4. Basics of Quantum Computer

Vaughan Sohn

October 7, 2024

Contents

Quantum Circuit model

Component of quantum circuit model

Qubit

Quantum Gates

Single-qubit gate

Single-qubit gate decomposition

Theorem 1 (ZY decomposition)

Suppose U is a unitary operation on a single qubit. Then there exist real numbers α, β, γ and δ such that,

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$$

Theorem 2

Suppose U is a unitary gate on a single qubit. Then there exist unitary operators A, B, C on a single qubit such that $ABC = I$ and

$$U = e^{i\alpha} AXBXC$$

where α is some overall phase factor and X is a Pauli-X operator.

Single-qubit gate decomposition

* Proof:

Controlled gate

Controlled gate decomposition

Controlled gate on multiple-qubit

Controlled gate on multiple-qubit decomposition

Summary

Some remarks

-

Universial Quantum gate set: $\{$CNOT, single qubit gates$\}$

Decomposition from n-qubit unitary gate to two-level unitary gates

Two-level unitary gate is controlled-U gate

Theorem 3

Unitary operator U which acts on a d-dimensional Hilbert space may be decomposed into a product of two-level unitary matrices;

$*$ Proof: from 3×3 example,

Two-level unitary gate is controlled-U gate

∗ Proof: (contd.)

Decomposition from n-qubit controlled-U gate to $\{$CNOT gates, single-qubit$\}$ $\Rightarrow$ Single qubit and CNOT gates are universal!

Theorem 4

n-qubit controlled-U gate can be decomposed into a single qubit gate and CNOT gates;

∗ Proof:

Decomposition from n-qubit controlled-U gate to $\{$CNOT gates, single-qubit$\}$ $\Rightarrow$ Single qubit and CNOT gates are universal!

$*$ Proof: (contd.)

Decomposition from n-qubit controlled-U gate to $\{$CNOT gates, single-qubit$\}$ $\Rightarrow$ Single qubit and CNOT gates are universal!

Corollary 5

single qubit and CNOT gates together can be used to implement an arbitrary n-qubit unitary operation.

$*$ Proof: Combine theorem 3 and 4, we can easily proof this corollary.$\square$

Circuit complexity

Summary

Some remarks

-

Universial Quantum Discrete gate set: $\{$CNOT, H, S, T$\}$

Approximating quantum circuits via discrete gate set

Definition 6 (approximation error)

We define the **error** when V is implemented instead of U by

$$E(U, V) \triangleq \max_{|\psi\rangle} \| (U - V) |\psi\rangle \|$$

where the maximum is over all normalized quantum states $|\psi\rangle$ in the state space.

✓ meaning:

Approximating quantum circuits via discrete gate set

Definition 7 (variational distance)

variational distance as

$$VD(P_U(m), P_V(m)) = \frac{1}{2}|P_U(m) - P_V(m)|$$

and total variational distance

$$TVD(P_U, P_V) = \frac{1}{2}\sum_m |P_U(m) - P_V(m)|$$

✓ meaning:

Approximating quantum circuits via discrete gate set

Theorem 8 (quantum gate error bound)

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

* Proof:

Approximating quantum circuits via discrete gate set

Theorem 9 (quantum circuit error bound)

$$E\left(U_m U_{m-1} \dots U_1, V_m V_{m-1} \dots V_1\right) \leq \sum_{j=1}^{m} E\left(U_j, V_j\right)$$

* Proof:

Generate two type of rotational gate $R_{\hat{n}}(\hat{\theta}), R_{\hat{m}}(\hat{\theta})$

Approximation error in arbitrary rotation gate is bounded by ϵ

Theorem 10

We can implement V via $\{H, T, S\}$ that satisfy following bound

$$E(U, V) \leq \epsilon,$$

where ϵ is target error rate. $*$ *Proof: (hint) using kronecker theorem*

Approximating n-qubit unitary gate via $R_{\hat{n}}(\hat{\theta}), R_{\hat{m}}(\hat{\theta})$ $\Rightarrow$ H, S, T and CNOT gates are universal!

Circuit complexity: for # of single qubit gates

Theorem 11 (Solovay Kitaev theorem)

$$n_1 = O\left(\log^c\left(\frac{1}{\epsilon_1}\right)\right) = O\left(\log^c\left(\frac{m}{\epsilon}\right)\right)$$

전체에 대해서는

$$m \times O\left(\log^c\left(\frac{m}{\epsilon}\right)\right) = O(m \log^c m)$$

Theorem 12

For implement arbitrary n-qubit unitary gate U needs $\Omega(2^n)$ number of gates.

$*$ Proof: U가 만들어낼 수 있는 $|\psi\rangle$의 경우의 수를 이용한다.

method 1

Circuit complexity: for # of qubits

method 2

Summary

Some remarks

-

Measurement

Computational basis: $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$

Principle of deferred measurement

Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit; if the measurement results are used at any stage of the circuit then the classically controlled operations can be replaced by conditional quantum operations.

✓ meaning:

Principle of implicit measurement

Without loss of generality, any unterminated quantum wires (qubits which are not measured) at the end of a quantum circuit may be assumed to be measured.

✓ meaning:

References

- M. A. Nielson and I. L. Chuang, Quantum Computation and Quantum Information
- Lecture notes for QU511: Quantum Computing (Fall 2024)