancel the first term in (17) against the denominator in (16) to obtain

$$P_h^{(\text{EP})} (\alpha|\beta) \approx \frac{1}{\sqrt{K(s)}} \sum_s \exp \left\{ i \left[ \varphi_b^\beta (\alpha|\beta) - \varphi_b^\beta (\alpha = 2) \right] \right\}^2 ,$$

(18)

where $K(s)$ is the number of terms in the $s$-sum. At this point, we recall that the distribution function of the phase angles of the complex exponentials in (18) is Gaussian. Further approximating the $s$-sum with an integral and extending its limits to $\pm$ infinity, we obtain

$$P_h^{(\text{EP})} (\alpha|\beta) \approx \int_{-\infty}^{+\infty} e^{ix} G_{s_h^{(\text{EP})} (\alpha|\beta)}^\beta dx ,$$

(19)

where $G_{s_h^{(\text{EP})} (\alpha|\beta)}^\beta$ is a normalized Gaussian with standard deviation $\sigma_h^{(\text{EP})} (\alpha|\beta)$, and

$$x \equiv \varphi_b^\beta (\alpha|\beta) - \varphi_b^\beta (\alpha = 2).$$

(20)
Fig. 3 Normalized performance $P$ of the (a) exponentially hierarchical and (b) power-law hierarchical, banded QFT with bandwidth $b = 8$ as a function of the hierarchy parameters $\alpha$ and $\beta$. The lines are the analytical results (21) with (a) $(\sigma^2)^{(E)}$ defined in (22) and (b) $(\sigma^2)^{(P)}$ defined in (23), for qubit numbers $n = 12$ (dashed line), $n = 16$ (solid line), and $n = 20$ (dash-dot line). The numerical data in (a) and (b), computed for $n = 12$ (pluses), $n = 16$ (squares), and $n = 20$ (asterisks) are imported, unchanged, from Figs. 1 and 2, respectively.

Computing the integral in (19), we obtain

$$P_b^{(E|P)}(\alpha|\beta) \approx \exp[-(\sigma^2)^{(E|P)}(\alpha|\beta)],$$

where

$$(\sigma^2)^{(E)} = \pi^2 \sum_{j=1}^{b} \frac{3(n-j)}{64} \left( \frac{1}{2^j} - \frac{1}{\alpha^j} \right)^2 \quad (22)$$

and

$$(\sigma^2)^{(P)} = \pi^2 \sum_{j=1}^{b} \frac{3(n-j)}{64} \left( \frac{1}{2^j} - \frac{1}{2j^2} \right)^2 \quad (23)$$
In Figs. 3 (a) and (b), together with the corresponding numerical data imported from Figs. 1 and 2, we plot (21) with (22) and (23) for the exponential and power-law cases, respectively. While the agreement between theory and numerical results is far from ideal, the analytical lines capture the scaling and the overall shape of the data to a good qualitative approximation. Apparently, away from the performance maxima, in the left and right wings of the performance curves, the analytical curves grossly over-estimate the performance. This, however, is expected since (i) contrary to our simplifying assumptions, and strictly speaking, different \( f^{(np)} \) respond (slightly) differently to alterations in the hierarchy, (ii) the correlations between the two terms on the right-hand side of (17) were neglected (separation ansatz), and (iii) the central limit theorem is only marginally applicable for \( n \sim b \) [see (13) and (14)], which results in only a crude approximation of the distribution of \( \varphi_b^{(E)}(\alpha/\beta) - \varphi_b^{(E)}(\alpha = 2) \) in (18) as a Gaussian. We note that for increasing \( n \), as shown in Figs. 3 (a) and (b), the analytical lines become better approximations, since for increasing \( n \) the statistics improves and the three limitations discussed above become less significant.

4 Discussion

Having explained the locations of peak performance and obtained a qualitative impression of the shape of the performance curves, let us now take a look at the limits \( \alpha \to 1 \) and \( \beta \to 0 \) in which the performances of both modified QFTs are zero (see Figs. 1 - 3). These are the two cases in which the rotation angles \( \theta_j^{(E)} \) in (3) and \( \theta_j^{(P)} \) in (9) of the associated CROT gates are constant as a function of \( j \), the rotation-angle hierarchy is completely wiped out, and zero performance is expected. Quantitatively, we show this in the following way. For \( \alpha = 1 \), \( \varphi_b^{(E)}(s,l; \alpha = 1) \) in (8) is equal to a multiple of \( \pi \). As a consequence, the phases \( \Phi_b^{(E)}(s,l; \alpha = 1) \) in (7) take only two values, \( -1 \) and \( 1 \). Assuming that both \( s_m \) and \( l_{(n-j-1-m)} \) assume the two values \( 0 \) and \( 1 \) randomly as a function of their indices \( m \) and \( n - j - 1 - m \), respectively, we see that \( \Phi_b^{(E)}(s,l; \alpha = 1) \) assumes the values \(-1\) and \(1\) with equal probability. Therefore, the sum over \( \Phi_b^{(E)}(s,l; \alpha = 1) \) in (16) has expectation value zero, explaining the zero performance of the exponentially hierarchical QFT at \( \alpha = 1 \). This explains our numerical results shown in Fig. 1.

Similar arguments hold for the power-law hierarchical case. Here, for \( \beta = 0 \), the phase angles \( \varphi_b^{(P)}(s,l; \beta = 0) \) in (11) are multiples of \( \pi/2 \). Again using the argument of randomness of the binary digits of \( s \) and \( l \), the sum over \( \Phi_b^{(P)}(s,l; \beta = 0) \) in (16) averages out, resulting in zero performance. This explains our numerical results shown in Fig. 2.

Now, let us take the other limit, i.e., \( \alpha \to \infty \) and \( \beta \to \infty \). In this case, \( \theta_j^{(E)} \) in (3) and \( \theta_j^{(P)} \) in (9) are both 0, except for \( \theta_j^{(P)} \), which is \( \pi/2 \). Hence, for the exponentially hierarchical, banded QFT, we expect, in the limit \( \alpha \to \infty \), the
Fig. 4. Normalized performance $P$ of the power-law hierarchical, banded QFT with bandwidth $b = 8$ as a function of the inverse-log hierarchy parameter $\gamma$. Shown are the cases with $n = 12$ (pluses), $n = 16$ (squares), and $n = 20$ (asterisks).

performance corresponding to a pure Hadamard QFT ($b = 0$), i.e., the case in which only Hadamard gates and no CROT gates are present. Also, since for the power-law hierarchical banded QFT the CROT gates with $j = 1$ operate correctly, we expect the performance in this case to be that of the exact QFT with $b = 1$. For $n = 10, \ldots, 20$ we numerically confirm that this is indeed the case. All checks were performed for periodicity $\omega = 30$.

So far in this paper, while varying the hierarchical structure, we have considered the banded QFT. As pointed out earlier, the bandwidth $b = 8$ was chosen since according to [14], a QFT with $b = 8$ is sufficient for its use in code-breaking. While it may be of limited value for practical applications, the exact QFT may still be studied by letting $b = n - 1$ in the analytical results above. In this case, while the qualitative behavior of the performance as a function of $\alpha$ or $\beta$ should remain roughly the same for both the exponential and power-law cases, respectively, we expect a reduction of the peak performance in $\beta$, since the minimum of the variance at $\beta = \beta_c$ [see (14)] is an increasing function of $b$, hence $n$, for the non-banded QFT. Our numerical investigations confirm this expectation.

To further confirm the vital importance of the hierarchy in the QFT, we also investigated the logarithmically hierarchical QFT. Specifically, we chose

$$\theta_j \rightarrow \tilde{\theta}_j^{(L)} = \frac{\pi}{\log_2(j + 1)},$$

where $\gamma$ is a real number. As expected, in Fig. 4, a behavior similar to the one observed in Figs. 1 and 2 emerges when the normalized performance $P$ is plotted against the control parameter $\gamma$ that specifies the strength of the logarithmic hierarchy. Together with the exponential and power-law hierarchy results, this cements previous indications [15] that hierarchy is more important than the precise implementation of gates.
Although our paper is theoretical in nature, it may have significant practical implications for the construction of quantum information processors. Currently, experimental implementations of the QFT are limited to fewer than five qubits [17], although no fundamental laws of physics forbid the scaling up of these quantum processors [18] to reach the number of qubits discussed in this paper. However, while many different physical realizations of the QFT may be envisioned, they all have one problem in common, i.e., how to implement, in a practical way, the phase-rotation angles required to operate the QFT. Here our paper provides the insight that the precise implementation of the theoretically required exponential hierarchy may be unnecessary in practice for building a realistic QFT processor with acceptable performance. We illustrate this observation explicitly with two hierarchies (power-law and logarithmic) that are vastly different, qualitatively and quantitatively, from the exponential hierarchy, but still yield acceptable performance. It stands to reason, therefore, that many other types of hierarchies will achieve the same goal. To emphasize this point even further, we recently investigated yet another hierarchy, which we call the random hierarchy, and which may have a real impact on facilitating actual hardware realizations of the QFT. We generated 100 random phase angles between 0 and $\pi$ and selected those eight phase angles that best matched the phase angles $\pi/2, \pi/4, \ldots, \pi/256$, required for a $b = 8$ QFT. This method emulates a manufacturing process in which quantum gates are generated at random, selecting those that most closely match requirements. Although this process, for some gates, results in very large relative errors, this phase-angle selection process yields astonishingly good performance, better than 90%. This means that experimentalists and engineers do not have to produce or realize quantum gates with a targeted specification in mind, but may produce quantum gates at random, choosing the best matches, irrespective of relative error, according to a method of selection. To emphasize our point, we reduced the number of random rotation angles generated to 20 in the interval $[0, \pi]$, which resulted in even larger individual phase-angle errors, but still resulted in a performance of better than 80%. More details of this method will be published elsewhere [19].

We also mention the fact that some quantum error correction schemes [3] require the resolution of rotation gates into a sequence of elementary, universal gates [20–25]. Realizing the exponential hierarchy with accuracy $\epsilon$ is expensive and requires gate sequences of length $\sim \log(1/\epsilon)$ [22]. However, our latest results on the random hierarchy teach us that it is not necessary to decompose each rotation gate to within a stringent $\epsilon$ requirement, but that the QFT still works using selected gates from a random set. This procedure may be re-interpreted as a much relaxed $\epsilon$, resulting in much shorter, decomposed realizations of quantum rotation gates that are much easier, and in particular cheaper, to implement.

Thus, based on the results in this paper, experimentalists and quantum engineers may take advantage of some significant quantum short-cuts resulting in tremendous anticipated savings in quantum resources. The best economy of resources is obtained as a result of a process that optimizes between target...
QFT performance and the optimal choice of hierarchy that best achieves the desired QFT accuracy with the minimal requirement of quantum resources.

5 Conclusion

This research was motivated by Landauer [1], who clearly separated the adverse effects experienced by a quantum processor into two logically and physically independent classes: decoherence and hardware flaws. While decoherence may be dealt with using quantum error correction [3–8], flaws in the hardware implementation of quantum gates are of a different nature. In fact, the effect of hardware flaws may be considered more fundamental than decoherence, since the issue of decoherence is a moot point if, for proper functioning of some quantum processor, the hardware tolerances can be proved to be too stringent to even consider practical implementation of the processor.

Since in the absence of decoherence any quantum processor may be interpreted as a unitary transformation of input states into output states governed by a quantum Hamiltonian, the effect of flaws in the hardware implementation of a quantum processor may be interpreted as a new quantum processor with an altered Hamiltonian, executing a different unitary transformation. Whether the new unitary transformation produces desirable results that are close to those produced by the original, intended Hamiltonian, depends on whether the original Hamiltonian governing the quantum processor is structurally stable. Structural stability is a term derived from dynamical systems theory [26] and refers to Hamiltonian systems in which small perturbations of the Hamiltonian lead to only small changes in the dynamics governed by the Hamiltonian. In this spirit, investigating the structural stability of the QFT, we changed the structural form of the phase rotation angles of the QFT’s CROT gates and computed the resulting change in performance of the QFT thus perturbed. The central result obtained is that even drastic alterations of the hierarchical structure of the QFT’s phase rotation angles do not significantly diminish the performance of the QFT. This result is astonishing since the altered QFT, from a number-theoretical point of view, is the QFT for a number system that is no longer binary, but rather a number system defined according to $\nu = \sum_j \phi_j x_j$, where $\phi_j$ is 0 or 1 and $x_j$ may be $1/x^j$, $1/j^\alpha$, or $1/\log_j(j+1)$, or any other choice, if desired. As an example, let us look at the number system $\nu = \sum_j \phi_j (1/3)^j$. In this case the set $\nu$ is isomorphic to the well-known middle-thirds Cantor fractal [26], which has measure zero in the set of real numbers. As a consequence, the numbers $\nu$ that are actually representable in this number system, although uncountable, are a vanishing fraction of all real numbers in the unit interval. This means that this “1/3 number system”, which in our context corresponds to $\alpha = 3$, is vastly incomplete. Viewed in this light, it is even more astonishing that the corresponding QFT performs at all, and, in fact, operates with greater than 10% efficiency.

Thus, our structural studies presented in this paper are fundamentally different from our studies of random, static gate defects [15], in which the binary
number system, including its completeness, still hold. Thus, combined with our earlier results on the stability of the QFT with respect to static gate defects [15], the structural stability with respect to changes in the gate rotation angle hierarchy shows that the QFT is stable against all major flaws in potential future hardware implementations of the QFT and manufacturing tolerances may be relatively relaxed in the actual production of future quantum hardware.

References

Addressing Landauer’s question concerning the influence of static gate defects on quantum information processor performance, we investigate analytically and numerically the case of the quantum Fourier transform (QFT) with defective controlled rotation (CROT) gates. Two types of defects are studied, separately and in combination: systematic and random. Analytical scaling laws of QFT performance are derived with respect to the number of qubits $n$, the size $\delta$ of systematic defects, and the size $\epsilon$ of random defects. The analytical results are in excellent agreement with numerical simulations. In addition, we present an unexpected result: The performance of the defective QFT does not deteriorate with increasing $n$, but approaches a constant that scales in $\epsilon$. We derive an analytical formula that accurately reproduces the $\epsilon$ scaling of the performance plateaus. Overall, we observe that the CROT gates may exhibit static and random defects of the order of 30% and larger, and still result in satisfactory QFT performance. Thus we answer Landauer’s question in the case of the QFT: far from being lethal, the QFT can tolerate tremendous static gate defects and still perform its function. The extraordinary robustness of the QFT with respect to static gate defects displayed in our numerical and analytical calculations should be a welcome boon for laboratory and industrial realizations of quantum circuitry.

Keywords: Quantum Fourier Transform, Performance, Defects

Communicated by: R Cleve & G Milburn

1 Introduction

Unless its operation is trivial, any quantum information processor, if it is designed to communicate its output to the “classical” world of our everyday existence, is necessarily a probabilistic device. Therefore, how well it performs under realistic conditions, is primarily a function of the probability of success with which it returns a desired result. While ultimately the speed of execution might also play a role in characterizing the performance of a quantum information processor, for the purposes of this paper, it is sufficient to define performance as the success probability of a quantum information processor to deliver a desired result in a
single run of the processor. Realistically, when operating a quantum information processor, i.e., a physical realization of a quantum algorithm, there are many different kinds of noise and circuit defects, static and dynamic, that may negatively impact the performance of the processor. Well-known negative influences, e.g., are quantum decoherence [1] and unwanted coupling between qubits [2]. An early list of mechanisms and effects that may be fatal for quantum computing was compiled by Landauer [3]. Manufacturing flaws in the physical implementations of quantum gates is one of the adverse mechanisms stressed in [3] and forms the main topic of investigation of this paper. We call these manufacturing flaws static gate defects [4], and, from the outset, it is indeed not clear how sensitively the performance of a quantum information processor reacts to static imperfections of its gates. Taking the controlled rotation gate (CROT) as an example: how accurately does the rotation angle have to be implemented for the processor to work with satisfactory performance? How does the performance scale with the size of the gate errors and the number of qubits?

In this paper we answer these questions quantitatively for the case of the quantum Fourier transform (QFT) as a specific example of a quantum information processor with static defects in its CROT gates. Since the purpose of the QFT is to find the embedded periodicity of an input state, we define our performance measure as the success probability of finding the periodicity (see Sec. 3 for detail).

Typically, a QFT circuit, both the coherent two-qubit version [1] and the semiclassical version [5], contains controlled rotation (CROT) gates, rotating the phase angle of qubit number \( t \) (the target qubit) by an angle \( \theta_j \), if the control qubit \( c \) is in state \( |1\rangle \). The rotation angle \( \theta_j \) is given by [1]

\[
\theta_j = \frac{\pi}{2^j}, \tag{1}
\]

where \( j = |t - c| \).

Previously [4, 6], in a first attempt at addressing Landauer’s question [3] of what happens to the performance of quantum circuits if they are not precisely implemented, but exhibit static defects, we subjected the QFT to four different classes of static defects in the CROT gates, characterized by \( \theta_j \rightarrow \theta_j + R \), where \( R \) is a random number. Four different cases were studied in detail [4, 6], characterized by whether \( R \) is correlated with \( j \) or not, or whether \( R \) is an absolute or a relative error.

In this paper we relax the condition of symmetric (on average) perturbation around the exact CROT rotation angle (1) and, in addition to random defects, introduce a systematic offset angle such that the class of static defects to be studied takes the form

\[
\theta_j \rightarrow \tilde{\theta}_j = \frac{\delta + \epsilon r}{2^j}, \tag{2}
\]

where \( \delta \) is the offset, \( \epsilon \) denotes the random defect strength, and \( r \) is a flat-distributed random variable taking values between \(-1\) and \(1\), not correlated with \( j \). This means that each CROT gate of type \( j \) in the circuit will have a different rotation angle \( \tilde{\theta}_j \) that corresponds to a different realization of the random variable \( r \). This is closest to a possible experimental realization of the QFT, where successive gates, even if they are of the same type (same \( j \)) will, in general, have different defects. The exact, defect-free case is included and corresponds to the case \( \delta = \pi \) and \( \epsilon = 0 \).
The introduction of the static offset \( \delta \) is not just an incremental change with respect to the case of purely random defects, since \( \delta = 0, \epsilon \neq 0 \), e.g., corresponds to truly random CROT gates, and, for \( 0 < \delta \ll 1 \), the effects of a small positive offset in angle, masked by large random defects, may be studied. The surprise here is that acceptable performance is already achieved in cases where \( \delta \) is small but \( \epsilon \) is larger than \( \delta \), seemingly overpowering the average drift \( (\delta \neq 0) \) toward the exact rotation angle \( \pi \).

Apart from deriving performance scaling laws for static defects that include systematic errors, we also report a qualitatively new phenomenon. Although, with increasing number of qubits, an increasing number of defective CROT gates are added into the QFT circuit, the performance of the circuit does not deteriorate, but approaches a plateau. This observation is counterintuitive and quite unexpected. It holds strictly in the ideal case where external influences on the QFT circuit, such as ambient noise, are neglected. The presence of ambient noise breaks the plateau behavior at a critical number of qubits \( n_c \) that depends on the ambient noise level. However, \( n_c \to \infty \) for noise level \( \to 0 \).

