Carmichael Numbers on a Quantum Computer

A. Carlini and A. Hosoya

Department of Physics, Tokyo Institute of Technology, Oh-Okayama, Meguro-ku, Tokyo 152, Japan

We present a quantum probabilistic algorithm which tests with a polynomial computational complexity whether a given composite number is of the Carmichael type. We also suggest a quantum algorithm which could verify a conjecture by Pomerance, Selfridge and Wagstaff concerning the asymptotic distribution of Carmichael numbers smaller than a given integer.

PACS numbers: 03.67.Lx, 89.70.+c, 02.10.Lh

I. INTRODUCTION

In the last few years the area of quantum computation has gained much momentum (for a review see, e.g., ref. [2]). The power of quantum computers is mainly due to the possibility of working with a superposition of \(|0\rangle\) and \(|1\rangle\) qubits with coefficients being complex numbers \(\alpha\) and \(\beta\), i.e. with states \(|\psi\rangle = \alpha|0\rangle + \beta|1\rangle\), providing an enormous number of parallel computations by the generation of a superposed state of a large number of terms. Quantum computers can do unitary transformations and (final) measurements inducing an instantaneous state reduction to \(|0\rangle\) or \(|1\rangle\) with the probability \(|\alpha|^2\) or \(|\beta|^2\), respectively [1]. Two of the most important achievements so far have been the discoveries of the quantum algorithms for factoring integers [3] and for the search of unstructured databases [4], which achieve, respectively, an exponential and a square root speed up compared to their classical analogues. Another interesting algorithm exploiting the above mentioned ones in conjunction is that counting the cardinality \(t\) of a given set of elements present in a flat superposition of states [5].

In a recent work [6], we showed how an extended use of this counting algorithm can be further exploited to construct unitary and fully reversible operators emulating at the quantum level a set of classical probabilistic algorithms. Such classical probabilistic algorithms are characterized by the use of random numbers during the computation, and they give the correct answer with a certain probability of success, which can be usually made exponentially close to one by repetition. The quantum randomized algorithms described in ref. [6] also naturally select the 'correct' states with a probability and an accuracy which can be made exponentially close to one in the end of the computation, and since the final measuring process is only an option which may not be used, they can be included as partial subroutines for further computations in larger and more complex quantum networks. As explicit examples, we showed how one can design polynomial time algorithms for studying some problems in number theory, such as the test of the primality of an integer, of the 'prime number theorem' and of a certain conjecture about the asymptotic number of representations of an even integer as a sum of two primes.

In this paper we will use the methods of ref. [6] to build a polynomial time quantum algorithm which checks whether a composite number \(k\) is of Carmichael type. We start in section II by recalling the main definitions and properties of Carmichael numbers. In section III we describe the quantum algorithm for the test of Carmichael numbers. Section IV is devoted to the description of a quantum algorithm which counts the number of Carmichaels smaller than a given integer. Finally, we conclude in section V with some discussion on the results obtained.

II. CARMICHAEL NUMBERS

Carmichael numbers are quite famous among specialists in number theory, as they are quite rare and very hard to test. They are defined as composite numbers \(k\) such that [7, 8] 

\[ a^{k-1} \equiv 1 \mod k \]  

for every base \(1 < a < k\), \(a\) and \(k\) being relative coprimes, or \(GCD(a, k) = 1\). For later convenience, we also introduce the function \(G_k(a) = \Theta(GCD(a, k))\), where \(\Theta[1] = 1\) and \(\Theta = 0\) otherwise. In particular, it can be shown that an integer \(k\) is a Carmichael number if and only if \(k\) is composite and the maximum of the orders of a mod \(k\), for every \(1 \leq a < k\) coprime to \(k\), divides \(k - 1\). It then follows that every Carmichael number is odd and the product of three or more distinct prime numbers (the smallest Carmichael number is \(561 = 3 \times 11 \times 17\). Recently, it has also been proven that there are infinitely many Carmichael numbers [9]. On a classical computer, it is hard to test whether a composite number \(k\) is Carmichael, as it requires \(O(k / \log \log k)\) evaluations of \(a^{k-1} \mod k\).

