Quantum Boolean Circuit Approach for Searching an Unordered Database

I-Ming Tsai, Sy-Yen Kuo, and David S.L. Wei†

Department of Electrical Engineering
National Taiwan University
Taipei, Taiwan
tsai@lion.ee.ntu.edu.tw ; sykuo@cc.ee.ntu.edu.tw

ABSTRACT — **The discovery of polynomial time prime factorization, secure key distribution, and fast database search algorithm have recently made quantum computing the most rapidly expanding research field. For a quantum algorithm to be useful, it is essential that the algorithm can be implemented using quantum circuits. Nanotechnology, in particular quantum mechanics based devices, can be used to realize such an algorithm. In this paper, we show how quantum boolean circuits can be used to implement the oracle circuit and the inversion-about-average function in Grover's search algorithm. We also show that a slight modification of the oracle circuit can be used to search multiple targets.**

I. INTRODUCTION

The discovery of secure key distribution [1], polynomial time prime factorization [2], and fast database search algorithm [3] have recently made quantum computing the most rapidly expanding research field. The fast database search algorithm is important because, from an engineering point of view, many problems can be formulated as a database searching process. For instance, cracking a 1024-digit secret key in a 2^{1024} key space is essentially a searching process in an unordered database. To search an unsorted database, the only way is to test the elements sequentially against the condition until the target is found. For a database of n elements, this brute-force search requires an average of $n/2$ comparisons. However, Grover's algorithm can identify the target in an unordered database in $\sqrt{n}$ steps. The idea of Grover's algorithm is to prepare a register in an equal superposition state, *selectively invert* the target, then perform an *inversion-about-average* operation. The selective inversion of the target followed by an inversion-about-average has the effect of amplitude amplification. After $\sqrt{n}$ operations the probability of measuring the marked state approaches 1.

As we can see, the only request in Grover's algorithm is the information regarding to whether a selected item is the target. This is also known as the *oracle*. If we label the items in a database with the integers $0, 1, 2, \ldots, 2^n \quad 1$ and denote the label of the unknown marked record by x_0, the oracle is an n bit binary function

$$f : \{0,1\}^n \quad \rightarrow \{0,1\} \tag{1}$$

defined by

$$f(x) = \begin{cases} 1 & \text{if} \quad x = x_0 \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

Note that, as a standard oracle, we have no access to the internal structure of the function f. It operates transparently in Grover's algorithm as a black-box function, which we can query as many times as we like.

Using the oracle, the selective inversion can be defined as the unitary function

$$I_{|x_0\rangle}(|x\rangle) = (\quad 1)^{f(x)}|x\rangle = \begin{cases} |\quad x_0\rangle & \text{if} \quad x = x_0 \\ |x\rangle & \text{otherwise.} \end{cases} \tag{3}$$

This function does an inversion on the input if it is the target, while leaving all other cases unchanged. Due to the linearity of quantum mechanics, every item in the database can be processed at the same time by applying the selective inversion to the superposition state of all items. When this operation is applied to such a superposition state, it is equivalent to

$$I_{|x_0\rangle} = I \quad 2|x_0\rangle\langle x_0|. \tag{4}$$

Note that the unitary transformation $I_{|x_0\rangle}$ is actually an inversion in $\mathcal{H}$ about the hyperplane perpendicular to $|x_0\rangle$. Following the same notation, if we define

$$|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n \quad 1} |i\rangle, \tag{5}$$

the inversion-about-average operation can be regarded as an inversion in $\mathcal{H}$ about the hyperplane perpendicular to $|\psi_0^{\perp}\rangle$, and [4]

$$I_{|\psi_0^{\perp}\rangle} = \quad I_{|\psi_0\rangle}. \tag{6}$$

†David S.L. Wei is with Department of Computer and Information Science, Fordham University, Bronx, NY.

0-7803-7538-6/02/$17.00©2002 IEEE

The operation of a selective inversion followed by an inversion-about-average can be represented as

$$G = \quad I_{|\psi_0\rangle} I_{|x_0\rangle}. \tag{7}$$

Based on this operator, Grover's algorithm can find the target with a high probability (approaching 1) by applying the operator G to the superposition state

$$|\psi_0\rangle = H|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n \quad 1} |i\rangle \tag{8}$$

for $\sqrt{n}$ times before the final measurement.

The optimality of Grover's algorithm has been studied [5] and a generalization of the algorithm has been proposed to search multi-object [6]. In this paper, we focus on the circuit design aspect of the algorithm.

II. Circuit Block Diagram

The first step of implementing the operator G is to construct a circuit which performs the function of selective inversion $I_{|x_0\rangle}$. An important property called *eigenvalue kickback* is used in the construction of the circuit, as shown in Fig.1.