We shall see that the QFT circuit exhibits astonishing resilience to static gate defects, even if the circuit consists of thousands of qubits, relevant for applications in quantum cryptography [1]. This may be of importance for all researchers and engineers who are interested in designing and building quantum information and computation hardware based on the gate model of quantum computing.

Our paper is structured in the following way. First, in Sec. 2, we briefly review some historical backgrounds pertaining to the performance of the QFT with respect to gate defects and justify our choice of defect model. We also clarify the fundamental difference between spontaneous, correctable errors introduced by decoherence and systematic, uncorrectable errors introduced by faulty hardware. In Sec. 3, we numerically study the performance of the QFT circuit equipped with defective CROT gates. We will see that acceptable performance is obtained for large \( \epsilon \) even if \( \delta \) is small. In Sec. 4, we investigate how the performance of the QFT depends on the number \( n \) of qubits. It is in this section that we encounter the plateauing phenomenon, i.e., the fact that the performance of the QFT stays high for increasing \( n \) even though the quantum state is processed by an increasing number of defective gates. Then, in Sec. 5, we derive an analytical scaling law for the performance of the QFT with defective CROT gates. We discuss our results in Sec. 6, and summarize and conclude our paper in Sec. 7.

2 Our defect model in the historical context

The problem of fragility of quantum computing has been pointed out by many physicists since the inception of quantum computing. In particular, Landauer [3] was among the first to compile a list of physical processes that may prove detrimental to quantum computing. Since then, much effort has been devoted to overcoming many of the obstacles pointed out by Landauer, culminating in novel paradigms such as quantum error correction and fault-tolerant quantum computing (see [7] and references therein). Furthermore, in the pursuit of a full-scale, physical quantum computer, useful for practical purposes, many numerical studies of the QFT have been performed throughout the past decades, for instance the investigation of approximation techniques [8, 9, 10], the effects of imprecise quantum operations [11, 12], and modeling the effects of decoherence [9, 12, 13].
The recent discovery of surface codes and their ingenious working principle further illustrate the relentless efforts toward making quantum computing a practical reality. By encoding logical quantum information in a non-local degree of freedom, surface codes allow us to detect and localize local errors occurring on physical qubits that realize a logical qubit. This results in an astonishingly improved level of protection of quantum information, raising the threshold level, i.e., the maximal physical, unencoded error rate that may be tolerated to still result in a lower logical, encoded error rate, to 1% [14]. With the availability of software such as LIQUID [15] and AutoTune [16, 17], the research frontiers continue to determine experimental targets that quantum hardware should aim for, and anticipated further developments will be of interest to many quantum engineers and experimentalists.

Among the numerous investigations available in the literature, we find that our work is most closely related to the works of Coppersmith [8], Barenco et al. [9], and Fowler and Hollenberg [10]. Coppersmith, in 1994 [8], discovered that the QFT may be approximated with banding, i.e., removing all rotation gates $\theta_j = \pi/2^j$ with $j > b$, where $b$ is the chosen bandwidth, without suffering from significant loss of performance for a sufficiently large $b$. Followed by Barenco et al. in 1996 [9], the QFT was then further investigated, this time subjected to both banding and decoherence, modeled by extra phase-angle rotations applied every time the phase rotation gate $\theta_j$ was applied. This, in fact, corresponds closely to one of the four types of defects studied in [4], where, in addition, an explicit analytical scaling result is reported. A more extensive numerical simulation was then performed by Fowler and Hollenberg in 2004 [10]. Not only was the QFT affected by banding and extra phase-angle rotations similar to the cases studied in [9], but was also the justification for the choice of the noisy rotation gate model provided, this time with fault-tolerant construction of the gates in mind.

Our work attempts to extend this line of research in the following way. First, quantum error correction will be a crucial component of an implementation of a quantum computer, and will require significant additional resources in terms of qubits and quantum gates. Each logical qubit is represented by a set of physical qubits and each logical quantum gate is replaced by a fault-tolerant operation on the physical qubits. For a given quantum error correction code, only a discrete set of rotation gates can be implemented fault-tolerantly. Therefore, each rotation gate must be decomposed into a sequence of gates drawn from the fault-tolerant basis. According to the Solovay-Kitaev theorem, if the basis is universal, then such a sequence can always be found [18]. Now, the obtained sequence, of course, results in an approximate rotation gate, provided that the sequence has to be finite. While recent developments in techniques and new methods of decomposition [19, 20, 21, 22, 23] allows us to straightforwardly obtain the sequence with an arbitrarily chosen accuracy (see for instance [24] for open-source software), the fact that the resulting rotation is approximate remains true. Thus, considering that resources required for quantum error correction are demanding, investigating how sensitively a quantum computer (in our case the QFT) reacts to deviations from the exact operation of its rotation gates becomes important, as low sensitivity can help ease the accuracy requirement, which implies a step forward into the direction of practical quantum computing.

While fault-tolerant implementation via sequence decomposition and surface codes allow us to fight many types of errors [14], including some of the systematic [25] and intrinsic
[26, 27, 28] types, some errors will always remain in quantum gates and states. This is obvious, since, in general, an error correcting code never fully restores the corrupted state; rather when compared to the unencoded counterparts, the encoded one performs better [7, 29]. Accordingly, in practice, there will always be some residual errors left in individual decomposed gates of a rotation gate, for instance, and they will (differentially) accumulate through the pulse sequences. It is then interesting to see how the QFT circuit, used in many algorithms, performs under various types of errors, which forms the main topic of this paper. If the QFT is very tolerant to these errors, this in turn means we may relax required precision, saving on quantum resources. The exact description of these errors will of course be hardware dependent, and we will learn more about the expression of the errors as hardware advances. For now, without the availability of the hardware at present, we conclude that our model of the rotation gate in (2) closely models an actual experimental realization. The strengths and of systematic and random errors may then be adjusted to reflect the actual, physical realization architecture of the quantum gate. The more general case, modeled by a general $2 \times 2$ unitary matrix, will be discussed briefly in Sec. 6.

3 Defective Phase Rotation Gates

The exact $n$-qubit QFT of an integer input state $|a\rangle$ is defined as

$$|a'\rangle = \frac{1}{\sqrt{2^n}} \sum_{b=0}^{2^n-1} \Phi(a, b) |b\rangle,$$

(3)

where

$$\Phi(a, b) = \exp(2\pi i ab/2^n)$$

(4)
is the associated normalized phase between the input state $|a\rangle$ and the output state $|b\rangle$. Constructing (4) on a gate–by–gate level, we obtain

$$\Phi(a, b) = \prod_{m=0}^{n-1} e^{i\pi a[m] b[n-m-1]} \prod_{j=1}^{n-1} \prod_{l=0}^{n-j-1} e^{i a[j] b[n-j-l-1] \theta_j},$$

(5)

where $\theta_j$ is defined in (1), and the subscript $[\ldots]$ of $a[m]$ and $b[n-m-1]$ denotes the $m$th and $(n-m-1)$th binary digit of $a$ and $b$, respectively. We note that the $m$ product in (5) arises from the Hadamard operations in the QFT, and the $j$ and $l$ products are due to the CROT gates in the QFT.

In this paper we study the QFT equipped with defective CROT gates, i.e., we replace the exact rotation angle $\theta_j$ in (5) with the modified angles $\tilde{\theta}_j$, defined in (2). Clearly, the introduction of defects into the CROT gates of the QFT reduces the ability of the QFT to detect the periodicity $\omega$ of an input state. We call the success probability with which $\omega$ can be determined in a single run of the QFT the performance of the QFT. For simplicity we compute the success probability as the probability $\tilde{P}$ of finding the periodicity $\omega$ of an input state with a single run of classical post processing (CPP$_1$) via the continued fraction method [1]. In order to form a first impression of how static defects affect the performance of the QFT, we choose $n = 10$ and $\omega = 30$ and plot in Fig. 1 the performance $\tilde{P}$ of the defective QFT, obtained via CPP$_1$, as a function of $\delta$ for three different values of $\epsilon$. 

Appendix A. List of Publications

Y. S. Nam and R. Blümel
Performance scaling of the quantum Fourier transform with defective rotation gates

Fig. 1. Success probability $\tilde{P}$ of finding the periodicity $\omega = 30$ with a 10-qubit, defective QFT as a function of rotation-angle offset $\delta$. Shown are three cases with random defect strengths $\epsilon = 0$ (pluses), $\epsilon = 0.5$ (crosses), and $\epsilon = 1$ (asterisks). Smooth, dashed, interpolation lines are drawn through the data points to guide the eye. The horizontal line corresponds to the pure-chance performance of the QFT.

Fig. 2. Success probability of finding the periodicity $\omega = 30$ with a 14-qubit, defective QFT as a function of rotation-angle offset $\delta$. Shown are three cases with random defect strengths $\epsilon = 0$ (pluses), $\epsilon = 0.5$ (crosses), and $\epsilon = 1$ (asterisks). The smooth, dashed lines are imported from Fig. 1 to show that the widths of the performance peaks centered around $\pm \pi$ are not altered. The horizontal line corresponds to the pure-chance performance of the QFT.
Clearly, according to Fig. 1, the performance sacrifice is less than 50% when we shift by up to $\pm \pi/3$ away from the peak locations at $\pm \pi$. This is surprising since the result points to the fact that we can use rotation gates with large defects in actual hardware implementations of the QFT circuit, and are still able to find the periodicity $\omega$ with reasonable probability. In order to further confirm this observation, we show, in Fig. 2, the numerical results of the performance of the QFT with $n=14$ and $\omega=30$. Surprisingly, as demonstrated by the dashed lines in Fig. 2, imported from Fig. 1, the performance is nearly identical to the case with $n=10$ (see Fig. 1). In particular, the widths of the performance peaks around $\delta=\pi$ (the $\delta$ corresponding to the exact QFT), are unaltered.

Another surprising observation, found in both Figs. 1 and 2, is the fact that even for $\omega=0$, which corresponds to completely random CROT gates, we obtain a positive performance of the defective QFT of about 3%. This may be contrasted with the pure-chance performance of the QFT, which is obtained by assuming that each output state appears with equal probability. In this pure-chance case, the QFT is about 1% effective. Therefore, at $\delta=0$, the 3% performance of the defective QFT is clearly significant compared to the pure-chance case. The 2% difference is explained by the action of the Hadamard gates.

4 Performance scaling: numerical results

The question of why the interpolation lines in Fig. 1 represent the data points in Fig. 2 so well is hard to answer analytically. Numerically, however, we find a new phenomenon that corroborates this observation. In Fig. 3, we plot the performance $\tilde{P}$ for a fixed periodicity $\omega=30$ and fixed offset $\delta=\pi$ as a function of the number of qubits $n$ of the defective QFT for four different defect strengths $\epsilon$. We see that for all $\epsilon$ shown in Fig. 3, the performance $\tilde{P}$ quickly reaches a plateau for increasing $n$. This is unexpected since, naively, one might think that more qubits $n$ lead to more defective CROT gates, which pick up more errors, and thus reduce the performance. Heuristically, we obtain the following functional form of the plateaus

$$\tilde{P}_{n\to\infty}(n, \omega, \epsilon) = \tilde{P}_{n\to\infty}(n, \omega, \epsilon = 0) e^{-\gamma \epsilon^2},$$

represented by the solid lines in Fig. 3. This behavior may be explained in the following way.

First, $\tilde{P}_{n\to\infty}(n, \omega, \epsilon = 0)$ is expected to be

$$\tilde{P}_{n\to\infty}(n, \omega, \epsilon = 0) = \frac{\nu(\omega)}{\omega},$$

where $\omega$ is the periodicity of the input state and $\nu(\omega)$ is the co-prime counting function that returns the number of co-primes of $\omega$ that are larger than 0 and smaller than $\omega$. This is so, since the CPP$_1$-based performance criterion essentially picks those Fourier peaks, say indexed with $q$, whose indices are relatively prime to $\omega$. Since the index $q$ runs from 0 to $\omega-1$ inclusively, and the effective probability contribution that the $q$th peak and its vicinity represent is approximately $1/\omega$ for an exact QFT, we obtain (7). We note that for the current case of $\omega=30$, $\nu(\omega=30) = 8$, i.e., $\tilde{P}_{n\to\infty}(\omega=30, \epsilon = 0) = 8/30$. The initial sub-plateau performance for small $n$ (see Fig. 3) is also expected since in such cases the classical post-processing criterion does not include enough vicinity around the useful $q$th peak.

The $\epsilon$-scaling in (6) is motivated by the $\epsilon$-scaling results obtained in Ref. [4]. We have previously shown [4] that the effect of random defects with strength $\epsilon$ on the normalized
8 Performance scaling of the quantum Fourier transform with defective rotation gates

![Graph](image)

Fig. 3. Success probability of finding the periodicity $\omega = 30$ with an $n$-qubit QFT with fixed $\delta = \pi$ as a function of the number of qubits $n$. Shown are four cases with random defect strengths $\epsilon = 0$ (pluses), $\epsilon = 0.1$ (crosses), $\epsilon = 0.2$ (asterisks), and $\epsilon = 0.3$ (squares). The solid lines are the analytical prediction (6) with $\gamma = 1.25$ and $P_{n \to \infty}(\omega = 30, \epsilon = 0) = 8/30$.

performance $P = \hat{P}(\epsilon)/\hat{P}(\epsilon = 0)$, of a quantum computer equipped with a defective QFT is Gaussian, i.e., the normalized performance $P$ of the quantum computer decreases according to a Gaussian function in $\epsilon$. The difference with respect to [4] is that, in the current paper, the success criterion incorporates the classical post-processing criterion CPP, a more advanced success criterion compared with the non-trivial nearest-peak criterion used in Ref. [4]. Therefore, while we expect that the Gaussian functional form in $\epsilon$ carries over, it is not justified to use the analytical result for the coefficient $\gamma$ of $\epsilon^2$ as computed in Ref. [4] in (6). As a consequence, we leave $\gamma$ as a free fit parameter. For the specific case of $\omega = 30$, we find $\gamma = 1.25$.

5 Performance scaling: analytical results

Having identified the reasons for why the performances of the defective QFTs with $n = 10$ and $n = 14$ qubits are nearly identical (see Figs. 1 and 2), we now continue our investigation of performance scaling in $n$, $\delta$, and $\epsilon$, with an emphasis on analytical results. It is of utmost importance to assess the behavior of the width of the performance peaks in Figs. 1 and 2 as a function of $n$, since practical implementations of the QFT will always be realized with real-world CROT gates that have some non-zero defects. If the peaks would narrow quickly, say exponentially, as a function of $n$, we would have to impose impossibly small defect tolerances on the CROT gates of the QFT to be of any use in practical applications. Luckily, as we shall see, this is not the case. As already indicated by Figs. 1 and 2, the following analytical calculations will show that the width of the performance peaks stays constant as a function of $n$. In order to show this, and in order to get an analytical grip on the problem, we start by defining the normalized performance proxy

$$\hat{P}(s_0, \delta) = \frac{1}{K(s_0)} \sum_{k=0}^{K(s_0)-1} \hat{\Phi}(s_0 + k\omega; \hat{b}, \delta)$$

(8)
where $K(s_0)$ is the number of elements of the equivalence class $[s_0]$ that comprises the integers $s_0 + k \omega < 2^n$, where $k \geq 0$ is an integer, $b$ is the proxy output state, and $\hat{\Phi}$ denotes the amplitude defined in (5), where the exact phase angle $\theta_j$ defined in (1) is replaced by $\tilde{\theta}_j$ defined in (2). For the time being we will also set $\epsilon = 0$. According to (8), the performance proxy is the probability to obtain $\tilde{b}$ as the result of a measurement of the output state of the defective QFT. The probability $\hat{P}(s_0, \delta)$ is a “proxy” measure because $|\tilde{b}|$ is assumed to represent all other states that may be obtained with high probability as the result of a measurement of the QFT output state, and it is assumed additionally that classical post processing of $\tilde{b}$ reveals $\omega$ with certainty. Currently, both assumptions are necessary to make any analytical headway in the analysis of the performance scaling of the defective QFT for large $n$. Both assumptions are benign, since we checked previously [4, 6, 30] that (i) the probability of obtaining output states $|b\rangle$ in the vicinity of a main Fourier peak produced by the QFT, i.e., the set of states from which the proxy state $|\tilde{b}\rangle$ is chosen, are correlated in the sense that they respond in unison to the introduction of static defects into the gates of the QFT, and (ii) the probability of obtaining $\omega$ via classical post-processing from any of the states $|b\rangle$ close to a main Fourier peak is indeed 1 or close to 1.

The central ingredient in the proxy measure $\hat{P}(s_0, \delta)$ defined in (8) are the amplitudes $\hat{\Phi}(s_0 + k \omega, \tilde{b}, \delta)$ and it is convenient to define the phases $\Delta(k, \delta)$ according to

$$
\hat{\Phi}(s_0 + k \omega, \tilde{b}, \delta) \equiv e^{i\Delta(k, \delta)}.
$$

Evaluating the amplitudes $\hat{\Phi}$ for the special case $\delta = 0$, we notice that there are two equivalence classes, denoted by $[[1]]$ and $[[-1]]$, depending on whether $\hat{\Phi}(s_0 + k \omega, \tilde{b}, \delta = 0)$ evaluates to 1 or to $-1$ for given $s_0 + k \omega$ and $\tilde{b}$. Since for $\delta = 0$ (and $\epsilon = 0$; see assumptions above) only the $m$ product in (5) is active, whether $\hat{\Phi}(s_0 + k \omega, \tilde{b}, \delta = 0)$ is 1 or $-1$ depends entirely on the number of non-zero $(s_0 + k \omega)[m](1)\tilde{b}[n-m-1]$ terms in the exponent of the $m$ product in (5). We also note that the phases $\Delta(k, \delta = 0)$ take only two values. We denote them by $\Delta_1(k, \delta = 0) = 0$ for amplitudes in equivalence class $[[1]]$ and $\Delta_{-1}(k, \delta = 0) = \pi$ for amplitudes in equivalence class $[[-1]]$.

We now examine the amplitudes $\hat{\Phi}(s_0 + k \omega, \tilde{b}, \delta)$ in the other special case, i.e., $\delta = \pi$. Recalling that we currently have $\epsilon = 0$, $\delta = \pi$ is the case in which the QFT is exact. In this case, in order to produce the sharp peaks in $b$, characteristic for the exact QFT, all amplitudes $\hat{\Phi}(s_0 + k \omega, \tilde{b}, \delta)$, independent of $k$, have nearly the same value, which corresponds to a sharp clustering of the phases $\Delta(k, \delta = \pi)$ around a constant, denoted by $\Delta_\pi$.

