Homework 6

Name: 方嘉聪 ID: 2200017849

Problem 1.(12 points). Learn the definition of **P**-complete(Arora Textbook def 6.28). Show that if L is **P**-complete then $L \in \mathbf{NC}$ iff $\mathbf{P} = (\text{uniform})\mathbf{NC}$.

Def: A language is **P**-complete if it is in **P** and every language in **P** is log-space reducible to it. ◀

Solution. (1) 如果 (uniform)$\mathbf{NC} = \mathbf{P}$, 而 L 是 **P**-complete, 即 $L \in \mathbf{P} = (\text{uniform})\mathrm{NC}$.

(2) 如果 $L \in \mathbf{NC}$, 只要证明 $\mathbf{P} \subseteq \text{uniform}\mathbf{NC}$, 即证明对于任意 $L' \in \mathbf{P}$, 存在 `poly(n)` size 和 `polylog(n)` depth 的电路族 $\{D_n\}$, 使得 $\{D_n\}$ 可以计算 L' 且存在一个 implicit log-space 的图灵机 M 使得输入 1^n, M 可以输出 D_n 的描述 (uniform).

首先由于 L 是 **P**-complete, 故存在一个 log-space 的规约 f 使得 $x \in L' \iff f(x) \in L$, 而 $L \in \mathbf{NC}$, 故存在一个 `poly(n)` size 和 `polylog(n)` depth 的电路族 $\{C_n\}$ 可以计算 L. 不妨设 $\{C_n\}$ 的深度是 $O(\log^i n)$, 由于 $f(x)$ 的大小是 $\texttt{poly}(|x|)$, 故 $f(x)$ 对应的电路 $C_{f(x)}$ 的深度为 $O(\log^i |f(x)|) = O(\log^i |x|)$. 这里实际上 $L \in (\text{uniform})\mathbf{NC}$, 那么这里得到的电路族已经是 uniform 的了. 那么只需要再证明规约 f 可以被一个 (uniform)**NC** 中的电路计算.

为此需要证明 $\mathbf{NL} \subseteq (\text{uniform})\mathbf{AC}^1$. 如果成立我们有 $\mathbf{L} \subseteq (\text{uniform})\mathbf{NC}^2 \subseteq (\text{uniform})\mathbf{NC}$, 即规约 f 可以被一个 (uniform)**NC** 中的电路 $\{C'_n\}$ 计算. 将 $\{C'_n\}$ 和 $\{C_n\}$ 连接起来, 即可得到一个 (uniform)**NC** 电路族来计算 L', 这就是我们需要的电路族 $\{D_n\}$.

下面给出 $\mathbf{NL} \subseteq (\text{uniform})\mathbf{AC}^1$ 的证明[1]:

我们来证明对 $\forall L \in \mathbf{NL} \implies L \in (\text{uniform})\mathbf{AC}^1$. 设一个 NDTM M 在空间 $t = O(\log n)$ 内判定了 L, 记 M 的格局数为 $N(n) = 2^{O(\log n)} = \texttt{poly}(n)$, 给定任意的 n, 记 $N = N(n)$, 对于任意输入 $w \in \{0,1\}^n$, 我们如下构造电路:

- 构造邻接矩阵 $A_x \in \{0,1\}^{N \times N}$, 其中 $A_x[i,j] = 1$ 当且仅当 $\delta(i) = j$. 这里 $\delta(i)$ 表示 M 在格局 i 上的下一个格局. 这可以在常数层的电路中完成, 读取一下格局 i 的状态, 然后读取一下格局 j 的状态, 然后判断是否是邻接的状态即可.
- 计算 A_x 的传递闭包 (transitive closure)[2], 即我们需要计算 $A^+ = I \vee A \vee A^2 \vee \cdots$, 这反映了从任意一个格局 i 到任意一个格局 j 是否存在一条路径.

