סיבוכיות תקשורת אינפורמציה:

רותם אושמן roshman@tau.ac.il

שעת קבלה: חמישי 17:30-18:30

מבנה הציון: - שיעורי בית - 30% (בערך כל 2-3 שבועות)
- פרויקט סיום - 70% (בזוגות, תהיה הצגה [illegible] בשיעור.)
(אין מבחן).

ספר: (חלק I בעיקר)
Communication Complexity
Kusuilevitz Nisan, 2006

נושאים:

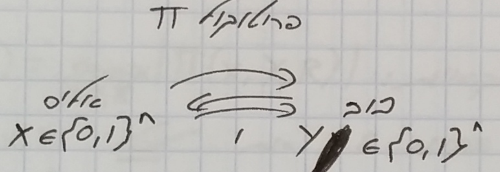
I) סיבוכיות תקשורת "קלאסית".

II) סיבוכיות אינפורמציה.

III) אפליקציות ונושאים מתקדמים: מודלים, מבני נתונים, חישוב מבוזר.

שיעור 1:

הגדרות: סיבוכיות תקשורת:



- שני שחקנים, אליס ובוב, רוצים לחשב $f(X, Y)$.

כמה ביטים צריך להעביר?

כמה תקשורת צריכה להיות כשמפרקים חישוב/בעיה לשני חלקים.

פרוטוקול דטרמיניסטי:

$$\Pi : \underbrace{\{0,1\}^*}_{\substack{\text{היסטוריה} \\ \text{transcript} \\ \text{מה ששודר} \\ \text{עד עכשיו.}}} \times \underbrace{\{0,1\}^n}_{\text{הקלט של אליס}} \times \underbrace{\{0,1\}^n}_{\text{הקלט של בוב}} \longrightarrow \underbrace{\{A, B, O\}}_{\substack{\text{תור מי לדבר} \\ \text{(לא תלוי ב-} X,Y)}} \times \underset{(\text{לא תלוי ב-}Y)}{\{0,1\}} \times \underset{(\text{לא תלוי ב-}X)}{\{0,1\}} \times \underbrace{\{0,1\}}_{\substack{\text{פלט} \\ \text{(כן תלוי ב-} X,Y)}}$$

דוגמא 1- equality:

$$f_{eq}(X, Y) = \begin{cases} 1, & \text{if } x=y \\ 0, & \text{else} \end{cases}$$

פרוטוקול טריוויאלי: - אליס שולחת את X.
- בוב שולח האם Y=X.

סיבוכיות: $n+1$ ביטים.

אופטימלי לפרוטוקול דטרמיניסטי.

הגדרה: סיבוכיות תקשורת:

$$CC(\Pi) = \max_{x,y\in\{0,1\}^n} |\underbrace{\Pi(x,y)}_{\text{תמליל } \Pi \text{ על } x,y.}|$$

$$CC(f) = \min_{\Pi \text{ פותר את } f} CC(\Pi)$$

Π פותר את f אם לכל x,y Π מחשב נכון את f(x,y).

הגדרה: אקראיות:

- אקראיות פומבית: $\Pi: trans \times X \times Y \times R \to \ldots$
- אקראיות פרטית: $\Pi: \ldots \to \ldots \times R_A \times R_B$

כלומר, באקראיות פומבית יש מחרוזת של ביטים אקראיים שידועה לכולם, ובאקראיות פרטית לאליס ולבוב יש מחרוזות משלהם.

הגדרה: סיבוכיות תקשורת עם אקראיות: $CC(\Pi) = \max_{x,y,R} |\Pi(x,y,R)|$

נאמר ש- Π מחשב את f עם שגיאה ε אם לכל x,y,

$$P_R(output(\Pi(x,y,R)) \neq f(x,y)) \le \varepsilon.$$

עבור $\varepsilon > 0$:

$$R^{pub}_{\varepsilon}(f) = \min_{\substack{\Pi \text{ עם} \\ \text{שגיאה } \le \varepsilon.}} CC(\Pi)$$

עבור $\varepsilon = 0$:

$$R^{pub}_{0}(f) = \min_{\substack{\Pi \\ \text{שמחשב את} \\ f \text{ ללא שגיאה.}}} \max_{x,y} E_R[|\Pi(x,y,R)|]$$

(תוחלת גודל ה- transcript).

טענה: אם קיים פרוטוקול תקשורת Π עם שגיאה ε, $C = \max_{x,y}(E_R[|\Pi(x,y,R)|])$,
אז ניתן לבנות פרוטוקול Π' עם שגיאה $\le \delta + \varepsilon$, $CC(\Pi) \le \frac{C}{\delta}$,
(ע"י מרקוב, אם זמן הריצה גדול מ- $\frac{C}{\delta}$ עוצרים ויש שגיאה).

בכיוון השני נכון ע"י צ'רנוף.

גם אפשר להשתמש בהגדרה בתוחלת או ב- worst-case.

בעיית ה- equality:

עם אקראיות פומבית: נגריל את R כוקטור $\{0,1\}^n$ ($R \neq 0$).

- אליס שולחת את $\langle X,R \rangle \bmod 2$ (מכפלה פנימית).
  בוב עונה האם $\langle X,R \rangle = \langle Y,R \rangle$.

סיבוכיות: 2 ביטים.

- אם $X = Y$ הפרוטוקול צודק.
- אם $X \neq Y$: $X-Y \neq 0$, $\langle X-Y, R \rangle = 0$ בהסתברות חצי.
  כלומר, התשובה נכונה בהסתברות חצי.

מסקנה: $R^{\text{פומ}}_{\frac{1}{2}}(eq) \leq 2$ (אי אפשר בביט אחד).

עם אקראיות פרטית:

- אליס בוחרת מספר ראשוני p בין n^2, $2n^2$ $(\mathbb{F}_p)$ (קיים ממשפט הראשוניים)
  ומחשבת את הפולינומים:
  $$X_0 + X_1 Z + \dots + X_{n-1} Z^{n-1} \mod p$$
  $$y_0 + y_1 Z + \dots + y_{n-1} Z^{n-1} \mod p$$
- אליס בוחרת $b \in \mathbb{F}_p$ ושולחת את $p, b, X(b)$. $[O(\log n)]$.
- בוב מחזיר האם $X(b) = Y(b)$.