In principle, there is a quite straightforward method to check whether a composite number \(k\) is of the Carmichael type, provided a complete factorization of \(k\) itself is known. The algorithm would use the fact that the number of bases \(1 < a < k\) coprime to \(k\) and which satisfy eq. (1), i.e. for which \(k\) is a pseudoprime, can be written as \(F(k) = \prod p_i GCD(p_i - 1, k - 1)\), where the \(p_i\)'s are the prime factors of \(k\), i.e. \(k = \prod p_i^t \) [10].
II. COUNT FOR ESTIMATING A PERIOD

Our quantum algorithm uses COUNT for estimating the number \( t_k \equiv \phi(k) - F(k) \) of bases for which a given composite \( k \) is not pseudoprime (i.e., the number of bases coprimes to \( k \) which do not satisfy condition (1)), and of \( R \) ancilla qubits \(|m_i\rangle > \) which will be finally measured. At first, we have to select the composite number \( k \), which can be done, e.g., by use of the quantum analogue of Rabin’s randomized primality test [12] as described in ref. [2], and which will take only \( poly(\log k) \) steps. We can then proceed with the main core of the quantum Carmichael test algorithm, by starting with the state

\[
|\psi_0\rangle \equiv |0\rangle ... |0\rangle > R |0\rangle > |0\rangle > ,
\]

act on each of the first \( R + 1 \) qubits with a Walsh-Hadamard transform \( W \), producing, respectively, the flat superpositions \( \sum_{m=0}^{p-1} |m\rangle > / \sqrt{P} \), for \( i = 1, ..., R \), and \( \sum_{a=0}^{k-1} |a\rangle > / \sqrt{k} \), then perform a \( CTRL \cdot NOT \) operation on the last qubit (i.e., flipping the value of this qubit) subject to the condition that the state \(|a\rangle > \) is co-

\[
F|a\rangle \equiv \frac{1}{\sqrt{k}} \sum_{b=0}^{k-1} e^{2i\pi ab/k} |b\rangle > .
\]

The COUNT algorithm can be summarized by the following sequence of operations:

COUNT:

1) \( \langle W|0\rangle (W|0\rangle > = \sum_{m=0}^{P-1} |m\rangle > / \sqrt{P} \),
2) \( (F \otimes I) \sum_{m=0}^{P-1} |m\rangle > / \sqrt{P} > \sum_{a=0}^{k-1} |a\rangle > / \sqrt{k} \),
3) \( \rightarrow \) measure \(|m\rangle > \).

Since the amplitude of the set of states \(|w\rangle > \) after \( m \) iterations of \( G \) is a periodic function of \( m \), the estimate of such a period by Fourier analysis and the measurement of the ancilla qubit \(|m\rangle > \) will give information on the size \( t \) of this set, on which the period itself depends. The parameter \( P \) determines both the precision of the estimate \( t \) and the computational complexity of the COUNT algorithm (which requires \( P \) iterations of \( G \)).

Our quantum algorithm uses COUNT for estimating the number \( t_k \equiv \phi(k) - F(k) \) of bases for which a given composite \( k \) is not pseudoprime (i.e., the number of bases coprimes to \( k \) which do not satisfy condition (1)), and of \( R \) ancilla qubits \(|m_i\rangle > \) which will be finally measured. At first, we have to select the composite number \( k \), which can be done, e.g., by use of the quantum analogue of Rabin’s randomized primality test [12] as described in ref. [2], and which will take only \( poly(\log k) \) steps. We can then proceed with the main core of the quantum Carmichael test algorithm, by starting with the state

\[
|\psi_0\rangle \equiv |0\rangle ... |0\rangle > R |0\rangle > |0\rangle > ,
\]

act on each of the first \( R + 1 \) qubits with a Walsh-Hadamard transform \( W \), producing, respectively, the flat superpositions \( \sum_{m=0}^{p-1} |m\rangle > / \sqrt{P} \), for \( i = 1, ..., R \), and \( \sum_{a=0}^{k-1} |a\rangle > / \sqrt{k} \), then perform a \( CTRL \cdot NOT \) operation on the last qubit (i.e., flipping the value of this qubit) subject to the condition that the state \(|a\rangle > \) is co-

\[
F|a\rangle \equiv \frac{1}{\sqrt{k}} \sum_{b=0}^{k-1} e^{2i\pi ab/k} |b\rangle > .
\]

The COUNT algorithm can be summarized by the following sequence of operations:

COUNT:

1) \( \langle W|0\rangle (W|0\rangle > = \sum_{m=0}^{P-1} |m\rangle > / \sqrt{P} \),
2) \( (F \otimes I) \sum_{m=0}^{P-1} |m\rangle > / \sqrt{P} > \sum_{a=0}^{k-1} |a\rangle > / \sqrt{k} \),
3) \( \rightarrow \) measure \(|m\rangle > \).

Since the amplitude of the set of states \(|w\rangle > \) after \( m \) iterations of \( G \) is a periodic function of \( m \), the estimate of such a period by Fourier analysis and the measurement of the ancilla qubit \(|m\rangle > \) will give information on the size \( t \) of this set, on which the period itself depends. The parameter \( P \) determines both the precision of the estimate \( t \) and the computational complexity of the COUNT algorithm (which requires \( P \) iterations of \( G \)).

