A family of sure-success quantum algorithms for solving a generalized Grover search problem

Chia-Ren Hu
Department of Physics, Texas A& M University, College Station, Texas 77843-4242

(Jan. 12, 2002)

This work considers a generalization of Grover's search problem, *viz.*, to find any one element in a set of acceptable choices which constitute a fraction f of the total number of choices in an unsorted data base. An infinite family of sure-success quantum algorithms are introduced here to solve this problem, each member for a different range of f. The nth member of this family involves n queries of the data base, and so the lowest few members of this family should be very convenient algorithms within their ranges of validity. The even member $\mathcal{A}_{2n}$ of the family covers ever larger range of f for larger n, which is expected to become the full range $0 \leq f \leq 1$ in the limit $n \to \infty$.

PACS numbers:

Quantum computing as a new powerful approach to solve difficult computational problems is still in its infancy. Only a handful useful algorithms have been proposed so far. Most of them fall into two categories: Those for factorizing large integers, and those for "searching a needle in a haystack", or finding the only acceptable element in a large unsorted data base. The main idea in the former category is due to Shor, [1] and in the latter category is due to Grover. [2] Here we wish to consider a generalization of Grover's search problem, *viz.*, to find any one element in a set of acceptable choices which form a fraction f of the total number of choices in an unsorted data base of size N. [3] An infinite family $\{\mathcal{A}_n \,|\, n = 1, 2, 3, \cdots\}$ of qunatum algorithms is introduced here, each similar to one stage of Grover's algorithm, except that, unlike Grover's original algorithm, which requires iteration to some optimal stage, which in general is still not a sure-success algorithm, [4] here each member is an independent sure-success algorithm within its range of validity. Each member of the family introduced here is characterized by an iteration number, n, in the sense introduced in the original Grover algorithm. This number is also the number of times the data base is queried. Here we only analyze four members of this family, corresponding to the iteration numbers 1,2, 4, and 6. We find that $\mathcal{A}_1$ is valid for $0.25 \leq f \leq 1.0$; $\mathcal{A}_2$ is valid for $0.095491502 \cdots \leq f \leq 0.65450849 \cdots$; $\mathcal{A}_4$ is valid for $0.030153689 \cdots \leq f \leq 0.88302222 \cdots$; and $\mathcal{A}_6$ is valid for $0.014529091 \cdots \leq f \leq 0.94272801 \cdots$. These results strongly indicate that by using $\mathcal{A}_{2n}$ of ever larger n, an ever larger range of f can be covered which in the limit of $n \to \infty$ approaches the full range $0 \leq f \leq 1$, but a general proof has not yet been obtained. The validity or non-validity of this statement, and the properties of the odd members of this family, will be discussed in a future work. All members of this family of algorithms are characterized by two phase parameters, θ and ϕ. These two parameters are individually adjusted in order to make each member a sure-success algorithm. I find that (i) at least for the members $\mathcal{A}_2$, $\mathcal{A}_4$, $\mathcal{A}_6$, but most-likely also for all higher even members of the family, $\phi = 2\theta$ is an acceptable choice for ϕ, (ii) for each of the even members $\mathcal{A}_2$, $\mathcal{A}_4$, $\mathcal{A}_6$, and most-likely also for each of all higher even members of the family, the required value for θ for it to work is a unique function of f just inside the boundary of its validity range of f, but the number of acceptable values of θ graduately increases to n deep inside the validity f-range for $\mathcal{A}_{2n}$. The algorithm member $\mathcal{A}_1$, on the other hand, requires $\phi = -2\theta$, then θ depends uniquely on f within the validity range. No other odd members have yet been analyzed. In all cases studied, I find the required θ and ϕ to be independent of N, and to only depend on f. There is strong indication that this statement is true for all members of the family.

