Homework 5

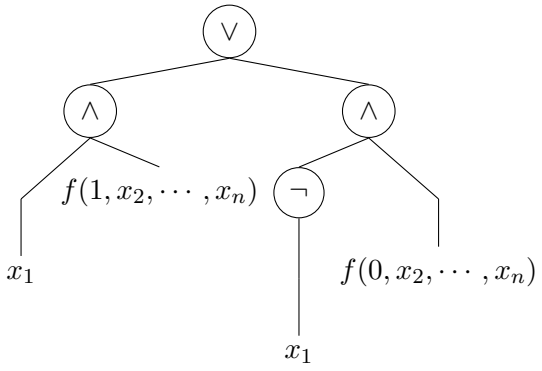
Name: 方嘉聪 ID: 2200017849

Problem 1(16 points). Prove that every function $f : \{0,1\}^n \to \{0,1\}$ can be computed by a circuit of size less than $10 \cdot 2^n$. ◀

Answer. 不妨设一个布尔函数为 $f(x_1, x_2, \cdots, x_n)$, 考虑如下的分解:

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

具体的, 分解(1)对应的电路如下:



迭代的重复上述分解. 设 $T(n)$ 为计算 $f(x_1, x_2, \cdots, x_n)$ 的电路大小, 则有 (注意到 $T(1) \leq 1$):

$$T(n) \leq 2T(n-1) + 4 \implies T(n) \leq 2^{n-1}(T(1)+4) - 4 < 10 \cdot 2^n$$

证毕. ◁

Problem 2(21 points). Improve this bound to show that every function $f : \{0,1\}^n \to \{0,1\}$ can be computed by a circuit of size less than $1000 \cdot 2^n/n$. ◀

Answer. 大致思路: 考虑第一题的分解(1), 运行 $n-k$ 步之后, 不再继续分解下去, 而是选择去计算所有的布尔函数在最后 k 位上的结果, 这样可以实现电路的复用, 从而得到一个电路大小更优的上界. 当 n 比较小时, 会有 $1000 \cdot 2^n/n < 10 \cdot 2^n$, 直接使用第一题的分解即可, 下面考虑 n 较大的情况:

具体的, 设函数 $g_k : \{0,1\}^k \to \{0,1\}^{2^{2^k}}$ 表示输入长度为 k 时所有可能的布尔函数的输出, 即:

$$g_k(x_1, x_2, \cdots, x_k) = (f_1(x_1, x_2, \cdots, x_k), f_2(x_1, x_2, \cdots, x_k), \cdots, f_{2^{2^k}}(x_1, x_2, \cdots, x_k))$$

其中 f_i 表示第 i 个布尔函数. 由第一题知计算 g_k 所需电路大小的上界为 $10 \cdot 2^k \cdot 2^{2^k}$.

那么对于 $f(x_1, x_2, \cdots, x_n)$, 我们先预处理得到 g_k 对应的电路, 而后运行第一题的分解方式 $n-k$ 轮, 余下的 k 轮直接计算 g_k 的输出. 于是总的电路大小上界 $\mathcal{C}(f)$ 为:

$$\begin{aligned}
\mathcal{C}(f) &\leq 10 \cdot 2^k \cdot 2^{2^k} + 4(2^0 + 2^1 + \cdots + 2^{n-k-1}) \\
&= 10 \cdot 2^k \cdot 2^{2^k} + 4(2^{n-k} - 1) \\
[\text{let } k = \log_2(n) - 1] &< 10 \cdot 2^{\log_2(n)-1+n/2} + 4 \cdot 2^{n+1-\log_2(n)} \\
&= \left(\frac{5n^2}{2^{n/2}} + 8\right)\frac{2^n}{n} < 1000 \cdot \frac{2^n}{n}
\end{aligned}$$

设 $t(n) = 5n^2/2^{n/2}$, 那么 $t'(n) = (4n - \ln 2 \cdot n^2)/2^{n/2+1}$, 故 $\max t(n) < t(4/\ln 2) < 1000$, 故上述最后一个不等号成立, 证毕.

注: 1000 看起来是一个比较松的常数, 这里 k 也可以取其他的值. 如果考虑渐进复杂度, 可以证明

$$\mathcal{C}(g_k) \leq 2^{2^k}(1 + o(1)) \implies \mathcal{C}(f) = (1 + o(1))\frac{2^n}{n}.$$

◁

Problem 3(21 points). Show that for every $k > 0$ that **PH** contains languages whose circuit complexity is $\Omega(n^k)$. ◀

Answer. 我们先来证明如下的引理:

Lemma 1. $\forall n, k \in \mathbf{N}^+$, 存在一个大小为 $2 \cdot n^{2k+2}$ 的电路 C_n, 使得 $\exists \mathcal{S} \subseteq \mathcal{X}$, $s.t.\ \forall w \in \mathcal{S}, C_n(w) = 1$ 且使得对任意的大小不超过 n^k 的电路 C'_n, $\exists w, C'_n(w) \neq C_n(w)$, 其中 $\mathcal{X} = \{X_1, \cdots, X_{2^n}\}, X_i \in \{0,1\}^n$.

