Improved Estimation of Success Probability of the Shor's Algorithm

Piotr Zawadzki

Institute of Electronics,
Silesian University of Technology,
Akademicka 16, 44-100 Gliwice, Poland
Piotr.Zawadzki@polsl.pl

Abstract. The quantum factorization is probably the most famous algorithm in quantum computation. The algorithm succeeds only when some random number with an even order relative to factorized composite integer is fed as an input to the quantum period finding algorithm. Moreover, post processing of the quantum measurement recovers the correct order only for some subset of possible values. It is well known that numbers with even orders are found with probability not less than 1/2. However, numerical simulation proves that probability of such event exhibits grouping on some discrete levels above that limit. Thus, one may conclude that usage of the common bound leads to underestimation of the successful factorization probability. Empirical formulas on expected success probability introduced in the paper give rise to the more profound analysis of classic part behaviour of the Shor's algorithm. The experimentally observed grouping still awaits for theoretical explanation.

Keywords: quantum computation, factorization.

1 Introduction

Theoretical study of quantum systems serving as computational devices has achieved tremendous progress in the last several years. There exist strong theoretical evidence that quantum computers are able to break all presently used asymmetrical algorithms whose security is based on computational complexity. Qualitative progress results from the massive parallel computation realized as the quantum system controlled evolution. The efficient function period finding seems to be one of the most stimulating development in the field, as it provides efficient solution for factorization problem, which seems to be the Holy Grail of the classic algebra. Presently, interest in the factoring problem is especially great for composite integers being a product of two large prime numbers – the ability to factor such integers is equivalent to the ability to read information encoded via the RSA cryptographic system [1]. Thus, quantum computers, if built, pose a serious challenge for the security of today's asymmetric cryptographic systems. However, the quantum factorization is a probabilistic process, unlike the classical one, and profound analysis of its efficiency is required. The algorithm random

A. Kwiecień, P. Gaj, and P. Stera (Eds.): CN 2010, CCIS 79, pp. 49–57, 2010.

behavior comes both from the inherent nature of quantum measurement and specific construction of supporting classic calculations. The researchers in the field are mainly interested in the probability of success of the quantum part and proposed many modifications improving that aspect of the original Shor's proposal [2,3]. It is reported that quantum devices are extremely reliable if multiple measurements and sophisticated post processing are employed [4]. Much less attention was devoted the classic part, although it has large impact on the overall factorization procedure efficiency. It was proved in [5] that lower bound on probability of finding parameter suitable for factorization is equal to $1/2$. The classic parameter selection failure causes entire algorithm repetition that is very undesirable as the repetitive runs of quantum device are undoubtedly costly both in terms of time and money. The fine grained formulas on the above mentioned probability are vital to overall cost estimation of the factorization procedure.

The aim of this paper is to provide an analysis of the randomness introduced by that classical part of the algorithm. The influence of that step on the overall algorithm performance one can find in [6]. Next two sections describe quantum and classic part of the quantum factorization and provide some hints about expected success probability. The methodology of the quantum factorization with classic computer is introduced in Sect. 4. The Section 5 presents simulation results and novel analytical expressions on the expected success probability.

2 Quantum Period Finding

Consider the circuit from Fig. 1. It processes the control register and the targed one composed from K and L qubits, respectively. Both registers are initialized to the state $|0\rangle$ on the start of the device. The symbol $H^{\otimes K}$ denotes the tensored product of the operator which is, in fact, an independent application of the transformation to each of the K qubits which are forming the register. The Hadamard operator applied to a single qubit $|0\rangle$ results in the state with equally likely qubits $|0\rangle$ and $|1\rangle$

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right) \tag{1}$$

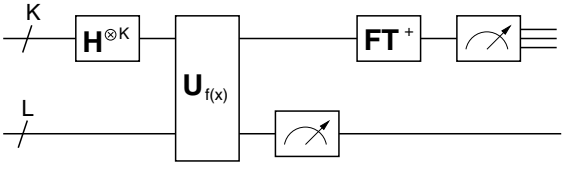

Fig. 1. Quantum circuit for period finding

The tensored product of Hadamard operators transforms the input state into equiprobable superposition of all possible configurations of the control register

$$|\psi\rangle = H^{\otimes K}|0\rangle|0\rangle = \sum_{x=0}^{M-1} |x\rangle|0\rangle \tag{2}$$

where $M = 2^K$. The unitary transformation $U_{f(x)}$ calculates the value of the function under consideration for all x

$$|\psi\rangle = \sum_{x=0}^{M-1} |x\rangle|f(x)\rangle \ . \tag{3}$$

Let the function $f(x)$ have the period r and be injective within the period. The measurement of the target register selects randomly one of the possible function values and quantum state collapses to

