A Quantum Circuit Design for Grover's Algorithm

Zijian Diao, M. Suhail Zubairy[a], and Goong Chen[b]

Department of Mathematics, Texas A&M University, College Station, TX 77843, U.S.A.
[a] Institute for Quantum Studies and Department of Physics, Texas A&M University, College Station, TX 77843, U.S.A.
[b] Institute for Quantum Studies and Department of Mathematics, Texas A&M University, College Station, TX 77843, U.S.A.

Reprint requests to Prof. G. Ch.; Fax (979) 862-4190; gchen@math.tamu.edu

Z. Naturforsch. **57a,** 701–708 (2002); received May 15, 2002

We present a circuit design realizing Grover's algorithm based on 1-bit unitary gates and 2-bit quantum phase gates implementable with cavity QED techniques. In the first step, we express the circuit block which performs a key unitary transformation that flips only the sign of the state $|11\cdots11\rangle$ using 1-bit and 2-bit gates. The Grover's iteration operator can then be constructed using this key unitary transformation twice, plus other operations involving only 1-bit unitary gates on each qubit. Mathematical proofs are given to justify that the cricuiting satisfies the desired operator properties.

Key words: Quantum Search; Grover's Algorithm.

1. Introduction

Quantum computing utilizes unique quantum features such as quantum coherence and quantum entanglement to solve some problems much faster than on classical Turing machines. The most dramatic example of the power of quantum computing is Shor's algorithm for factoring a large integer [1]. This algorighm is substantially faster than any known classical algorithms of subexponential complexity. Another major example is the search of an object in unsorted data containing N elements. Classically it would require, on the average, $O(N)$ searches. However, Grover showed that, by employing quantum superposition and quantum entanglement, the search can be carried out with only $O(\sqrt{N})$ steps [2–4]. Grover's algorithm thus represents a polynomial advantage over classical counterparts.

In recent years, Grover's algorithm has been realized in NMR [5], optical systems [6], and a proposal has been made for its implementation in cavity QED systems [7]. All these studies are, however, restricted to $N = 4$ for which only one step is required to recover the target state with probability 1. An extension to higher values of N would be rather complicated [8]. The first step towards realizing the search algorithm for arbitrary N is to construct a circuit diagram in terms of quantum logic gates. It is the objective of this paper to devise such a circuit consisting of basic quantum logic gates.

Due to the coherent nature of quantum mechanics, quantum computing algorithms are based on unitary transformations. The one-bit unitary gate and two-bit quantum phase gate suffice as the basic building blocks for quantum algorithms. The design circuit elements are based on the following gates that are representable in matrix forms as

(i) 1-bit unitary gate

$$U^{(j)}_{\theta,\phi} = \begin{bmatrix} \cos\theta & -ie^{-i\phi}\sin\theta \\ -ie^{i\phi}\sin\theta & \cos\theta \end{bmatrix}, \tag{1.1}$$

with respect to the ordered basis $\{|0\rangle, |1\rangle\}$. (The superscript (j) here denotes that this operation is on the j-th bit.)

(ii) 2-bit phase gate

$$Q_\eta = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\eta} \end{bmatrix}, \tag{1.2}$$

with respect to the ordered basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

The one-bit unitary gate is an elementary gate in common quantum operations, while the two-bit quantum phase gate has been experimentally demonstrated in cavity QED systems [9]. In our quantum circuit, qubits are carried by Rydberg three-level atoms. Our scheme for implementing Grover's algorithm is based on reso-

nant atomic interactions with classical fields and dispersive coupling with quantized cavity fields. More specifically, one-bit gate $U_{\theta,\phi}$'s are implemented via the resonant interaction with a classical field. We can specify the parameters θ and ϕ by choosing a proper Rabi frequency, interaction time, and phase of the driving field [10]. The two-bit quantum phase gate Q_η can be implemented via dispersive coupling to a cavity field having either 0 or 1 photon. The cavity field acts as the intermediary that causes one atom to interact with another. We can achieve the proposed phase shift by setting a proper coupling coefficient and interaction time.

