Quantum Inf Process (2013) 12:97–108
DOI 10.1007/s11128-012-0360-4

# Closed-form formula on quantum factorization effectiveness

**Piotr Zawadzki**

Received: 10 February 2011 / Accepted: 13 January 2012 / Published online: 26 January 2012

**Abstract** The quantum factorization effectiveness is limited both by inherent randomness of the quantum measurement and requirement of special selection of parameters controlling behavior of classic algorithms supporting quantum device operation. However, only coarse bounds on probability of successful parameters selection have been published so far. The proof of an exact expression on factorization efficiency constitutes the main contribution of the paper. The proved expression simply relates Shor's algorithm efficiency to properties of the factors forming the composite number.

**Keywords** Quantum computing · Factorization · Secure communication

## 1 Introduction

Theoretical study of quantum systems used in computational devices has achieved tremendous progress in the last few years. It is shown that quantum computers are capable of efficiently performing some tasks, which are intractable for presently used computers. The quantum order finding [8] is one of the most preeminent applications in quantum information processing. It stimulates research in the field as it provides time complexity reduction of factoring problem from sub-exponential to polynomial one. The interest in efficient solution of that problem is especially great for composite integers being a product of two large prime numbers—the ability to factor such integers is equivalent to breaking the Rivest, Shamir and Adleman (RSA) cryptographic system [3].

P. Zawadzki (✉)
Institute of Electronics, Akademicka 16, 44-100 Gliwice, Poland
e-mail: Piotr.Zawadzki@polsl.pl

The random behavior of Shor's algorithm is related to both inherent features of the quantum measurement and the selection of parameters that control the operation of classic algorithms that assist in quantum computations. It was shown that the uncertainty introduced by quantum measurements could be minimized to an arbitrarily small value by enlarging the size of the registers used by the quantum device [6]. The classic part of the algorithm leads to successful factorization only if some random number $x$ fed as input meets some specific requirements and the result of post processing of the quantum measurement by continued fraction expansion is relatively prime to the order of $x$. The lower bound on probability of finding parameter $x$ is derived in [2] as

$$p(x) = 1 - 2^{1-M} \tag{1}$$

where $M$ is the number of prime factors of $N$. That expression has a maximum value when the composite number is a product of only two prime numbers, which in fact represents the most interesting situation. Some proposals [1,4,5] related to the improvement of the algorithm efficiency have been put forth. However, those modifications have focused on probability of order recovery from quantum measurement. The aim of this paper is to provide a closed formula on factorization success probability expressed in terms of properties of the factors forming the composite number. The derived analytical expression provides additional insight into the algorithm properties and permits a statistical analysis of its behavior.

Factorization of the composite number $N$ is equivalent to order finding of some number $1 < x < N$ when the following conditions are simultaneously satisfied [8]:

$$\gcd(x, N) = 1, \quad r_N(x) \bmod 2 = 0, \quad x^{r_N(x)/2} \bmod N \neq -1 \tag{2}$$

where $r_N(x)$ denotes the order of $x$. Classical order finding gives no advantage over other factorization algorithms as its complexity is also exponential. However, it is possible to determine the order of $x$ in polynomial time by the quantum algorithm [8]. The quantum method for finding order is not a reliable procedure because of the inherent uncertainty of quantum measurement. The probability distribution of the possible quantum measurement outcomes has sharp peaks in the vicinity of values that may lead to the successful order recovery. However, there exists a nonzero probability of measurement failure. This probability may be arbitrarily minimized because of its direct relation to the size of the quantum registers [6]. The following steps summarize quantum factorization:

1. Select random number $x$ coprime to $N$ (otherwise $\gcd(x, N)$ is a factor of $N$). Only some $x$ are good candidates for further processing as the order $r_N(x)$ determined in the next step must satisfy conditions (2).
2. Find the order of $x$ with the quantum computer. The correct order value is successfully recovered only for some subset of valid quantum measurements.
3. Calculate divisor $\gcd\left(x^{r_N(x)/2} - 1, N\right)$ and return to point 1.

It is clear that the nature of the quantum factorization algorithm is probabilistic even if perfect fidelity of the quantum measurement is assumed. The success ratio of the algorithm depends on the following random factors:

- the selection of the ”lucky” $x$ that fulfills condition (2),
- the order recovery from the quantum measurement result.

