Scholars Journal of Physics, Mathematics and Statistics OPEN ACCESS
Abbreviated Key Title: Sch J Phys Math Stat
ISSN 2393-8056 (Print) | ISSN 2393-8064 (Online)
Journal homepage: https://saspublishers.com

Several Remarks on Grover's Quantum Search Algorithm with a Single Marked Element

Qi Han[1], Yanan Han[1*], Ziqiang Lu[1], Yaxin Kou[1]

[1]College of Mathematics and Statistics, Northwest Normal University, Lanzhou, 730070, Gansu P.R. China

DOI: 10.36347/sjpms.2021.v08i03.002 | **Received:** 09.02.2021 | **Accepted:** 19.03.2021 | **Published:** 28.03.2021

***Corresponding author:** Yanan Han

Abstract **Review Article**

The Grover's quantum search algorithm is one of the most important quantum algorithms. In this article, we mainly discuss related properties of the Grover's quantum search algorithm with a single marked element. We show that the range of constant c when the probability of measured value x_0 is p.

Keywords: Grover's algorithm; unitary operator; reflection operators; optimality.

Copyright © 2021 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution **4.0 International License (CC BY-NC 4.0)** which permits unrestricted use, distribution, and reproduction in any medium for non-commercial use provided the original author and source are credited.

INTRODUCTION

Search algorithm is a common algorithm. The efficiency of classical computer to the data search is relatively low, and the computational complexity is $O(N)$, where N is the number of database entries. Correspondingly, the Grover's quantum search algorithm in quantum computers, and the time complexity of Grover's algorithm is $O(\sqrt{N})$. Grover's quantum search algorithm originally designed to look for an element in an unsorted database with no repeated elements. In the case of a large number of database entries, the superiority of Grover's quantum search algorithm is extremely obvious. Grover's algorithm can realize the quadratic acceleration of classical algorithm; therefore, Grover's quantum search algorithm is introduced on this basis which has a wide applicability [1, 2, 3, 9].

The evolution operator and the initial condition of Grover's algorithm have real entries, then means that the entire evolution takes place in a real vector subspace of the Hilbert space H^{2N} [1]. However, the key to this algorithm is that evolution operator U is the product of two reflection operators $R_{x_0^{\perp}}$ and R_D, where $R_{x_0^{\perp}}$ is a reflection operator around the vector space spanned by the vector orthogonal to $|x_0\rangle$ with point x_0 is called a marked element, R_D is a reflection operator around the vector space spanned by $|D\rangle$. In real vector spaces, the operation of two successive reflection operators on the initial vector will cause the initial vector to rotate by an angle. Starting from initial condition $|D\rangle$, one application of U rotates $|D\rangle$ approximately by $\frac{2}{\sqrt{N}}$ degrees toward $|x_0\rangle$. So far, no algorithm can find the marked element faster than Grover's algorithm and the probability of success is greater than or equal to $1-\frac{1}{N}$. There are many other interesting results about Grover's quantum search algorithm. For example, the Grover's algorithm searches for repeated elements and amplitude amplification technique and operator coherence dynamics of Grover's algorithm [6, 7, 8, 10, 11].

In this paper, we show that the related properties of Grover's quantum search algorithm with single marked element. In Section 2, we briefly describe some concepts of Grover's algorithm. In Section 3, we show that related properties of unitary evolution and optimality of Grover's algorithm. In Section 4, we have a briefly summarize of the whole article.

2 Some concepts of Grover's algorithm

Definition 2.1 [5] (Classical search algorithm): Suppose that f is a function with domain

$\{0,\cdots,N-1\}$, where $N=2^n$ and n is some positive integers, and image

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

The function image is 1 only for a single point x_0 and 0 for all other points. In this problem, exhaustive search on point x_0 is carried out through query function f, and the time complexity of classical algorithm is $\Omega(N)$, function f is called query database, and point x_0 is called marked element.

In [1, 4], for the quantum context, the unitary operator is used based on function f, and the full description of this operator is called R_f, in the computational basis is

$$R_f|x\rangle|i\rangle=|x\rangle|i\oplus f(x)\rangle,$$

Here $\oplus$ means addition in modulo 2.