证明. 使用 Counting Argument. 类似课上的证明, 大小不超过 n^k 的电路有 $3^{n^k}\left(n^k\right)^{cn^k} = O\left(2^{n^{2k}}\right)$ 个, 其中 c 是一个常数. 有注意到 $X = \{X_1, \cdots, X_{n^{2k+1}}\} \subseteq \mathcal{X}$ 不同的子集有 $2^{n^{2k+1}}$ 个, 故存在一个一个 $\mathcal{S} \subseteq X \subseteq \mathcal{X}$ 使得不被任意一个大小不超过 n^k 的电路接受. 而存在大小为 $2 \cdot n^{2k+2}$ 的电路 C_n 使得 $C_n(w) = 1, \forall w \in \mathcal{S}$($2n$ 个节点接受输入 + n^{2k+1} 组这样的节点取"或"), 证毕. □

下面我们考虑如下的语言 $L \in \mathbf{PH}$, 设 $n = |w|$:

$$\forall w \in L \iff \exists e(C^*) \in \{0,1\}^{p(|w|)}\ s.t. \tag{2}$$

$$\wedge \left(\forall e(C') \in \{0,1\}^{p(|w|)}, \exists x \in \{0,1\}^n,\ s.t.\ C^*(x) \neq C'(x)\right) \tag{3}$$

$$\wedge \left(\forall e(C) \in \{0,1\}^{p(|w|)} \wedge e(C) \leq e(C^*), \exists e(C_0)\ s.t.\ \forall y \in \{0,1\}^n, C_0(y) = C(y)\right) \tag{4}$$

$$C^*(w) = 1 \tag{5}$$

其中 $p(\cdot)$ 为多项式函数, 且

$$e(C^*) \text{ 是大小为 } 2 \cdot n^{2k+4} \text{ 的电路 } C^* \text{ 的编码}, e(C') \text{ 是大小至多为 } n^{k+1} \text{ 的电路 } C' \text{ 的编码}, \tag{6}$$

$$e(C) \text{ 是字典序不超过 } e(C^*) \text{ 的电路 } C \text{ 的编码}, e(C_0) \text{ 是大小至多为 } n^{k+1} \text{ 的电路 } C_0 \text{ 的编码}. \tag{7}$$

由引理保证了第 (2)(3) 行的良定义, 进而 L 是良定义的. 如上的 formula 事实上实在模拟一个大小为 $2n^{2k+4}$ 的电路, 同时这一电路与任意一个大小至多为 n^{k+1} 的电路不等价, 同时 (4) 中的限制保证了取到了字典序意义上的"最小"的符合 (3) 约束的 C^*. 注意到上述的电路编码和量词可以在多项式时间内计算, 且 L 可以被大小为 $2n^{2k+4}$ 的电路族计算, 而不能被 $O(n^{k+1})$ 的电路族计算. 故存在一个 **PH** 中的语言使得其电路复杂度为 $\Omega(n^k)$. 证毕.

注: 证明参考了 Kannan 对这一命题的原论文, 这里 C^* 的大小也许可以更小, 没有做更精细的分析. ◁

Problem 4(21 points). Show that **P** = **NP**, then there is a language in **EXP** that requires circuits of size $2^n/n$. ◀

Answer. 由于 $\mathbf{P} = \mathbf{NP}$, 那么有 $\mathbf{PH} = \mathbf{P}$, 故第 3 题中的语言 L 是多项式时间可判定的. 下面我们修改 L 得到一个新语言 L' 使得 $L' \in \mathbf{EXP}$ 且需要 $\Omega(2^n/n)$ 大小的电路.

令 L 的 (2)-(5) 的定义保持不变, 其中设 $n = |w|$, 令 $p(\cdot) = O(2^{\mathrm{poly}(n)})$, 考虑:

$$|e(C^*)|, |e(C)| \geq \frac{2^n}{cn}, \quad |e(C')|, |e(C_0)| \leq \frac{2^n}{cn}, \text{ 其中 } c > 1 \text{ 为一个常数.}$$

这里的存在性和良定义性由课上的一个结论保证, 即:

$$\exists \text{ a Boolean function on } n \text{ bits that requires circuits of size } \Omega\left(\frac{2^n}{n}\right)$$

注意到这样定义的 L' 的规模是 L 的指数倍, 而 $L \in \mathbf{P} \implies L' \in \mathbf{EXP}$, 且由上述构造可知 L' 需要电路大小为 $\Omega(2^n/n)$, 证毕. ◁

Problem 5(21 points). Show that uniform $\mathbf{NC}^1 \subseteq \mathbf{L}$. Then show that $\mathbf{PSPACE} \neq$ uniform $\mathbf{NC}^1$. ◀

Answer. (1)$\forall L \in \mathbf{NC}^1$, 由定义知, 存在常数 c 使得 L 被一个 log-space 的 uniform circuit family $\{C_n\}$ 计算, 且 $\{C_n\}$ 的大小和深度分别为 $O(n^c), O(\log n)$. 注意到在 $\{C_n\}$ 中每个门的 fan-in/fan-out 不超过 2, 那么可以将整个电路转化为二叉树的形式, 从叶子结点开始递归的进行计算 (依次计算左子结点, 右子结点和父节点). 注意到我们不需要存储下整个电路, 只需要记住当前的计算状态 (当前节点的输出以及输出将要作为哪一个门的输入), 重复利用存储空间, 又由于这个树的深度是 $O(\log n)$, 故整个计算过程只需使用 log-space, 故 $L \in \mathbf{L} \implies$ uniform $\mathbf{NC}^1 \subseteq \mathbf{L}$.

(2) 由空间分层定理 (Space Hierarchy Theorem) 知 $\mathbf{L} \subsetneq \mathbf{PSPACE}$, 故 $\mathbf{PSPACE} \neq$ uniform $\mathbf{NC}^1$. ◁