The success of the order recovery depends on the order value itself. Assuming the infinite accuracy of the quantum measurement and the single use of the quantum device, the continued fraction expansion algorithm, which is applied to post process the measurement result, provides the correct order recovery when the result of its operation is formed by relatively prime numbers. The count of numbers relatively prime to $r_N(x)$ is given by Euler's totient function $\Phi(r_N(x))$. As a consequence, the order of $x$ may be recovered with probability $\Phi(r_N(x))/r_N(x)$. In a case of failure, the post processing procedure returns a value that is underestimated by some factor. However, if it is possible to use the quantum device over many repetitions, consecutive measurements lead to different factors of $r_N(x)$. The least common multiple of those factors gives the correct value of the order with probability quickly approaching certainty as the number of measurements grows [1]. It follows from the above discussion that the order recovery procedure may be regarded as reliable provided that multiple use of the quantum device is allowed.

Two scenarios of Shors algorithm operation were considered in provided herein analysis of its effectiveness. In the first one it was assumed that quantum device can be used only once. Such scenario will be used in the initial phase of quantum information processing deployment when repetitive runs of aquantum computer will be undoubtedly costly in terms of money and effort. The second scenario assumed that multiple usage of quantum device does not pose a technological challenge, so it is applicable when quantum computation technology will become a mature solution.

## 2 Mathematical preliminaries

The aim of this work is to provide closed form formulas on the effectiveness of the classic part of Shor's algorithm. However, the concise presentation of the proof requires an introduction of additional definitions and lemmas.

**Definition 1** Let $n$ be a positive integer. The factor level of $b$ relative to $n$ is the greatest integer $\alpha$ such that $b^\alpha$ divides $n$ ($n = b^\alpha \mu$ and $b$ does not divide $\mu$).

**Lemma 1** *Let $x \in Z_p^*$ for prime $p$. The order of $x$ relative to $p$ is given by $r_p(x) = (p-1)/\gcd(s, p-1)$ where $s$ is a positive integer such that $x = g^s \bmod p$ and $g$ is the generator of $Z_p^*$.*

*Proof* It follows from Euler's theorem and the order definition that

$$g^{\Phi(p)} \bmod p = 1 = g^{sr_p} \bmod p.$$

Thus, $sr_p$ must be multiple of totient function $\Phi(p) = (p-1)$. The order $r_p$ is by definition the smallest positive integer satisfying $sr_p = k(p-1)$. Thus, $sr_p = \operatorname{lcm}(s, p-1) = s(p-1)/\gcd(s, p-1)$. □

**Lemma 2** *Let $p > 2$ be a prime number. If $p - 1 = b^\alpha \mu$, where $b > 1$ is also prime, $\alpha$ is a positive integer, and $\mu$ is not divisible by $b$. Then $b^m$ ($m > 0$) is a factor of the order $r_p(x)$ of some $x \in Z_p^*$ with probability*

$$P_p\left(b,m\right)=\frac{b^{\max(\alpha-m+1,0)}-1}{b^{\max(\alpha-m+1,0)}}$$

*The number b is not a factor of $r_p\left(x\right)$ with probability $P_p\left(b,0\right)=b^{-\alpha}$.*

*Proof* All elements $x\in Z_p^*$ may be expressed as $x=g^s \bmod p$, where $g$ is the group generator. The generator exponents may be formally expressed as $s=b^{\beta}\nu$, where $\beta\geq 0$ and $\nu$ is not divisible by $b$. Then, for $\beta\geq\alpha$, the number $b$ is not a factor of the order of $x$ because $r_p\left(x\right)=\mu/\gcd\left(\nu,\mu\right)$, where $\mu$ and $\nu$ are not divisible by $b$. If $\beta<\alpha$ then $r_p\left(x\right)=b^{\alpha-\beta}\mu/\gcd\left(\nu,\mu\right)$. The number of exponents of the form $s=b^{\beta}\nu$ is equal to $[(p-1)/b^{\beta}][(b-1)/b]=b^{\alpha-\beta-1}\mu(b-1)$. The first term $(p-1)/b^{\beta}$ describes the number of exponents divisible by $b^{\beta}$, but from those ones only $(b-1)/b$ are not divisible by $b^{\beta+1}$. Thus, the number of orders divisible by $b^m$ can be found as

