TCS HW6

1

先证明一个引理: $\mathbf{NL} \subseteq \mathrm{AC}^1$.

对于任意 $A \in \mathbf{NL}$, 存在对数空间 NTM M 判定 A, M 有至多 $poly(n)$ 种格局, 至多运行 $poly(n)$ 步. 不妨设 M 有唯一的初始格局 b, 接受格局 a 和拒绝格局 r.

下面我们构造与 M 等价的电路族. 后面都默认电路中使用多元与或门.

首先, 设电路族 $\{A_n\}$ 以任意 n 比特串为输入, 输出 M 在 n 比特输入上的所有可能格局. 由于 M 的格局只与输入长度有关, 与具体输入无关, 因此 A_n 的输出也与输入无关, 故显然可以用常数层完成. M 至多有 $poly(n)$ 种格局, 因此 A_n 的总节点数也是 $poly(n)$ 的.

然后, 设电路族 $\{B_n\}$ 以 n 比特的 w 及 M 在 w 上的两个格局为输入, 输出这两个格局是否一步可达. 用与证明 Cook-Levin 定理时完全相同的方法, 可以将格局的可达性判定写作一个 CNF, 故 B_n 也是常数层, $poly(n)$ 规模的电路.

将 $\{A_n\}$ 和 $\{B_n\}$ 组合使用, 可以得到电路族 $\{C_n\}$, 它以 n 比特的 w 为输入, 输出 M 在 w 上格局图对应的邻接矩阵 P. 这只需要先计算 $A_n(w)$, 对于输出的每个格局对 $\langle i, j\rangle$, 再计算 $P_{ij} = B_n(w, i, j)$. P 的每个元素都可以被并行计算, 因此 C_n 仍是常数层, $poly(n)$ 规模的电路.

特别地, 我们规定 M 进入接受状态或拒绝状态后就停滞不动, 即 $P_{ai} = \delta_{ai}, P_{ri} = \delta_{ri}$, 这里 δ 是 Kronecker 记号.

注意到, $w \in A$ 等价于存在格局图上的从初始格局到接受格局的一条路径. 又归纳易证, P_{ij}^t 就是从格局 i 经历 t 步到达 j 的路径数. 设 M 在 n 位输入 w 上至多运行 $T = poly(n)$ 步, $w \in A$ 就等价于 $P_{ba}^T > 0$.

由于我们只关注 P_{ba}^T 是否为零, 即两个格局是否可达, 可以将所有矩阵视作布尔矩阵, 将计算矩阵乘法时的 $+\times$ 替换为 $\vee\wedge$. 这样一来, $(AB)_{ij} = \bigvee_k (a_{ik} \wedge b_{kj})$, 故矩阵乘法可用常数层, $poly(n)$ 规模的电路计算. 使用矩阵快速幂可以用 $O(\log T) = O(\log n)$ 次矩阵乘法算出 P^T, 因此计算 P^T 只需要对数层, $poly(n)$ 规模的电路. 将这个电路族记为 $\{D_n\}$, $D_n(P_{n\times n}) = P^T$.

至此, 我们得到了判定 A 的电路族 $\{E_n\}$, 即: 将 w 作为 C_n 的输入, 其输出再作为 D_n 的输入, 再以 D_n 输出的矩阵的 (b, a) 元作为总输出. 这个电路是对数深度, $poly(n)$ 规模的, 另外, 容易知道以上的每个电路族都是对数空间一致的, 这就证明了 $\mathbf{NL} \subseteq \mathrm{AC}^1$.

下面我们将用到这个引理的显然推论: $\mathbf{L} \subseteq \mathrm{NC}^2$.

($\Longleftarrow$)

$L \in \mathbf{P} = \mathbf{NC}$.

($\Longrightarrow$)

先证明 $\mathbf{NC} \subseteq \mathbf{P}$.

$\forall A \in \mathbf{NC}$, 存在多项式规模电路族 $\{C_n\}$ 判定 A, 且 C_n 可被图灵机 M 在多项式时间计算出.

令图灵机 M' = "对于输入 w, 先计算出 $C_{|w|} = M(1^{|w|})$, 再模拟 $C_{|w|}$ 运行, 输出其结果".

显然一个电路可被图灵机在其规模的多项式时间内模拟, 故 M' 在多项式时间判定 A, 即说明 $\mathbf{NC} \subseteq \mathbf{P}$.

再证明 $\mathbf{P} \subseteq \mathbf{NC}$.

$\forall A \in \mathbf{P}$, 存在对数空间可计算的函数 f, $w \in A \iff f(w) \in L$.

由引理, f 可被多项式规模, $O(\log^2 n)$ 深度的电路族 $\{C_n\}$ 计算.

设 L 被多项式规模, $O(\log^d n)$ 深度的电路族 $\{C'_n\}$ 判定.

将 $\{C_n\}$ 的输出作为 $\{C'_n\}$ 的输入, 就得到了在多项式规模, $O(\log^{d+2} n)$ 深度判定 A 的电路族, 即说明 $\mathbf{P} \subseteq \mathbf{NC}$.

2

设语言 $L = \{w | \bigoplus_i w_i = 1\}$. 我们知道 $L \notin \mathrm{AC}^0$, 因此只需证明 $maj \in \mathrm{AC}^0 \implies L \in \mathrm{AC}^0$.

