Available online at www.sciencedirect.com
ScienceDirect
Physics Letters A 366 (2007) 42–46
PHYSICS LETTERS A
www.elsevier.com/locate/pla

Phase matching in Grover's algorithm ☆

Panchi Li [a,b,*], Shiyong Li [a]

[a] Department of Control Science and Engineering, Harbin Institute of Technology, Harbin 150001, China
[b] Department of Computer Science and Engineering, Daqing Petroleum Institute, Daqing 163318, China

Received 29 October 2006; received in revised form 4 February 2007; accepted 5 February 2007

Available online 13 February 2007

Communicated by P.R. Holland

Abstract

When the Grover's algorithm is applied to search an unordered database, the probability of getting correct results usually decreases with the increase of marked items. The reason for this phenomenon is analyzed in this Letter, the Grover iteration is studied, and a new phase matching is proposed. With application of the new phase matching, when the fraction of marked items is greater than $1/3$, the probability of getting correct results is greater than $25/27$ with only one Grover iteration. The validity of the new phase matching is verified by a search example.

Keywords: Quantum computing; Quantum searching; Grover algorithm; Phase matching

1. Introduction

Grover's quantum search algorithm [1] is one of the most important developments in quantum computation. For searching a marked state in an unordered database, it achieves quadratic speed up over classical search algorithms. At present, Grover's quantum search algorithm has been greatly noticed and has become a challenging research field. However, the Grover's algorithm also has some limitations. When the fraction of marked items is greater than a quarter of the total items in the database, the success probability will rapidly decrease, and when the fraction of marked items is greater than half of the total items in the database, the algorithm will be disabled.

Up to now, many methods of improving Grover's algorithm have been proposed. The Grover's original algorithm consists of inversion of the amplitude in the desired state and inversion-about-average operation [1]. In [2], Grover presented a general algorithm: $Q = -I\gamma U^{-1} I\tau U$, where U is any unitary operation, U^{-1} is the adjoint of U, $I\gamma = I - 2|\gamma\rangle\langle\gamma|$, $I\tau = I - 2|\tau\rangle\langle\tau|$, $|\gamma\rangle$ is an initial state and $|\tau\rangle$ is a desired state. When $U^{-1} = U = W$, where W is the Walsh–Hadamard transformation, and $|\gamma\rangle = 0$, the general algorithm becomes the original algorithm. Long extended Grover's algorithm [3]. In Long's algorithm, $I\gamma$ and $I\tau$ are expressed as

$$I\gamma = I - \left(1 - e^{i\theta}\right)|\gamma\rangle\langle\gamma| \quad \text{and} \quad I\tau = I - \left(1 - e^{i\varphi}\right)|\tau\rangle\langle\tau|,$$

respectively. When $\theta = \varphi = \pi$, Long's algorithm becomes Grover's general algorithm. Li et al. proposed that U^{-1} in Long's algorithm can be replaced by any unitary operation V [4,5]. Biham generalized the Grover's algorithm to deal with an arbitrary pure initial state and an arbitrary mixed initial state [6,7]. In [8], Grover presented the new algorithm by replacing the selective inversions by selective phase shifts of $\pi/3$. Li et al. studied the fixed-point search algorithm obtained by replacing equal phase shifts of $\pi/3$ by different phase shifts [9].

The methods mentioned above cannot solve the problem that the algorithm efficiencies decrease as the marked items increase. In this Letter, we study the phase matching in Grover's algorithm, and propose a new matching, namely, $\theta = -\varphi = \pi/2$ that is different from the conclusion of Ref. [3]. When the fraction of marked items is greater than $1/3$, with application of this new phase matching, the success probability is greater than $25/27$ with only one Grover iteration.

This Letter is organized as follows. In Section 2, we introduce Grover's algorithm and its drawbacks. Section 3 is used to

☆ The Letter was supported by NSFC (Grant No. 50138010).
* Corresponding author at: Department of Control Science and Engineering, Harbin Institute of Technology, Harbin 150001, China.
E-mail address: lipanchi@vip.sina.com (P. Li).

0375-9601/$ – see front matter
doi:10.1016/j.physleta.2007.02.029

propose a new phase matching with the higher success probability. Section 4 gives an example to verify the validity of new phase matching. Section 5 summarizes the whole Letter.

2. Grover's algorithm and its problem

2.1. Grover's algorithm summary

Suppose we wish to search through a search space of N elements. Rather than search the elements directly, we concentrate on the *index* to those elements, which is just a number in range 0 to $N-1$. For convenience we assume $N=2^n$, so the index can be stored in n bits, and that the search problem has exactly M solutions, with $1 \leqslant M \leqslant N$.

