

NP 与 NP 完全性

岳镒

2025 年 5 月 16 日

回忆：语言和判定问题

- ▶ 只需要回答“是”或者“否”的问题被称为判定问题
- ▶ 用 $\{0, 1\}^*$ 表示所有有限长度的二进制串组成的集合
- ▶ 子集 $L \subseteq \{0, 1\}^*$ 称为一个语言
- ▶ L 对应的判定问题：输入 $x \in \{0, 1\}^*$ ，问 $x \in L$?
- ▶ 判定问题 Π 对应的语言：回答为“是”的实例组成的集合

NP 类

- ▶ P: 多项式时间可判定的语言集合
- ▶ NP: 多项式时间可验证的语言集合

NP 类

- ▶ P: 多项式时间可判定的语言集合
- ▶ NP: 多项式时间可验证的语言集合

定义 (验证机, Verifier)

称算法 V 为语言 L 的验证机, 若满足

- (1) 若 $x \in L$, 则存在 w 使得 $V(x, w) = \text{acc}$
- (2) 若 $x \notin L$, 则任意 w 均有 $V(x, w) = \text{rej}$

NP 类

- ▶ P: 多项式时间可判定的语言集合
- ▶ NP: 多项式时间可验证的语言集合

定义 (验证机, Verifier)

称算法 V 为语言 L 的验证机, 若满足

- (1) 若 $x \in L$, 则存在 w 使得 $V(x, w) = \text{acc}$
- (2) 若 $x \notin L$, 则任意 w 均有 $V(x, w) = \text{rej}$

多项式时间可验证

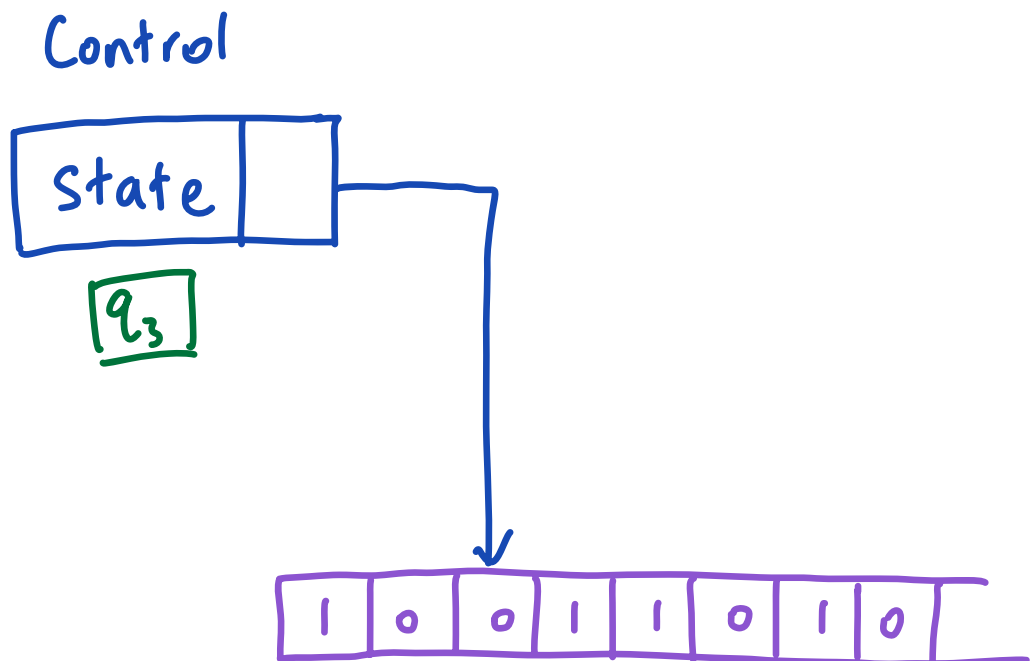
- ▶ “短” 证据:
 $|w| = \text{poly}(|x|)$
- ▶ 多项式运行时间

例子

- ▶ 3-SAT: x 是公式, w 是成真赋值
- ▶ 哈密顿回路: x 是图, w 是图中的哈密顿回路

等价定义：非确定型多项式时间可判定

回忆：图灵机模型



Read	State	Write	Move
$(q_0, 0)$	q_1	0	左
$(q_0, 1)$	q_2	1	左
$(q_3, 0)$	q_0	1	右
$(q_3, 1)$	q_0	1	左
$(q_{acc}, 0)$	q_{acc}	/	acc
$(q_{rej}, 1)$	q_{rej}	/	rej

等价定义：非确定型多项式时间可判定

回忆：图灵机模型

图灵机是一个 7 元组 $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{acc}}, q_{\text{rej}})$