סיבוכיות: $O(\log n)$.

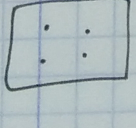
- אם $x=y$, תמיד עונה נכון.
- אם $x \neq y$, לפולינום $y-x$ יש $\leq n-1$ שורשים ב- $\mathbb{F}_p$, לכן
  $P(X(b) = Y(b)) \leq \frac{n-1}{n^2} = O(\frac{1}{n})$.

חסמים תחתונים לפרוטוקולים דטרמיניסטיים:

מלבן קומבינטורי: הגדרה 1: $A \times B$, $A,B \subseteq \{0,1\}^n$.

הגדרה 2: $R \subseteq \{0,1\}^n \times \{0,1\}^n$ שמקיים-

[redacted]



$(X,Y) \in R$, $(X',Y') \in R$ א״מ $(X',Y) \in R$, $(X,Y') \in R$

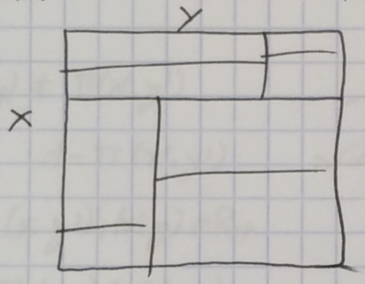
הערה שההגדרות שקולות:

(⇐) נתון $A\times B$. אם $(x,y),(x',y')\in A\times B$, אז $x,x'\in A$, $y,y'\in B$.
ולכן $(x,y'),(x',y)\in A\times B$.

(⇒) נתון R שמקיים את התכונה. אז $A=\{x \mid \exists y.\,(x,y)\in R\}$
$B=\{y \mid \exists x.\,(x,y)\in R\}$.

טענה: נגדיר $R_t:=\{(x,y) \mid \Pi(x,y)=t\}$.
אז R_t מלבן קומבינטורי מונוכרומטי. (אותו פלט).

ה-transcript-ים האפשריים מחלקים ל- $\leq 2^{CC(\Pi)}$ מלבנים קומבינטוריים מונוכרומטיים.



הוכחה: באינדוקציה על הצמתים.

בסיס: $R_\varepsilon=\{0,1\}^n\times\{0,1\}^n$. ($\varepsilon$ = מחרוזת ריקה)

צעד: נניח ש- $R_t=A\times B$, תור אליס לדבר, אליס שולחת ביט σ.

$R_{t\sigma}=\{(x,y) \mid \Pi(x,y)$ רישא של $t\sigma\}$

$=R_t\cap\{(x,y) \mid$ אליס שולחת σ כשמקבלת x ורואה את $t\}$

$=A'\times B$

כאשר $A'=A\cap\{x \mid$ אליס שולחת σ כשמקבלת x ורואה $t\}$.

חסמים על פרוטוקולים דטרמיניסטיים:

שיטה 1: fooling set.

הגדרה: קבוצה $S \subseteq \{0,1\}^n \times \{0,1\}^n$ נקראת fooling set עבור f אם:

(1) לכל $(x,y),(x',y') \in S$, $f(x,y) = f(x',y')$.

(2) לכל $(x,y),(x',y') \in S$ שונים, או ש- $f(x',y) \neq f(x,y)$
או ש- $f(x,y') \neq f(x,y)$.

טענה: אם יש fooling set בגודל $|S| = s$, אז לכל פרוטוקול Π שמחשב את f יש לפחות s עלים שונים.

לכן $CC(\Pi) \geq \log(s)$.

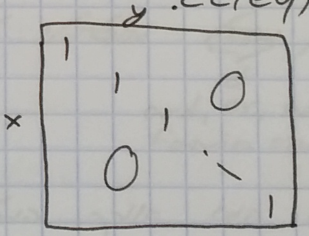
טענה: לכל $(x',y'),(x,y) \in S$ שונים, $\Pi(x,y) \neq \Pi(x',y')$.

הוכחה: נסמן $\Pi(x,y) = t$. נניח בשלילה $\Pi(x',y') = t$.
אז $(x,y),(x',y') \in R_t$, לכן $(x,y'),(x',y) \in R_t$.
מכיוון ש- $f(x,y') \neq f(x,y)$ או $f(x',y) \neq f(x,y)$, סתירה.

שימושים:

משפט: $CC(eq) \geq n$.

הוכחה:



רעיון:
אי אפשר לכסות עם מעט
מלבנים מונוכרומטיים.

נגדיר fooling set, $S = \{(x,x) \mid x \in \{0,1\}^n\}$.

מתקיים: (1) לכל $(x,x) \in S$, $f_{eq}(x,x) = 1$.

(2) אם $(x,x),(y,y) \in S$, $x \neq y$, אז
$f_{eq}(x,y) = f(y,x) = 0$.

לכן $CC(eq) \geq \log(s) = \log(2^n) = n$.

אפשר לקבל $\geq n+1$.

דוגמא (תשובה): Set Disjointness:

$$f_{disj}(X,Y)=\begin{cases}1, & X\cap Y=\phi\\ 0, & else\end{cases}$$ (וקטור = קבוצה).

טענה: $CC(f_{Disj})\ge n$.

הוכחה: נגדיר $S=\{(x,\bar{x}) \mid x\in\{0,1\}^n\}$. ($\bar{x}$ = המשלים של x).

(1) $f_{disj}(x,\bar{x})=1$ לכל x.

(2) אם $x\neq y$, אז קיים i כך שבה"כ $i\in x\setminus y$.
לכן $i\in x\cap\bar{y}$, $f_{disj}(x,\bar{y})=0$.

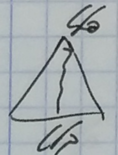
לכן:
$CC(disj)\ge\log(2^n)=n$.

משחקי Karchmer-Wigderson ('93): $KW(f)$.