Our quantum algorithm uses COUNT for estimating the number \( t_k \equiv \phi(k) - F(k) \) of bases for which a given composite \( k \) is not pseudoprime (i.e., the number of bases coprimes to \( k \) which do not satisfy condition (1)), and of \( R \) ancilla qubits \(|m_i\rangle > \) which will be finally measured. At first, we have to select the composite number \( k \), which can be done, e.g., by use of the quantum analogue of Rabin’s randomized primality test [12] as described in ref. [2], and which will take only \( poly(\log k) \) steps. We can then proceed with the main core of the quantum Carmichael test algorithm, by starting with the state

\[
|\psi_0\rangle \equiv |0\rangle ... |0\rangle > R |0\rangle > |0\rangle > ,
\]

act on each of the first \( R + 1 \) qubits with a Walsh-Hadamard transform \( W \), producing, respectively, the flat superpositions \( \sum_{m=0}^{p-1} |m\rangle > / \sqrt{P} \), for \( i = 1, ..., R \), and \( \sum_{a=0}^{k-1} |a\rangle > / \sqrt{k} \), then perform a \( CTRL \cdot NOT \) operation on the last qubit (i.e., flipping the value of this qubit) subject to the condition that the state \(|a\rangle > \) is co-

\[
F|a\rangle \equiv \frac{1}{\sqrt{k}} \sum_{b=0}^{k-1} e^{2i\pi ab/k} |b\rangle > .
\]
prime with \(k\) and also act on the \(|a\rangle >\) qubits with an \(|m_1 > \ldots m_R >\) ‘controlled’ Grover operation \(G^m\) selecting the bases \(|a\rangle >\) for which \(k\) is not a pseudoprime. We thus obtain the state

\[
|\psi_1\rangle = \frac{1}{\sqrt{P}} \sum_{m_1=0}^{P-1} m_1 > \ldots \frac{1}{\sqrt{P}} \sum_{m_R=0}^{P-1} m_R > \times G^{m_R} \frac{1}{\sqrt{k}} \sum_{\substack{G_k=1 \geq 0 \forall a \geq 0}} \sum_{G_k=0}^{G_k} |a\rangle > |1\rangle + \sum_{G_k=0}^{G_k} |a\rangle > |0\rangle >, \tag{5}
\]

where \(G\) for \(G\) we use \(S_1 = I - 2\sum_{a=0}^{2^i} |a\rangle < a\rangle\), with the function \(Z_k(a)\) defined as \(Z_k(a) = 0\) when condition \(\square\) is not satisfied, and \(Z_k(a) = 1\) if condition \(\square\) is satisfied. In the following we will also assume that \(P \approx O(\log^2 |k|)\), so that the steps required to compute the repeated Grover operations \(G^{m_1} \ldots G^{m_R}\) is polynomial in \(\log k\).

We then define the quantities

\[
\sin \theta_k = \sqrt{\frac{t_k}{k}} \tag{6}
\]

and

\[
\begin{align*}
&k_{m_1 \ldots m_R} = \sin[2(m_1 + \ldots + m_R) + 1] \theta_k \\
&m_{l_1 \ldots m_R} = \cos[2(m_1 + \ldots + m_R) + 1] \theta_k,
\end{align*} \tag{7}
\]

where \(t_k\) is the number of bases \(a\) for which \(Z_k(a) = 0\), and the states

\[
\begin{align*}
|B_1^k\rangle &\equiv \frac{1}{\sqrt{t_k}} \sum_{Z_k(a) = 0} |a\rangle > \\
|B_2^k\rangle &\equiv \frac{1}{\sqrt{\phi(k) - t_k}} \sum_{Z_k(a) = 1} |a\rangle >.
\end{align*} \tag{8}
\]

Next we apply Shor’s Fourier transform on each of the first \(R\) ancilla qubits in order to extract the periodicity \(\theta_k\) which is hidden in the amplitudes \(k_{m_1 \ldots m_R}\) and \(lm_{l_1 \ldots l_R}\), i.e. we transform \(|\psi_1\rangle >\) into

\[
|\psi_2\rangle = \frac{1}{\sqrt{P}} \sum_{m_1, l_1=0}^{P-1} e^{2\pi i m_1/P} |l_1\rangle > \ldots \frac{1}{\sqrt{P}} \sum_{m_R, l_R=0}^{P-1} e^{2\pi i m_R/P} |l_R\rangle > \times [k_{m_1 \ldots m_R} |B_1^k\rangle > + \sum_{l_1 \ldots l_R} |l_1\rangle > |B_2^k\rangle > |1\rangle > + |Rest\rangle > |0\rangle >, \tag{9}
\]

where the state \(|Rest\rangle >\) is the result of the operation \(G^m\) acting on the bases \(|a\rangle >\) which are not coprime with \(k\).