The algorithm begins with the state $|0\rangle^{\otimes n}$. The Walsh–Hadamard transform is used to put the state $|0\rangle^{\otimes n}$ in the equal superposition state,

$$|\phi\rangle = \frac{1}{N^{1/2}} \sum_{x=0}^{N-1} |x\rangle. \tag{1}$$

The Grover quantum search algorithm then consists of repeated application of a quantum subroutine, known as the *Grover iteration* or *Grover operator*, which we denote G. The Grover iteration may be broken up into four steps:

(1) Apply the oracle O. The oracle is a unitary operator defined by its action on the computational basis

$$|x\rangle|q\rangle \xrightarrow{O} |x\rangle\big|q \oplus f(x)\big\rangle \tag{2}$$

where $|x\rangle$ is the index register, $\oplus$ denotes addition modulo 2, and the oracle qubit $|q\rangle$ is a single qubit which is flipped if $f(x)=1$, and is unchanged otherwise.

(2) Applying the Walsh–Hadamard transform $H^{\otimes n}$.

(3) Perform a conditional phase shift, with every computational basis state except $|0\rangle$ receiving a phase shift of -1, $|x\rangle \to -(-1)^{\delta_{x0}}|x\rangle$.

(4) Applying the Walsh–Hadamard transform $H^{\otimes n}$.

It is useful to note that the combined effect of steps 2, 3, and 4 is

$$H^{\otimes n}\big(2|0\rangle\langle 0| - I\big)H^{\otimes n} = 2|\phi\rangle\langle\phi| - I \tag{3}$$

where $|\phi\rangle$ is the equally weighted superposition of states, (1). Thus the Grover iteration, G, may be written as $G = (2|\phi\rangle\langle\phi| - I)O$.

Let $\lambda = M/N$, and let $CI(x)$ denote the integer closest to the real number x, where by convention we round halves down. Then repeating the Grover iteration

$$R = CI\left(\frac{\arccos\sqrt{\lambda}}{2\arcsin\sqrt{\lambda}}\right) \tag{4}$$

times rotates $|\phi\rangle$ to within an angle $\arcsin\sqrt{\lambda} \leqslant \pi/4$ of a superposition state of marked states [10]. Observation of the state in the computational basis then yields a solution to the search problem with probability at least one-half.

2.2. The success probability of Grover's algorithm

In fact, the Grover iteration can be regarded as a rotation in the two-dimensional space spanned by the starting vector $|\phi\rangle$ and the state consisting of a uniform superposition of solutions to the search problem. Let $|\alpha\rangle$ represent a normalized states of a sum over all x which are not solutions to the search problem, and $|\beta\rangle$ represent a normalized states of a sum over all x which are solutions to the search problem. Simple algebra shows that the initial state $|\phi\rangle$ may be re-expresses as

$$|\phi\rangle = \cos(t)|\alpha\rangle + \sin(t)|\beta\rangle \tag{5}$$

where $t = \arcsin\sqrt{\lambda}$. After R Grover iteration, the initial state is taken to

$$G^R|\phi\rangle = \cos\big((2R+1)\arcsin\sqrt{\lambda}\big)|\alpha\rangle + \sin\big((2R+1)\arcsin\sqrt{\lambda}\big)|\beta\rangle. \tag{6}$$

Hence, the success probability is

$$P = \sin^2\big((2R+1)\arcsin\sqrt{\lambda}\big). \tag{7}$$

The curve of P is shown in Fig. 1.

2.3. The drawback of Grover's algorithm

It is easy to deduce from Eqs. (4) and (7) that $P_{\lambda=0.14645} = 0.85356$, $P_{\lambda=0.25} = 1.00$, $P_{\lambda=0.50} = 0.50$, and when $\lambda \in (0.14645, 0.50)$, $R=1$. Namely, when $\lambda = 0.25$, P_λ is maximum; when $\lambda > 0.25$, P_λ decreases rapidly; when $\lambda = 0.5$, P_λ is minimum; when $\lambda > 0.5$, there is $R=0$, $P_\lambda = \lambda$, and the algorithm is disabled. Hence, the Grover's algorithm is no longer useful when $\lambda > 0.25$.

The reason for the problem is that the two phase rotations in Grover iteration are fully equivalent in both amplitude and direction, namely π. According to Ref. [10], the result of such phase rotations is that, for the one Grover iteration, the phase of the $|\phi\rangle$ increases $2\arcsin\sqrt{\lambda}$ radian. When $0 < \lambda \leqslant 0.25$, the $|\phi\rangle$ will gradually approach to the $|\beta\rangle$, and when $\lambda > 0.25$, the $|\phi\rangle$ will rapidly keep away from the $|\beta\rangle$.

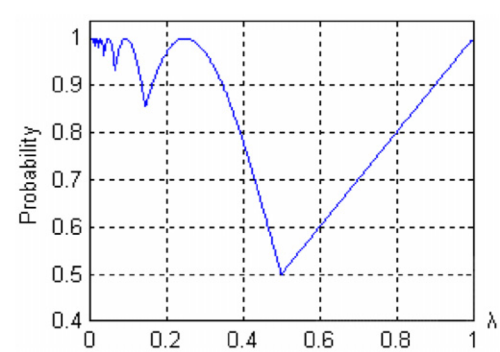

Fig. 1. The success probability curve of Grover's algorithm.