TCS HW5

1

我们归纳证明任意 n 元布尔函数可用不超过 $10 \cdot 2^n$ 规模的电路计算.

容易验证 $n \leq 5$ 时都成立.

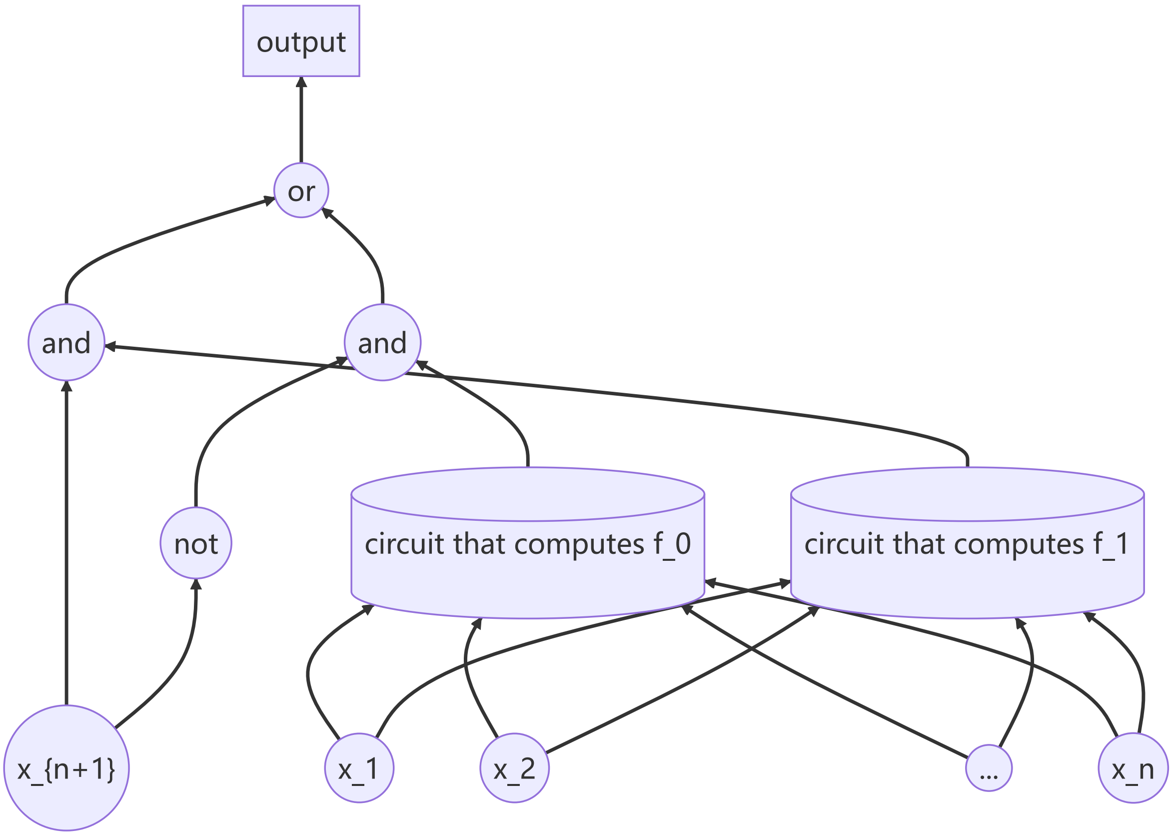
假设 n 时成立, 下证 $n+1$ 时成立, 即 $f(x_1, \cdots, x_n)$ 可用不超过 $10 \cdot 2^{n+1}$ 规模的电路计算.

记 $f_1 = f(x_1, \cdots, x_n, 1), f_0 == f(x_1, \cdots, x_n, 0)$.

注意到

$$f(x_1, \cdots, x_n, x_{n+1}) = (x_{n+1} \wedge f_1) \vee (\neg x_{n+1} \wedge f_0),$$

因此, 可如下构造计算 f 的电路:



如图, 该电路的规模不超过 $2(10 \cdot 2^n) + 5 - n \leq 10 \cdot 2^{n+1}$. 这里减去 n 是因为, 两个子电路可以共用输入顶点.

综上, 任意 n 元布尔函数可用不超过 $10 \cdot 2^n$ 规模的电路计算.

2

先证明一个引理.