Finally, we perform a measurement of the last qubit. If we get \(|0\rangle >\), we start again the whole algorithm from eq. (9). If, instead, we obtain \(|1\rangle >\), we can proceed since eq. (9) is reduced to the state (which contains only bases for which \(G_k(a) = 1\))

\[
|\psi_3\rangle \equiv \frac{1}{\sqrt{2}} \sum_{l_1 \ldots l_R=0} e^{-i \pi (l_1 + \ldots + l_R) P} \times \left[ e^{i \pi f_k(R)} \prod_{i=1}^{R} s_{l_i} |B_1^i\rangle > + |B_2^i\rangle > \right] + e^{-i \pi f_k(R)} \prod_{i=1}^{R} s_{l_i} |B_1^i\rangle > + |B_2^i\rangle >, \tag{10}
\]

where we have introduced the following quantities

\[
\begin{align*}
f_k &\equiv \frac{P \theta_k}{\pi}; \quad 0 \leq f_k \leq \frac{P}{2} \\
f_k(R) &\equiv f_k \left[R + \frac{(1 - R)\pi}{P}\right] \tag{11}
\end{align*}
\]

and

\[
s_{l_i} \equiv \frac{\sin \pi (l_i \pm f_k)}{P \sin \pi (l_i \pm f_k) / P}. \tag{12}
\]

It is easy to see that the probability of measuring the last qubit in eq. (9) in the state \(|1\rangle >\) is given by \(P_{1 >}) = \phi(k) / k\), which means that (using the asymptotic behaviour \(\phi(k) \approx k / \log \log k\)) we require an average number \(T_{av} \approx (P_{1 >})^{-1} \approx O(\log \log k)\) of steps to obtain eq. (11).

Now, with eq. (11) at hand, we can count the bases coprime with \(k\) for which \(k\) is not a pseudoprime. There are then two possibilities: either \(k \equiv k_C\) is Carmichael, in which case \(t_{k_C} = 0\) and therefore \(\theta_{k_C} = f_{k_C} = 0\); or \(k \equiv k_{NC}\) is not Carmichael, for which \(t_{k_{NC}} \geq k_{NC} / 2\) and \(\theta_{k_{NC}} \geq \pi / 4\), implying that \(P/4 \leq f_{k_{NC}} \leq P/2\). Looking at eq. (11), we can see that, in the case when \(k\) is Carmichael, \(G\) effectively acts as an identity operator, so that \(|\psi_3\rangle >\) simplifies to
The quantum algorithm (which is also discussed in more details in ref. [1]) consists of a sub-loop which checks whether a given composite $k$ is Carmichael, by counting the bases for which it is not a pseudoprime, and a main loop which counts the numbers of Carmichaels smaller than $N$. In particular, we have:

**MAIN-LOOP:**

Use **COUNT** with $G \to \hat{G}$ and $S_1 \to \hat{S}_1 = 1 - 2 \sum_{k_C} |k_C < k_C|$ (parameter $Q$)

**SUB-LOOP:**

Parallel compositeness and Carmichael certification tests $\forall k_{co} < N$ (parameter $P$) and (approximate) construction of $\hat{S}_1$.

The construction of the operator $\hat{S}_1$ in the SUB-LOOP of the algorithm first needs the selection of composites $k_{co} < N$. This is done, again, using the quantum randomized primality test described in ref. [1]. In particular, one starts with the state

$$|\psi_0 > \equiv \frac{1}{\sqrt{N}} \sum_{k=1}^{N} |k - 1 > |0 > 1 |0 > 2 |0 > 3 \times |0 > 4 |0 > G |0 > c, \qquad (16)$$

acting on the ancilla qubit $|0 > 1$ with $F$ (producing the flat superposition $\sum_{m=0}^{P-1} |m > 1 / \sqrt{P}$, on the ancilla qubit $|0 > 2$ with a $|k - 1 >$-‘controlled’ $F$ (producing the flat superposition $\sum_{a=1}^{k} \beta_a |a > 2 / \sqrt{k}$) and an $|m > 1$-‘controlled’ $G^m$ (with Grover’s $G$ selecting bases with $W_k(a) = 0$), again with an $F$ on the $|m > 1$ ancilla qubits, then evaluating the function $[1 - \Theta[m + 1]]$ on the $|0 > c$ ancilla qubit, and finally undoing all the previous operations except the last one, obtaining