All members of this family $\{\mathcal{A}_n \,|\, n = 1, 2, 3, \cdots\}$ are achieved with two unitary operators which generalize the two corresponding operators introduced by Grover:

In a Hilbert space spanned by a set of N orthonormal basis states $\{\,|i> \,|\, n = 1, 2, 3, \cdots, N\}$, each of which represents one element of the data base, Grover introduced an *unitary* operator, which I shall denote as $\hat{F}_\nu$, which changes the sign of the ν's amplitude C_ν in any quantum state $|\Psi >= \sum_{i=1}^{N} C_i \,|i>$. This operator is generalized to the operator $\hat{F}_\phi^{(a)}$, which introduces the extra phase factor $-e^{i\phi}$ to each of the amplitudes $\{C_\nu \,|\, \nu \in a\}$, where a denotes the set of acceptable elements in the data base. [5] Mathematically,

$$\hat{F}_\phi^{(a)} \equiv \hat{I} - (e^{i\phi} + 1) \sum_{\nu \in a} |\nu >< \nu| \,. \tag{1}$$

where $\hat{I} \equiv \sum_{i=1}^{N} |i >< i|$ is the identity operator. For $\phi = 0$, and a containing only one element ν, this operator reduces to the operator F_ν introduced by Grover.

A second *unitary* operator introduced by Grover is the "inversion about the mean" operator, which can be written in the form:

$$\hat{O} \equiv \sum_{i,j} [(2/N) - \delta_{i,j}] \,|i >< j|. \tag{2}$$

I generalize it to

$$\hat{O}_\theta \equiv \sum_{i,j} [(2\cos\theta/N) - e^{i\theta}\delta_{i,j}]\,|i><j|\,, \tag{3}$$

which reduces to Grover's "inversion about the mean" operator if $\theta = 0$. That $\hat{O}_\theta$ is unitary can be easily verified. It is also easy to show that it is the most general unitary operator of the form $\sum_{i,j}[(A + B\delta_{i,j}]\,|i><j|$, if one disregards an unimportant overall phase factor. I am not aware of any earlier published work introducing this umitary operator.

Since $\hat{F}_\phi^{(a)}$ and $\hat{O}_\theta$ are both complex operators, I also need their hermitian conjugate operators, $F_\phi^{(a)\,\dagger}$ and $\hat{O}_\theta^\dagger$, which are also the inverse operators of $\hat{F}_\phi^{(a)}$ and $\hat{O}_\theta$, respectively. Actually they are simply $\hat{F}_{-\phi}^{(a)}$ and $\hat{O}_{-\theta}$.

Before any algorithm is applied, every element in the data base should be regarded as to have equal probability of being the right choice. Grover represented this fact by starting with the quantum state:

$$|\Psi_0>= (1/\sqrt{N}) \sum_i^N |i>\,,$$

i.e., the state with every $C_i = 1/\sqrt{N}$, so that the probability of finding any element of the data base is $|C_i|^2 = 1/N$. The quantum algorithm he introduced is to repreatedly apply the unitary operator product $\hat{O}\hat{F}_\nu$ n times on the state $|\Psi_0>$, followed by a measurement to cause the state to collapse to one of the basis states. He showed that when n is of an optimal value of the order of $\sqrt{N}$, All $|C_i|^2$ will be very close to zero except the particular one $|C_\nu|^2$, corresponding to the desirable element ν in Grover's search problem, which will be very close to unity. However, except for some special values of N, one will not obtain exact unity for $|C_\nu|^2$, and exact zero for all other $|C_i|^2$. Thus Grover algorithm is in general not a sure-success alorithm, even in theory, when potenial implementation errors are not taken into account. We generalize Grover's algorithm to a family of *sure-success* algorithms, each member of which is characterized by an integer n. Denoting these member algorithms as $\{\mathcal{A}_n\}$, then the even $[(2n)\text{th}]$ member $\{\mathcal{A}_{2n}\}$ are defined as applying the unitary operator product $\hat{\Lambda} \equiv \hat{O}_\theta^\dagger \hat{F}_\phi^{(a)\,\dagger} \hat{O}_\theta \hat{F}_\phi^{(a)}$ n times to the state $|\Psi_0>$, followed by the same measurement used in the Grover algorithm. The odd $[(2n+1)th]$ member $\{\mathcal{A}_{2n+1}\}$, is to apply the unitary operator product $\hat{O}_\theta \hat{F}_\phi^{(a)} \hat{\Lambda}^n$ to the state $|\Psi_0>$, before the same measurement is made. Thus $\{\mathcal{A}_n\}$ makes n queries of the data base. "Sure success" of each of these algorithms is achieved by adjusting the two parameters θ and ϕ so that all $|C_i|^2$, with i not belonging to the set a of the generalized Grover search problem introduced here, are exactly zero. All $|C_i|^2$ with $i \in a$ will then be exactly equal to $1/(fN)$, where $fN \equiv N_a$ is the number of elements in the set a, since probability is conserved by unitary operations. Below we show how this is done explicitly for the four members $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{A}_4$, and $\mathcal{A}_6$. After that I will speculate about all even members $\mathcal{A}_{2n}$ of the family, leaving the odd members higher than the first to be discussed in a later work.