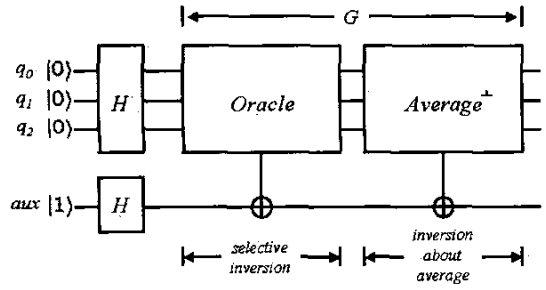

Fig. 1. The circuit block diagram of Grover's search algorithm.

The initial qubits in Fig.1 include n qubits prepared in the ground state $|\psi\rangle = |0\rangle \cdots |0\rangle$ and 1 auxiliary qubit in the excited state $|1\rangle$. This can be written as

$$|\psi\rangle \otimes |\phi\rangle = (|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle) \otimes (|1\rangle). \tag{9}$$

After the the Hadamard transform H^n and H, all possible states are superposed as $|\psi_0\rangle \otimes |\phi_0\rangle$, where

$$|\psi_0\rangle \quad = \quad \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n \quad 1} |i\rangle \tag{10}$$

$$|\phi_0\rangle \quad = \quad \frac{1}{\sqrt{2}}(|0\rangle \quad |1\rangle). \tag{11}$$

Theoretically, the oracle is only a function which checks whether a specific item is the target. However, due to the linearity of quantum mechanics, when the oracle circuit is applied to the superposition state $|\psi_0\rangle$, all possible items are examined against the criteria. It follows from the fact that the eigenvalue of $\frac{1}{\sqrt{2}}(|0\rangle \quad |1\rangle)$, *i.e.* 1, is kicked back to the state ψ'

$$O_f \quad \text{NOT}(|\psi_0\rangle \otimes |\phi_0\rangle) = (I_{|x_0\rangle}(|\psi_0\rangle)) \otimes \frac{|0\rangle \quad |1\rangle}{\sqrt{2}}, \tag{12}$$

The oracle circuit O_f plus the control-not gate is computationally equivalent to the operator $I_{|x_0\rangle}$, which inverts the unknown target in one single operation. From a circuit point of view, the oracle, which takes n qubits as input and 1 qubit as output, is a standard $n \times 1$ boolean function. It can be implemented using quantum boolean logic.

The second step of the operation G is the inversion-about-average circuit. When the operation is applied to a superposition state, it actually keeps the component in the $|\psi_0\rangle$ direction unchanged, while inverting the components in dimensions which are perpendicular to $|\psi_0\rangle$. This can be represented as

$$I_{|\psi_0^{\perp}\rangle} = \quad I_{|\psi_0\rangle} \tag{13}$$

where

$$|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n \quad 1} |i\rangle \tag{14}$$

represents the "average".

Using the same concept of eigenvalue kickback, the component in the $|\psi_0^{\perp}\rangle$ dimension can be selectively inverted, as shown in Fig.1. Note that this part of the circuit does not depend on the search criteria.

Since most practical engineering problems can be binary encoded, searching a target in the database is the same thing as finding a satisfiable solution for a binary boolean expression. In other words, the oracle function can be represented by boolean logic and implemented using quantum gates. The classical boolean logic can be simulated using elementary quantum boolean gates as follows:

- By sending the input into a quantum **N** gate, we can invert the quantum state and hence simulate a classical **NOT** operation.
- If we set $z = 0$ in a **CCN** gate, then the output $z' = x \cdot y$ simulates the output of a classical **AND** gate.
- The **OR** function can be done using DeMorgan's law. That is, $A \vee B = \overline{\bar{A} \wedge \bar{B}}$.

Another non-trivial quantum boolean logic function is **FANOUT**, which takes one bit as input and gives two copies of the same bit value as output. In the classical world, we can do this simply with a metallic contact. However, in this application, a **CN** gate can be used to create an entangled copy of the source qubit.

III. Circuit for Single-Target Search

Without loss of generality, we use the binary expression

$$(\bar{x} \vee y) \wedge \bar{z} \wedge (x \vee z) \tag{15}$$

0-7803-7538-6/02/$17.00©2002 IEEE

as an example to show how the solution is found using the circuit described in the previous section. The oracle circuit is an quantum implementation of the expression, which is shown in Fig.2.