We now turn to the general, interpolating case, i.e., we examine the amplitudes $\hat{\Phi}(s_0 + k \omega, \tilde{b}, \delta)$ in the $\delta$ interval $0 < \delta < \pi$. Apparently, switching from $\delta = 0$ to $\delta = \pi$, the phases $\Delta_1(k, \delta = 0) = 0$ and $\Delta_{-1}(k, \delta = 0) = \pi$, corresponding to the equivalence classes $[[1]]$ and $[[-1]]$, have to coalesce into the single phase $\Delta_1(k, \pi) = \Delta_{-1}(k, \pi) = \Delta_\pi$ at $\delta = \pi$. We confirmed numerically that the phase difference between the amplitudes of the two equivalence classes $[[1]]$ and $[[-1]]$ is a decreasing function of $\delta$, and moreover that it is linear according to

$$
\Delta_{-1}(k, \delta) - \Delta_1(k, \delta) = \pi - \delta.
$$

We check immediately that this formula reproduces the correct results in the two special cases $\delta = 0$ and $\delta = \pi$. Denoting by $\mu_1(s_0)$ and $\mu_{-1}(s_0)$ the number of elements of the two
equivalence classes $[[1]]$ and $[-1]$, respectively, the performance proxy (8) may be evaluated directly with the result

$$
\hat{P}(s_0, \delta) = \frac{\mu_1(s_0)^2 + \mu_{-1}(s_0)^2 + 2\mu_1(s_0)\mu_{-1}(s_0)\cos(\pi - \delta)}{K(s_0)^2}.
$$

(11)

This formula shows that the performance of the QFT with respect to $\delta$ is independent of $n$. Hence, the analytical formula (11), which is $n$-independent, supports our numerical result (see Sec. 3) that the width of the peaks in Fig. 1 and 2 stays constant when $n$ is increased from $n = 10$ to $n = 14$. The main power of (11), however, is that it is not only applicable in the low-$n$ case (for instance $n = 10$, $n = 14$) but is valid in the large-$n$ case (for instance $n \sim 1000$), not reachable by numerical calculations. We note that the worst case scenario [the minimum of $\hat{P}(s_0, \delta)$ under the constraint $\mu_1(s_0) + \mu_{-1}(s_0) = K(s_0)$] occurs for $\mu_1 = \mu_{-1}$, in which case the performance proxy simplifies to

$$
\hat{P}^{(W)}(\delta) = \frac{1 + \cos(\pi - \delta)}{2},
$$

(12)

which, up to a normalization factor, captures the behavior of $\hat{P}$ in Figs. 1 and 2 reasonably well.

Although the theory developed above assumes $\epsilon = 0$, it also works for non-zero $\epsilon$. We see this in the following way. Replacing $\tilde{\theta}_j$ in (5) with $\tilde{\theta}_j$ [see (2)], we may write approximately

$$
\Phi(a, b) \approx \prod_{m=0}^{n-1} e^{ia[n-m\delta]} \prod_{j=1}^{n-1} \prod_{l=0}^{n-j-1} e^{ia[n-i-j-l]\delta / 2l} \prod_{j'=1}^{n} \prod_{l'=0}^{n-j'\delta / 2l'}
$$

(13)

where we expanded the double product over $j, l$ into a quadruple product over $j, l, j', l'$, assuming that, because of the near statistical independence of $a[n-i-j-l \delta]$ and $a[n-i-j'-l' \delta]$, the off-diagonal elements average to a total factor 1, effectively reducing the quadruple product to the original double product on average. The form (13) of $\Phi(a, b)$ has the advantage that for $\delta = \pi$ the product in (13) for an input state with periodicity $\omega$ has already been evaluated in [4] and the resulting performance, consistent with the notation in Sec. 5, was denoted by $P(n, \omega, \epsilon)$. Thus, assuming that $\delta$ is close enough to $\pi$ that the phase angles resulting from the $m, j, l$ products for $\delta \neq \pi$ are still closely clustered (as is the case in the exact QFT), the double product over $j', l'$ in (13) results in $\hat{P}(n, \omega, \epsilon)$ and the normalized performance $P$ of the QFT may be written in the form

$$
P \approx \hat{P}(s_0, \delta) \frac{\hat{P}(n, \omega, \epsilon)}{\hat{P}(n, \omega, \epsilon = 0)}.
$$

(14)

In the limit $n \to \infty$, using (6), we obtain

$$
P_{n \to \infty} \approx \hat{P}(s_0, \delta) e^{-\gamma^2},
$$

(15)

which applies if the success criterion is based on CPP. Since $\hat{P}$ is normalized to 1 at $\delta = \pi$ and $\epsilon = 0$, $P_{n \to \infty}$ may now be written approximately in the form

$$
P_{n \to \infty}(\delta, \epsilon) \approx \left[ \frac{1 + \cos(\delta - \pi)}{2} \right] e^{-\gamma^2},
$$

(16)
where we used \( \hat{p}^{(W)} \) of (12). The analytical formula (16) qualitatively explains the double-hump structure in Figs. 1 and 2. It also explains why the widths of the peaks in Figs. 1 and 2 are constant, independent of \( \varepsilon \).

Formula (13) predicts \( P_{n \to \infty}(\delta, \varepsilon) = 0 \) for \( \delta = 0 \), independent of \( \varepsilon \), while Figs. 1 and 2 show a positive performance of the defective QFT of about 3%. This positive offset, previously explained due to the action of the Hadamard gates, is still included in formula (11). It disappeared in (16) only because we used the worst-case performance estimate (12) as input for (16). Still, in terms of an estimate and in terms of a concise analytical formula, a 3% underestimate of the actual performance of the defective QFT by (16) is acceptable.

In general, (16) may be used as a convenient first estimate of the performance of the defective QFT in situations where classical simulations are too expensive or simply impossible to perform.

6 Discussion

Generally in quantum computing and quantum information processing, analytical results are necessary since the \( n \)-regions of practical interest, i.e., \( n \) of the order of 1000 [1, 31], are completely inaccessible to numerical simulation on classical, digital computers. Thus, only analytical techniques are powerful enough to explore these large-\( n \) regions. Following this line of reasoning, we derived the scaling law (16) of the performance of the QFT equipped with defective CROT gates as defined in (2). Since \( \gamma \) in (16) is a free parameter when the performance measure is based on CPP\(_1\) instead of using the nearest non-trivial peak criterion as in Ref. [4], we need to better understand how \( \gamma \) behaves as a function of \( \omega \). To this end, we plot, in Fig. 4 (plus symbols), \( \gamma(\omega) \) for all \( \omega \) ranging from 3 to 30, excluding powers of 2, for which \( \gamma = 0 \) (since the QFT performs perfectly in these cases, independently of \( \varepsilon \) [4, 6, 30]). The dotted line \( \sim \ln(\omega) \) in Fig. 4 is drawn to guide the eye. It suggests that \( \gamma \) scales logarithmically in \( \omega \) on average.

An important remark regarding \( \gamma \) is to be noted here. Although in Ref. [4] we derived analytically that \( \gamma \) is a constant, strictly speaking, even with the nearest-peak criterion, the coefficient \( \gamma \) carries an \( \omega \)-dependence. In fact, we find that the dependence of \( \gamma \) on \( \omega \) for the nearest-peak criterion is nearly identical to that found in Fig. 4, i.e., \( \gamma \sim \ln(\omega) \). This discrepancy between the analytical, constant \( \gamma \) and the numerical, \( \omega \)-scaling \( \gamma \) arises, because the analytical procedures used in Ref. [4], which yield the performance scaling formula that is \( \omega \) independent, assume statistical independence wherever possible, i.e., the problem of solving for the performance scaling of the defective QFT is essentially reduced to how much drift in phase angle one obtains in (5) for a single integer input state toward a single integer output state. Since the multiplicity of the integer states for a periodic input state is then taken into account via an averaging process, together with the same procedure applied to the output state, the analytical performance scaling formulas in Ref. [4] are then \( \omega \) independent. As is correctly pointed out in Ref. [4], the \( \omega \)-dependence arises by taking the \( \omega \)-induced residual coupling into account, effectively resulting in \( \gamma \to \gamma(\omega) \). This modification is \( n \)-independent, as demonstrated in Fig. 8 of Ref. [4], which is consistent with our observations in Fig. 4 that \( \gamma \), for a given \( \omega \), is (trivially) independent of \( n \).

Previously, in Ref. [30], in connection with Shor’s algorithm, we showed that the periodicities \( \omega \) associated with the semiprimes \( N \) to be factored scale exponentially in \( n \), where \( n \) was
Performance scaling of the quantum Fourier transform with defective rotation gates

chosen such that it scales linearly in the bit-length of \( N \). Therefore, used in connection with Shor factoring, \( \gamma \) scales linearly in \( n \). This, however, should not distract from the fact that \( \gamma \) is primarily dependent on \( \omega \), and not on \( n \). It becomes dependent on \( n \) only indirectly if, e.g., in connection with Shor’s algorithm, the problem is posed in such a way that a one-to-one relationship exists between \( n \) and \( \omega \). In such cases, then, it does not matter whether we consider \( \gamma \) as a function of \( n \) or as a function of \( \omega \).

Because, as shown in Fig. 4, an approximate one-to-one correspondence exists between \( \gamma \) and \( \omega \), for fixed \( \omega \), we have \( \gamma \) independent of \( n \). As a consequence, for fixed \( \omega \), the performance of the defective QFT does not deteriorate as a function of \( n \). So far, we have been unable to uncover the underlying reason for this observation. Since the performance plateau does not show up using simpler performance criteria, such as the nearest-peak criterion \([4, 6, 30]\), the performance plateau must have something to do with the use of our more realistic post-processing criterion \( \text{CPP}_1 \), which captures the actual performance characteristics of the defective QFT more accurately. This indicates that the reason for the plateau is number-theoretic in origin (\( \text{CPP}_1 \) involves a continued fractions analysis of output states \(| b \rangle \ [1]\)) and certainly has something to do with the way defective CROT gates channel probability out of the main Fourier peaks into other useful states, bypassing states that are not useful for period-finding.

In an attempt to rule out any trivial explanations of the plateauing behavior shown in Fig. 3, for instance saturation of Fourier space with states useful for period-finding, we investigate the fraction \( \rho \) of useful states with respect to all possible output states. For instance, for the present example of \( \omega = 30 \), we find \( \rho_{n=10} = 12/2^{10} \), \( \rho_{n=15} = 404/2^{15} \), and \( \rho_{n=20} = 12892/2^{20} \), leading to, approximately, \( \rho \approx 1/80 \), which is constant, independent of \( n \). This means that for a totally randomized Fourier spectrum, we expect the success probability to be \( \tilde{P} \approx 1/80 \). This does not correspond to our observations, thus ruling out a simple, probabilistic explanation for the origin of the plateauing behavior. We note that the constancy of \( \rho \) is an interesting mathematical problem in itself, which might be accessible to a number-theoretic study of the \( \text{CPP}_1 \) criterion itself.
Since the total number of output states increases exponentially in $n$, and since for fixed $\omega$ the ratio of useful states to the total number of output states is a fixed constant $\rho$, the number of useful states for a fixed $\omega$, then, increases exponentially in $n$ as well. Hence, the average probability that a measurement of the output state of the QFT yields a state $|b\rangle$ useful for period-finding according to CPP, decreases exponentially in $n$ according to $\tilde{P}_b \sim 1/(\rho 2^n)$. This means, that in the presence of some fixed background noise, not all states $|b\rangle$ that are theoretically useful for period finding will be useful in practice; in order to be useful in practice, their probability $\tilde{P}_b$ has to rise above some probability cut-off $\tilde{P}_{\text{noise}}$, which depends on the background noise level. Therefore, we anticipate that despite the presence of exponentially many states that are theoretically useful, the probability cut-off may seriously limit the number of states that can be reliably used for period-finding, thus fundamentally modifying the plateau behavior of QFT performance.

In order to investigate this expectation more quantitatively, we plot, in Fig. 5, the performance $\tilde{P}^\ast = \sum_b \tilde{P}_b^\ast$ of the defective QFT with $\delta = \pi$ and $\epsilon = 0.3$ subjected to various cut-off levels $\tilde{P}_{\text{noise}}$, normalized by $\tilde{P} = \sum_b \tilde{P}_b$, its noise-free counterpart, as a function of the number of qubits $n$. We define $\tilde{P}_b = \tilde{P}_b$ if $\tilde{P}_b > \tilde{P}_{\text{noise}}$ and $\tilde{P}_b = 0$ if $\tilde{P}_b \leq \tilde{P}_{\text{noise}}$. Thus, if a measurement of the output state of the QFT yields a theoretically useful state $|b\rangle$ with probability $\tilde{P}_b \leq \tilde{P}_{\text{noise}}$, it is rejected from our performance measure. As might have been expected, for small $n$, where only relatively few useful states $|b\rangle$ with relatively large probabilities (probabilities have to sum to 1) exist, the background noise has little effect in suppressing these useful states and the plateau is relatively undisturbed. This is clearly demonstrated in Fig. 5, which shows a performance plateau for small $n$. However, Fig. 5 also shows that from some critical $n_c$ on, when the probability level in the beneficial states, on average, starts to dive below the specified noise level, the plateau behavior breaks, the performance deteriorates, and continues to deteriorate for all $n > n_c$. The cut-off $\tilde{P}_{\text{noise}}$ controls $n_c$, the onset of performance decay: the higher the noise cut-off $\tilde{P}_{\text{noise}}$, the smaller $n_c$, i.e., the earlier the deterioration of the performance occurs in $n$. The plateau and its break at $n = n_c$ are predictions that can be checked experimentally.

The peeling off of useful output states $|b\rangle$ with rising noise cut-off $\tilde{P}_{\text{noise}}$ provides us with a justification for choosing the nearest-peak criterion as a measure of period-finding success [4, 6, 30]: In the presence of noise, the peaks nearest to the theoretically expected main peak locations of the QFT output state, i.e., the highest peaks in the spectrum, are the ones that survive the longest as a function of $n$. Thus, the nearest-peak criterion may be used to measure QFT performance in situations with large background noise, while for low background noise levels, CPP is more appropriate.

Now, an important question arises: How does the fraction $\rho$ scale in $\omega$? This needs to be investigated since, if $\rho$ were a constant, say $\rho = 1/80$, as in the case $\omega = 30$, then, with probability 1 in 80 we would be able to obtain the periodicity of an input state simply with trial and error (picking random numbers we would be successful in 1 out of 80 trials on average), no matter how large $\omega$. We might use this scheme to factor large integers, which cannot possibly be true. Therefore, we anticipate that $\rho$ is a decreasing function of $\omega$ and the only remaining question is the functional form of this decrease.

In order to answer this question, Fig. 6 shows $\rho$ as a function of $\omega$. We see that $\rho$ decreases approximately as $\rho \sim 1/\omega$ as $\omega$ increases. Therefore, as suspected, in the case of exponentially
Performance scaling of the quantum Fourier transform with defective rotation gates

Fig. 5. Normalized success probability of finding the periodicity \( \omega = 30 \) as a function of the number of qubits \( n \) for fixed \( \delta = \pi \) and \( \epsilon = 0.3 \), subjected to different noise levels \( P_{\text{noise}} \). Shown are the data with \( P_{\text{noise}} = 1 \times 10^{-5} \) (pluses), \( P_{\text{noise}} = 3 \times 10^{-5} \) (crosses), and \( P_{\text{noise}} = 7 \times 10^{-5} \) (asterisks). The transitions occur at \( n_c = 14, 13, \) and \( 12 \) for \( P_{\text{noise}} = 1 \times 10^{-5}, 3 \times 10^{-5}, \) and \( 7 \times 10^{-5} \), respectively.

large \( \omega \), this functional behavior prohibits us from detecting the periodicity \( \omega \) by simple trial and error. Moreover, since those \( \omega \) that are of interest in cryptanalysis are exponentially large (see, e.g., [1, 30, 31]), we conclude, on the basis of Fig. 6, that \( \rho \) decays exponentially in \( n \) with exponentially increasing \( \omega \).

A note on our use of the CPP\(_1\) criterion instead of the complete CPP criterion [1] is in order. We used CPP\(_1\) for convenience only, expediting the (surprisingly time-consuming) classical post-processing procedure. If CPP\(_1\) decides that an output state \( |b\rangle \) is useful for period-finding, it is also useful according to CPP. Conversely, if CPP\(_1\) rejects a state \( |b\rangle \), CPP might find it useful. Thus, CPP\(_1\) does not do anything wrong, it simply underestimates (slightly) the performance of the defective QFT. Thus, all performance estimates in this paper are lower bounds; the actual performance of the defective QFT is even better.

Most of our numerical simulations were performed with \( n = 10 \) or \( n = 14 \) qubits, and only the calculations in Fig. 3 were performed with up to \( n = 20 \) qubits. This seems on the low side given the formidable computer power regularly available in modern research labs. Indeed, we had access to a state-of-the-art 300-core cluster computer on which all of our numerical computations were performed. However, as is generally known, the processing power of quantum computers is exponentially larger than the processing power of a classical digital computer, and while it is known that a digital computer can simulate all operations of a quantum computer, this simulation is exponentially inefficient. Therefore, at \( n = 20 \), even our 300-core cluster computer runs into a wall (the execution times become too large in real time) and if ensembles have to be simulated (in our case statistical ensembles of QFTs with systematic and random gate errors), the reasonable limit in classical computer resources that was available to us to be expended on this project dictated an \( n \) cut-off for our simulations at \( n = 14 \). We note that in Fig. 3, for instance, each point in the plot is the result of averaging over 10000 ensembles of random numbers. Clearly, larger \( n \) would be desirable, in particular
Fig. 6. Fraction $\rho$ of states useful for period-finding to all possible $2^n$ output states as a function of the periodicity $\omega$ of the input state with $\omega$ ranging up to $2^{10}$. The data shown are obtained from computing $\rho$ with $n = 20$. Apparently, $\rho$ scales like $\sim 1/\omega$.

for checking our analytical scaling laws. However, even with the help of supercomputers, because of the exponential explosion of required computational resources with $n$, the increase in accessible $n$ values would only increase marginally. If not anything else, this situation illustrates two important points. (i) The awesome power of quantum computers (by dwarfing the classical computers used for their simulation) and (ii) the need for analytical formulas to access the large-$n$ regimes forever inaccessible to classical computers.

While the current paper focuses on the model characterized by (2), we did run numerical simulations with a generic $2 \times 2$ unitary matrix, perturbed around the exact operation. Preliminary results show that population or amplitude errors in the rotation gate in fact result in noticeable deterioration of the performance of the QFT, apparently destroying the plateauing behavior shown in Fig. 3. This suggests that when it comes to manufacturing quantum hardware, one should try to minimize the amplitude errors as much as possible in order to fully take advantage of the performance plateau behavior associated with the phase-angle errors. The exact scaling relation of the combined errors are the subject of current investigations and their results will be reported elsewhere.

