Semiclassical Shor's Algorithm

Paolo Giorda[a*], Alfredo Iorio[b†], Samik Sen[c‡], Siddhartha Sen[c,d§]
[a] *Institute for Scientific Interchange, Villa Gualino*
Viale Settimio Severo 65, 10133 Turin - Italy
[b] *Center for Theoretical Physics, Massachusetts Institute of Technology*
77, Massachusetts Avenue, Cambridge MA 02139-4307 - U.S.A.
and I.N.F.N. - Italy
[c] *School of Mathematics, Trinity College Dublin, Dublin 2 - Ireland*
[d] *I.A.C.S., Jadavpur, Calcutta 700032 , India*
(May 18, 2004)

Abstract

We propose a semiclassical version of Shor's quantum algorithm to factorize integer numbers, based on spin-1/2 SU(2) generalized coherent states. Surprisingly, we find evidences that the algorithm's success probability is not too severely modified by our semiclassical approximation. This suggests that it is worth pursuing practical implementations of the algorithm on semiclassical devices.

PACS No.: 03.67.-a, 03.67.Lx, 03.65.Sq
Keyword(s): Quantum Information, Quantum Computation, Semiclassical Theories and Applications
MIT-CTP-3346 quant-ph/0303037

*E-mail: giorda@isiosf.isi.it

†E-mail: iorio@lns.mit.edu

‡E-mail: samik@maths.tcd.ie

§E-mail: sen@maths.tcd.ie, tcss@mahendra.iacs.res.in

I. INTRODUCTION

The discovery by P. Shor of an efficient algorithm to factorize integer numbers based on the laws of quantum mechanics [1] (see also [2]), was a landmark event in quantum computing [3] (see also [4] and [5]). Shor's quantum algorithm determines the prime factors of a composite l-bit number N in[1] $O[l^2 \log l \log\log l]$ steps, while the best classical algorithm of A.K. Lenstra and H.W. Lenstra [6] requires $O[\exp\{cl^{1/3}\log^{2/3} l\}]$ steps, for some c. This shows how powerful a quantum computer could be.

This discovery fueled the theoretical and experimental search for practical realizations of such a "machine of wonders" (see for instance [2], [4], [7], [8], and references therein). Nonetheless, to build a quantum computer with the required power is a very challenging and still not accomplished task. This makes Shor's algorithm a theoretically important work which, at present, cannot be implemented if not for very small numbers [9], [10]. It is then of strong interest to explore *semiclassical* limits of Shor's algorithm, and to see how much the related approximations affect the algorithm. Some ideas along these lines are already present in the literature [11]. There it is shown that the Quantum Fourier Transform (the core of the algorithm), could be simplified if one uses a macroscopic signal to control the quantum gates.

We assume here that semiclassical devices should be easier to handle than quantum devices, a semiclassical device being (in this context) a physical system performing the computation, whose dynamics is partially governed by the laws of classical physics and partially by those of quantum mechanics. A cogent example is the system imagined in [11], where the macroscopic signal controlling the quantum gates is a pulse of several volts in a coaxial cable. It is easy to convince oneself that, on general grounds, it is a lot handier to deal with such a classical pulse than to deal with more "fragile" (decohering) quantum signals.

The approach we take in this paper is fundamental and general, as we would like to give the mathematical prescriptions for implementing Shor's algorithm on generic semiclassical devices. We shall make use of generalized coherent states, and tackle the difficult problem to find out what a semiclassical approximation is in this framework. Our primary goal is to see if the semiclassical limit of Shor's algorithm is still more powerful than the classical factoring algorithm. If it is, the task of constructing a semiclassical computer would be worth pursuing.

The method we present here (based on generalized coherent states $|\lambda\rangle$ of SU(2) for spin $j = 1/2$) is made of two parts:

First, we show that in the $|\lambda\rangle$ basis a symplectic structure arises. Hence the physical system making the computation could, in principle, be described by a classical phase-space, and the computation itself as an evolution in this phase-space. In this setting, the quantum fluctuations are naturally dropped by mapping $j(j+1) \to j^2$. A fully classical version of Shor's algorithm would then be the one where all the quantum operators (gates) $\mathcal{O}$ are replaced by their classical counterparts $\langle\lambda|\mathcal{O}|\lambda\rangle$, and the quantum evolution replaced by a classical path over the phase-space.

---

[1]Here, and in what follows $\log \equiv \log_2$ and $\ln \equiv \log_e$, unless otherwise stated.

In particular this philosophy applies to the Quantum Fourier Transform Φ. A classical version of Φ would be the one with the string of operators R_is, and $S_{i,j}$s, entering the expression of Φ, replaced by $\langle\lambda|R_i|\lambda\rangle$s, and $\langle\lambda|S_{i,j}|\lambda\rangle$s, respectively. We define to be *semiclassical* the approximation that replaces Φ with $\langle\lambda|\Phi|\lambda\rangle$. This is the second part of our recipe for semiclassicality in this framework.
In the next Section, we shall introduce the notation and review the key ideas of Shor's algorithm. In Section III, we shall explain the two parts of our coherent state semiclassical approximation: the classical time-evolution for the spin 1/2 system making the computation (Subsection III.A); and the coherent state approximation of the Quantum Fourier Transform (Subsection III.B). Eventually, in Section IV we shall evaluate the effects of the semiclassical approximations on the success probability of Shor's algorithm, and we shall perform some numerical tests and comment on them. The last Section is devoted to the conclusions.

II. INTEGER FACTORING AND QUANTUM MECHANICS

Given an l-bit integer number N, the fastest way to factor it into relative co-primes $N = n_1 \cdot n_2 \cdot ...$ is to find t_1 and t_2 such that $t_1^2 = t_2^2(\mathrm{mod}N)$, and $t_1 \neq \pm t_2(\mathrm{mod}N)$, thus one can write

$$(t_1 + t_2)(t_1 - t_2) = 0(\mathrm{mod}N)\,, \tag{II.1}$$

where neither $(t_1 + t_2)$ nor $(t_1 - t_2)$ is zero $(\mathrm{mod}N)$. It is then matter of finding the greatest common divisors: $\gcd(t_1 + t_2, N)$, and $\gcd(t_1 - t_2, N)$ to have two of the factors, and so on. This approach is used by both the best known classical and best known quantum algorithms for factoring.
The quantum algorithm uses a further result of number theory: if one randomly picks an integer $1 < x < N$, and $\gcd(x, N) = 1$ (otherwise we would have been so lucky to have already found a factor of N), then the period L of the function

$$f(a) = x^a(\mathrm{mod}N)\,, \quad \text{with} \quad f(a + L) = f(a)(\mathrm{mod}N)\,, \tag{II.2}$$

determines the factors of N, provided L is even and $x^{L/2} \neq -1(\mathrm{mod}N)$. This can be easily seen from the fact that $x^a = x^{a+L}(\mathrm{mod}N)$ implies

$$x^L = 1(\mathrm{mod}N)\,, \tag{II.3}$$

and, for L even, both sides are squares. Thus, since $x^{L/2} \neq \pm 1(\mathrm{mod}N)$, one can proceed as in Eq. (II.1), and compute $\gcd(x^{L/2} \pm 1, N)$. This procedure, on which the Shor's method to determine L "quickly" is based, would take a polynomial time on a computer that makes use of the laws of quantum mechanics.
Let us now introduce a mathematical and physical framework to describe a quantum computer, give some of the details of Shor's algorithm, and introduce our notation.
As any quantum system, a quantum computer is described by a Hilbert space [12], and its logic is implemented by operators (quantum gates) acting on this Hilbert space. In the usual model one considers the Hilbert spaces that are tensor products of two-state systems or quantum bits. In the spin-1/2 representation of a quantum bit, a spin state with $j = -\hbar/2$

(spin down) represents the binary digit zero, and a spin state with $j = +\hbar/2$ (spin up) represents the binary digit one. These states form a basis of the two-level Hilbert space $\mathcal{H}_2$, and are usually represented as

$$\text{(i) } |\frac{1}{2}, -\frac{1}{2}\rangle \text{ or (ii) } |0\rangle \text{ or (iii) } \begin{pmatrix} 1 \\ 0 \end{pmatrix} , \tag{II.4}$$

for spin down, and

$$\text{(i) } |\frac{1}{2}, +\frac{1}{2}\rangle \text{ or (ii) } |1\rangle \text{ or (iii) } \begin{pmatrix} 0 \\ 1 \end{pmatrix} , \tag{II.5}$$

for spin up, depending on the notation. The notation (i) will be used only in Section III.A to make the role of the spin $j = 1/2$ explicit. The full Hilbert space used to represent a l-bit number is then

$$\mathcal{H} = \bigotimes_{i=0}^{l-1} \mathcal{H}_2^i \, . \tag{II.6}$$

Clearly such two-level systems can be physically realized in many other ways, see for instance [13]. However, in all cases, the algebraic structure of importance can be represented by such a tensor product space.

The spin states above form a representation of the Lie algebra SU(2) of angular momentum. As is well known, this Lie algebra has three generators J_0, J_1, and J_2, and one can introduce the step-up, $J_+ = J_1 + iJ_2$, and step-down, $J_- = J_1 - iJ_2$, generators to write the defining commutation relations of SU(2) as

$$[J_+, J_-] = 2\hbar J_0 \, , \quad [J_0, J_\pm] = \pm\hbar J_\pm \, , \tag{II.7}$$

also known as the Cartan-Weyl form of the Lie algebra. In the next Section we shall present a semiclassical version of this quantum system.

We now want to briefly summarize Shor's quantum factoring algorithm. We start with the definition of the Quantum Fourier Transform (QFT) acting on a state

$$|a\rangle = |a_{l-1}, ..., a_0\rangle \, , \tag{II.8}$$

where $a_i = 0, 1$, $\forall i = 0, ..., l-1$. This is the quantum representative of the l-bit number $a = \sum_{i=0}^{l-1} a_i 2^i$, $a_{\max} = 2^l - 1 \equiv q - 1$, hence $q \equiv 2^l$. Note the order of the entries in Eq. (II.8).