המשחק: אליס מקבלת x, בוב מקבל y.
ישנה פונק' f שידועה מראש, כך ש- $f(x)=1,\ f(y)=0$.
המטרה היא למצוא $i\in[n]$ כך ש- $x_i\neq y_i$.

משפט: עומק $\underbrace{\text{מעגל}}_{\substack{\text{and, or, not}\\ \text{fan-in}=2}}$ אופטימלי ל- f = $CC(KW(f))$.

עומק [redacted] הוא אורך המסלול הארוך ביותר ~~[illegible]~~ מפלט לקלט.



הוכחה:

[⇐] יהי C מעגל בעומק d ל-f. נבנה פרוטוקול תקשורת:
אם במעגל יש שער AND, אז ל-x שתי הכניסות 1, ול-y אחת הכניסות 0. בוב יבחר "ימינה/שמאלה".
אם במעגל יש שער OR, אליס אומרת לאן ללכת.
וכך הלאה. not - מחליפים תפקידים.

בכניסות של המעגל, מגיעים לנקודה שבה $x\neq y$.

[⇒] בונים מעגל שמחכה את הפרוטוקול. ויתרנו כי אין זמן.

משחקי Karchme[illegible]-Wigderson מונוטוניים:

נותן x, y כך ש- $f(x)=1, f(y)=0$, f מונוטונית.

המטרה למצוא i כך ש- $x_i=1$, $y_i=0$.

אין not (כי מונוטוני).

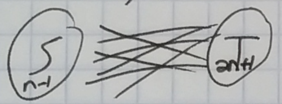
משפט Raz (׳94): אין מעגל מונוטוני שבודק אם בגרף נתון יש שידוך (matching) בגודל $\geq n$ בעומק $< o(n)$.

הוכחה: (עד השבוע הבא.) המשחק KW: x = גרף עם שידוך בגודל $\geq n$.
y = גרף בלי שידוך בגודל $\geq n$. } גרפים עם $3n$ קודקודים.

x, y בגודל $\sim (3n)^2$.

המטרה: למצוא קשת ב- x שאינה ב- y.

נתמקד בקלטים מהצורה: x = שידוך בגודל n (ללא קשתות נוספות).
y = גרף דו-צדדי מלא $|S|=n-1$, $|T|=2n+1$



נעשה כמה רדוקציות.

בעיית pair disjointness: אליס מקבלת סדרה של n זוגות מתוך $1,\dots,3n$, כאשר מספר אינו מופיע פעמיים. בוב מקבל קבוצה P של $n-1$ מספרים מ- $1,\dots,3n$, כך שקיים i יחיד שמקיים את הדרישה.
מטרה: למצוא i כך ש- $L_i \cap P = \phi$ (L_i הזוג ה-i של אליס).

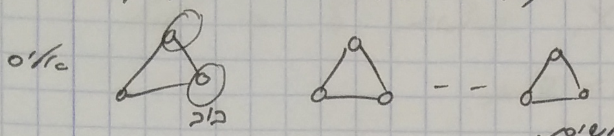
רדוקציה מ- pair disj. ל- matching: בהינתן L, P, נבנה קלט ל- matching.
$x = L$, $y = P \times ([3n] \setminus P)$.

בעיה P: אליס- סדרה L כמו קודם.
בוב- קבוצה P עם n איברים.
מטרה: האם קיים i כך ש- $L_i \cap P = \phi$?

רדוקציה מבעיה P ל- pair disj.: בוב יזרוק איבר אקראי מהקלט שלו.
השחקנים פותרים pair disj., ומקבלים אינדקס i. אליס שולחת את L_i.
בוב בודק אם האיבר שנזרק הוא ב- L_i. אם כן, נכשלנו- פלט 0.
אחרת, פלט 1.

רדוקציה מ- disj. ל- IP

אליס מקבלת n משולשים, בוב קודקודים.



נחשוב על X,Y כעל אוסף משולשים.

האם יש משולש ששניהם קבלו?

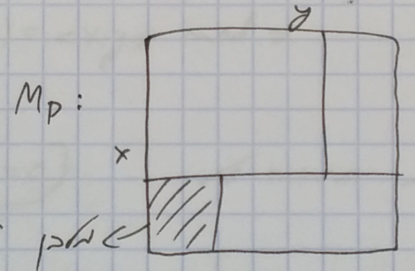
במשולש ה-i, אם $i\in X$, אליס לוקחת את $\{1,2\}$ במשולש.
ואם $i\notin X$, אליס לוקחת את $\{1,3\}$ במשולש.

אם $i\in Y$, בוב לוקח 3.
אם $i\notin Y$, בוב לוקח 2.

כשמרכיבים את הרדוקציות, זה מוכיח את המשפט.

שיעור 2:

תזכורת: $D(f) = \min_{\pi \text{ שמחשב את } f} \max_{x,y} |\pi(x,y)|$ (סימון אחר מהרצאה קודמת.)



מלבן f-מונוכרומטי!

שיטה ראשונה: fooling-set: קבוצת קלטים בעלי אותו ערך f, שאין לשום שניים מהם להוות מלבן.

אם קיים fooling-set S עבור f אז $D(f) \ge \log|S|$.

דוגמאות: $D(EQ) \ge n$, $D(Disj) \ge n$.

מה נעשה היום: (1) rectangle size bound.

(2) rank bound.

(3) פרוטוקולים לא דטרמיניסטים (אם נספיק).

Rectangle Size:

שיטה: נגדיר התפלגות μ על $X \times Y$, ונמצא δ כך שלכל מלבן f-מונוכרומטי R מתקיים $\mu(R) \le \delta$.

אז מסיקים ש- $D(f) \ge \log\left(\frac{1}{\delta}\right)$, כי

$$1 \underset{\text{התפלגות}}{=} \mu(X \times Y) = \sum_{\substack{\text{מלבנים} \\ \text{f-מונוכרומטיים}}} \mu(R) \le \delta \cdot (\#\text{מלבנים}) \le \delta \cdot 2^{D(f)}$$

fooling set vs. rectangle size:

fooling set הוא מקרה פרטי של rectangle size, ולכן זו שיטה לא יותר חזקה.

