Scalability of Shor's algorithm with a limited set of rotation gates

Austin G. Fowler and Lloyd C. L. Hollenberg
Centre for Quantum Computer Technology, School of Physics, University of Melbourne, Victoria 3010, Australia
(Received 15 December 2003; revised manuscript received 26 April 2004; published 29 September 2004)

Typical circuit implementations of Shor's algorithm involve controlled rotation gates of magnitude $\pi/2^{2L}$ where L is the binary length of the integer N to be factored. Such gates cannot be implemented exactly using existing fault-tolerant techniques. Approximating a given controlled $\pi/2^d$ rotation gate to within $\delta = O(1/2^d)$ currently requires both a number of qubits and a number of fault-tolerant gates that grows polynomially with d. In this paper we show that this additional growth in space and time complexity would severely limit the applicability of Shor's algorithm to large integers. Consequently, we study in detail the effect of using only controlled rotation gates with d less than or equal to some $d_{\max}$. It is found that integers up to length $L_{\max} = O(4^{d_{\max}})$ can be factored without significant performance penalty implying that the cumbersome techniques of fault-tolerant computation only need to be used to create controlled rotation gates of magnitude $\pi/64$ if integers thousands of bits long are desired factored. Explicit fault-tolerant constructions of such gates are also discussed.

DOI: 10.1103/PhysRevA.70.032329 PACS number(s): 03.67.Lx

Shor's factoring algorithm [1,2] is arguably the driving force of much experimental quantum computing research. It is therefore crucial to investigate whether the algorithm has a realistic chance of being used to factor commercially interesting integers. This paper focuses on the difficulty of implementing the quantum Fourier transform (QFT), an integral part of the algorithm. Specifically, the controlled $\pi/2^d$ rotations that comprise the QFT are extremely difficult to implement using fault-tolerant gates protected by quantum error correction (QEC).

To factor an L-bit integer N, a $2L$-qubit QFT is required that at first glance involves controlled rotation gates of magnitude $\pi/2^{2L}$. Prior work on simplifying the QFT so that it only involves controlled rotation gates of magnitude $\pi/2^{d_{\max}}$ has been performed by Coppersmith [3] with the conclusion that the length $L_{\max}$ of the maximum length integer that can be factored scales as $O(2^{d_{\max}})$ and that factoring an integer thousands of bits long would require the implementation of controlled rotations as small as $\pi/10^6$. This paper refines this work with the conclusion that $L_{\max}$ scales as $O(4^{d_{\max}})$, with $\pi/64$ rotations sufficient to enable the factoring of integers thousands of bits long.

The paper is organized as follows. In Sec. I Shor's algorithm is revised with emphasis on extracting useful output from the quantum period finding (QPF) subroutine. This subroutine is described in detail in this section. In Sec. II Coppersmith's approximate quantum Fourier transform (AQFT) is described, followed by Sec. III which outlines the techniques used to implement the gate set required by the AQFT using only fault-tolerant gates protected by QEC. In Sec. IV the relationship between the probability of success s of the QPF subroutine and the period r being sought is investigated. In Sec. V the relationship between the probability of success s and both the length L of the integer being factored and the minimum angle controlled rotation $\pi/2^{d_{\max}}$ is studied. This is then used to relate $L_{\max}$ to $d_{\max}$. Section VI concludes with a summary of results.

I. SHOR'S ALGORITHM

Shor's algorithm factors an integer $N = N_1 N_2$ by finding the period r of a function $f(k) = m^k \bmod N$ where $1 < m < N$ and $\gcd(m, N) = 1$. Provided r is even and $f(r/2) \neq N-1$ the factors are $N_1 = \gcd\big(f(r/2)+1, N\big)$ and $N_2 = \gcd\big(f(r/2)-1, N\big)$, where gcd denotes the greatest common divisor. The probability of finding a suitable r given a randomly selected m such that $\gcd(m, N) = 1$ is greater than 0.75 [4]. Thus on average very few values of m need to be tested to factor N.

The quantum heart of Shor's algorithm can be viewed as a subroutine that generates numbers of the form $j \simeq c2^{2L}/r$. To distinguish this from the necessary classical pre- and postprocessing, this subroutine will be referred to as QPF (quantum period finding). For physical reasons, the probability s that QPF will successfully generate useful data may be quite low with many repetitions required to work out the period r of a given $f(k) = m^k \bmod N$. Using this terminology, Shor's algorithm consists of classical preprocessing, potentially many repetitions of QPF with classical postprocessing, and possibly a small number of repetitions of this entire cycle. This cycle is summarized in Fig. 1.