$$L_b\left(m\right)=\sum_{\beta=0}^{\alpha-m}b^{\alpha-\beta-1}\mu(b-1)=\mu b^{m-1}\left(b^{\alpha-m+1}-1\right)$$

for $0<m\leq\alpha$. The first part of the thesis results after division by $p-1=b^{\alpha}\mu$ and generalization for any $m>0$. The number of orders not divisible by $b$ is equal to

$$L_{\not b}=(p-1)-L_b\left(1\right)=b^{\alpha}\mu-\mu\left(b^{\alpha}-1\right)=\mu$$

Division of $L_{\not b}$ by $p-1=b^{\alpha}\mu$ directly leads to the second part of the thesis. □

*Remark 1* The factor level of $b$ relative to $r_p\left(x\right)$ is equal to $m$ with probability

$$Q_p\left(b,m\right)=\begin{cases}P_p\left(b,m\right)-P_p\left(b,m+1\right) & m>0\\ P_p\left(b,0\right) & m=0\end{cases}\tag{3}$$

**Lemma 3** *Let $p>2$ be a prime number. If prime number b is not a divisor of $(p-1)$, then it is also not a divisor of $r_p\left(x\right)$.*

*Proof* Suppose that there exists $x$ such that $b$ divides $r_p\left(x\right)$, i.e. $r_p\left(x\right)=b^m\mu$ where $\mu$ is not divisible by $b$. It follows from the definition of order and Euler's theorem that

$$x^{\Phi(p)} \bmod p=1=x^{r_p} \bmod p$$

Thus, for some integer $k$, $kr_p\left(x\right)=\Phi\left(p\right)=p-1$. But because of $r_p\left(x\right)$'s divisibility by $b^m$, the $(p-1)$ must also contain $b^m$ as a factor which leads to a contradiction. □

*Remark 2* Let $p-1$ have the following factorization

$$p-1=b_1^{\alpha_1}b_2^{\alpha_2}\cdots b_K^{\alpha_K}=\prod_{l=1}^{K}b_l^{\alpha_l}$$

It follows from Lemmas 2 and 3 that the order of any $x \in Z_p^*$ can be represented as follows

$$r_p(x) = b_1^{m_1} b_2^{m_2} \cdots b_N^{m_K} = \prod_{l=1}^{K} b_l^{m_l} \tag{4}$$

where $0 \le m_l \le \alpha_l$. The probability of occurrence of the set of specified divisors results from Remark 1 and is given by the following expression

$$Q_p(b_1, m_1, \ldots, b_K, m_K) = \prod_{l=1}^{K} Q_p(b_l, m_l)$$

The special case $m_1 = m_2 = \cdots = m_K = 0$ corresponds to selection of the element with order $r_p(x) = 1$. If $p$ is prime, there exists only one such element $x = 1$. The probability of such an event is equal to

$$Q_p(b_1, m_1 = 0, \ldots, b_K, m_K = 0) = \prod_{l=1}^{K} P_p(b_l, 0) = \prod_{l=1}^{K} b_l^{-\alpha_l}$$

**Lemma 4** *Let $N = \prod_{k=1}^{M} p_k$ where prime factors have representation $p_k = b^{\beta_k}\mu_k + 1$, $b$ is also prime relatively prime to $N$, $\beta_k \ge 0$ and $\mu_k$ are not divisible by $b$. The probability that $b^m$ for $m > 0$ divides the order relative to $N$ of some randomly selected $x \in Z_N^*$ that is relatively prime to $N$ is equal to*

$$P_N(b, m) = \frac{\left(\prod_{k=1}^{M} b^{\max(\beta_k - m + 1, 0)}\right) - 1}{\prod_{k=1}^{M} b^{\max(\beta_k - m + 1, 0)}}$$