The QFT acts by replacing $|a\rangle$ by

$$|a\rangle \to \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} |c\rangle \exp\{2\pi i \frac{a \cdot c}{q}\} \, , \tag{II.9}$$

where, as for $|a\rangle$, $|c\rangle$ is the quantum representative of the l-bit number $c = \sum_{j=0}^{l-1} c_j 2^j$, $c_i = 0, 1$ $\forall i = 0, ..., l-1$. This is achieved by acting on $|a\rangle$ with the string of $l(l-1)/2$ operators in the given order

$$\Phi = R_0 S_{0,1} S_{0,2} ... S_{0,l-2} S_{0,l-1} R_1 S_{1,2} S_{1,3} ... S_{1,l-2} S_{1,l-1} R_2 ... R_{l-2} S_{l-2,l-1} R_{l-1} \ , \tag{II.10}$$

where the operators R_i act on the i^{th} two-states Hilbert space $\mathcal{H}_2^i$, and the operators $S_{i,j}$, $j > i$, act on tensor products of two-states Hilbert spaces $\mathcal{H}_2^i \otimes \mathcal{H}_2^j$. While the expression for Φ in Eq. (II.10) is independent on the notation, the operators R_i can be expressed as

$$R_i = \frac{1}{\sqrt{2}} [|0_i\rangle\langle 0_i| + |0_i\rangle\langle 1_i| + |1_i\rangle\langle 0_i| + e^{i\pi} |1_i\rangle\langle 1_i|] \ , \tag{II.11}$$

in notation (i), or

$$R_i = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \ , \tag{II.12}$$

in notation (ii), and the operators $S_{i,j}$ are given by

$$S_{i,j} = [|0_j, 0_i\rangle\langle 0_j, 0_i| + |0_j, 1_i\rangle\langle 0_j, 1_i| + |1_j, 0_i\rangle\langle 1_j, 0_i| + e^{i\theta_{ij}} |1_j, 1_i\rangle\langle 1_j, 1_i|] \ , \tag{II.13}$$

in notation (i), or

$$S_{i,j} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta_{ij}} \end{pmatrix} \ , \tag{II.14}$$

in notation (ii), where $\theta_{ij} = \pi / 2^{j-i}$. It can be shown [1] that the string of operators in Φ generates the required state (II.9) only after the bits representing the output have been reversed. Since this can be done in polynomial time, we omit this step except where the analysis requires more care.

The state one starts from for the implementation of Shor's procedure is simply $|0\rangle|0\rangle$. Thus one first obtains $\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle|0\rangle$ by acting with Φ on the first register. Then the modular exponentiation on the second register gives the state

$$|s\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle |x^a (\text{mod} N)\rangle \ , \tag{II.15}$$

where N is the number to be factored. It is now matter of applying again the QFT Φ to the first register in $|s\rangle$ to obtain

$$|s'\rangle = \frac{1}{q} \sum_{a,c=0}^{q-1} \exp\{2\pi i \frac{a \cdot c}{q}\} |c\rangle |x^a (\text{mod} N)\rangle \ . \tag{II.16}$$

The probability of observing $\hat{c}$, and $x^k (\text{mod} N)$ is easily computed as

$$\begin{aligned} \mathbf{P}(\hat{c}, x^k (\text{mod} N)) &\equiv \left| \langle \hat{c}, x^k (\text{mod} N) | s' \rangle \right|^2 \\ &= \left| \frac{1}{q} \sum_{a=0}^{q-1} \exp\{2\pi i \frac{a \cdot \hat{c}}{q}\} \right|^2_{a = k (\text{mod} L)} \ . \end{aligned} \tag{II.17}$$

The probability (II.17) is thus a function of the period L of $x^a(\mathrm{mod}N)$ which we want to determine. Hence measuring $\hat{c}$, and $x^k(\mathrm{mod}N)$ turns into a way of determining L. This is seen by noticing that $a = k(\mathrm{mod}L)$ means $a = k + fL$ for some integer f, hence

$$\mathbf{P}(\hat{c}, x^k(\mathrm{mod}N)) = \left| \frac{1}{q} \sum_{f=0}^{[(q-k-1)/L]} \exp\{2\pi i f \frac{\{L\hat{c}\}_q}{q}\} \right|^2 , \tag{II.18}$$

where $[A]$ is the integer part of A, and $\{L\hat{c}\}_q \equiv L\hat{c} - dq$ for some integer d. One also would like to maximize this probability by choosing the phases in the sum (II.18) to point as close as possible to the same direction in the complex plane. This is achieved in [1] by requiring

$$-\frac{L}{2} < \{L\hat{c}\}_q < \frac{L}{2} , \tag{II.19}$$

or, equivalently, (using the definition of $\{L\hat{c}\}_q$)

$$\left| \frac{\hat{c}}{q} - \frac{d}{L} \right| < \frac{1}{2q} . \tag{II.20}$$

When this condition is satisfied, for large qs the sum in (II.18) can be approximated to order $O(1/q)$ by the integral

$$\frac{1}{L} \int_0^1 \exp\{2\pi \frac{\{L\hat{c}\}_q}{L} u\} du , \tag{II.21}$$

where $u \equiv Lf/q$. This integral is minimized when $\{L\hat{c}\}_q/L = \pm 1/2$, giving the lower bound $4/(\pi L)^2 \sim 1/3L^2$ for the probability (II.18):

$$\mathbf{P}(\hat{c}, x^k(\mathrm{mod}N)) > \frac{1}{3L^2} . \tag{II.22}$$

In Fig. 1 we plot $\mathbf{P}$ against $\hat{c}$ for $q = 256$, $L = 10$. By inspection of (II.20) one immediately sees that L was found: $\hat{c}$ was measured, q is known, and d/L is the best rational representation of the real number $\hat{c}/q$, and can be determined by using a continuous fraction expansion.

There are two leading contributions to the complexity of this algorithm:

i) The modular exponentiation. This part of the algorithm could be implemented classically (it is not known a quantum way to speed it up), and the complexity of this procedure is known to be $O(l^2 \log l \log\log l)$.

ii) The QFT Φ. By counting how many operators enter the expression (II.10) of Φ, we notice that this part of the algorithm involves $O(l^2)$ steps.

One thus conclude that the overall complexity is $O(l^2 \log l \log\log l)$.

III. THE SEMICLASSICAL APPROXIMATIONS

To present our semiclassical approximation, we want now to exploit the semiclassical nature of the coherent states associated with the Lie algebra SU(2). First we shall construct the classical phase-space associated with the Lie algebra of the angular momentum (II.7). Then we shall introduce our coherent states approximation of Shor's algorithm, with special emphasis on the QFT Φ.

A. Symplectic Structure and Classical "Time-Evolution"

Mathematically a classical representation of the Lie algebra SU(2) corresponds to determine the associated phase-space, with its symplectic structure, such that *commutators* of the Lie algebra are realized as *Poisson brackets* of appropriate functions derived in this phase-space. The procedure for doing so is well known, and is based on generalized coherent states [14]. Let us briefly summarize it.

We start by defining an unnormalized coherent state

$$|\lambda\rangle = \exp\{\lambda \frac{J_+}{\hbar}\}|\frac{1}{2}, -\frac{1}{2}\rangle \ , \tag{III.1}$$

where λ is a complex number, we use the basis (i) in (II.5), $|\frac{1}{2}, -\frac{1}{2}\rangle$, $|\frac{1}{2}, +\frac{1}{2}\rangle$, and the angular momentum operators $\tilde{J}_0 = J_0/\hbar$, $\tilde{J}_+ = J_+/\hbar$, and $\tilde{J}_- = J_-/\hbar$ are dimensionless. This last point is of some importance since we are going to introduce *dimensionless* Poisson brackets, whereas the standard Poisson brackets have dimension [action]$^{-1}$. Thus we shall eventually end up with a symplectic structure for the dimensionless operators $\tilde{J}_0$, $\tilde{J}_+$, and $\tilde{J}_-$. In the coherent state representation these operators, suitably normalized, are the complex functions

$$\begin{aligned} \mathcal{J}_0 &\equiv \frac{\langle\lambda|\tilde{J}_0|\lambda\rangle}{\langle\lambda|\lambda\rangle} = -\frac{1}{2}\frac{1-|\lambda|^2}{1+|\lambda|^2} \ , \\ \mathcal{J}_+ &\equiv \frac{\langle\lambda|\tilde{J}_+|\lambda\rangle}{\langle\lambda|\lambda\rangle} = \frac{\bar{\lambda}}{1+|\lambda|^2} \ , \\ \mathcal{J}_- &\equiv \frac{\langle\lambda|\tilde{J}_-|\lambda\rangle}{\langle\lambda|\lambda\rangle} = \frac{\lambda}{1+|\lambda|^2} \ . \end{aligned} \tag{III.2}$$

They have the general property that

$$\mathcal{J}_+\mathcal{J}_- + \mathcal{J}_0^2 = j^2 \, . \tag{III.3}$$

In our case, $j = 1/2$. Hence the vector $(\mathcal{J}_0, \mathcal{J}_1, \mathcal{J}_2)$ has length $j = 1/2$, and represents a point on the surface of the sphere $S^2 \sim SU(2)/U(1)$ of radius 1/2. On this see also [14].

The first part of our semiclassical description is to represent the SU(2) algebra of quantum angular momentum in the coherent state functional form (III.2). This causes: i) the quantum fluctuations in the angular momentum to be automatically dropped via $j(j+1) \to j^2$, as can be seen from Eq. (III.3) above; and ii) a symplectic structure over the space of the stereographic coordinates on the sphere naturally to arise. To see how point ii) is achieved we introduce the Kähler potential [15], $V(\lambda, \bar{\lambda}) = \ln\langle\lambda|\lambda\rangle = \ln(1+|\lambda|^2)$, to construct the associated symplectic form ω on the phase-space defined by the complex variables λ, and $\bar{\lambda}$

$$\omega = \omega_{\lambda,\bar{\lambda}} d\lambda \wedge d\bar{\lambda} \tag{III.4}$$

where

$$\omega_{\lambda,\bar{\lambda}} = -\omega_{\bar{\lambda},\lambda} \equiv \frac{\partial^2 V}{\partial\lambda\partial\bar{\lambda}} = (1+|\lambda|^2)^{-2} \ , \tag{III.5}$$

and of course $(\omega^{-1})_{\lambda,\bar{\lambda}} = (1+|\lambda|^2)^2$.
The Poisson brackets of any two functions on the λ, $\bar{\lambda}$ phase-space[2], $f(\lambda,\bar{\lambda})$, $g(\lambda,\bar{\lambda})$ can then be defined as

$$\{f,g\} \equiv (\omega^{-1})_{\lambda,\bar{\lambda}}\partial_\lambda f \partial_{\bar{\lambda}} g + (\omega^{-1})_{\bar{\lambda},\lambda}\partial_{\bar{\lambda}} f \partial_\lambda g \ , \tag{III.6}$$

leading to the following Poisson brackets of $\mathcal{J}_0, \mathcal{J}_+, \mathcal{J}_-$

$$\{\mathcal{J}_+, \mathcal{J}_-\} = 2\mathcal{J}_0 \ , \quad \{\mathcal{J}_0, \mathcal{J}_\pm\} = \pm\mathcal{J}_\pm \ . \tag{III.7}$$