7 Summary and conclusions

In this paper, using the example of the QFT with defective CROT gates, we address Landauer’s question [3] of whether static gate defects are fatal for quantum information processors. In general we find that the QFT is astonishingly resilient to the introduction of static defects, called “manufacturing flaws” by Landauer [3]. We investigate two types of static defects in the CROT rotation angles, systematic and random. Overall we find that even for defect strengths on the order of 30% and larger, acceptable QFT performance can be guaranteed, corroborating our findings in previous research [4, 6, 30] that already pointed to the extraordinary robustness of quantum information processors with respect to static gate defects. This means that static gate defects should not be an immediate source of worry for engineers and scientists working on designing and implementing these information processors as actual hardware com-
ponents. We also find that using a more advanced classical post-processing criterion (CPP₁, as described in Sec. 3) instead of the simpler nearest-peak criterion [4, 6, 30], the performance of the defective QFT reaches a performance plateau as a function of the number of qubits \( n \), a prediction that may be checked experimentally. This result is significant both for the theoretical properties of the QFT and for practical applications, since it means that despite the proliferation of defective gates for increasing \( n \), the performance stays the same. While this is a firm result, confirmed numerically by our simulations and supported by analytical arguments, the microscopic mechanism according to which this performance plateau arises currently remains an open problem awaiting further numerical and analytical work. While the fundamental origin of the performance plateaus is not clear at present, our analytical scaling laws reproduce the plateau levels with high accuracy.

**References**

Analytical formulas for the performance scaling of quantum processors with a large number of defective gates

Y. S. Nam and R. Blümel

Department of Physics, Wesleyan University, Middletown, Connecticut 06459-0155, USA

(Received 11 March 2015; revised manuscript received 4 July 2015; published 1 October 2015)

Removing a single logical gate from a classical information processor renders this processor useless. This is not so for a quantum information processor. A large number of quantum gates may be removed without significantly affecting the processor’s performance. In this paper, focusing on the quantum Fourier transform (QFT) and quantum adder, we show even more: Even if most of its gates are eliminated and the remaining gates are selected from a randomly generated set, the QFT, one of the most useful quantum processors, and the quantum adder, one of the most basic building blocks of a universal quantum computer, still operate with satisfactory success probability, comparable to that of a quantum computer constructed with perfect gates. We support these conclusions by first laying out a general analytical framework and then deriving analytical scaling relations, which are in excellent agreement with our numerical simulations. The demonstrated robustness of the QFT and quantum adder, to the point where randomly generated quantum gates take the place of the exact gates, is an important boon for the construction of quantum computers, since it shows that stringent gate error tolerances do not have to be met to obtain satisfactory performance of the corresponding quantum processors. Our analytical techniques are powerful enough to generate asymptotic scaling laws for any gate defect model of quantum information processors and we illustrate this point by explicitly computing asymptotic analytical scaling formulas for several other defect models as well.

DOI: 10.1103/PhysRevA.92.042301

PACS number(s): 03.67.Lx, 03.67.Ac

I. INTRODUCTION

More than two decades have passed since the discovery of Shor’s algorithm [1], capable of factoring a semiprime faster than any known classical algorithm to date. Proving for the first time that a quantum computer is indeed practically useful and poses a threat to the widely employed Rivest-Shamir-Adleman cryptosystem [2]. Shor’s algorithm has attracted many scientists and engineers to the field of quantum computing, an interdisciplinary subject encompassing mathematics, computer science, physics, and chemistry with applications ranging from national security to search engines. To date, however, no universal quantum computer exists that is of practical interest. Even with novel breakthroughs such as fault-tolerant, error-correcting codes (see [3] and references therein), record-breaking experimental achievements in storing quantum information [4,5], and surface codes [6], the realization of practically useful quantum computers seems to lie in the distant future. Thus, in order to build a practical quantum computer, much work still needs to be done, in particular in the realm of robustness of quantum computers with respect to imprecise quantum hardware as will necessarily be found in any realistic implementation of a quantum processor.

It is no surprise, then, that there have been numerous investigations, both theoretical and experimental, studying the effects of imperfect hardware for a wide variety of quantum computer architectures. In the field of Rydberg quantum processors, e.g., we find investigations of decoherence and fidelity of single- and two-qubit gates [7], a proposal of a new scheme for realizing a controlled-phase gate and quantifying its expected gate error level [8], studies of the effect of imperfections in the external hardware (e.g., control of field power or duration) on quantum-gate performance [9], and characterizations of the effect of errors accumulating over a sequence of single- and two-qubit gates [10]. Technological advances have resulted in reliable performance of Clifford gates in a spin-qubit system [11] with the reported error rate below the tolerable threshold required by surface codes [6]. Yet another advance has been reported by Zu et al. [12], where universal geometric rotation gates in a spin-qubit system have been experimentally realized. Experimental realization of the gate have also been reported in a superconducting system [13]. Recently, phase noise in a superconducting system has been characterized and investigated in detail in Ref. [14].

In this paper, further advancing the investigations of the effect of hardware errors on a quantum computer, we focus on the analytical analysis of the effects of gate errors in large-scale quantum processors. In particular, we develop analytical scaling laws that tell us how the processor’s fidelity scales in the limit of a very large number of qubits. This is necessary since classical computers cannot simulate this quantum regime even in principle [15] and analytical scaling formulas, therefore, are the only way to assess the effects of imperfect gates in the practically relevant regime of a large number of qubits. In particular, analytical scaling formulas may give us an idea of the level of gate errors that may be tolerated for satisfactory quantum-computer performance in the large-scale limit. In addition, on the basis of these formulas, we may assess quantitatively whether a large-scale quantum processor reacts sensitively to gate errors or exhibits a more tolerant and robust response to gate errors.

We start with investigating the robustness of the quantum Fourier transform (QFT), one of the most important quantum information processors. Our choice is based on the universal applicability of the QFT in many useful quantum algorithms known to date (see [16] and references therein). For this reason, numerous works are available in the literature, investigating the robustness of the QFT, including approximation techniques [15,17–19], faulty gates [16,20–22], and structural stability...
Further corroborating the robustness of the QFT is the random hierarchy approach [23], which we investigate in detail in this paper.

Yet another quantum processor we focus on in this paper is the quantum adder. As one of the most basic components of universal quantum computers, the quantum adder plays a central role in the construction of quantum arithmetic units [24]. Employing the QFT-based architecture [25], the respective quantum adder, mostly made of controlled rotation gates, will prove robust with respect to errors following a random hierarchy.

We shall demonstrate that in spite of deleting most of the controlled rotation gates from the QFT and quantum adder processors and replacing the remaining rotation gates with gates drawn from a small, randomly generated set, the quantum processors still display acceptable performance. We also derive explicit analytical scaling laws that support our prediction of robustness with respect to these drastic alterations of the QFT and quantum adder circuits.

Our paper is structured as follows. In Sec. II A, in the context of the QFT, we introduce the random hierarchy and present numerical results. Also introduced in this section is the concept of banding, a type of pruning technique that is necessary for practical quantum computing. Then, in Sec. II B we approach the same problem analytically and show that the resulting analytics and the numerical results found in Sec. II A are in excellent agreement. In Sec. III A we introduce the QFT-based quantum adder and its associated numerics in the context of gate errors including random hierarchy and banding. This is followed by Sec. III B, where we investigate the same problem analytically, whose results are once again in excellent agreement with the numerical results found in Sec. III A. Additionally, in Sec. III B we present analytical scaling laws of the performance of the quantum adder whose constituent quantum gates are subjected to perturbations whose statistical profiles follow normal or uniform distributions. Then, in Sec. IV we discuss our results. We summarize our paper in Sec. V.

II. ROBUSTNESS OF THE QFT

A. Numerics

An n-qubit QFT has exact rotation angles \( \theta_j = \pi/2^j \), \( j = 1, \ldots, n - 1 \), where \( j \) is the distance between control and target qubits (see Fig. 1 for a sample circuit of a five-qubit QFT). In order to investigate the robustness of the \( n \)-qubit QFT to a class of drastic changes \( \theta_j \rightarrow \tilde{\theta}_j \) of its rotation angles, we employ the following methodology. We produce a set \( S_N \), of \( N \geq n - 1 \) random numbers, uniformly distributed in \((0, \pi) \). From \( S_N \), we draw those random numbers that are closest to the exact rotation angles \( \theta_j \) (repetitions are permitted) and denote them by \( \tilde{\theta}_j \). Since the new angles \( \tilde{\theta}_j \) are drawn from the same random set \( S_N \), but still constructed in such a way that they are ordered hierarchically in descending order, we call this implementation of the QFT a realization with a random hierarchy. Figure 2 illustrates the result of this procedure for \( N = 20 \). The red squares are the exact angles \( \theta_j \), while the green closed circles are the best matches \( \tilde{\theta}_j \), for the exact angles \( \theta_j \), drawn from a set of \( N = 20 \) random numbers. Although seemingly close on the logarithmic scale of Fig. 2, the relative errors \( r_j = |\tilde{\theta}_j - \theta_j|/\theta_j \) for this particular realization of random angles \( \theta_j \) are large, ranging from 4% for \( j = 1 \) to 48% for \( j = 5 \), exceeding 100% from \( j = 9 \) on. These are large errors, deliberately introduced into the QFT, since our point is to show that even in the case of a random realization of rotation angles, the QFT still performs satisfactorily. Of course, in the limit \( N \rightarrow \infty \), \( \tilde{\theta}_j \) approaches \( \theta_j \). Our point, however, is that even if \( N \) is small, and consequently \( r_j \) may be large, the QFT still performs at an astonishingly high level.

We note that scaling noise models, such as perturbing the angles \( \theta_j \) with noise whose level scales in the size of \( \theta_j \), for instance, have been studied in great detail for the QFT in Ref. [16]. In Sec. II B, where we discuss our analytical calculations, we will further establish how our work here connects to that in Ref. [16]. Our choice of the random hierarchy here is deliberate since the errors introduced by the random hierarchy are not adapted to the natural exponential behavior of the rotation angles in either the QFT or the quantum
adders. Thus this type of errors is a stringent test of the robustness of both the QFT and adder quantum processors.

We start with the statement that the QFT equipped with the random hierarchy performs at an astonishingly high level even when $N$ is small. We denote by $\hat{Q}$ the ideal QFT operation, equipped with $\theta_j$ gates, and by $\hat{Q}^r$ the modified QFT operation, equipped with $\theta^r_j$ gates. As a test state for these two QFTs we choose $|\psi_{\text{init}}\rangle = |2^n - 1\rangle$ since this is the most unfavorable case for both QFTs. This is so because $|\psi_{\text{init}}\rangle$ ensures that all rotation gates in the QFT (see Fig. 1), together with their respective errors (in the case of $\hat{Q}^r$), are always switched on. In contrast, choosing $|0\rangle$ as an input state would always result in perfect performance, even in the case of completely random rotation gates, since for this input state none of the rotation gates is triggered. To illustrate this point more clearly, we plot in Fig. 3 the fidelity of the QFT defined according to $F = \langle |\psi_{\text{actual}}\rangle |\psi_{\text{ideal}}\rangle^2$ as a function of $\alpha$, where for any integer input state $|\psi_{\text{init}}\rangle = |\alpha\rangle$ the states $|\psi_{\text{ideal}}\rangle$ and $|\psi_{\text{actual}}\rangle$ are computed according to $|\psi_{\text{ideal}}\rangle = \hat{Q}|\psi_{\text{init}}\rangle$ and $|\psi_{\text{actual}}\rangle = \hat{Q}^r|\psi_{\text{init}}\rangle$ and the angular brackets in the definition of $F$ indicate averaging over multiple realizations of the random set $S_N$. We observe that as more controlled-rotation gates turn on, i.e., the bit spectra of $\alpha$ get filled in with 1’s, the fidelity $F$ decreases. A detailed analytical proof demonstrating that $|2^n - 1\rangle$ is indeed the least-favorable input state is available in Appendix A.

Having chosen an appropriate test state, we now assess the performance of the modified QFT by computing the fidelity $F$, averaged over 100 realizations of the random set $S_N$, as a function of the number of qubits $n$. The result is shown in Fig. 4(a). As expected, the larger the number of randomly generated gates $N$, the better the quantum computer performs. In addition, as shown in Fig. 4(a), even with $N$ as small as $N = 20$, a 17-qubit QFT still performs well above 30%. Figure 4(a) also shows that for fixed $N$ the performance of the QFT decreases with increasing number of qubits $n$. This result is intuitively obvious since the more gates we need to approximate with only a finite number $N$ of random gates at hand, the worse the performance of the quantum computer is expected to become.

We now band the QFT with bandwidth $b$, i.e., we prune those rotation gates from the QFT circuit whose ideal rotation angles are $\pi/2^j$, where $j > b$ [15,17–19]. The results for $b=8$ are shown in Fig. 4(b). Comparing with the corresponding cases of Fig. 4(a), we notice that the fidelity computed with $b = 8$ is significantly better than that with full bandwidth. This confirms the conjecture in Ref. [27] that banding, in the presence of imperfect hardware, boosts QFT performance by removing faulty rotation gates that do nothing useful but instead channel noise and errors into the still useful parts of the quantum processor. As a consequence, we expect that for given $n$ and $b$ there is a transition point $N_t$ between the regimes of $N$ in which banding increases ($N < N_t$) and decreases.
Appendix A. List of Publications

Y. S. Nam and R. Blumel

PHYSICAL REVIEW A 92, 042301 (2015)

(N > N₀) QFT performance. Thus, N₀ is the critical N, where banding has no effect on the performance of the QFT. The latter regime is expected since for N → ∞ the full-bandwidth QFT converges to F = 1, whereas the banded QFT converges to some constant F with F < 1. According to (46), derived in Sec. IV, N₀ = 470 for the example (n = 17, b = 8) presented in Fig. 4. This explains that in this case banding substantially improves performance.

B. Analytics

While the numerical simulations help us see how the QFT performs when equipped with modified rotation gates, the practically interesting regime with thousands of qubits cannot ever be simulated on a classical computer. This regime can only be accessed via analytical calculations.

We start our analytical derivations by characterizing the statistics of the modified gates ˜θ_j. Writing ˜θ_j = θ_j + ϵ_j, we note that ϵ_j follows a bivariate distribution function. This is so because the probability of finding the closest random number θ_j to θ_j, within a distance d for N given random numbers, distributed uniformly between 0 and π, scales like (|π − 2d|/π)^N, which, for d ∼ π/N and large N, may be written as exp(−2Nd/π). According to this point of view, the random hierarchy QFT studied here is no different from the absolute typed error case studied in Ref. [16], except for the fact that the statistical distribution of the perturbing term ϵ_j is now bivariate exponential, rather than uniform, as was the case in Ref. [16].

While the performance criterion used in Ref. [16] (nearest-peak criterion) is not identical with the criterion used in this paper (fidelity), we note that, in the limit in which the perturbation is small, the two criteria are interchangeable. This is so because the fidelity F = ⟨〈|ψ_{ideal}⟩|ψ_{actual}⟩^2 can be rewritten as ⟨⟨ψ_{ideal}ψ_{actual}⟩⟩_β = ∑_β Φ(α, β)β), where with 〈ψ_{ideal}⟩ = 〈α| for α an integer, and a similar expression for the modified QFT with ˜Q and ˜Φ(α, β) and 〈ψ_{actual}⟩ = 〈α| for α an integer, and a similar expression for the modified QFT with ˜Q and ˜Φ(α, β). Assuming that the perturbation phase ΔΦ^{def}(α, β), defined according to ˆΦ(α, β) = Φ(α, β)ΔΦ^{def}(α, β), fluctuates rapidly, we arrive at the analytical fidelity expression

\[
F ≈ \langle |\langle ΔΦ^{def}(α, β)\rangle| β \rangle^2, \tag{2}
\]

where ⟨···⟩_β denotes averaging over β, which is identical to Eq. (33) of Ref. [16] up to summation. Summation, however, is irrelevant, as we further assume for the following statistical analysis that the bits in both the input α and the output β are random sequences of 0’s and 1’s.

Closely following the steps of the analytical analysis developed in Ref. [16] and taking care to replace the uniform distributions assumed in Ref. [16] with the bivariate exponential probability distribution of the difference angles ϵ_j, we obtain the analytical fidelity function of the randomly hierarchical, full-bandwidth QFT to be

\[
F ≈ \exp \left[ -\frac{n(n - 1)}{8(2N/π)^2} \right]. \tag{3}
\]

In order to demonstrate the quality of our analytical results, we plot in Fig. 5(a) the complement 1 − F of the fidelity F of the full-bandwidth QFT as a function of N for various n values, obtained from numerical simulations (plot symbols), together with the analytical results (3) (solid lines). The analytical results match the numerical results to an excellent degree. As expected, the fit is better in the large-N regime (small ϵ_j), demonstrating that the analytical results capture the scaling in both n and N correctly.

At this point, we introduce banding in our analytical analysis. Once again we start with the fidelity definition, only this time we have F_b = ⟨⟨|ψ_{ideal}⟩|ψ_{banded}⟩|ψ_{actual}⟩^2 with

\[
|ψ_{banded}⟩ = ˜Q_b|ψ_{in}⟩ = α = ∑_β Φ_b(α, β)|β⟩. \tag{4}
\]

FIG. 5. (Color online) Complement 1 − F of the fidelity F of the QFT equipped with the randomly hierarchical rotation gates ˜θ_j as a function of the number of random gates N. In order to match the random bit spectrum assumption used in the analytical calculations, all numerical simulation data are averaged over all possible integer input states |α⟩, where α = 0, . . . , 2^n − 1, for an n-qubit QFT, in addition to the averaging over 100 realizations of N random gates. (a) Full-bandwidth QFT and (b) banded QFT with bandwidth b = 4. Shown are the cases with n = 5, 6, 7, and 8, corresponding to pluses (red), crosses (green), asterisks (blue), and squares (purple), respectively.
Appendix A. List of Publications

where \( \hat{Q}_a \) and \( \Phi_b \) denote the banded QFT operator and the associated phase with bandwidth \( b \), respectively. Assuming (i) a statistical independence between \( \langle \hat{y}_{\text{ideal}} | \hat{y}_{\text{ideal}} \rangle \) and (ii) a rapidly fluctuating, random hierarchy perturbation phase \( \Delta \Phi^{(n)} \), defined according to \( \Phi_b(\alpha, \beta) = \Phi_b(\alpha, \beta) \Delta \Phi^{(n)}(\alpha, \beta) \), where \( \Phi_b(\alpha, \beta) \) denotes the modified banded QFT phase, we arrive at the analytical banded QFT fidelity expression

\[
F_b \approx \sum_{\beta} \Phi^*(\alpha, \beta) \Phi(\alpha, \beta) e^{i\Phi(\alpha, \beta)} \approx \frac{\langle \Phi_b^*(\alpha, \beta) \Phi_b(\alpha, \beta) \Delta \Phi^{(n)}(\alpha, \beta) \rangle^2}{\langle |\Phi_b(\alpha, \beta)\rangle^2 \rangle^2},
\]

where we used \( \Phi_b = \Phi e^{i\Phi} \) and \( \phi_b \) denotes the phase-angle offset of \( \Phi_b \) from \( \Phi \), arising from banding with bandwidth \( b \). Together with \( \sum_{\beta} |\Phi_b(\alpha, \beta)\rangle^2 \approx |\langle \Phi_b(\alpha, \beta)\rangle|^2 \), assuming a rapidly fluctuating \( \phi_b \), and using the results derived in Refs. [15,16], we obtain

\[
F_b \approx \exp \left[ -\frac{\pi^2 2^{b-2} / (n - b - 1) + \delta}{12} \right] \times \exp \left[ \frac{-nb - (b + 1) / 2}{4(N/n)^2} \right],
\]

where \( \delta = c(n - b) \) (\( c \) is a constant) is a small offset, which is due to residual correlations not included in our statistical analysis. Its linear dependence on \( n \) is expected since \( \delta \) represents the residual inaccuracy in finding the variance of the accumulated phase angles, which scales like \( \sim n \). The constant \( c \) is determined by fitting to simulation data. For \( b = 4 \), e.g., the best fit is obtained for \( \delta = -0.012(n - b) \) for \( n > b + 1 \). Figure 5(b) shows that for this choice of \( \delta \), the analytical scaling formula \( F_b \) in Eq. (6) matches the numerical simulation results to an excellent degree.

