# 计算理论导论 第六次作业

周书予

2000013060@stu.pku.edu.cn

May 25, 2022

## 1

$L \notin \text{uni-}\mathbf{NC} \Rightarrow \mathbf{P} \neq \text{uni-}\mathbf{NC}$ 是显然的, 因为此时 $L \in \mathbf{P} \setminus \text{uni-}\mathbf{NC}$.

当 $L \in \text{uni-}\mathbf{NC}$ 时, 考虑识别 $L$ 的, 规模为 $O(n^c)$ 深度为 $O(\log^d n)$ 的 logspace-uniform 线路 $\{C_n\}$. 任取 $L' \in \mathbf{P}$, 我们希望构造满足同样条件的线路 $\{D_n\}$ 识别语言 $L'$.

$L \in \mathbf{P}$-complete 说明存在 implicitly logspace reduction $f$ 满足 $x \in L' \Leftrightarrow f(x) \in L$. 根据定义存在图灵机 $M_{f,i}$ 可以在 $O(\log |x|)$ 空间内计算 $f(x)_i$, 考虑构造其 configuration graph $G_{M_{f,i},x}$, 容易发现 $M_{f,i}(x) = 1 \Leftrightarrow \langle G_{M_{f,i},x}, C_{\text{start}}, C_{\text{accept}} \rangle \in \mathsf{PATH}$. 如果证明了 $\mathsf{PATH} \in \text{uni-}\mathbf{NC}$, 那么只需要如下地构造线路 $\{D_n\}$: 对于输入 $x$, 首先计算出 $|f(x)|$, 然后**并行地**根据 $M_{f,i}$ 计算出 $f(x)$ 的每一位, 得到 $f(x)$, 再接上线路 $C_{|f(x)|}$, 得到

$$D_{|x|}(x) = C_{|f(x)|}(f(x)) = [f(x) \in L] = [x \in L']$$

由于 $\{D_n\}$ 的两部分 (实现 $\mathsf{PATH}$, 以及接上 $C_{|f(x)|}$) 都是 uni-$\mathbf{NC}$ 的, 故其自身也是 uni-$\mathbf{NC}$ 的.

**引理 1.** $\mathsf{PATH} \in \text{uni-}\mathbf{NC}$.

*证明.* 考虑图 $G$ 的邻接矩阵 $A$. 记 $B_{i,j}^k$ 表示图 $G$ 中是否存在长度不超过 $2^k$ 的从 $i$ 到 $j$ 的路径, 有初值 $B^0 = A$, 以及递推关系

$$B_{i,j}^k = \bigvee_l B_{i,l}^{k-1} \wedge B_{l,j}^{k-1}$$

因此若 $B^{k-1}$ 能被多项式规模, 深度为 $d$ 的线路计算, 则 $B^k$ 也能被多项式规模, 深度为 $d+2$ 的线路计算.

取 $K = \lceil \log n \rceil$ 其中 $n$ 是图 $G$ 的点数, 则 $\langle G, s, t \rangle \in \mathsf{PATH}$ 当且仅当 $B_{s,t}^K = 1$. 计算 $B^K$ 的线路是 poly-size, log-depth 以及 uniform 的, 故 $\mathsf{PATH} \in \text{uni-}\mathbf{NC}$. $\square$

## 2

如果 $\mathsf{MAJ} \in \mathbf{AC}^0$, 考虑构造计算 $\mathsf{PARITY}$ 的 poly-size const-depth 线路.

假设任意 $\mathsf{MAJ}_n$ 都可以在 $O(n^c)$ 规模, $d$ 深度内计算, 考虑记 $A_i = \{x | x \text{ has at least } i \text{ 1s }\}$, 根据输入规模 $n$ 适当补充输入的 0 或 1 的数量便可以由 $\mathsf{MAJ}$ 的线路构造出 $A_i$ 的线路.

注意到

$$\mathsf{PARITY}_n = (A_0 \wedge \overline{A_1}) \vee (A_2 \wedge \overline{A_3}) \vee \cdots \vee (A_{2k} \wedge \overline{A_{2k+1}})$$

其中 $2k+1 \geqslant n$. 故一旦构造出了 $A_i$ 的 poly-size const-depth 线路, 便也可以构造出 $\mathsf{PARITY}$ 的 poly-size const-depth 线路, 即 $\mathsf{PARITY} \in \mathbf{AC}^0$.

由 Switching Lemma 知 $\mathsf{PARITY} \notin \mathbf{AC}^0$, 产生矛盾. 故 $\mathsf{MAJ} \notin \mathbf{AC}^0$.

## 3

1. 取 $k=\lceil \log_2 N\rceil$, 随机算法 $\mathcal{A}$ 消耗 $k$ 个随机比特, 即以 $k$ 位 01 串作为输入, 且满足

$$\mathcal{A}(r)=\begin{cases}\langle r\rangle+1, & \langle r\rangle<N\\ ?, & \langle r\rangle\geqslant N\end{cases}$$

其中 $\langle r\rangle$ 表示将 $r$ 看成一个 $k$ 位二进制数得到的非负整数.