Consider first the algorithm member $\mathcal{A}_1$. One has the identity:

$$\hat{O}_\theta \hat{F}_\phi^{(a)} |\Phi_0>= [2\cos\theta(1 - f - fe^{i\phi}) - e^{i\theta}\hat{F}_\phi^{(a)}]|\Phi_0>\,. \tag{4}$$

Since the operator $\hat{F}_\phi^{(a)}$ is equivalent to an identity operator in the subspace corresponding to all unacceptable elements of the data base, sure success of this algorithm is achieved by demanding

$$2\cos\theta(1 - f - fe^{i\phi}) - e^{i\theta} = 0\,. \tag{5}$$

which has the solution $\phi = -2\theta$, and

$$\theta = (1/2)\cos^{-1}[(1/2f) - 1]\,. \tag{6}$$

Note that if $(\phi,\,\theta)$ is a solution, then $(-\phi,\,-\theta)$ is also a solution. This is true for all higher members of the family also, and one can easily see why. Equation (6) has solution only for $1/4 \le f \le 1$, which is the validity range of this algorithm. Within this range, I have plotted θ as a function of f in Fig. 1 assuming $\theta > 0$. The following special cases are of interest: (i)

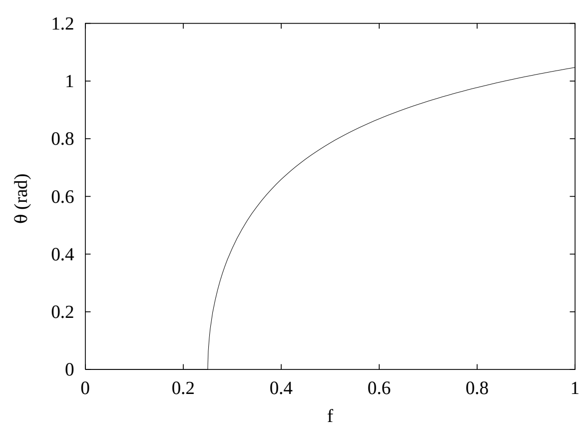

FIG. 1. Plotted is θ versus f for the algorithm $\mathcal{A}_1$.

For $f = 1/4$, I find $\phi = \theta = 0$, and the operators reduce to those introduced by Grover, and this algorithm becomes a special case of Grover's algorithm. (ii) For $f = 1/3$, I find $\phi = \pm\pi/3$ and $\theta = \mp\pi/6$. (iii) For $f = 1/2$, I find $\phi = \pm\pi/2$, and $\theta = \mp\pi/4$. (iv) For $f = 2/3$, I find $\phi = \pm 104.477\cdots^\circ = \pm 0.580430...\pi$ and $\theta = \mp 52.2387\cdots^\circ = \mp 0.290215\cdots\pi$. Finally, (v) for $f = 1$, I find $\phi = \pm 2\pi/3$, and $\theta = \mp\pi/3$, but in this case the operator product $\hat{O}_\theta \hat{F}_\phi^{(a)}$ acting on $|\Phi_0>$ simply reproduces $|\Phi_0>$.