Consider the quantum circuit design for two qubits presented in [7]. A key feature in that design is that it embodies quantum entanglement. Here we furnish the complete circuit design for the general n-qubit case. First, we wish to point out that the two types of quantum gates in (1.1) and (1.2) do satisfy *universality*, even though, when $n=1$, e.g., a unitary operator of the form

$$\begin{bmatrix} e^{i\phi} & 0 \\ 0 & e^{i\phi} \end{bmatrix}, \quad \phi \neq k\pi, k = 0, \pm 1, \pm 2, \ldots \tag{1.3}$$

can not be approximated with arbitrary accuracy by (1.1) because the 1-bit gates (1.1) generate only the special unitary group $SU(2)$, since the determinant of (1.1) is always 1. However, the phase shift matrix (1.3) hardly matters according to the results in [11], and thus the basic quantum gates (1.1) and (1.2) are indeed universal for $n \geq 2$. Therefore this assures that a quantum circuit design can be made. Albeit this fact is true, there obviously exist many alternative ways of design, and considerable technical details need to be worked out. Our major task here actually is to achieve a design *with as much simplicity as possible.* In this paper, the complexity of our design, measured in terms of the total number of elementary quantum gates (1.1) and (1.2) needed in a single Grover iteration, is $O(\log N)$, where N is the size of the database.

For the ease of quantum network representation in order to be able to utilize the elegant results by Barenco et al. [11], we have adopted the following convention: throughout the paper, matrix representations are always with reference to the binary string basis in increasing lexicographic order:

$$|00\cdots00\rangle, |00\cdots01\rangle, |00\cdots010\rangle, \ldots,$$
$$|11\cdots10\rangle, |11\cdots11\rangle, \tag{1.4}$$

for the 2^n dimensional Hilbert space $\mathcal{H}$. Without loss of generality we assume $N=2^n$. Throughout all the quantum networks given below, the top wire always represents the most significance qubit; see Figure 1.

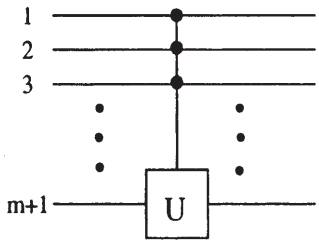

Fig. 1. The network notation for $\Lambda_m(U)$; see Definition 1 for $\Lambda_m(U)$.

We now give a brief overview of Grover's algorithm in the mathematical formalism as given in [12]. Let

$$D = \{w_i \,|\, i = 0, 1, \ldots, N-1\}, \ (N = 2^n)$$

be a database which is encoded in an n-bit quantum computer as

$$\hat{D} = \{|w_i\rangle \,|\, i = 0, 1, \ldots, N-1\} \quad \text{with} \quad \mathcal{H} = \operatorname{span} \hat{D}.$$

Without loss of generality, assume that $|w_0\rangle$ is the intended (unknown) search target in $\hat{D}$. Associated with this target $|w_0\rangle$, the only information available is through a black-box oracle function

$$f\colon \hat{D} \to \{0,1\}, \ f(|w_i\rangle) = \delta_{i0}, \quad i = 0, 1, \ldots, N-1. \tag{1.5}$$

Let the binary symbol for $|w_0\rangle$ be

$$|w_0\rangle = |a_1 a_2 \cdots a_n\rangle, \ a_i \in \{0,1\}, \quad i = 0, 1, \ldots, n. \tag{1.6}$$

For future needs, let us also represent (1.6) as

$$|w_0\rangle = \sigma_x^{(i_1)} \sigma_x^{(i_2)} \cdots \sigma_x^{(i_k)} |11\cdots11\rangle, \tag{1.7}$$

where

$$\sigma_x^{(j)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad j = i_1, i_2, \ldots, i_k, \tag{1.8}$$

is a Pauli matrix (or, the NOT-gate) acting on the j-th qubit, i.e., in (1.6), $a_j = 0$ for $j = i_1, i_2, \cdots i_k$. All the other a_j's are 1.

Let

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |w_i\rangle$$

be the uniform superposition of all basis states in $\mathcal{H}$. We define

$$\begin{aligned} I_{w_0} &= I - \frac{1}{2} \sum_{i=0}^{N-1} [|w_i\rangle - (-1)^{f(|w_i\rangle)} |w_i\rangle] \\ &\quad \cdot [\langle w_i| - (-1)^{f(|w_i\rangle)} \langle w_i|] \\ &= I - 2\,|w_0\rangle\langle w_0|, \quad \text{and} \end{aligned} \tag{1.9}$$

$$I_s = I - 2\,|s\rangle\langle s|. \tag{1.10}$$

Both I_{w_0} and I_s are unitary operators, and

$$G \equiv -I_s I_{w_0} \tag{1.11}$$

is *Grover's unitary operator* to be used in the iterative search for $|w_0\rangle$. Using $|s\rangle$ as the initial state, and applying the operator G, k times, i.e.,

$$G^k|s\rangle, \quad k \approx \frac{\pi}{4}\sqrt{N}, \tag{1.12}$$

we will obtain $|w_0\rangle$ with a high probability (close to 1).