- (1) Q 是状态集合
- (2) Σ 是输入字母表，即 $\Sigma = \{0, 1\}$
- (3) Γ 是纸带字母表，包含空白字符。 $\Sigma \subseteq \Gamma$
- (4) $\delta: Q \times \Gamma \rightarrow Q \times \Gamma \times \{L, R\}$ 称为转移函数
- (5) $q_0 \in Q$ 称为初始状态
- (6) $q_{\text{acc}} \in Q$ 称为接受状态
- (7) $q_{\text{rej}} \in Q$ 称为拒绝状态

等价定义：非确定型多项式时间可判定

回忆：图灵机模型

非确定型图灵机 (NTM) 是一个 7 元组

$$N = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{acc}}, q_{\text{rej}})$$

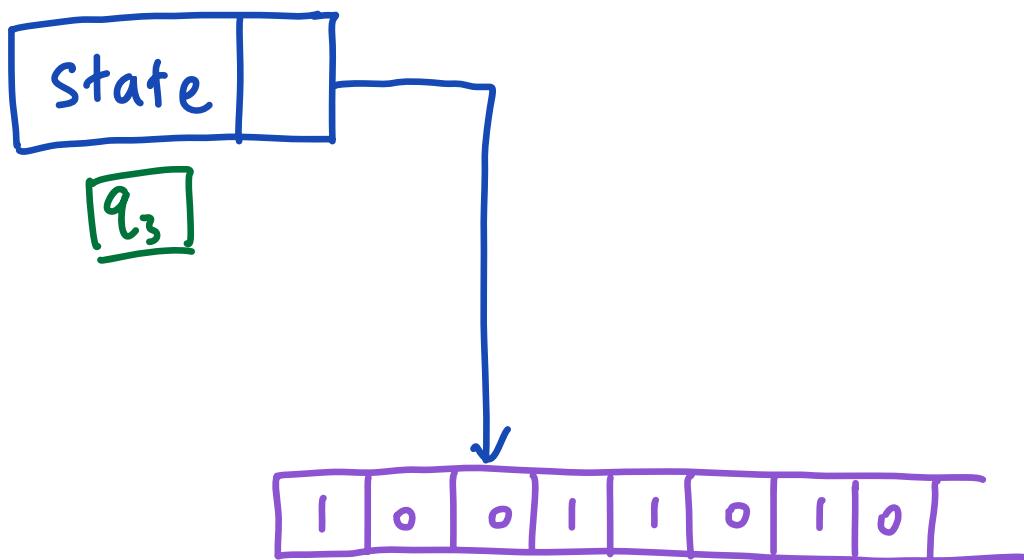
- (1) Q 是状态集合
- (2) Σ 是输入字母表, 即 $\Sigma = \{0, 1\}$
- (3) Γ 是纸带字母表, 包含空白字符。 $\Sigma \subseteq \Gamma$
- (4) $\delta: Q \times \Gamma \rightarrow \mathcal{P}(Q \times \Gamma \times \{L, R\})$ 称为转移函数
- (5) $q_0 \in Q$ 称为初始状态
- (6) $q_{\text{acc}} \in Q$ 称为接受状态
- (7) $q_{\text{rej}} \in Q$ 称为拒绝状态

称 N 接受 x 当且仅当 N 在输入 x 上存在一个接受计算分支

等价定义：非确定型多项式时间可判定

回忆：图灵机模型

Control



Read	State	Write	Move
$(q_0, 0)$	q_1	0	左
	q_2	0	右
$(q_0, 1)$	q_2	1	左
	q_3	0	左
	q_1	0	右
$(q_3, 0)$	q_0	1	右
	q_{acc}	0	右
$(q_3, 1)$	q_0	1	左
	q_{rej}	0	右
$(q_{acc}, 0)$	q_{acc}	/	acc
$(q_{rej}, 1)$	q_{rej}	/	rej

等价定义：非确定型多项式时间可判定

例子：哈密顿回路问题的一个非确定型判定算法（图灵机）

输入：图 $G = (V, E)$

1. 任选 $v_0 \in V, S \leftarrow \{v_0\}$
2. For $i = 1, 2, \dots, n - 1$ do
3. 任选 $v_i \in V$
4. 若 $v_i \in S$ ，立即拒绝
5. 若 $(v_{i-1}, v_i) \notin E$ ，立即拒绝
6. $S \leftarrow S \cup \{v_i\}$
7. 若 $(v_{n-1}, v_0) \in E$ ，接受；否则拒绝

等价定义：非确定型多项式时间可判定

定理 (NP 等价定义)

语言 L 多项式时间可验证 \iff 存在 L 的非确定型多项式时间判定算法（图灵机）

多项式时间变换 (Karp 归约)