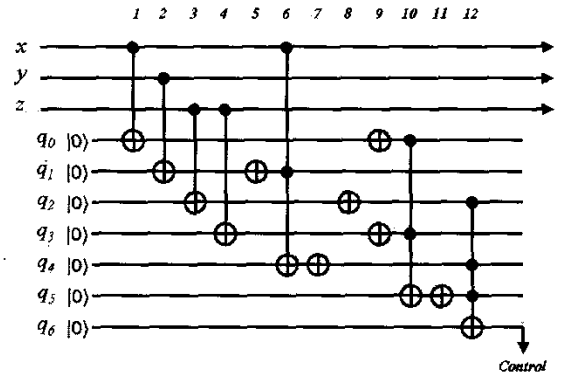

Fig. 2. The oracle circuit for a single-target search.

In Fig.2, gate 1, 2, 3, and 4 duplicate the input x, y, and z to q_0, q_1, q_2, and q_3 for later use, so the original copy won't be affected by the subsequent operations. Gate 5, 6, and 7 implement the function $(\bar{x} \vee y)$. Gate 8 inverts z. Gate 9, 10, and 11 implement the function $(x \vee z)$. Finally, gate 12 performs the **AND** function for these three clauses. The final result is in qubit q_6, which is the control bit for the selective inversion circuit in Fig.1. Note that although the three-input **AND** function can be implemented by cascading two two-input **AND** gates, it is shown as one 4-bit generalized Toffoli gate for simplicity. An $m+1$ bit generalized Toffoli gate is defined as

$$\wedge_m(|x_1, \cdots, x_m, y\rangle) = |x_1, \cdots, x_m, (\wedge_{k=1}^{m} x_k) \oplus y\rangle. \tag{16}$$

The second part of the circuit performs the function of inversion-about-average. To invert the component in the $|\psi_0\rangle$ dimension, Hadamard gates are used to transform $|\psi_0\rangle$ to $|0\rangle$, then the state $|0\rangle$ is selectively inverted. After the inversion, the state is transformed back by another set of Hadamard gates. The circuit can be represented by

$$I_{|\psi_0\rangle} = H I_{|0\rangle} H, \tag{17}$$

where

$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}, \tag{18}$$

as shown in Fig.3. Similarly, the function of $I_{|0\rangle}$ can be done using the eigenvalue kickback property. It is shown in Fig.3 as a generalized Toffoli gate with the exception that the target is inverted when all the control qubits are 0's. This is shown by the circles, instead of solid dots, in Fig.3.

Although it does not effect the measurement, the minus sign in $I_{|\psi_0\rangle}$ can be implemented by applying a π phase shift to any one of the qubits. This is shown as the U transform in Fig.3, where

$$U = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{19}$$

Note that since this part of the circuit is completely independent of the search criterion, it can be used to do any single- or multi-target search.

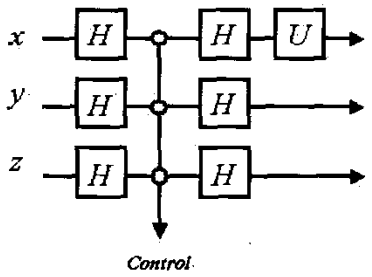

Fig. 3. The circuit of inversion-about-average.

The complete circuit for G is shown in Fig.4. After $\sqrt{n}$ steps of G, a final measurement on the state of x, y, and z reveals the target with high probability.

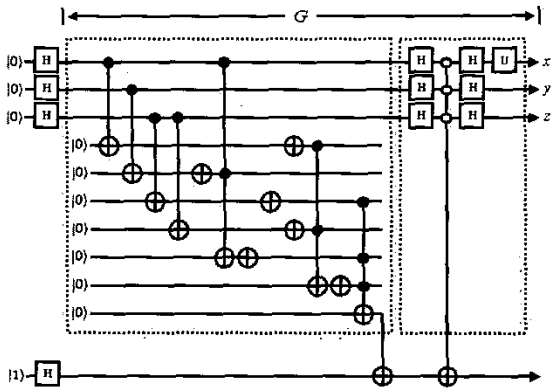

Fig. 4. The circuit G in the quantum search algorithm.

IV. Circuit for Multi-target Search

The circuit design for a single-object search can be easily generalized to search multiple objects. The only difference is that after each target is found, the oracle circuit is modified to exclude this target. A typical scenario is shown in the following example.

Assuming the problem is binary encoded as

$$(\bar{x} \vee z) \wedge y. \tag{20}$$

The equivalent oracle circuit is shown in Fig.5.

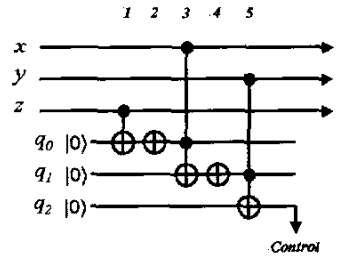

Fig. 5. The oracle circuit for searching the first target.