其中我们可以采取布尔矩阵的乘法来优化计算, 例如 $(A \vee I)$ 表示是否两个点能否一步到达, $(A \vee I)^2$ 表示是否两个点能否至多两步到达. 一般的, 需要计算的是 $(A \vee I)^N$. 而对布尔矩阵乘法, 我们可以采取如下的方法:

$$(AB)_{i,j} = \bigvee_{k=1}^{n} (A_{i,k} \wedge B_{k,j}) \tag{1}$$

式(1)中的 $\bigvee$ 操作可以在常数层的电路中完成 (考虑 fan-in 不限的电路门). 而为了计算 $(A \vee I)^N = (A \vee I)^{2^{O(\log n)}}$, 我们可以采取树形结构进行计算, 即第一层计算 $(A \vee I) \cdot (A \vee I)$, 第二层计算 $(A \vee I)^2 \cdot (A \vee I)^2$,

[1] 这个证明部分参考了`https://www.cs.umd.edu/~jkatz/complexity/f11/lecture11.pdf`

[2] 对于一个有向图 $G = (V,E)$, 传递闭包 $G^* = (V, E^*)$ 定义如下: $(u,v) \in E^* \iff \exists k \geq 1, \exists w_1, w_2, \cdots, w_{k-1} \in V$, 使得 $(u, w_1), (w_1, w_2), \cdots, (w_{k-1}, v) \in E$.(Sipser, page 429.)

以此类推, 直到计算到 $(A \vee I)^{2^{O(\log n)}}$. 复用相同的部分, 这样得到的树的深度是 $O(\log n)$, 每一层的计算是常数层的电路, 故整个计算的电路深度是 $O(\log n)$, 大小为 $\texttt{poly}(n)$, 故属于 $\mathbf{AC}^1$. 证毕.

注: 第一次接触传递闭包的概念, 使用了布尔矩阵乘法的优化, 感觉这个这个证明相当的繁琐 (主要是为了说明 uniform), 过程里还有些细节没有详尽写出. 类似的如果考虑 **NC** 电路, 那么计算式(1)需要 $\log(n)$ 深度的电路, 进而也可以得到 $\mathbf{NL} \subseteq \mathbf{NC}^2$. ◁

Problem 2.(24 points). Show that the majority function cannot be computed in $\mathbf{AC}^0$.
The majority function $maj : \{0,1\}^n \to \{0,1\}$: output 1 if number of 1s in the input is at least $n/2$; outputs 0 otherwise. ◀

Solution. 我们来证明如下的引理:

Lemma 1. $maj \in \mathbf{AC}^0 \implies PARITY \in \mathbf{AC}^0$.

证明. 设电路族 $\{C_n\} \in \mathbf{AC}^0$ 计算 maj 函数. 对于任意 $w \in \{0,1\}^n$, 我们可以设计如下的电路来判断 $|w|_1 \geq k$ 是否成立, 其中 $k \in \mathbb{N}^+$, $|w|_1$ 表示 w 中 1 的个数:

- 当 $k \geq n/2$ 时, 将字符串 $0^{2k-n}w$ 输入电路 C_{2k}, 输出即为 $\mathbf{1}_{\{|w|_1 \geq k\}}$.
- 当 $k < n/2$ 时, 将字符串 $1^{n-2k}w$ 输入电路 C_{2n-2k}, 输出即为 $\mathbf{1}_{\{|w|_1 \geq k\}}$.

由于 C_n 是 $\mathbf{AC}^0$ 电路, 所以上述电路也是 $\mathbf{AC}^0$ 电路 (通过上述操作可以得到一个新的电路族, 将所需的额外 0/1 串直接固定在对应电路上即可, 记为 $\{C_n^1\}$). 类似的, 可以设计 $\mathbf{AC}^0$ 电路族来判断 $|w|_1 \leq k$ 是否成立 (电路将 w 先取反后类似上述构造即可, 这里不详细给出, 记得到的电路为 $\{C_n^2\}$). 将电路族 $\{C_n^1\}$ 与 $\{C_n^2\}$ 的输出用 $\wedge$ 操作连接, 即可得到一个 $\mathbf{AC}^0$ 电路族 $\{\widehat{C}_n\}$ 来判断 $|w|_1 = k$ 是否成立.

下面从 $\{\widehat{C}_n\}$ 出发, 设计一个 $\mathbf{AC}^0$ 电路族来计算 $PARITY$ 函数.