III. ROBUSTNESS OF THE QUANTUM ADDER

A. Numerics

So far, we investigated the robustness of the QFT in detail, both analytically and numerically. In this section, we extend our analysis to a quantum adder, the fundamental component of quantum arithmetic, which is universally applicable to any serious quantum computation. In particular, we investigate a quantum Fourier adder [25], shown in Fig. 6, which also serves as a test-bed application of the QFT processor that has been analyzed in detail in Secs. II A and II B. Hereafter, we make the following distinction: We refer to the quantum circuit that performs a quantum addition as the quantum adder and the associated part of the circuit that performs an addition in Fourier space as the quantum Fourier adder (see Fig. 6).

To start with, we implement randomly hierarchical controlled rotation gates to our quantum adder. Since we now have an additional gate to approximate, i.e., a \( \pi \) gate denoted by \( \theta_\pi \), we extend the domain from which the random numbers are drawn from \( (0, \pi/2) \) to \( (0, 2\pi) \). The results are shown in Fig. 7(a), where, consistent with the methodology presented in Sec. II A, we used the input state \( |\psi_{\text{in}}\rangle = |2^n - 1\rangle \) and the addend \( \nu = 2^n - 1 \) for an \( n \)-qubit quantum adder. The analytical proof showing why this is statistically the least-favorable case scenario in terms of fidelity is provided in Appendix B. The fidelity \( F_r \), plotted against the number of qubits \( n \), is expected, as shown in Fig. 7(a), even with \( N \) as small as 40, a 17-qubit quantum adder still performs at a level of about 20%. Figure 7(a) also shows that for fixed \( N \), the performance of the quantum adder decreases with increasing number of qubits \( n \). This result, in analogy to the QFT, is intuitively obvious since the more gates we need to approximate with a finite number of random gates, the poorer the quality of the quantum processor becomes.

This time, we band the quantum adder with bandwidth \( b \), deleting all rotation gates with their rotation angle less than \( \pi/2^b \). Figure 7(b) shows the results for the case \( b = 8 \). Just as in the case of the QFT, we find that the banded quantum adder significantly outperforms the full-bandwidth quantum adder. For \( N = 40 \) and \( n = 17 \), for instance, i.e., the case we considered in connection with Fig. 7(a), the performance of the banded adder is above 90%, significantly better than the 20% performance of the adder without banding. This is consistent with the results reported in Sec. II A in connection with the QFT in the sense that erroneous gates with large \( j \) do more harm than good to the fidelity of a quantum processor by channeling noise into the system.

B. Analytics

We now approach the quantum adder fidelity problem analytically. We do this in two steps. First, we lay out a general analytical framework to arrive at the fidelity expression without specifying the types of errors. Only then, after obtaining the general fidelity expression, do we specify the types of
errors. This keeps our analytical results on the most general level, so that our analytical formulas are generally applicable to a wide range of error models. To demonstrate the general applicability of our analytical results to different kinds of error models, in this section, in addition to the random hierarchy, we also investigate Gaussian and uniformly distributed errors.

To start, we recall the definition of fidelity $F = \langle \psi_{\text{ideal}} | \psi_{\text{actual}} \rangle ^2$. Defining $\Phi^{\text{QFA}}(\beta; v)$ as the phase associated with the quantum Fourier adder (see Fig. 6), where $\beta$ is an integer input and $v$ is the addend of the adder, together with (1) and its inverse expression, we may write the quantum adder fidelity

$$F^{\text{QFA}} = \left[ \left\langle \sum_{\beta, \gamma} | \Phi(\beta, \gamma) \rangle \Phi^{\text{QFA}}(\beta; v) \Phi^*(\alpha, \beta) \right\rangle \left\langle \sum_{\beta, \gamma} \Phi(\alpha, \beta') \Phi^{\text{QFA}}(\beta'; v) \Phi^*(\beta', \gamma') \langle \gamma' | \right\rangle \right]^2. \quad (7)$$

where $\Phi$ and $\Phi^{\text{QFA}}$ denote the phases of the defective QFT and quantum Fourier adders, respectively, and $\alpha$ is the input integer. Defining $\Phi = \Phi^{\text{QFA}}(\alpha, \beta)$ and $\Phi^{\text{QFA}} = \Phi^{\text{QFA}}(\alpha, \beta) \Delta \Phi^{\text{QFA}}(\beta, v) \Delta \Phi^{\text{QFA}}(\alpha, \beta)$, together with $\langle \gamma | \gamma' \rangle = \delta_{\gamma, \gamma'}$, where $\delta$ is the Kronecker delta, (7) may now be written as

$$F^{\text{QFA}} = \left[ \left\langle \sum_{\beta, \gamma} \Phi(\beta, \gamma) \Phi^{\text{QFA}}(\beta; v) \Phi^*(\alpha, \beta) \right\rangle \right]^2. \quad (8)$$

Assuming that the defect phases fluctuate fast, we may approximate (8) as

$$F^{\text{QFA}} \approx \langle |(\Delta \Phi^{\text{def}}(\alpha, \beta'))_\beta \rangle_\beta \langle |(\Delta \Phi^{\text{QFA}}(\beta', v) \Delta \Phi^{\text{def}}(\alpha, \beta'))_\beta \rangle_\beta \langle |(\Delta \Phi^{\text{QFA}}(\beta', v) \Delta \Phi^{\text{def}}(\beta', \gamma')_\gamma \rangle_\gamma \rangle_\gamma, \quad (9)$$

where $\langle \cdots \rangle_\beta$ denotes averaging over $\beta'$ and $n$ is the number of qubits. We note that the exact-adder parts in Eq. (8) evaluate to $\delta_{\gamma, (\alpha + v) \mod 2^n}$, explaining the origin of the second argument $\langle \gamma | \gamma' \rangle = \delta_{\gamma, \gamma'}$, where $\delta$ is the Kronecker delta. Further assuming a statistical independence between the three terms in Eq. (9), we obtain

$$F^{\text{QFA}} \approx \langle |(\Delta \Phi^{\text{def}}(\alpha, \beta'))_\beta \rangle_\beta \langle |(\Delta \Phi^{\text{QFA}}(\beta', v) \Delta \Phi^{\text{def}}(\alpha, \beta'))_\beta \rangle_\beta \langle |(\Delta \Phi^{\text{QFA}}(\beta', v) \Delta \Phi^{\text{def}}(\beta', \gamma')_\gamma \rangle_\gamma \rangle_\gamma. \quad (10)$$

Now we inspect each term in Eq. (10) individually. First, we recall that the defective phases arise from the defects included in phase-rotation gates. According to the analysis shown in Ref. [16], then, as long as the central limit theorem [28] on random phase-angle accumulation holds, without loss of generality, we may write

$$F^{\text{QFA}} \approx e^{-\sigma^2_\beta^2} e^{-\sigma^2_\gamma^2}. \quad (11)$$

where $\sigma_\beta$ and $\sigma_\gamma^{\text{QFA}}$ are the standard deviations of the defective phase angles accumulated from gate errors associated with an
Appendix A. List of Publications

ANALYTICAL FORMULAS FOR THE PERFORMANCE . . . PHYSICAL REVIEW A 92, 042301 (2015)

FIG. 8. (Color online) Complement $1 - F$ of the fidelity $F$ of the quantum adder equipped with the randomly hierarchical rotation gates $\phi_i$ as a function of the number of random gates $N$. In order to match the random bit spectrum assumption used in the analytical calculations, all numerical simulation data are averaged over all possible integer input states $|a\rangle$, where $a = 0, \ldots, 2^n - 1$ and all possible integer addends $v = 0, \ldots, 2^n - 1$. Shown are the results of averaging over 10000 realizations of the random set $S_n$. (a) Full-bandwidth quantum adder and (b) banded quantum adder with bandwidth $b = 4$. The cases with $n = 5, 6, 7$, and 8 correspond to pluses (red), crosses (green), asterisks (blue), and squares (purple), respectively.

$n$-qubit QFT and an $n$-qubit quantum Fourier adder, respectively. Notice that there are two differences between the QFT and the quantum Fourier adder: (i) The quantum Fourier adder has no Hadamard gates, i.e., it purely consists of controlled phase-rotation gates, and (ii) compared to the QFT it has $n$ additional $\pi$ gates. With $\sigma_{QFA}^2 = 4(\pi/2)^2 n N_{\text{bit}}/4$, where $N_{\text{bit}}$ is the variance associated with the defect of a $\pi$ phase-rotation gate, our general fidelity expression reads

$$F_{\text{QFA}} \approx e^{-\nu^2 n^2 N_{\text{bit}}/4}. \quad (12)$$

At this point we are ready to choose a specific type of error for the quantum adder fidelity expression. To this end, we insert the random hierarchy case into (12) and obtain, to leading order in $n$,

$$F_{\text{RH}}^{(QA)} = \exp \left( - \frac{3\nu^2}{4 N/N_{\pi}^2} \right). \quad (13)$$

We are not able to compute the next term in a systematic $n$ expansion of the argument of the exponent in Eq. (13) analytically. However, we may take a cue from our work in Ref. [15]. Although focused on scaling relations of Shor’s algorithm in the absence of noise, and therefore not directly related to our work here, [15] nevertheless suggests that the next-order correction term, which will dominate the other correction terms for $n \geq z$, should have the form

$$s(n - u - v)/(N/N_{\pi})^2, \quad (14)$$

where $s, u, v, \nu$, and $z$ are integer constants. Unable to determine these constants analytically, we determined them numerically. The best fit was found for $s = 3, u = 2, v = 1$, and $\nu = 5$. Therefore, adding the term $3(n - 2 - 1)/(N/N_{\pi})^2$ for $n \geq 5$ to the exponent of (13), we obtain our final analytical formula, which is compared with numerical simulations in Fig. 8(a). We see that the analytical formula matches the numerical results to an excellent degree, i.e., the analytical formula correctly predicts the scaling of the quantum adder fidelity.

Closely following the steps outlined in Sec. II B, it can be shown that, in analogy to (10), the banded adder performs with fidelity

$$F_{b}^{(QA)} \approx \exp \left( - \frac{n^2}{2 \pi^2} (n - b - 1) + \delta \right) \times \exp \left( -6 \sigma_{a,b}^2 - \frac{n(N/N_{\pi})}{4} \right), \quad (16)$$

where $\sigma_a$ and $\sigma_b$ denote, respectively, the phase-angle offsets associated with the QFT and the quantum Fourier adder due to banding and $\Delta \Phi_{b}$ denote the respective defect phases. Using the results from Sec. II B, [15,16] and denoting the variance of the phase-angle defects of the banded QFT with bandwidth $b$ as $\sigma_{a,b}$, we obtain

$$F_{b}^{(QA)} \approx \exp \left( - \frac{n^2}{2 \pi^2} (n - b - 1) + \delta \right) \times \exp \left( -6 \sigma_{a,b}^2 - \frac{n(N/N_{\pi})}{4} \right), \quad (17)$$

where we assumed $b \geq 1$, leaving the $\pi$-gate part intact. Imposing the random hierarchy condition results in the fidelity of the banded adder

$$F_{b}^{(QA)} \approx \exp \left( - \frac{n^2}{2 \pi^2} (n - b - 1) + \delta \right) \times \exp \left( -6 \sigma_{a,b}^2 - \frac{n(N/N_{\pi})}{4} \right).$$
Appendix A. List of Publications

[111x350]integer addends

where the presence or absence of the subscript

distributed random numbers between

random numbers with standard deviation

(\(\sigma\)). The cases with

gates

defective rotation gates may be modeled as

\(\text{AU}\) errors, respectively, following Eqs. (18), absolute correlated (AC), and absolute uncorrelated
gates correlated or uncorrelated with respect to the types

we investigated relative and absolute errors that may be

conventional, models of gate errors. In Ref. [16], we

general scaling expressions to some additional, perhaps more

the scaling of the random hierarchy, we now apply our

ing Eq. (17) matches the numerical results in the practically

interesting, small \(1 - F\) region to an excellent degree.

Following our detailed investigation of the effects and

the scaling of the random hierarchy, we now apply our
general scaling expressions to some additional, perhaps more

conventional, models of gate errors. In Ref. [16], for instance,

we investigated relative and absolute errors that may be

correlated or uncorrelated with respect to the types \(j\) of the
gates \(\theta_j\). For the relative correlated (RC), relative uncorrelated
(RU), absolute correlated (AC), and absolute uncorrelated
(AU) errors, respectively, following Eqs. (5)–(8) of [16], the
defective rotation gates may be modeled as

\[
\begin{align*}
\text{RC} & : \hat{\theta}_j = \theta_j [1 + R_j(\sigma | \epsilon)], \\
\text{RU} & : \hat{\theta}_j = \theta_j [1 + R(\sigma | \epsilon)], \\
\text{AC} & : \hat{\theta}_j = \theta_j + R_j(\sigma | \epsilon), \\
\text{AU} & : \hat{\theta}_j = \theta_j + R(\sigma | \epsilon),
\end{align*}
\]

where \(R_j(\sigma | \epsilon)\) or \(R(\sigma | \epsilon)\) stand for Gaussian distributed random numbers with standard deviation \(\sigma\) or uniformly
distributed random numbers between \(-\epsilon\) and \(\epsilon\), respectively,

where the presence or absence of the subscript \(j\) denotes the
correlated or uncorrelated defects with respect to the rotation
gate of type \(j\).

To demonstrate the power of our general analytical scaling
formulas (12) and (16) for the quantum adder fidelities, we

are now going to derive the corresponding analytical fidelity
scaling formulas for each of the eight error models specified
in Eq. (18). In fact, these eight cases are covered by just four
fidility scaling formulas since, as proved in Ref. [16], there is

no statistical difference between the correlated error models
and the uncorrelated error models in Eq. (18).

We start with the case of Gaussian noise introduced into

the full-bandwidth quantum adder and assume that the central
limit theorem [28] holds for the phase-angle defects. Then,
to first and zeroth order in \(n\), the analytical fidelity scaling
formulas for RC, RU, AC, and AU noise are given by

\[
\begin{align*}
\text{RC}_n(F^{(\text{QA})}) &= \frac{\text{RU}_n(F^{(\text{QA})})}{\text{RU}_0(F^{(\text{QA})})} = \exp \left[ - \frac{6\sigma^2(3\pi n - 4)}{144} + \frac{\lambda n \pi^2}{4} \sigma^2 \right], \\
\text{AC}_n(F^{(\text{QA})}) &= \frac{\text{AU}_n(F^{(\text{QA})})}{\text{AU}_0(F^{(\text{QA})})} = \exp \left[ - \frac{6n(n - 1)}{32} + \frac{\mu n^2}{4} \right],
\end{align*}
\]

FIG. 9. (Color online) Complement \(1 - F\) of the fidelity \(F\) of the full-bandwidth quantum adder equipped with Gaussian-defective rotation
gates \(\theta_j\) as a function of the standard deviation \(\sigma\) of the gate errors. In order to match the random bit spectrum assumption used in the analytical
calculations, all numerical simulation data are averaged over all possible integer input states \(|\alpha\rangle\), where \(\alpha = 0, \ldots, 2^n - 1\) and all possible
integer addends \(\nu = 0, \ldots, 2^n - 1\). Shown are the results of averaging over 10 000 realizations of the defects: (a) RC, (b) RU, (c) AC, and
(d) AU. The cases with \(n = 5, 6, 7, \text{and } 8\) correspond to pluses (red), crosses (green), asterisks (blue), and squares (purple), respectively.
FIG. 10. (Color online) Complement $1 - F$ of the fidelity $F$ of the banded quantum adder (bandwidth $b = 4$) equipped with the Gaussian-defective rotation gates $\tilde{\theta}_j$ as a function of the standard deviation $\sigma$ of the gate errors. In order to match the random bit spectrum assumption used in the analytical calculations, all numerical simulation data are averaged over all possible integer input states $|\alpha\rangle$, where $\alpha = 0, \ldots, 2^n - 1$ and all possible integer addends $\nu = 0, \ldots, 2^n - 1$. Shown are the results of averaging over 10000 realizations of the defects: (a) RC, (b) RU, (c) AC, and (d) AU. The cases with $n = 5, 6, 7,$ and 8 correspond to pluses (red), crosses (green), asterisks (blue), and squares (purple), respectively.

where the left superscripts RC, RU, and AC, AU denote relative and absolute errors, respectively, and $\lambda, \mu$ are phenomenological constants. In Figs. 9(a)–9(d), for RC, RU, AC, and AU, respectively, plotting the complement $1 - F$ of the fidelity vs the noise $\sigma$, we show the results of our numerical simulations (plot symbols) together with the analytical results (solid lines) according to (19) and (20) with $\lambda = 3/5$ and $\mu = 7/4$. We see that the numerical simulations and the analytical predictions agree to an excellent degree. In addition, our numerical simulations confirm that the correlated and uncorrelated cases are statistically equivalent.

We now turn to the case of Gaussian noise introduced into the banded quantum adder with bandwidth $b$. From (16) we obtain

$$R_{\sigma,b}^{(QA)} = RU_{\sigma,b}^{(QA)} = \exp\left[-\frac{\pi^22^{-b}(n-b-1)+\delta}{2}\right] \exp\left[-\frac{6\pi^2[(3n-4)-2^{-2b}(3n-3b-4)]}{144} + \frac{\lambda n\pi^2}{4}\right] \sigma^2. \tag{21}$$

$$AC_{\sigma,b}^{(QA)} = AU_{\sigma,b}^{(QA)} = \exp\left[-\frac{\pi^22^{-b}(n-b-1)+\delta}{2}\right] \exp\left[-\frac{6\pi n(n-1)(n-b(n-b-1))}{32} + \frac{\mu n}{4}\right] \sigma^2. \tag{22}$$

In Figs. 10(a)–10(d) we show the complement $1 - F$ of the fidelity, comparing our numerical simulations (plot symbols) and our analytical results (solid lines) according to (21) and (22) for $b = 4$, the same choices for $\lambda$ and $\mu$ as in Fig. 9, and the same choice of $\delta$ as in Fig. 8(b). We see that our analytical fidelity scaling laws match the correspondent numerics to an excellent degree.
integer addends (d) AU. The cases with rotation gates Y. S. NAM AND R. BLUMEL
calculations, all numerical simulation data are averaged over all possible integer input states \(|\alpha|\), where \(\alpha = 0, \ldots, 2^n - 1\) and all possible integer addends \(\nu = 0, \ldots, 2^n - 1\). Shown are the results of averaging over 10 000 realizations of the defects: (a) RC, (b) RU, (c) AC, and (d) AU. The cases with \(n = 5, 6, 7,\) and 8 correspond to pluses (red), crosses (green), asterisks (blue), and squares (purple), respectively.

