

Notes on quantum search algorithm

Zhongwei Jiang, Linfeng Zhao

August 2, 2024

1 Quantum Computation

1.1 Quantum Gate

1.1.1 Single-qubit gate

The number of qubits in a quantum state depends on the number of classical bits in its dimension, so we usually call a vector $|\psi\rangle = a|0\rangle + b|1\rangle$ parameterized by two complex numbers a and b satisfying $|a|^2 + |b|^2 = 1$ a qubit. According to the constraints and phase redundancy, the quantum state can be mapped to the Bloch sphere with two parameters:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\varphi}|1\rangle \quad (1.1.1)$$

Operations on a qubit must preserve the norm, and thus are described by 2×2 unitary matrices. By $\det|U| = e^{2i\alpha}$ Then

$$e^{-i\alpha}U \in SU(2) \quad (1.1.2)$$

They're only off by one global phase, so we usually ignore the global phase and only consider $SU(2)$.

The Lie group $SU(2)$ has three generators $i\sigma_j$, σ_j called Pauli matrices:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (1.1.3)$$

From Lie group elements, any single-qubit unitary can be written as a product of exponentials of Pauli matrices by a global phase:

$$U = e^{i\alpha} \exp\left(-i\frac{\theta}{2}\vec{n} \cdot \vec{\sigma}\right) \quad (1.1.4)$$

\vec{n} is the coordinates of the rotation axis on the Bloch sphere. There is a homomorphism:

$$\begin{aligned} SU(2) &\rightarrow SO(3) \\ R_{\vec{n}}(\theta) &\mapsto \exp\left(-i\frac{\theta}{2}\vec{n} \cdot \vec{\sigma}\right) \end{aligned} \quad (1.1.5)$$

The former refers to the transformation on the Bloch sphere, and the latter for a single-qubit gate. Since we often need transformations on the Bloch sphere to visualize quantum gates, we will use $R_{\vec{n}}(\theta)$ to refer to $\exp\left(-i\frac{\theta}{2}\vec{n} \cdot \vec{\sigma}\right)$ directly in the following. So $R_{\vec{n}}(\theta) = \exp\left(-i\frac{\theta}{2}\vec{n} \cdot \vec{\sigma}\right)$.

According to the theorem:

Theorem 1.1.1. *The real number x and the matrix A such that $A^2 = I$ give us*

$$e^{iAx} = \cos(x)I + i\sin(x)A \quad (1.1.6)$$

we know that:

$$R_{\vec{n}}(\theta) = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)(\vec{n} \cdot \vec{\sigma}) \quad (1.1.7)$$

There is another form about $V \in SU(2)$:

$$V = R_{\vec{n}}(\beta)R_{\vec{m}}(\gamma)R_{\vec{n}}(\delta) \quad (1.1.8)$$

where $\vec{n} \neq k\vec{m}$, so we have:

$$U = e^{i\alpha}R_{\vec{n}}(\beta)R_{\vec{m}}(\gamma)R_{\vec{n}}(\delta) \quad (1.1.9)$$

In the following, we use XYZ instead of $\sigma_x\sigma_y\sigma_z$, here are some other single-qubit gate, which are frequently used listed here:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}. \quad (1.1.10)$$

1.1.2 Controlled operation

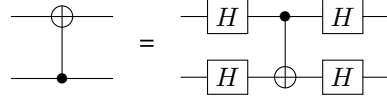
Analogous to the if statement of a classical circuit, we can use controlled-NOT gate to control target qubit with control qubit, its matrix form and circuit are shown as follows:

$$CNOT = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix} \quad (1.1.11)$$



$$(1.1.12)$$

CNOT gate makes the state of the target qubit be flipped when the control qubit is 1 and remain unchanged when the control qubit is 0. That is $|c\rangle|t\rangle \rightarrow |c\rangle X^c|t\rangle$. Considering a different basis then the control qubit does change and the control qubit could be flipped depending on the state of the 'target' qubit, show that:



$$(1.1.13)$$

We expect to extend this control from X to an arbitrary single-qubit gate U . That is, $|c\rangle|t\rangle \rightarrow |c\rangle U^c|t\rangle$ which is known as a controlled-U gate. Show that:



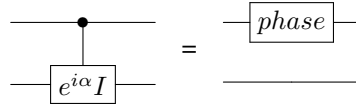
$$(1.1.14)$$

We wish to decompose this into a combination of single quantum bit gates and CNOT gates by introducing the theorem:

Theorem 1.1.2. *If U is a single quantum bit gate, then there exists $A, B, C \in SU(2)$, $ABC = I$, and then there is*

$$U = e^{i\alpha} AXBXC \quad (1.1.15)$$

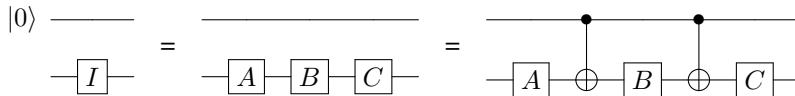
With this theorem, we can divide the controlled-U gate into several parts, looking first at the global phase part, which obviously has:



$$(1.1.16)$$

where $phase = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$.