Grover's algorithm uses a second unitary defined by

$$R_D=(2|D\rangle\langle D|-I_N)\otimes I_2,$$

Where $|D\rangle$ the diagonal state of the first is register, I_N and I_2 are unit operators of N dimensional and 2 dimensional space, respectively. Thus the evolution operator that performs one step of the algorithm is

$$U=R_DR_f.$$

The initial condition is $|\psi_0\rangle=|D\rangle|-\rangle$ Where $|-\rangle=\frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

Remark 2.1 [1] (The process of Grover's quantum search algorithm) When the Grover's algorithm input is N and f in formula (2.1), and when the following four conditions are fulfilled

1, Use a 2-register quantum computer with $n+1$ quantum bits;
2, Prepare the initial state $|D\rangle|-\rangle$;
3, Apply U^t, where $t=\left\lfloor\frac{\pi}{4}\sqrt{N}\right\rfloor$ and U is given by (2.2);
4, Measure the first register in the computational basis,
Where $\lfloor\ \rfloor$ is the integral to the left of a real number?

Then the output of the algorithm is x_0 and its probability is greater than or equal to $1-\frac{1}{N}$.

3 Basic properties of unitary evolution and optimality of Grover's algorithm

In [1, 5, 6], the evolution operator and the initial condition of Grover's algorithm have real entries, this means that the entire evolution takes place in a real vector subspace of the Hilbert space H^{2N}, the key of the algorithm is the product operator U of two reflection operators R_f and R_D. Let $|x_0^{\perp}\rangle$ be a unit vector that is orthogonal to $|x_0\rangle$, which is in the plane spanned by $|x_0\rangle$ and $|D\rangle$ and has the smallest angle with $|D\rangle$, the expression for $|x_0^{\perp}\rangle$ in the computer is $|x_0^{\perp}\rangle=\frac{1}{N-1}\sum_{x\neq x_0}|x\rangle$, and in the evolution of the plane spanned by $|x_0\rangle$ and

$|D\rangle$, the operator R_f can be replaced by $R_{x_0^{\perp}}$,

$$R_{x_0^{\perp}}=2|x_0^{\perp}\rangle\langle x_0^{\perp}|-I_N.$$

Therefore, the evolution operator U of the Grover's algorithm is replaced by $U=R_DR_{x_0^{\perp}}$, where the initial condition is $|D\rangle$.

The initial condition of Grover's algorithm is state $|D\rangle$. After applying the operator R_f, state $|D\rangle$ is reflected around the plane orthogonal to vector $|x_0\rangle$. After applying operator R_D, vector $R_f|D\rangle$ is reflected around $|D\rangle$. That is, one application of U rotates the initial vector by θ degrees toward vector $|x_0\rangle$.

Lemma 3.1 [1] Let $\frac{\theta}{2}$ be the angle between vectors $|x_0^{\perp}\rangle$ and $|D\rangle$, which is the complement of the angle between $|x_0^{\perp}\rangle$ and $|D\rangle$. So

$$\sin\frac{\theta}{2}=\cos(\frac{\pi}{2}-\frac{\theta}{2})=\langle x_0|D\rangle=\frac{1}{\sqrt{N}},$$

When function f has a large domain, we obtain

$$\theta=\frac{2}{\sqrt{N}}+\frac{1}{3N\sqrt{N}}+O(\frac{1}{N^2}),$$

and at $t_f = \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor$, the probability of finding x_0 is

$$p_{x_0} = \left|\langle x_0 | U^{t_f} | D\rangle\right|^2 = \cos^2\frac{\theta}{2} = 1 - \frac{1}{N}.$$

After understanding basic concepts of the algorithm, we discuss some fundamental properties of the algorithm. For example, properties of unitary operator and the rotation angle θ.

lemma 3.1 For a diagonal state $|D\rangle$, the t-th power of evolution operator U has the following form:

$$U^t|D\rangle = \sin(t\theta + \frac{\theta}{2})|x_0\rangle + sos(t\theta + \frac{\theta}{2})|x_0^{\perp}\rangle.$$

In order to understand the relationship between the probability of success (find the marked element) and the probability of failure (unfound the marked element), we give the following proposition.

Proposition 3.2 For all case $x \neq x_0$ and $x = x_0$, the sum of the probability of Grover's algorithm at $N \geq 1$ is asymptotically equal to 1.