*The probability that $b$ does not divide $r_N(x)$ is equal to*

$$P_N(b, 0) = 1 / \left(\prod_{k=1}^{M} b^{\beta_k}\right)$$

*Proof* Let $r_{p_k}(x)$ and $r_N(x)$ denote orders of $x$ relative to $p_k$ and $N$, respectively. It follows from $r_{p_k}(x)$'s definition that

$$x^{\prod_{k=1}^{M} r_{p_k}} \bmod \prod_{k=1}^{M} p_k = 1$$

Elimination of repeating terms in the factorization of $r_{p_k}$'s leads to $r_N = \operatorname{lcm}\left(r_{p_1}, \ldots, r_{p_M}\right)$. This means that $b^m$ does not divide $r_N(x)$ if it does not divide any of $r_{p_k}(x)$'s. It follows from Lemma 2 that the probability of such event is equal to $1/\prod_{k=1}^{M} b^{\max(\beta_k-m+1,0)}$ thus $b^m$ is a factor of $r_N$ with probability

$$P_N(b,m) = \frac{\left(\prod_{k=1}^{M} b^{\max(\beta_k-m+1,0)}\right)-1}{\prod_{k=1}^{M} b^{\max(\beta_k-m+1,0)}}$$

It also immediately follows that $b$ is not a factor of $r_N$ with probability

$$P_N(b,0) = 1 - P_N(b,1) = \prod_{k=1}^{M} 1/b^{\beta_k}$$

□

*Remark 3* One can define function $Q_N(b,m)$ that returns the probability that $m$ is a factor level of $b$ relative to $r_N(x)$ (i.e. $r_N(x) = b^m\mu$ and $b$ does not divide $\mu$) as follows

$$Q_N(b,m) = \begin{cases} P_N(b,m) - P_N(b,m+1) & m > 0 \\ P_N(b,0) & m = 0 \end{cases}$$

If the following factorization is assumed

$$\mathrm{lcm}(p_1-1, p_2-1, \ldots, p_M-1) = c_1^{\gamma_1} c_2^{\gamma_2} \cdots c_K^{\gamma_K}$$

then for each $x < N$ and coprime to $N$, there exists a set of exponents $0 \le m_l \le \gamma_l$ such that

$$r_N(x) = c_1^{m_1} c_2^{m_2} \cdots c_K^{m_K}$$

The probability of the given set occurring is given by

$$Q_N(c_1, m_1, \ldots, c_K, m_K) = \prod_{l=1}^{K} Q_N(c_l, m_l) \tag{5}$$

**Lemma 5** *Let $N = \prod_{k=1}^{M} p_k$ and $p_k$ be primes. Also let order $r_N(x)$ of some $x \in Z_N^*$ be even. The equality $x^{r_N/2}$ mod $N = -1$ holds if and only if factor levels of 2 relative to $r_{p_k}(x)$ for each $1 \le k \le M$ and $r_N(x)$ are equal and positive.*

*Proof* The equality $x^{r_N(x)/2}$ mod $N = -1$ is equivalent to the set of linear equations

$$x^{r_N(x)/2} \bmod p_k = -1$$

for $k = 1, \ldots, M$. It follows that $r_N(x)$ cannot be an even multiple of $r_{p_k}(x)$. If $r_N(x)$ would be an even multiple of $r_{p_k}(x)$ then $r_N(x) = 2sr_{p_k}$ for some $s$ and

$$x^{r_N(x)/2} \bmod p_s = x^{sr_{p_k}} \bmod p_k = 1$$

what contradicts initial assumption. Due to symmetry the above reasoning holds for any $p_k$ what leads to conclusion that factor level of 2 is the same relative to all $r_{p_k}$ and in consequence to $r_N(x) = \operatorname{lcm}(p_1, p_2, \ldots, p_M)$. This proves the if clause. Lets assume that 2 has the same positive factor level relative to any $r_{p_k}$, thus each $r_{p_k}$ may be represented as $r_{p_k} = 2^\alpha \mu_k$, where $\alpha > 0$ and $\mu_k$ is odd. If factor level of 2 relative to $r_{p_k}$ is nonzero, then $(x^{r_{p_k}/2} - 1)(x^{r_{p_k}/2} + 1) \bmod p_k = 0$. There are only trivial solutions to this equation, namely $x^{r_{p_k}/2} \bmod p_k = 1$ and $x^{r_{p_k}/2} \bmod p_k = -1$ for the prime modulus, and the first solution must be excluded because it contradicts the definition of $r_{p_k}$ as the order. This leads to the set of $M$ equations of the form

