COMPLEXITY CONSIDERATIONS QUANTUM COMPUTATION

Article · January 2013

DOI: 10.1142/9789814460026_0001

1 author:

Luigi Accardi
University of Rome Tor Vergata
573 PUBLICATIONS **6,306** CITATIONS

SEE PROFILE

Quantum Bio-Informatics V

pp. 1–13

COMPLEXITY CONSIDERATIONS QUANTUM COMPUTATION

LUIGI ACCARDI

Centro Vito Volterra,
Università degli Studi di Roma "Tor Vergata", Roma, Italy,
E-mail: accardi@volterra.uniroma2.it

It is usually calimed that quantum computer can outperform classical computer. Is this statement true? We discuss this issue, not in general, but in the context of the most famous algorithm of quantum computation: Shor's algorithm.

1. Introduction

Shor's algorithm is supposed to achieve integer factorization faster than classical algorithms. In order to discuss this issue we shortly review Shor's algorithm and the strictly related Simon's period-finding algorithm (see section (2)). Then we argue that, since quantum computer is an analogical machine, the complexity estimates on quantum algorithms should involve the analysis of the concrete implementation of the operations whose use is required by these algorithms. An outline of this analysis is done in section (3).

Finally, in order to compare the performance of Shor's algorithm with some classical probabilistic factorization algorithms, the latter ones are shortly reviewed in section (4).

The essence of the factorization problem can be described as follows:

Given a natural integer $N = pq$, which is the product of two primes $p \neq q$, find p and q. If p and q are large and satisfy additional diophantine conditions, the problem is hard and this difficulty has been exploited by a famous cryptographic algorithm.

A classical argument of number theory reduces the factorization problem to the problem of finding the period of the function $a \mapsto y^a \pmod N$ (see section (4)).

At the moment there is no classical algorithm that can find the period of the function $a \mapsto y^a \pmod N$ (hence the factorization problem) in a num-

ber of steps of order $O(\log N)$
It was however known a classical probabilistic algorithm that achieves this goal, not exactly, but with probability of order $O(1/\log N)$.
D. Simon [Sim94] proposed a quantum algorithm that allows to find, using $O(\log N)$ operations and with probability of order $O(1/\log N)$, the period of an arbitrary function $f : \{0, \ldots, N-1\} \to \{0, \ldots, N-1\}$ each value of which can be calculated with an algorithm of complexity of order $O(\log N)$ (with respect to some standard measure of complexity).
P. W. Shor [Sho94a] applied Simon's period finding algorithm to the function $a \mapsto y^a \pmod N$ to construct a quantum factorization algorithm which needs a number of steps of the same order of magnitude as the classical probabilistic algorithm and achieves the same result with a probability of the same order of magnitude.

Contrarily to the classical probabilistic algorithm, Simon's (hence Shor's) algorithm is based on additional physical assumptions the experimental verification of some of which is at the moment not available.
The goal of the present note is to point out some of these assumptions.
Some of the considerations in the present notes are contained in the unpublished lectures of the author at the Volterra-CIRM International School "Quantum Computer and Quantum Information", Trento, July 25-31, 2001.

2. Simon's period-finding quantum algorithm

Given $N \in \mathbb{N}$ let $f : \{0, 1, \ldots, N-1\} \to \{0, 1, \ldots, N-1\}$ be a periodic function with period r, i.e. r is the smallest number in the domain of f such that

$$f(x) = f(x +_N r) \qquad ; \qquad \forall x \in \{0, 1, \ldots, N-1\} \tag{1}$$

where the symbol $+_N$ denotes addition modulo N.
Since addition is taken modulo N, if (1) is satisfied by r, then it is also satisfied by $N - r$. Thus by definition of period, one must have

$$r \leq N - r \Leftrightarrow r \leq N/2$$

Suppose that we know that f is an efficiently computable function, i.e. that, for each x, $f(x)$ can be efficiently computed (i.e. in a number of steps which is polynomial in the number of digits of x).
If these are the only informations on f, the only way to find exactly the period is to carry out an exhaustive search. This requires to calculate $f(x)$ for a set of x of cardinality $N/2$. This algorithm is exponential in the

number of bits required to specify N, which is of order $\log N$.
In absence of exact results one turns to probabilistic algorithms, either classical or quantum.
As we have seen the performances of the two are essentially the same.