Proof. The known fact:

$$P_{x_0} = \left|\langle x_0 | U^{t_f} | D\rangle\right|^2,$$

$$U^{t_f}|D\rangle = \sin(t_f\theta + \frac{\theta}{2})|x_0\rangle + \cos(t_f\theta + \frac{\theta}{2})|x\rangle,$$

$$\theta = \frac{2}{\sqrt{N}} + \frac{1}{3N\sqrt{N}} + O(\frac{1}{N^2}), t_f = \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor,$$

then

$$P_x = \left|\langle x | U^{t_f} | D\rangle\right|^2 = \left|\cos(t_f\theta + \frac{\theta}{2})\right|^2 = \cos^2(t_f\theta + \frac{\theta}{2})$$

$$= \left[\cos(\frac{\pi}{4}\sqrt{N} \times \frac{2}{\sqrt{N}} + \frac{1}{2}\frac{2}{\sqrt{N}})\right]^2$$

$$= \left[\cos(\frac{\pi}{2} + \frac{1}{\sqrt{N}})\right]^2 = \sin^2\frac{1}{\sqrt{N}} \approx \left|\frac{1}{\sqrt{N}}\right|^2 = \frac{1}{N},$$

and

$$P_{x_0} = \sin^2(\frac{\pi}{2} + \frac{1}{\sqrt{N}}) = \cos^2\frac{1}{N} = \frac{1 - \cos\frac{2}{\sqrt{N}}}{2} \approx \frac{1 + 1 - \frac{2}{N}}{2} = 1 - \frac{1}{N}.$$

So

$$P_x + P_{x_0} \approx 1.$$

In [1, 5, 6, 7], the Grover's quantum search algorithm finds the marked element by querying the oracle $O(\sqrt{N})$ times. And have proved that Grover's algorithm is optimal, that is, no algorithm can find the marked element faster than Grover's algorithm and the probability of success is greater than or equal to $1 - \frac{1}{N}$, by [1] we can know that the $|\psi_0\rangle$ be the initial state, the quantum state after t steps is given by

$$|\psi_t\rangle = U_t R_f \cdots U_1 R_f U_0 |\psi_0\rangle,$$

Where $U_1, \cdots, U_t$ are generic unitary operators, further, the quantum state is defined as

$$|\phi_t\rangle = U_t \cdots U_0 |\psi_0\rangle,$$

by iteration of general unitary operators.

To prove the optimality of the Grover's algorithm, one way that is to compare state $|\psi_t\rangle$ and $|\phi_t\rangle$, then define a quantity again

$$D_t = \frac{1}{N}\sum_{x_0=0}^{N-1}\left\||\psi_t\rangle - |\phi_t\rangle\right\|^2,$$

Which measures the deviation between $|\psi_t\rangle$ and $|\phi_t\rangle$ after t steps.

Through [1, 7], the Grover's quantum search algorithm is optimal when the following inequality is true

$$c \le D_t \le \frac{4t^2}{N},$$

Where c is a strictly positive constant.

We know that the constant c is related to the probability of measuring the return value of x_0, without loss of generality, we will talk about the range of constant c when the probability is a general number p.

Proposition 3.3 If the probability of measurement value x_0 is greater than or equal to p, the constant c is in the range of

$$0 < c < (\sqrt{2} - \sqrt{2-2\sqrt{p}})^2.$$

Proof. According to the optimality of Grover's algorithm, the following formula holds:

$$c \le D_t \le \frac{4t^2}{N}$$

Where $D_t = \frac{1}{N}\sum_{x_0=0}^{N-1}\left\||\psi_t\rangle - |\phi_t\rangle\right\|^2$, $|\psi_t\rangle = U_t R_f \cdots U_1 R_f U_0 |\psi_0\rangle$, $|\phi_t\rangle = U_t \cdots U_0 |\psi_0\rangle$,

$|\psi_0\rangle$ is the initial state, $R_f = I - 2|x_0\rangle\langle x_0|$, $U_1, \cdots, U_t$ are generic unitary operators.