Similarly, in Figs. 11(a)–11(d), corresponding to the cases RC, RU, AC, and AU, respectively, we plot the complement \(1 - F\) of the full-bandwidth adder fidelity

\[
RCF_{x,b}^{(QA)} = RU_{x,b}^{(QA)} = \tilde{R}_{x,b}^{(QA)} \approx \exp \left\{ - \frac{6\pi^2(3n - 4) - \frac{\epsilon(n(1 - n) - \frac{\epsilon(1 - n)}{12}) + \frac{\epsilon\pi^2}{12}}{432}}{10} \right\},
\]

and in Figs. 12(a)–12(d) we plot the banded counterparts with bandwidth \(b\),

\[
RCF_{x,b}^{(QA)} = RU_{x,b}^{(QA)} = \tilde{R}_{x,b}^{(QA)} \approx \exp \left\{ - \frac{6\pi^2(3n - 4) - \frac{2b}{3} - \frac{2b - 4}{3} + \epsilon\pi^2}{432} \right\},
\]

where this time the adder processor was subjected to uniform noise. As in the Gaussian noise cases, we chose \(\lambda = 3/5, \mu = 7/4\) and the same form of \(\delta\) as in Fig. 8(b).  Our analytical results match the numerical results in Figs. 11 and 12 to an excellent degree.

For completeness we present here the formulas analogous to (19), (20), (23), and (24) for the full bandwidth QFT and (21), (22), (25), and (26) for the banded QFT, which we derived in complete analogy to our derivations of the corresponding quantum
All possible integer addends
the analytical calculations, all numerical simulation data are averaged over all possible integer states \( |\nu\rangle \), where \( \nu = 0, \ldots, 2^n - 1 \) and all possible integer addends \( v = 0, \ldots, 2^n - 1 \). Shown are the results of averaging over 10 000 realizations of the defects: (a) RC, (b) RU, (c) AC, and (d) AU. The cases with defective rotation gates
adder formulas. The QFT formulas (full bandwidth and banded) for relative and absolute Gaussian noise, respectively, are

\[
\text{RC}_F^{(\text{QFT})} = \text{RU}_F^{(\text{QFT})} = F_{b,\sigma}^{(\text{QFT})} \approx \exp\left[-\frac{\pi^2(3n - 4)}{144}\right].
\]

(27)

\[
\text{RC}_{F,b}^{(\text{QFT})} = \text{RU}_{F,b}^{(\text{QFT})} = F_{b,\sigma}^{(\text{QFT})} \approx \exp\left[-\frac{\pi^2}{12}\frac{(3n - 4) - 2^{-60}(3n - 3b - 4)}{\sigma^2}\right].
\]

(28)

\[
\text{AC}_F^{(\text{QFT})} = \text{AU}_F^{(\text{QFT})} = F_{b,\sigma}^{(\text{QFT})} \approx \exp\left[-\frac{n(n - 1)}{32}\right].
\]

(29)

\[
\text{AC}_{F,b}^{(\text{QFT})} = \text{AU}_{F,b}^{(\text{QFT})} = F_{b,\sigma}^{(\text{QFT})} \approx \exp\left[-\frac{n(n - 1) - (n - b)(n - b - 1)}{32}\right].
\]

(30)

and the formulas for uniformly distributed noise, relative and absolute, respectively, are

\[
\text{RC}_F^{(\text{QFT})} = \text{RU}_F^{(\text{QFT})} = F_{b,\sigma}^{(\text{QFT})} \approx \exp\left[-\frac{\pi^2(3n - 4)}{432}\right].
\]

(31)

\[
\text{RC}_{F,b}^{(\text{QFT})} = \text{RU}_{F,b}^{(\text{QFT})} = F_{b,\sigma}^{(\text{QFT})} \approx \exp\left[-\frac{\pi^2}{12}\frac{(3n - 4) - 2^{-60}(3n - 3b - 4)}{432}\right].
\]

(32)

\[
\text{AC}_F^{(\text{QFT})} = \text{AU}_F^{(\text{QFT})} = F_{b,\sigma}^{(\text{QFT})} \approx \exp\left[-\frac{n(n - 1)}{96}\right].
\]

(33)

\[
\text{AC}_{F,b}^{(\text{QFT})} = \text{AU}_{F,b}^{(\text{QFT})} = F_{b,\sigma}^{(\text{QFT})} \approx \exp\left[-\frac{n(n - 1) - (n - b)(n - b - 1)}{96}\right].
\]

(34)
IV. DISCUSSION

Our motivation for developing analytical scaling formulas is the fact that even the resources of the entire universe are insufficient for building a classical computer that would be capable of simulating a quantum processor in the regime of a large number of qubits [15]. Only analytical methods are powerful enough to explore this regime. Of course, if practical realizations of quantum processors were ideal, there is no need for additional simulations; the processor would perform according to the drawing-board specifications of its quantum circuit. However, by necessity, actual, practical realizations of quantum processors are constructed from hardware components that are not exact implementations of their circuit specifications, but will contain errors and defects. Therefore, a crucial question arises: How do these unavoidable defects influence the performance of quantum processors in a qubit regime that is inaccessible to classical simulation? For two examples of quantum processors, the QFT and the quantum adder, we answer this question by deriving analytical formulas for their performance when implemented with faulty rotation gates whose defects are described statistically with the help of several different error models that are close to what will be encountered in future large-scale quantum processors. Should it turn out that, in practice, the gate defects of these processors follow statistical laws different from those discussed in this paper, our analytical methods are powerful enough to encompass these cases as well. For given quantum hardware and its limitations it is essential for experimentalists and quantum engineers to be able to extrapolate the performance of a desired large-scale quantum processor before building it. This way it can be decided beforehand whether it makes sense to build the quantum processor with available quantum hardware, or whether such an endeavor is fruitful only after a new, more accurate generation of quantum hardware is available.

Quantum hardware defects are, of course, only one side of the issue. Decoherence [26] is the other performance-limiting factor. There are two reasons why we focus on quantum hardware defects: (i) It is much more straightforward to provide analytically reliable and comprehensive performance estimates for defective quantum hardware than it is to accurately model and estimate decoherence effects and (ii) if it turns out that it is already unrealistic to realize a working quantum processor on the basis of available quantum hardware, it is not necessary to study decoherence effects. Therefore, it seems prudent to study the limiting effects of defective quantum hardware first and only then worry about decoherence. This course of action is in line with a similar recommendation by Landauer [20].

Naively one might think that since the action of any quantum processor is equivalent to the action of a large unitary matrix, and because of the linearity of matrix operations, small errors in the matrix elements should result in a small degradation of quantum-processor performance. That this linear thinking is not correct is clearly demonstrated by our fidelity formulas presented in Sec. III B, which show that quantum-processor performance decreases exponentially according to

\[ F \sim \exp(-\alpha n^\beta \gamma^3) \]

where \( \alpha \) and \( \beta \) are positive constants, \( n \) is the number of qubits, and \( \gamma > 0 \) is a measure of the size of the defects. This form of fidelity scaling is valid for both the QFT and the quantum adder.

In this connection we mention that it is not just a matter of waiting for the next generation of hardware. According to (35) the fidelity scales badly in the number of qubits \( n \) and thus implies a practical if not fundamental (e.g., natural transition line widths) limit on the number of qubits, even without considering decoherence. Since we need \( F \geq 0.1 \) for acceptable quantum-processor performance, the exponent in Eq. (35) needs to be \( \gamma \geq 1 \), which implies

\[ \gamma \leq \frac{1}{\sqrt{\alpha n^\beta}} \]  

(36)

Obviously, for given practical or fundamentally achievable bounds on \( \gamma \), this limit depends sensitively on the constants \( \alpha \) and \( \beta \), thus providing an additional reason for accurate scaling formulas in the large-\( n \) regime.

Our work is not the first to address hardware defects in quantum processors. Coppersmith [17] noticed that both the classical and quantum Fourier transforms incur only exponentially small errors if matrix elements (or quantum gates) with exponentially small rotation angles are deleted. Since this pruning operation of matrix elements (or quantum gates) results in a banded structure of the respective classical and quantum circuit diagrams, we called this pruning operation banding [15,19]. The banding idea, introduced by Coppersmith, was further developed, both analytically and numerically, by Fowler and Hollenberg [18], who showed that, assuming ideal quantum gates without defects, a banded matrix with bandwidth \( b = 8 \) is sufficient for code-breaking applications. In Refs. [15,19], with simulations of QFT performance up to 40 qubits, we confirmed this result and provided traditional analytical scaling relations.

While the possibility of banding is already a substantial boon for practical quantum-processor construction, since, instead of scaling quadratically in \( n \) for full bandwidth, the size of a given device with fixed bandwidth scales only linearly in the number of qubits \( n \), the question remains of how gate defects in the remaining, active, gates affect quantum-processor performance. First numerical simulations addressing this point were performed by Cirac and Zoller [20], who considered the case of \( n = 8 \) qubits and assumed that all gates are active (no banding). The main result of this investigation was that an eight-qubit circuit is able to sustain an error level of up to 5\%, i.e., this eight-qubit system was found to be robust with respect to gate errors. These calculations were extended by Miquel et al. [30] to a system with \( n = 18 \) qubits, again confirming robustness of the quantum processor. An analytical fidelity formula, similar in structure to (35) and based on a phase-diffusion model, was also provided.

Thus, the general idea of robustness of quantum processors with respect to gate defects, due to both banding and defects in the active quantum gates, is well established and has been around since about the mid 1990s. However, the general notion of robustness is not enough. As discussed in connection with (35), it has to be analyzed and carefully characterized in order to be able to exploit it experimentally and technologically. For instance, there is a qualitative difference between \( \beta = 1 \) and \( \beta = 0 \).
and $\beta = 2$ in Eq. (35). In the first case, i.e., for $\beta = 1$, gate defects, even for quantum processors consisting of several thousand computational qubits, are relatively benign since the required gate accuracy, according to (36), scales like $1/\sqrt{N}$. In the second case, i.e., for $\beta = 2$, gate defects are more critical and, depending on $\alpha$, may seriously limit the possible size of quantum processors.

While earlier published work focused on numerical investigations for a small number of qubits [20,30] or analytical and numerical investigations of banding that do not include gate defects [17,18], our work goes qualitatively beyond these works by providing asymptotic, reliable, analytical $n$-scaling formulas that can be used for processors consisting of thousands of qubits that simultaneously include banding and defects. In addition, with the help of numerical simulations, all of our formulas are carefully checked for accuracy in the classically accessible small-$n$ regime.

While in our earlier work we investigated the effects of banding [15,19,27,31] and defects [16,22,23] separately, in this paper, we studied formulas including banding and defects simultaneously. Deriving these formulas required the development of a more powerful analytical technique. Furthermore, this technique is generally applicable to the computation of combined asymptotic scaling formulas for a wide range of defect models, which include simultaneous gate pruning (banding) and defects. These combined scaling formulas are not just the product of the fidelity for banding and the fidelity for the defects, separately. A nontrivial interference of banding [15,19,27,31] and numerical investigations of banding that do not include gate defects, even if the number $N$ of angles in the set is small (on the order of 20), excellent performance of the quantum processor operated with these angles will result. This example shows how the set $S_N$ may come about naturally and may lead to a valuable shortcut in the construction of the quantum hardware for realistic quantum processors.

So far in this paper we have investigated the fidelity of a QFT processor and a quantum adder processor in the presence of gate errors, both analytically and numerically. In particular, we focused on the random hierarchy, i.e., we draw approximate rotation gates that best match the exact rotation gates from a randomly generated set of numbers whose statistical distribution is uniform. The uniform distribution represents the larger gate angles relatively accurately, but completely misses the exponentially small angles (see Fig. 2). This might suggest that the uniform distribution is not appropriate and should be replaced with a distribution better tailored to the exponentially decreasing nature of the rotation angles in $j$. Following this line of reasoning, we replaced the uniform distribution in angle with a uniform distribution in $j$. We generate $N$ random numbers that range from 0 to $n$ and pick those that are closest to the integers ranging from 1 to $n - 1$ to replace the integer parameter $j$ of the exact gates, $\theta_j = \pi/2^j$, in an $n$-qubit QFT. Denoting the best approximate gates of $\theta_j$ as $\tilde{\theta}_j = \pi/2^j$, where the $\xi_j$ are those random numbers drawn from the randomly generated set $S_N$ of size $N$ that best match $j$, we show in Fig. 13 the rotation gate angles $\tilde{\theta}_j$ (red closed squares) compared with their corresponding approximations $\theta_j$ (green closed circles) as a function of qubit distance $j$ for $j = 1, \ldots, 10$. The approximations $\tilde{\theta}_j$ are the best matches for their corresponding $\theta_j$, drawn from a set of $N = 20$ random numbers whose statistical distribution is uniform on an exponential scale ranging from 0 to $n$. Shown in the figure is the case of $n = 17$. 

![FIG. 13. (Color online) Exact rotation angles $\theta_j$ (red closed squares) compared with their corresponding approximations $\tilde{\theta}_j$ (green closed circles) as a function of qubit distance $j$ for $j = 1, \ldots, 10$. The approximations $\tilde{\theta}_j$ are the best matches for their corresponding $\theta_j$, drawn from a set of $N = 20$ random numbers whose statistical distribution is uniform on an exponential scale ranging from 0 to $n$. Shown in the figure is the case of $n = 17$.](042301-13)
Appendix A. List of Publications

Y. S. NAM AND R. BLUMEL

PHYSICAL REVIEW A 92, 042301 (2015)

![Fig. 14](color online) Exact rotation angles \( \theta_j \) (red closed squares) compared with their approximations \( \tilde{\theta}_j \) for the uniform (green closed circles) and exponential (blue closed triangles) hierarchies, as a function of qubit distance \( j \) for \( N = 20 \) and \( n = 17 \) as the ones used in Fig. 14, the difference \( \epsilon_j = |\theta_j - \tilde{\theta}_j| \), where \( \tilde{\theta}_j \) are the best approximations of \( \theta_j \) produced according to the uniform or the exponential hierarchies, averaged over 10,000 realizations of the random number set \( S_N \), as a function of \( j \). As expected, the uniform hierarchy better approximates the rotation gates \( \theta_j \) with small \( j \) (large rotation angles) and the exponential hierarchy better approximates the rotation gates \( \theta_j \) with large \( j \) (small rotation angles). In particular, on average the uniform ensemble represents the rotation angles of the first gate with an accuracy that is about 6 times better than the exponential ensemble, where the factor becomes 3 for the second gate and about 1.5 for the third gate. We also observe that there is a crossover between the two hierarchies at \( j \) between 3 and 4, i.e., for the current case of \( N = 20 \) and \( n = 17 \), the uniform hierarchy is better at approximating \( \theta_j \) with \( j \leq 3 \) and the exponential hierarchy is better at approximating \( \theta_j \) with \( j > 4 \). In addition, while the uniform hierarchy exhibits two plateaus at \( \epsilon \approx 0.07 \sim 0.08 \) (see the inset of Fig. 14, small-\( j \) values) and 0.15 (see the inset of Fig. 14, large-\( j \) values), the exponential hierarchy case exhibits an exponential scaling of \( \epsilon \approx 0.8 \times 2^{-j} \) (fit not shown).

In order to explain the origins of these observations, we now turn to the following analytical analysis. Given \( N \) random numbers generated between 0 and \( n \), the probability \( P(d; N) \) to find a random number \( \xi_j \) between 1 and \( n - 1 \), inclusively, within a distance \( d \) of \( j \), is \( \sim(n-2d)/n^N \), which, for \( d \sim n/N \) and large \( N \), may be written as \( \exp(-2dN/n) \). This means that the approximate gate \( \tilde{\theta}_j \) has the form \( \pi/2^{1/2} \cdot r_j \), where \( r_j \) is a random number distributed, up to normalization, according to the bivariate exponential function \( \exp(-2dN/n) \).

Rewriting \( \tilde{\theta}_j \) as \( \pi/2^{1/2} \cdot r_j \), we see that, if \( r_j \) is sufficiently small or \( N \) is large enough, we may approximate \( \tilde{\theta}_j \approx \theta_j [1 - \ln(2) n] \). Solving for \( \epsilon_j = |\tilde{\theta}_j - \theta_j| \), then, since the ensemble average of \( r_j \) evaluates to \( n/2N \), we obtain

\[
\langle \epsilon_j \rangle_{\text{exp}} \approx \frac{\pi}{2N} \frac{n \ln(2)}{2^{j/2}},
\]

where \( \langle \cdots \rangle \) denotes an ensemble average.

Following the analysis shown in Sec. 1B, i.e., \( \epsilon_j = |\tilde{\theta}_j - \theta_j| \) follows a bivariate exponential distribution function that scales like \( \sim \exp(-2Nd/\pi) \) for the uniform hierarchy, given \( \theta_j \) is sufficiently larger than the error \( \epsilon_j \), we may write

\[
\langle \epsilon_j \rangle_{\text{univariate}} \approx \frac{\pi}{2N}.
\]

If, however, \( \theta_j \ll \epsilon_j \), we may no longer use a bivariate distribution; rather, we must employ a univariate distribution in the limit \( \theta_j \ll \epsilon_j \) since the best approximate angle \( \tilde{\theta}_j \) will be larger than the exact angle \( \theta_j \). In this case, we obtain

\[
\langle \epsilon_j \rangle_{\text{univariate}} \approx \frac{\pi}{N}.
\]

Evaluations of (37)–(39) with \( N = 20 \) and \( n = 17 \) match the previously discovered exponential and plateau behaviors of \( \langle \epsilon_j \rangle \) in Fig. 14 to an excellent degree. In addition, the transition \( j \) that marks the crossover from the left to the right plateau in the uniform hierarchy case is correctly predicted by letting \( \epsilon_j \) be comparable to \( \pi/j/N \). Furthermore, equating (37) and

\[
042301-14
\]
Appendix A. List of Publications

ANALYTICAL FORMULAS FOR THE PERFORMANCE . . .

PHYSICAL REVIEW A 92, 042301 (2015)

(38) yields the crossover
\[ I_{\text{crossover}} = \frac{\ln[n \ln(2)]}{\ln(2)} \]  
(40)
below which the uniform hierarchy performs better than the exponential hierarchy in approximating \( \theta \) and vice versa, which correctly predicts the aforementioned crossover shown in the inset of Fig. 14. We point out that (40) is independent of \( N \), meaning, regardless of the size of the random set \( S_N \), there always exists a critical \( n \), such that for \( n > n_c \), a \( \theta \) for a given \( j \) is always better approximated by the uniform hierarchy than the exponential hierarchy. In particular, the smaller the \( j \), the smaller \( n \), is, implying a more favorable \( n \)-scaling relation of fidelity for the uniform hierarchy than for the exponential hierarchy.