注意到对于任意 $w \in \{0,1\}^n$, 当 $|w|_1$ 为奇数时, $PARITY$ 函数的输出为 1, 否则为 0. 故考虑电路

$$C_n' = \bigvee_{k \text{ is odd}} \widehat{C}_k$$

常数个 $\wedge$ 操作后得到的电路仍是 $\mathbf{AC}^0$ 电路, 且其输出即为 $PARITY$ 函数. 故 $PARITY \in \mathbf{AC}^0$. □

回到原题, 假设 $maj \in \mathbf{AC}^0$, 由引理可知 $PARITY \in \mathbf{AC}^0$. 但已经证明过 $PARITY \notin \mathbf{AC}^0$, 矛盾. 故 maj 函数不能在 $\mathbf{AC}^0$ 中计算. ◁

Problem 3.(20 points). Show that one can efficiently simulate choosing a random number from 1 to N(donete this set as $[N]$) using coin tosses. That is, show that for every N and $\delta > 0$, there is a probabilistic algorithm A running in $\texttt{poly}(\log N \log(1/\delta))$ time with output in $\{1, 2, \cdots, N, ?\}$ such that
(a) conditional on not outputting ?, A's output is uniformaly distributed in $[N]$ and
(b) the probability that A outputs ? is at most δ. ◀

Solution. 考虑如下的随机算法:

Algorithm 1 Simulate choosing a random number from $[N]$

Input: $N \in \mathbb{N}^+, \delta > 0$

Output: $x \in [N]$ 或 ?

1: 取 $n \in \mathbb{N}^+$ 使得 $N \in \left[2^{n-1}, 2^n\right)$. 即 $n \leftarrow \lfloor \log N \rfloor + 1$.

2: **for** $i = 1, 2 \cdots \lceil \log(1/\delta) \rceil$ **do**

3:     投掷 n 次硬币, 记结果为 $b_1, b_2, \cdots, b_n$.

4:     $b \leftarrow (b_1 b_2 \cdots b_n)_2$, 即将 n 次硬币的结果看作一个二进制数.

5:     **if** $1 \le b \le N$ **then**

6:         **return** b

7:     **else**

8:         `continue`

9: **return** ?

下面我们来证明这个算法符合题目要求.

(1) 在不输出 ? 的条件下, 即在第 i 次迭代中输出了 $b \le N$. 第 3 行投掷硬币得到每一位 0/1 概率相同, 故 $\Pr(b = x \mid x \in [N]) = 1/N$, 故在不输出 ? 的条件下, 输出是均匀分布的.

(2) 设第 i 循环中 b^i 的取值是 $\{0, 1, 2, \cdots, 2^n - 1\}$ 上的均匀分布, 共有 2^n 种取值. 故

$$\Pr[b^i = 0 \vee b^i > N] = \frac{2^n - N}{2^n} \le \frac{2^n - 2^{n-1}}{2^n} = \frac{1}{2}.$$

那么循环 $\lceil \log(1/\delta) \rceil$ 次后输出 ? 的概率为:

$$A := \{\text{output } ?\} = \bigwedge_{i=1}^{\lceil \log(1/\delta) \rceil} \{b^i = 0 \vee b^i > N\}$$

$$\Pr[A] = \prod_{i=1}^{\lceil \log(1/\delta) \rceil} \Pr[b^i = 0 \vee b^i > N] \le \left(\frac{1}{2}\right)^{\lceil \log(1/\delta) \rceil} \le \delta.$$

即输出 ? 的概率不超过 δ.

(3) 每次循环内运行时间为 $\mathtt{poly}(\log N)$, 共循环 $\lceil \log(1/\delta) \rceil$ 次, 故总的运行时间为 $\mathtt{poly}(\log N \log(1/\delta))$. 证毕. ◁

Problem 4.(22 points). Learn the definition of randomized polynomial time reduction and the definition of **BP·NP** in Arora Textbook section 7.6. and solve the following problem.

A nondeterministic circuit C has two inputs x, y. We say that C accepts x iff there exist y such that $C(x, y) = 1$. The size of the circuit is measured as a function of $|x|$. let **NP/poly** be the languages that are decided by polynomial size nondeterministic circuits. Show that **BP·NP** $\subseteq$ **NP/poly**.