We know the fact that $D_t \le \frac{4t^2}{N}$, so let us prove the range of c. Let us define two new quantities given by

$$E_t = \frac{1}{N}\sum_{x_0=0}^{N-1}\left\||\psi_t\rangle - |x_0\rangle\right\|^2, F_t = \frac{1}{N}\sum_{x_0=0}^{N-1}\left\||\phi_t\rangle - |x_0\rangle\right\|^2.$$

We obtain an inequality involving D_t, E_t and F_t as following:

$$\begin{aligned}
D_t &= \frac{1}{N}\sum_{x_0=0}^{N-1}\left\||\psi_t\rangle - |\phi_t\rangle\right\|^2 \\
&= \frac{1}{N}\sum_{x_0=0}^{N-1}\left\|(|\psi_t\rangle - |x_0\rangle) + (|x_0\rangle - |\phi_t\rangle)\right\|^2 \\
&\ge \frac{1}{N}\sum_{x_0=0}^{N-1}[\left\||\psi_t\rangle - |x_0\rangle\right\|^2 - 2\left\||\psi_t\rangle - |x_0\rangle\right\|\left\||\phi_t\rangle - |x_0\rangle\right\| + \left\||x_0\rangle - |\phi_t\rangle\right\|^2] \\
&= E_t + F_t - \frac{2}{N}\sum_{x_0=0}^{N-1}\left\||\psi_t\rangle - |x_0\rangle\right\|\left\||\phi_t\rangle - |x_0\rangle\right\| \\
&\ge E_t + F_t - \frac{2}{N}\sum_{x_0=0}^{N-1}(\left\||\psi_t\rangle - |x_0\rangle\right\|)^{\frac{1}{2}}(\left\||\phi_t\rangle - |x_0\rangle\right\|)^{\frac{1}{2}} \\
&= E_t + F_t - 2\sqrt{E_t F_t} = (\sqrt{F_t} - \sqrt{E_t})^2.
\end{aligned}$$

We now show that $F_t \geq 2-2\frac{1}{\sqrt{N}}$, define θ_{x_0} as the phase of $\langle x_0|\phi_t\rangle$, that is

$$\langle x_0|\phi_t\rangle = e^{i\theta_{x_0}}\left|\langle x_0|\phi_t\rangle\right|.$$

Define the state

$$|\theta\rangle = \frac{1}{\sqrt{N}}\sum_{x_0=0}^{N-1} e^{i\theta_{x_0}}|x_0\rangle.$$

So,

$$\langle\theta|\phi_t\rangle = \frac{1}{\sqrt{N}}\sum_{x_0=0}^{N-1} e^{-i\theta_{x_0}}\langle x_0|\phi_t\rangle$$

$$= \frac{1}{\sqrt{N}}\sum_{x_0=0}^{N-1}\left|\langle x_0|\phi_t\rangle\right| = \frac{1}{\sqrt{N}}\times N = \sqrt{N}.$$

Using the Cauchy-Schwarz inequality, we obtain $\left|\langle\theta|\phi_t\rangle\right| \leq 1$, we use the above inequality and the fact that the real part of $\langle x_0|\phi_t\rangle$ is smaller than or equal to $\left|\langle x_0|\phi_t\rangle\right|$:

$$F_t = \frac{1}{N}\sum_{x_0=0}^{N-1}\left\||\phi_t\rangle - |x_0\rangle\right\|^2$$

$$= \frac{1}{N}\sum_{x_0=0}^{N-1}(\langle\phi_t| - \langle x_0|)(|\phi_t\rangle - |x_0\rangle)$$

$$= \frac{1}{N}\sum_{x_0=0}^{N-1}(\langle\phi_t|\phi_t\rangle - \langle\phi_t|x_0\rangle - \langle x_0|\phi_t\rangle + \langle x_0|x_0\rangle)$$

$$= 2-\frac{2}{N}\mathrm{Re}\{\langle x_0|\phi_t\rangle\} \geq 2-\frac{2}{N}\sum_{x_0=0}^{N-1}\left|\langle x_0|\phi_t\rangle\right| \geq 2-\frac{2}{\sqrt{N}}$$