引理: 所有 t 元布尔函数对应的电路规模之和不超过 $10 \cdot 2^{t+2^t}$.

t 元布尔函数共有 2^{2^t} 个, 由上一题结果, 每个都可用不超过 $10 \cdot 2^t$ 规模的电路计算出, 因此引理得证.

对于一个 n 元布尔函数, 如果先像上一题那样展开 $n-t$ 层, 会使用不超过 $5\cdot 2^{n-t}$ 个门, 并留下 2^{n-t} 个待计算的 t 元布尔函数, 而由引理, 使用不超过 $10\cdot 2^{t+2^t}$ 个门就能将这些 t 元布尔函数全部计算出. 最终我们使用了不超过 $S_t(n)=5\cdot 2^{n-t}+10\cdot 2^{t+2^t}$ 个门.

当 $n\le 100$ 时, 根据上一题结果直接有 $10\cdot 2^n\le 1000\cdot\frac{2^n}{n}$.

当 $n>100$ 时, 令 $t=\lfloor\log_2 n\rfloor-1$, 计算可得 $S_t(n)\le 1000\cdot\frac{2^n}{n}$.

综上, 任意 n 元布尔函数可用不超过 $1000\cdot\frac{2^n}{n}$ 规模的电路计算.

3

我们知道, 对于任意给定的 t, 存在一个 t 元布尔函数, 计算它的布尔电路的规模是 $\Omega(2^t/t)$ 的.

设 $t(n)=\lceil 2(k+1)\log n\rceil$, 有 $2^{t(n)}/t(n)\ge n^{k+1}$. 因此存在一个布尔函数族 $\{f_n\}$, 其中每个 f_n 是 $t(n)$ 元布尔函数, 且计算它的布尔电路的规模是 $\Omega(n^{k+1})$ 的.

t 元布尔函数总是可以用 2^t 位编码, 只需让其中第 i 位表示按字典序第 i 种变量赋值下布尔函数的值即可, 因此上述 f_n 可用 $O(n^{2k+2})$ 位编码.

记 g_n 是编码字典序最小的, 需要用至少 n^k 规模的布尔电路才能计算的 $t(n)$ 元布尔函数. 上述讨论保证了 g_n 存在且可用 n 的多项式位编码.

g_n 可用量词表述为:

- $\forall g'_n$, g'_n 是字典序小于 g_n 的 $t(n)$ 元布尔函数, $\exists|C'_n|<n^k$, $\forall|x|=t(n)$, $g'_n(x)=C'_n(x)$;
- 且 $\forall|C_n|<n^k$, $\exists|x|=t(n)$, $g_n(x)\ne C_n(x)$.

于是, 语言 $\{g_n\}$ 可表示为一个 Π_3^p 中语言和一个 Π_2^p 中语言的交, 由于 $\Pi_2^p\subseteq\Pi_3^p$, 且易证 Π_3^p 对交封闭, 故 $\{g_n\}\in\Pi_3^p$.

记 $L=\{w|g_{|w|}(w_t)=1\}$, 其中 w_t 是 w 的 $t(|w|)$ 元前缀.

由于 $\{g_n\}$ 中每个 i 元布尔函数有且仅有一个, $g_{|w|}(w_t)=1$ 可写为 $\exists g\in\{g_n\}$, g 是 $t(|w|)$ 元布尔函数, $g(w_t)=1$. 这样一来, 就说明了 $L\in\Sigma_4^p\subseteq\mathbf{PH}$.

再证明 L 的电路复杂性是 $\Omega(n^k)$. 设电路族 $\{C_n\}$ 判定 L, 那么

$$C_{|w|}(w)=1\iff w\in L\iff g_{|w|}(w_t)=1,$$

即 C_n 事实上计算了 g_n, 由 g_n 的定义, 显然 $\{C_n\}$ 的规模是 $\Omega(n^k)$ 的.

4

仿照 $\Sigma_i^p,\Pi_i^p,\mathbf{PH}$ 的定义方法, 可以定义 $\Sigma_i^{exp},\Pi_i^{exp},\mathbf{EXPH}$, 并证明指数层次具有与多项式层次完全平行的性质.