2.1. *Ingredients of Simon's quantum period finding algorithm (QPFA)*

The state space of this algorithm is

$$\mathcal{H}^{2^n} \otimes \mathcal{H}^{2^n} \equiv (\mathbb{C}^2)^{\otimes n} \otimes (\mathbb{C}^2)^{\otimes n} \tag{2}$$

where $\mathcal{H} := \mathbb{C}^2$ is the so–called q–bit space (the reason why, in (2), one uses two copies of the space $\mathcal{H}^{2^n}$ is explained in Step (3) of the algorithm described in section (2.2)).
In the space $\mathbb{C}^2$ we fix the *computational basis*,

$$|0\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad ; \qquad |1\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

which induces the basis (still called computational) in $(\mathbb{C}^2)^{\otimes n}$

$$|\varepsilon_1\rangle \otimes \cdots \otimes |\varepsilon_n\rangle =: |\varepsilon_1, \ldots, \varepsilon_n\rangle \quad ; \ \varepsilon_j \in \{0,1\} \tag{3}$$

Identifying the binary string $(\varepsilon_1, \ldots, \varepsilon_n)$ to the binary expansion of a natural integer through the formula

$$x = \sum_{j=1}^{N} \varepsilon_j 2^{j-1} \quad ; \ x \in \{0, \ldots, N-1 = 2^n - 1\}; \ \varepsilon_j \in \{0,1\} \tag{4}$$

and extending this notation to the corresponding vectors:

$$|x\rangle = |\varepsilon_1, \ldots, \varepsilon_n\rangle \quad ; \ x \in \{0, \ldots, N-1\}; \ \varepsilon_j \in \{0,1\} \tag{5}$$

we will use both the binary and the decimal notation so that the vectors of the form

$$|x\rangle \otimes |y\rangle = |\varepsilon_1, \ldots, \varepsilon_n\rangle \otimes |\eta_1, \ldots, \eta_n\rangle \ ; \ x, y \in \{0, \ldots, N-1\}; \quad \varepsilon_j, \eta_j \in \{0,1\} \tag{6}$$

define the computational basis for the state space $\mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n}$.

2.2. *Steps of Simon's quantum period finding algorithm (QPFA)*

Step (1).

The initial state of the quantum system is,

$$|0\rangle_n \otimes |0\rangle_n \in \mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n} \equiv \mathbb{C}^N \otimes \mathbb{C}^N \tag{7}$$

i.e. all $2n$ q–bits are in the state $|0\rangle$.
Step (2).
Apply to the initial state the unitary operator

$$U_H := H^{\otimes n} \otimes 1$$

where H is the discrete Fourier (or Hadamard) transform on $\mathbb{C}^2$ defined by linear extension of the map:

$$|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad ; \quad |1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

and

$$H^{\otimes n} := H \otimes H \otimes \cdots \otimes H \qquad n\text{–times}$$

Since

$$H^{\otimes n}|0\rangle_n = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

the action of U_H brings the initial state to

$$\psi_o := U_H|0\rangle_n = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|0\rangle_n \tag{8}$$

Step (3a).
Among the unitary extensions of the partial isometry defined by

$$|x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle \qquad ; \quad x \in \{0, \ldots, N-1\} \tag{9}$$

choose one, denoted U_f, that can be physically realized.
Step (3b).
Realize the physical implementation of U_f.
Step (3c).
Apply to the state (8) the unitary operator U_f. This gives

$$U_f\psi_o =: \psi = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|f(x)\rangle \tag{10}$$

Step (4a).
Fix arbitrarily $u \in \{0, \ldots, N-1\}$ and construct the filter defined by the projection

$$P := 1_n \otimes |u\rangle\langle u| \tag{11}$$

Step (4b).
Apply the filter (11) to the quantum state described by the vector (10). This amounts to filter all the elements of the ensemble (10) for which $f(x) = u$ and to suppress all the remaining ones.
Theoretical conclusion from Step 4b
By by applying the Luders–Zumino formula of the quantum theory of measurement quantum information theorists conclude that the new quantum state of the total system is the one associated to the vector:

$$|\phi\rangle\langle\phi| := \frac{P|\psi\rangle\langle\psi|P}{Tr(P|\psi\rangle\langle\psi|)} = \frac{|P\psi\rangle}{\|P\psi\|}\frac{\langle P\psi|}{\|P\psi\|} \tag{12}$$

where ψ is defined by (10) so that:

$$P\psi = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\langle u|f(x)\rangle|x\rangle|u\rangle = \frac{1}{\sqrt{N}}\sum_{x\in\{0,1,\ldots,N-1\}, f(x)=u}|x\rangle|u\rangle \tag{13}$$