定义 (多项式时间变换, Karp 归约)

称映射 $f: \{0, 1\}^* \rightarrow \{0, 1\}^*$ 是语言 A 到语言 B 的多项式时间变换 (Karp 归约), 若满足

- (1) f 多项式时间可计算
- (2) $\forall x, x \in A$ 当且仅当 $f(x) \in B$

此时称 A 多项式时间变换 (Karp 归约) 到 B ; 记作 $A \leq_p B$

多项式时间变换 (Karp 归约)

定义 (多项式时间变换, Karp 归约)

称映射 $f: \{0, 1\}^* \rightarrow \{0, 1\}^*$ 是语言 A 到语言 B 的多项式时间变换 (Karp 归约), 若满足

- (1) f 多项式时间可计算
- (2) $\forall x, x \in A$ 当且仅当 $f(x) \in B$

此时称 A 多项式时间变换 (Karp 归约) 到 B ; 记作 $A \leq_p B$

要点

- ▶ 直觉: \leq_p 是一种关于“难度”的偏序
- ▶ f 多项式时间可计算
- ▶ “当且仅当”: 需要验证两个方向
- ▶ 请对比课上讲的 Turing 归约 (Cook 归约)

多项式时间变换 (Karp 归约)

例：证明 $3\text{-SAT} \leq_p \text{CLIQUE}$

补充内容：Cook 归约

定义 (Cook 归约)

称问题 A 可 Cook 归约到问题 B ，若存在多项式时间的谕示图灵机 M ，使得对于计算 B 的任意算法 f ，均满足 M^f 计算 A 。其中 M^f 表示允许 M 以算法 f 的计算结果作为谕示。记作 $A \leq_T B$

补充内容: Cook 归约

定义 (Cook 归约)

称问题 A 可 Cook 归约到问题 B , 若存在多项式时间的谕示图灵机 M , 使得对于计算 B 的任意算法 f , 均满足 M^f 计算 A 。其中 M^f 表示允许 M 以算法 f 的计算结果作为谕示。记作 $A \leq_T B$

- ▶ 谕示图灵机 M^f : M 在运行过程中, 允许使用任意输入 x 向 $f(\cdot)$ 提问, 并在 $O(1)$ 时间得到回复 $f(x)$
- ▶ 在 M 的视角下: 类似于请求神谕 (oracle), 只关心结果 $f(x)$, 并不关心 $f(\cdot)$ 具体是怎么计算的

补充内容：Cook 归约

例：证明 3-SAT 搜索问题 \leq_T 3-SAT 判定问题

补充内容：其他复杂性类

定义 (coNP)

称语言 $L \in \text{coNP}$, 若 $\bar{L} \in \text{NP}$

例子

- ▶ $L = \{\phi: \phi(x_1, x_2, \dots, x_n) \text{ 不可满足}\}$
- ▶ $\text{FACTOR} = \{\langle x, y \rangle: x \text{ 存在不超过 } y \text{ 的非平凡因子}\}$

性质

- ▶ $P \subseteq \text{NP} \cap \text{coNP}$
- ▶ 注意: coNP 不是 NP 的补集!

补充内容：其他复杂性类

定义 (PCP)

给定函数 $r, q: \mathbb{N} \rightarrow \mathbb{N}$ 。称语言 $L \in \text{PCP}(r, q)$ ，若存在多项式时间随机算法 V ，满足以下条件：

- (1) 若 $x \in L$ ，则存在 w ，满足 $V(x, w) = \text{acc}$
- (2) 若 $x \notin L$ ，则任意 w ， $\Pr[V(x, w) = \text{acc}] \leq 1/2$
- (3) 对于输入 $\langle x, w \rangle$ ， V 至多使用 $r(|x|)$ 个随机比特，访问 w 的至多 $q(|x|)$ 个比特

补充内容：其他复杂性类

定义 (PCP)

给定函数 $r, q: \mathbb{N} \rightarrow \mathbb{N}$ 。称语言 $L \in \text{PCP}(r, q)$ ，若存在多项式时间随机算法 V ，满足以下条件：

- (1) 若 $x \in L$ ，则存在 w ，满足 $V(x, w) = \text{acc}$
- (2) 若 $x \notin L$ ，则任意 w ， $\Pr[V(x, w) = \text{acc}] \leq 1/2$
- (3) 对于输入 $\langle x, w \rangle$ ， V 至多使用 $r(|x|)$ 个随机比特，访问 w 的至多 $q(|x|)$ 个比特

定理 (PCP 定理)

$$\text{NP} = \text{PCP}(O(\log n), O(1))$$

可能的应用场景：签到、批改作业、~~复习期末考试...~~