בהינתן fooling set S, נגדיר

$$\mu(x,y) = \begin{cases} \frac{1}{|S|} & , (x,y) \in S \\ 0 & , \text{else} \end{cases}$$

אז $\delta = |S|$.

לכל מלבן מונוכרומטי R יש $(x,y) \in S$ יחיד לכל היותר, ולכן $\mu(R) \le \frac{1}{|S|}$.

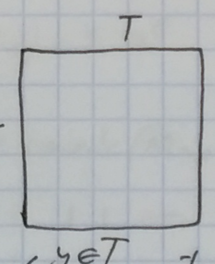
דוגמה: Inner Product

$$f_{IP}(x,y) = \langle x,y \rangle \bmod 2$$

טענה: $D(f_{IP}) \ge n-1$.

הוכחה: יהי μ ההתפלגות האחידה על $\underbrace{\{(x,y) \mid f_{IP}(x,y)=0\}}_{2^{2n-1}\text{ קלטים}}$.

נתבונן ב-0-מלבן $S \times T$:



יהיו $S' = \text{span}(S)$
$T' = \text{span}(T)$

לפי הגדרת f_{IP}, לכל $x \in S$ ו- $y \in T$, אז $\langle x,y \rangle = 0$.

לכן לכל $x' \in S'$, $y' \in T'$, $\langle x',y' \rangle = 0$.

לכן S',T' תתי מרחבים ניצבים (אורתוגונלים), ומכאן

$$\dim(S') + \dim(T') \le n$$

$$|S'| \le 2^{\dim(S')} , \quad |T'| \le 2^{\dim(T')}$$

$$\Downarrow$$

$$|S'| \cdot |T'| \le 2^n$$

$$\Downarrow$$

$$\mu(S \times T) \le \mu(S' \times T') \le \frac{2^n}{2^{2n-1}} = 2^{-n+1}$$

המשך:

נסתכל על inner product:

$$IP_1: \begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

$$IP_2: \begin{array}{c|cc|cc} & 00 & 01 & 10 & 11 \\ \hline 00 & 0 & 0 & 0 & 0 \\ 01 & 0 & 1 & 0 & 1 \\ \hline 10 & 0 & 0 & 1 & 1 \\ 11 & 0 & 1 & 1 & 0 \end{array}$$

Rank Lower Bound:

משפט: לכל פונק' f ושדה $\mathbb{F}$,

$D(f) \geq \log \text{rank}_{\mathbb{F}}(M_f)$.

הוכחה: יהי Π פרוטוקול תקשורת עם סיבוכיות c.

Π משרה חלוקה של M_f ל-2^c מלבנים f-מונוכרומטיים $R_1,..,R_{2^c}$.

(M_R אינדיקטור לערך המלבן).

$$M_f = \sum_{\substack{R \text{ מלבן} \\ \text{עם ערך } 1}} M_R$$

$$\text{rank}(M_f) \leq \sum \underbrace{\text{rank}(M_R)}_{=1} \leq 2^c$$

(מספר של המלבנים עם ערך 1, [illegible])

$(\text{not} f = \neg f)$

$$M_{\neg f} = \sum_{\substack{R \text{ מלבן} \\ \text{עם ערך } 0}} M_R$$

$$\text{rank}(M_{\neg f}) \leq 2^c$$ (כנ"ל, עם ערך 0)

מסקנה:

$$\text{rank}(M_f) + \text{rank}(M_{\neg f}) \leq \sum M_R \leq 2^c$$

$$M_{\neg f} = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 1 & \cdots & & 1 \\ \vdots & & & & & \vdots \\ 1 & 1 & 1 & \cdots & & 1 \end{pmatrix} - M_f$$

$$\text{rank}(M_{\neg f}) \geq \text{rank}(M_f) - 1$$

$$2\text{rank}(M_f) - 1 \leq 2^c$$

$$\Downarrow$$

~~rank~~

$$c \geq \log(2\text{rank}(M_f) - 1)$$

שדה "מעניינים": GF_2.

רגיל: $\mathbb{R}$.

טענה: לכל שדה F, ומטריצה $M \in F^{n\cdot m}$,

$rank_F(M) \le rank_{\mathbb{R}}(M)$.

(לכן בדרך כלל משתמשים את החסם של כל שדה).

אולי נוכיח בהמשך, זה אלגברה לינארית.

דוגמא: שוב inner product.

נמפה $0 \mapsto 1$, $1 \mapsto -1$, ע"י $f_{\tilde{IP}}(x,y) = (-1)^{<x,y>}$.

$$M_{\tilde{IP}} = -2M_{IP} + \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{pmatrix}.$$

לכן מספיק להבין את הדרגה של $M_{\tilde{IP}}$.

$$\tilde{IP}_1: \begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 1 & 1 \\ 1 & 1 & -1 \end{array} \qquad \tilde{IP}_2: \begin{array}{c|cc|cc} & 00 & 01 & 10 & 11 \\ \hline 00 & 1 & 1 & 1 & 1 \\ 01 & 1 & -1 & 1 & -1 \\ \hline 10 & 1 & 1 & -1 & -1 \\ 11 & 1 & -1 & -1 & 1 \end{array}$$

באופן כללי: $\tilde{IP}_n = (\tilde{IP}_1)^{\otimes n}$

(מכפלה טנזורית, לכל איבר במטריצה מכפילים במטריצה ויוצרים בלוק.)

תכונה:

$$rank(A \otimes B) = rank(A) \cdot rank(B)$$

$$\Downarrow$$

$$rank_{\mathbb{R}}(\tilde{IP}_n) = 2^n$$

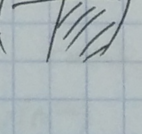
$$rank_{\mathbb{R}}(IP_n) \ge 2^n - 1$$

$$D(IP) \ge \log(2\cdot(2^n-1) - 1) \approx n$$

דרגת M_{IP} מעל GF_2?

$$M_{IP} = (<x,y>_{GF_2}) = \Big(\sum_{i=1}^{n} \underbrace{(x_i y_i)}_{\text{דרגה 1}}\Big)$$

מטריצה



$$\Downarrow$$

$$rank(M_{IP}) \le n$$

הוכחנו $D(f) \ge \log(\text{rank}(M_f))$.