In the following sections we describe our procedures for the quantum optical circuit design. The idea centers on first constructing, and then using a key n-bit unitary transformation

$$K_n \equiv I - 2|11\cdots1\rangle, \langle 11\cdots1| \tag{1.13}$$

as a building block for both I_{w_0} and I_s. More specifically:

Step 1: Construct the 3-bit key transformation $K_3 = I - 2|111\rangle\langle 111|$, and the Toffoli gate Controlled-Controlled-NOT $\Lambda_2(X)$, where X is the NOT-gate. See **2**.

Step 2: Construct the n-bit transformation $\Lambda_{n-1}(X)$ (cf. Theorem 5 below) and then K_n. See **3**.

Step 3: Use K_n as two major building blocks and assemble other 1-bit gates to construct the Grover operator G for iteration. This is done in **4**.

2. Construction of the Toffoli Gate and K_3 from the Basis Gates

We inherit the following definition from p. 52 in [11].

Definition 1. Let

$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

be a unitary matrix and $m \in \{0, 1, 2, \ldots\}$. Define the operator $\Lambda_m(U)$ on $(m+1)$-qubits through its action on the basis by

$$\Lambda_m(U)(|x_1 \cdots x_m y\rangle) = \begin{cases} |x_1 \cdots x_m y\rangle & \text{if } \Lambda_{k=1}^m x_k = 0, \\ u_{0y}|x_1 \cdots x_m 0\rangle + u_{1y}|x_1 \cdots x_m 1\rangle & \text{if } \Lambda_{k=1}^m x_k = 1, \end{cases}$$

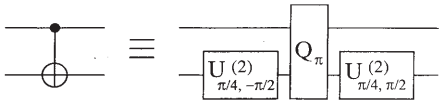

Fig. 2. Equivalent networks for the equation (2.2).

where "Λ" denotes the Boolean operator AND. □

The matrix representation for $\Lambda_m(U)$ is

$$\Lambda_m(U) = \begin{bmatrix} 1 & & & & & \\ & \circ & & & 0 & \\ & & \circ & & & \\ & & & 1 & & \\ & & 0 & & \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix} & \end{bmatrix}_{2^{m+1}\times 2^{m+1}} \tag{2.1}$$

and the network notation is given in Fig. 1. We use X to denote the NOT-gate σ_x in (1.8). Then $\Lambda_1(X)$ and $\Lambda_2(X)$ are, respectively, the well known Controlled-NOT and the Toffoli gates.

Lemma 1. *We have*

$$\Lambda_1(X) = U^{(2)}_{\pi/4,\,\pi/2}\, Q_\pi\, U^{(2)}_{\pi/4,\,-\pi/2}. \tag{2.2}$$

Proof. Withe respect to the ordered basis $\{|00\rangle, |00\rangle, |10\rangle, |11\rangle\}$, we have the matrix representations

$$\Lambda_1(X) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad U^{(2)}_{\pi/4,-\pi/2} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix},$$

$$Q_\pi = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}, \quad U^{(2)}_{\pi/4,\pi/2} = \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}.$$

It is now straightforward to verify by matrix multiplication that (2.2) holds. □

The equivalence of the two networks in (2.2) is depicted in Figure 2.

Lemma 2. *Let*

$$U_0 \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad V_0 = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \quad V_0^* = \begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix}. \tag{2.3}$$

Then the unitary transformation $K_3 = I - 2|111\rangle, \langle 111| = \Lambda_2(U_0)$ *can be simulated by the network depected in Figure 3.*

Proof. It is easy to check from (2.3) that the equations

$$V_0^2 = U_0, \quad V_0 V_0^* = V_0^* V_0 = I$$

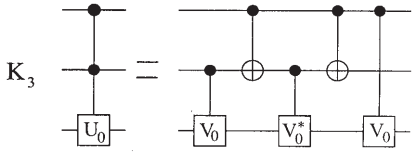

Fig. 3. An equivalent network for the transformation K_3.

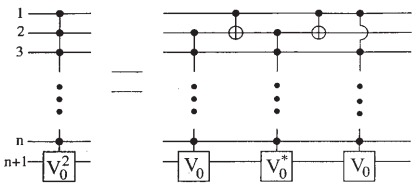

Fig. 4. An equivalent network for $\Lambda_n(V_0^2)$.