Notice that

$$\|P\psi\|^2 = \frac{|\{x \in \{0,1,\ldots,N-1\}, f(x) = u\}|}{N} = \frac{|f^{-1}(u)|}{N} \tag{14}$$

We will discuss only the case in which f satisfies the following additional conditions:

Assumption 2.1. *If f is injective on the interval $[0, r)$.*

Assumption 2.2. *r divides N exactly, i.e. independently of $u \in \{0, \ldots, N-1\}$*

$$|f^{-1}(u)| =: M = N/r \in \mathbb{N} \tag{15}$$

In this case from (13), (14) one deduces that

$$\phi = \frac{P\psi}{\| P\psi \|} = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\frac{\langle u|f(x)\rangle}{\| P\psi \|}|x\rangle|u\rangle = \frac{1}{\sqrt{M}}\sum_{j=0}^{M-1}|d_u + jr\rangle|u\rangle \tag{16}$$

where $d_u + jr$, for $j = 0, 1, 2 \ldots M-1$, are all the values of x for which $f(x) = u$ and $d_u < r$.
Step (5a).

Construct an apparatus implementing physically the unitary operator $U_{FT} \otimes 1_n$, where U_{FT} is the discrete Fourier transform, given by:

$$U_{FT}|x\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{i2\pi kx/N}|k\rangle$$

Step (5b).
Apply to ϕ the unitary operator $U_{FT} \otimes 1_n$. This leads to the state

$$\begin{aligned}
&\frac{1}{\sqrt{N/r}} \sum_{j=0}^{N/r-1} U_{FT}|d_u + jr\rangle|u\rangle \\
&= \frac{1}{\sqrt{N}} \frac{1}{\sqrt{N/r}} \sum_{j=0}^{N/r-1} \sum_{k=0}^{N-1} e^{i2\pi kd_u/N} e^{i2\pi kjr/N}|k\rangle|u\rangle \\
&= \frac{1}{\sqrt{r}} \sum_{k=0}^{N-1} \left(\frac{1}{\sqrt{N/r}} \sum_{j=0}^{N/r-1} e^{i2\pi jrk/N} \right) e^{i2\pi kd_u/N}|k\rangle|u\rangle \\
&= (U_{FT} \otimes 1_n)\phi
\end{aligned} \tag{17}$$

Since, if kr/N is not an integer, then

$$\sum_{j=0}^{N/r-1} e^{i2\pi jrk/N} = \frac{e^{i2\pi(N/r)rk/N} - 1}{e^{i2\pi rk/N} - 1} = 0$$

the non zero terms in the j–sum are precisely those for which

$$kr/N \in \mathbb{N}$$

i.e. those for which k is a multiple of $M = N/r$. Summing up: at the end of the 5–th step the state of the quantum system is:

$$\xi := (U_{FT} \otimes 1_y)\phi = \frac{1}{\sqrt{r}} \sum_{\{k \in \{0,\ldots,N-1\} : k \text{ is a multiple of } M = N/r\}} |k\rangle|u\rangle \tag{18}$$

Step (6).
The final step of the algorithm is usually described in the quantum computer literature as follows (see [St97]):
... The final state of the x register is now measured, and we see that the value obtained must be a multiple of w/r *...* (In our notations $w/r = N/r$)
In other words, as a result of a measurement, one obtains an integer k satisfying

$$k = \lambda N/r = \lambda M \Leftrightarrow k/N = \lambda/r \tag{19}$$

for some unknown integer $\lambda \in \{0, 1, \ldots, r-1\}$. Thus, if we make many of these measurements, we have a non zero probability to find a λ which is coprime to r.
Because of (18), in the relation (19), all these multiples will arise with equal probability $(1/r)$. Therefore one can apply the estimate (29), with λ and r replacing y and N respectively, and deduce that

$$P(\{\lambda \in \{2, \ldots, r-1\} \ : \ \lambda \ \text{ is coprime to r}\} \ ) \geq \frac{1}{\log r} \qquad (20)$$

If λ is coprime to r, we reduce the fraction k/N to an irreducible fraction and this gives λ and r separately.
If we repeat the measurement of the $|k\rangle$–basis $h = O(\log r) \leq O(\log N)$ times, this will give h possible candidates, $r_1, \ldots, r_h$, for the period and the estimate (20) shows that, with high probability, one of them should be the desired period.