$$x^{r_{p_k}/2} \bmod p_k = -1$$

for even $r_{p_k}$. If 2 has the same factor level $\alpha > 0$ relative to each of $r_{p_k}$'s, then $r_N = \operatorname{lcm}\left(r_{p_1}, r_{p_2}, \ldots, r_{p_M}\right) = 2^\alpha \operatorname{lcm}(\mu_1, \mu_2, \ldots, \mu_M)$, where $\mu_k$ are odd. Thus, $r_N$ is an odd multiple of any of the $r_{p_k}$'s. Multiplication of $r_{p_k}/2$ by odd number $\operatorname{lcm}(\mu_1, \mu_2, \ldots, \mu_M)/\mu_k$ does not change the value of any of the above equations. Thus, for any $k$

$$x^{r_N/2} \bmod p_k = -1$$

This is equivalent to $x^{r_N/2} \bmod N = -1$. □

## 3 Effectiveness of Shor's algorithm

Let $X_N^*$ and $F_N^*$ be the sets of all $x$ entering order finding algorithm and the values of parameters suitable for successful factorization, respectively

$$X_N^* = \{x : \gcd(x, N) = 1\}$$
$$F_N^* = \{x : \text{ conditions (2) are satisfied}\}$$

The probability of the algorithm success in the single run is the quotient

$$P_S = \frac{\sum_{x \in F_N^*} \Phi(r_N(x))}{\sum_{x \in X_N^*} r_N(x)}. \tag{6}$$

The calculation of the denominator is straightforward

$$\mathrm{DEN} = \sum_{x=1}^{N-1} r_N(x) = \sum_{k=1}^{Q} r_k l_k(x) \tag{7}$$

where $r_k$ are distinct values of the possible orders of $x$ and $l_k(x)$ is the number of $x$ with the specified value of the order. But the value of $r_k$ is unambiguously defined by its factorization, thus the number of elements with the given $r_k$ value is equal to

$$l_k(x) = \left|X_N^*\right| \prod_{l=1}^{K} Q_N(c_l, m_l) \tag{8}$$

where $\left|X_N^*\right| = \prod_{k=1}^{M}(p_k - 1)$ denotes the number of $x$ relatively prime to $N$ and $\prod_{l=1}^{K} Q_N(c_l, m_l)$ describes the probability of occurrence of the given factorization of $r_N(x)$. In consequence the summation may be carried out over all distinct factorizations of $r_N(x)$

$$\mathrm{DEN} = \left|X_N^*\right| \sum_{m_1=0}^{\gamma_1} \cdots \sum_{m_K=0}^{\gamma_K} \left( \prod_{l=1}^{K} Q_N(c_l, m_l)\, c_l^{m_l} \right) \tag{9}$$

where identity $r_N(x) = \prod_{l=1}^{K} c_l^{m_l}$ was used.

Similarly, the numerator of (6) can be found. Additional complications come from the constraints specified in $F_N^*$ definition. First of all, the order $r_N(x)$ of parameters suitable for factorization has to be even. But because of $p_k$'s primality, the numbers $(p_k - 1)$ are even and the factor 2 is always present in $\mathrm{lcm}(p_1 - 1, p_2 - 1, \ldots, p_M - 1)$. This is equivalent to setting $c_1 = 2$, $\gamma_1 \geq 1$ and summation should be carried out for $m_1 \geq 1$. The condition $x^{r_N(x)/2} \bmod N \neq -1$ may be expressed in terms of the order factors with the help of Lemma 5. It follows that number of orders $r_N(x)$ with factor level of 2 equal to $m$ that are taken into account in the numerator calculation should be diminished by the number of parameters $x$ with orders $r_{p_k}(x)$ that have concurrently factor level of 2 also equal to $m$. The probability of finding $x$ conforming with that constraint is equal to

$$Q_N(2, m) - \prod_{k=1}^{M} Q_{p_k}(2, m)$$

for $m > 0$. Thus, the second condition resulted in special handling of the first term of (5). The probability that the given set of exponents $m_l$ corresponds to the number suitable for factorization is given by the product of the following terms

$$g_N(c, m) = \begin{cases} Q_N(2, m) - \prod\limits_{k=1}^{M} Q_{p_k}(2, m) & c = 2, m > 0 \\ 0 & c = 2, m = 0 \\ Q_N(c, m) & c > 2, m \geq 0 \end{cases} \tag{10}$$