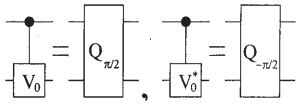

Fig. 5. Equivalent networks for $Q_{\pi/2}$ and $Q_{-\pi/2}$, where V_0 and V_0^* are given in (2.3).

are satisfied. We now quote Lemma 6.1 in [11] to conclude the equivalence of networks in Figure 3. □

Incidentally, we note that a more general version of Lemma 6.1 in [11] can be stated as follows: Let U_0 and V_0 be 2×2 unitary matrices such that $V_0^2 = U_0$. Then the $(n+1)$-bit gate $\Lambda_n(U_0)$ can be simulated by the network shown in Figure 4.

We now note that we have the following equivalent networks, in Figure 5.

Using Figs. 2 and 5 in Fig. 3, we obtain Figure 6.

Corollary 3. *The key transformation K_3 can be simulated by the network in terms of the basic $U_{\theta,\phi}$ and Q_η gates as depicted in Figure 6.*

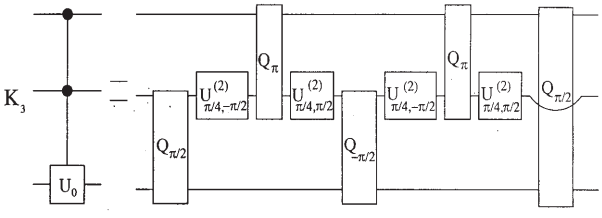

Fig. 6. The network simulating K_3 using the basic gates $U_{\theta,\phi}$ and Q_η.

We also obtain the following.

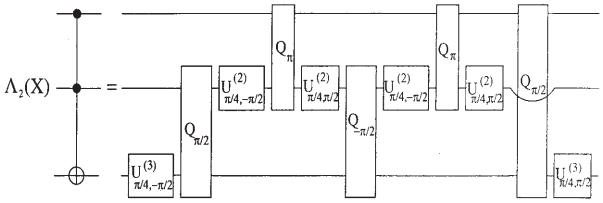

Fig. 7. The network simulating the Toffoli gate using the basic gates $U_{\theta,\phi}$ and Q_η.

Corollary 4. *The Toffoli gate $\Lambda_{n-2}(X)$ can be simulated by a network in terms of the basic $U_{\theta,\phi}$ and Q_η gates as depicted in Figure 7.*

Proof. It follows from Corollary 3 and the same kind of argument as in Lemma 1. □

Remark 1. From Fig. 7 we see that to make a Toffoli gate, we need 11 basic gates: 6 $U_{\theta,\phi}$ 1-bit gates and 5 Q_η 2-bit phase gates. □

3. Construction of the *n*-Bit Key Transformation with Linear Complexity from the Basic Gates

As pointed out in [11], there are many ways to construct the n-bit transformation $\Lambda_{n-1}(X)$. Some of such constructions have exponential complexity (Lemma 7.1 in [11]). Here, we first design a network for $\Lambda_{n-1}(X)$ from the reversible Toffoli gates with linear complexity. The n-bit key transformation then easily follows as a result.

Theorem 5. *The n-bit gate $\Lambda_{n-1}(X)$ can be simulated by a network consisting of $2n-7$ Toffoli gates as shown in Fig. 8, where $n-3$ scratch bits, $(s)1, (s)2, \ldots, (s)n-3$, are used.*

Proof. We note that except for the two Toffoli gates $\Lambda_2(X)$ controlled by bits 1 and 2 (see the top two wires in the network on the right of Fig. 8), every $\Lambda_2(X)$ else is controlled by a scratch bit $(s)j$, $j=1,2,\ldots,n-3$ with the value $|0\rangle$ prescribed. Hence, if there is any $|0\rangle$ appearing in any one of the input qubits $1,2,\ldots,n-1$, the $\Lambda_2(X)$ gate controlled by that input bit will act trivially on the scratch bit, say $(s)j$, which is the controlled bit, leaving its value equal to $|0\rangle$ throughout that wire. This affects the functioning of the $\Lambda_2(X)$ gate controlled by the scratch bit, again leaving the value of the next