This is the Lie algebra SU(2) we started from, but in a dimensionless semiclassical form. This establishes the fact that the phase-space corresponding to SU(2) is $S^2 \sim SU(2)/U(1)$ with stereographic coordinates $\mathcal{J}_+$,$\mathcal{J}_-$, and $\mathcal{J}_0$.
We can move further to define the Hamiltonian H associated with the symplectic form ω. To this end, we introduce a vector field $v = v^\lambda\partial_\lambda + v^{\bar{\lambda}}\partial_{\bar{\lambda}}$ that keeps ω invariant

$$\mathbf{L}_v\omega = \left(v^\lambda\partial_\lambda\omega_{\lambda\bar{\lambda}} + v^{\bar{\lambda}}\partial_{\bar{\lambda}}\omega_{\bar{\lambda}\lambda} + \omega_{\lambda\bar{\lambda}}\partial_\lambda v^\lambda + \omega_{\bar{\lambda}\lambda}\partial_{\bar{\lambda}}v^{\bar{\lambda}}\right) d\lambda\wedge d\bar{\lambda} \equiv 0 \ , \tag{III.8}$$

where $\mathbf{L}_v$ is the Lie derivative associated with the vector field v [15]. By computing the Lie derivative one obtains the following conditions for the vector field $v^\lambda = C\lambda$, and $v^{\bar{\lambda}} = C\bar{\lambda}$, with C a complex constant.
One can also write the Lie derivative as $\mathbf{L}_v = d\cdot i_v + i_v\cdot d$, where the exterior derivative d and the internal product (or contraction) i_v act on p-forms $\omega\in\Omega^p$ as $d:\Omega^p\to\Omega^{p+1}$, and $i_v:\Omega^p\to\Omega^{p-1}$, respectively. To be more explicit let us write a p-form in local coordinates on a symplectic manifold M of even dimension $2n$

$$\omega = \frac{1}{p!}\omega_{i_1\ldots i_p}(x_1,\ldots,x_{2n})dx_{i_1}\wedge\ldots\wedge dx_{i_p} \ , \tag{III.9}$$

where $\omega_{i_1\ldots i_p}$ is a totally antisymmetric tensor field, and $x_1,\ldots,x_{2n}$ are the local coordinates on the $2n$ dimensional symplectic manifold M. Thus

$$d\omega = \frac{1}{(p+1)!}\partial_k\omega_{i_1\ldots i_p}dx_k\wedge dx_{i_1}\wedge\ldots\wedge dx_{i_p} \ , \tag{III.10}$$

while

$$i_v\omega = \frac{1}{(p-1)!}(-1)^j v^j\omega_{i_1\ldots j\ldots i_p}dx_{i_1}\wedge\ldots\wedge\hat{dx_j}\wedge\ldots\wedge dx_{i_p} \ , \tag{III.11}$$

where $v = v^j\partial_j$, and $\hat{dx_j}$ means that dx_j is missing.

---

[2]Although, for the sake of simplicity, we shall denote the phase-space variables as λ and $\bar{\lambda}$, from the definition (III.6) it is clear that, if, for instance, we choose λ as the generalized coordinate, its conjugate momentum is $p_\lambda = \bar{\lambda}/(1+\lambda\bar{\lambda})$, so that $\{\lambda, p_\lambda\} = 1$. For the other choice, $\bar{\lambda}$ is the generalized coordinate, and its conjugate momentum is $p_{\bar{\lambda}} = -\lambda/(1+\lambda\bar{\lambda})$.

In our case ω is a symplectic two-form, hence it is closed, $d\omega = 0$. Then, $\mathbf{L}_v\omega = 0$ implies that $d(i_v\omega) = 0$. According to the lemma of Poincarè it follows that locally the one-form $i_v\omega$ is equal to d acting on a function (a zero-form) which we call $-H$

$$i_v\omega = -dH \ . \tag{III.12}$$

If H can also be globally defined, then it can be taken as the Hamiltonian corresponding to the vector field v.
By using the definition (III.11), and the above given conditions for the vector field to leave ω invariant (with $C = 1/2$) we obtain

$$i_v\omega = -v^\lambda\omega_{\lambda\bar{\lambda}}d\bar{\lambda} + v^{\bar{\lambda}}\omega_{\bar{\lambda}\lambda}d\lambda = -\frac{1}{2}\frac{\lambda d\bar{\lambda} + \bar{\lambda}d\lambda}{(1+\lambda\bar{\lambda})^2} \ , \tag{III.13}$$

which gives

$$H = -\frac{1}{2}\frac{1-\lambda\bar{\lambda}}{1+\lambda\bar{\lambda}} \ , \tag{III.14}$$

as a possible classical Hamiltonian. Once H is chosen it determines the dynamics in the phase-space, generating the "time-evolution" of any function $f(\lambda, \bar{\lambda})$ as

$$\dot{f} \equiv \{H, f\} \ . \tag{III.15}$$

It is straightforward to check that $\dot{f} = i\partial f/\partial\phi$, where $\lambda = re^{i\phi}$. Hence the dimensionless time parameter of the semiclassical evolution is $t = -i\phi$.
By noticing that $\mathcal{J}_0 = H$, and using (III.7) one has

$$\dot{\mathcal{J}}_\pm = \pm\mathcal{J}_\pm \ , \quad \dot{\mathcal{J}}_0 = 0 \ . \tag{III.16}$$

Thus, in the semiclassical limit, the quantum spin system we started out with has been replaced by coordinates on S^2, with the associated symplectic form. A Hamiltonian consistent with this symplectic form can be introduced. That leads to uniformly precessing coordinates $\mathcal{J}_+$, and $\mathcal{J}_-$, always preserving the length of the vector. This is a classical spinning vector. Note also that

$$\{\mathcal{J}_+, \mathcal{J}_-\} = 2H \ . \tag{III.17}$$

The first step towards our attempt to construct a semiclassical version of Shor's algorithm is now complete. The key observation is that λ can be interpreted as a variable that describes a classical spinning particle.

B. Coherent State Approximation of Shor's Algorithm

We now move to the second stage of the semiclassical approximation. The steps of the quantum procedure we propose to modify are the ones involving the QFT which consists in the following replacement

$$|a\rangle \to \sum_{c=0}^{q-1} |c\rangle\langle c|\Phi|a\rangle \ , \tag{III.18}$$

with $\langle c|\Phi|a\rangle = q^{-1/2}\exp\{2\pi i a\cdot c/q\}$. We want to write (III.18) in the basis of *normalized* coherent states $|\lambda\rangle = |\lambda_{l-1},...,\lambda_0\rangle$

$$|\lambda_i\rangle \equiv (1+\lambda_i\bar{\lambda}_i)^{-1/2}(|0_i\rangle + \lambda_i|1_i\rangle) \quad \forall i = 0,...,l-1\,. \tag{III.19}$$

This can be done as follows

$$\langle c|\Phi|a\rangle = \int d\mu(\lambda)d\mu(\lambda')\langle c|\lambda\rangle\langle\lambda|\Phi|\lambda'\rangle\langle\lambda'|a\rangle \ , \tag{III.20}$$

where the measure is defined by requiring $\int d\mu(\lambda)|\lambda\rangle\langle\lambda| \equiv \mathbf{1}$, and is given by

$$\int d\mu(\lambda) = \prod_{i=0}^{l-1}\int \frac{[d\lambda_i]^2}{(1+\lambda_i\bar{\lambda}_i)^2} = \prod_{i=0}^{l-1}\frac{2}{\pi}\int_0^{2\pi} d\phi_i \int_0^{\infty}\frac{r_i dr_i}{(1+r_i^2)^2}\,, \tag{III.21}$$

with $\lambda_i = r_i e^{i\phi_i}$, and

$$\langle c|\lambda\rangle = \prod_{i=0}^{l-1}(1+\lambda_i\bar{\lambda}_i)^{-1/2}\lambda_i^{c_i} = \prod_{i=0}^{l-1}(1+r_i^2)^{-1/2}r_i^{c_i}e^{ic_i\phi_i} \ , \tag{III.22}$$

$$\langle\lambda'|a\rangle = \prod_{i=0}^{l-1}(1+\lambda'_i\bar{\lambda}'_i)^{-1/2}\bar{\lambda}_i'^{a_i} = \prod_{i=0}^{l-1}(1+r'^2_i)^{-1/2}r'^{a_i}_i e^{-ia_i\phi'_i} \ . \tag{III.23}$$

Here no approximation has been made yet. This is a simple change of basis that, of course, preserves all the information content of $\langle c|\Phi|a\rangle$.
The approximation we now make in Eq. (III.20) consists in keeping only the diagonal entries in the coherent state basis, namely

$$\langle\lambda|\Phi|\lambda'\rangle \sim \delta_{\lambda\lambda'}\langle\lambda|\Phi|\lambda\rangle\,, \tag{III.24}$$

and then perform the λ integrals. In what follows we shall introduce the short-hand notation $\langle\lambda|\mathcal{M}|\lambda\rangle \equiv \mathcal{M}^\lambda$, for any matrix $\mathcal{M}$.
In Appendix A it is proved that, for any matrix $\mathcal{M}$, $\mathcal{M}^\lambda$ preserves all the information. It is important to stress that, although no *quantum* information is lost by considering the $\mathcal{M}^\lambda$s, these functions are now described in terms of a set of variables that have a *classical* interpretation. Using the technique described in detail in Appendix A, we can write R_i^λ, $S_{i,j}^\lambda$

$$R_i^\lambda = \frac{\Lambda_i}{\sqrt{2}}[1+\lambda_i+\bar{\lambda}_i-\lambda_i\bar{\lambda}_i] \ , \tag{III.25}$$

$$S_{i,j}^\lambda = \Lambda_{i,j}[1+\lambda_i\bar{\lambda}_i+\lambda_j\bar{\lambda}_j+e^{i\theta_{ij}}\lambda_i\bar{\lambda}_i\lambda_j\bar{\lambda}_j] \ , \tag{III.26}$$

and Φ^λ

$$\Phi^\lambda = \frac{1}{\sqrt{q}}\Lambda_{0,...,l-1}\sum_{b,d=0}^{q-1} e^{2\pi i\frac{b\cdot d}{q}}\prod_{i=0}^{l-1}\lambda_i^{b_i}\bar{\lambda}_i^{d_{l-1-i}}\,, \tag{III.27}$$

where

$$\Lambda_{0,...,l-1} \equiv \prod_{i=0}^{l-1}(1+|\lambda_i|^2)^{-1} \ ,$$

and as in the case of the QFT of the standard Shor's algorithm (see Eq. (II.9)) the integer numbers b and d in $\exp\{2\pi i b\cdot d/q\}$ are given as $b=\sum_{i=0}^{l-1} b_i 2^i$, $b_i=0,1$, $\forall i=0,...,l-1$, and similarly for d, and we explicitly wrote the "label reversed" version of d only in the exponents of $\bar{\lambda}$.
One could go further and approximate Φ^λ with the appropriate product of R^λs and S^λs as

$$\Phi^\lambda \sim R^\lambda_0 S^\lambda_{0,1}...S^\lambda_{0,l-2}S^\lambda_{0,l-1}R^\lambda_1...R^\lambda_{l-2}S^\lambda_{l-2,l-1}R^\lambda_{l-1} \ . \tag{III.28}$$