A number of different quantum circuits implementing QPF have been designed [5–8]. Table I summarizes the number of qubits required and the depth of each of these circuits. The depth of a circuit has been defined to be the minimum number of 2-qubit gates that must be applied sequentially to complete the circuit. It has been assumed that multiple disjoint 2-qubit gates can be implemented in parallel, hence the total number of 2-qubit gates can be significantly greater than the depth. For example, the Beauregard circuit has a 2-qubit gate count of $8L^4$ to leading order in L. Note that in general the depth of the circuit can be reduced at the cost of additional qubits.

The underlying algorithm common to each circuit begins by initializing the quantum computer to a single pure state $|0\rangle_{2L}|0\rangle_L$. Note that for clarity the computer state has been broken into a $2L$-qubit k-register and an L-qubit f-register.

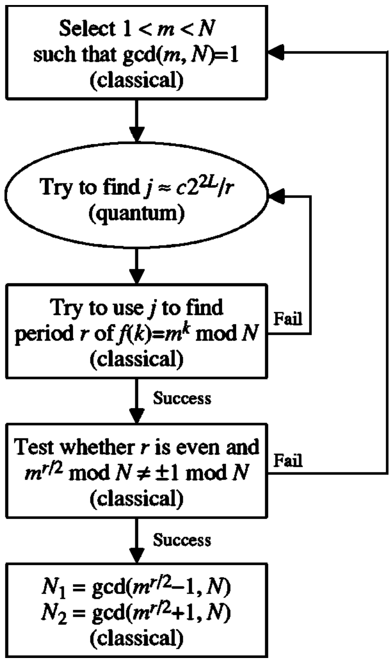

FIG. 1. The complete Shor's algorithm including classical pre- and postprocessing. The first branch is highly likely to fail, resulting in many repetitions of the quantum heart of the algorithm, whereas the second branch is highly likely to succeed.

The meaning of this will become clearer below.

Step two is to Hadamard transform each qubit in the k-register yielding

$$\frac{1}{2^L}\sum_{k=0}^{2^{2L}-1}|k\rangle_{2L}|0\rangle_L. \tag{1}$$

Step three is to calculate and store the corresponding values of $f(k)$ in the f-register

$$\frac{1}{2^L}\sum_{k=0}^{2^{2L}-1}|k\rangle_{2L}|f(k)\rangle_L. \tag{2}$$

Note that this step requires additional ancilla qubits. The exact number depends heavily on the circuit used.

Step four can actually be omitted but it explicitly shows the origin of the period r being sought. Measuring the f-register yields

TABLE I. Number of qubits required and circuit depth of different implementations of Shor's algorithm. Where possible, figures are accurate to first order in L.

Circuit	Qubits	Depth
Beauregard [7]	$\sim 2L$	$\sim 32L^3$
Vedral [5]	$\sim 5L$	$\sim 240L^3$
Zalka I [8]	$\sim 5L$	$\sim 3000L^2$
Zalka II [8]	$\sim 50L$	$\sim 2^{19}L^{1.2}$
Gossett [6]	$O(L^2)$	$O(L \log L)$

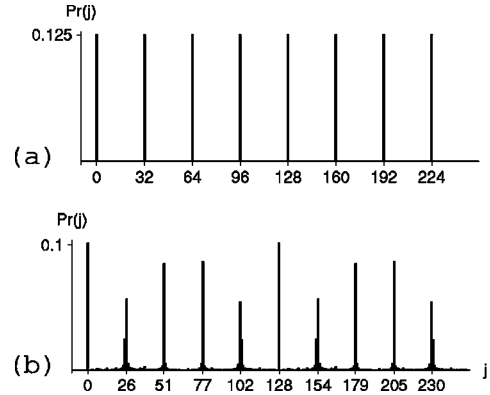

FIG. 2. Probability of different measurements j at the end of quantum period finding with total number of states $2^{2L}=256$ and (a) period $r=8$, (b) period $r=10$.

$$\frac{\sqrt{r}}{2^L}\sum_{n=0}^{2^{2L}/r-1}|k_0+nr\rangle_{2L}|f_M\rangle_L \tag{3}$$

where k_0 is the smallest value of k such that $f(k)$ equals the measured value f_M.

