Homework 2

5130309059 李佳骏

taringlee@sjtu.edu.cn

2015.10.8

Theorem 2.11(COMBINATORIAL VERSION)

Prove that for every function $f : X \times Y \to \{0,1\}$,

$$D(f) = O(N^0(f)N^1(f))$$

首先我们制定一些定义和规定。

- 定义 F_B 表示所有布尔函数的集合。
- 定义一个二元函数 $L(k,l)$, 满足:

$$L(k,l) = \max_{g \in F_B}^{C^1(g)\le k, C^0(g)\le l} C^P(g)$$

考虑布尔函数 f 的最优化覆盖。令 $R = S \times T$ 为其中的一个 0 单色矩形阵 (rectangle)，$R' = S' \times T'$ 为其中的一个 1 单色矩形阵。由于 $R \cap R' = \varnothing$，所以 $S \cap S' = \varnothing$ 或 $T \cap T' = \varnothing$ 至少有一个成立。不失一般性的，令至少有一半的 R' 存在且满足 $S \cap S' = \varnothing$；否则对矩阵 M_f 做转置即可。

现在构造一个合适的协议 (protocol)。

- 首先，Alice 向 Bob 传达信息 $x \in S$ 是否成立。
- 若成立，则空间可缩小到 $S \times Y$，而这样的话至多只有 $\frac{k}{2}$ 个 1 单色矩形阵。
- 若不成立，则空间可缩小到 $\overline{S} \times Y$，而这样的话至多只有 $l-1$ 个 0 单色矩形阵。

由此，可得公式

$$L(k,l) \le L(\frac{k}{2}, l) + L(k, l-1) \le (l+1)^{\log k}$$

由定理 2.8，$D(f) = O(\log C^P(f))$，可得

$$D(f) = O(\log(L(C^1(f), C^0(f)))) = O(\log(C^0(f)+1)^{\log C^1(f)}) = O(\log C^0(f)\log C^1(f))$$

即，

$$D(f) = O(N^0(f)N^1(f))$$

Exercise 2.13

Let f be any function for which $X \times Y$ can be covered by t f-monochromatic geometric rectangles(possibly with overlaps). Prove that $D(f) = O(\log t)$.

对于任意一种覆盖方案，都可以直接构建一个协议，则满足 $C^P(f) \le t$；显然的，$t \le 2^{D(f)}$。所以得，

$$C^P(f) \le t \le 2^{D(f)}$$

这样的协议 (protocol) 构建有很多种方法，以下举证其中的一种：

- Alice 和 Bob 预处理，将 rectangle 进行离散化处理。
- Alice 把 x 所在的区域的编号传个 Bob
- Bob 综合信息，找到 M_{xy}，输出结果

根据定理 2.8，可知 $D(f) = O(\log C^P(f))$。由广义夹逼定理可得，$D(f) = O(\log t)$。

Exercise 2.18

Show that most functions $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ satisfy $N^1(f) = \Omega(n)$, and yet the size of the largest fooling set for f is $O(n)$.

考虑一个随机布尔函数 $f_r : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$。其中对于任意的 (x,y) 与 (x',y')，满足 $x,x' \in X$，$y,y' \in Y$，$f(x,y)$ 与 $f(x',y')$ 的取值相互独立，且为 0 或 1 的概率相等。

因此，矩阵 M_{f_r} 的元素为 1 的个数的期望是 $2^n * 2^n/2 = 2^{2n-1}$. 由 Chernoff 不等式，1 的个数小于 2^{2n-2} 的概率是 $\epsilon_1 = 2e^{-\frac{n}{8}}$.

而若 $N^1(f_r) = \Omega(n)$，则有极大的概率不存在 $8 * 2^n = 2^{n+3}$ 个矩形阵 (rectangle)，存在单个这样的 rectangle 的概率是 $2^{-2^{(n+3)}}$。则整体存在这样一个矩形阵的概率为 $\epsilon_2 = 2^{2^n} 2^{2^n} 2^{-2^{(n+3)}} = 2^{-6 \cdot 2^n}$.

在不存在这样的矩形下继续讨论。而若"the size of the largest fooling set for f is $O(n)$" 成立。则可假设不存在大小为 $8n$ 的 fooling set。出现这样的一个 fooling set 的可能性为 $(\frac{3}{4})^{C(8n,2)} < 2^{-80n^2}$，而出现的次数为 $C(2^{2n}, 8n) < 2^{16n^2}$. 所以存在 $8n$ 的 fooling set 的概率为 $\epsilon_3 = 2^{-80n^2} * 2^{16n^2} = 2^{-64n^2}$

由此，with high probability$(1 - \epsilon_1 - \epsilon_2 - \epsilon_3)$，一个随机函数 f 满足 $N^1(f) = Omega(n)$ 且最大的 fooling set 不超过 $O(n)$

Exercise 2.23

Subproblem 1

Show that the rank of M_{INTER} is n.

不难发现 INTER 作为点积，和矩阵乘法类似。所以可以构造 $2^n \times n$ 的 01 矩阵 A，其中该矩阵每一行表示 X 的一个元素，共 2^n 个。事实上由于 X 集合和 Y 集合的元素相同，可得 $M_{\text{INTER}} = AA^T$。显然的，矩阵 A 的秩为 n。

由线性代数定理可知:

$$rank(A) + rank(A^T) - n \leq rank(AA^T) = rank(M_{\text{INTER}}) \leq \min(rank(A), rank(A^T))$$

解得，$rank(M_{\text{INTER}}) = n$.

显然的，$D(f) = n + 1$。所以,$D(f)$ and $\log rank(f)$ may be exponential.

Subproblem 2

Show that the rank of M_{IP} over $GF(2)$ is n.

不难发现 INTER 和 IP 这两个操作极为相似。做类似的代换即可获得答案，即 $rank(M_{\text{IP}}) = n$。

当然，类似的可以求得 $D(f) = \Omega(n)$。所以，$D(f)$ and $\log rank(f)$ may be exponential。