### 4. Basics of Quantum Computer

Vaughan Sohn

October 7, 2024

#### **Contents**

Quantum Circuit model

Quantum Gates

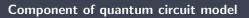
Universial Quantum gate set: {CNOT, single qubit gates}

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

Measurement

1





### Qubit

## Quantum Gates



#### Single-qubit gate decomposition

#### Theorem 1 (ZY decomposition)

Suppose U is a unitary operation on a single qubit. Then there exist real numbers  $\alpha, \beta, \gamma$  and  $\delta$  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

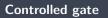
$$U = e^{i\alpha} AXBXC$$

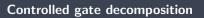
where  $\alpha$  is some overall phase factor and X is a Pauli-X operator.

5

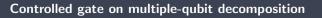
## Single-qubit gate decomposition

\* Proof:









## Summary

## 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  $3 \times 3$  example,

## Two-level unitary gate is controlled-U gate

\* Proof: (contd.)

Decomposition from n-qubit controlled-U gate to {CNOT gates, single-qubit} ⇒ 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,  $\begin{array}{l} \textbf{single-qubit} \\ \Rightarrow \textbf{Single qubit and CNOT gates are universal!} \end{array}$ 

\* Proof: (contd.)

Decomposition from n-qubit controlled-U gate to {CNOT gates, single-qubit} ⇒ 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

## Summary

Some remarks

Universial Quantum Discrete gate set: {CNOT, H,

S, T

#### **Definition 6 (approximation error)**

We define the  ${\bf error}$  when  ${\cal V}$  is implemented instead of  ${\cal U}$  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:

#### **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:

## Theorem 8 (quantum gate error bound)

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

\* <u>Proof</u>:

#### Theorem 9 (quantum circuit error bound)

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

\* <u>Proof</u>:

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  $\epsilon$ 

#### Theorem 10

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

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

where  $\epsilon$  is target error rate. \* <u>Proof</u>: (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

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

#### Circuit complexity: for # of qubits

#### Theorem 12

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

\*  $\underline{\text{Proof}}$ : U가 만들어낼 수 있는  $|\psi\rangle$ 의 경우의 수를 이용한다.  $\underline{\text{method } 1}$ 

28

Circuit complexity: for # of qubits

method 2

## Summary

## Summary

Some remarks

•

# Measurement

## Principle of deferred measurement

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

#### 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

#### 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)