计算理论导论 第五次作业

周书予

2000013060@stu.pku.edu.cn

May 23, 2022

1

考虑

$$f(x_1,x_2,\cdots,x_n)=(x_1\wedge f(1,x_2,\cdots,x_n))\vee(\neg x_1\wedge f(0,x_2,\cdots,x_n))$$

其中 $f(1,x_2,\cdots,x_n)=f_1(x_2,\cdots,x_n), f(0,x_2,\cdots,x_n)=f_0(x_2,\cdots,x_n)$ 是另外两个输入 $n-1$ 比特的布尔函数, 可以递归构造. 归纳可知任意 n 比特布尔函数都可以在 $10\cdot 2^n-5$ 的线路规模内被构造出.

2

考虑 k 比特布尔函数只有 2^{2^k} 个, 可以使用前述方法将这些函数对应的线路全部预构造出来. 修改 **1** 中描述的递归构造方法, 在递归到 $n=k$ 时停止递归, 转而直接利用预构造得到的结果. 这种构造方法的电路规模为 $2^{2^k}\cdot 10\cdot 2^k+10\cdot 2^{n-k}$, 取 $k=\log n-1$, 电路规模为

$$10\left(2^{n-k}+2^{2^k+k}\right)=10\left(\frac{2^{n+1}}{n}+2^{n/2+\log n-1}\right)\leqslant 1000\cdot\frac{2^n}{n}$$

.

3

我们知道对于任意 l, 存在无法被规模为 $\frac{2^l}{10l}$ 的线路所计算的 l 比特布尔函数, 而任意 l 比特布尔函数都可以被规模为 $10l2^l$ 的线路所计算. 取 $l=k(\log n+\log\log n)$, 考虑语言

$$\begin{aligned}L_k=\{w\in\{0,1\}^n|&\exists f \text{ a } l\text{-bit boolean function}, C_f \text{ a circuit of size } \in\left[\frac{2^l}{10l},10l2^l\right],\\&\forall g \text{ a } l\text{-bit boolean function}, C_g \text{ a circuit of size } \in\left[\frac{2^l}{10l},10l2^l\right],\\&\forall C'_f \text{ a circuit of size } <|C_f|, C'_g \text{ a circuit of size } <|C_g|\\&\exists y\in\{0,1\}^l, z_f\in\{0,1\}^l, z_g\in\{0,1\}^l,\\&\forall x\in\{0,1\}^l,\\&f(x)=C_f(x)\wedge g(x)=C_g(x)\wedge C_f(z_f)\neq C'_f(z_f)\wedge C_g(z_g)\neq C'_g(z_g)\\&\wedge(x\succcurlyeq y\vee f(x)=g(x))\wedge f(y)<g(y)\wedge f(w[:l])=1\\&\}\end{aligned}$$

也即, L_k 中包含了所有 $f(w[:l])=1$ 的 $w\in\{0,1\}^n$, 其中布尔函数 f 需要满足: (a) 需要规模为至少 $\frac{2^l}{10l}=\frac{(n\log n)^k}{10k(\log n+\log\log n)}=\Omega(n^k)$ 的线路所计算, (b) 在满足前者条件下“字典序”最小的.

因此使用 $\exists C_f$ 来构造 f 的线路, 使用 $\forall C'_f$ 来保证 f 无法被比 C_f 规模更小的线路计算, 从而保证条件 a 成立, 设置 C_f 规模上界是为了满足条件保证 certificate 规模是关于 n 多项式.

为了满足条件 b, 使用相同的方式构造了任意满足条件 a 的布尔函数 g, f 的“字典序”小于 g 等价于存在某一个 $y \in \{0,1\}^l$, f, g 对于字典序小于 y 的输入 x(记作 $x \prec y$) 的输出结果都相同, 而对于 y 有 $f(y) < g(y)$.

不难验证每个 quantifier 下的 certificate 都是关于 n 的多项式量级, 因此 $L_k \in \mathbf{PH}$. 显然 L_k 的电路复杂性是 $\Omega(n^k)$, 于是结论得证.

4

类似 **3**, 我们可以构造如下语言

$$
\begin{aligned}
L = \{w \in \{0,1\}^n | &\exists f \text{ a } n\text{-bit boolean function}, C_f \text{ a circuit of size } \in \left[\frac{2^n}{10n}, 10n2^n\right], \\
&\forall g \text{ a } n\text{-bit boolean function}, C_g \text{ a circuit of size } \in \left[\frac{2^n}{10n}, 10n2^n\right], \\
&\forall C'_f \text{ a circuit of size } < |C_f|, C'_g \text{ a circuit of size } < |C_g| \\
&\exists y \in \{0,1\}^n, z_f \in \{0,1\}^n, z_g \in \{0,1\}^n, \\
&\forall x \in \{0,1\}^n, \\
&f(x) = C_f(x) \wedge g(x) = C_g(x) \wedge C_f(z_f) \neq C'_f(z_f) \wedge C_g(z_g) \neq C'_g(z_g) \\
&\wedge (x \succcurlyeq y \vee f(x) = g(x)) \wedge f(y) < g(y) \wedge f(w) = 1 \\
&\}
\end{aligned}
$$

也即, L 中包含了所有 $f(w) = 1$ 的 $w \in \{0,1\}^n$, 其中 f 满足: **(a)** 需要规模为至少 $\frac{2^n}{10n}$ 的线路所计算, **(b)** 在满足前者条件下“字典序”最小的.

注意到利用 padding 技术, 我们有 $\mathbf{P} = \mathbf{NP} \Rightarrow \mathbf{EXP} = \mathbf{NEXP}$, 如上 L 的每一个 quantifier 下的 certificate 都是关于 n 指数级, 考虑由内而外地利用 $\mathbf{EXP} = \mathbf{NEXP} = \mathbf{coNEXP}$ 的结论去掉 quantifier, 最终可以验证 $L \in \mathbf{EXP}$.

5

任取 $L \in$ uniform-$\mathbf{NC}^1$, L 可以由 logspace-uniform 的线路族 $\{C_n\}_{n\in\mathbb{N}}$ 计算. 考虑构造判定 L 的 DTM M, 其针对输入 w, 在 $C_{|w|}$ 上 (得益于 $C_{|w|}$ 的结构是 implicitly-logspace-computable 的) 进行 DFS 并计算 $C_{|w|}(w)$. 由于 C_w 的深度为 $O(\log |w|)$, 所以 DFS 的过程只需要 $O(\log |w|)$ 的额外空间保存搜索栈. 这说明 $L \in \mathbf{SPACE}(\log n) = \mathbf{L}$. 故 uniform-$\mathbf{NC}^1 \subseteq \mathbf{L}$.

根据 Space Hierarchy Theorem 知 $\mathbf{L} = \mathbf{SPACE}(\log n) \subsetneq \mathbf{SPACE}(n) \subseteq \mathbf{PSPACE}$, 故 uniform-$\mathbf{NC}^1 \neq \mathbf{PSPACE}$.