The last modification is related to the summed term. The value of totient function can be calculated as

$$\Phi\left(n\right)=\prod_{l=1}^{K}\left(c_l-1\right)c_l^{\left(\alpha_l-1\right)} \tag{11}$$

when $n=\prod_{l=1}^{K}c_l^{\alpha_l}$. Unfortunately, the above schema cannot be directly applied as not all factors of lcm $\left(p_1-1,p_2-1,\ldots,p_M-1\right)$ are always present in $r_N\left(x\right)$ factorization. One can easily overcome that difficulty by substitution of 1 when the given factor is absent

$$f\left(c_l,m_l\right)=\begin{cases}(c_l-1)c_l^{m_l-1} & m_l>0\\ 1 & m_l=0\end{cases} \tag{12}$$

and

$$\Phi\left(r_N\left(x\right)\right)=\prod_{l=1}^{K}f\left(c_l,m_l\right) \tag{13}$$

where $0\leq m_l\leq\gamma_l$ and $\gamma_l$ are taken from factorization 1cm$(p_1-1,p_2-1,\ldots,p_M-1)=\prod_{l=1}^{K}c_l^{\gamma_l}$. The value of the numerator may be then calculated as

$$\mathrm{NUM}=\left|X_N^*\right|\sum_{m_1=1}^{\gamma_1}\sum_{m_2=0}^{\gamma_0}\cdots\sum_{m_K=0}^{\gamma_K}\left(\prod_{l=1}^{K}g_N\left(c_l,m_l\right)f\left(c_l,m_l\right)\right) \tag{14}$$

where special handling of $m_1$ is taken into account. The probability of the successful quantum factorization of the composite number in the single execution of Shor's algorithm is given by

$$P_S=\frac{\sum_{m_1=1}^{\gamma_1}\sum_{m_2=0}^{\gamma_2}\cdots\sum_{m_K=0}^{\gamma_K}\left(\prod_{l=1}^{K}g_N\left(c_l,m_l\right)f\left(c_l,m_l\right)\right)}{\sum_{m_1=0}^{\gamma_1}\cdots\sum_{m_K=0}^{\gamma_K}\left(\prod_{l=1}^{K}Q_N\left(c_l,m_l\right)c_l^{m_l}\right)} \tag{15}$$

The above probability solely depends on the properties of factors $p_k$.

In the second scenario, when repetitive runs of quantum device are permitted, the probability of successful factorization is just given by the quotient of number of elements in the sets $F_N^*$ and $X_N^*$, respectively

$$P_R=\frac{\left|F_N^*\right|}{\left|X_N^*\right|}=\frac{\sum_{x\in F_N^*}1}{\sum_{x\in X_N^*}1}\ . \tag{16}$$

Observations used in calculation of the numerator of (6) still may be used. The only difference relies in the summed term. Thus, the number of elements in the set $F_N^*$ is equal to

$$\left|F_N^*\right| = \left|X_N^*\right| \sum_{m_1=1}^{\gamma_1} \sum_{m_2=0}^{\gamma_2} \cdots \sum_{m_K=0}^{\gamma_K} \left( \prod_{l=1}^{K} g_N\left(c_l, m_l\right) \right) \tag{17}$$

and the sought probability is given by

$$\begin{aligned} P_R &= \sum_{m_1=1}^{\gamma_1} \sum_{m_2=0}^{\gamma_2} \cdots \sum_{m_K=0}^{\gamma_K} \left( \prod_{l=1}^{K} g_N\left(c_l, m_l\right) \right) \\ &= \left( \sum_{m_1=1}^{\gamma_1} g_N\left(c_1, m_1\right) \right) \prod_{l=2}^{K} \left( \sum_{m_l=0}^{\gamma_l} g_N\left(c_l, m_l\right) \right). \end{aligned} \tag{18}$$

