

# Circuit Complexity

## 1. quantum circuit complexity

定义：任意 gate 可以被用一个 universal set 中 gate 组成 (如 H, T, CNOTs).

使用该 set + 门的数量即为 ~.

## 2. Query Complexity

### 2.1 背景

我们考虑“查询(query)”。它可以是向数据库查询，也可以是验证正确性等。

当 Query 的复杂度很大时，我们可以着重研究 Query 的次数，也即 query complexity.

Query 可以看作一个函数  $f(x)$ ，其中  $x$  为我们的“问题”，我们接下来考虑如何基于这个查询模型(Oracle Model) 量子化。

### 2.2. definition

我们考虑一个量子查询系统：

$$f: \{0, 1, \dots, M-1\} \rightarrow \{0, 1, \dots, N-1\}$$

但我们发现一个问题：在 Quantum Circuit 中，所有操作都应该是 可逆的，

但  $f(x)$  可能做不到这样。

故我们考虑使用一个 辅助系统(Ancilla Register)  $|q\rangle$ 。我们将造一个

酉算符  $O_f$ ，有：  $\xrightarrow{\text{主系统}}$

$$\xrightarrow{\text{ } \equiv q + f(x) \pmod{N}}$$

$$O_f: |x\rangle|q\rangle \rightarrow |x\rangle|q \oplus f(x)\rangle$$

而  $O_f$  的意义为：保持输入态  $|x\rangle$  不变，将 query 的结果存至  $|q\rangle$  上。

因此 query 对于  $|x\rangle$  “可逆”（无影响）

## 2.3 phase kick-back

我们把 ancilla qubit 设为  $|-\rangle$

$$|x\rangle |-\rangle \xrightarrow{O_f} \begin{cases} \text{若 } f(x) = 0 & |x\rangle |-\rangle \\ \text{若 } f(x) = 1 & |x\rangle (-|-\rangle) \end{cases}$$

$$\begin{aligned} \text{即 } O_f &= \sum_x (-1)^{f(x)} |x\rangle \langle x| \\ &= \sum_x |x\rangle \langle x| \otimes X^{f(x)} \end{aligned} \quad \rightarrow O_f |x\rangle |q\rangle = |x\rangle (X^{f(x)} |q\rangle)$$

## 2.4. Quantum - Classical fairness.

若函数  $f: x \rightarrow f(x)$  可被经典电路实现，则可以 Quantum Circuit 以相似的复杂度实现。

## 3. Deutsch Game

我们假设  $f: \{0, \dots, 2^n-1\} \rightarrow \{0, 1\}$  是下列两种函数之一：

① balanced:  $f$  有一半的结果为 0，一半为 1

② constant: 所有  $f$  的输出均为 0 或 1

对于经典电路，我们只能进行  $\mathcal{O}(2^{n-1})$  次 query  $f$ 。

不过对于量子电路，我们以极大的简化 complexity。

Step 1. 初始化  $n$  个 qubits  $|0\rangle = |0\rangle^{\otimes n} |1\rangle$

Step 2. 对所有 qubits 应加  $H$  [ ]

$$|\Psi_1\rangle = |+\rangle^{\otimes n} |-\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=1}^{2^n} |x\rangle |-\rangle$$

$$\rightarrow |+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} (|0\rangle + |1\rangle)^{\otimes n} \rightarrow = \text{项式展开}$$

Step 3. 对所有 qubits 逐位加  $O_f = \sum_x (-1)^{f(x)} |x\rangle \langle x|$

$$|\Psi_2\rangle = O_f |\Psi_1\rangle = \left( \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle \right) \cdot |-\rangle$$

Step 4. 对所有 qubits 逐位加  $H$  :

$$|\Psi_3\rangle = H^{\otimes n} |\Psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} \cdot H^{\otimes n} |x\rangle \cdot |-\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x,z} (-1)^{f(x) + x \cdot z} |z\rangle \cdot |-\rangle$$

$\downarrow$  binary product  
let  $x = \underline{x_1 \dots x_n}$ ,  $z = \underline{z_1 \dots z_n}$ ,  $x \cdot z = \sum x_i z_i$

$$\begin{aligned} H^{\otimes n} |x\rangle &= \sum_i H |x_i\rangle = \mp \frac{1}{\sqrt{2}} (-1)^{x_i z_i} |z_i\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_z (-1)^{x \cdot z} |z\rangle \end{aligned}$$

Step 5. 以计算基准则  $\begin{cases} 00\dots0 \rightarrow \text{constant} \\ \text{otherwise} \rightarrow \text{balanced} \end{cases}$

找  $i$  只关心  $|z\rangle = |0\dots0\rangle$  的系数.

(因为  $x \cdot \overline{00\dots0} = 0$ )

$$\alpha_0 = \frac{1}{2^n} \sum_z (-1)^{x \cdot z} \quad \begin{cases} \text{若 constant. } \alpha_0 = \pm 1 \\ \text{若 balanced. } \alpha_0 = 0 \end{cases}$$

至此成功地把  $O(2^n) \rightarrow O(1)$  (Query Complexity)

# 4. Complexity Class

## 4.1 definition. (粗略定义)

- Complexity Class 是有相同 复杂度范围 的问题的集合.

## 4.2 efficiency

我们称 complexity 不超过多项式级别的为 "efficiency".

