计算理论导论 第七次作业

周书予
2000013060@stu.pku.edu.cn

June 11, 2022

1

我们知道 **IP** = **PSPACE**. 在 **PSPACE** $\subseteq$ **IP** 的证明中, 我们构造了一种基于多项式求值的, 用于证明 $\mathsf{TQBF} \in$ **IP** 的验证协议, 这种协议对于正确的实例 $\Psi \in \mathsf{TQBF}$ 一定会接受, 即具有 perfect completeness. 也就是说, 我们证明的实际上是 **PSPACE** $\subseteq$ **IP'**.

注意到又有 **IP'** $\subseteq$ **IP** $\subseteq$ **PSPACE**, 因此 **IP** = **IP'**.

2

任取 $L \in$ **MIP**, 存在多项式时间图灵机 (verifier) V_1, V_2 使得

$$x \in L \Rightarrow \exists P_1, P_2, \mathbb{P}_r[\mathsf{out}(V_1, V_2, P_1, P_2, x, r) = 1] \geqslant \frac{2}{3}$$
$$x \notin L \Rightarrow \forall P_1, P_2, \mathbb{P}_r[\mathsf{out}(V_1, V_2, P_1, P_2, x, r) = 1] \leqslant \frac{1}{3}$$

其中 $\mathsf{out}(V_1, V_2, P_1, P_2, x, r)$ 表示 verifier V_1, V_2 与 multiprover P_1, P_2 基于输入 x 与随机串 r 进行交互验证的输出结果.

考虑构造 NDTM M, 其先利用 nondeterminism 搜索出两个 prover 图灵机 P_1, P_2, 再依次枚举随机串 r 的所有可能, 然后确定性地计算 $\mathsf{out}(V_1, V_2, P_1, P_2, x, r)$, 并统计其中等于 1 的占比, 如果这个占比超过 $\frac{2}{3}$ 就接受. 换言之, M 接受 x 当且仅当存在 P_1, P_2 使得 $\mathbb{P}_r[\mathsf{out}(V_1, V_2, P_1, P_2, x, r) = 1] \geqslant \frac{2}{3}$, 故 $L = L(M)$.

由于 P_1, P_2 本身都是 $\{0,1\}^{p(|x|)} \to \{0,1\}^{q(|x|)}$ 的函数, p, q 是多项式, 因此 P_1, P_2 可以用 $q(|x|) \cdot 2^{p(|x|)}$ 位二进制串来表示, 即关于输入规模指数级. r 的规模也是多项式, 因此枚举 r 所花费的时间也是指数级的.

因此 M 的运行时间是关于输入规模指数级, 故 $L = L(M) \in$ **NEXP**.

3

- **AM**[2] $\subseteq$ **BP** $\cdot$ **NP**.

  任取 $L \in$ **AM**[2], 存在多项式时间 verifier V, 其在交互证明过程中先向 prover 发送随机串 r, 得到对方反馈 $a = P(x, r)$ 后, 输出交互证明结果 $V(x, r, a)$, 满足

  $$x \in L \Rightarrow \exists P, \mathbb{P}_r[V(x, r, P(x, r)) = 1] \geqslant \frac{2}{3}$$
  $$x \notin L \Rightarrow \forall P, \mathbb{P}_r[V(x, r, P(x, r)) = 1] \leqslant \frac{1}{3}$$

  考虑语言 $L' = \{(x, r) | \exists a, V(x, r, a) = 1\} \in$ **NP**, 从而有多项式时间规约 f 满足 $(x, r) \in L' \Leftrightarrow \phi_{x,r} = f(x, r) \in \mathsf{3SAT}$. 注意到 $V(x, r, P(x, r)) = 1 \Rightarrow \phi_{x,r} \in \mathsf{3SAT}$, 从而可以进一步得到

  $$\exists P, \mathbb{P}_r[V(x, r, P(x, r)) = 1] \geqslant \frac{2}{3} \Rightarrow \mathbb{P}_r[\phi_{x,r} \in \mathsf{3SAT}] \geqslant \frac{2}{3}$$
  $$\forall P, \mathbb{P}_r[V(x, r, P(x, r)) = 1] \leqslant \frac{1}{3} \Rightarrow \mathbb{P}_r[\phi_{x,r} \in \mathsf{3SAT}] \leqslant \frac{1}{3}$$

即 $L \leqslant_r \mathsf{3SAT}$, 说明 $L \in \mathbf{BP} \cdot \mathbf{NP}$.

- $\mathbf{BP} \cdot \mathbf{NP} \subseteq \mathbf{AM}[2]$.

  任取 $L \in \mathbf{BP} \cdot \mathbf{NP}$, 存在多项式时间可计算函数 f, 记 $\phi_{x,r} = f(x,r)$, 则有

  $$x \in L \Rightarrow \mathbb{P}_r[\phi_{x,r} \in \mathsf{3SAT}] \geqslant \frac{2}{3}$$
  $$x \notin L \Rightarrow \mathbb{P}_r[\phi_{x,r} \in \mathsf{3SAT}] \leqslant \frac{1}{3}$$

  可以设计如下的交互式证明协议: verifier 发送随机串 r, prover 根据 f 计算出 $\phi_{x,r}$ 并返回其一组可满足赋值 u, verifier 检验 u 的满足性并输出结果.

  不难验证这个协议可以用于识别语言 L. 因此 $L \in \mathbf{AM}[2]$.