If one does so, powers of λ_i and $\bar{\lambda}_i$ higher than 0 and 1 would be obtained. Thus one loses the matching between the dimension of the original Hilbert space and the dimension of the space of parameters. This last step could be seen as a high spin approximation of the QFT: the truly "classical" setting. We call "semiclassical" the approximation that stops at Φ^λ as given in Eq. (III.27) (see also Eq. (III.24)).
In this semiclassical setting, it is *only when we perform the integration over the λs* in Eq. (III.20), using (III.24), that some information is lost. To show this, let us first write Φ^λ in Eq. (III.27) in polar coordinates

$$\Phi^\lambda = \frac{1}{\sqrt{q}}\left(\prod_{i=0}^{l-1}[(1+r_i^2)]^{-1}\right)\sum_{b,d=0}^{q-1} e^{2\pi i\frac{b\cdot d}{q}}\prod_{i=0}^{l-1} r_i^{(b_i+d_i)}e^{i[(b_i-d_i)]\phi_i} \ , \tag{III.29}$$

where, to simplify the following computations, we substituted $d_{l-1-i}\to d_i$ as we shall consider $\langle c|\Phi|a\rangle$ rather than $\langle c^{\rm rev}|\Phi|a\rangle$, and read the entries of $\langle c|$ in reverse order only at the very end.
Using (III.29), the definition of the measure (III.21), and the expressions (III.22) and (III.23) for $\langle c|\lambda\rangle$ and $\langle\lambda|a\rangle$, respectively, we obtain

$$\langle c|\Phi|a\rangle \sim \int d\mu(\lambda)\langle c|\lambda\rangle\Phi^\lambda\langle\lambda|a\rangle = \frac{\sqrt{q}}{\pi^l}\sum_{b,d=0}^{q-1} e^{2\pi i\frac{b\cdot d}{q}}\mathcal{I}_{acbd} \ , \tag{III.30}$$

where

$$\mathcal{I}_{acbd} \equiv \prod_{i=0}^{l-1}\int_0^\infty \frac{r_i dr_i}{(1+r_i^2)^4} r_i^{(c_i+a_i)+(b_i+d_i)}\int_0^{2\pi} d\phi_i e^{i[(c_i-a_i)+(b_i-d_i)]\phi_i} \ . \tag{III.31}$$

The final effect of the integration is to modify the state of Shor's algorithm $|s'\rangle$ (see Eq. (II.16)), on which one has to perform the measurement, to the state $|\mathcal{S}'\rangle$ given by

$$|\mathcal{S}'\rangle \equiv \frac{1}{\pi^l}\sum_{a,c=0}^{q-1}\left(\sum_{b,d=0}^{q-1} e^{2\pi i\frac{b\cdot d}{q}}\mathcal{I}_{acbd}\right)|c\rangle|x^a(\mathrm{mod}N)\rangle \ . \tag{III.32}$$

By inspection

$$\mathcal{I}_{acbd} = A_{acbd}\delta_{d,\,b+c-a}\,, \tag{III.33}$$

and the nonzero coefficients are[3]

$$A_{acbd} = q\pi^l \prod_{i=0}^{l-1} \frac{1}{12}(1+\delta_{b_i c_i}) = \frac{\pi^l}{q3^l}\prod_{i=0}^{l-1}(1+\delta_{b_i c_i}) \equiv \frac{\pi^l}{q3^l}h(b,c)\,, \tag{III.34}$$

where

$$h(b,c) \equiv \prod_{i=0}^{l-1}(1+\delta_{b_i c_i}) \in \{1,2,...,2^{l-1},2^l\}\,, \tag{III.35}$$

depending on how many bits of the numbers c and b are equal[4].
Thus some of the original information is now clearly lost:

$$|\mathcal{S}'\rangle = \frac{1}{3^l}\frac{1}{q}\sum_{b,\,a,c=0}^{q-1} h(b,c)\exp\{i\frac{2\pi}{q}\,b\,(b+c-a)\}|c\rangle|x^a(\mathrm{mod}N)\rangle\,, \tag{III.36}$$

as compared to (II.16)

$$|s'\rangle = \frac{1}{q}\sum_{a,c=0}^{q-1}\exp\{i\frac{2\pi}{q}\,a\,c\}|c\rangle|x^a(\mathrm{mod}N)\rangle\,,$$

and

$$\begin{aligned}\langle\mathcal{S}'|\mathcal{S}'\rangle &= \frac{1}{3^{2l}}\frac{1}{q^2}\sum_{b,b',\,a,a',c,c'=0}^{q-1} h(b,c)h(b',c')e^{i\frac{2\pi}{q}\,[b\,(b+c-a)-b'\,(b'+c'-a')]}\delta_{aa'}\delta_{cc'} \\ &= \frac{1}{3^{2l}}\frac{1}{q^2}\sum_{b,b',\,a,c=0}^{q-1} h(b,c)h(b',c)e^{i\frac{2\pi}{q}\,[(c-a)\,(b-b')+b^2-b'^2]} \\ &\neq 1\,,\end{aligned} \tag{III.37}$$

---

[3]The ϕ-integrations give $q\pi^l$, while each of the r-integrals is of the form

$$\int_0^\infty \frac{r_i dr_i}{(1+r_i^2)^4} r_i^{2(b_i+c_i)}\,,$$

which is equal to 1/6 for $b_i = c_i$, or to 1/12 for $b_i \neq \hat{c}_i$.

[4]The value 1 is obtained when *none* of the bits of b is equal to the corresponding bit of c, the value 2 is obtained when *only one* of the bits of b is equal to the corresponding bit of c, and so forth, up to the value 2^l which is obtained only when *all* the bits are equal, i.e. when $b = c$.

while $\langle s'|s'\rangle = 1$. To evaluate an upper bound B for $\langle \mathcal{S}'|\mathcal{S}'\rangle$ we set all the phases to zero, and notice that $h(x,y)$ can also be written as[5]

$$h(x,y) \in \{2^{l-n} : n \in \{0,1,...,l\}\}\,, \tag{III.39}$$

where n is the number of bits of x that *differ* from the corresponding bits of y

$$\begin{aligned}\langle \mathcal{S}'|\mathcal{S}'\rangle \leq B &= \frac{1}{3^{2l}}\frac{1}{q^2}\sum_{a=0}^{q-1}\sum_{b,b',c=0}^{q-1} h(b,c)h(b',c) = \frac{q}{3^{2l}}\left(\sum_{n=0}^{l}\binom{l}{n}2^{-n}\right)^2 \\ &= \frac{q}{3^{2l}}\left((1+2^{-1})^l\right)^2 = \frac{1}{q}\,. \end{aligned} \tag{III.40}$$

IV. SUCCESS PROBABILITY OF THE SEMICLASSICAL ALGORITHM

To test the efficiency of our approximation we compute the probability $\mathcal{P}(\hat{c}, x^k(\mathrm{mod}N)) \equiv |\langle \hat{c}, x^k(\mathrm{mod}N)|\mathcal{S}'\rangle|^2$. From the expression (III.32) for $|\mathcal{S}'\rangle$ we have

$$\mathcal{P}(\hat{c}, x^k(\mathrm{mod}N)) = \left|\frac{1}{\pi^l}\sum_{a=0}^{q-1}\left(\sum_{b,d=0}^{q-1} e^{2\pi i\frac{b\cdot d}{q}}\mathcal{I}_{a\hat{c}bd}\right)\right|^2_{a=k(\mathrm{mod}L)}\,, \tag{IV.1}$$

where, as in Eq. (II.18), $a = k(\mathrm{mod}L)$ can be written as $a = k + fL$, with integer f. From the results of the previous Section this probability is nonzero if and only if $d_i = \hat{c}_i + b_i - a_i$, $\forall i = 0,...,l-1$. Hence, using Eq. (III.36)

$$\mathcal{P}(\hat{c}, x^k(\mathrm{mod}N)) = \frac{1}{q^2 3^{2l}}\left|\sum_{f=0}^{[\frac{q-k-1}{L}]}\sum_{b,d=0}^{q-1} h(b,\hat{c})e^{i\frac{2\pi}{q}bd}\delta_{d,\,\hat{c}+b-k-fL}\right|^2 \tag{IV.2}$$

$$= \frac{1}{q^2 3^{2l}}\left|\sum_{b=0}^{q-1} h(b,\hat{c})e^{-i\frac{2\pi}{q}b(\hat{c}+b-k)}\sum_{f=0}^{[\frac{q-k-1}{L}]} e^{i\frac{2\pi}{q}fbL}\right|^2\,. \tag{IV.3}$$

Comparing it with Shor's expression (II.18)

$$\mathbf{P}(\hat{c}, x^k(\mathrm{mod}N)) = \frac{1}{q^2}\left|\sum_{f=0}^{[\frac{q-k-1}{L}]} e^{i\frac{2\pi}{q}f\{L\hat{c}\}_q}\right|^2\,,$$

---

[5]To rewrite the sums over b, b' in (III.37) as sums over n, m notice that the number of terms is the same: b takes 2^l values $(0,1,2,...,2^l-1)$, and

$$\sum_{n=0}^{l}\binom{l}{n} = 2^l\,, \tag{III.38}$$

where the combinatorial factor tells us how many terms in the sum over b differ by l bits from c.

we see the supplementary overall factor $1/3^{2l}$ and sum over b. Each term in the sum over f is now modulated by $\sum_b h(b,\hat{c})\exp\{2\pi i b(\hat{c}+b-k)/q\}$.
We could expect that the peaks would now be spread over such a wider range of values of $\hat{c}$ that the period-finding power of the algorithm would be badly spoiled. But two features come in hand: i) the coefficients $h^2(b,\hat{c})$ tend to zero for large n, i.e. for b very different from $\hat{c}$; ii) by construction (see Section II, and [1], [2]) the $\sum_f$ in (IV.3) works like a "filter" of the values of b, being a maximum at $b=\hat{c}$ and falling down to zero otherwise. The combination of these two phenomena has the pleasant effect of maximizing $\mathcal{P}$ around the same values of $\hat{c}$ where $\mathbf{P}$ is maximum, i.e. the values that solve the factorization problem in the first place. The leading contribution to $\mathcal{P}$ is then[6]

$$\mathcal{P} \sim \frac{1}{3^{2l}}\frac{1}{q^2}h^2(\hat{c},\hat{c})\left|\sum_{f=0}^{[\frac{q-k-1}{L}]} e^{i\frac{2\pi}{q}f\{L\hat{c}\}_q}\right|^2 = \frac{1}{3^{2l}}\left|\sum_{f=0}^{[\frac{q-k-1}{L}]} e^{i\frac{2\pi}{q}f\{L\hat{c}\}_q}\right|^2 \ . \tag{IV.5}$$