对于任意 $k=1,2,\cdots,N$, 有

$$\mathbb{P}(\mathcal{A}(r)=k|\mathcal{A}(r)\neq ?)=\frac{\mathbb{P}(\mathcal{A}(r)=k)}{\mathbb{P}(\mathcal{A}(r)\neq ?)}=\frac{2^{-k}}{N\cdot 2^{-k}}=\frac{1}{N}$$

故 $\mathcal{A}$ 的输出是 $[N]$ 的均匀分布. 显然 $\mathcal{A}$ 的运行时间是 $O(\log N)$.

2. 仍然取 $k=\lceil \log_2 N\rceil$, 随机算法 $\mathcal{B}$ 消耗 $k\cdot\lceil\log_2(1/\delta)\rceil$ 个随机比特, 满足

$$\mathcal{B}(r_1,\cdots,r_k)=\begin{cases}\langle r_i\rangle+1, & \langle r_1\rangle,\cdots,\langle r_{i-1}\rangle\geqslant N, \langle r_i\rangle<N\\ ?, & \langle r_1\rangle,\cdots,\langle r_{\lceil\log_2(1/\delta)\rceil}\rangle\geqslant N\end{cases}$$

容易验证 $\mathcal{B}$ 的输出也是 $[N]$ 的均匀分布, 且 $\mathcal{B}$ 的运行时间是 $O(\log N\log(1/\delta))$. 分析 $\mathcal{B}$ 输出 ? 的概率:

$$\mathbb{P}(\mathcal{B}(r_1,\cdots,r_k)=?)=\left(\frac{2^k-N}{2^k}\right)^{\lceil\log_2(1/\delta)\rceil}\leqslant\left(\frac{1}{2}\right)^{\lceil\log_2(1/\delta)\rceil}\leqslant\left(\frac{1}{2}\right)^{\log_2(1/\delta)}=\delta$$

## 4

只需要证明 $L\leqslant_r \textsf{3SAT}\Rightarrow$ 存在 poly-size nondeterministic circuit $\{C_n\}$ 可以识别 $L$.

$L\leqslant_r \textsf{3SAT}$ 说明存在多项式时间图灵机 $M$ 满足 $\mathbb{P}_{r\in\{0,1\}^{m(n)}}[L(x)=\textsf{3SAT}(M(x,r))]\geqslant 2/3$, 其中 $n=|x|, m(n)=\text{poly}(n)$ 是 $M$ 消耗的随机比特数量. 根据 error reduction 的结论, 我们知道也存在多项式时间图灵机 $M'$ 满足 $\mathbb{P}_{r\in\{0,1\}^{m'(n)}}[L(x)\neq\textsf{3SAT}(M'(x,r))]\leqslant 2^{-n-1}$, 其中 $m'(n)=\text{poly}(n)$.

根据 Union Bound,

$$\begin{aligned}&\mathbb{P}_{r\in\{0,1\}^{m'(n)}}\left(\exists x\in\{0,1\}^n, L(x)\neq\textsf{3SAT}(M'(x,r))\right)\\ \leqslant&\sum_{x\in\{0,1\}^n}\mathbb{P}_{r\in\{0,1\}^{m'(n)}}[L(x)\neq\textsf{3SAT}(M'(x,r))]\\ \leqslant& 2^n\cdot 2^{-n-1}=1/2<1\end{aligned}$$

故存在 $r_n\in\{0,1\}^{m'(n)}$ 使得 $L(x)=\textsf{3SAT}(M'(x,r_n))$ 对任意 $x\in\{0,1\}^n$ 成立.

于是 $x\in L\Leftrightarrow\exists r_n, M'(x,r_n)\in\textsf{3SAT}\Leftrightarrow\exists r_n,\exists$ assignment $u, M'(x,r_n)(u)=$ True. 构造线路 $C_n$ 接受输入 $x,r_n,u$, 根据 $M'$ 计算出 3CNF $M'(x,r_n)$, 再检验赋值 $u$ 是否是可满足赋值. $C_n$ 显然是多项式规模的, 因此 $L\in\mathbf{NP}_{/\mathbf{poly}}$.

## 5

任取 $L\in\mathbf{BPL}$, 存在 $O(\log n)$ 空间的 PTM $M$ 使得 $\mathbb{P}[M(x)=L(x)]\geqslant 2/3$. 对于输入 $x$, 考虑 configuration graph $G_{M,x}$, 其有 $m=\text{poly}(n)$ 个点, 每条转移边都有 0/0.5/1 的转移概率, 可以写成一个转移矩阵 $A\in\mathbb{R}^{m\times m}$.

利用矩阵乘法可以计算出 $t$ 步的转移概率 (即 $A^t_{i,j}$ 表示从点 $i$ 出发走 $t$ 步, 走到点 $j$ 的概率), 其中 $t=\text{poly}(n)$ 为 $M$ 的运行时间. 此时 $x\in L\Leftrightarrow A^t_{q_{\text{start}},q_{\text{accept}}}\geqslant 2/3$, 可以多项式时间地将 $A^t$ 算出, 故 $L\in\mathbf{P}$.