$$|\psi_1 > \equiv \frac{1}{\sqrt{N}} \left[ \left( \sum_{k_{pr}} |k > |0 > 1,2 \right. \right.$$

$$+ \sum_{k_{co}} |k > |C^k > 1,2 \left. \right) |0 > c$$

$$+ \sum_{k_{co}} |k > (|0 > 1,2 - |C^k > 1,2 |1 > ) |0 > 3,4,G, \qquad (17)$$

where $|C^k > 1,2$ is a correction term which has been defined in ref. [1] and is s.t. $C^k|C^k > 1,2 = 1 < C^k|0 > 1,2 = \beta_{k_{pr}}, \quad$ with $\beta_k \equiv (\sin \pi g_k)/(P \sin \pi g_k / P), g_k \equiv P(\arcsin \sqrt{t_k/k})/\pi$, and $\beta_{k_{pr}} = 1 (\beta_{k_{co}} \leq 2/\sqrt{3P})$.

Then, we proceed with the selection of Carmichael numbers among the composites $k_{co} < N$. To do so, one has to act on the $|0 > q$ qubit with $F$ (producing the flat superposition $\sum_{m=0}^{P-1} |m > 3 / \sqrt{P}$), on $|0 > 4$ with a $|k - 1 >$-‘controlled’ $F$ (producing the superposition of

$$|\psi_2 > \equiv \frac{1}{\sqrt{N}} \left[ \left( \sum_{k_{pr}} |k > |0 > 1,2 \right. \right.$$

$$+ \sum_{k_{co}} |k > |C^k > 1,2 \left. \right) |0 > c$$

$$+ \sum_{k_{co}} |k > (|0 > 1,2 - |C^k > 1,2 |1 > ) |0 > 3,4,G, \qquad (17)$$

where $|C^k > 1,2$ is a correction term which has been defined in ref. [1] and is s.t. $C^k|C^k > 1,2 = 1 < C^k|0 > 1,2 = \beta_{k_{pr}}, \quad$ with $\beta_k \equiv (\sin \pi g_k)/(P \sin \pi g_k / P), g_k \equiv P(\arcsin \sqrt{t_k/k})/\pi$, and $\beta_{k_{pr}} = 1 (\beta_{k_{co}} \leq 2/\sqrt{3P})$.

Then, we proceed with the selection of Carmichael numbers among the composites $k_{co} < N$. To do so, one has to act on the $|0 > q$ qubit with $F$ (producing the flat superposition $\sum_{m=0}^{P-1} |m > 3 / \sqrt{P}$), on $|0 > 4$ with a $|k - 1 >$-‘controlled’ $F$ (producing the superposition of

IV. COUNTING CARMIHAEL NUMBERS

One further and interesting problem in which the quantum algorithm of the previous section can be explicitly used is for the test of a conjecture by Pomerance et al. [14] concerning the asymptotic distribution $t_N$ of Carmichael numbers smaller than a given integer $N$, which, $\forall$ fixed $\epsilon > 0$ and $\forall N > N_0(\epsilon)$, should be lower bounded by

$$t_N|_{th} \geq O \left[ \frac{N}{l(N)^{2+\epsilon}} \right]$$

$$l(N) \equiv N^{\log \epsilon / (\log \log \log N)} / (\log \log N). \tag{15}$$

**Footnote: The existence of the upper bound $t_N|_{th} \leq O[Nl(N)^{-1-\epsilon}]$ is proven in ref. [14] (see also ref. [13]).**
base states $\sum_{a=0}^{k-1} |a >_4 / \sqrt{k}$, on $|0 >_G$ with an $|a >_4$ - 'controlled' Euclid $E(a)$ operation (selecting the $a$ co-primes with $k$), with an $|m >_3$-'controlled' Grover transform $G^m$ on the $|a >_4$ qubits (selecting the bases for which $k$ is not a pseudoprime), followed by a Fourier transform $F$ and a phase change $S_0$ on the ancilla qubit $|m >_3$ conditioned upon the last ancilla qubit in $|\tilde{\psi} >_1$ being in the state $|1 >_c$, undo again the previous operations (except $S_0$, $E(a)$ and the first $F$ on $|m >_3$) and finally also undo $[1 - \Theta(m+1)]$ on the $| >_c$ qubit. In this way, defining $\tilde{S}_1$ as the sequence of all these unitary transformations, one obtains the state (see FIG. 1) \[ \tilde{S}_1|\tilde{\psi}_0 > \equiv [(|\tilde{\psi} > + |E >)|1 >_G
+ |REST > |0 >_G||0 >_c], \tag{18} \]

where $|\Psi > \equiv \frac{1}{\sqrt{N}} \sum_{k=1}^{N} (-1)^{F_k} |k - 1 >_1 |0 >_{1,2,3} |G_{k-1}=1 |a >_4 / \sqrt{k}$