对于 n 比特串 w, 记在 w 后补 k 个 0 和 $n-k$ 个 1 得到的串为 w_k.

注意到 $maj(w_k) = 1$ 当且仅当 w 有至少 k 个 1. 因此, 我们可以用常数层电路并行地计算 $maj(w_0), \cdots, maj(w_n)$. 设 w 中有 r 个 1, 结果将是

$$\begin{aligned} maj(w_0) = \cdots = maj(w_r) = 1, \\ maj(w_{r+1}) = \cdots = maj(w_n) = 0. \end{aligned}$$

这样一来, 记 $\mathbb{O}$ 为奇数集, 有

$$\begin{aligned} w \in L &\iff r \in \mathbb{O} \\ &\iff \bigwedge_{2k+1 \le n} (maj(w_{2k}) \oplus maj(w_{2k+1})) = 0, \end{aligned}$$

而最后一式显然可被 AC^0 计算, 故 $L \in \mathrm{AC}^0$. 由逆否命题, 这就说明 $maj \notin \mathrm{AC}^0$.

3

构造概率图灵机 M = "对于输入 1^n, 创建初始区间 $[1, 2^n]$. 掷随机比特, 若为 0, 将区间缩小为 $[1, 2^{n-1}]$, 否则缩小为 $[2^{n-1}+1, 2^n]$. 像这样做 n 轮后, 区间只剩下一个数, 将这个数作为输出". 易知 M 在 $O(n^2)$ 时间内运行.

再构造概率图灵机 M' = "对于输入 1^N, 计算 k 使得 $2^{k-1} < N \le 2^k$. 运行 $M(k)$, 若输出不超过 N, 将其作为最终输出, 否则再次运行 $M(k)$. 如果 $\log_2 \frac{1}{\delta}$ 轮后仍失败 (即 $M(k)$ 超过 N), 输出 ?". 易知 M' 在 $O(\log^2 n \log \frac{1}{\delta})$ 时间内运行.

显然, 在不输出 ? 的前提下, M' 会等概率地输出 $1, 2, \cdots, N$ 其中一个.

M' 输出 ? 的概率就是连续失败 $\log_2 \frac{1}{\delta}$ 轮的概率, 即

$$(\frac{2^k - N}{2^k})^{\log_2 \frac{1}{\delta}} \le (\frac{1}{2})^{\log_2 \frac{1}{\delta}} = \delta.$$

至此, 我们证明了题目所需的两个性质.

4

我们知道 $\mathbf{P} \subseteq \mathbf{P}_{/\mathbf{poly}}$, 使用相同的方法可以证明 $\mathbf{NP} \subseteq \mathbf{NP}_{/\mathbf{poly}}$. 故 3SAT 可被非确定性电路族 $\{C_n(\cdot, \cdot)\}$ 判定, 即 $x \in 3\mathrm{SAT} \iff \exists y, C_n(x, y) = 1$.

$\forall L \in \mathbf{BP} \cdot \mathbf{NP}$, $L \le_r 3\mathrm{SAT}$, 故存在从 L 到 3SAT 的随机归约 f. 由于 $\mathbf{BPP} \subseteq \mathbf{P}_{/\mathbf{poly}}$, 存在多项式规模的 $\{C'_n(\cdot)\}$, $L(w) = 3\mathrm{SAT}(C'_{|w|}(w))$, $\forall w$.

因此, $w \in L \iff \exists y, C_m(C'_n(w), y) = 1$, 其中 $m = |C'_n(w)|$.

综上, $L \in \mathbf{NP}_{/\mathbf{poly}}$ 即 $\mathbf{BP} \cdot \mathbf{NP} \subseteq \mathbf{NP}_{/\mathbf{poly}}$.

5

$\forall A \in \mathbf{BPL}$, 存在概率图灵机 M 在对数空间判定 A. 设 M 至多运行 $T(n)$ 步, 至多有 $C(n)$ 种可能格局, 显然 T, C 都是多项式规模. 将这些格局按字典序编码为 $1, 2, \cdots, C(n)$.

容易改造 M, 使其有唯一的初始格局 b, 接受格局 a 和拒绝格局 r.

考虑 $C(n)$ 维矩阵 P, P_{ij} 是 M 从格局 i 一步转移到格局 j 的概率, 具体来说:

- 若 M 从格局 i 必定下一步转移到格局 j, $P_{ij} = 1$;
- 若 M 从格局 i 通过掷随机比特有可能下一步转移到格局 j, $P_{ij} = \frac{1}{2}$;
- 否则, $P_{ij} = 0$.

特别地, 我们规定 M 进入接受状态或拒绝状态后就停滞不动, 即 $P_{ai} = \delta_{ai}, P_{ri} = \delta_{ri}$, 这里 δ 是 Kronecker 记号.

易归纳证明, P_{ij}^t 就是 M 从格局 i 开始, 经历 t 步恰好到达格局 j 的概率. 于是, $p = P_{ba}^T$ 就是 M 接受 w 的概率.

因此, 只需按照上述步骤构造 P, 计算矩阵乘法, 求和得到 p, 如果 $p \geq \frac{2}{3}$ 就接受, 否则拒绝. 这样就得到了多项式时间判定 A 的算法, 故 $A \in \mathbf{P}$, 即 $\mathbf{BPL} \subseteq \mathbf{P}$.