### Complexity Class P

可以 efficiently 解决的问题集

### Complexity Class NP

可以 efficiently 验证的问题集

### NP-complete

NP 问题中，最难的问题被称为 NP-complete

所有 NP problem 都可 efficiently 被归约到 NP-complete

### NP-hard

不简单于 NP-complete 的问题是被称为 NP-hard

$$(NP\text{-complete} = NP \cap NP\text{-hard})$$

### BQP (Bounded-error Quantum Polynomial)

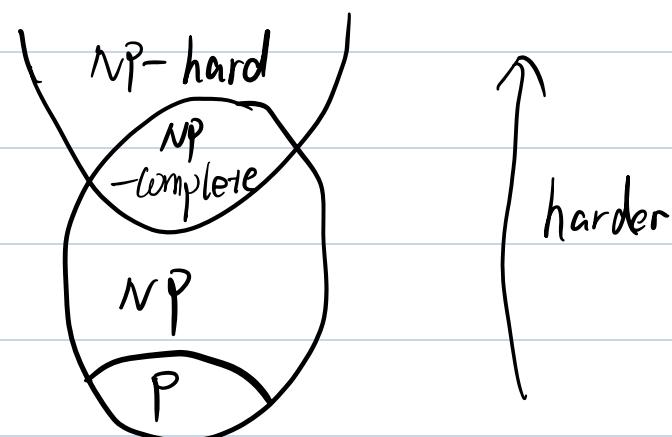
可以在有上界的 error 率下，被 Quantum Computer efficiently 解决。

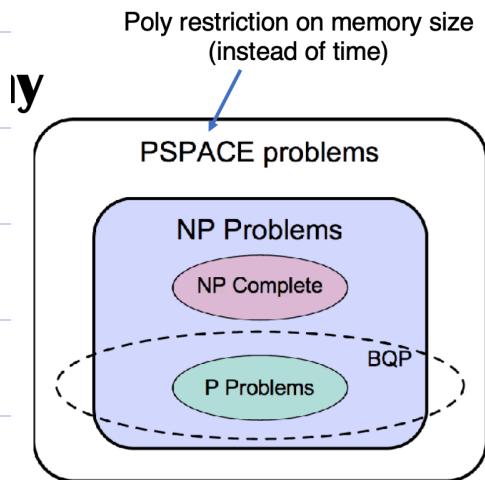
i.e. BQP  $\approx$  feasible via QC

$$BQP = P \text{ for QC}$$

### QMA (Quantum Merlin-Arthur)

$$QMA \approx NP \text{ for QC}$$





$P \subset BQP \subset PSPACE \subset EXP$

### 4.3. 算法

对于一些 **structured problem**, 可以指教级  $\rightarrow$  多项式  
(有特定数学结构 e.g. 整数分解  $\rightarrow$  shor's algorithm in lec 4 )  
 $e^{\frac{1}{3}} \rightarrow n^2 \log n \log \log n$

对于 **unstructured problem**, 可以实现平方加速  $n^2 \rightarrow n$   
(e.g. search)

## 5. 经典计算机上模拟 QC .

### 5.1. Schrodinger Picture

薛定谔绘景.

① State 随时间演化

② Quantum Gate 是固定的

我们考虑跟踪这个 system 中所有 qubit.

$$|0\rangle^{\otimes n} \rightarrow |0\rangle^{\otimes n} U_1^\dagger \cdots U_m^\dagger H U_m \cdots U_1 |0\rangle^{\otimes n}$$

对于  $n$ -qubit system, 每个 state 是一个  $2^n$  维向量, gate 是  $2^n \times 2^n$  matrix.

我们进行的矩阵运算显然呈指数级别的.

我们考虑跟踪“算符变化”

### 5.2 Heisenberg Picture

海森堡绘景

#### 5.2.1 Pauli Group

$n$ -qubit Pauli group " $P_n$ " 是形如:

$$c(A_1 \otimes A_2 \cdots A_n)$$

的算符集合, 其中:

①  $A_i \in \{I, X, Y, Z\}$  (单比特 Pauli matrix)

②  $c \in \{\pm 1, \pm i\}$  (全局相位)

Prop:  $(1)$  在乘法下封闭

(2)  $P_n$  只有  $4^n$  个元素.

(3) 均为酉矩阵且  $P^2 = \pm I$

(4)  $\forall U, V \in P_n, [U, V] = 0$  or  $\{U, V\} = 0$

## 5.2.2 Clifford Group

$$C_n = \{ C \mid \forall P \in \mathbb{P}_n \quad (C^\dagger P C \in \mathbb{P}_n) \}$$

现在我们回归主题：

### Stabilizer Formalism — Heisenberg Picture 在 QC 中的应用

我们注意到，初始 state： $|0\rangle^{\otimes n}$  是  $n$  个对易 (commuting) 算符  $\{Z_1, \dots, Z_n\}$

的联合 “+1 本征态”

$$\text{i.e. } Z_k |0\rangle^{\otimes n} = (+1) |0\rangle^{\otimes n}, \quad \forall k \in \{1, \dots, n\}$$

其中， $Z_k$  表示第  $k$  位为 2，其余为 1. (如  $Z_1 = I \otimes Z \otimes I \cdots I$ )

并且  $|0\rangle^{\otimes n}$  是唯一这样的态.

也即： $n$ -qubit 下，对于  $n$  个满足下列条件的 Pauli 算符：

① 两两对易

② 独立 (线性无关)

③ 取 +1 eigenvalue

那么它们的 +1 eigenstate 是一维的

也即 维一确定。

→ 我们追踪该算符集  $\Leftrightarrow$  追踪 state

注意到： $|\psi_1\rangle = U_1 |\psi_0\rangle$  是  $\{U_1^\dagger Z_1 U_1, \dots, U_n^\dagger Z_n U_n\}$

的联合 +1 本征态。

我们只需要维护这个算符集，即可得到 QC 的结果。

(只适用于有简单形式的运算，否则也可能退化为指数组级别)