Int J Theor Phys (2009) 48: 1945–1949
DOI 10.1007/s10773-009-9968-2

Quantum Computer Algorithm for Parity Determination Based on Quantum Counting

Hong-Fu Wang · Shou Zhang

Received: 10 December 2008 / Accepted: 11 February 2009 / Published online: 26 February 2009

Abstract A new quantum computer algorithm is proposed for determining the parity of function $f(x)$ by using quantum counting algorithm. The parity of function $f(x)$ can be determined by counting exactly the number of satisfying $f(x) = -1$, which is equivalent to determine the number of solutions, M, to an N item search problem. The algorithm can be accomplished in time of order $\Theta(\sqrt{k(N-k)})$.

Keywords Parity determination · Quantum computer · Quantum counting

Quantum computers [1], which are built based on the fundamental principle of quantum mechanics, can efficiently perform some tasks that are not feasible on a classical computer using quantum parallelism and interference effect, such as factoring problem [2], phase estimation problem [3], hidden subgroup problem [4, 5], and so on. Shor's algorithm for factorizing a large composite number can be achieved in polynomial time, which provides an exponential speedup over the best known classical algorithm [2]. The Grover algorithm gives a quadratic speedup over the most efficiently classical search algorithms for searching a marked item from an unordered database [6–8]. Most important, however, Grover quantum search algorithm did not depend for the impact on the unproven difficulty of the factorization problem. Zalka [9] has proven that the algorithm is as efficient as theoretically possible, and a variety of applications in which the algorithm is used to solve other problems [10–12]. In 1998, Brassard et al. [13] proposed a quantum counting algorithm whose aim is to determine the number of solutions, M, to an N item search problem (here M is not known in advance) by combining the ideas of Grover's and Shor's quantum algorithm.

H.-F. Wang
Center for the Condensed-Matter Science and Technology, Harbin Institute of Technology, Harbin, Heilongjiang 150001, People's Republic of China

S. Zhang (✉)
Department of Physics, College of Science, Yanbian University, Yanji, Jilin 133002, People's Republic of China
e-mail: szhang@ybu.edu.cn

Mosca [14] also proposed a quantum counting algorithm from the point of view of quantum eigenvalue estimation. Quantum Fourier transform based phase estimation procedure enables us to estimate the solutions, M, using $\Theta(\sqrt{N})$ oracle applications, while on a classical computer it takes $\Theta(N)$ consultations with an oracle to determine M. The power of quantum computation is based on the fact that the quantum state of a quantum computer can be a superposition of basis states and we can simultaneously perform the unitary operations on multiple quantum states.

In 1998, Farhi et al. [15] proposed a quantum algorithm for determining the parity problem with a sequence of unitary operators. In the algorithm, Farhi et al. established the lower bound of determining the parity of a function $f(x)$, i.e., at least $N/2$ applications of oracle should be performed to determine the parity. Thus Farhi et al. pointed out that the quantum computer had a limit on the speed of quantum computation and a quantum computer could not outperform a classical computer in determining parity. Subsequently, Stadelhofer et al. [16] proposed another quantum algorithm for determining the parity of a string of N binary digits. The algorithm required a sequence of unitary operations to be performed and $N/2$ oracle to be calculated. Comparing with Ref. [15], Stadelhofer et al.'s algorithm only required a single qubit measurement, while n measurements must be made in Ref. [15]. Thus Stadelhofer et al.'s algorithm was optimal in the sense of Ref. [15]. In this paper, we propose a new and fast quantum computer algorithm for solving the parity problem. The proposed algorithm is, in fact, equivalent to the quantum counting algorithm in Refs. [13, 14], except the process of implementation of Grover quantum iteration is done using different basis and unitary operators. The parity of function $f(x)$ can be determined by counting the number of satisfying $f(x)=-1$, which is equivalent to determine the number of solutions, M, to an N item search problem. We discuss the lower and upper bounds of the algorithm in different cases.