In this circuit, gate 1 duplicates the variable z, gate 2, 3, and 4 implement the function $(\bar{x} \vee z)$. Finally, gate 5 performs the **AND** function for these two clauses. The oracle circuit is then followed by the same circuit in Fig.3 to perform the function of inversion-about-average. These form the operation G. A measurement after $\sqrt{n}$ steps of G results in one of the targets with equal probability.

At the end of the first measurement, the criterion is modified to exclude the target that has been found. Assume the first result is $x = 0, y = 1, z = 0$, the oracle is then changed to be

$$(\bar{x} \vee z) \wedge y \wedge \overline{\bar{x} \cdot y \cdot \bar{z}}. \tag{21}$$

The clause $\overline{\bar{x} \cdot y \cdot \bar{z}}$ is used to exclude the combination of $x = 0$, $y = 1$, and $z = 0$. The new oracle circuit is shown in Fig.6. In this circuit, gate 7, 8, and 9 are used to implement $\overline{\bar{x} \cdot y \cdot \bar{z}}$. At the same time, gate 10 includes q_4 as one reference to form the new oracle. This new oracle circuit and the same circuit of inversion-about-average are used to find the second target.

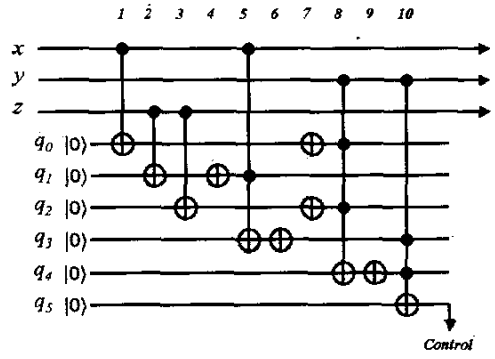

Fig. 6. The oracle circuit for searching the second target.

Similarly, if the result of the second measurement is $x = 1, y = 1$, and $z = 1$, the oracle is then changed to be

$$(\bar{x} \vee z) \wedge y \wedge \overline{\bar{x} \cdot y \cdot \bar{z}} \wedge \overline{x \cdot y \cdot z}. \tag{22}$$

The new clause $\overline{x \cdot y \cdot z}$ is added to exclude the second target. Although further reduction can be done on the boolean expression, the original form is used to illustrate the modification. The oracle circuit is shown in Fig.7. Again, gate

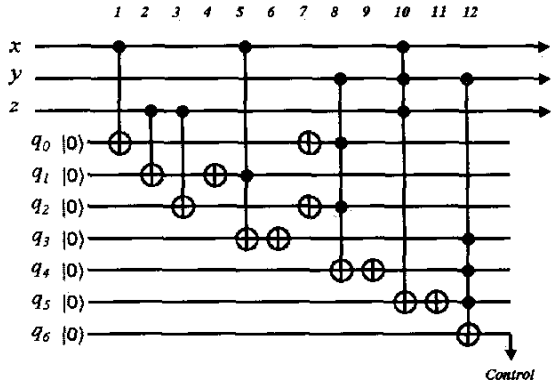

Fig. 7. The oracle circuit for searching the third target.

10 and 11 are used to implement the new criterion $\overline{x \cdot y \cdot z}$, gate 12 takes the result q_5 and forms the new oracle. This new oracle circuit, together with the circuit of inversion-about-average, are used to query the third target.

V. Conclusions

Due to its wide application in classical engineering problems, Grover's quantum search algorithm is one of the important applications in quantum computing. This algorithm shows a dramatic improvement compared with the classical brute-force search process, especially when n is large. The algorithm is built on top of two key operations, namely: selective inversion and inversion-about-average. In this paper, we present how quantum boolean circuits can be used to implement the selective inversion and inversion-about-average in the quantum search algorithm. We also show that a slight modification of the oracle circuit can be used to do a multi-object database search.

References

[1] C. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proc. of IEEE International Conference on Computers Systems and Signal Processing*, 1984, pp. 175-179.

[2] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proc. of the 35th Annual IEEE Symposium on the Foundations of Computer Science*, 1994, pp. 124-134.

[3] L. Grover, "A fast quantum mechanical algorithm for database search," *Proc. of the 28th Annual ACM Symposium on the Theory of Computing*, 1996, pp. 212-219.

[4] S. Lomonaco. (2000, Oct.). *Grover's quantum search algorithm* . [Online]. Available: http://www.arXive.org/quant-ph/0010040/.

[5] C. Zalka. "Grover's quantum searching algorithm is optimal," *Phys. Rev. A*, vol. 60, 2746-2751 (1999).

[6] G. Chen, S. Fulling, J. Chen, S. Sun (2000, Jul.). *Generalization of Grover's algorithm to multiobject search in quantum computing.* [Online]. Available: http://www.arXive.org/quant-ph/0007123/ and http://www.arXive.org/quant-ph/0007124/.