Thus the semiclassical approximation leaves the algorithm very efficient at spotting the required periodicity L (which is the main task of the algorithm): L is determined as before from the maximizing condition in (II.20)

$$\left|\frac{\hat{c}}{q}-\frac{d}{L}\right| < \frac{1}{2q} \ ,$$

for some integer d.
Our plots of the semiclassical probability in (IV.3), obtained for $\langle\mathcal{S}'|\mathcal{S}'\rangle^{-1}\mathcal{P}$ and $10^{-1}\mathbf{P}$, confirm this result. For instance, the plots for $q=256$ could be regarded as the actual spotting of the periods $L=10$, and $L=16$ for the factorization of $N=33$ (taking $x=5$), and $N=51$ (taking $x=2$), respectively. To appreciate the k dependence see Figs. 3, 4, and 5.
From our plots, see for instance Figs. 3, 6, and 7, we also see, for $k=1$,

$$\langle\mathcal{S}'|\mathcal{S}'\rangle^{-1}\mathcal{P} \sim 5\times 10^{-2}\,\mathbf{P} \ . \tag{IV.6}$$

This confirms, from yet another perspective, that the values where $\mathcal{P}$ has a maximum are not too widely spread around the corresponding Shor's values.
The last question left to answer concerns the behaviour of the success probability $\mathcal{P}$ for large l. Two things are important: i) the ratio $R_1(l)\equiv\mathcal{P}/\mathbf{P}$; ii) the ratio $R_2\equiv\mathcal{P}_{\max}/\mathcal{P}_{\min}$.

---

[6]One might also move away from the leading term, and consider more contributions from the sum over b, "coarse graining" the $\hat{c}$-axis by summing up all the contributions to $\mathcal{P}$ from the interval $\hat{c}\pm\Delta\hat{c}$. For instance, choosing $\Delta\hat{c}=1$ amounts to consider also the bs differing by 1 bit ($n=1$). In this case

$$\mathcal{P} \sim (1+l/4+l/2)\frac{1}{3^{2l}}\left|\sum_{f=0}^{[\frac{q-k-1}{L}]} e^{i\frac{2\pi}{q}f\{L\hat{c}\}_q}\right|^2 \ . \tag{IV.4}$$

The first tells us how smaller than Shor's the semiclassical probabilities get, and it is easy to compute

$$R_1(l) = \frac{\mathcal{P}}{\mathbf{P}} \sim \left(\frac{2}{3}\right)^{2l} \sim 10^{-(2/5)l} \ . \tag{IV.7}$$

For large l the magnitude of the semiclassical probabilities exponentially falls off. The second ratio is independent from l and, as proved in the earlier discussion, nearly as big as Shor's

$$R_2 = \frac{\mathcal{P}_{\max}}{\mathcal{P}_{\min}} \sim \frac{\mathbf{P}_{\max}}{\mathbf{P}_{\min}} \ . \tag{IV.8}$$

This seems to us quite encouraging, as we might conclude that, despite the fact that the actual value of the semiclassical probability $\mathcal{P}$ scales exponentially with l, the semiclassical "signal-to-noise" ratio R_2 is nearly as good as the quantum one.
In Appendix B we present an alternative method to study the scaling properties of $\mathcal{P}$.

V. CONCLUSIONS

We have invented a semiclassical version of Shor's quantum factoring algorithm based on SU(2) generalized coherent states, and we have investigated its impact on the algorithm's efficiency.
The coherent states $|\lambda\rangle$ for the spin-1/2 systems are the superpositions $|-1/2\rangle + \lambda|+1/2\rangle$, where the complex variables λ have a classical interpretation. Under this interpretation, a classical phase-space for λ can be constructed by a well known procedure. This clarifies in which sense the quantum evolution, necessary for the implementation of the algorithm, could be, in principle, mimicked in a classical fashion.
We expressed the Quantum Fourier Transform (the essential part of Shor's algorithm) by a coherent state diagonal representation, where the variables introduced have the aforementioned classical interpretation, although the operation itself is still quantum.
This representation does not lead to a loss of information. It is only after integration over the classical variables that some information is lost, and an approximation is made. Our analytic and numerical results show that this semiclassical step is very effective at spotting the required periodicity: despite the fact that the actual value of the semiclassical success probability decreases exponentially with l, the semiclassical "signal-to-noise" ratio is nearly as good as Shor's. In other words, our semiclassical procedure preserves most of the power of the quantum algorithm.
Finally, with the above results in hand, we are confident that future searches along this line, for the implementation of Shor's factoring algorithm on semiclassical devices, could lead to important new discoveries.

ACKNOWLEDGMENTS

We acknowledge the positive criticism of the referees. A.I. thanks Andrew Landahl for a useful proofreading of the manuscript, and the Dublin Institute for Advanced Studies for

their warm hospitality. P.G., A.I. and Siddhartha S. are grateful to Giuseppe Vitiello for his interest and enjoyable discussions, and thank the Department of Physics "E.R. Caianiello", University of Salerno, for hosting them while an ancestor of this paper was conceived.
This work is supported in part by funds provided by the U.S. Department of Energy (D.O.E.) under cooperative research agreement DF-FC02-94ER40818.

APPENDIX A

INFORMATION PRESERVATION

We show here, in full generality, that $\mathcal{M}^\lambda$ has the same information as $\mathcal{M}$. This is seen from the fact that one can reconstruct the original information contained in any $q \times q$ matrix $\mathcal{M}$ acting on the Hilbert space $\mathcal{H} = \bigotimes_{i=0}^{l-1} \mathcal{H}_2^i$ in the following way. In notation (ii)

$$\mathcal{M} = \sum_{n,m=0}^{q-1} M_{nm} |n\rangle\langle m| \,, \tag{A.1}$$

where $|n\rangle = |n_{l-1}, ..., n_0\rangle$, $\langle m| = \langle m_{l-1}, ..., m_0|$, n labels the rows, m the columns, and $n_i, m_j \in \{0, 1\}$. Thus

$$\begin{aligned} \mathcal{M}^\lambda &= \sum_{n,m=0}^{q-1} M_{nm} \langle\lambda|n\rangle\langle m|\lambda\rangle \\ &= \Lambda_{0,...,l-1} \sum_{n,m=0}^{q-1} M_{nm} (\bar{\lambda}_{l-1}^{n_{l-1}} \cdots \bar{\lambda}_0^{n_0})(\lambda_{l-1}^{m_{l-1}} \cdots \lambda_0^{m_0}) \,, \end{aligned} \tag{A.2}$$

where $\Lambda_{0,...,l-1} \equiv \prod_{i=0}^{l-1} (1 + |\lambda_i|^2)^{-1}$, and our statement is proved.
All one has to do is to keep track of the powers of the λs and $\bar{\lambda}$s, in the given order, and no information is lost. This feature is due to the fact that λ is a complex number, hence the dimension of the space of parameters is equal to the dimension of the original Hilbert space $\mathcal{H}$. Furthermore, there is a one-to-one correspondence with the binary numbers and the powers of $(\bar{\lambda}_{l-1}^{n_{l-1}} \cdots \bar{\lambda}_0^{n_0})(\lambda_{l-1}^{m_{l-1}} \cdots \lambda_0^{m_0})$, with $n_i, m_j \in \{0, 1\}$. Let us stress again that no *quantum* information is lost, but the $\mathcal{M}^\lambda$s are functions of *classical* variables. As a simple example let us consider Φ^λ for the case $l = 2$

$$\begin{aligned} \Phi^\lambda = \frac{1}{2}&[(1 + |\lambda_1|^2)(1 + |\lambda_0|^2)]^{-1} \\ &(1 + \lambda_0 + \lambda_1 + \lambda_1\lambda_0 \\ &+\bar{\lambda}_0 - \lambda_0\bar{\lambda}_0 + \lambda_1\bar{\lambda}_0 - \lambda_1\lambda_0\bar{\lambda}_0 \\ &+\bar{\lambda}_1 + \beta\lambda_0\bar{\lambda}_1 - \lambda_1\bar{\lambda}_1 - \beta\bar{\lambda}_1\lambda_1\lambda_0 \\ &+\bar{\lambda}_1\bar{\lambda}_0 - \beta\lambda_0\bar{\lambda}_1\bar{\lambda}_0 - \lambda_1\bar{\lambda}_1\bar{\lambda}_0 + \beta\lambda_1\bar{\lambda}_1\lambda_0\bar{\lambda}_0) \,, \end{aligned} \tag{A.3}$$

where $\beta = \exp\{i\pi/2\}$, and the original matrix $\Phi = R_0 S_{0,1} R_1$ is easily reconstructed as

$$\Phi^{\lambda} \to \frac{1}{2}[(1+|\lambda_1|^2)(1+|\lambda_0|^2)]^{-1} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & \beta & -1 & -\beta \\ 1 & -\beta & -1 & \beta \end{pmatrix}, \tag{A.4}$$

where, as explained in detail in the general case, the powers of $\bar{\lambda}$ label the rows, the powers of λ label the columns, and we used notation (iii) for the 4×4 matrix[7]. This matrix differs from Φ only in the overall factor $[(1+|\lambda_1|^2)(1+|\lambda_0|^2)]^{-1}$, but the trace is left invariant

$$\mathrm{Tr}\Phi = \frac{(\beta-1)}{2} = \int d\mu(\lambda)\Phi^{\lambda}\,. \tag{A.5}$$

Trace-preservation, $\mathrm{Tr}\Phi = \int d\mu(\lambda)\Phi^{\lambda}$, is a general property of some importance as a check on the correctness of our normalizations, which are used in the computation of the semiclassical efficiency.