$$|\psi\rangle = \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} |x_0 + kr\rangle|f(x_0)\rangle \tag{4}$$

where x_0 is some random offset and $Q = \lfloor M/r \rfloor$ is the number of periods in the observed domain. The inverse Fourier transform applied to the control register extracts the random offset to the phase factor

$$\begin{aligned} |\psi\rangle = FT^{\dagger} \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} |x_0 + kr\rangle = \frac{1}{\sqrt{MQ}} \sum_{k=0}^{Q-1} \sum_{l=0}^{M-1} e^{-2\pi j \frac{l(x_0+kr)}{M}} |l\rangle = \\ = \frac{1}{\sqrt{MQ}} \sum_{l=0}^{M-1} e^{-2\pi j \frac{lx_0}{M}} \left(\sum_{k=0}^{Q-1} e^{-2\pi j \frac{lkr}{M}} \right) |l\rangle = \\ = \frac{1}{\sqrt{MQ}} \sum_{l=0}^{M-1} \frac{\sin\left(\pi \frac{lr}{M} Q\right)}{\sin\left(\pi \frac{lr}{M}\right)} e^{-2\pi j \frac{l}{M}(x_0 + r(Q-1)/2)} |l\rangle \ . \end{aligned} \tag{5}$$

The subsequent measurement of that register selects the state $|l\rangle$ with probability

$$p(l) = \frac{1}{MQ} \left(\frac{\sin\left(\pi \frac{lr}{M} Q\right)}{\sin\left(\pi \frac{lr}{M}\right)} \right)^2 \ . \tag{6}$$

When M is a multiple of r the numerator always vanishes. The probability is different from zero only when denominator also vanishes – number lr/M is an integer for $l \in [0, rM - 1]$ (Fig. 2). If M is not the multiple of r, then probability distribution has sharp peaks when lr/M is close to an integer k. Thus, from measurement output l and target register size M one has to find estimate for the fraction k/r, where k is some integer and r is unknown period. It is proved that continued fraction expansion leads to correct k/r from estimate l/M if

$$\left| \frac{l}{M} - \frac{k}{r} \right| < \frac{1}{r^2} \tag{7}$$

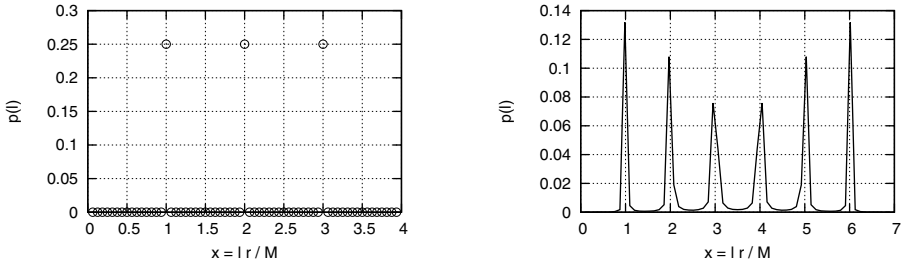

Fig. 2. Probability distribution for $r = 4$ (left) and $r = 7$ (right) with target register size $M = 2^6 = 64$

that means that one can recover k/r if measured l is sufficiently close to the local maximum. The failure probability is directly related to the width of peaks that in turn depends on the control register size [7]. Thus the confidence of quantum measurement may be enlarged to arbitrary accuracy by appropriate selection of the control register size. However, for k not being coprime to r, the estimated period would be divided by a common factor and period recovery fails.

The finding of the function period seems to be not too exciting application of quantum computers. However, the security of the RSA and ElGamal cryptosystems is based on the difficulty of exponential function ($f(x) = a^x \bmod N$) period finding. The knowledge of the function period allows for efficient modulus factorization or discrete logarithm calculation. In effect, an polynomial time period finding algorithm opens a way to breaking those asymmetrical cryptosystems.

3 Shor's Algorithm

At the core of the RSA cryptosystem security lays the assumption that factorization of the composite number formed as the product of two large primes cannot be performed in polynomial time. Presently, the best classic algorithm performs factorization in time proportional to $e^{n^{1/3}(\log n)^{2/3}}$, where n is the composite number size expressed in bits. However, the assumption of factorization ineffectiveness is purely empirical – there is no theoretical proof that this property holds even for classic computers.

The algorithm proposed in [8] completely changed the view on factorization complexity. It exploits reduction of factorization to order finding based on the following observation. Let N be the composite number and $a < N$ is coprime to N. The order of a is the smallest number such that $a^r \bmod N = 1$, thus r is the period of exponential function. If the order of a is even then one may write

$$\left(a^{r/2} - 1\right)\left(a^{r/2} + 1\right) \bmod N = 0 \tag{8}$$

and

$$p = \gcd\left(a^{r/2} - 1, N\right) \tag{9}$$

is a nontrivial factor of N provided that

$$a^{r/2} \bmod N \neq N - 1 \ . \tag{10}$$

Thus factorization of composite number N is reduced to the order finding of some number a. Classical order finding gives no advantage over other factorization algorithms as its complexity is also exponential. However, it was shown in Sect. 2 that the order of a may be determined in polynomial time with the help of the quantum computer.