To confirm that this is indeed true, once again, we start with \( \tilde{\theta}_j \approx \theta_j[1 - \ln(2)/j] \) for the exponential hierarchy. We see that this is identical to the RC noise investigated in Sec. III B for the quantum adder (see [16] for the case of the QFT), which can be shown to result in the QFT fidelity
\[ F \approx \exp\left[ \frac{\pi^2 \ln^2(2)}{36(2N)} n^2 \right]. \]  
(41)
Consistent with our earlier expectations, this result shows that the QFT equipped with the exponential random hierarchy yields a fidelity scaling law, which, to leading order in \( n \), is of the form \( \ln(F) \sim -n^2 \), one power in \( n \) worse than the results reported in Eq. (3), i.e., \( \ln(F) \sim -n^3 \), for the regular, uniformly distributed random hierarchy. Therefore, surprisingly, the exponential distribution performs worse than the uniform distribution. On the upside, this is good news for quantum engineering, since it is far more straightforward to realize uniformly distributed rotation angles than it is to realize exponentially distributed rotation angles. In addition, this result confirms our general rule that it is better to represent large rotation angles than small rotation angles, which here is expressed via the fact that the uniform distribution performs better than the exponential distribution. It also provides yet another example of the power of our analytical methods, which are able to deal successfully [see (41)] with a rather unconventional distribution of rotation angles (uniformly distributed in the exponents).

The least-favorable state \([2^n - 1] \) plays a special role in our analytical derivations. It is the state that, statistically speaking, produces the worst results in terms of quantum-processor performance and therefore serves as a test state to produce a lower limit of processor fidelity. The following may be perceived as a problem with this procedure. When focusing on a particular realization of defective gates, i.e., a single copy of a quantum processor, it is possible that a particular state, different from \([2^n - 1] \) but more adapted to a certain particular realization of gate defects, might actually yield results worse than \([2^n - 1] \), while \([2^n - 1] \) may actually be the most-favorable state. However, this scenario is statistically extremely unlikely. Therefore, without preknowledge of specific realizations of gate defects in an actually existing quantum processor, we have to assume that gate defects follow a statistical distribution, which requires us to average over many realizations of gate defects (typically hundreds or thousands, as done in this paper) to arrive at statistically meaningful conclusions. As shown in Fig. 3 and analytically proved in Appendix A, when ensemble averages are properly taken, \([2^n - 1] \) is indeed the least-favorable state. The same considerations apply to the addend state \([2^n - 1] \), which, in Appendix B, in conjunction with the state \([2^n - 1] \), is shown to be the least-favorable addend state in the statistical sense.

The central theme of our paper is banding in the presence of defects. Intuitively, it is clear that it may be better to discard an obviously wrong gate rather than keep it. However, what is the formal criterion? What is the noise threshold that decides which gates to keep and which ones to discard? Based on the interference term, derived in this paper, between bandwidth and the size of the defects, we are able to answer these questions quantitatively.

Let us start with the Gaussian RC and RU cases defined in Sec. III B and address the following question: For a chosen fixed bandwidth \( b \), for what values of \( \sigma \) is \( g_{opt,RU}^F > g_{opt,\sigma}^F \)? With (27) and (28) we obtain
\[ \sigma > \frac{12}{\sqrt{6}} \frac{n - b - 1}{n - b - 4/3} \approx 5. \]  
(42)
This shows that in the case of relative errors the crossover between harmful banding and beneficial banding occurs only if \( \sigma \) is very large. Clearly, such large \( \sigma \) are uninteresting since, inserted in Eqs. (27) or (28), we obtain exponentially small fidelities. We conclude that in the case of relative errors, banding is never useful. This, however, requires that the relative errors in \( \theta \) can be controlled at any level, which is experimentally impossible. Due to the exponentially decreasing nature of the rotation angles, exponential smallness is very quickly and completely impossible to distinguish \( \theta \) from \( \theta_j \) (say, \( j > 20 \)) and thus to keep the relative errors at their prespecified levels. Therefore, for a sufficiently large number of qubits (e.g., \( n > 20 \)), banding is always beneficial, experimentally. As a result, because of the limitation of experimental equipment, the model of absolute errors is more realistic.

In the case of absolute errors there is indeed a meaningful crossover between harmful and beneficial banding. We see this in the following way. Starting from (30), the maximum in performance corresponds to the minimum of the argument of the exponential functions in Eq. (30), viewed as a function of \( b \) for constant \( \sigma \). Under the assumptions \( n \gg 1 \) and \( n \gg b \), the minimum occurs at
\[ b_{opt,\sigma}^F = \frac{1}{2 \ln(2)} \ln \left[ \frac{8\sigma^2 \ln(2)}{3b^2} \right]. \]  
(43)
This criterion is independent of \( n \) and depends only logarithmically on \( \sigma \). Therefore, even for the smallest reasonable \( \sigma \), the criterion \( b_{opt,\sigma}^{F} < n - 1 \) is easily fulfilled. For \( \sigma = 10^{-3} \), e.g., we obtain \( b_{opt,\sigma}^{F} = 12 \), compatible with banding estimates ranging from \( b = 8 \) [18] to \( b = 22 \) [32] for the QFT with perfect gates. The analogous formula for the quantum adder, obtained from (22), is
\[ b_{opt,\sigma}^{(QA)} = \frac{1}{2 \ln(2)} \ln \left[ \frac{8\sigma^2 \ln(2)}{3b^2} \right]. \]  
(44)
identical to (43). Derived from (34) and (26), the formula analogous to (43) and (44) for optimal banding in the uniformly
distributed case is
\[ b_{\text{optimal}}^{(\text{QFT})} = \frac{1}{2 \ln(2)} \ln \left( \frac{8\pi^2 \ln(2)}{e^2} \right). \] (45)

In the case of the uniform and exponential hierarchies, the parameter \( N \), i.e., the size of the random set \( S_N \), takes the place of the error levels \( \sigma \) and \( \epsilon \) and we may expect that, depending on \( N \), there may also be a crossover between regions in which banding is helpful versus harmful. In general, we expect that banding is harmful if \( N \) is very large since in this case the rotation angles \( \theta_j \) can be approximated with excellent accuracy. This is particularly clear in the limit of \( N \to \infty \) since in this case all rotation angles are represented perfectly and any banding obviously reduces the performance of the corresponding quantum processor. However, for small \( N \), banding may be helpful since in this case, in particular in the case of the uniform hierarchy, small rotation angles (large \( j \)) are not well approximated. Therefore, we expect the existence of a critical \( N_c \) below which (in \( N \)) banding is helpful and above which (in \( N \)) banding is harmful.

We use the full-bandwidth QFT fidelity scaling law (3) together with the banded QFT fidelity scaling law (6) to determine where the crossover between the helpful banding regime \((N < N_c)\) and the harmful banding regime \((N > N_c)\) occurs for the QFT. For given \( b \), equating (3) and (6), and assuming small \( \delta \), we obtain
\[ N_c^{(\text{QFT,URH})} \approx \frac{2}{\sqrt{8}} \left( n - b \right), \] (46)
where URH stands for uniform random hierarchy. Now that we know how to compute \( N_c \) for given \( b \), we would like to choose \( b \) as optimally as possible. Computing the maximum of the fidelity (6) as a function of \( b \) for fixed \( N \), we obtain
\[ b^{(\text{QFT,URH})}_{\text{optimal}} = \frac{1}{2 \ln(2)} \ln \left( \frac{8 \ln(2) N^2}{3} \right). \] (47)

As an example, for \( N = 20 \), used in Sec. II A, we obtain \( b^{(\text{QFT,URH})}_{\text{optimal}} = 5 \). Therefore, the bandwidths chosen in Figs. (4b) and (5b) are close to optimal.

A similar analysis can be done for the quantum adder as well. Equating (13) and (17) and assuming small \( \delta \) and large \( n \), we obtain
\[ N_c^{(\text{QA,URH})} \approx \frac{2}{\sqrt{3}} \left( n - b \right), \] (48)
and, similar to the QFT case (47), the optimal bandwidth reads
\[ b^{(\text{QA,URH})}_{\text{optimal}} = \frac{1}{2 \ln(2)} \ln \left( \frac{2 \ln(2) N^2}{3} \right). \] (49)

Although less useful in practice, for completeness, we provide here the corresponding formulas for the exponential random hierarchy. For the QFT we obtain
\[ N_c^{(\text{QFT,ERH})} \approx \frac{n \ln(2)}{2} \ln \left( \frac{1}{3(n-b-1)} \right), \] (50)
and for the quantum adder, extending the domain from which we draw random numbers from \((0,n)\) to \((-1,n)\), we obtain
\[ b^{(\text{QA,ERH})}_{\text{optimal}} = n - 1 + \frac{1}{2 \ln(2)} \ln \left( \frac{1}{3 - 12 N^2 / (n+1)^2 \ln^2(2)} \right). \] (51)

V. CONCLUSION

In this paper we investigated the fidelity of quantum processors subjected to rotation gate defects. In particular, we derived analytically the scaling of the fidelity of the QFT and the quantum adder processors equipped with randomly hierarchical gates. In addition, we derived analytical fidelity scaling laws for the quantum adder, subjected to gate errors with Gaussian or uniform distributions. Our analytical analysis, which matches numerical results to an excellent degree, shows that the QFT and the quantum adder processors are surprisingly robust against any type of gate errors in general and in particular against gate errors introduced according to the uniformly distributed random hierarchy, a particularly unfavorable type of defect, since it completely disregards the natural exponential ordering (hierarchy) of the rotation gates.

By demonstrating the extraordinary robustness of quantum processors with respect to hardware flaws, to the effect that the QFT and the quantum adder, e.g., still work even if most of their controlled-rotation gates are pruned and the surviving ones are implemented via selection from a randomly generated set, our work adds to the expectation that a quantum computer is a realizable and practical instrument that will change the paradigm of computation.

APPENDIX A: LEAST-FAVORABLE INPUT STATE FOR THE QFT

In this Appendix we show that the input state \( |\psi_{\text{actual}}\rangle = |2^w - 1\rangle \) is the most-unfavorable integer input state for an \( n \)-qubit QFT, whose performance is measured in terms of the fidelity
\[ F = |\langle \psi_{\text{ideal}} | \psi_{\text{actual}} \rangle|^2. \]

We start by invoking the approximate fidelity expression (2), which we can rewrite as
\[ F \approx |\langle \psi_{\text{ideal}} | \Delta \psi_{\text{ideal}} \rangle|^2, \] (A1)

where \(|\psi\rangle\) is the integer input state of the QFT; \(\beta\), an integer that ranges from 0 to \(2^n - 1\), denotes the integer state spectrum of the output state of the QFT; \(\cdot \cdot \cdot \beta\) stands for averaging over \(\beta\); and \(\Delta \psi_{\text{ideal}}\) denotes the phase-angle defects associated with the \(n\)-qubit QFT with the input state \(|\alpha\rangle\) and one of the output integer states \(|\beta\rangle\). Since in this paper we focus attention on defective rotation gates with rotation angles \(\theta_1 = \theta_j + \Delta \psi_j\), where the exact rotation angles are given by \(\theta_j = \pi/2^l\), we may write
\[ \Delta \psi_{\text{ideal}} = \sum_{j=1}^{n-1} \sum_{l=1}^{n-j} \theta_{j+l-1} \Delta \psi_{j+l-1}. \] (A2)

where the subscripts \([n-l]\) and \([j+l-1]\) of \(\alpha\) and \(\beta\) denote the \((n-l)\)th and the \((j+l-1)\)th binary digits of the integers.
\[ F \approx \left| \exp \left( \sum_{j=1}^{n-1} a_{|\psi_a\rangle} \Delta \psi_j / 2 \right) \right|^2. \] (A3)

At this point, we clearly see that, if all \( a_{|\psi_a\rangle} \) are 1, we obtain the maximal variance of the phase-angle sum in Eq. (A3). In other words, we obtain the minimal fidelity. Hence, we conclude that \(|\psi_m\rangle = |2^n - 1\rangle\) is indeed the input state of the \( n \)-qubit QFT, which incurs the maximal fidelity penalty.

**APPENDIX B: LEAST-FAVORABLE INPUT STATE FOR THE QUANTUM ADDER**

In the spirit of Appendix A, we show in this Appendix that the choice of \(|\psi_m\rangle = |2^n - 1\rangle\) as input state and \(|\nu\rangle = |2^n - 1\rangle\) as addend state is the most unfavorable combination of integer input and addend states for the \( n \)-qubit quantum adder whose performance is measured in terms of fidelity \( F = \left| \langle \psi_{\text{ideal}} | \psi_{\text{actual}} \rangle \right|^2\). We start with the analytical fidelity expression (10) of the \( n \)-qubit quantum adder, which we can rewrite as

\[ F^{(\text{QFA})} \approx \left| \left\langle \rho^{(\text{QFA})} \right| \psi(m), \nu \rangle \right|^2, \] (B1)

where, in analogy to the description of (A1), \( |\alpha\rangle \) is the integer input state of the quantum adder; \( |\beta\rangle \), denoting the integer state spectrum of the intermediate state immediately following the QFT [the first operation of the quantum adder (see Fig. 6)], is an integer ranging from 0 to \( 2^n - 1 \); \( \{\cdots\}|p\rangle \) stands for averaging over \( |\beta\rangle \); \( \Delta \psi(\alpha, |\beta\rangle) \) denotes the phase angle defects associated with an \( n \)-qubit quantum adder with addend \(|\nu\rangle\) acting on the integer input state \(|\beta\rangle\). According to the gate operations of the quantum Fourier adder in Fig. 6, denoting by \( \theta_j = \theta_j + \Delta \psi_j \) the defective rotation angles, we may write

\[ \Delta \psi(\text{QFA})^{(\text{b}); N} = \sum_{j=0}^{n-1} \sum_{l=1}^{\nu_{|\nu\rangle} \Delta \psi_j,} \] (B2)

which, together with \( \Delta \psi \) of the QFT in Eq. (A2), results in the adder fidelity

\[ F^{(\text{QFA})} \approx \frac{1}{4} \left| \sum_{j=0}^{n-1} \sum_{l=1}^{\nu_{|\nu\rangle} \Delta \psi_j,} \right|^2, \] (B3)

where we performed the \( \beta \) averaging and replaced all occurrences of binary bits of \( \beta \) with \( 1/2 \). At this point, we clearly see that, if the bit spectra of (i) \( \alpha \), (ii) \( \nu \), and (iii) \( (\alpha + \nu) \) mod \( 2^n \) are as saturated as possible with 1, we obtain the minimal quantum adder fidelity. This is obtained when \( \alpha = 2^n - 1 \), \( \nu = 2^n - 1 \), and \( (\alpha + \nu) \) mod \( 2^n = 2^n - 2 \). This implies that the choice \(|\psi_a\rangle = |2^n - 1\rangle\) and \(|\nu\rangle = |2^n - 1\rangle\) is the combination of input and addend states for the quantum adder, which incurs the maximal fidelity penalty.

It is well known that ions stored in a Paul trap, one of the most versatile tools in atomic, molecular, and optical (AMO) physics, may undergo a transition from a disordered cloud state to a geometrically well-ordered crystalline state, the Wigner crystal. In this paper we predict that close to the transition, the average lifetime $\tau_n$ of the metastable cloud follows a power law, $\tau_n \sim (\gamma - \gamma_c)^{-\beta}$, where $\gamma_c$ is the value of the damping constant at which the transition occurs. The exponent $\beta$ depends on the trap control parameter $q$, but is independent of both the number of particles $N$ stored in the trap and the trap control parameter $a$, which determines the shape (oblate, prolate, or spherical) of the ion cloud. In addition, we find that for given $a$ and $q$, $\gamma_c$ scales approximately like $\gamma_c = C \ln(\ln(N)) + D$ as a function of $N$, where $C$ and $D$ are constants.

Our predictions may be tested experimentally with equipment already available at many AMO laboratories. In addition to their importance in AMO trap physics, we also discuss possible applications of our results to other periodically driven many-particle systems, such as, e.g., particle accelerator beams, and, based on our trap results, conjecture that power laws characterize the phase transition to the Wigner crystal in all such systems.

DOI: 10.1103/PhysRevA.93.043424

I. INTRODUCTION

The Paul trap [1,2] is an electrodynamic device for storing charged particles free from contact with material walls for very long periods of time. Trapping is achieved by applying suitable dc and ac voltages to the hyperbolic electrodes of the trap. The resulting electric potentials create an effective potential minimum at the center of the trap, an immaterial trough that confines charged particles, in principle, forever. Storage times ranging from a few hours [3] to a few days [4] have been reported.

One of the most interesting phenomena that has attracted considerable interest in the atomic, molecular, and optical (AMO) community for some time is the observation that ions stored in a Paul trap can occur in two completely different states, a well-ordered crystalline state [5–15], also called the Wigner crystal [10,13,16], and a disordered cloud state [17–20]. Experimentally observed transitions between these two states [3,4,21–24], as well as their theoretical interpretations [3,15,21,25], have also attracted attention in the AMO community. Technological applications of ion crystals are now emerging. For instance, linear and higher-dimensional ion crystals have been proposed as quantum hardware components for quantum computers [9,10].

Theoretically and experimentally, trapping of a single charged particle in an ideal Paul trap is understood in detail [1,2], and even its quantum regime has already been explored [26,27]. However, if multiple particles are stored in the trap simultaneously, the Coulomb interactions between the particles cause their motions to be chaotic [23,28,29]. In this case it is no longer possible to solve their equations of motion analytically. The chaotic motion of the particles has two consequences. (i) Due to the resulting high temperatures, we do not have to worry about quantum effects; a classical description of the trapped particles is sufficient. (ii) The chaotic motion of the particles in the trap causes the phenomenon of radio-frequency (rf) heating [3,19–21,30,31]. Damping must be imparted to this system to counteract the heating, whether by laser cooling [3], buffer gas cooling [4], or some other method, for instance, cooling by the cold, neutral particles of a magneto-optic trap [32]. With a relatively small damping, the rf heating power of the ion cloud will come into equilibrium with the cooling power, resulting from the damping mechanism, and a stationary-state gas cloud will result [3,19–21]. However, with stronger damping, the heating of the cloud can be overcome, and the particles will transition into the crystalline state [3,4,22–24].

In this paper we use large-scale molecular dynamics simulations to predict that close to the cloud $\rightarrow$ crystal transition the lifetimes of ion clouds stored in a Paul trap follow a power law, which may be tested experimentally with equipment available at many AMO laboratories. We also obtain a scaling law for the critical amount of damping required to collapse ion clouds into ion crystals.

Our paper is organized as follows. In Sec. II we present the equations that govern the motion of ions in a Paul trap together with our method of solving these equations and extracting lifetime information from our molecular-dynamics simulations. In Sec. III we present the results of our molecular-dynamics simulations that lead us directly to our two main predictions, i.e., the power-law scaling of the lifetimes of metastable clouds and the scaling of the critical damping required to force the transition from the cloud state into the crystal state. In Sec. IV we discuss our results and their potential applications in a broad class of periodically driven multiparticle systems, such as particle accelerator beams [33,34], dusty plasmas [35,36], surface state electrons [37], and colloidal suspensions [38,39]. We summarize and conclude our paper in Sec. V.