Now we briefly review the basic property of the parity problem. Given a function $f(x)$,

$$f(x)=\pm 1, \quad \text{for } x=1,2,\ldots,N. \tag{1}$$

Here x is defined on the integers from 1 to N and $f(x)$ takes the values either $+1$ or -1. The parity of $f(x)$ is defined as the product of $f(x)$ over all the values which x can take, that is,

$$P(f)=\prod_{x=1}^{N} f(x)=\pm 1. \tag{2}$$

The most efficient classical algorithm for this problem is to calculate the function $f(x)$ over all x from 1 to N one by one, requiring N oracle calls.

Before proposing our algorithm for determining the parity of function $f(x)$, we first introduce the Grover iteration and its performance revealed in Refs. [13, 14]. The Grover iteration operator in quantum search algorithm has the following form,

$$\mathcal{G}=\mathcal{W}\mathcal{U}_x\mathcal{W}^{-1}\mathcal{U}_f, \tag{3}$$

where $\mathcal{U}_f$ is an unitary operator of calculating the function $f(x)$ defined as $\mathcal{U}_f: |x\rangle \to (-1)^{f(x)}|x\rangle$, $\mathcal{W}$ is the Walsh-Hadamard transform defined as $\mathcal{W}: |i\rangle \to (1/\sqrt{2}) \sum_{j=0}^{1}(-1)^{ij}|j\rangle$, and $\mathcal{U}_x$ is defined as $\mathcal{U}_x: |x\rangle \to -(-1)^{\delta_{x,0}}|x\rangle$.

Initially, the state of the system in the search problem is

$$|\varphi\rangle_0=\mathcal{W}^{\otimes n}|00\ldots 0_n\rangle=\frac{1}{N^{1/2}}\sum_{x=0}^{N-1}|x\rangle, \tag{4}$$

where $N = 2^n$. Define the new normalized basis vectors

$$|\nu\rangle = \frac{1}{\sqrt{M}}\sum_x^{\alpha} |x\rangle, \tag{5}$$

$$|\mu\rangle = \frac{1}{\sqrt{N-M}}\sum_x^{\beta} |x\rangle. \tag{6}$$

Here $\sum_x^{\alpha}$ and $\sum_x^{\beta}$ represent the sums over all x which correspond to M searched items and $N-M$ unsearched items to the search problem, respectively. Thus the initial state of the system can be written as [14]

$$\begin{aligned} |\varphi\rangle_0 &= \sin(\pi\theta_M)|\nu\rangle + \cos(\pi\theta_M)|\mu\rangle \\ &= \frac{-\mathrm{i}e^{\mathrm{i}\pi\theta_\mathrm{M}}}{\sqrt{2}}|\psi_\alpha\rangle + \frac{\mathrm{i}e^{-\mathrm{i}\pi\theta_\mathrm{M}}}{\sqrt{2}}|\psi_\beta\rangle, \end{aligned} \tag{7}$$

where $|\psi_\alpha\rangle = 1/\sqrt{2}(|\nu\rangle + \mathrm{i}|\mu\rangle)$ and $|\psi_\beta\rangle = 1/\sqrt{2}(|\nu\rangle - \mathrm{i}|\mu\rangle)$, which are the eigenvectors of the iteration operator $\mathcal{G} = \mathcal{W}\mathcal{U}_x\mathcal{W}^{-1}\mathcal{U}_f$ with eigenvalues $e^{2\pi\mathrm{i}\theta_M}$ and $e^{-2\pi\mathrm{i}\theta_M}$, respectively. $0 \le \theta_M \ge \frac{1}{2}$, with

$$\cos(2\pi\theta_M) = 1 - \frac{2M}{N}, \quad \sin(2\pi\theta_M) = \frac{2\sqrt{M(N-M)}}{N} \quad \text{and} \quad \sin(\pi\theta_M) = \sqrt{\frac{M}{N}}. \tag{8}$$

From (8) we can see that the number of the solutions, M, can be obtained if we can calculate the value of θ_M.