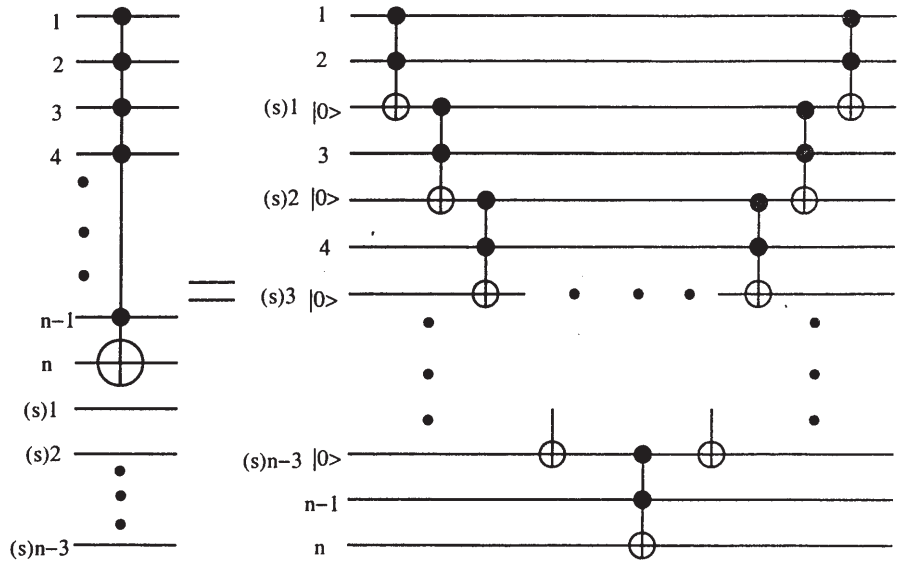

Fig. 8. Construction of the n-bit transformation $\Lambda_{n-1}(X)$ using $2n-7$ Toffoli gates and $n-3$ scratch bits $(s)1, (s)2, \ldots, (s)n-3$.

scratch bit $(s)j+1$ to be $|0\rangle$, unchanged. This process carries on to the very last bit $(s)n-3$. Since $(s)n-3$ is a control bit for bit n, thus the value of bit n is unchanged. Only when all of the input qubits take the value $|1\rangle$, all the $\Lambda_2(X)$ gates act nontrivially, flipping the value of the $(s)j$ bit from $|0\rangle$ to $|1\rangle$, and then from $|1\rangle$ back to $|0\rangle$ on the remaining part of the $(s)j$ wire, for $j=1,2,\ldots,n-3$. Hence the $\Lambda_{n-1}(X)$ transformation is accomplished. □

Corollary 6. *The n-bit key transformation K_n (1.13) can be simulated by the network as shown in Figure 9.*

Proof. Same as Corollary 3.

Remark 2. From Remark 1, Theorem 5 and Corollary 6, we see that in order to simulate the transformation K_n, we need

$$(2n-7)\times 5 = 10n-35 \qquad Q_\eta \text{ gates},$$
$$(2n-7)\times 6+2 = 12n-40 \qquad U_{\theta,\phi} \text{ gates},$$

for a total of $22n-75$ basic gates. Hence the linear complexity as far as n is concerned. □

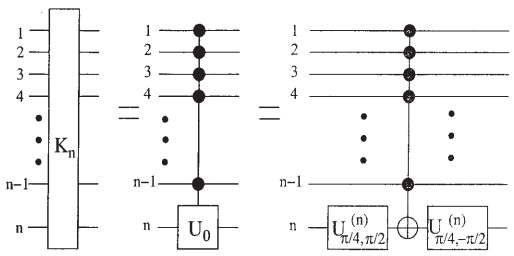

Fig. 9. The network simulating the n-bit key transformation K_n.

4. Assembling the Quantum Optical Circuit Blocks for the Grover Unitary Operator

We are now in a position to present the major result of the paper, i.e. the design given in the block diagram Fig. 10 with interpretation and justification that it indeed constitutes the Grover unitary operator G in (1.11).

There are three major blocks in Fig. 10:

$\mathcal{W}$: the Walsh-Hadamard block, which prepares the input state

$$|00\ldots 0\rangle \to |s\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |w_i\rangle ; \tag{4.1}$$

O: the oracle block, which is the unitary operator flipping the sign of the target state $|w_0\rangle$:

$$|w_i\rangle \to (-1)^{f(w_i)}|w_i\rangle, \quad i=0,1,\ldots,N-1; \tag{4.2}$$

cf. (1.9)

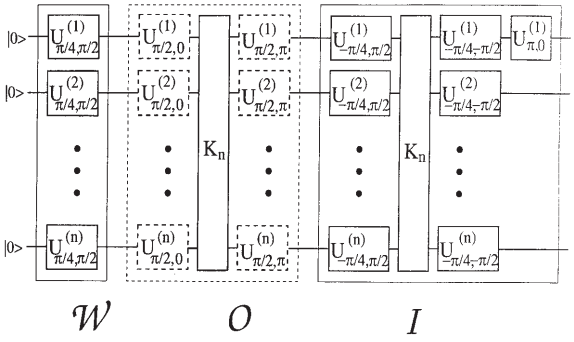

Fig. 10. Quantum circuitry for the Grover iteration operator.