APPENDIX B

MORE ON THE SCALING OF THE SUCCESS PROBABILITY

We want to give here an alternative approach to study the scaling behaviour of the semiclassical success probability in Eq. (IV.3). Write

$$b = \hat{c} + (b - \hat{c}) = \hat{c} + \sum_{p=0}^{l-1} (b_p - \hat{c}_p) 2^p\,, \tag{B.1}$$

where $(b_p - \hat{c}_p) = 0, \pm 1$. Thus, using the rewriting explained earlier in the footnote with Eq.(III.38), the structure of the sum over b becomes

$$\sum_{b=0}^{2^l-1} e^{ibA} = e^{i\hat{c}A} \sum_{n=0}^{l} \left[1 + \underbrace{(e^{\pm i2^0 A} + e^{\pm i2^1 A} + \cdots + e^{\pm i2^{l-1} A})}_{l = \binom{l}{1}\text{terms}} + \binom{l}{2}\text{terms} + \cdots \right], \tag{B.2}$$

for the given A. We can approximate this expression by taking only one "effective" phase term for each n, say $\gamma(n)$ (for instance $\gamma(n=0)=0$ is exact). Eventually, the sum over b can be approximated as

---

[7]The $1 \times q$ or $q \times 1$ *vectors* in notation (iii) are, of course, obtained from the tensor product of the basis vectors of the two-state Hilbert spaces $\mathcal{H}_2^i$, and follow the convention: $(1,0,0,...,0) \equiv 0$, $(0,1,0,...,0) \equiv 1$, $(0,0,1,...,0) \equiv 2$, ..., $(0,0,0,...,1) \equiv q-1$, for the $1 \times q$ row-vectors, and similarly for the $q \times 1$ column-vectors.

$$\sum_{b=0}^{2^l-1} e^{bA} \sim e^{\hat{c}A} \sum_{n=0}^{l} \left(\begin{array}{c} l \\ n \end{array} \right) e^{\gamma(n)A} \,. \tag{B.3}$$

The probability (IV.3) then reads

$$\begin{aligned} \mathcal{P}(\hat{c}, x^k (\mathrm{mod} N)) &= \left| \frac{1}{q3^l} \sum_{b=0}^{q-1} h(b,\hat{c}) e^{2\pi i \frac{b\cdot(\hat{c}-k+b)}{q}} \sum_{f=0}^{[\frac{q-k-1}{L}]} e^{-2\pi i f \frac{b\cdot L}{q}} \right|^2 \\ &\sim \left| \frac{1}{q3^l} (e^{2\pi i \frac{\hat{c}\cdot(2\hat{c}-k)}{q}}) \sum_{f=0}^{[\frac{q-k-1}{L}]} e^{-2\pi i f \frac{\hat{c}\cdot L}{q}} \sum_{n=0}^{l} \left(\begin{array}{c} l \\ n \end{array} \right) 2^{l-n} e^{2\pi i \frac{\gamma(n)\cdot(\gamma(n)+\hat{c}-k-fL)}{q}} \right|^2 \\ &\equiv \left| \frac{1}{q3^l} \sum_{f=0}^{[\frac{q-k-1}{L}]} e^{-2\pi i f \frac{\hat{c}\cdot L}{q}} \sum_{n=0}^{l} \left(\begin{array}{c} l \\ n \end{array} \right) 2^{l-n} e^{iz(n,f)} \right|^2 , \end{aligned} \tag{B.4}$$

where

$$z(n,f) \equiv \frac{2\pi}{q} \cdot \gamma(n)(\gamma(n) + \hat{c} - k - fL) \,. \tag{B.5}$$

The actual behaviour of $z(n,f)$ is quite complicated, and it deserves farther study. What we intend to do here, instead, is to show that a rough approximation already gives indications on the scaling behaviour of $\mathcal{P}$. To this end we take $z(n,f) \sim n\hat{z}$, with $\hat{z}$ constant

$$\mathcal{P} \sim \left| \frac{(2+e^{i\hat{z}})^l}{q3^l} \sum_{f=0}^{[\frac{q-k-1}{L}]} e^{-2\pi i f \frac{\hat{c}\cdot L}{q}} \right|^2 \sim \tilde{h}(\hat{z},l) \left| \frac{1}{q} \sum_{f=0}^{[\frac{q-k-1}{L}]} e^{2\pi i f \frac{\{\hat{c}\cdot L\}_q}{q}} \right|^2 , \tag{B.6}$$

which is Shor's probability with a different oscillating overall factor

$$\tilde{h}(\hat{z},l) \equiv 9^{-l}(|2+e^{i\hat{z}}|^2)^l = 9^{-l}(5+4\cos\hat{z})^l \,. \tag{B.7}$$

The difficult problem is to find the right constant $\hat{z}$ to suitably approximate $z(n,f)$. Let us study the behaviour of the function $\tilde{h}(\hat{z},l)$. This symmetric ($\tilde{h}(-\hat{z},l) = \tilde{h}(\hat{z},l)$), periodic ($\tilde{h}(\hat{z}+2m\pi,l) = \tilde{h}(\hat{z},l)$), bounded ($\tilde{h}(\hat{z},l) \in [9^{-l},1]$) function, in the range $\hat{z} \in [-\pi,\pi]$, reaches its maximum at $\hat{z}=0$, and its minima at $\hat{z} = \pm\pi$. If ζ is such that $\tilde{h}(\zeta,l) = \frac{1}{2}\,\tilde{h}_{\max} = \frac{1}{2}$, we find that $\zeta(l) = \arccos[\frac{1}{4}(\frac{9}{2^{1/l}} - 5)] \to 0$ very rapidly as l increases. Thus, for big l, $\tilde{h}(\hat{z},l)$ is zero everywhere, except at $\hat{z}=0$, where it is 1.

REFERENCES

[1] P. Shor, Proceedings of the 35$^{\text{th}}$ Annual Symposium of the Foundations of Computer Science, IEEE Press (1994).

[2] P. Shor, SIAM J. Sci. Statist. Comput. **26** (1997) 1484; and *Introduction to Quantum Algorithms*, quant-ph/0005003 (July 2001).

[3] Yu. Manin, Sovetskoye Radio, Moscow (1980);
R.P. Feynman, Int. J. Theo. Phys. **21** (1982) 467.

[4] Yu. Manin, *Classical Computing, Quantum Computing, and Shor's Factoring Algorithm*, Talk at the Bourbaki Seminar (June 1999), quant-ph/9903008.

[5] R.P. Feynman, Found. Phys. **16** (1986) 507.

[6] A.K. Lenstra, H.W. Lenstra Jr., Eds., The Development of the Number Field Sieve, Spinger Verlag (Berlin) 1993.

[7] I.V. Volovic, *Quantum Computing and Shor's Factoring Algorithm*, Lectures at the Volterra-CIRM International School "Quantum Computer and Quantum Information", Trento - Italy (July 2001), quant-ph/0109004.

[8] Proceedings of the III International Workshop on "Macroscopic Quantum Coherence and Computing", Istituto di Studi Filosofici di Napoli, 3-7 June 2002 (unpublished). Abstracts available at the URL: http://www.mqc2.it/mqc2002.

[9] L.M.K. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood, I.L. Chuang, Nature **414** (2001) 883.

[10] D.J. Wineland, M. Barrett, J. Britton, J. Chiaverini, B. De Marco, W.M. Itano, B. Jelenkovic, C. Langer, D. Leibfried, V. Meyer, T. Rosenband, T. Schaetz, *Quantum Information Processing with Trapped Ions*, Proceedings of the Discussion Meeting on Practical Realizations of Quantum Informations Processing, Royal Society, Nov.13-14 2002.

[11] R.B. Griffiths, C.-S. Niu, Phys. Rev. Lett. **76** (1996) 3228.

[12] P.A.M. Dirac, The Principles of Quantum Mechanics, Clarendon Press (Oxford) 1958.

[13] M. Rasetti, E. Tagliati, R. Zecchina, Phys. Rev. **A 55** (1997) 2594.

[14] A. Perelomov, Generalized Coherent States, Springer-Verlag (Berlin) 1986.

[15] M. Nakahara, Geometry, Topology and Physics, Adam Hilger (Bristol) 1990;
C. Nash, S. Sen, Topology and Geometry for Physicists, Academic Press (London) 1983;
Y. Choquet-Bruhat, C. DeWitt-Morette, Analysis, Manifolds, and Physics, North Holland (Amsterdam - New York - Oxford) 1982.

Plots

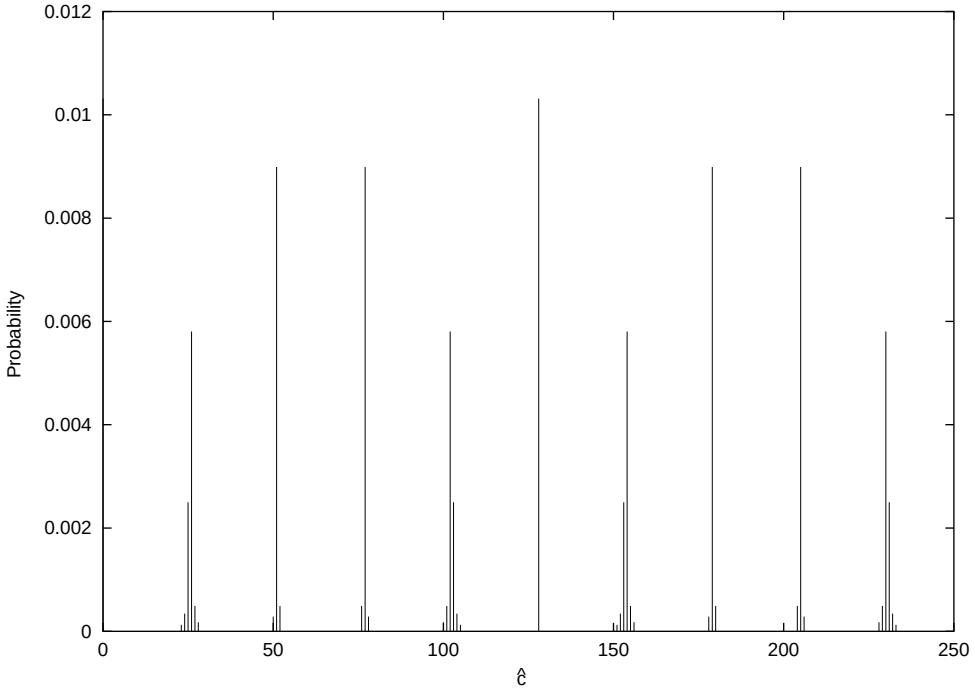

Figure 1: Shor Probability for $q = 256$, $L = 10$.