Step five is to apply the quantum Fourier transform

$$|k\rangle \to \frac{1}{2^L}\sum_{j=0}^{2^{2L}-1}\exp\left(\frac{2\pi i}{2^{2L}}jk\right)|j\rangle \tag{4}$$

to the k-register resulting in

$$\frac{\sqrt{r}}{2^{2L}}\sum_{j=0}^{2^{2L}-1}\sum_{p=0}^{2^{2L}/r-1}\exp\left(\frac{2\pi i}{2^{2L}}j(k_0+pr)\right)|j\rangle_{2L}|f_M\rangle_L. \tag{5}$$

The probability of measuring a given value of j is thus

$$\Pr(j,r,L)=\left|\frac{\sqrt{r}}{2^{2L}}\sum_{p=0}^{2^{2L}/r-1}\exp\left(\frac{2\pi i}{2^{2L}}jpr\right)\right|^2. \tag{6}$$

If r divides 2^{2L} Eq. (6) can be evaluated exactly. In this case the probability of observing $j=c2^{2L}/r$ for some integer $0\leqslant c<r$ is $1/r$ whereas if $j\neq c2^{2L}/r$ the probability is 0. This situation is illustrated in Fig. 2(a). However, if r divides 2^{2L} exactly a quantum computer is not needed as r would then be a power of 2 and easily calculable. When r is not a power of 2 the perfect peaks of Fig. 2(a) become slightly broader as shown in Fig. 2(b). All one can then say is that with high probability the value j measured will satisfy $j\simeq c2^{2L}/r$ for some $0\leqslant c<r$.

Given a measurement $j\simeq c2^{2L}/r$ with $c\neq 0$, classical postprocessing is required to extract information about r. The process begins with a continued fraction expansion. To illustrate, consider factoring 143 ($L=8$). Suppose we choose m equal 2 and the output j of QPF is 31 674. The relation $j\simeq c2^{2L}/r$ becomes $31\,674\simeq c65\,536/r$. The continued fraction expansion of c/r is

$$\frac{31\,674}{65\,536}=\frac{1}{\frac{32\,768}{15\,837}}=\frac{1}{2+\frac{1094}{15\,837}}=\frac{1}{2+\frac{1}{14+\frac{1}{2+\frac{1}{10+1/52}}}}. \quad (7)$$

The continued fraction expansion of any number between 0 and 1 is completely specified by the list of denominators which in this case is $\{2, 14, 2, 10, 52\}$. The nth convergent of a continued fraction expansion is the proper fraction equivalent to the first n elements of this list. An introductory exposition and further properties of continued fractions are described in Ref [4].

$$\{2\}=\frac{1}{2},$$

$$\{2,14\}=\frac{14}{29},$$

$$\{2,14,2\}=\frac{29}{60},$$

$$\{2,14,2,10\}=\frac{304}{629},$$

$$\{2,14,2,10,52\}=\frac{15\,837}{32\,768}. \quad (8)$$

The period r can be sought by substituting each denominator into the function $f(k)=2^k \bmod 143$. With high probability only the largest denominator less than 2^L will be of interest. In this case $2^{60} \bmod 143=1$ and hence $r=60$.

Two modifications to the above are required. First, if c and r have common factors, none of the denominators will be the period but rather one will be a divisor of r. After repeating QPF a number of times, let $\{j_m\}$ denote the set of measured values. Let $\{c_{mn}/d_{mn}\}$ denote the set of convergents associated with each measured value $\{j_m\}$. If a pair c_{mn}, $c_{m'n'}$ exists such that $\gcd(c_{mn},c_{m'n'})=1$ and d_{mn}, $d_{m'n'}$ are divisors of r then $r=\mathrm{lcm}(d_{mn},d_{m'n'})$, where lcm denotes the least common multiple. It can be shown that given any two divisors d_{mn}, $d_{m'n'}$ with corresponding c_{mn}, $c_{m'n'}$ the probability that $\gcd(c_{mn},c_{m'n'})=1$ is at least $1/4$ [4]. Thus only $O(1)$ different divisors are required. In practice, it will not be known which denominators are divisors so every pair d_{mn}, $d_{m'n'}$ with $\gcd(c_{mn},c_{m'n'})=1$ must be tested.

The second modification is simply allowing for the output j of QPF being useless. Let s denote the probability that $j=\lfloor c2^{2L}/r\rfloor$ or $\lceil c2^{2L}/r\rceil$ for some $0<c<r$ where $\lfloor\,\rfloor$, $\lceil\,\rceil$ denote rounding down and up, respectively. Such values of j will be called useful as the denominators of the associated convergents are guaranteed to include a divisor of r. The period r sought can always be found provided $O(1/s)$ runs of QFT can be performed.