$|E > \equiv \frac{1}{\sqrt{N}} \left[ 2 \sum_{k_{c,0},C} |k > |C^k >_{1,2} |0 >_3 \sum_{G_{k}=1} |a >_4 / \sqrt{k} + \sum_{k_{c,0,NC}} \sin \Phi_k |k > (|C^k >_{1,2} - |0 >_{1,2}) e^{k >_{3,4}} \right], \tag{19} \]

$F_{k+1} \equiv 1$ for $k = k_C$ and $F_{k+1} = 0$ for $k = k_{NC}$,

$\sin \Phi_k \equiv \sqrt{\frac{\phi(k)}{k}}. \tag{20} \]

$|REST >$ defines the contribution (which, together with the state $|e^k >_{3,4}$ - with norm $3,4 < e^k |e^k >_{3,4} = 4 \alpha_4^2$ - we do not write here for the sake of simplicity) from the bases with $G_k(a) = 0$, and the last qubit selects the contribution from the bases with $G_k(a) = 1 (|1 >_G)$ or with $G_k(a) = 0 (|0 >_G)$.

FIG. 1. The quantum network for the construction of the state $\tilde{S}_1 |\tilde{\psi}_0 >$. Selection of composites is done in $|\tilde{\psi}_1 >$, selection of Carmichaels is done in $\tilde{S}_1 |\tilde{\psi}_0 >$. The operator $C$ is defined as $C \equiv 1 - \Theta_{m+1}$.

In particular, one can show that the norm of the correction term $|E >$ in eq. (19) is upper bounded by

$$< E |E > \leq \frac{4}{3} \sum_{k=1}^{N} \frac{\phi(k)}{k} \beta_k^2 + \frac{1}{3} \sum_{k_{NC}} \frac{\phi(k)}{k} (1 - \beta_k^2) \alpha_k^2 \leq \frac{4 \pi^2}{3 \sqrt{5}}. \tag{21} \]

Moreover, it can be shown that the overall contribution to the state (14) coming from the bases $a$ for which $G_k(a) = 1$ and the last ancilla qubit is in the state $|1 >_G$, i.e. $|\Phi > \equiv |\Psi > + |E >$, has a norm $< \Phi |\Phi > \equiv \sum_{k=1}^{N} \frac{\phi(k)}{k} / N \approx \pi^2 / 6$.

Next, Grover’s transform $\tilde{G}$ entering the MAIN-LOOP of the algorithm, i.e. that counting the total number $t_N < N$, can be written as

$$\tilde{G} \equiv U_2 \tilde{S}_1 ; \quad U_2 \equiv -W^{(k)} S^{(k)} W^{(k)}, \tag{22} \]

where now the operations $W^{(k)}$ and $S^{(k)}$ are acting on the states $|k >$.

Then, starting from $|\tilde{\psi}_0 >$ given by formula (10) and tensoring it with another flat superposition of ancilla states, i.e.

$$|\tilde{\psi}_2 > \equiv \frac{1}{\sqrt{Q}} \sum_{m=0}^{Q-1} |m >_5 |\tilde{\psi}_0 >, \tag{23} \]

acting on $|\tilde{\psi}_0 >$ with the $|m >_5$-'controlled’ $G^m$ and with $F$ on $|m >_5$, and exploiting the linearity of the unitary transformation $\tilde{S}_1$ when acting on $|\Phi > |1 >_G$ and on $|REST > |0 >_G$, after some elementary algebra we get (see ref. [1] for more details)\[ [1]$$

$$|\tilde{\psi}_3 > \equiv \left[ \frac{1}{2} \sum_{n=0}^{Q-1} e^{\pi n (1-1/Q)} |n >_5 \ e^{-i \pi f_\alpha s_{n-}} \times (i|G > + |B >) + e^{i \pi f_\alpha s_{n+}} (-i|G > + |B >) \right] \sum_{m,n=0}^{Q-1} e^{2i \pi mn/Q} |m >_5 |E_m > |1 >_G
+ \frac{1}{Q} \sum_{m,n=0}^{Q-1} e^{2i \pi mn/Q} |n >_5 |\tilde{G}^m |REST > |0 >_G, \tag{24} \]

where we have defined, similarly to section III,

\[ [1]We omit $|0 >_c$ in eq. (24) for simplicity.
\sin \theta_N \equiv \sqrt{\frac{t_N}{N}}
\quad f_Q \equiv \frac{Q\theta_N}{\pi},
(25)