II. THEORY AND METHODS

The coupled equations of motion governing the dynamics of $N$ particles stored in the Paul trap, in dimensionless units [19],
are

\[
\ddot{r}_i + \gamma \dot{r}_i = \frac{a - 2q \sin(2\tau)}{\left(1 + 2x_i + 2y_i - 2z_i\right)} - 2z_i, \quad i = 1, \ldots, N,
\]

where \(\vec{r}_i = (x_i, y_i, z_i)\) is the position vector of ion number \(i\), \(x\) is the dimensionless time, \(\gamma\) is the damping constant, \(N\) is the number of trapped particles, and \(a, q\) are the trap's dimensionless control parameters [19], proportional to the dc and ac voltages applied to the trap’s electrodes, respectively. The conversion between time \(T\) and the number \(n\) of rf cycles is accomplished via \(n = T/\tau\). For given values of \(N, a, q\), and \(\gamma\), we solve (1) numerically with a standard fifth-order Runge-Kutta integrator [40]. Each of our simulations starts at \(t = 0\) with randomly chosen initial conditions drawn from the phase-space box \(-10 < x, y, z < 10\), \(-1 < v_x, v_y, v_z < 1\) with a uniform distribution. We checked that, because of the chaotic nature of the particle dynamics in the trap, all of our results are completely insensitive to both the particular choice of random distribution and the size of the box. To monitor the progress of our simulations, we plot \(\langle x^2(\tau_n)\rangle = \sum_{i=1}^{N} x_i^2(\tau_n) = n\pi/\tau\), \(n\) integer.

III. RESULTS

The result of a typical simulation run is shown in Fig. 1. Since they are chosen at random, all of our initial conditions correspond to energetic particle clouds with large initial values of \(\langle x^2\rangle\) (see data points for \(\tau \approx 0\) in Fig. 1). However, because of the chaotic nature of its dynamics, the particle cloud very quickly loses the memory of its initial conditions and thermalizes. This corresponds to the initial transient (see the near-exponential decay over the first \(\sim 1000\) rf cycles \((\approx 0\) to \(\tau \approx 3000)\) in Fig. 1), followed by the establishment of a metastable stationary state (see the plateau in Fig. 1 of length \(\tau_m \approx 28,000\), where the heating of the cloud comes into equilibrium with the damping. Following this, if, as in Fig. 1, a relatively large \(\gamma\) was chosen, the cloud eventually collapses into the crystal state. In Fig. 1 this final collapse manifests itself as the exponential decay phase immediately following the metastable state (to the right of the second dashed line in Fig. 1) and ending in the crystalline state, characterized by the absence of fluctuations in \(\langle x^2\rangle\) for \(\tau \approx 40,000\). We checked explicitly that during its plateau state the ion cloud is stable in the sense that in addition to \(\langle x^2\rangle\) we checked the expectation values of several other dynamical variables, but did not find any that would decay during \(\tau_m\).

Confirming previous experimental [3,4] and numerical [3] observations, we find that for given \(N, a, q\) the cloud \(\rightarrow\) crystal transition (the final collapse of the cloud in Fig. 1) occurs in the vicinity of a critical value of \(\gamma\), denoted by \(\gamma_c\). In addition, corroborating earlier qualitative experimental observations (see, e.g., Fig. 3 in [3]), we find that, for finite \(N\), and a given finite simulation time \(\tau_{max}\), \(\gamma_c\) is not sharply defined. Therefore, to determine \(\gamma_c\) and its uncertainty, we proceed in the following way. For given \(N, a, q\), we scan \(\gamma\) from \(\gamma_{min} = 10^{-4} \rightarrow \gamma_{max} = 2 \times 10^{-4}\) a \(\gamma\) interval that we know from experience contains \(\gamma_c\) with certainty for \(N\) ranging between 20 and 2000 trapped particles. We find that in the interval \(\gamma_{min} < \gamma < \gamma_{N, a, q}\), \(N\)-particle clouds are stable and never transition into the crystal. Following this is the interval \(\gamma_{c}(N, a, q) < \gamma < \gamma_{max}\), an interval of uncertainty, in which the clouds sometimes transition into the crystal and sometimes not. Adjacent to this is the interval \(\gamma_{c}(N, a, q) < \gamma < \gamma_{c}(N, a, q)\). In which all \(N\)-particle clouds, independently of initial conditions, always transition into crystal. Defining \(\Delta\gamma_c = \gamma_c - \gamma_c\) as the width of the uncertainty interval, we find that \(\Delta\gamma_c\) shrinks, i.e., \(\gamma_c\) and \(\gamma_c\) both move toward each other with increasing number \(N\) of stored particles according to \(\Delta\gamma_c \sim 1/\sqrt{N}\), and also with the maximal time \(\tau_{max}\) allowed for our simulations. To be practical, however, we limited the run time of our simulations to \(\tau_{max} = 5 \times 10^n\), very much larger than the typical decay time \(1/\gamma\) of our system. We found that this choice of \(\tau_{max}\) yielded consistent results, and we saw no need to increase \(\tau_{max}\). Having determined the uncertainty interval \([\gamma_1, \gamma_2]\), we define \(\gamma_c = (\gamma_1 + \gamma_2)/2\). As an example, for \(q = 0.2, a = q^2/2\), and \(N\) ranging from 25 to 1000 particles, we plot, in Fig. 2, the \(\gamma_c\) values (red, closed circles) determined according to the numerical procedure described above. The uncertainty \(\Delta\gamma_c\) of \(\gamma_c\) is smaller than the size of the plot symbols in Fig. 2. We found that neither a power law \((\gamma_c = AN^B + C, \text{ where } A, B, C \text{ are fit parameters; blue, solid line in Fig. 2})\) nor a log law \((\gamma_c = A \ln(N) + B, \text{ where } A, B \text{ are fit parameters; green, solid line in Fig. 2})\) fits the \(N\) dependence of \(\gamma_c\) satisfactorily, but that the iterated log law,

\[
\gamma_c(N, q = 0.2, a = 0.02) = C \ln[\ln(N)] + D \tag{2}
\]

(red, solid line in Fig. 2), provides an excellent fit, where \(C = 7.49 \times 10^{-4}\) and \(D = -2.97 \times 10^{-4}\). For \(N = 100\), \(\gamma_c = 8.47 \times 10^{-4}\). This is the reason for why the cloud in Fig. 1, subjected to \(\gamma = 8.81 \times 10^{-4}\) for \(\tau \approx 40,000\), ultimately collapses into the crystal state.

At present, we are not able to provide an analytical explanation for the origin of the iterated-log scaling of \(\gamma_c\). However, the weak \(N\) dependence of \(\gamma_c\) reflects in its \(\ln[\ln(N)]\)
scaling, may be understood qualitatively in the following way. Since, in the large-$N$ limit, and close to the cloud $\rightarrow$ crystal transition, charged particles in the interior of the Paul trap have a near-constant density (similar to a charged liquid in a confining harmonic-oscillator potential), all particles deep in the interior of the trap may be treated as equivalent, since they are experiencing approximately the same homogeneous surrounding charge density. Given that $\gamma$ represents the energy loss per particle [see (1)], $\gamma_c(N)$ is expected to be constant. Thus, the small deviation of the $\gamma_c(N)$ scaling from constancy, i.e., the presence of the $\ln(\ln(N))$ term, is a finite-size (surface) effect that is hard to capture analytically.

We now turn to a more in-depth investigation of the cloud $\rightarrow$ crystal transition, i.e., we focus on the interval $\gamma > \gamma_2 > \gamma_c$. In particular, we are interested in the time it takes for a cloud to crystallize, once it has achieved its metastable state (the plateau in Fig. 1), i.e., we are interested in the length of time $\tau_m$ the cloud spends in the metastable state before quickly transitioning into the crystalline state (ultimate exponential decay in Fig. 1). It is intuitively clear that the larger $\gamma$, the shorter $\tau_m$. Conversely, when approaching $\gamma_2$ from above, and taking into account that clouds are stable for $\gamma < \gamma_1 \approx \gamma_c$, $\tau_m$ should increase as $\gamma$ approaches $\gamma_2 \approx \gamma_c$. This suggests a power law of the form,

$$\tau_m(N,a,q;\gamma) \sim [\gamma - \gamma_c(N,a,q)]^{-\beta(N,a,q)},$$

for $\gamma \gtrsim \gamma_c$, where $\beta > 0$. To find $\beta$ we ran our simulations for fixed $N,a,q$ for $\gamma$ values that approach $\gamma_c(N,a,q)$ from above and extracted $\tau_m$ via an automated, objective process [41]. Since the motion of the particles in the Paul trap is fully chaotic, small changes in the initial conditions can produce different values of $\tau_m$. Therefore, we ran our simulations with 50 different initial conditions and defined $\tau_m$ as the average over the 50 resulting $\tau_m$ values. To characterize the statistical

![Graph](https://example.com/graph.png)

FIG. 2. Critical value $\gamma_c(N,q = 0.2, a = 0.02)$ of the damping constant $\gamma$ (see (1)) as a function of $N$ at which the cloud $\rightarrow$ crystal transition occurs (red, closed circles). The best-fitting power law (blue, solid line), log law (green, solid line), and the iterated log law (red, solid line) are also shown. Only the iterated log law, according to (2), provides a satisfactory fit.

![Graph](https://example.com/graph.png)

FIG. 3. Average time $\tau_m$ spent in the metastable state versus the distance $\gamma - \gamma_c$ from the critical point $\gamma_c$. (a) $q = 0.15$, (b) $q = 0.20$, and (c) $q = 0.25$ for the spherical case $a = q^2/2$. Shown are $N = 100, 200, 500$ (blue, red, green, respectively). (d) $q = 0.20$, where $a = 0$ (oblate, red), $a = q^2/2$ (spherical, blue), and $a = 4q^2/5$ (prolate, green) for $N = 100$. The exponents $\beta$ and the goodness of the fit, tested according to $\chi^2$ statistics, are available in Table 1.
TABLE I. Exponents $\beta$ and the corresponding goodness-of-fit parameters $\chi^2$ obtained from fitting the power law (3) to the data in Fig. 3. In the case of spherical clouds ($a = q^2/2$), for a given $q$ and several different $N$, the exponents $\beta$ lie within the margins of error, with the exception of $q = 0.15$ and $N = 100$, which is an outlier. The exponents $\beta$ obtained from different shapes of clouds resulting from several different choices of $a$ lie within the margins of error as well. Thus, $\beta$ is approximately independent of $a$ and $N$.

<table>
<thead>
<tr>
<th>Simulation parameters</th>
<th>$\beta$</th>
<th>$\chi^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a = q^2/2$ (spherical)</td>
<td>$q = 0.15$</td>
<td>$N = 100$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$N = 200$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$N = 500$</td>
</tr>
<tr>
<td></td>
<td>$q = 0.20$</td>
<td>$N = 100$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$N = 200$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$N = 500$</td>
</tr>
<tr>
<td></td>
<td>$q = 0.25$</td>
<td>$N = 100$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$N = 200$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$N = 500$</td>
</tr>
<tr>
<td>$N = 100, q = 0.2$</td>
<td>$a = 0$</td>
<td>(oblate)</td>
</tr>
<tr>
<td></td>
<td>$a = q^2/2$</td>
<td>(spherical)</td>
</tr>
<tr>
<td></td>
<td>$a = 4q^2/5$</td>
<td>(prolate)</td>
</tr>
</tbody>
</table>

spread of the $\tau_m$ values, we also computed the standard error $\sigma = [(1/50) \sum_{i=1}^{50} (\tau_m - \bar{\tau})^2]^{1/2}/\sqrt{50}$. For $q = 0.15$, 0.20, and 0.25 and $a = q^2/2$ (spherical clouds), Figs. 3(a)–3(c) show the resulting dependence of $\tau_m$ on $(\gamma - \gamma_i)$ (plot symbols). The length of the horizontal error bars in Fig. 3 equals $\Delta \gamma_i$. The vertical error bars in Fig. 3, of length $\sigma$, are smaller than the plot symbols. If (3) holds, the data in Fig. 3 should fall on straight lines. According to Fig. 3, this is indeed the case.

Following [40], we extracted the exponents $\beta$ of the power law (3) from the data presented in Fig. 3 according to the following procedure. We define

$$\chi^2(d, \beta) = \sum_{i=1}^{v} \frac{(\eta_i - d - \beta \xi_i)^2}{\sigma_i^2 + \beta^2 \xi_i^2},$$

where, for given $N, a, q, i$ counts the $v$ data points available in each data set, $\eta_i = \ln(\tau_m)$, $\xi_i = \ln(\gamma_i - \gamma)$, $\sigma_i = \Delta \eta_i = \Delta \xi_i$, and $\sigma_i^2 = \Delta \xi_i^2 = \Delta \gamma_i^2/\gamma_i^2$. The intercept $d$ and the exponent $\beta$ are then obtained by minimizing (4) with respect to $d$ and $\beta$. We report the $\beta$ values and associated $\chi^2$ values obtained at the $\chi^2$ minima in Table I. The $\chi^2$ values are all of the order or smaller than 1, indicating that the straight-line fits in Fig. 3 are meaningful. The uncertainties in $\beta$ were computed according to formula 15.3.5 of [40] as the extrema of the error ellipse defined by the second derivatives of $\chi^2$ with respect to $d$ and $\beta$. The values of the uncertainties in $\beta$, obtained this way, are also stated in Table I.

IV. DISCUSSION

Figure 3 and the results summarized in Table I, support the validity of the power law (3) with an exponent $\beta$ that depends only on $q$, but not on $a$ or $N$. According to the quoted uncertainties in $\beta$ (see Table I), we see that the individual exponents are more accurately defined for smaller values of $q$. The reason for this is straightforward. According to (1), $q$ determines the strength of the ac drive of the trap, which, in turn, determines the degree of chaos in the trap. Therefore, smaller $q$ means less chaos, which implies smaller $\Delta \gamma_i$, which, in turn, results in a better defined $\beta$.

According to Fig. 3, for $\gamma - \gamma_i \gtrsim 3 \times 10^{-4}$, the duration $\tau_m$ of the metastable state is smaller than 1000 (i.e., smaller than $\approx 300$ rf cycles), which, on the scale of Fig. 1, is a very small time interval. In fact, as corroborated by Fig. 1, it is no longer possible in this case to clearly separate the metastable state from the initial thermalization stage. This is expected since, for a relatively large $\gamma > \gamma_i$, the cloud is cooled so fast that the metastability does not have enough time to clearly manifest itself. This provides us with a natural cutoff damping parameter, i.e., $\gamma_{cutoff}(N, a, q) = \gamma_i(N, a, q) + 3 \times 10^{-4}$, above which metastability can no longer be defined. It also provides us with an estimate for the onset of the power-law behavior, i.e., we expect the power law to hold for $\gamma - \gamma_i \lesssim 3 \times 10^{-4}$. Although, according to (2), $\gamma_{cutoff}$ depends, via $\gamma$, on $N$ and both trap control parameters, the dependence on $N$ is weak, especially for large $N$.

Our results are directly applicable to currently conducted Paul-trap experiments. Our work may, for instance, be used to determine the cooling power and its duration that need to be applied to the charged particles stored in a Paul trap in order to ensure crystallization. Using our results shown in Fig. 3(b), for instance, one can predict that, for a typical rf-frequency of $f = 1$ MHz, a damping constant 5% above the critical damping $\gamma_i$ results in a metastable-state lifetime of $\tau_m \sim 10^3$, or $\approx 3$ ms.

In this paper we focused on the cloud $\rightarrow$ crystal transition. But what about crystal $\rightarrow$ cloud transitions? Indeed, these were reported in the experimental [4] as well as in the theoretical [12,13,15] AMO literature. They are, however, of a completely different nature than the phenomena studied in this paper. Corroborating earlier results [3,21], we found that in an ideal Paul trap described by (1), even in the absence of damping (i.e., $\gamma = 0$), crystal $\rightarrow$ cloud transitions do not occur. We checked this fact explicitly for many different $a, q$ combinations, and $N$ ranging from 25 to 200. The explanation is straightforward. There is no chaos in the crystal state. Therefore, crystals do not heat, and are therefore stable even in the absence of damping. In experiments that do observe crystal $\rightarrow$ cloud transitions, the crystals are heated by an outside source, for instance, by coupling to the hot, ambient air in the experiments reported in [4]. Thus, while crystal $\rightarrow$ cloud transitions certainly occur in experiments in which the crystals are coupled to a heat bath, their underlying mechanism is completely different from the self-contained, dynamical transitions studied in this paper.

In addition to radio-frequency traps, widely used in AMO physics, our results and methods are also applicable to a host of many-particle systems in various other areas of physics, which also show Wigner crystallization [33–39]. Of particular importance in our context are crystalline beams [33,34]. This is so, since in their rest frame the dynamics of the beam particles are described by equations very similar to (1), and a phase transition, very similar to the one described in this paper, induced by laser or electron cooling, precedes the transition into the Wigner crystal [42]. We mention that beam
crystallization has already been observed in a mini-storage ring [43], an excellent system for testing the universality of our predictions.

V. SUMMARY AND CONCLUSIONS

Summarizing, we showed that for ions stored in a Paul trap, a critical value, $\gamma_c(N,a,q)$, of the damping constant $\gamma$ exists at which the cloud $\rightarrow$ crystal transition occurs. We showed that $\gamma_c$ scales approximately like $\ln[\ln(N)]$ in the number $N$ of stored particles in the trap. In addition, we showed that close to the cloud $\rightarrow$ crystal transition the mean lifetime $\tau_m$ of the metastable cloud follows a power law. Many AMO laboratories, nationally and internationally, are equipped to test our predictions. We are confident that our predictions will hold up to experimental tests.

[References]

41. We compute a moving average of $(t^2)_{\Delta t}$ (averaging over a time interval $[t - \Delta t, t + \Delta t]$), which yields very sharp transitions suitable for an automatic and objective extraction of $\tau_m$ via a computer program. The choice of the interval $\Delta t$, which is of the order of the temporal transition width of the cloud $\rightarrow$ crystal transition, is not critical.
Bibliography


[41] B. Verkhovsky, *Generalized Baby-Step Giant-Step Algorithm for Discrete Loga-
BIBLIOGRAPHY


[51] D. G. Cory, M. D. Price, A. F. Fahmy and T. F. Havel, Nuclear magnetic reso-


[95] V. Kliuchnikov, D. Maslov, and M. Mosca, *Asymptotically optimal approximation
of single qubit unitaries by Clifford and T circuits using a constant number of ancillary qubits, Phys. Rev. Lett. 110, 190502 (2013).


[106] S. Hallgren, Polynomial-time quantum algorithms for Pell’s equation and the prin-


[125] Y. S. Nam and R. Blümel, *Optical simulator of the quantum Fourier transform*, Accepted for publication in Euro. Phys. Lett..


BIBLIOGRAPHY


BIBLIOGRAPHY