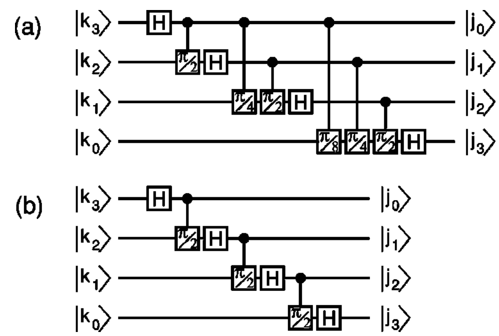

FIG. 3. Circuit for a 4-qubit (a) quantum Fourier transform (b) approximate quantum Fourier transform with $d_{\max}=1$.

To summarize, as each new value j_m is measured, the denominators d_{mn} less than 2^L of the convergents of the continued fraction expansion of $j_m/2^{2L}$ are substituted into $f(k)=m^k \bmod N$ to determine whether any $f(d_{mn})=1$ which would imply that $r=d_{mn}$. If not, every pair d_{mn}, $d_{m'n'}$ with associated numerators c_{mn}, $c_{m'n'}$ satisfying $\gcd(c_{mn},c_{m'n'})=1$ must be tested to see whether $r=\mathrm{lcm}(d_{mn},d_{m'n'})$. Note that as shown in Fig. 1, if r is even or $m^{r/2} \bmod N=\pm 1 \bmod N$ then the entire process needs to be repeated $O(1)$ times. Thus Shor's algorithm always succeeds provided $O(1/s)$ runs of QPF can be performed.

II. APPROXIMATE QUANTUM FOURIER TRANSFORM

A circuit that implements the QFT of Eq. (4) is shown in Fig. 3(a). Note the use of controlled rotations of magnitude $\pi/2^d$. In matrix notation these 2-qubit operations correspond to

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\pi/2^d} \end{pmatrix}. \quad (9)$$

The approximate QFT (AQFT) circuit is very similar with just the deletion of rotation gates with d greater than some $d_{\max}$. For example, Fig. 3(b) shows an AQFT with $d_{\max}=1$. Let $[j]_m$ denote the mth bit of j. The AQFT equivalent to Eq. (4) is [3]

$$|k\rangle \to \frac{1}{\sqrt{2^{2L}}}\sum_{j=0}^{2^{2L}-1}|j\rangle \exp\left(\frac{2\pi i}{2^{2L}}\tilde{\Sigma}_{mn}[j]_m[k]_n 2^{m+n}\right), \quad (10)$$

where $\tilde{\Sigma}_{mn}$ denotes a sum over all m, n such that $0\leq m,n<2L$ and $2L-d_{\max}+1\leq m+n<2L$. It has been shown by Coppersmith that the AQFT is a good approximation of the QFT [3] in the sense that the phase of individual computational basis states in the output of the AQFT differ in angle from those in the output of the QFT by at most $2\pi L 2^{-d_{\max}}$. The purpose of this paper is to investigate in detail the effect of using the AQFT in Shor's algorithm.

III. FAULT-TOLERANT CONSTRUCTION OF SMALL ANGLE ROTATION GATES

When the 7-qubit Steane code [4,9,10] and its concatenated generalizations are used to do computation, only the limited set of gates controlled-NOT (CNOT), Hadamard (H), X, Z, S, and $S^\dagger$ can be implemented easily, where

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \quad (11)$$

Complicated circuits of depth ~100 and requiring a minimum of 19 qubits are required to implement the T and $T^\dagger$ gates. The exact circuits shall be presented in a separate work specifically on fault-tolerant constructions

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}. \quad (12)$$

Note, however, that if it is acceptable to add an additional 12 qubits for every T and $T^\dagger$ gate in a sequence of fault-tolerant single-qubit gates [see, for example, Eq. (13)], the effective depth of each T and $T^\dagger$ gate circuit can be reduced to 2. Together, the set CNOT, H, X, Z, S, $S^\dagger$, T, and $T^\dagger$ enables the implementation of arbitrary 1- and 2-qubit gates via the Solovay-Kitaev theorem [4,11]. For example, the controlled $\pi/2^d$ gate can be decomposed into a single CNOT and three single-qubit rotations as shown in Fig. 4. Approximating single-qubit $\pi/2^d$ rotations using the fault-tolerant gate set is much more difficult. For convenience, such rotations will henceforth be denoted by R_{2^d}. The simplest (least number of fault-tolerant gates) approximation of the R_{128} single-qubit rotation gate that is more accurate than simply the identity matrix is the 31 gate product

