

4.5.10

סימונים - שיעור 8

הוכחה אינדוקציונית
- שיהיה בין הוכחה למכונה
- הוכחה אינדוקציונית

IP - מערכת סוגיות de הוכחה
AM - " (מכונה פואנטה) *

גרסה של GNISO

$$S = \{ (H, \tau) \mid ((H \sim G_1) \text{ או } (H \sim G_2)) \text{ ו } \tau \in \text{Aut}(H) \}$$

ישם לב: הקיפה שיהיה מקבוצה S נמצא

המחלקה NP.

ההנחה (H, τ) אכן הוכחה נמצא

הוא S →
צריך להוכיח:

$$\begin{aligned} \text{IP} \leadsto \text{Prio} \left\{ \begin{array}{l} H \sim G_2 \text{ או } H \sim G_1 \\ \pi \in \text{Aut}(H) \\ \pi \text{ (קבוצה ב, ופונקציה)} \\ H = \pi(G_2) \end{array} \right. \\ \text{P} \rightarrow \text{Prio} \left\{ \begin{array}{l} \tau \in \text{Aut}(H) \\ \tau(H) = H \end{array} \right. \end{aligned}$$

אינדוקציה בסיס S (הוא) גדול? $S \subseteq \{0,1\}^N$
המקרה של 1. $N = 2^{\log n}$
תאור פונקציה גורם n קבוצות
לבסוף יש: גדול 10

סיון 1:

$$p = \frac{|S|}{2^N}$$

לדוגמה

נניח $X_1, \dots, X_T$ כוונת שיהיה $\{0,1\}^N$

נניח מהם שיהיה S- (גרסה) (המוכר)

לדוגמה T ממוקד S- (גרסה)

$$p \sim \frac{t}{T}$$

4.5.10

קריטריון 2: כל סדר ממוצע מ"ר.

נניח X_a סדר ממוצע, $a \in \{0,1\}^n$ מ"ר
הערה -

$$X_a = h(a)$$

$$2^n \text{ מ"ר מ"ר}$$

1. X_a סדר ממוצע

2. ג"ר ג"ר

הוכחה נכונה על הפרדוקס:

אם G_1, G_2 סדר ממוצע, $|S|=n!$ סדר ממוצע, $V \cdot e$ הערה נכונה

$$pr_{b \in \{0,1\}^n} [\exists a \in S, h(a) = b] = \frac{|I_n(S)|}{2^n} \leq \frac{|S|}{2^n} = \frac{n!}{2^n} = q$$

אם G_1, G_2 סדר ממוצע, $|S|=2 \cdot n!$ סדר ממוצע, $b \in \{0,1\}^n$

$$pr_{h \in H} [\exists a \in S, h(a) = b] \geq \sum_{a \in S} pr_{h \in H} [h(a) = b] = \frac{1}{2} \sum_{a_1, a_2 \in S, h(a_1) = h(a_2) = b} pr_{h \in H} [h(a_1) = b, h(a_2) = b]$$

$$= |S| \cdot 2^{-n} - \frac{1}{2} |S|^2 \cdot 2^{-2n} = \frac{|S|}{2^n} - \frac{1}{2} \left(\frac{|S|}{2^n} \right)^2$$

$$= \frac{2n!}{2^n} - \frac{1}{2} \cdot 2 \cdot \left(\frac{2n!}{2^n} \right)^2 = 2q - 2q^2 = 2q(1-q)$$

$$\left(|S| \leq 2^n \leq 2n!, \frac{1}{20} \leq q \leq \frac{1}{10}, 1-q \geq \frac{9}{10} \right)$$