But $g_N\left(c_l, m_l\right) = Q_N\left(c_l, m_l\right)$ for $l > 1$ and $\sum_{m_l=0}^{\gamma_l} Q_N\left(c_l, m_l\right) = 1$, thus

$$P_R = \sum_{m_1=1}^{\gamma_1} \left[ Q_N\left(2, m_1\right) - \prod_{k=1}^{M} Q_{p_k}\left(2, m_1\right) \right]. \tag{19}$$

Further simplification results from calculation of the failure probability

$$1 - P_R = Q_N\left(2, 0\right) + \sum_{m_1=1}^{\gamma_1} \prod_{k=1}^{M} Q_{p_k}\left(2, m_1\right) \tag{20}$$

Let the factors of $N$ be represented as $p_k = 2^{\alpha_k} \mu_k$ where $\mu_k$ is odd. The value of the first term directly follows from Remark 3 and Lemma 4

$$Q_N\left(2, 0\right) = P_N\left(2, 0\right) = \prod_{k=1}^{M} P_{p_k}\left(2, 0\right) = \prod_{k=1}^{M} \frac{1}{2^{\alpha_k}} = 2^{-\left(\sum_{k=1}^{M} \alpha_k\right)}$$

In the second term the upper summation limit is equal to $\gamma_1 = \max\left(\alpha_1, \alpha_2, \ldots, \alpha_M\right)$. On the basis of Lemma 2 and Remark 1: $Q_{p_k}\left(2, m_1\right) = 0$ for $m_1 > \alpha_k$ because in this case $P_{p_k}\left(2, m_1\right) = 0$. Therefore the summed term does not vanish only if $m_1 \leq \min\left(\alpha_1, \alpha_2, \ldots, \alpha_M\right) = \alpha_{min}$. In the calculation of $Q_{p_k}\left(2, m_1\right)$ two separate cases $0 < m_1 < \alpha_k$ and $m_1 = \alpha_k$ must be considered. In the first case

$$\begin{aligned} Q_{p_k}\left(2, m_1\right) &= P_{p_k}\left(2, m_1\right) - P_{p_k}\left(2, m_1 + 1\right) \\ &= \frac{2^{\alpha_k - m_1 + 1} - 1}{2^{\alpha_k - m_1 + 1}} - \frac{2^{\alpha_k - m_1} - 1}{2^{\alpha_k - m_1}} = \frac{2^{m_1 - 1}}{2^{\alpha_k}} \end{aligned}$$

In the second case

$$Q_{p_k}\left(2, \alpha_k\right) = P_{p_k}\left(2, \alpha_k\right) - P_{p_k}\left(2, \alpha_k + 1\right) = P_{p_k}\left(2, \alpha_k\right) = \frac{1}{2}$$

Thus, independently of the case (i.e., for $0 < m_1 \leq \alpha_k$), $Q_{p_k}(2, m_1) = 2^{m_1-1}/2^{\alpha_k}$. Finally, the probability that $x$ is not suitable for factorization is equal to

$$1 - P_R = 2^{-\left(\sum_{k=1}^{M} \alpha_k\right)} + \sum_{m_1=1}^{\alpha_{min}} \prod_{k=1}^{M} \left(\frac{2^{m_1-1}}{2^{\alpha_k}}\right) = \frac{1 + \sum_{m_1=1}^{\alpha_{min}} \left(2^{m_1-1}\right)^M}{2^{\left(\sum_{k=1}^{M} \alpha_k\right)}} \tag{21}$$

The lower bound (1) is reached when all prime factors of $N$ may be represented as $p_k = 2\mu_k$ for odd $\mu_k$. In this case $\alpha_{min} = 1$ and $\sum_{k=1}^{M} \alpha_k = M$. The expression (21) may be also easily adapted to the case of quantum cracking of Rivest, Shamir and Adleman (RSA) cryptographic system [7], which is one of the most widely used methods for key agreement and document signing. Its security is based on the assumed computational inability to perform factoring of a modulus comprised of the product of two large prime numbers. Let modulus $N = pq$, $p = 2^\alpha \mu + 1$, $q = 2^\beta \nu + 1$. The RSA resistance to quantum attack is then described by the expression

$$P_R = 1 - \frac{1 + \sum_{m=1}^{\min(\alpha,\beta)} 4^{m-1}}{2^{\alpha+\beta}} \tag{22}$$