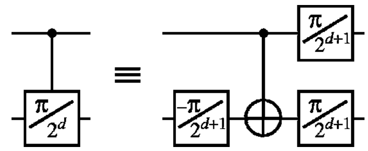

FIG. 4. Decomposition of a controlled rotation into single-qubit gates and a CNOT.

$$U_{31} = HTHT^\dagger HTHTHTHT^\dagger HT^\dagger HTHTHT^\dagger HT^\dagger HTHT^\dagger HT^\dagger HT^\dagger H. \quad (13)$$

Equation (13) was determined via an exhaustive search minimizing the metric

$$\mathrm{dist}(U,V) = \sqrt{\frac{2 - |\mathrm{tr}(U^\dagger V)|}{2}}. \quad (14)$$

The rationale of Eq. (14) is that if U and V are similar, $U^\dagger V$ will be close to the identity matrix (possibly up to some global phase) and the absolute value of the trace will be close to 2. By subtracting this absolute value from 2 and dividing by 2 a number between 0 and 1 is obtained. The overall square root is required to ensure that the triangle inequality

$$\mathrm{dist}(U,W) \leq \mathrm{dist}(U,V) + \mathrm{dist}(V,W) \quad (15)$$

is satisfied.

The identity matrix is a good approximation of R_{128} in the sense that $\mathrm{dist}(R_{128},I)=8.7\times10^{-3}$. Equation (13) is only slightly better with $\mathrm{dist}(R_{128},U_{31})=8.1\times10^{-3}$. A 46 gate sequence has been found satisfying $\mathrm{dist}(R_{128},U_{46})=7.5\times10^{-4}$. Note that this is still only 10 times better than doing nothing. Further investigation of the properties of fault-tolerant approximations of arbitrary single-qubit unitaries will be performed in the near future. For the present discussion it suffices to know that the number of gates grows somewhere between linearly and quadratically with $\ln(1/\delta)$ [4] where $\delta=\mathrm{dist}(R,U)$, R is the rotation being approximated, and U is the approximating product of fault-tolerant gates (the exact scaling is not known). In particular, this means that approximating a rotation gate R_{2^d} with accuracy $\delta=1/2^d$ requires a number of gates that grows linearly or quadratically with d.

In addition to the inconveniently large number of fault-tolerant gates n_δ required to achieve a given approximation δ, each individual gate in the approximating sequence must be implemented with probability of error p less than $O(\delta/n_\delta)$. Note that δ is not a probability of error but rather a measure of the distance between the ideal gate and the approximating product so this relationship is not exact. If the required probability $p\sim\delta/n_\delta=1/(n_\delta 2^d)$ is too small to be achieved using a single level of QEC, the technique of concatenated QEC must be used. Roughly speaking, if a given gate can be implemented with probability of error p, adding an additional level of concatenation [12] leads to an error rate of cp^2 where $c<1/p$. If the Steane code is used with seven qubits for the code and an additional five qubits for fault-tolerant correction, every additional level of concatenation requires approximately 12 times as many qubits. This implies that if a gate is to be implemented with accuracy $1/(n_\delta 2^d)$, the number of qubits q scales as $O(d^{\ln_2 12})$ $=O(d^{3.58})$. While this is a polynomial number of qubits, for even moderate values of d this leads to thousands of qubits being used to achieve the required gate accuracy.

Given the complexity of implementing T and $T^\dagger$ gates, the number of fault-tolerant gates required to achieve good approximations of arbitrary rotation gates and the large number of qubits required to achieve sufficiently reliable operation, it is clear that for practical reasons the use of $\pi/2^d$ rotations must be restricted to those with very small d.

IV. DEPENDENCE OF OUTPUT RELIABILITY ON THE PERIOD OF $f(k)=m^k$ mod N

Different values of r [the period of $f(k)=x^k$ mod N] imply different probabilities s that the value j measured at the end of QPF will be useful (see Fig. 1). In particular, as discussed in Sec. I if r is a power of 2 the probability of useful output is much higher (see Fig. 2). This section investigates how sensitive s is to variations in r. Recall Eq. (6) for the probability of measuring a given value of j. When the AQFT [Eq. (10)] is used this becomes

$$\Pr(j,r,L,d_{\max}) = \left| \frac{\sqrt{r}}{2^{2L}} \sum_{p=0}^{2^{2L}/r-1} \exp\left(\frac{2\pi i}{2^{2L}} \sum_{mn} [j]_m [pr]_n 2^{m+n} \right) \right|^2 . \quad (16)$$