Next, let us consider the second member $\mathcal{A}_2$. One has the identity:

$$\begin{aligned}\hat{\Lambda}|\Phi_0> &= \{[(2\cos\theta)^2|(1-f-fe^{i\phi})|^2 - e^{2i\theta}] \\ &\quad -(2\cos\theta)e^{-i\theta}(1-f-fe^{i\phi})\hat{F}_\phi^{(a)\dagger}\}|\Phi_0> \\ &\equiv (A_1 - B_1\hat{F}_\phi^{(a)\dagger})|\Phi_0> \ . \end{aligned} \tag{7}$$

(Note that $A_1 = |B_1|^2 - e^{2i\theta}$.) Thus to ensure that this is a sure-success algorithm, one needs only demand $A_1 - B_1 = 0$. The imaginary part of this condition can be written as

$$\mathrm{Im}(A_1 - B_1) = (2f\cos\theta)[\sin(\phi-\theta) - \sin\theta)] = 0\,. \tag{8}$$

so it can be satisfied with $\phi = 2\theta$. (It is easy to see that $\cos\theta \neq 0$.) Then the real part of this condition reduces to

$$\mathrm{Re}(A_1 - B_1) = 1 + 4f\mu^2 - 16f(1-f)\mu^4 = 0 \tag{9}$$

where $\mu \equiv \cos\theta$. It has the solution

$$\theta = \frac{1}{2}\cos^{-1}\{\frac{1}{4(1-f)}[\sqrt{\frac{4}{f} - 3} + (4f-3)]\}\,, \tag{10}$$

This equation has solution only if $0.095491502\cdots \leq f \leq 0.65450849\cdots$. Within this range, I have plotted θ as a function of f for this algorithm in Fig. 2, assuming $\theta > 0$.

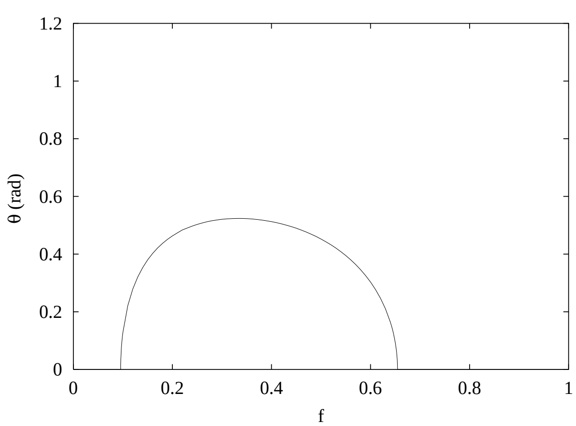

FIG. 2. Plotted is θ versus f for the algorithm $\mathcal{A}_2$.

Note that with the lagorithm $\mathcal{A}_2$ we can cover f down to slightly below 0.1.

Next, let us consider the algorithm member $\mathcal{A}_4$, leaving $\mathcal{A}_3$ and higher odd members for future discussion, since they are deemed less important. I have first established the following theorem: If $\hat{\Lambda}^n|\Psi_0>= [A_n - B_n F_\phi^{(a)\dagger}]|\Psi_0>$, then

$$\begin{aligned}\hat{\Lambda}^{n+1}|\Psi_0> &= \{[A_1A_n - e^{-2i\theta}B_1^*B_n] \\ &\quad -[B_1A_n - e^{-2i\theta}B_n]F_\phi^{(a)\dagger}\}\,|\Psi_0> . \end{aligned} \tag{11}$$

That is,

$$\begin{pmatrix} A_{n+1} \\ B_{n+1} \end{pmatrix} = \begin{pmatrix} A_1 & -B_1^* e^{-2i\theta} \\ B_1 & -e^{-2i\theta} \end{pmatrix} \begin{pmatrix} A_n \\ B_n \end{pmatrix} . \tag{12}$$