We now give a quantum algorithm for determining the parity of function $f(x)$ by applying the iteration operator $\mathcal{G}$ mentioned above. Here, for convenience, we assume that the maximal value that x can take for function $f(x)$ is $N = 2^n$, and the number of satisfying $f(x) = -1$ is k. The algorithm consists of the following steps.

Step (i)—Initialize the registers in the state

$$|\Psi\rangle_0 = \frac{1}{\sqrt{p}}\sum_{z=0}^{p-1}|y\rangle_1 \otimes \frac{1}{\sqrt{2N}}\sum_{x=0}^{2N-1}|x\rangle_2 \otimes |q\rangle_3. \tag{9}$$

Step (ii)—Apply the iteration operator $\mathcal{G}$ y times when the state of the first register is $|y\rangle$. Here we should point out that when the function $f(x)$ is evaluated using operator $\mathcal{U}_f$ in the process of iteration, the function $f(x)$ satisfies the following conditions

$$f(x) = \begin{cases} f(x), & \text{for } 1 \le x \le N, \\ +1, & \text{for } x = 0 \text{ and } N < x \le 2N-1. \end{cases} \tag{10}$$

Step (iii)—Apply the inverse quantum Fourier transform F_t^-, which maps each state $|a\rangle$ into a superposition given by $F_t^-|a\rangle = \frac{1}{\sqrt{2^t}}\sum_{c=0}^{2^t-1} e^{-2\pi\mathrm{i}ac/2^t}|c\rangle$ with t is the number of qubits, to the first register. We have

$$|\Psi\rangle_0 \longrightarrow \frac{-\mathrm{i}e^{\mathrm{i}\pi\theta_k}}{\sqrt{2}p}\sum_{z=0}^{p-1}\sum_{y=0}^{p-1} e^{2\pi\mathrm{i}y(\theta_k - z/p)}|z\rangle_1 \otimes |\psi_\alpha\rangle_2 \otimes |q\rangle_3$$

$$+\frac{\mathrm{i}e^{-\mathrm{i}\pi\theta_k}}{\sqrt{2}p}\sum_{z=0}^{p-1}\sum_{y=0}^{p-1}e^{-2\pi\mathrm{i}y(\theta_k+z/p)}|z\rangle_1\otimes|\psi_\beta\rangle_2\otimes|q\rangle_3$$

$$=\frac{-\mathrm{i}e^{\mathrm{i}\pi\theta_k}}{\sqrt{2}p}|\widetilde{\theta_k}\rangle_1\otimes|\psi_\alpha\rangle_2\otimes|q\rangle_3+\frac{\mathrm{i}e^{-\mathrm{i}\pi\theta_k}}{\sqrt{2}p}|\widetilde{-\theta_k}\rangle_1\otimes|\psi_\alpha\rangle_2\otimes|q\rangle_3, \qquad (11)$$

where $\sin(\pi\theta_k)=\sqrt{\frac{k}{2N}}$ and $\widetilde{\theta_k}$ is a close estimate of θ_k with high precision.

Step (iv)—Measure the first register, obtaining

$$\theta_k=\begin{cases} z/p, & \text{for } 0\le z\le p/2,\\ 1-z/p, & \text{for } p/2<z\le p. \end{cases} \qquad (12)$$

Finally, we substitute the value of θ_k into the equation $\sin(\pi\theta_k)=\sqrt{\frac{k}{2N}}$ and obtain the exact value of k that is the number of satisfying $f(x)=-1$ with high precision through simple calculation. In this way we can determine the parity of function $f(x)$ depending on the value of k, namely,

$$P(f)=\begin{cases} +1, & \text{if } k \text{ is an even integer},\\ -1, & \text{if } k \text{ is an odd integer}. \end{cases} \qquad (13)$$

In the above algorithm, we add a qubit in the second register making the range of x for $f(x)$ from $1\le x\le N$ to $0\le x\le 2N-1$, which ensures that $0\le\frac{k}{2N}\le\frac{1}{2}$ and makes the algorithm can be successfully implemented during the process of applying Grover iterations. The expected running time of the whole algorithm for determining exactly k requires $\Theta(\sqrt{k(N-k)})$ iterations of $\mathcal{G}$ and the success probability of correctly determining k is at least $2/3$.