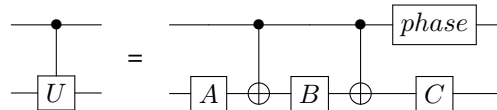
Looking at the $AXBXC$ part again, we have the expectation that if the control qubit is $|0\rangle$, then we do nothing, and adding a CNOT gate anywhere doesn't change that, so we have.



$$(1.1.17)$$

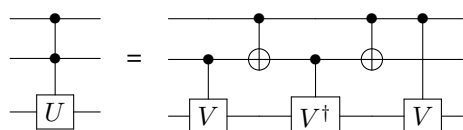
This construction also satisfies: if the control qubit is $|1\rangle$, then we apply $AXBXC$ to the target qubit.

So we have the controlled-U gate decomposition in this form:



$$(1.1.18)$$

Considering the case of multiple control Qubits, first look at the case of two control Qubits, you can construct: if V is a single qubit gate satisfying $V^2 = U$, we have:



$$(1.1.19)$$

Then we can extend this to the case of n control qubits, there are many kinds of construction methods, here we use recursive method to construct:

(1.1.20)

Ultimately we will show that any unitary operation can be composed to an arbitrarily good approximation from just H, S, T, CNOT gates. Here is the construction of the Toffoli gate:

(1.1.21)

1.2 Universal Gate Set

1.2.1 Single-qubit and CNOT gates are universal

In the previous subsection, we showed that $C^n(U)$ gate can be decomposed into a combination of single-qubit gates and CNOT gates. In this section, we will show that any unitary gate can be combined from $C^n(U)$ gate.

First, we introduce the theorem:

Theorem 1.2.1. Any D -dimensional unitary transformation U can always be decomposed into the product of $d(d-1)/2$ two-level unitary transformations under natural basis.

So exists two-level unitary transformations V_j made $U = \prod_{j=1}^{d(d-1)/2} V_j$ ¹. Two-level unitary transformations are unitary matrices which act non-trivially only on two-or-fewer vector components. The proof idea of this theorem is simple², let's focus on the two-level unitary transformations V .

Consider the binary expansion of the two bases $|s\rangle$ and $|t\rangle$ on which V operates, where $s = s_1 \dots s_n$ and $t = t_1 \dots t_n$. We can use Toffoli gate to turn s_j into t_j , after $n-1$ steps $|s_1 \dots s_{k-1} s_k s_{k+1} \dots s_n\rangle$ into $|t_1 \dots t_{k-1} s_k t_{k+1} \dots t_n\rangle$. It puts $|s\rangle$ and $|t\rangle$ in the same qubit and makes V into a $C^n(\tilde{V})$ gate which \tilde{V} is the non-trivial 2×2 unitary submatrix of V .

Let's take an example to illustrate this theorem, consider the U gate:

$$V = \begin{pmatrix} a & 0 & 0 & c \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ b & 0 & 0 & d \end{pmatrix} \quad \text{and} \quad \tilde{V} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \quad (1.2.1)$$

Notice that V acts non-trivially only on the states $|00\rangle$ and $|11\rangle$, so we can use the CNOT gate to turn $|00\rangle$ into $|01\rangle$, then we can get the $C(\tilde{V})$ gate. Here is the circuit of V :

(1.2.2)

So we have:

Theorem 1.2.2. Any unitary gate can be combined from single-qubit gates and CNOT gates.

¹Unless otherwise specified, the conjunction sign in this document is calculated according to the composite order of the map, that is $\prod_{j=1}^n a_j = a_n a_{n-1} \dots a_1$.

²Each single-qubit gates has $d(d-1)/2$ degrees of freedom and each two-level unitary transformations turn one of single-qubit gates elements into zero in order. So exists two-level unitary transformations V_j made $\left(\prod_{j=1}^{d(d-1)/2} V_j \right) U = I$.

1.2.2 Approximate universal operators with a discrete set

It is hard to implement all single-qubit, so we consider to approximate it with a discrete set which we can implement. We introduce the induced norm of operators to measure the degree of approximation:

$$E(U, V) = \|U - V\| = \sup_{\substack{|\psi\rangle \in \mathbb{C}^n \\ \|\psi\rangle = 1}} \|(U - V)|\psi\rangle\| \quad (1.2.3)$$

Where U is the target unitary operator that we wish to implement, V is the unitary operator that is actually implemented in practice, and $E(U, V)$ is the error when V is implemented instead of U . It is natural that:

Theorem 1.2.3. *in the approximation of m gates, the error add at most linearly:*

$$E\left(\prod_{j=1}^m U_j, \prod_{j=1}^m V_j\right) \leq \sum_{j=1}^m E(U_j, V_j) \quad (1.2.4)$$