Thus $A_2 = |B_1|^4 - [2\cos(2\theta) + e^{2i\theta}]|B_1|^2 + e^{4i\theta}$ and $B_2 = [|B_1|^2 - 2\cos(2\theta)]B_1$. To ensure sure-success for this algorithm, one needs to require $A_2 - B_2 = 0$. It is easy to show that

$$\mathrm{Im}(A_2 - B_2) = [|B_1|^2 - 2\cos(2\theta)]\mathrm{Im}(A_1 - B_1)\,. \tag{13}$$

I shall consider in a future work the possibility of satisfying this equation by setting the first factor equal to zero. Here I concentrate on the fact that due to its second factor this equation can be satisfied by letting $\phi = 2\theta$. Then θ is given by

$$\begin{aligned}\mathrm{Re}(A_2 - B_2) &= 1 + 8f\mu^2 - 48f(1-f)\mu^4 \\ &\quad -64f^2(1-f)\mu^6 + 256f^2(1-f)^2\mu^8 = 0\,. \end{aligned} \tag{14}$$

I have plotted θ as a function of f for this algorithm in Fig. 3 assuming $\theta > 0$. It is seen that solution exists only

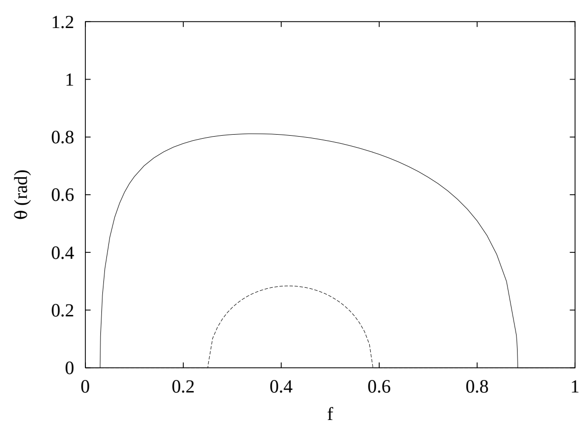

FIG. 3. Plotted is θ versus f for the algorithm $\mathcal{A}_4$.

for $0.030153689\cdots \leq f \leq 0.88302222\cdots$, and that in the narrower range $0.25 \leq f \leq 0.58682408\cdots$ A second solution for θ appears for each f. It should be obvious that this algorithm is valid for those values of f only, for which at least one solution for θ exists, thus the larger f range is also the validity range of this algorithm.

Finally, let us consider the algorithm member $\mathcal{A}_6$. Eq. (12) allows me to obtain $A_3 = |B_1|^6 - [4\cos(2\theta) + e^{2i\theta}]|B_1|^4 + 2[\cos(4\theta) + 1 + e^{4i\theta}]|B_1|^2 - e^{6i\theta}$, and $B_3 = \{|B_1|^4 - 4\cos(2\theta)|B_1|^2 + [2\cos(4\theta)+1]\}B_1$. Thus I find

$$\mathrm{Im}(A_3 - B_3) = \{[|B_1|^2 - 2\cos(2\theta)]^2 - 1\}\mathrm{Im}(A_1 - B_1)\,. \tag{15}$$

Again, I shall not consider here letting the first factor equal to zero. Then again $\phi = 2\theta$ from $\mathrm{Im}(A_3 - B_3) = 0$, and θ is given by

$$\text{Re}(A_3 - B_3) = 1 + 12f\mu^2 - 96f(1-f)\mu^4 \\ -256f^2(1-f)\mu^6 + 1280f^2(1-f)^2\mu^8 \\ +1024f^3(1-f)^2\mu^{10} - 4096f^3(1-f)^3\mu^{12} = 0\,. \quad (16)$$

I have plotted θ as a function of f for this algorithm in Fig. 4 assuming $\theta > 0$. It is seen that solution exists only