Let us now consider when different values of k are chosen, the influence to the running time of the proposed algorithm. It can be easily obtained that when $k\ll N$, we need approximately $\Theta(\sqrt{N})$ iterations of $\mathcal{G}$. An interesting special case occurs when $k=N/2$. In this case we need $N/2$ iterations of $\mathcal{G}$, which has the same computing complexities as the quantum algorithms that require at least $N/2$ oracle calls proposed in Refs. [15, 16]. For the other values of k, the computing complexity of our algorithm is less than $N/2$. In Fig. 1, we plot the required iteration times of $\mathcal{G}$ for implementing the proposed algorithm when different values of k are chosen, and we can see that our algorithm is faster than the algorithms in Refs. [15, 16].

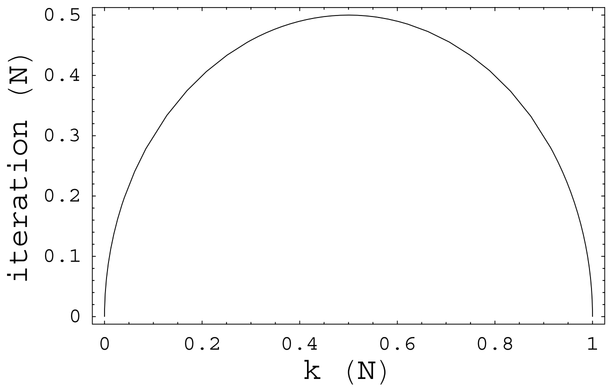

Fig. 1 The required iteration times of $\mathcal{G}$ for achieving the algorithm corresponding to different values of k

In conclusion, we have proposed a fast quantum computer algorithm for determining the parity of function $f(x)$ based on quantum counting algorithm. In contrast to Refs. [15, 16] in which at least $N/2$ oracle calls were required to determine the parity, our algorithm required less than $N/2$ applications of the unitary operator $\mathcal{U}_f$, which led to a potential speed up for determining the parity.

Acknowledgement This work was supported by the National Natural Science Foundation of China under Grant No. 60667001.

References

1. Fernman, R.P.: Int. J. Theor. Phys. **21**, 467 (1982)
2. Shor, P.W.: In: Proceedings of the Symposium on the Foundations of Computer Science, Los Alamitos, California, 1994, pp. 124–134. IEEE Computer Society Press, New York (1994)
3. Kitaev, A.Y.: quant-ph/9511026
4. Simon, D.: In: Proceedings of the Symposium on the Foundations of Computer Science, Los Alamitos, California, 1994, pp. 116–123. IEEE Computer Society Press, New York (1994)
5. Jozsa, R.: quant-ph/9707033
6. Grover, L.K.: Phys. Rev. Lett. **79**, 325 (1997)
7. Grover, L.K.: Phys. Rev. Lett. **79**, 4709 (1997)
8. Grover, L.K.: Phys. Rev. Lett. **80**, 4329 (1998)
9. Zalka, C.: quant-ph/9711070 (1997)
10. Brassard, G., Hoyer, P., Tapp, A.: quant-ph/9705002 (1997)
11. Terhal, B.M., Smolin, J.A.: Phys. Rev. A **58**, 1822 (1998)
12. Farhi, E., Gutmann, S.: Phys. Rev. A **57**, 2403 (1998)
13. Brassard, G., Høyer, P., Tapp, A.: quant-ph/9805082 (1998)
14. Mosca, M.: Theor. Comput. Sci. **264**, 139 (2001)
15. Farhi, E., Goldstone, J., Gutmann, S., Sipser, M.: Phys. Rev. Lett. **81**, 5442 (1998)
16. Stadelhofer, R., Suter, D., Banzhaf, W.: Phys. Rev. A **71**, 032345 (2005)