4 Numerical Simulation

The following steps summarize the Shor's algorithm for quantum factorization of the composite number N:

1. Select a random number a coprime to N (otherwise $\gcd(a, N)$ is a factor of N). Only some a are good candidates as the order of a determined by the next step has to be even and condition (10) must be fulfilled.
2. Find the order of a with the quantum computer. The order is successfully recovered only for some subset of valid quantum measurements.
3. Calculate divisor p from the Equation (9) and return to the point 1) with $N = N/p$.

It is clear, that the nature of the above algorithm is probabilistic. The sources of uncertainty are twofold: the randomness of the quantum period finding and the random selection of the number a with desired properties (10). The success

```
success(N) {
  coprime=1 ;
  lucky=0 ;
  a=2 ;
  while (a<N) {
    if (gcd(a,N)==1) {
      ++coprime ;
      x=a ;
      r=1 ;
      while ( x != 1 ) {
        x=x*a mod N ;
        ++r ;
      }
      if ( r mod 2 == 0  )
        if ( a^(r/2) mod N != N-1 )
          ++lucky   ;
    }
    ++a ;
  }
return lucky/coprime ;
}
```

Fig. 3. Pseudocode for calculation of Shor's factorization success probability

probability of a quantum step is well known. However, the influence of the second factor requires further investigation. The literature on the second subject provides only a lower bound on its success probability [5]

$$p(a) \geq 1 - 2^{-(k-1)} \tag{11}$$

where k is the number of prime factors of N. That lower bound has maximal value when composite number is a product of only two prime numbers, what in fact represents the most interesting situation.

The relatively simple code is required for numeric calculation of $p(a)$ (see Fig. 3). The classic order finding algorithm has exponential complexity and very quickly becomes a daunting task for typical PC architectures. Moreover, exponentiation of a very quickly leads to register overflow of constant length integer representation. To overcome that problem one have to take advantage of library for efficient computations in arbitrary precision, what in turn, additionally slows down the program execution.

5 Results

The probability of selection of the parameter a, suitable for factorization, was calculated for composite numbers of the form $N = pq$, where p, q are taken from the list of the first 500 prime numbers. The calculated probability is shown on the Fig. 4, but due to clarity only composites not exceeding 5000 are included on the plot. The observed probabilities are always greater than $1/2$ as predicted by the bound (11). However, presented simulation results exhibit a deeper structure in probability distribution. The grouping of points around some discrete levels is evident and that indicates the existence of a class of composites less resistant to quantum factorization than others. Observed behavior comes from the factors' properties, but there is no satisfactory theoretical explanation of the obtained results in the literature known to the author.

The introduction of empirical formulas on the observed probability levels is the main contribution of the paper. The factors are primes numbers, so they have to be odd (the trivial case of factor 2 is excluded) and may be expressed as

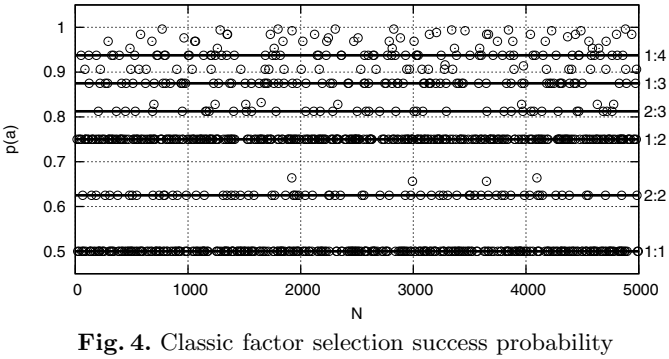

Fig. 4. Classic factor selection success probability

$$p = 2^{\alpha}\mu + 1 \ , \tag{12}$$

$$q = 2^{\beta}\nu + 1 \ . \tag{13}$$

Lets name α and β as the *parity levels* of the factors. The probability of "lucky" parameter a selection for the composite $N = pq$ is then given by the expression

$$p(a) = f(\alpha, \beta) = 1 - \frac{1 + \sum_{\delta=1}^{\min\{\alpha,\beta\}} 4^{\delta-1}}{2^{\alpha+\beta}} \ . \tag{14}$$

The levels predicted by (14) are shown on Fig. 4 as solid lines with respective values of α and β labeled on the right. The perfect matching of simulation results and theoretical predictions is visible. The points not included in the marked levels come from less probable combinations of parity levels that are not placed on figure because of clarity.

