Quantum Database Searching by a Single Query

DONG PYO CHI *† and JINSOO KIM *‡

15 July 1997

Abstract

In this paper we give a quantum mechanical algorithm that can search a database by a single query, when the number of solutions is more than a quarter. It utilizes modified Grover operator of arbitrary phase.

1 Introduction

For $N \in \mathbb{N}$, let $\mathbb{Z}_N = \{0, 1, \ldots, N - 1\}$ denote the additive cyclic group of order $N$ and consider an arbitrary function $F : \mathbb{Z}_N \to \mathbb{Z}_2$. The database searching problem is to find some $i \in \mathbb{Z}_N$ such that $F(i) = 1$ under the assumption that such an $i$ exists. We assume that the structure of $F$ is unknown so that it is not possible to obtain a knowledge about $F$ without evaluating it on $\mathbb{Z}_N$.

Let $t = |\{i \in \mathbb{Z}_N : F(i) = 1\}|$. There is a quantum mechanical algorithm to solve this problem in expected time of order $O(\sqrt{N/t})$, which is optimal up to a multiplicative constant [4, 2, 1]. Especially when $t = N/4$ is known, the original Grover algorithm in [4] can search a solution only by a single query [2]. It uses the $\pi$-phase, i.e., marking the states by multiplying $e^{\pi i} = -1$. When $t = N/2$, by changing this phase to $\pi/2$, that is, by marking the states by multiplying $e^{\pi i/2} = i$ and modifying the corresponding diffusion transform according to this phase, the solution can be found with certainty after a single iteration [3].

In this paper, we generalize Grover algorithm for arbitrary phase. When $t \geq N/4$, we give generalized conditional phase and diffusion transform.

---

*Department of Mathematics, Seoul National University, Seoul 151-742, Korea.
†E-mail address: dpchi@math.snu.ac.kr
‡E-mail address: jskim@math.snu.ac.kr
depending on \( t \), and then formulate a quantum mechanical algorithm that solves the database searching problem in a single query.

2 Grover Operator of Arbitrary Phase

Let \( \mathcal{B}_N = \{ |a\rangle \}_{a \in \mathbb{Z}_2^N} = \{ |e_1\rangle, |e_2\rangle, \ldots, |e_N\rangle \} \) be the standard basis of an \( n \)-qubit quantum register with \( N = 2^n \) and \( \mathcal{H}_N \) be the corresponding Hilbert space, which represents the state vectors of a quantum system. Let \( \mathcal{H}_m \) be an \( m \)-dimensional subspace of \( \mathcal{H}_N \) spanned by a basis \( \mathcal{B}_m = \{ |e_{i_1}\rangle, |e_{i_2}\rangle, \ldots, |e_{i_m}\rangle \} \). Let \( l \) be a positive integer such that \( 1 \leq l \leq m \).

For \( \gamma \in \mathbb{R} \), the conditional \( \gamma \)-phase transform on a subspace \( \mathcal{H}_m \), \( S^\mathcal{H}_m : \mathcal{H}_m \to \mathcal{H}_m \) is defined by

\[
S^\mathcal{H}_m |e_{ik}\rangle = (e^{i \gamma})^F(e_{ik}) |e_{ik}\rangle,
\]

for \( k = 1, 2, \ldots, m \), where \( i = \sqrt{-1} \). Let \( S^\mathcal{H}_m \) denote \( S^\mathcal{H}_m \), where \( F_l(e_{ik}) = \delta_{ik} \).

Let \( W^\mathcal{H}_m \) be any unitary transformation on \( \mathcal{H}_m \) satisfying

\[
W^\mathcal{H}_m |e_{il}\rangle = \frac{1}{\sqrt{m}} \sum_{k=1}^{m} |e_{ik}\rangle.
\]

For example, when \( m \) is a power of 2, in a suitably arranged basis we may set \( W^\mathcal{H}_m \) to be the Walsh-Hadamard transform. When \( m \) is not a power of 2, the approximate Fourier transform in [5] can be used.

For \( \beta \in \mathbb{R} \), the \( \beta \)-phase diffusion transform on a subspace \( \mathcal{H}_m \), \( D^\mathcal{H}_m : \mathcal{H}_N \to \mathcal{H}_N \) is defined by

\[
D^\mathcal{H}_m |e_i|D^\mathcal{H}_m |e_j\rangle = \begin{cases} 
\frac{e^{i \beta} - 1}{m} & \text{when } |e_i\rangle, |e_j\rangle \in \mathcal{B}_m \text{ and } i \neq j, \\
1 + \frac{e^{i \beta} - 1}{m} & \text{when } |e_i\rangle, |e_j\rangle \in \mathcal{B}_m \text{ and } i = j, \\
\delta_{ij} & \text{otherwise}.
\end{cases}
\]

If we rearrange the basis \( \mathcal{B}_N \) so that \( \mathcal{B}_m = \{ |e_1\rangle, |e_2\rangle, \ldots, |e_m\rangle \} \) and represent \( D^\mathcal{H}_m \) by its matrix \( D^\mathcal{H}_m = (D^\mathcal{H}_{m,ij}) \), then we have

\[
D^\mathcal{H}_m = \begin{bmatrix}
W^\mathcal{H}_m S^{\mathcal{H}_m} W^\mathcal{H}_m & 0 \\
0 & I
\end{bmatrix} = \begin{bmatrix}
I + (e^{i \beta} - 1)P^\mathcal{H}_m & 0 \\
0 & I
\end{bmatrix},
\]
where $P^{H_m} = (P^{H_m})$ is a projection matrix in $H_m$ with $P_{ij}^{H_m} = \frac{1}{m}$. Note that $S_{F,\gamma}^{H_m}$ and $D^{H_m}_\beta$ are unitary.