$$\geq 2 \cdot \frac{9}{10} q \geq 2 \cdot \frac{9}{10} \cdot \frac{1}{20}$$

הוכחה נכונה: אם G_1, G_2 סדר ממוצע, $|S|$ סדר ממוצע

$$pr_{h \in H} \left[\sum_{a \in S} h(a) \geq \frac{|S|}{2} \right] \geq q$$

אם G_1, G_2 סדר ממוצע, $|S|$ סדר ממוצע, $|S| \geq \frac{1}{2} |S|$

$$pr_{h \in H} \left[\sum_{a \in S} h(a) \geq \frac{|S|}{2} \right] \geq 1.5q$$

$$\frac{1}{20} \leq q \leq \frac{1}{10}, \text{ GUISOAM } q, 1.5q$$

$$(0n! \leq 2^n \leq 20n! \quad , \quad G_1, G_2 \quad (d) -$$

(Public wins) $P-J$ $2/16$ N/E

1.259 $\leq$ $\rho_{\text{min}}(\lambda)$ q_i $\rightarrow$ Sink ρ_{cc} $\Delta_i^+ V^-$

$$P = A_m(\omega)$$

0 1 112

$$P = 1 \quad S = 1 \times 10^{-11} = 111$$
$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{pmatrix}$$
$$A_1 = -7/2 \cdot 1000$$

∴ $\{y, z\} = \mu_2(A_1) \cdot P \rightarrow M(x, y, z)$ $\frac{1}{1} \cdot \frac{1}{1} \cdot \frac{1}{1}$

$$\exists y \forall z M(x, y, z) \rightarrow 1 \quad \in \chi \in L$$
$$\forall z \cdot M(x, y, z) = 1 \quad (\Rightarrow x \neq L)$$
$$\forall z \exists x, y, z \leq 0$$

0

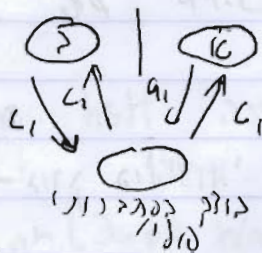
31-15

$$GI \subseteq NP = \exists P \quad \therefore NP \subseteq P$$

$$GNI_{50} \in AM = \exists \rho$$

$NP^{\#}$ סים $GNIS0$ הא $NP^{\#}$ סה $GNIS0$ סה
 קורס $(P \neq \Sigma_k)$ קורס (3) $NP^{\#}$ סה
 הסק: סה $NP^{\#}$ סה $NP^{\#}$ סה
 גס' $NP^{\#}$ סה

NEXP $\sim \rho$ $\rightarrow$ ρ $\rightarrow$ ρ



שמה בין בוזק (הסתדרות)
ס"ב מוכותים כל יבול'ם
שמה יבול'ם מוקדש ביניהם.

2 12111) 11111)

4.5.10

הצגה

$$H = \{h_{a,d} \mid a,d \in F\}$$

$h_{a,d} : F \rightarrow F$
 $\{a\}^N \rightarrow \{a\}^N$

$|H| = |F|^2 = 2^{2N}$

על ידי כך נראה כי H היא קבוצת פונקציות

$$\Pr_{h \in H}(h(a) = b) = \Pr_{c,d \in F}(h_{c,d}(a) = b)$$

$$= \Pr_{c,d \in F}(c \cdot a + d = b) = \Pr_{d \in F}(d = b - c \cdot a) = \frac{1}{|F|} = 2^{-N}$$

$$\Pr_{c,d} (h_{c,d}(a_1) = b_1 \wedge h_{c,d}(a_2) = b_2) = \Pr_{c,d} \left(\begin{matrix} a_1 c + d = b_1 \\ a_2 c + d = b_2 \end{matrix} \right)$$

$$= \Pr_{c,d} \left(\begin{pmatrix} a_1 & 1 \\ a_2 & 1 \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \right)$$

$$A = \begin{pmatrix} a_1 & 1 \\ a_2 & 1 \end{pmatrix}$$

$$\det A = a_1 - a_2 \neq 0$$

$$= \Pr_{c,d} (A \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}) = \Pr_{c,d} \left(\begin{pmatrix} c \\ d \end{pmatrix} = A^{-1} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \right) = \frac{1}{|F|^2} = 2^{-2N}$$