שאלה פתוחה: האם/עד כמה החסם הדוק.

האם $D(f) \le O(\log \text{rank}(M_f))$? לא.

יש דוגמאות שבהן $D(f) \ge (\log \text{rank}(M_f))^{\log_3 6}$ ($\log_3 6 \approx 1.6$)

השערה (שאלה פתוחה): קיים c כך שלכל f,

Log Rank Conjecture

$$D(f) \le O((\log \text{rank}(M_f))^c)$$

חסם עליון: $D(f) \le O(\sqrt{\text{rank}(M_f)} \cdot \log \text{rank}(M_f))$ (הוכח ב־2014 שחר לובט)

:Rank vs. Fooling Set

טענה: אם קיים fooling set S עבור f, אז $\text{rank}(M_f) \ge \sqrt{|S|}$.

הוכחה: יהי $S=\{(x_1,y_1),\dots(x_s,y_s)\}$ fooling set בעל ערך 1. (למשל).

$$A: \begin{array}{c|ccc} & y_1 & \cdots & y_s \\ \hline x_1 & 1 & & \\ \vdots & & \ddots & \\ x_s & & & 1 \end{array}$$

לכל i, $A_{x_ix_i}=1$.

לכל $i\neq j$, $A_{x_iy_j}\cdot A_{x_jy_i}=0$.

נסמן $A_{x_ix_j}=A_{ij}$.

נסתכל על A^t:

$$\underset{\text{מכפלה טנזורית}}{A\otimes A^t} = \begin{pmatrix} A_{11}(A^t) & \cdots & A_{1s}(A^t) \\ \vdots & & \vdots \\ A_{s1}(A^t) & \cdots & A_{ss}(A^t) \end{pmatrix}$$

נסתכל על האיבר ה־ij בבלוק ה־ij. הוא $A_{ij}\cdot A_{ji}$ (כי A^t_{ij} זה A_{ji})

לכן I היא תת־מטריצה של $A\otimes A^t$.

$$\text{rank}(M_f)\cdot\text{rank}(M_f) = \text{rank}(A)\cdot\text{rank}(A^t) \ge \text{rank}(I) = |S| = s$$

$$\Downarrow$$

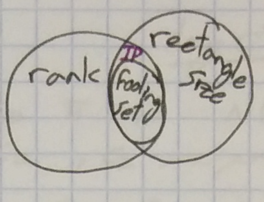
$$\text{rank}(M_f) \ge \sqrt{s}$$

ראינו של IP

$$\text{rank}_{GF_2}(M_{IP}) \le n$$

לכן אין fooling set בגודל $\omega(n^2)$.

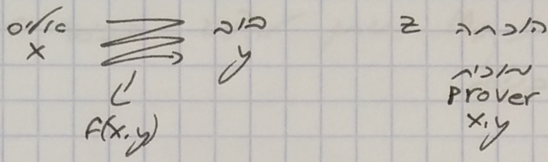
השוואת שיטות:



פרוטוקולים לא דטרמיניסטיים:

הגדרה: מערכת הוכחה עבור f.

רעיון: הוכחה z



אליס ובוב מוודאים נכונות. (המוכיח שולח לאליס ולבוב אותו דבר).

נכונות: לכל y,x, f(x,y)=1 אמ״מ קיים z עבורו השחקנים מוציאים 1.

סיבוכיות התקשורת של Π: התקשורת בין השחקנים. + |z|

$N(f) = \min_{\substack{\Pi \text{ לא דט׳} \\ \text{עבור } f}} \left(\text{סיבוכיות תקשורת של } f\right)$ (הסיבוכיות התקשורת של f)

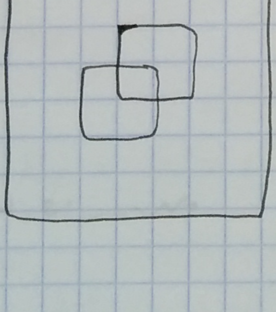
דוגמה: [redacted] disj(x,y).

[redacted]

$N(\neg disj) \leq \log n$ -ב

$N(disj) \geq \Omega(n)$

פרוטוקול לא דטרמיניסטי ״כפעולה״ על המטריצה M_f:



כיסוי / cover: מכסים את המטריצה במלבנים עם חפיפות ביניהם.

C^1 = מס׳ מינימלי של [redacted] 1-מלבנים שניתן לכסות בעזרתם את M_f (עם חפיפה). (1-מלבנים = מלבנים עם ערך 1.)

C^0 = כנ״ל עם 0-מלבנים.

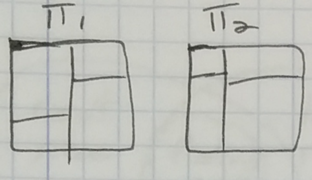
[redacted]

שקילות בין N ו-$\log C^1$:

[⇐] נניח ש- $N(f)=c$. יהי Π פרוטוקול עם אורך הוכחה c_1, ואורך תקשורת בין השחקנים c_2, $c=c_1+c_2$.

אפשר לחשוב על Π כאוסף של 2^{c_1} פרוטוקולים דטרמיניסטיים.

כל Π_i משרה חלוקה ל-2^{c_2} מלבנים f מונו'.



(or) $$f(x,y) = \bigvee_{i=1}^{2^{c_1}} \Pi_i(x,y)$$

לכן, את M_f ניתן להציג ככיסוי עם 2^c מלבנים.

[⇒] יהי $\mathcal{C}=\{R_1,\dots,R_{C^1}\}$ כיסוי של M_f ב-1-מלבנים.

מוכיח x,y בוב y אליס x

<u>פרוטוקול:</u>

מוכיח: אינדקס i של R_i כך ש-$(x,y)\in R_i$.

אליס: $x\in R_i$?

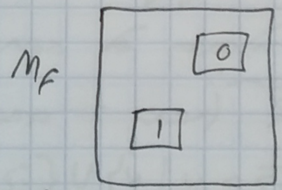
בוב: $y\in R_i$?