After t steps, the state of the quantum computer after the application of the oracles is $|\psi_t\rangle$. Similar to the calculation used for F_t, we have

$$E_t = \frac{1}{N}\sum_{x_0=0}^{N-1}\left\||\psi_t\rangle - |x_0\rangle\right\|^2 = 2-\frac{2}{N}\sum_{x_0=0}^{N-1}\mathrm{Re}\{\langle x_0|\psi_t\rangle\}.$$

Let us assume that the probability of a measurement to return value x_0 is greater than or equal to p, that is, $\left|\langle x_0|\psi_t\rangle\right|^2 \geq p$ for all x_0. Value p is arbitrary between 0 and 1. we use basis $\{e^{i\alpha_0}|0\rangle,\cdots,e^{i\alpha_{N-1}}|N-1\rangle\}$, where α_{x_0} for $0 \leq x_0 \leq N$ is define as the phase of $\langle x_0|\psi_t\rangle$. In this basis, $\langle\tilde{x}_0|\psi_t\rangle$ is a real number, that is, $\mathrm{Re}\{\langle\tilde{x}_0|\psi_t\rangle\} = \left|\langle\tilde{x}_0|\psi_t\rangle\right|$. Therefore,

$$E_t = 2-\frac{2}{N}\sum_{x_0=0}^{N-1}\mathrm{Re}\{\langle\tilde{x}_0|\psi_t\rangle\}$$

$$= 2-\frac{2}{N}\sum_{x_0=0}^{N-1}\left|\langle\tilde{x}_0|\psi_t\rangle\right| \leq 2-\frac{2}{N}\sum_{x_0=0}^{N-1}\sqrt{p}$$

$$= 2-\frac{2}{N}\times N\sqrt{p} = 2-2\sqrt{p}$$

Using inequalities $E_t \leq 2-2\sqrt{p}$ and $F_t = \geq 2-\frac{2}{\sqrt{N}}$, We obtain

$$D_t \geq (\sqrt{F_t}-\sqrt{E_t})^2 \geq (\sqrt{2-\frac{2}{\sqrt{N}}}-\sqrt{2-2\sqrt{p}})^2$$

$$= (\sqrt{2}-\sqrt{2-2\sqrt{p}})^2 + O(\frac{1}{\sqrt{N}}).$$

This completes the proof of inequality $c \leq D_t$ for N large enough. Constant c must obey

$$0 < c < (\sqrt{2}-\sqrt{2-2\sqrt{p}})^2.$$

CONCLUSIONS

In this article, we prove the related properties of unitary evolution in Grover's quantum search algorithm, and prove the range of constant c when the probability of the measured value is p. However, we can further discuss properties related to the Grover's quantum search algorithm ability to find elements in a database of repeating elements and its algorithm optimality.

REFERENCES

1. Portugal R. Quantum walks and search algorithms. New York: Springer; 2013 Feb 16.
2. Grover LK. Quantum mechanics helps in searching for a needle in a haystack. Physical review letters. 1997 Jul 14;79(2):325.
3. Grover LK. Quantum computers can search rapidly by using almost any transformation. Physical Review Letters. 1998 May 11;80(19):4329.
4. Aharonov D. Quantum computation. Annual Reviews of Computational Physics VI. 1999:259-346.
5. Bennett CH, Bernstein E, Brassard G, Vazirani U. Strengths and weaknesses of quantum computing. SIAM journal on Computing. 1997 Oct;26(5):1510-23.
6. Nielsen MA and Chuang I. Quantum computation and quantum information; 2002.
7. Zalka C. Grover's quantum searching algorithm is optimal. Physical Review A. 1999 Oct 1;60(4):2746.
8. Taha MM, Perkowski M. Realization of arithmetic operators based on stochastic number frequency signal representation. In2018 IEEE 48th

International Symposium on Multiple-Valued Logic (ISMVL) 2018 May 16 (pp. 215-220). IEEE.
9. Zhang W. Quantum Algorithms for Two-Arm robot and generalization to Travelling Salesman Problem (2020, in Preparation); 2020.
10. Pan M, Qiu D. Operator coherence dynamics in Grover's quantum search algorithm. Physical Review A. 2019 Jul 31;100(1):012349.
11. Liu L, Xiao M, Song X. Authenticated semiquantum dialogue with secure delegated quantum computation over a collective noise channel. Quantum Information Processing. 2018 Dec;17(12):1-7.