3. Complexity considerations on Simon's quantum period finding algorithm (QPFA)

Step (1).
The initial state of the quantum system must be physically prepared so that all $2n$ q–bits are in the state $|0\rangle$.
An interesting n has an order of a few thousands bits.
Step (2).
The unitary operator $U_H := H^{\otimes n} \otimes 1$ must be:
– constructed
– applied to the initial state
Step (3a).
One can appeal to a theorem of K.R. Parthasarathy [KRP01a] to conclude that, for any given function f, all the unitary extensions of the partial isometry defined by (9) can be physically realized by means of quantum gates, i.e. unitary operators acting only on a single pair of q–bits.
However the same theorem gives an upper estimate, on the number of gates to be used, which is exponential in the number of factors. In our case this number is $2n$.
Therefore, in absence of a proof that, among all the unitary extensions of the partial isometry defined by (9), there exists at least one that can be physically realized by a number of quantum gates which is polynomial in $2n$, it makes no sense to speak of the practical realizability of the algorithm.
Step (3b).

Even in presence of such a proof the actual physical implementation of the unitary operator might be a formidable task, given the fact that the q–bits involved are of order of thousands.
An alternative way could be the discovery of a physically realizable interaction (Hamiltonian) embedding the given unitary in a continuous time evolution. But, even supposing that this can be done, the continuous time evolution will create serious problems due to the extreme non robustness of the algorithm against small perturbations of the unitary operator U_f.
Step (3c).
Even supposing that the above problems can be solved, the concrete application of the unitary operator U_f to the state (8) is a problem whose solution requires additional costs in terms of time and of experimental work to be done.
Step (4a).
The filter defined by the projection (11) must be constructed.
Step (4b).
The above comment, on the cost of the concrete realization of Step (3c), also holds for the application of the filter (11) to the quantum state described by the vector (10).
Theoretical conclusion from Step 4b
This conclusion heavily depends on the application of the Luders–Zumino formula of quantum measurement theory. This is quite different from the original von Neumann formula and implies that, after an incomplete measurement on a quantum system in a pure state, the system will still remain in a pure state.
Although not logically impossible, such a situation is against physical intuition because an incomplete measurement by definition does not produce maximal information while, in quantum mechanics, a pure state defines a situation of maximal information.
Only some very strong experimental evidence could prove that this natural intuition is wrong.
Step (5a).
One must construct an apparatus implementing the discrete Fourier transform on arbitrary quantum states (see above comments to Step (3c)).
Step (5b).
One must apply the above apparatus to the quantum state given by (16) (see above comments to Step (3c)).
Step (6).
Taken literally, the statement ... *The final state of the x register is now*

measured ..., means that the last step of the algorithm consists in the determination of a quantum state.
But it is well known such a determination, in a space of dimension d requires an order of d measurements (d^2 in case of a mixture).
In our case $d = 2^{2n}$, i.e. it is exponential in n.
One might try a probabilistic approach, choosing at random a $k \in \{0, \ldots, N-1\}$ and evaluating experimentally the transition probability $|\langle k, \xi \rangle|^2$, which will be zero unless k is a multiple of $M = N/r$. But, in the interesting cases, r is of the same order of magnitude of N so that $M = N/r$ is much smaller. This means that on average the number of trials to be done, before a multiple of $M = N/r$ appears, is of order N. Since $N = 2^n$, this is again exponential in n.

4. Classical reduction of the factorization problem to period finding

Lemma 4.1. *Let $x \in \mathbb{N}$ and define $x_1 := x + 1 \quad ; \quad x_2 := x - 1$ then 2 is the only possible common divisor of x_1 and x_2. In particular, if x_1, x_2 are both odd, then they have no common divisors.*

Proof Up to exchange odd indices we can assume that

$$x_1 > x_2$$

Suppose that $n \in \mathbb{N}$ is a common divisor of x_1, x_2. Then there are natural integers x_1^1, x_2^1 such that

$$x + 1 = n x_1^1 \quad ; \quad x - 1 = n x_2^1$$

$$n x_2^1 + 2 = n x_1^1 \Leftrightarrow x_2^1 + \frac{2}{n} = x_1^1$$

but $2/n \in \mathbb{Z} \Leftrightarrow n = 1, 2$. Thus 2 is the only possible common divisor for $x + 1$ and $x - 1$.