The lack of correlation between bits in the prime number representation is the one of its most useful cryptographic properties. It is also very helpful in counting prime numbers with the given parity level. The least significant bit of the prime number representation is always set to "1", as the prime number have to be odd and parity level $\alpha \geq 1$. The prime numbers with parity level $\alpha \geq 2$ have the second least significant bit set to "0", and numbers with $\alpha \geq 3$ have the second and third least significant bit set to "0", and so on. Thus probability that randomly selected prime number has parity level not less than α equals to $2^{-(\alpha-1)}$. Probability that randomly selected prime number has parity level exactly equal to α is given by

$$P(\alpha) = 2^{-(\alpha-1)} - 2^{-\alpha} = 2^{-\alpha} \ . \tag{15}$$

The above considerations have been verified experimentally. The parity level probability density function $P(\alpha)$ was computed for primes less than 10^7. The comparison of numerical experiment and theoretical consideration (15) is presented on Fig. 5.

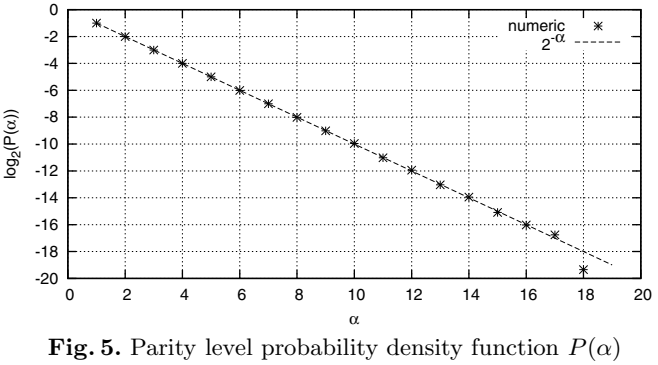

Fig. 5. Parity level probability density function $P(\alpha)$

Some interesting conclusions follow from (14) and (15). The lower bound $p(a) = 1/2$ is reached only when $\alpha = \beta = 1$. Only $P(\alpha = 1)P(\beta = 1) = 25\,\%$ composite numbers of the RSA form fulfill this condition. Thus, for $75\,\%$ factorization cases one may expect faster algorithm convergence than the one estimated from the commonly used bound (11). On average, the selection probability of the lucky parameter is equal to

$$\sum_{\alpha=1}^{\infty}\sum_{\beta=1}^{\infty} f(\alpha,\beta)P(\alpha)P(\beta) = 0.736 \ . \tag{16}$$

Also from (14) and (15). one can numerically estimate the percentage of composite numbers for which lucky parameter selection probability is above some threshold, for instance, more than $20\,\%$ composites have $p(a) > 0.9$

$$\sum_{\alpha,\beta: f(\alpha,\beta)>0.9} P(\alpha)P(\beta) = 20.5\,\% \ . \tag{17}$$

6 Conclusion

The quantum factorization algorithm represents a breakthrough in complexity theory and modern cryptography. The Shor's algorithm owes its fame to polynomial time breaking of virtually all presently used public key algorithms. Unfortunately, the practical breaking is out of reach yet because factorization of the number 15 is still one of the most complicated quantum computations [9]. However, very rapid progress in that field is observed so it is difficult to estimate the time horizon when practical computation will be in scientists' reach. The quantum factorization was analyzed many times and several modifications were proposed to the original algorithm version improving its speed and efficiency. However, the researchers were concentrated so far on the probabilistic aspect of the quantum measurement. The randomness introduced by the classical parts of the algorithm still requires further investigation. The computer simulation results presented herein expose that success rate of the algorithm is usually underestimated. Theoretical considerations are required to validate empirical formulas introduced in the paper.

References

1. 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)
2. 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)
3. McAnally, D.: A refinement of Shor's algorithm (2001)
4. Bourdon, P.S., Williams, H.T.: Probability estimates for Shors algorithm. Quant. Inf. Comput. 7(5&6), 522–550 (2007)

5. Ekert, A., Jozsa, R.: Quantum computation and Shor's factoring algorithm. Rev. Mod. Phys. 68(3), 733–753 (1996)
6. Zawadzki, P.: A numerical simulation of quantum factorization success probability. In: Tkacz, E., Kapczyski, A. (eds.) Internet – Technical Developments and Applications. Advances in Intelligent and Soft Computing, vol. 64, pp. 223–231. Springer, Heidelberg (2009)
7. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
8. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Sci. Statist. Comput. 26, 1484–1509 (1997)
9. Vandersypen, L.M.K., Steffen, M., Breyta, G., Yannoni, C.S., Sherwood, M.H., Chuang, I.L.: Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. Nature 414, 883–887 (2001)