Definition 7.16: language B reduces to language C under randomized polynomial time reduction, denoted by $B \le_{\mathrm{r}} C$, if there is a probabilistic polynomial time TM M such that for all $x \in \{0,1\}^*$,

$$\Pr[B(x) = C(M(x))] \ge 2/3$$

Definition 7.17: **BP·NP** $= \{L : L \le_r \text{3SAT}\}$. ◀

Solution. 对任意的 $L \in \mathbf{BP}\cdot\mathbf{NP}$, 有 $L \leq_r$ 3SAT, 即存在一个多项式时间的 PTM M 使得

$$\forall x \in \{0,1\}^*,\ \Pr[L(x) = \mathtt{3SAT}(M(x,r))] \geq 2/3,\ \left(r \in \{0,1\}^{p(n)}\right) \tag{2}$$

其中 $p(\cdot)$ 是一个多项式函数. 对于给定的输入长度 n, 这里不能直接使用 error reduction, 我们考虑如下的多项式时间图灵机 M_n':

运行 M 足够多的次数, 那么利用 Chernoff Bound, 存在一个多项式 $t(n)$ 使得:

$$\forall x \in \{0,1\}^n, \Pr\left[\text{majority}_{i\in[t(n)]}\{\mathtt{3SAT}(M_n'(x,r_i))\} \neq L(x)\right] \leq 2^{-(n+1)}. \tag{3}$$

这里 $r_i \in \{0,1\}^{p(n)}, 1 \leq r_i \leq t(n)$ 是随机比特串.

那么由 Union Bound, 对于 $\forall x \in \{0,1\}^n$, 有

$$\begin{aligned}
&\Pr\left[\bigcup_{x\in\{0,1\}^n} L(x) \neq \text{majority}_{i\in[t(n)]}\{\mathtt{3SAT}(M_n'(x,r_i))\}\right] \\
&\leq \sum_{x\in\{0,1\}^n} \Pr\left[L(x) \neq \text{majority}_{i\in[t(n)]}\{\mathtt{3SAT}(M_n'(x,r_i))\}\right] \\
&= 2^{-(n+1)} \cdot 2^n = 1/2 < 1.
\end{aligned}$$

那么存在一个 $r_n' = r_1 r_2 \cdots r_{t(n)} \in \{0,1\}^{p(n)\cdot t(n)}$, 使得

$$\forall x \in \{0,1\}^n, \text{majority}_{i\in[t(n)]}\{\mathtt{3SAT}(M_n'(x,r_i))\} = L(x).$$

故可以构造 $\mathtt{poly}(n)$ 的非确定性电路 C_n, 将这一组随机比特串 r_n' 固定在电路里, 对任意 $x \in \{0,1\}^n$, 都存在 $v_1 \in \{0,1\}^{\mathtt{poly}(n)}$ 作为判断 $M_n'(x,r_i) \in$ 3SAT 的证书 (存在性由 3SAT $\in$ **NP** 保证), 使得 $C_n(x,v_1)$ 可以计算 $L(x)$, 若 $x \in L$, 则电路输出 $w = M_n'(x,r_i) \in$ 3SAT, 反之亦然.

对于 3SAT, 设对应的多项式时间验证机为 $M_{3\text{SAT}}$, 证书为 $v_2 \in \{0,1\}^{\mathtt{poly}(n)}$. 那么存在一个多项式大小的非确定性电路 $C_{3\text{SAT}}$, 令 $y = v_2$, 则有 $C_{3\text{SAT}}(x,y) = M_{3\text{SAT}}(x,y)$. 进而将 C_n 的输出作为 $C_{3\text{SAT}}$ 的输入, 即可得到一个多项式大小的非确定性电路 C, 使得对于任意的 $x \in \{0,1\}^n$, 有