פלט 1 אם״ם גם וגם.

<u>סיבוכיות:</u> [illegible] $\log(C^1)+2$.

$N(f)=O(\log C^1)$, $N(\neg f)=O(\log C^0)$

משפט: $D(f)\le O(N(f)\cdot N(\neg f))$.



הוכחה:

סימ' R_0 הוא 0-מלבן
ו-R_1 הוא 1-מלבן

אז הם זרים בשורות או בעמודות (או שניהם). אחרת יש משהו בחיתוך.

יהי $\mathcal{C}_0$ כיסוי לאפסים ב-M_f ע״י C^0 מלבנים.
״ $\mathcal{C}_1$ ״ לאחדות ״ C^1 ״ .

צ.ל. $D(f)\le O(\log(C^0)\cdot\log(C^1))$.

פרוטוקול: מלבן אחדות זר בשורות או בעמודות ללפחות חצי ממלבני האפסים.

- אליס מחפשת 1-מלבן שמכיל את x וזר בשורות ללפחות חצי מה-0-מלבנים. אם היא מצליחה היא שולחת את האינדקס לבוב ($\log C^1$ ביטים).
- אם אין, בוב עושה אותו דבר ל-y ועמודות ואם יש שולח לאליס. ($\log C^1$)
אם בוב לא מוצא, התשובה 0.

(המשך בעמוד הבא)

המשך:

חוזרים על השלבים הקודמים עד שאין יותר מלבנים של 0. (כל פעם פולינומיאלי).
לכל היותר $\log(c^0)$ איטרציות, של $\log(c^1)$ ביטים, לכן $\log(c^1)\cdot\log(c^0)$.

שעור ג:

תזכורת: סיבוכיות תקשורת דטרמיניסטית:

סיבוכיות תקשורת לא דטרמיניסטית:
$\approx$ cover size
$D(f) \leq N(f)N(\neg f)$

דוגמא: k-disj: x,y קבוצות בגודל k, מתוך $\{1,\dots,n\}$.

$$k\text{-disj}(x,y)=1 \iff x\cap y=\phi$$

טענה:

סיבוכיות דטרמיניסטית: [redacted]

$$D(k\text{-disj}) \leq \log\binom{n}{k} \approx k\log\left(\frac{n}{k}\right)$$

סיבוכיות לא דטרמיניסטית:

$$N(\overline{k\text{-disj}}) \leq \log(n)$$

עד: קבוצה z כך ש- $z\subseteq x,\ z\subseteq y$.

טענה: $N(k\text{-disj}) \leq O(k+\log\log n)$

צ.ל. כיסוי ב-1-מלבנים של האחדות ב- $M_{k\text{-disj}}$.
נשתמש בשיטה ההסתברותית:
נגריל קבוצות $S_1,\dots,S_t$ (נבחר t בהמשך),

$$R_{S_i}=\{x \mid x\subseteq S_i\}\cup\{y \mid y_i\subseteq \bar{S}_i\}$$

(כל איבר נבחר לקבוצה בהסתברות $\frac{1}{2}$)

השאלה היא מה גודל t צריך להיות כדי ש-

$$\forall x,y.\ \exists S_i.\ (x,y)\in R_{S_i}$$

עבור (x,y) נתון, ההסתברות ש- $(x,y)\in R_{S_i}$ עבור i נתון היא 2^{-2k}.
ההסתברות ש- (x,y) לא יהיה מכוסה, היא לכל היותר $(1-2^{-2k})^t$.
$(1-2^{-2k})^t \leq e^{-2^{-2k}\cdot t}$. לכן:

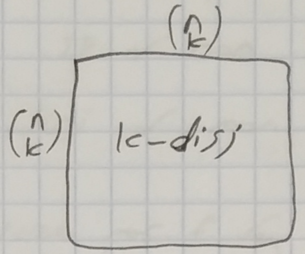
$$\underset{S_1,\dots,S_t}{P}\left(\exists (x,y)\ \text{לא מכוסה}\right) \leq \sum_{(x,y)} \underset{S_1,\dots,S_t}{P}\left((x,y)\ \text{לא מכוסה}\right) \leq \binom{n}{k}^2\cdot e^{-2^{-2k}\cdot t} \leq 1$$

מתי t? $t \geq O\left(\log\binom{n}{k}\cdot 2^{2k}\right)$.

המשך: לכן קיימות קבוצות כאלה כך שכל ה-(y,x) מכוסים.
(עדיין לא k-disj).

טענה: סיבוכיות דטרמיניסטית $\Omega(\log\binom{n}{k})$.

הוכחה: הדרגה:



נראה שהדרגה מלאה,
כלומר $\binom{n}{k}$.

באינדוקציה על (k,n):

(*) $k=0$, n כלשהו: המטריצה (1). (תמיד זר כי $x\cap y=\emptyset\cap$ [illegible] $\emptyset=\emptyset$).

(*) $n=2k$

$$\begin{array}{c|ccccc} & \bar{x} & x & \bar{x'} & x' & \cdots \\ \hline x & 1 & 0 & & & \\ \bar{x} & 0 & 1 & & 0 & \\ x' & & & 1 & & \\ \bar{x'} & 0 & & & \ddots & \\ \vdots & & & & & 1 \end{array}$$

$x\cap y=\emptyset$ אמ"מ $y=\bar{x}$.

(*) צעד: נחלק את D_k^n לפי קבוצות עם או בלי n:

$$\begin{array}{c|c|c} & Y_1 \text{ קבוצות בלי } n & Y_2 \text{ קבוצות עם } n \\ \hline X_1 \text{ קבוצות בלי } n & D_k^{n-1} & ? \\ \hline X_2 \text{ קבוצות עם } n & ? & 0 \end{array}$$

נפעיל טרנספורמציה לשורות של D_k^n, שתיתן מטריצה D', שתהיה לה דרגה מלאה. לכן גם ל-D_k^n שכן יש דרגה מלאה, $rank(D')\le ran(D_k^n)$

נרצה לקבל את D' הבא:

$$\begin{pmatrix} D_k^{n-1} & 0 \\ 0 & D_{k-1}^{n-1} \end{pmatrix}$$

נסמן ב-$\vec{x}$ את השורה המתאימה לקבוצה x ב-D_k^n
וב-$\vec{z}$ את השורה ב-D'.