Equation (22) predicts minimal value of $P_R = 1/2$ for $\alpha = \beta = 1$, which is consistent with the lower bound presented in [2]. It is also in agreement with numerical Monte-Carlo estimation of probability $P_R$ for small composite numbers of the form $N = pq$ obtained in [9] and presented on Fig. 1. The numbers $\alpha$ and $\beta$ are positive integers, thus based on (22), the probability $P_R$ can take values only in discrete set. Those values are plotted by solid lines and respective combination of $\alpha$ and $\beta$ is marked on the right axis. The points on Fig. 1 which are not associated with solids lines can be assigned to other levels resulting from (22) which are not marked on the figure for clarity reasons.

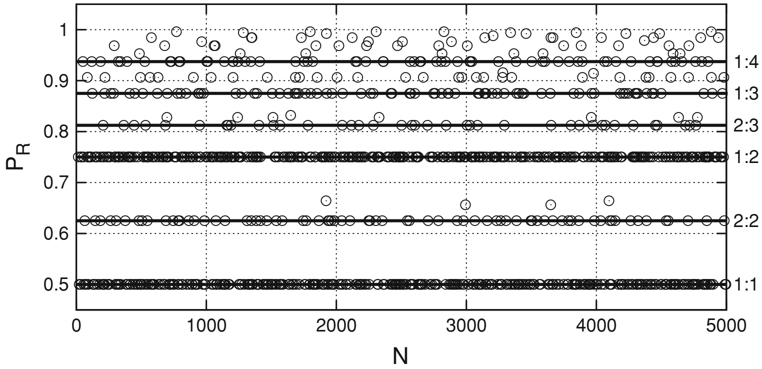

**Fig. 1** Probability of successful factorization for small composite numbers $N = pq$ computed numerically (*points*) and from (22) (*solid lines*). The values of the $\alpha$ and $\beta$ are marked on the *right* axis

## 4 Conclusion

Prior work has been focused on the analysis of the quantum portion of Shor's algorithm [1,5]. However, little attention has been paid to the properties of the classic algorithms that support its operation, and only crude estimations of their efficiency have been proposed [2]. In this study, the probabilistic behavior of classic algorithms that assist in quantum factorization was analyzed also in the context of code-breaking RSA cryptographic systems. An expression that relates factorization effectiveness with the properties of the factors forming the composite number was introduced. The derived analytical expression provides additional insight into the algorithm's properties and permits an in-depth analysis of its efficiency.

## References

1. Bourdon, P.S., Williams, H.T.: Probability estimates for Shors algorithm. Quant. Inf. Comput. **7**(5 & 6), 522–550 (2007)
2. Ekert, A., Jozsa, R.: Quantum computation and Shor's factoring algorithm. Rev. Mod. Phys. **68**(3), 733–753 (1996). doi:10.1103/RevModPhys.68.733
3. Gerjuoy, E.: Shor's factoring algorithm and modern cryptography. An illustration of the capabilities inherent in quantum computers. Am. J. Phys. **73**(6), 521–540 (2005). http://arxiv.org/pdf/quant-ph/0411184
4. Knill, E.: On Shor's quantum factor finding algorithm: Increasing the probability of success and tradeoffs involving the Fourier Transform modulus. Technical Report, LAUR-95-3350, Los Alamos National Laboratory (1995) http://www.eskimo.com/knill/cv/reprints/knill:qc1995c.ps
5. McAnally, D.: A refinement of Shor's algorithm (2001). http://xxx.lanl.gov/pdf/quant-ph/0112055
6. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
7. Rivest, R., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978). doi:10.1145/359340.359342. http://theory.lcs.mit.edu/rivest/rsapaper.pdf
8. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Sci. Stat. Comput. **26**, 1484–1509 (1997). http://www.citebase.org/abstract?id=oai:arXiv.org:quant-ph/9508027
9. Zawadzki, P.: Numerical estimation of the quantum factorization effectiveness. Theor. Appl. Inform. **22**(1), 63–72 (2010). doi:10.2478/v10179-010-0019-8