the 'good' and 'bad' states, respectively, as
\[ |G> \equiv \frac{\sum_{|k> | 0> | 1,2}}{\sqrt{t_N}} |k>, \]
\[ |B> \equiv \frac{\sum_{|k> | 0> | 1,2}}{\sqrt{N-t_N}} |k>, \]
(26)

the 'error' term as
\[ |E_n> \equiv \sec \theta_N \left[ \sum_{j=1}^{n} l_{n-j} \tilde{G}^{-1}_j \right] U_2 |E>, \]
(27)

with \( l_j = \cos((2j+1)\theta_N), \) and \( s_n^{(Q)} \) as in eq. (12).

Finally, we measure the last ancilla qubit \(| :G>\): If we get \(| :G>\), we start again building the state \(| \psi_0>\) as in eq. (10). Otherwise, if we get \(| 1> :G\) (i.e., the part of \(| \psi_3 >\) coming from the bases with \( G_k(a) = 1\), we can go on to the last step of the algorithm and further measure the first ancilla qubit \(| >:G\) \(\bar{\psi}_3\).\] Using the expected estimate that \( \theta_N \sim O[1/(N^{1+\epsilon/2})] \), and by choosing
\[ Q \equiv O[l(N)^{\beta}] \quad ; \quad \beta > 1 + \epsilon/2, \]
(28)

we get the ansatz \( 1 < f_Q < Q/2 - 1 \), for which it can be shown \[ \tilde{W} \] that the probability \( \tilde{W} \) to obtain any of the states \(| f_- > 5, | f_+ > 5, | Q - f_- > 5 \) or \(| Q - f_+ > 5 \) in the final measurement is given by
\[ \tilde{W} \geq \frac{8}{\pi^2}. \]
(29)

This means that with a high probability we will always be able to find one of the states \(| f_- > 5 \) or \(| P - f_+ > 5 \)
and, therefore, to evaluate the number \( t_N \) from eq. (25).

Since in general \( f_Q \) is not an integer, the measured \( \tilde{f}_N \) will not match exactly the true value of \( f_Q \), and consequently (defining \( \tilde{t}_N \equiv N \sin^2 \theta_N, )\) with \( \theta_N = \theta_N(\tilde{f}_Q) \) we will have an error over \( t_N \) \[ \equiv \frac{Q \theta_N}{\pi} \] given by
\[ |\Delta t_N|_{\text{exp}} \equiv |\tilde{t}_N - t_N| \leq \frac{N}{Q} \left[ \frac{\pi}{2} + \sqrt{\pi} \right] \equiv O \left[ \frac{N}{Q} l(N)^{-(1+\epsilon/2)} \right]. \]
(30)

Then, if we want to check the theoretical formula for \( t_N \) with a precision up to some power \( \delta \), with \( 0 < \delta \ll \epsilon \) in \( l(N) \), i.e. with
\[ |\Delta t_N|_{th} \equiv O[N l(N)^{-2(\epsilon+\delta)}], \]
(31)

we have to impose that \( |\Delta t_N|_{exp} < |\Delta t_N|_{th} \), which implies that we can take \( Q \) as given by eq. (25) with \( \beta > 1 + \epsilon/2 + \delta. \] The computational complexity of the quantum algorithm can be finally estimated as \( S_Q \equiv O[QPS_Q] \geq O[l(N)^{2(\epsilon+2\delta)}], \) i.e. superpolynomial but still subexponential in \( \log N \).

V. DISCUSSION

Our quantum algorithms testing and counting Carmichael numbers make essential use of some of the basic blocks of quantum networks known so far, i.e. Grover’s operator for the quantum search of a database \[ [5], \] Shor’s Fourier transform for extracting the periodicity of a function \[ [5] \] and their combination in the counting algorithm of ref. \[ [5] \]. The most important feature of our quantum probabilistic algorithms is that the coin tossing used in the correspondent classical probabilistic ones is replaced here by a unitary and reversible operation, so that the quantum algorithm can even be used as a subroutine in larger and more complicated networks. Our quantum algorithm may also be useful for other similar tests and counting problems in number theory if there exists a classical probabilistic algorithm which somehow can guarantee a good success probability. Finally, it is known that in a classical computation one can count, by using

\[ 555\text{Since the probability of measuring the last qubit in eq. (24) in the state } | 1 > :G \text{ is given, this time, by } P_{1:G} = \langle \Psi | 1 > :G | \Psi >, \text{ this means that we require only an average number } T_{av} \approx (P_{1:G})^{-1} \equiv O[1] \text{ of repetitions of the algorithm from eq. (14) to eq. (20).} 
\]