עבור $x\in X_2$, יהי $x'=x\setminus\{n\}$. $\vec{z}=\frac{1}{n-2k+1}\cdot\sum_{\substack{w:|w|=k\\ x'\subseteq w\\ w\neq x}}\vec{w}-\frac{n-2k}{n-2k+1}\cdot\vec{x}$

[צריך להראות שנקבל D_{k-1}^{n-1} במקום המתאים, לא נעשה את זה עכשיו.]

נוכיח שב-$X_2\times Y_1$ יהיו מטריצת 0: לכל $y\in Y_1$,
כלומר $\vec{z}[y]=0$.

אם $x\cap y\neq\emptyset$, אז $\vec{x}[y]=0$,
וכן $\vec{w}[y]=0$ לכל w, ולכן $\vec{z}[y]=0-0=0$.

אם $x\cap y=\emptyset$, אז $\vec{x}[y]=1$. יש בדיוק $n-2k$ דרכים להשלים את x' לקבוצה w בגודל k כך ש-$w\cap y=\emptyset$.

$\vec{z}[y]=\frac{1}{n-2k+1}\cdot(n-2k)-\frac{n-2k}{n-2k+1}=0$.

סיבוכיות תקשורת אקראית:

(*) $R^{pub}(k\text{-disj}) = O(k)$

(*) קשר בין ד"ג אקראיות.

(*) משפט ניומן, על הקשר בין אקראיות פרטית ופומבית.

(*) שיטת discrepancy: נראה חסם ל- IP. בתרגיל בית נראה שלא טוב ל- disj.

(*) שיטת corruption: חסם ל- disj.

סימונים: $R(f)$ = סיבוכיות של f עם שגיאה $\frac{1}{3}$ ואקראיות פרטית.
(עד שגיאה $\frac{1}{3}$ לכל קלט).

$R_\varepsilon(f)$ = שגיאה ε, אקראיות פרטית.

$R^{pub}_\bullet$, R^{pub}_ε - כנ"ל עם אקראיות פומבית.

$R^{pub}(k\text{-disj})$: נפרש את האקראיות כסדרה של [illegible] פוטנציאליות, $S_1, S_2, \ldots$.
(כל איבר ב-S_i בהסתברות $\frac{1}{2}$).
לא משתמשים שוב בקבוצה (עד) שכבר השתמשו בה.

- אליס שולחת את האינדקס i ה__הבא__ הקטן ביותר כך ש- $S_i \subseteq x$.
- בוב מבצע $y \leftarrow S_i \cap y$.
- בוב: באופן סימטרי.
- אם $x=\phi$ או $y=\phi$, עוצרים ומודיעים שאין חיתוך.
- אם כבר שלחנו ck ביטים, אז עצרנו, עוצרים ומודיעים שיש חיתוך.
(צריך לבחור c).

אם $\overset{\text{המקורי}}{x=\phi}$ או $y=\phi$, בהכרח אין חיתוך.

זה פרוטוקול עם שגיאה חד צדדית.

ניתוח: (הניתוח בנפנוף ידיים, ההוכחה המלאה במאמר של Håstad-Wigderson 07')

נניח ש- $s=|x|$, ברגע מסוים. קבוצה S מכסה את x בהסתברות 2^{-s},
לכן $E[i] = 2^{s}$. [illegible] לפי Jensen:

$$E[\log(i)] \le \log E[i] = s$$

S_i ב"ת ב-y כשאליס שולחת את i, ולכן $E[|S_i \cap y|] = \frac{|y|}{2}$
כנ"ל עבור x.

log k צעדים, ובצעד ה-i הקבוצות הן בגודל $\approx \frac{k}{2^i}$.
תוחלת המחיר: $k + \frac{k}{2} + \ldots + 1 = O(k)$.

פרוטוקול דט' מול אקראי: $R(f)\ge\Omega(\log(D(f)))$.

הוכחה (בערך):

בהינתן פרוטוקול $\overset{\text{אקראי}}{\Pi}$ עם סיבוכיות c, יש 2^c תמלילים.

איך נחשב לתמליל t את $P(\Pi(x,y)=t)$?

טענה: ניתן לכתוב $P(\Pi(x,y)=t)=q^A(x,t)\cdot q^B(y,t)$.

נבנה פרוטוקול דט' Π':

(*) אליס שולחת קירוב של $q^A(x,t)$ לכל $t\in\{0,1\}^c$. (כי $q^A(x,t)$ מספר ממשי).

(*) בוב מחשב את $q^B(y,t)$, ואז יודע קירוב של $P(\Pi(x,y)=t)$ לכל t.

(*) בוב מקבל אותה $P(\Pi(x,y)=t)\ge 1-\varepsilon$.

הוכחה לטענה: באינדוקציה על אורך התמליל:

בסיס: לפני שנאמרו כלום, מתקיים.

צעד: נניח ש- $P(\overbrace{\Pi(x,y)^r}^{\text{רישא באורך r}}=t)=q^A(x,t)\cdot q^B(y,t)$.

נניח שאליס מדברת אחרי ש-t נאמר.

נתבונן ב $t\sigma=t'$.

$$P(\Pi(x,y)^{r+1}=t\sigma)=P(\Pi(x,y)^r=t)\cdot P\left(\begin{smallmatrix}\text{אליס אומרת } \sigma\\ \text{אחרי } t \text{ על } x\end{smallmatrix}\right)$$

נגדיר $q'^A(x,t)=q^A(x,t)\cdot P\left(\begin{smallmatrix}\text{אליס}\\ \text{אומרת}\\ \sigma\\ \text{אחרי } t\\ \text{על } x\end{smallmatrix}\right)$, $q'^B(y,t)=q^B(y,t)$.

אז $P(\Pi(x,y)^{r+1}=t\sigma)=q'^A(x,t)\cdot q'^B(y,t)$.