Lemma 4.2. *Let $x \in \{2, \ldots, N-2\}$ be any solution of the equation*

$$x^2 = 1 \qquad (mod\ N) \tag{21}$$

such that $(x \pm 1) \neq 0$ (mod N) and define x_1, $x_2 \in \{2, \ldots, N-1\}$ by

$$x_1 = x + 1 \qquad (mod\ N)\ ; \qquad x_2 = x - 1 \qquad (mod\ N) \tag{22}$$

Denote $gcd(x, N)$ the greatest common divisor of x and $\mathbb{N}$.
Then the following factorization of N:

$$N = gcd(x_1, N) \cdot gcd(x_2, N) \tag{23}$$

takes place and is not trivial (i.e. both factors are $\neq 1$).

Proof. In view of (22), (21) is equivalent to

$$x_1 x_2 = (x+1)(x-1) = x^2 + x - x - 1 = 0 \qquad (\text{mod } N) \tag{24}$$

which means that the product $x_1 x_2 = (x+1)(x-1)$ is a multiple of N. By construction both x_1 and x_2 can be identified to numbers satisfying

$$1 < x_1, x_2 < N \tag{25}$$

and we know that there exist an integer $\lambda \geq 1$ such that

$$x_1 x_2 = \lambda N$$

For $j = 1, 2$ denote

$$g_j := gcd(x_j, N)$$

Then

$$x_j = g_j y_j$$

where y_j does not divide N. In these notations

$$g_1 y_1 g_2 y_2 = \lambda N$$

and, since $y_1 y_2$ does not divide N, it must divide λ. Therefore

$$g_1 g_2 = \frac{\lambda}{y_1 y_2} N =: \lambda' N$$

where $\lambda' := \lambda / y_1 y_2 \in \mathbb{N}$. But g_1 and g_2 divide N and, being x_1 and x_2 both odd, they have no common factor. Thus their product divides N so that

$$1 = \lambda' \left(\frac{N}{g_1 g_1} \right)$$

Since both λ' and $N/g_1 g_2$ are integers, this identity is possible if and only if

$$\lambda' = N / g_1 g_2 = 1$$

which is the factorization (23). Finally g_1 cannot be 1 because otherwise x_1 has no common factor with N and therefore the product $x_1 g_2 y_2$ cannot

be a multiple of N. Since g_1 and g_2 enter symmetrically in the argument, this factorization (23) is non trivial which is the thesis.
The following Lemma clarifies the connections between the factorization and the period–finding problem.

Definition 4.1. Let V be a vector space. a function $V : V \to V$ is called periodic if there exists a vector $r \in V$ such that

$$F(x + r) = F(x) \qquad ; \qquad \forall x \in V \tag{26}$$

If V is a ring identified to a totally ordered set (e.g. $\{0, 1, \ldots, N\}$ for some $N \in \mathbb{N}$) then the smallest r satisfying (4.1) is called the period of F.

Lemma 4.3. *If $y \in \mathbb{N}$ is such that the function*

$$F(a) := y^a \ (mod\ N) \qquad ; \qquad a \in \{0, 1, \ldots, N-1\} \tag{27}$$

has an even period r, then $y^{r/2}$ is a solution of (21).

Proof. Under our assumptions $r/2 \in \mathbb{N}$ and

$$(y^{r/2})^2 = y^r = 1 \qquad (\text{mod } N) \tag{28}$$

4.1. *Classical probabilistic factorization algorithms*

Definition 4.2. $y \in \mathbb{N}$ is called coprime to $N \in \mathbb{N}$ if y and N have no non trivial common factors.
In this case the minimum $r \in \mathbb{N}$ which satisfies (28) is called the *order of* $y(\text{mod } N)$ and denoted $r_{y,N}$.