I: the block for the unitary operator "inversion about the average", i.e.,

$$I_s = I - 2|s\rangle\langle s|; \quad \text{cf. (1.10)} \tag{4.3}$$

In the following, we provide the mathematical proofs justifying that the circuitry blocks in Fig. 10 indeed satisfy the properties (4.1)–(4.3) as intended.

The operation (4.1) in the $\mathcal{W}$ block of Fig. 10 is interpreted in the following.

Theorem 7.

$$\begin{aligned} &U^{(1)}_{\pi/4,\pi/2}|0\rangle \otimes U^{(2)}_{\pi/4,\pi/2}|0\rangle \otimes \text{L} \otimes U^{(n)}_{\pi/4,\pi/2}|0\rangle \\ &= \frac{1}{2^{n/2}}[|00\text{L}\ 00\rangle + |00\text{L}\ 01\rangle + |00\text{L}\ 10\rangle \\ &\qquad +\text{L} + |11\text{L}\ 10\rangle + |11\text{L}\ 11\rangle] \\ &= |s\rangle . \end{aligned} \tag{4.4}$$

Proof. This is a well-known fact. We have

$$U_{\pi/4,\pi/2}|0\rangle = \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]. \tag{4.5}$$

Therefore the tensor product in (4.4) gives $|s\rangle$ as in (4.1). □

Next, we interpret the oracle block O in Fig. 10 through the following.

Theorem 8. *Let $|w_0\rangle$ be given by (1.6) satisfying (1.7). Then*

$$U^{(i_1)}_{\pi/2,\pi} U^{(i_2)}_{\pi/2,\pi} \text{L}\ U^{(i_k)}_{\pi/2,\pi} K_n U^{(i_k)}_{\pi/2,0} \text{L}\ U^{(i_2)}_{\pi/2,0} U^{(i_1)}_{\pi/2,0} = I_{w_0}. \tag{4.6}$$

Proof. We first note that

$$\begin{aligned} U_{\pi/2,0} &= \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} = -i\sigma_x , \\ U_{\pi/2,\pi} &= \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} = -i\sigma_x = U^*_{\pi/2,0} . \end{aligned} \tag{4.7}$$

Therefore, by (1.6) and (1.7),

$$\begin{aligned} |w_0\rangle &= (iU^{(i_1)}_{\pi/2,0})(iU^{(i_2)}_{\pi/2,0}) \text{L}\ (iU^{(i_k)}_{\pi/2,0})|11\text{L}\ 1\rangle \\ &= i^k U^{(i_1)}_{\pi/2,0} U^{(i_2)}_{\pi/2,0} \text{L}\ U^{(i_k)}_{\pi/2,0}|11\text{L}\ 1\rangle \end{aligned}$$

and, thus,

$$\begin{aligned} I_{w_0} &= I - 2|w_0\rangle\langle w_0| \\ &= I - 2(i^k)U^{(i_1)}_{\pi/2,0})U^{(i_2)}_{\pi/2,0} \text{L}\ U^{(i_k)}_{\pi/2,0}|11\text{L}\ 1\rangle \\ &\quad \cdot \langle 11\text{L}\ 1|U^{(i_k)}_{\pi/2,\pi} \text{L}\ U^{(i_2)}_{\pi/2,\pi} U^{(i_1)}_{\pi/2,\pi} (-i)^k \\ &= I - 2U^{(i_1)}_{\pi/2,0} U^{(i_2)}_{\pi/2,0} \text{L}\ U^{(i_k)}_{\pi/2,0}|11\text{L}\ 1\rangle \\ &\quad \cdot \langle 11\text{L}\ 1|U^{(i_k)}_{\pi/2,\pi} \text{L}\ U^{(i_2)}_{\pi/2,\pi} U^{(i_1)}_{\pi/2,\pi} \\ &= U^{(i_1)}_{\pi/2,0} U^{(i_2)}_{\pi/2,0} \text{L}\ U^{(i_k)}_{\pi/2,0} (I - 2|11\text{L}\ 1\rangle \cdot \langle 11\text{L}\ 1|) \\ &\quad \cdot U^{(i_k)}_{\pi/2,\pi} \text{L}\ U^{(i_2)}_{\pi/2,\pi} U^{(i_1)}_{\pi/2,\pi} , \end{aligned} \tag{4.8}$$