$$C(x, v_1 \cdot v_2) = C_{3\text{SAT}}(C_n(x,v_1), v_2) = 1 \iff x \in L.$$

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

注: 式(3)可以证明如下: 运行 k 次 M, 记结果为 $M_1, \cdots, M_k$, 引入指示随机变量 Y_i. 若 $L(x) = \mathtt{3SAT}(M_1(x)), Y_i = 1$; 否则为 0. 那么由式(2)知:

$$\Pr[Y_i = 1] \geq \frac{2}{3} \implies \mathbb{E}[Y_i] \geq \frac{2}{3}.$$

记 $Y = \sum Y_i$, 那么由 Chernoff Bound 有:

$$\Pr[Y < (1-\delta)\mathbb{E}[Y]] < e^{-\frac{\delta^2\mathbb{E}[Y]}{2}} \implies \Pr\left[Y < \frac{2(1-\delta)k}{3}\right] < \exp\left(-\frac{k\delta^2}{3}\right)$$

取 $\delta = 1/4, k = \lceil 48(n+1)\ln 2\rceil$ 则有:

$$\Pr\left[Y < \frac{k}{2}\right] < e^{-\frac{k}{48}} \leq 2^{-(n+1)}.$$

进而有式(3)成立.

注: 前半部分的证明和吴悦天同学讨论过, 主要纠结的点在于如何绕过 C_n 的输出是一个字符串的障碍 (因为这一点所以没有办法直接用 error reduction) 并且说明 r'_n 的存在性. 不知道还有没有其他的方式来实现将式(2)的错误降低到指数级, 以及感觉还有一些细节没有写明白, 助教学长见谅:(◁

Problem 5.(22 points). Show that **BPL** $\subseteq$ **P**. ◀

Solution. 大体思路: 先计算概率图灵机 M 的转移概率矩阵 P, 看作一个随机游走过程, 然后计算 P^t 的概率, 判断 $P^t(c_{start}, c_{accept}) \geq 2/3$. 证明这一过程是 $\texttt{poly}(n)$ 的.

对 $\forall L \in \mathbf{BPL}$, 存在空间为 $O(\log n)$ 的 PTM M, 使得 $L(M) = L$. 对任意输入 $x \in \{0,1\}^n$, 记 $M(x, r)$ 的格局数为 $C = 2^{O(\log n)} = n^{O(1)}$. 由于 M 是 log-spqce 的, 则 M 运行时间是多项式时间的, 记为 $t(n)$. 考虑如下的算法 A:

1. 首先构造 M 的格局图对应的 $C \times C$ 的邻接矩阵 P, 其中 $P(c_i, c_j) = 1/2$ 当 M 在格局 c_i 上可以 1 步转移到格局 c_j. 在其他情况, 令 $P(c_i, c_j) = 0$. 这个邻接矩阵的构造容易在多项式时间内完成.
2. 那么对任意的 t, $P^t(c_i, c_j)$ 表示能够在 t 步从格局 c_i 转移到格局 c_j 的概率. 可以把这一过程看作一个随机游走, 每一步都是独立的, 且转移矩阵为 P.
3. 若 $x \in L$, 则存在一条长度不超过 $t(n)$ 的路径, 使得从初始格局到接受格局的概率大于 2/3. 故若 $P^t(c_{start}, c_{accept}) \geq 2/3$, 则令 A 接受 x.

下面来分析第 2 步的运行时间, 首先每一次的矩阵乘法所需的时间为 $O(C^3)$. 而对于 $t(n)$ 次的矩阵乘法, 我们可以用快速幂的方法来计算 (分别计算 $P, P^2, P^4, \cdots$), 那么所需的总时间为

$$O(\log(t(n)) \cdot C^3) = \texttt{poly}(n)$$

注意到这里的 $t(n)$ 是 $\texttt{poly}(n)$ 的.

最后还需要注意这里计算概率的精度 (可能需要的字符串表示长度会比较长). 注意到 P^t 中的概率都是 $1/2^{t(n)}$ 的整数倍, 故我们可以用不超过 $\texttt{poly}(n)$ 的比特位表示且保证精度. 故 A 是一个多项式时间的确定性算法, 对应着一个多项式时间的确定性图灵机 M', 且 M' 可以判定 L.

综上所述, **BPL** $\subseteq$ **P**. 证毕. ◁