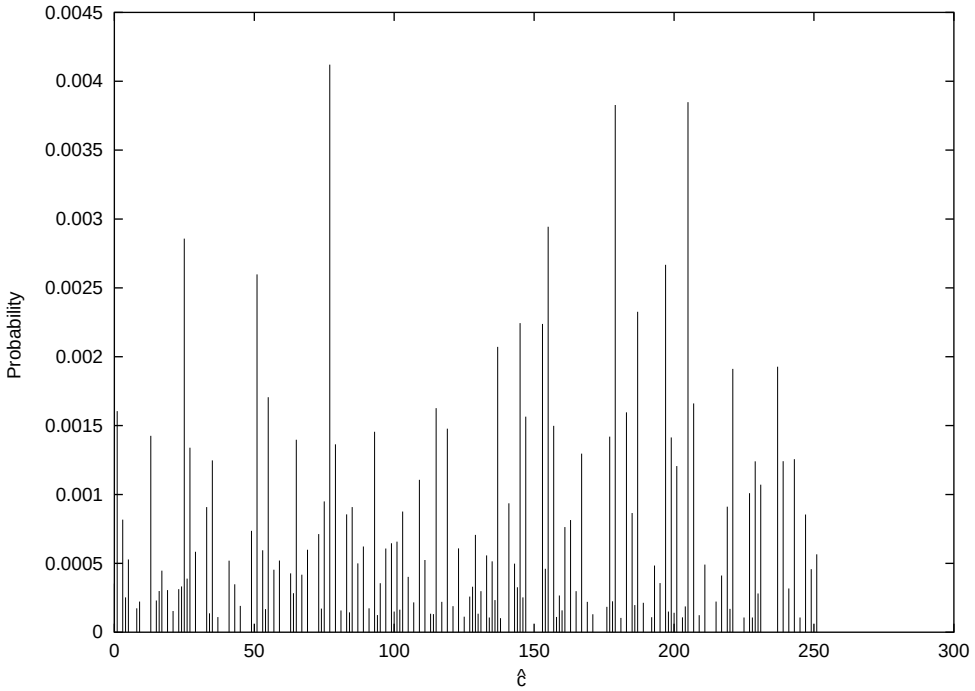

Figure 2: Semiclassical Probability for $q = 256$, $L = 10$, $k = 1$.

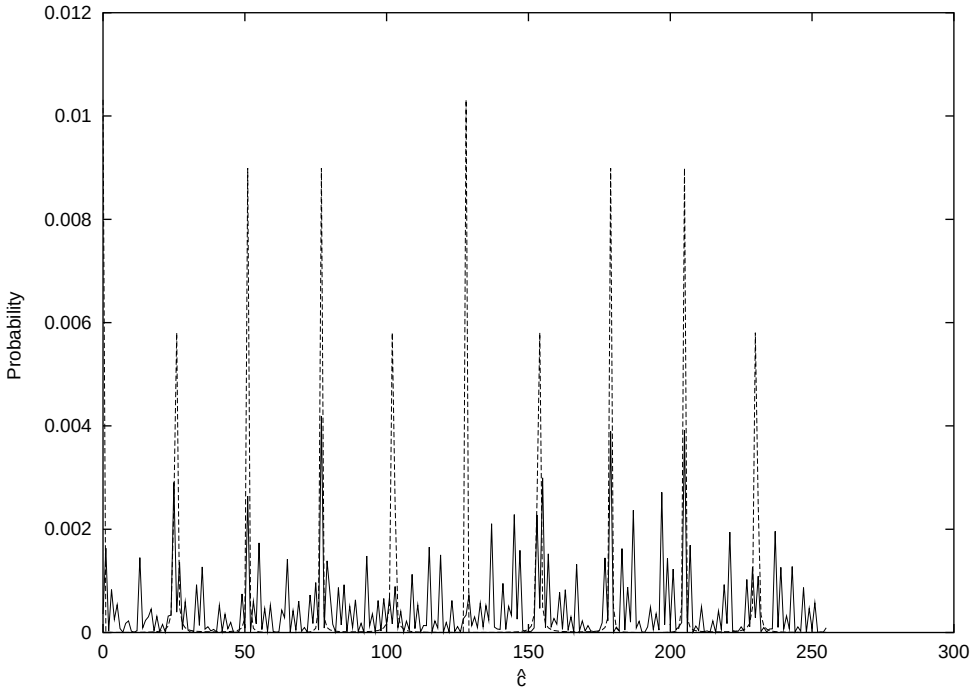

Figure 3: Shor (dashed lines) and Semiclassical (full lines) Probabilities for $q = 256$, $L = 10$, and $q = 256$, $L = 10$, $k = 1$, respectively. For the Shor Probability the plotted values are a factor of 10 smaller than the actual values.

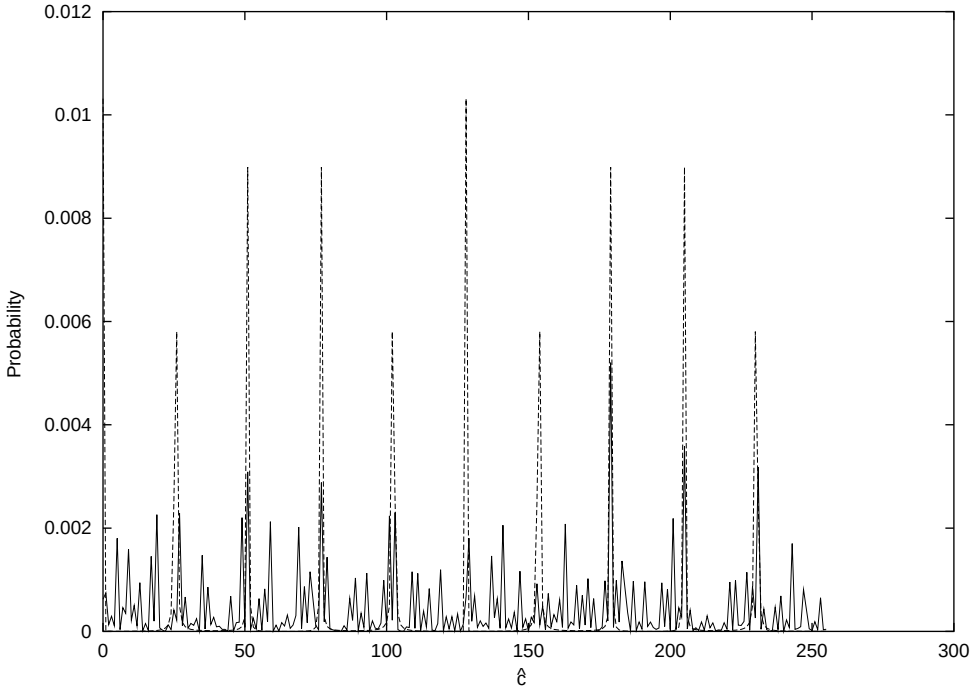

Figure 4: Shor (dashed lines) and Semiclassical (full lines) Probabilities for $q = 256$, $L = 10$, and $q = 256$, $L = 10$, $k = 5$, respectively. For the Shor Probability the plotted values are a factor of 10 smaller than the actual values.

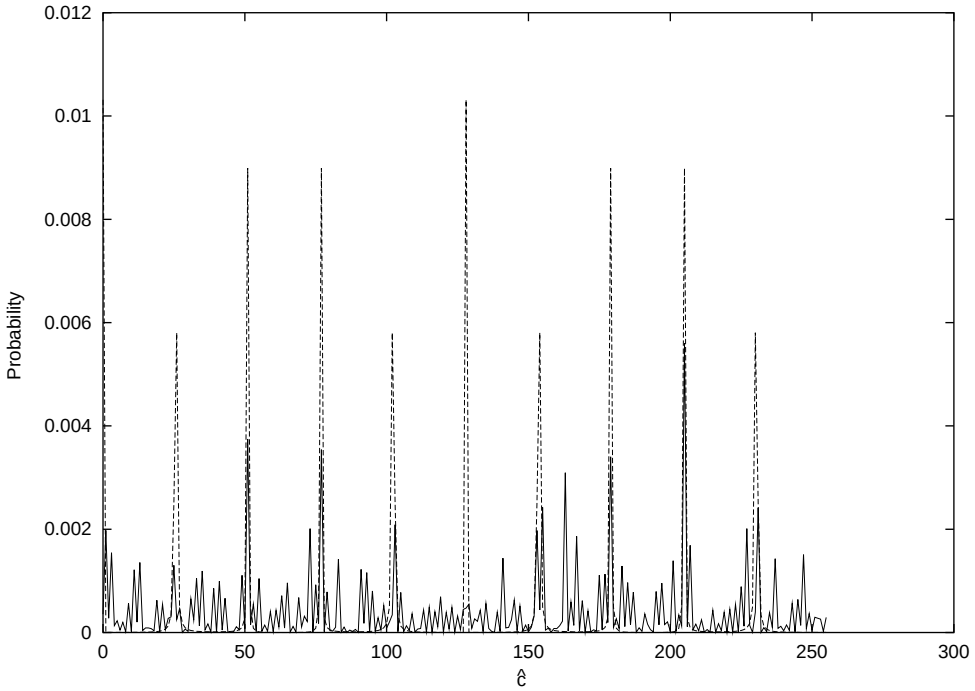

Figure 5: Shor (dashed lines) and Semiclassical (full lines) Probabilities for $q = 256$, $L = 10$, and $q = 256$, $L = 10$, $k = 9$, respectively. For the Shor Probability the plotted values are a factor of 10 smaller than the actual values.

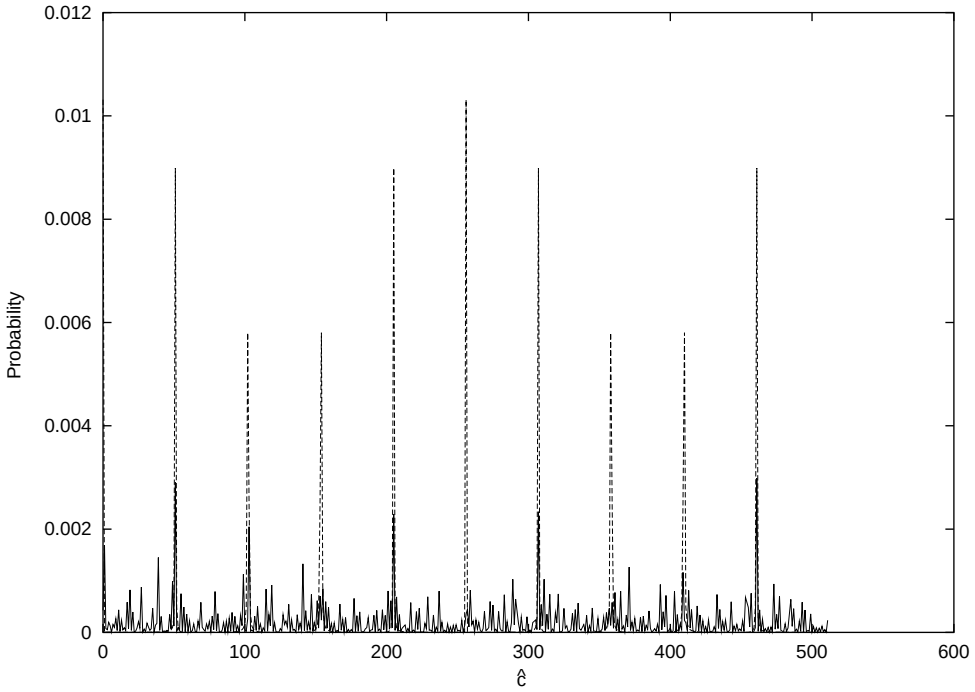

Figure 6: Shor (dashed lines) and Semiclassical (full lines) Probabilities for $q = 512$, $L = 10$, and $q = 512$, $L = 10$, $k = 1$, respectively. For the Shor Probability the plotted values are a factor of 10 smaller than the actual values.