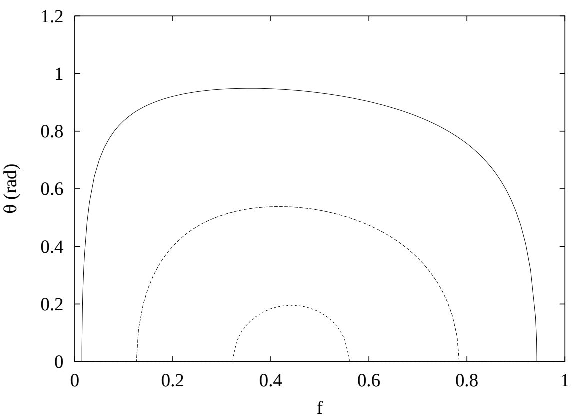

FIG. 4. Plotted is θ versus f for the algorithm $\mathcal{A}_6$.

for $0.014529091 \cdots \leq f \leq 0.94272801 \cdots$, which is the validity range of this algorithm. In the narrower range $0.12574462 \cdots \leq f \leq 0.78403237 \cdots$ a second solution for θ appears for each f, and in the even narrower range $0.32269755 \cdots \leq f \leq 0.56026834 \cdots$ a third solution for θ appears for each f.

A trend is clearly established by the above study of the first three even members. It strongly suggests that for all even members, (i) $\phi = 2\theta$ is always a valid solution, with θ depending on f, but not on N; (ii) the f-range in which at least one θ value exists becomes ever larger if $\mathcal{A}_{2n}$ of ever larger n is considered, with the $n \to \infty$ limit being very likely the full range $0 \leq f \leq 1$; (iii) in general the number of valid choices for θ increases to n deep inside the validity f-range for $\mathcal{A}_{2n}$. General proofs of these statements have not yet been obtained.

In summary, an infinite family of sure-success quantum algorithms is introduced here for solving the generalized Grover search problem of finding any one element of a set of acceptable choices which constitute a fraction f of all elements in an unsorted data base. This is achieved by two unitary operators each containing a phase parameter. These operators are generalizations of the two operators introduced by Grover for his original search problem. The two phase parameters are adjusted for each member of the family to ensure its sure-success, which is found possible only within a different f-range for each member of the algorithm family. An infinite sub-family (the "even" members) appears to have the property that the validity f-range of a lower member is totally embedded inside that of a higher member, with the limit being very likely the full range $0 \leq f \leq 1$. As long as f is within the validity range, the lowest member of the sub-family is then the most convenient, since it requires the least number of queries of the data base.

[1] P. W. Shor, SIAM J. Computing **26**, 1484 (1997).

[2] L. V. Grover, Phys. Rev. Lett. **79**, 325 (1997).

[3] This generalized Grover search problem has been considered before. [See, for example, R. M. Gingrich, C. P. Williams, and N. J. Cerf, Phys. Rev. A **61**, 052313 (2000); P. Høyer, Phys. Rev. A **62**, 052304 (2000); C. Zalka, Lanl-eprint/quant-ph/9902049; G. Brassard, P. Høyer, M. Mosca, and A. Tapp, Lanl-eprint/quant-ph/0005055.] However, none of them appear to solve this problem simply by the idea presented in this work.

[4] Grover's original algorithm is not a sure-success one, but there are at least three revisions of it to make it a sure-success algorithm. [See G. L. Long, Phys. Rev. A **64**, 022307 (2001), and two earlier references cited therein. C. Zalka in Lanl-eprint/quant-ph/9902049 has also outlined another revision without giving explicit details.] However, since they are all aiming at solving the original Grover's search problem, they are not identical to the idea presented in this work.

[5] This unitary operator has been introduced in many earlier works to solve either the original Grover search problem or its generalization discussed here. [See, for example, P. Høyer, Phys. Rev. A **62**, 052304 (2000); G.-L. Long, W. L. Zhang, Y. S. Li, and L. Niu, Lanl-eprint/quant-ph/9904077; G.-L. Long, Y. S. Li, W. L. Zhang, and L. Niu, Lanl-eprint/quant-ph/9906020; G.-L. Long, Y. S. Li, W. L. Zhang, and C. C. Tu, Lanl-eprint/quant-ph/9910076; G.-L. Long, L. Xiao, and Y. Sun, Lanl-eprint/quant-ph/0107013.] However, none of them appear to have combined it with the unitary operator given in Eq. 3 to solve either search problem.