Remark. Otherwise stated, the order of $y(\text{mod } N)$ is the period of the function $a \in \{0, 1, \ldots, N-1\} \mapsto y^a \ (\text{mod } N)$. If $y \in \mathbb{N}$ is coprime to $N \in \mathbb{N}$, then $r_{y,N}$ is well defined by Euler theorem and coincides with the period of the function (27).
It is known from number theory that, denoting P the uniform measure on the set $\{0, 1, \ldots, N-1\}$, i.e.

$$P(x) := 1/N \qquad ; \qquad x \in \{0, 1, \ldots, N-1\}$$

as a probability space with , one has:

$$P(\{y \in \{0, 1, \ldots, N-1\} \ : \ y \text{ is coprime to } N\}\ ) \geq \frac{1}{\lg N} \tag{29}$$

This means that the overwhelming majority (more than $N/\log N$) of numbers in $\{0, 1, \ldots, N-1\}$ are coprime with N. This fact suggests the following

probabilistic strategy to look for solutions of the factorization problem.
– Pick at random, with uniform distribution, an $y \in \{0, \dots, N-1\}$.
– By the above discussion the probability that, in $O(\log N)$ independent extractions, y is coprime to N is high.
– If y is coprime to N and $r_{y,N}$ is even, the number $x = y^{r_{y,N}/2}$ is a solution of equation (21).
– If x is not a trivial solution, then by Lemma (4.2) we have a nontrivial factorization of N.
Since $y \in \{0, 1, \dots, N-1\}$ is picked at random, the probability to have such a nontrivial factorization of N is equal to the joint probability of the following three events:

$$[y \text{ is coprime to N}] \cap [r_{y,N} \text{ is even}] \cap [y^{r_{y,N}/2} \neq \pm 1 (\text{mod } N)] \tag{30}$$

Let us introduce the following assumption.

Assumption 4.1. *With respect to the uniform distribution on* $\{0, \dots, N-1\}$*, the events*

$$[y \text{ is coprime to } N] \text{ and } [r_{y,N} \text{ is even}] \cap [y^{r_{y,N}/2} \neq \pm 1 (\text{mod } N)]$$

are independent.

Under the above assumption the probability of the event (30) becomes equal to

$$P([y \text{ is coprime to N}])\, P\left([r_{y,N} \text{ is even}] \cap [y^{r_{y,N}/2} \neq \pm 1 (\text{mod } N)]\right)$$

and the estimate (29) implies that this is

$$\geq \frac{P\left([y \ : \ r_{y,N} \text{ is even and } y^{r_{y,N}/2} \neq \pm 1 (\text{mod } N)\ ] \mid [y \text{ is coprime to N}]\right)}{\lg N} \tag{31}$$

where $P(\cdot|\cdot)$ denotes conditional probability. This conditional probability is estimated by the following theorem of number theory.

Theorem 4.1. *Let N be odd with $k \geq 2$ different primes in its factorization. Then, one has:*

$$P\left([y \ : \ r_{y,N} \text{ is even and } y^{r_{y,N}/2} \neq \pm 1 (\text{mod } N)\ ] \mid [y \text{ is coprime to } N]\right)$$
$$\geq 1 - \frac{1}{2^{k-1}} \tag{32}$$

In particular the probability of the event (30) is estimated by

$$P([y \ : \ r_{y,N} \text{ is even; } y^{r/2} \neq \pm 1(\text{mod } N]) \text{ and } gcd(y,N) = 1) \geq \left(1 - \frac{1}{2^{k-1}}\right) \frac{1}{\lg N} \geq \frac{1}{2 \lg N}$$

Once this problem is solved, one picks y at random and calculates $r_{y,N}$ according to Theorem (4.1).
In $O(\log N)$ trials, the probability that the pair $(y, r_{y,N})$ satisfies (30) in greater than $1/2 \lg N$.
Given a pair $(y, r_{y,N})$, satisfying (30), one solves the factorization problem using Lemma (4.2).

References

1. Ekert A., Jozsa R.: Quantum computation and Shor's factoring algorithm, Rev. Mod. Phys. 68 (1996) 733
2. Parthasarathy K.R.: A remark on the unitary group of a tensor product of n finite dimensional Hilbert spaces, Preprint Volterra n. 479 (2001)
3. Shor P. W.: "Algorithms for quantum computation: Discrete logarithms and factoring." In: Proceedings of the 35th IEEE Annual Symposium on Foundations of Computer Science, S. Goldwasser (ed.) IEEE Computer Society Press, New York (1994) 124-134
4. Shor P. W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, in: Proc. 35th Annual Symp. on Foundations of Computer Science, Santa Fe, IEEE Computer Society Press (1994); revised version 1995a preprint quant-ph/9508027
5. Simon D.: On the power of quantum computation, in Proc. 35th Annual Symposium on Foundations of Computer Science IEEE Computer Society Press, Los Alamitos (1994) 124-134
6. Andrew Steane: Quantum computing quant-ph/9708022