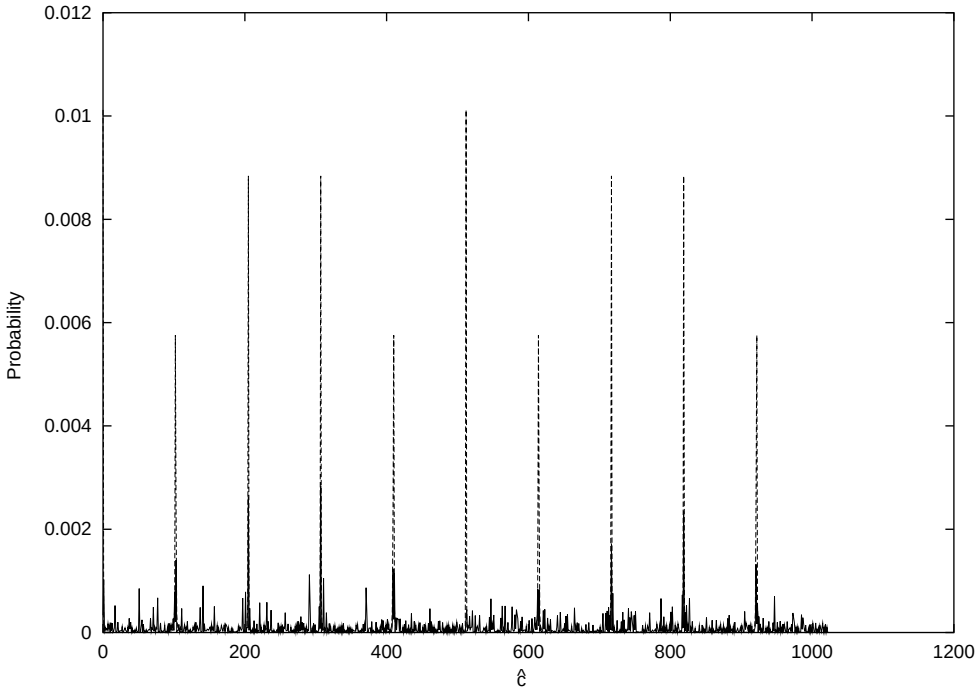

Figure 7: Shor (dashed lines) and Semiclassical (full lines) Probabilities for $q = 1024$, $L = 10$, and $q = 1024$, $L = 10$, $k = 1$, respectively. For the Shor Probability the plotted values are a factor of 10 smaller than the actual values.

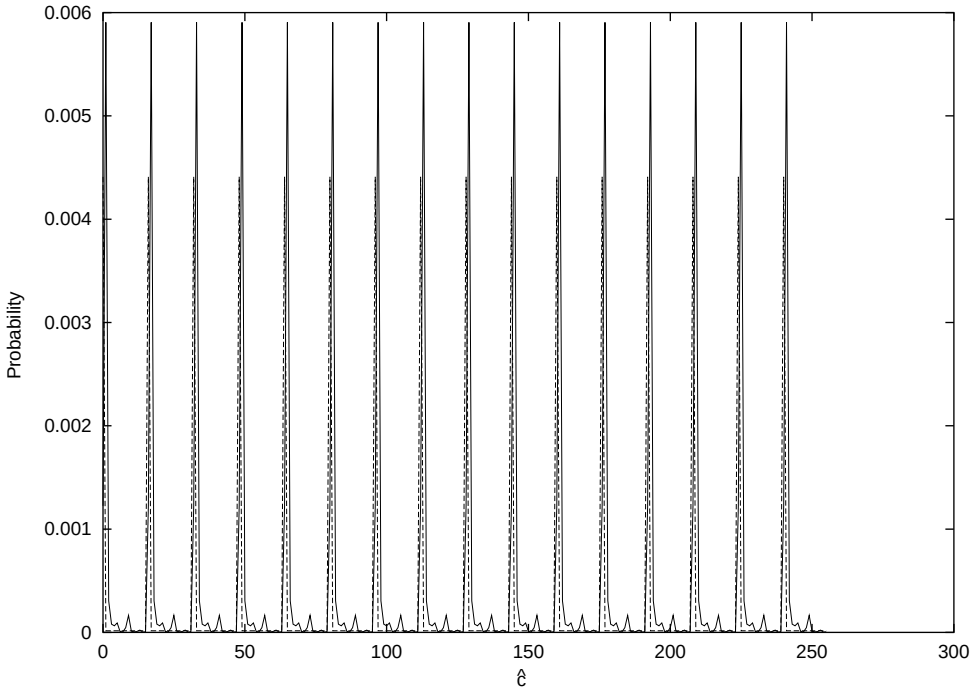

Figure 8: Shor (dashed lines) and Semiclassical (full lines) Probabilities for $q = 256$, $L = 16$, and $q = 256$, $L = 16$, $k = 1$, respectively. For the Shor Probability the plotted values are a factor of 10 smaller than the actual values.

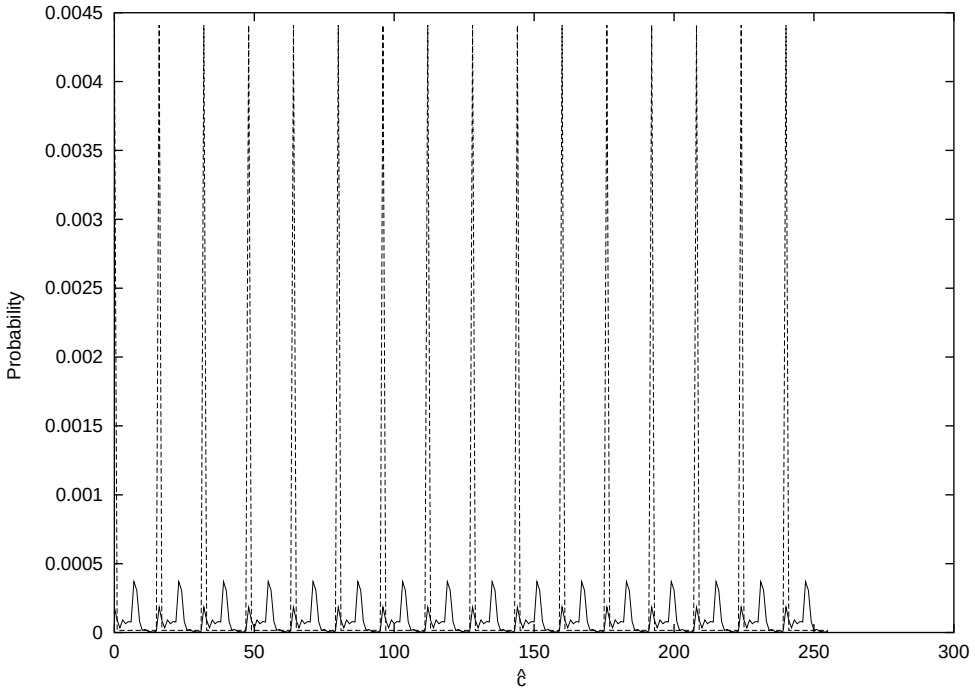

Figure 9: Shor (dashed lines) and Semiclassical (full lines) Probabilities for $q = 256$, $L = 16$, and $q = 256$, $L = 16$, $k = 7$, respectively. For the Shor Probability the plotted values are a factor of 10 smaller than the actual values.

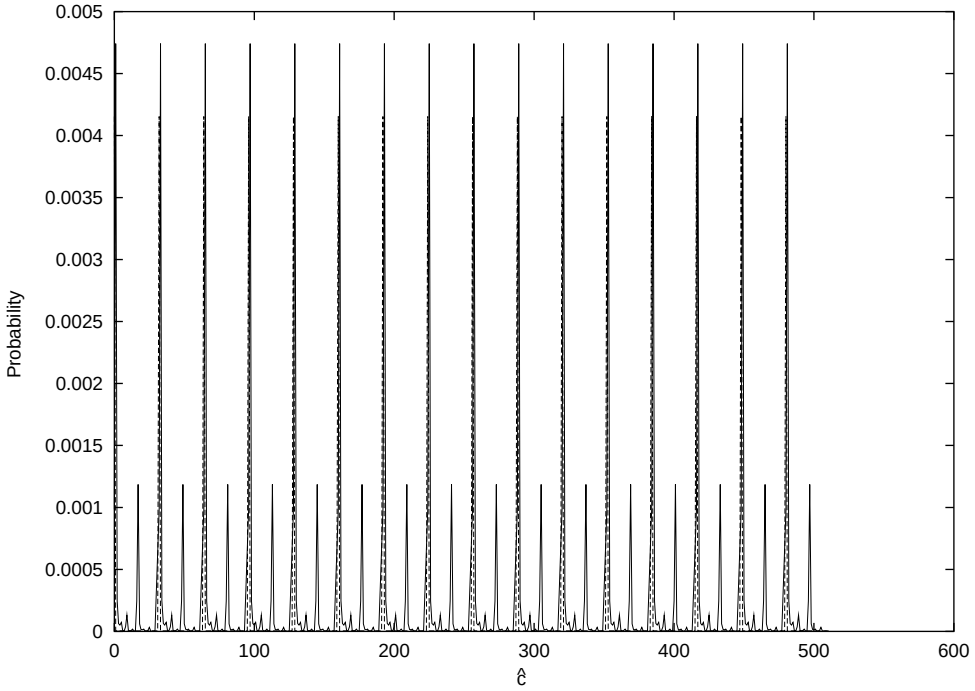

Figure 10: Shor (dashed lines) and Semiclassical (full lines) Probabilities for $q = 512$, $L = 16$, and $q = 512$, $L = 16$, $k = 1$, respectively. For the Shor Probability the plotted values are a factor of 10 smaller than the actual values.