先罗列一些相关的基本结果:

1. $\mathbf{P}=\mathbf{NP}\implies\mathbf{P}=\mathbf{PH}$.
2. $\mathbf{P}=\mathbf{NP}\implies\mathbf{EXP}=\mathbf{NEXP}$.
3. $\mathbf{P}=\mathbf{PH}\implies\mathbf{EXP}=\mathbf{EXPH}$. 使用与证明上一条结果时完全相同的技巧 (padding) 即可证明.

运用结果 1 和结果 3, 显然我们只需证明 $\mathbf{EXPH}$ 中存在至少 $2^n/n$ 规模电路才能判定的语言. 事实上, 这一过程与上一题是完全一样的, 下面再写一遍.

根据教材中提到的结果, 对于充分大的 n, n 元布尔函数的电路复杂度上界不小于 $\frac{2^n}{n}(1+\frac{\log n}{n}-O(\frac{1}{n}))$, 故存在一个 n 元布尔函数, 其电路复杂度至少是 $2^n/n$.

n 元布尔函数总是可以用 2^n 位编码, 只需让其中第 i 位表示按字典序第 i 种变量赋值下布尔函数的值即可.

记 g_n 是编码字典序最小的, 需要用至少 $2^n/n$ 规模的布尔电路才能计算的 n 元布尔函数. 上述讨论保证了 g_n 存在且可用 n 的指数位编码.

g_n 可用量词表述为:

- $\forall g_n'$, g_n' 是字典序小于 g_n 的 n 元布尔函数, $\exists|C_n'|<2^n/n, \forall|x|=n, g_n'(x)=C_n'(x)$;
- 且 $\forall|C_n|<2^n/n, \exists|x|=n, g_n(x)\neq C_n(x)$.

于是, 语言 $\{g_n\}$ 可表示为一个 Π_3^{exp} 中语言和一个 Π_2^{exp} 中语言的交, 由于 $\Pi_2^{exp}\subseteq\Pi_3^{exp}$, 且易证 Π_3^{exp} 对交封闭, 故 $\{g_n\}\in\Pi_3^{exp}$.

记 $L=\{w|g_{|w|}(w)=1\}$.

由于 $\{g_n\}$ 中每个 i 元布尔函数有且仅有一个, $g_{|w|}(w)=1$ 可写为 $\exists g\in\{g_n\}$, g 是 $|w|$ 元布尔函数, $g(w)=1$. 这样一来, 就说明了 $L\in\Sigma_4^{exp}\subseteq\mathbf{EXPH}$.

再证明 L 的电路复杂性至少是 $2^n/n$. 设电路族 $\{C_n\}$ 判定 L, 那么

$$C_{|w|}(w)=1 \iff w\in L \iff g_{|w|}(w)=1,$$

即 C_n 事实上计算了 g_n, 由 g_n 的定义, 显然 $\{C_n\}$ 的规模至少是 $2^n/n$.

5

下面将一致 NC^1 就简称为 NC^1, 在本题中这不会引起混淆.

先证明 $\mathrm{NC}^1\subseteq\mathbf{L}$.

对于任意 $A\in\mathrm{NC}^1$, 存在电路族 $\{C_n\}$ 判定 A, C_n 的规模是 $O(n^c)$ 的, 深度是 $O(\log n)$ 的, 且存在图灵机 M, C_n 的每一位可由 M 在对数空间计算出.

构造图灵机 M', 对于输入 w, $|w|=n$, M' 模拟 C_n 的运行, 当需要用到 C_n 的某一位时, M' 模拟 M, 用对数空间计算出这一位. 为了使用不超过对数大小的空间, 对 C_n 的模拟以递归的方式进行, 即, 为了计算最终输出, 先依次计算输出门所连接的两个门的输出, 像这样不断递归调用下去, 直到抵达输入顶点. C_n 的深度是 $O(\log n)$ 的, 因此递归深度最大也是 $O(\log n)$ 的, 由于每一层递归只需记录 $O(1)$ 的信息, 因此模拟 C_n 只需要对数空间.

于是, 我们得到了在对数空间判定 A 的图灵机 M', 也就证明了 $\mathrm{NC}^1\subseteq\mathbf{L}$.

再证明 $\mathbf{PSPACE}\neq\mathrm{NC}^1$. 事实上 $\mathrm{NC}^1\subseteq\mathbf{L}\subset\mathbf{PSPACE}$, 故结论显然. 这里 $\mathbf{L}$ 真包含于 $\mathbf{PSPACE}$ 是空间分层定理的直接推论.