The probability s of useful output is thus

$$s(r,L,d_{\max}) = \sum_{\{\text{useful } j\}} \Pr(j,r,L,d_{\max}), \quad (17)$$

where {useful j} denotes all $j=\lfloor c2^{2L}/r \rfloor$ or $\lceil c2^{2L}/r \rceil$ such that $0<c<r$. Figure 5 shows s for r ranging from 2 to 2^L-1 and for various values of L and $d_{\max}$. The decrease in s for small values of r is more a result of the definition of {useful j} than an indication of poor data. When r is small there are few useful values of $j \simeq c2^{2L}/r]$, $0<c<r$ and a large range of states is likely to be observed around each one resulting superficially in a low probability of useful output s as s is the sum of the probabilities of observing only values $j = \lfloor c2^{2L}/r \rfloor$ or $\lceil c2^{2L}/r \rceil$, $0<c<r$. However, in practice values much further from $j \simeq c2^{2L}/r$ can be used to obtain useful output. For example, if $r=4$ and $j=16\,400$ the correct output value (4) can still be determined from the continued fraction expansion of $16\,400/65\,536$ which is far from the ideal case of $16\,384/65\,536$. To simplify subsequent analysis each pair $(L,d_{\max})$ will from now on be associated with $s(2^{L-1}+2,L,d_{\max})$ which corresponds to the minimum value of s to the right of the central peak. The choice of this point as a meaningful characterization of the entire graph is justified by the discussion above.

For completeness, Fig. 5(e) shows the case of noisy controlled rotation gates of the form

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i(\pi/2^d+\delta)} \end{pmatrix}, \quad (18)$$

where δ is a normally distributed random variable of standard deviation σ. This has been included to simulate the effect of using approximate rotation gates built out of a finite number of fault-tolerant gates. The general form and probability of successful output can be seen to be similar despite $\sigma=\pi/32$. This σ corresponds to $\pi/2^{d_{\max}+2}$. For a controlled $\pi/64$ rotation, single-qubit rotations of angle $\pi/128$ are required, as shown in Fig. 4. Figure 5(e) implies that it is acceptable for this rotation to be implemented within $\pi/512$, implying

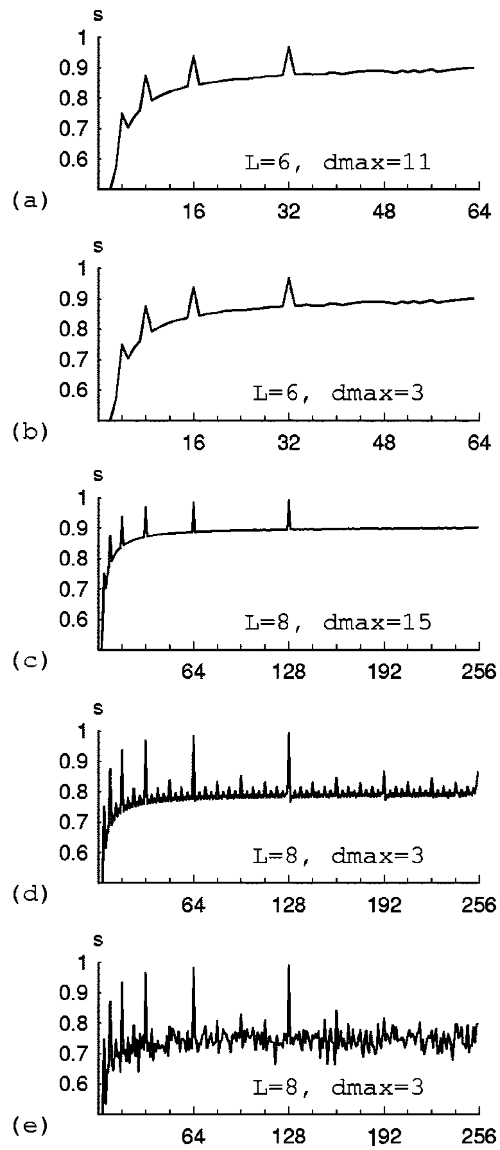

FIG. 5. Probability s of obtaining useful output from quantum period finding as a function of period r for different integer lengths L and rotation gate restrictions $\pi/2^{d_{\max}}$. The effect of using inaccurate controlled rotation gates ($\sigma=\pi/32$) is shown in (e).

$$U = \begin{pmatrix} 1 & 0 \\ 0 & e^{i(\pi/128+\pi/512)} \end{pmatrix} \quad (19)$$

is an acceptable approximation of R_{128}. Given that $\text{dist}(R_{128},U)=2.1\times10^{-3}$, the 46 fault-tolerant gate approximation of R_{128} mentioned above is adequate.