Let $G^{H_m}_{F,\beta,\gamma} : H_N \rightarrow H_N$ be the Grover operator of $(\beta, \gamma)$-phase in $H_m$ defined by

$$G^{H_m}_{F,\beta,\gamma} = D^{H_m}_\beta S^{H_m}_{F,\gamma}.$$ 

When $\beta = \gamma$ set $G^{H_m}_{F,\gamma} = G^{H_m}_{F,\gamma,\gamma}$. For simplicity, we shall assume that $m = N$ and omit the superscript $H_m$.

Let $A = \{ e_j \in \mathbb{Z}_N^2 | F(e_j) = 1 \}$, 

$B = \{ e_j \in \mathbb{Z}_N^2 | F(e_j) = 0 \}$,

and let $t = |A|$. For $k, l \in \mathbb{C}$ such that $t|k|^2 + (N - t)|l|^2 = 1$, define

$$|\psi(k,l)\rangle = \sum_{e_j \in A} k|e_j\rangle + \sum_{e_j \in B} l|e_j\rangle.$$ 

**Lemma 1** For $\beta, \gamma \in \mathbb{R}$, let

$$|\psi(k_j,l_j)\rangle = G^{H_m}_{F,\beta,\gamma}|\psi(k_0,l_0)\rangle.$$ 

Then after applying $j + 1$ Grover operator of $(\beta, \gamma)$-phase, we have

$$\begin{cases} 
k_{j+1} = (e^{i\beta} - 1) t + N e^{i\gamma} k_j + \frac{(e^{i\beta} - 1)(N - t)}{N} l_j, \\
l_{j+1} = (e^{i\beta} - 1) t + N e^{i\gamma} l_j + \frac{(e^{i\beta} - 1)(N - t) + N}{N} l_j. \end{cases}$$

(2.1)

**Theorem 1** Assume that $k_0 = l_0$ and $\beta, \gamma \in [0, 2\pi]$. Then $l_1 = 0$ if and only if $\frac{N}{4} \leq t \leq N$ and $\beta = \gamma = \cos^{-1} \left(1 - \frac{N}{2t}\right)$. In this case, $k_1 = (e^{i\gamma} - 1)k_0$.

**Proof.** By (2.1), we get

$$\begin{cases} 
k_1 = \left[(e^{i\beta} - 1)(e^{i\gamma} - 1) \frac{t}{N} + e^{i\gamma} + e^{i\beta} - 1\right] k_0, \\
l_1 = \left[(e^{i\beta} - 1)(e^{i\gamma} - 1) \frac{t}{N} + e^{i\beta}\right] l_0. \end{cases}$$

(2.2)

By considering the imaginary part of $e^{-i\beta} \frac{t}{l_0}$, the equation

$$\frac{t}{N} \{ (1 - \cos \beta) \sin \gamma + (\cos \gamma - 1) \sin \beta \} = 0$$

3
is equivalent to
\[
\frac{1 - \cos \beta}{\sin \beta} = \frac{1 - \cos \gamma}{\sin \gamma} \quad .
\]
(2.3)

Considering the real part of \( e^{-i\beta \frac{t}{N}} \), from (2.3) it follows that the equation
\[
\frac{t}{N} \{(1 - \cos \beta)(1 - \cos \gamma) + \sin \beta \sin \gamma\} - 1 = 0
\]
is equivalent to
\[
\cos \beta = \cos \gamma = 1 - \frac{N}{2t} \quad .
\]
Again by (2.3), we get \( \beta = \gamma \) and \( t \geq \frac{N}{4} \). Furthermore, by (2.2) we obtain \( k_1 = (e^{i\gamma} - 1)k_0 \). This completes the proof.

For the case of \( \pi \)-phase in [4], \( -D_\pi = -I + 2P \) is an inversion about average operation and we have
\[
-D_\pi |\psi(k,l)\rangle = \left| \psi\left( -\frac{N-2t}{N}k + \frac{2(N-t)}{N}l, \frac{N-2t}{N}l + \frac{2t}{N}k \right) \right| .
\]
In this case, there is an explicit closed-form formula for \( k_j \) and \( l_j \);
\[
\begin{cases}
  k_j = (-1)^j \frac{1}{\sqrt{t}} \sin ((2j + 1)\theta), \\
  l_j = (-1)^j \frac{1}{\sqrt{N-t}} \cos ((2j + 1)\theta),
\end{cases}
\]
for \( j = 0, 1, \ldots \), where the angle \( \theta \) is defined so that \( \sin^2 \theta = \frac{t}{N} \) [2]. Especially when \( t = N/4 \), we have \( l_1 = 0 \).

Grover operator of \( \frac{\pi}{2} \)-phase was used in [3]. Since
\[
D_{\frac{\pi}{2}} |\psi(k,l)\rangle = \left| \psi\left( \left( \frac{1-1}{N} + \frac{(1-1)(N-t)}{N}k + \frac{(1-1)(N-t)}{N}l, \frac{(1-1)(N-t)}{N}l + \frac{(1-1)}{N}Nk \right) \right) \right| ,
\]
when \( t = \frac{N}{2} \), we have
\[
G_{F,\frac{\pi}{2}} |\psi(k,k)\rangle = |\psi((t-1)k,0)\rangle .
\]

By Theorem 1, When \( t \in [N/4, N] \), we have
\[
G_{F,\gamma} |\psi(k_0,k_0)\rangle = |\psi((e^{i\gamma} - 1)k_0,0)\rangle ,
\]
where the phase \( \gamma \) is defined by \( \gamma = \cos^{-1}\left( 1 - \frac{N}{2t} \right) \).
References