Proof. Considering $|\psi_0\rangle$ which maximizes $\left\|\left(\prod_{i=1}^m U_i - \prod_{i=1}^m V_i\right)|\psi\rangle\right\|$ and definition $|\psi_i\rangle = V_i|\psi_{i-1}\rangle$, $|\Delta_i\rangle = U_i|\psi_{i-1}\rangle - |\psi_i\rangle$, we can see that

$$E\left(\prod_{j=1}^m U_j, \prod_{j=1}^m V_j\right) = \left\|\Delta_m\right\| + \sum_{j=1}^{m-1} \left\|\prod_{k=j+1}^m U_k\right\| \|\Delta_j\| \leq \sum_{j=1}^m \|\Delta_j\| \leq \sum_{j=1}^m E(U_j, V_j) \quad (1.2.5)$$

□

We are more concerned with the error of the approximation in the measurement. considering M is a POVM element in an arbitrary measurement POVM, and P_U (or P_V) is the probability of obtaining this outcome if U (or V) were performed with the state $|\psi\rangle$, We can prove¹ that:

$$|P_U - P_V| \leq 2E(U, V) \quad (1.2.6)$$

This makes it possible that if we want the probability difference between the approximate line and the ideal line on a certain outcome to be within a tolerance $\Delta > 0$, we only need to ensure that $E(U_j, V_j) \leq \Delta/(2m)$.

From the decomposition given by 1.1.9, we can further care about the degree of approximation of $R_{\vec{n}}(\theta)$. Let's start by introducing a neat theorem:

Theorem 1.2.4. *Considering $\alpha, \theta \in \mathbb{R}/2\pi\mathbb{Z}$, if $\theta/\pi \in \mathbb{R} \setminus \mathbb{Q}$, we can find a subsequences $\{x_n\}$ of sequences $\{n\}$ makes $\lim_{n \rightarrow \infty} x_n \theta = \alpha$.*

Proof. $\forall \epsilon > 0, \exists N = \frac{2\pi}{\epsilon}$, when $n > N$, we can find $|j\theta - k\theta| \leq \frac{2\pi}{n}$ which $j, k \in \{n\}, j > k$, let $x_n = (j - k) \left\lfloor \frac{\alpha}{|j\theta - k\theta|} \right\rfloor$, so we have $|x_n \theta - \alpha| < |j\theta - k\theta| \leq \frac{2\pi}{n} < \epsilon$. □

Further we have²:

$$\begin{aligned} & E(R_{\vec{n}}(\alpha), R_{\vec{n}}(\theta)^{x_n}) \\ &= E(R_{\vec{n}}(\alpha), R_{\vec{n}}(\alpha + (x_n \theta - \alpha))) \\ &= |1 - \exp((x_n \theta - \alpha)/2)| \leq \epsilon/2 \end{aligned} \quad (1.2.7)$$

According the proof, we just need to find the gate that has the Angle that the theorem requires. Fortunately, $THTH$ gate has the angel we need. It is a rotation of the Bloch sphere about an axis along $\vec{n} = (\cos \frac{\pi}{8}, \sin \frac{\pi}{8}, \cos \frac{\pi}{8})$ and through an angle θ defined by $\cos \frac{\theta}{2} = \cos^2 \frac{\pi}{8}$, so we just let $R_{\vec{n}}(\theta) = THTH$. To construct unitary operator U , we still need to approximate the rotation of the other axis, but even more fortunate is that $HR_{\vec{n}}(\theta)H$ is exactly what we need, has axis $\vec{m} = (\cos \frac{\pi}{8}, -\sin \frac{\pi}{8}, \cos \frac{\pi}{8})$ and the Angle, like $R_{\vec{n}}(\theta)$, is an irrational multiple of π . After layers and layers of preparation, let's list the final approximation with suitable positive integers x_n, y_n, z_n to U :

$$E(U, R_{\vec{n}}(\theta)^{x_n} H R_{\vec{n}}(\theta)^{y_n} H R_{\vec{n}}(\theta)^{z_n}) \leq \frac{3}{2}\epsilon \quad (1.2.8)$$

Theorem 1.2.5. *Given any single qubit unitary operator U and any $\epsilon > 0$, it is possible to approximate U to within ϵ ¹ using a circuit composed of H gates and T gates alone.*

¹Let $|\Delta\rangle = (U - V)|\psi\rangle$, notice that $\langle\psi|U^\dagger MU|\psi\rangle - \langle\psi|V^\dagger MV|\psi\rangle = \langle\psi|U^\dagger M|\Delta\rangle + \langle\Delta|MV|\psi\rangle$.

²The construction of x_n in this part is only to prove the existence, without considering the complexity. There are actually far less complex constructs.

¹The difference between Equation 1.2.8 and here by one coefficient can be solved by the setting of ϵ in the proof of Theorem 1.2.4, but it does not matter.

1.2.3 talking about complexity

1.3 Quantum Circuit Model

Read Section 4.6 of

2 Quantum Search Algorithm

Read Section 6.1 of [1].

References

- [1] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, December 2010.