V. DEPENDENCE OF OUTPUT RELIABILITY ON INTEGER LENGTH AND GATE RESTRICTIONS

In order to determine how the probability of useful output s depends on both the integer length L and the minimum allowed controlled rotation $\pi/2^{d_{\max}}$, Eq. (17) was solved

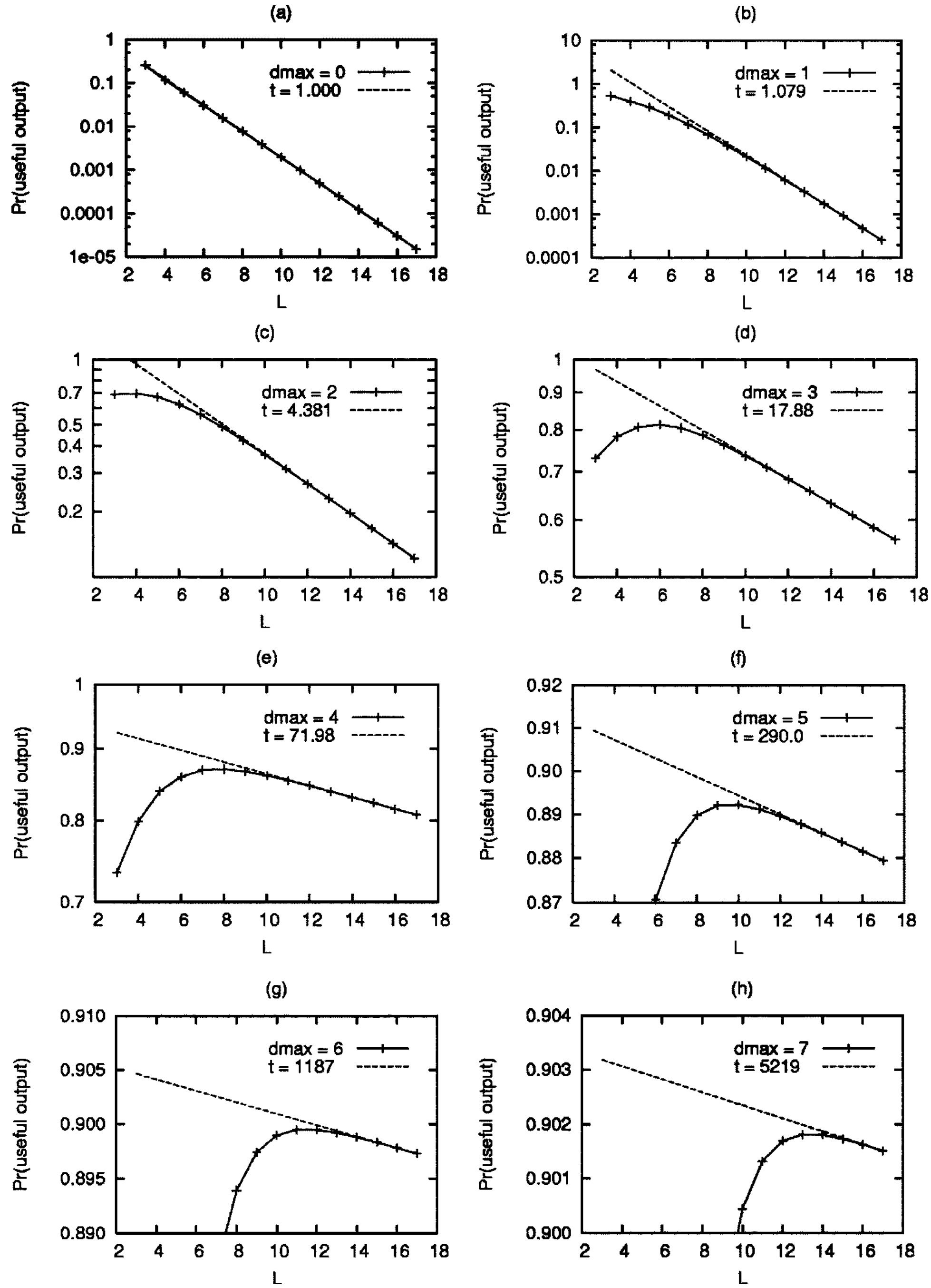

FIG. 6. Dependence of the probability of useful output from the quantum part of Shor's algorithm on the length L of the integer being factored for different levels of restriction of controlled rotation gates of angle $\pi/2^{d_{\max}}$. The parameter L_0 characterizes lines of best fit of the form $s \propto 2^{-L/L_0}$.

with $r=2^{L-1}+2$ as discussed in Sec. IV. Figure 6 contains semilog plots of s versus L for different values of $d_{\max}$. Note that Eq. (17) grows exponentially more difficult to solve as L increases.