which is exactly (4.6). Note that in the derivation of (4.8), we have utilized the property

$$U^{(i_1)}_{\pi/2,0} U^{(i_2)}_{\pi/2,0} \text{L}\ U^{(i_k)}_{\pi/2,0} I U^{(i_k)}_{\pi/2,\pi} U^{(i_{k-1})}_{\pi/2,\pi} \text{L}\ U^{(i_1)}_{\pi/2,\pi} = I. \qquad \square$$

Remark 3. The currently well-known standard approach implementing the unitary operator I_{w_0} is via the unitary transformation $U_f : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$, with the auxiliary qubit $|y\rangle$ set to $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Furthermore, the implementation of f has to be done via another unitary transformation $|x\rangle|0\rangle \to |x\rangle|f(x)\rangle$, with one more auxiliary qubit, since f is in general not reversible. Taking this fact into account, Fig. 11 renders us a complete picture of the construction. However, this approach calls for a concrete realization of f, and it is not within the scope of task of this article. We would rather concentrate on the operators directly related to Grover's algorithm. We adopt a different approach in that, for given $|w_0\rangle$ satisfying (1.5)–(1.7) (known only to the oracle), the 1-bit unitary gates $U^{(i_1)}_{\pi/2,0}$, $U^{(i_1)}_{\pi/2,\pi}$, $U^{(i_2)}_{\pi/2,0}$, $U^{(i_2)}_{\pi/2,\pi}$, …, $U^{(i_k)}_{\pi/2,0}$, $U^{(i_k)}_{\pi/2,\pi}$, are *selected and activated* by an oracle

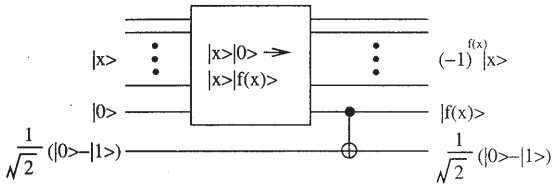

Fig. 11. Alternative circuit for the oracle call I_{w_0}.

subroutine and transmitted to the oracle block O in Fig. 10, yielding the unitary operator I_{w_0}. This "hard wiring" approach is easy to implement. □

Finally, the following theorem interprets the I block in Figure 10.

Theorem 9.

$$U_{\pi,0}^{(1)} U_{-\pi/4,\pi/2}^{(1)} U_{-\pi/4,\pi/2}^{(2)} \cdots U_{-\pi/4,\pi/2}^{(n)} K_n \cdot U_{\pi/4,-\pi/2}^{(n)} U_{\pi/4,-\pi/2}^{(n-1)} \cdots U_{\pi/4,-\pi/2}^{(1)} = -I_s . \quad (4.9)$$

Proof. First note that

$$U_{\pi/4,-\pi/2}|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle].$$

Thus, similarly to (4.4) and (4.5), we have

$$\begin{aligned} &(U_{\pi/4,-\pi/2}^{(1)}|1\rangle) \otimes (U_{\pi/4,-\pi/2}^{(2)}|1\rangle) \otimes \cdots \otimes (U_{\pi/4,-\pi/2}^{(n)}|1\rangle) \quad (4.10)\\ &= U_{\pi/4,-\pi/2}^{(1)} U_{\pi/4,\pi/2}^{(2)} \cdots U_{\pi/4,-\pi/2}^{(n)}|11\cdots 1\rangle \\ &= \frac{1}{2^{n-2}}[|00\cdots 00\rangle + \cdots + |11\cdots 11\rangle] = |s\rangle . \end{aligned}$$

Hence, from (4.10) and the fact that $U^*_{\pi/4,-\pi/2} = U_{\pi/4,\pi/2}$, we have

$$\begin{aligned} I_s &= I - 2|s\rangle\langle s| \\ &= I - 2U_{\pi/4,-\pi/2}^{(1)} U_{\pi/4,\pi/2}^{(2)} \cdots U_{\pi/4,-\pi/2}^{(n)}|11\cdots 1\rangle \\ &\quad \cdot \langle 11\cdots 1|U_{\pi/4,\pi/2}^{(n)} \cdots U_{\pi/4,\pi/2}^{(1)} \\ &= U_{\pi/4,-\pi/2}^{(1)} U_{\pi/4,-\pi/2}^{(2)} \cdots U_{\pi/4,-\pi/2}^{(n)} [I - 2|11\cdots 1\rangle \cdot \langle 11\cdots 1|] \\ &\quad \cdot U_{\pi/4,\pi/2}^{(n)} \cdots U_{\pi/4,\pi/2}^{(1)} . \end{aligned}$$