\[ 555\text{Where } f_- \equiv |f_Q| + \delta f \text{ and } f_+ \equiv f_+ + 1, \text{ with } 0 < \delta f < 1. \]

\[ 555\text{Formula (24) is calculated (see ref. [5]) from the estimate of } W_{E_n} \text{ (the contribution coming from terms in eq. (23), involving } |E_n>, \text{ using the upper bound } E_n|E_n| \leq O[n^2] < E|E > \text{ and choosing } P \approx c Q, \text{ with } c > 1. \text{ An alternative to this choice, for reducing the 'error' probability } W_{E_n}, \text{ is to repeat the counting algorithm a sufficient number of times, as done in section III.} \]

\[ 555\text{One can further minimize the errors (i.e., boost the success probability } W \text{ exponentially close to one and achieve an exponential accuracy) by repeating the whole algorithm and using the majority rule [5].} \]

\[ 555\text{The contribution from a single Grover’s transform is } S_G \equiv O[poly(\log N)] \text{, which is dominated by the contribution coming from } QP \approx c Q^2. \text{ Furthermore, the use of } R \text{ ancilla qubits, as done in section III, instead of the choice } P \approx c Q, \text{ would lead to the (subexponential in } \log N \text{) complexity } S_Q \geq l(N)^{(1+\epsilon/2+\delta)(1+1/R)}. \]
Monte-Carlo methods, the cardinality of a set which satisfies some conditions, provided that the distribution of the elements of such a set is assumed to be known (e.g., homogeneous). One further crucial strength and novelty of our algorithm is also in the ability of efficiently and successfully solve problems where such a knowledge or regularities may not be present.

Acknowledgements

A.H.’s research was partially supported by the Ministry of Education, Science, Sports and Culture of Japan, under grant n. 09640341. A.C.’s research was supported by the EU under the Science and Technology Fellowship Programme in Japan, grant n. ERBIC17CT970007; he also thanks the cosmology group at Tokyo Institute of Technology for the kind hospitality during this work. Both authors would like to thank Prof. N. Kurokawa for helpful discussions.

[1] P. Benioff, Journ. Stat. Phys., 22, 563 (1980); D. Deutsch, Proc. Roy. Soc. London, Ser. A 400, 96 (1985); R.P. Feynman, Found. Phys., 16, 507 (1986).
[2] D.P. DiVincenzo, Science, 270, 255 (1995); A. Steane, Rep. Prog. Phys., 61, 117 (1998).
[3] P.W. Shor, in Proceedings of the 35th Annual Symposium on Foundations of Computer Science, ed. S. Goldwater (IEEE Computer Society Press, New York, 1994), p. 124; SIAM Journ. Comput., 26, 1484 (1997).
[4] L.K. Grover, in Proceedings of the 28th Annual Symposium on the Theory of Computing (ACM Press, New York, 1996), p. 212; Phys. Rev. Lett., 79, 325 (1997).
[5] G. Brassard, P. Hoyer and A. Tapp, Los Alamos e-print quant-ph/9805082; M. Boyer, G. Brassard, P. Hoyer and A. Tapp, in Proceedings of the 4th Workshop on Physics and Computation, ed. T. Toffoli et al. (New England Complex Systems Institute, Boston, 1996), p. 36; also in Los Alamos e-print quant-ph/9605034 (1996) and Fortsch. Phys., 46, 493 (1998).
[6] A. Carlini and A. Hosoya, Los Alamos e-print quant-ph/9907026.
[7] P. Ribenboim, The New Book of Prime Number Records (Springer-Verlag, New York, 1996).
[8] R.D. Carmichael, Bull. Am. Math. Soc., 16, 232 (1910).
[9] W.R. Alford, A. Granville and C. Pomerance, Ann. Math., 140, 703 (1994).
[10] L. Monier, Theor. Comp. Sci., 12, 97 (1980).
[11] R. Baillie and S.S. Wagstaff Jr., Math. Comp., 35, 1391 (1980).
[12] P. Erdos and C. Pomerance, Math. Comp., 46, 259 (1986).
[13] M.O. Rabin, Journ. Num. Th., 12, 128 (1980); also in Algorithms and Complexity, Recent Results and New Directions, ed. J.F. Traub (Academic Press, New York, 1976), p. 21; C.L. Miller, J. Comp. Syst. Sci., 13, 300 (1976).
[14] C. Pomerance, J.L. Selfridge and J.J. Wagstaff Jr., Math. Comp., 35, 1003 (1980).
[15] P. Erdos, Publ. Math. Debrecen., 4, 201 (1956).