For $d_{\max}$ from 0 to 5, the exponential decrease of s with increasing L is clear. Asymptotic lines of best fit of the form

$$s \propto 2^{-L/L_0} \tag{20}$$

have been shown. Note that for $d_{\max}>0$, the value of L_0 increases by greater than a factor of 4 when $d_{\max}$ increases by 1. This enables one to generalize Eq. (20) to an asymptotic lower bound valid for all $d_{\max}>0$

$$s \propto 2^{-L/4^{d_{\max}-1}} \tag{21}$$

with the constant of proportionality approximately equal to 1.

Keeping in mind that the required number of repetitions of QPF is $O(1/s)$, one can relate $L_{\max}$ to $d_{\max}$ by introducing an additional parameter $f_{\max}$ characterizing the acceptable number of repetitions of QPF,

$$L_{\max} \simeq 4^{d_{\max}-1} \log_2 f_{\max}. \quad (22)$$

Available RSA [13] encryption programs such as PGP typically use integers of length L up to 4096. The circuit in [5] runs in $150L^3$ steps when an architecture that can interact arbitrary pairs of qubits in parallel is assumed and fault-tolerant gates are used (the fault-tolerant Toffoli gate has smaller depth than the nonfault-tolerant Toffoli gate used in the construction of Table I. Note that to leading order in L the number of steps does not increase as additional levels of QEC are used. Thus $\sim 10^{13}$ steps are required to perform a single run of QPF. On an electron spin or charge quantum computer [14,15] running at 10 GHz this corresponds to $\sim$15min of computing. If we assume $\sim$24h of computing is acceptable then $f_{\max} \sim 10^2$. Substituting these values of $L_{\max}$ and $f_{\max}$ into Eq. (22) gives $d_{\max}=6$ after rounding up. Thus provided controlled $\pi/64$ rotations can be implemented accurately, implying the need to accurately implement $\pi/128$ single-qubit rotations, it is conceivable that a quantum computer could one day be used to break a 4096-bit RSA encryption in a single day.

VI. CONCLUSION

We have demonstrated the scalability of Shor's algorithm when a limited set of rotation gates is used. The length $L_{\max}$ of the longest factorable integer can be related to the maximum acceptable runs of quantum period finding $f_{\max}$ and the smallest accurately implementable controlled rotation gate $\pi/2^{d_{\max}}$ via $L_{\max} \sim 4^{d_{\max}-1} \log_2 f_{\max}$. Integers thousands of digits in length can be factored provided controlled $\pi/64$ rotations can be implemented with a rotation angle accurate to $\pi/256$. Sufficiently accurate fault-tolerant constructions of such controlled rotation gates have been described.

ACKNOWLEDGMENTS

This work was supported by the Australian Research Council and the Army Research Office under Contract No. DAAD19-01-1-0653.

[1] P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Press, Los Alamos, CA, 1994), pp. 124–134.
[2] P. W. Shor, e-print quant-ph/0005003.
[3] D. Coppersmith, IBM Research Report No. RC19642, 1994 (unpublished).
[4] M. A. Nielson and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[5] V. Vedral *et al.*, Phys. Rev. A **54**, 147 (1996).
[6] P. Gossett, e-print quant-ph/9808061.
[7] S. Beauregard, Quantum Inf. Comput. **3**, 175 (2003).
[8] C. Zalka, e-print quant-ph/9806084.
[9] A. M. Steane, Proc. R. Soc. London, Ser. A **425**, 2551 (1996).
[10] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1995).
[11] A. Y. Kitaev, Russ. Math. Surveys **52**, 1191 (1997).
[12] E. Knill *et al.*, e-print quant-ph/9610011.
[13] R. L. Rivest *et al.*, Commun. ACM **21**, 120 (1978).
[14] G. Burkard *et al.*, Fortschr. Phys. **48**, 965 (2000).
[15] L. C. L. Hollenberg *et al.*, Phys. Rev. B **69**, 113301 (2004).