The rightmost gate in the I Block in Fig 10, $U_{\pi,0}^{(1)}$, just represents $-I$. Hence (4.9) follows. □

Remark 4. Using Remark 2 and Fig. 10, we see that in order to perform one iteration $G|s\rangle$, we need as many as

$$2(22n-75)+5n+1 = 49n - 149$$

elementary quantum gates. To perform $G^k|s\rangle$, we need no more than

$$2k(22n-75)+n+(4n+1)k = (48k+1)n - 149k$$

elementary quantum optical operations. The total number of qubits required is actually $n+(n-3) = 2n-3$, where we recall that $n-3$ is the number of scratch bits used in Theorem 5. □

Summary

In this paper, we have presented a circuit design for the implementation of Grover's algorithm for an arbitrary number of objects in the search database. The circuit consists of only two types of quantum gates, namely the 1-bit unitary gate and the 2-bit phase gate. A physical realization still remains a formidable task, as the number of phase gates increase significantly, though polynomially with increasing values of $\log N$. Even though we have used 1-bit gates based on resonant coupling of atoms with classical fields and 2-bit gates based on dispersive coupling of atoms with cavity fields, there is good evidence that devices made of ion traps or quantum dots are modelled similarly or even identically by the same 1-bit and 2-bit gates and, thus, the circuit design should remain little changed. Also, the "hard wiring" oracle call needs to be addressed more carefully.

Acknowledgements

[1] P. Shor, Algorithms for quantum computation: Discrete Logarithms and Factoring, in Proceedings of the 35th IEEE Symposium on the Foundations of Computer Science, IEEE Press, Piscataway, NJ 1994, pp. 124–134.

[2] L. Grover, Quantum Mechanics helps in Searching for a Needle in a Haystack, Phys. Rev. Lett. **78**, 325 (1997).

[3] E. Farhi and S. Gutmann, Analog Analogue of a Digital Quantum Computation, Phys. Rev. **A57**, 2403 (1998).

[4] S. Lloyd, Quantum Search without Entanglement, Phys. Rev. **A61**, 010301(R) (2000).

[5] I. L. Chuang, N. Gershenfeld, and M. Kubinec, Experimental Implementation of fast quantum searching, Phys Rev. Lett. **80**, 3408 (1998).

[6] P. G. Kwiat, J. R. Mitchell, P. D. D. Schwindt, and A. G. White, Grover's Search Algorithm: An Optical Approach, J. Mod. Optics **47**, 257 (1999).

[7] M. O. Scully and M. S. Zubairy, Quantum Optical Implementation of Grover's Algorithm, Proc. Natl. Acad. Sci. USA **98**, 9490 (2001).

[8] J. Ahn, T. C. Weinacht, and P. H. Bucksbaum, Information Storage and Retrieval through Quantum Phase, Science **287**, 463 (2000).

[9] A. Rauschenbeutel, G. Nogues, S. Osnaghi, P. Bertet, M. Brune, J. M. Raimond, and S. Haroche, Coherent Operation of a Tunable Quantum Phase Gate in Cavity QED, Phys. Rev. Lett. **83**, 5166 (1999). See also, Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble, Measurement of Conditional Phase Shifts for Quantum Logic, Phys. Rev. Lett. **75**, 4710 (1995).

[10] M. O. Scully and M. S. Zubairy, Quantum Optics, Cambridge Univ. Press, Cambridge, U.K. 1997.

[11] A. Barenco, C. H. Bennett, R. Cleve, D. DiVincenzo, N. Mangolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Elementary Gates for Quantum Computation, Phys. Rev. **A52**, 3457 (1995).

[12] G. Chen, S. A. Fulling, and J. Chen, Generalization of Grover's Algorithm to Multi-object Search in Quantum Computing, Part I: Continuous Time and Discrete Time, quant-ph/0007123. Also, in Chapt. 6 of "Mathematics of Quantum Computation", edited by R. K. Brylinski and G. Chen, CRC Press, Boca Raton, Florida, 2002, pp. 135–160.