משפט ניומן: לכל f,ε,δ, $R_{\varepsilon+\delta}(f)\le R^{pub}_{\varepsilon}(f)+O(\log n+\log\frac{1}{\varepsilon})$.

הוכחה: קיימים $r_1,\dots,r_t$ כך שלפרוטוקול הבא שגיאה $\le\delta+\varepsilon$:

- אליס מגרילה $i\in\{1,\dots,t\}$ ושולחת את i.
- השחקנים מריצים את הפרוטוקול המקורי Π עם אקראיות r_i.

נראה שקיימים $r_1,\dots,r_t$: (השיטה ההסתברותית).

נגריל את $r_1,\dots,r_t$ באופן ב"ת מההתפלגות שלהם לפי Π.

- עבור כל (x,y), יהי $Z(x,y,r)$ אינדיקטור למאורע $\Pi(x,y,r)\ne f(x,y)$.

$E_r[Z(x,y,r)]\le\varepsilon$.

המשך: מאורע ״רע״:

$$P_{r_1,\dots,r_t}\left(E_i[z(x,y,r_i)] > \varepsilon+\delta\right) =$$

$$= P_{r_1,\dots,r_t}\left(\frac{1}{t}\sum_{i=1}^{t} z(x,y,r_i) - \varepsilon > \delta\right) \leq 2e^{-2\delta^2 \cdot t} \underset{\text{רוצים}}{<} 2^{-2n}$$

נבחר $t \approx \frac{n}{\delta^2}$.

$$P_{r_1,\dots,r_t}\left(\exists (x,y).\ E_i[z(x,y,r_i)] > \varepsilon+\delta\right) \leq 2^{2n} \cdot 2e^{-2\delta^2 \cdot O(\frac{n}{\delta^2})} < 1$$

לסיכום: מחיר אקראיות פומבית $\geq O(\log n)$.

זה הדוק, כי יש $D(eq)=\Theta(n)$, $R^{pub}(eq)=O(1)$, $\underbrace{R(eq)=O(\log n)}$

לא הראינו חסם תחתון, עכשיו נוכיח-

$R(eq)=\Theta(\log n)$

עקרון המינימקס של יאו:

הרעיון: $\max_{\mu}$ (סיבוכיות של פרוטוקול דט' שצודק בהסתברות $1-\varepsilon$ על $\mu \sim (x,y)$) = סיבוכיות של אלג' אקראי שצודק בהסתברות טובה (לכל קלט)

פורמלית: distributional complexity:

$$D^{\mu}_{\varepsilon}(f) = \min_{\substack{\pi \text{ שצודק} \\ \text{בהסתברות } \geq 1-\varepsilon \\ \text{על } \mu \sim (x,y), \\ \pi \text{ דטרמיניסטי.}}} |\pi|$$

(מסמנים גם את זה ב-D...)

טענה: $R^{pub}_{\varepsilon}(f) = \max_{\mu} D^{\mu}_{\varepsilon}(f)$.

(*) כיוון ראשון: $\geq$. בהינתן π אקראי עם שגיאה $\leq \varepsilon$,

$$\forall (x,y).\ P[\pi(x,y,r) \neq f(x,y)] \leq \varepsilon$$

$$\sum_{(x,y)} \mu(x,y) \cdot \left(\sum_r P(r) \cdot z(x,y,r)\right) \leq \varepsilon$$

$$\sum_r P(r) \cdot P_{(x,y)\sim\mu}\left(\pi(x,y,r) \neq f(x,y)\right) \leq \varepsilon$$

לכן קיים r כך ש- $P_{(x,y)\sim\mu}\left(\pi(x,y,r) \neq f(x,y)\right) \leq \varepsilon$. ($r$ תלוי ב-μ).

(*) כיוון שני: נובע ממשפט minimax למשחקים עם סכום 0. (לא נוכיח).

שיעור 4:

סיבוכיות תקשורת אקראית:

תזכורת: (*) ראינו $R(f)=\Omega(\log D(f))$

כפרט - $R(eq)=\Theta(\log n)$

(*) עקרון המינימקס של יאו: $R_{\varepsilon}(f) \geq D^{\mu}_{\varepsilon}(f)$.

שיטת Descrepancy: מסתכלים על פרוטוקולים דטרמיניסטיים, וקלט אקראי, כדי לקבל חסם על פרוטוקולים אקראיים.

עבור מלבן $R \subseteq X \times Y$, נגדיר

$$\underset{\mu}{Disc}(R,f)=\left|\underset{x\sim\mu}{P}(x\in R \cap f(x)=1)-\underset{y\sim\mu}{P}(x\in R\cap f(x)=0)\right|$$ (בערך מוחלט).

$$\underset{\mu}{Disc}(f)=\max_R \underset{\mu}{Disc}(R,f)$$

משפט: $$D^{\mu}_{\frac{1}{2}-\varepsilon}(f) \geq \log\left(\frac{2\varepsilon}{\underset{\mu}{Disc}(f)}\right)$$

הוכחה: יהי Π פרוטוקול דטרמיניסטי עבור f עם שגיאה $\leq \frac{1}{2}-\varepsilon$, על μ.
תהי c סיבוכיות התקשורת של Π.

$$\underset{(x,y)\sim\mu}{P}(\Pi(x,y)=f(x,y)) \geq \frac{1}{2}+\varepsilon$$
$$\underset{(x,y)\sim\mu}{P}(\Pi(x,y)\neq f(x,y)) \leq \frac{1}{2}-\varepsilon$$
$$\Downarrow$$
$$\circledast = \underset{\mu}{P}(\Pi(x,y)=f(x,y)) - P(\Pi(x,y)\neq f(x,y)) \geq 2\varepsilon$$

$$\circledast = \underset{\substack{t\\(\text{עלים})}}{\sum}\left|\underset{(x,y)\sim\mu}{P}(\Pi=f \wedge R_t) - \underset{(x,y)\sim\mu}{P}(\Pi\neq f\wedge R_t)\right| \leq$$

$$\leq \sum_t \left|\underset{(x,y)\sim\mu}{P}(f(x,y)=0 \wedge (x,y)\in R_t) - \underset{(x,y)\sim\mu}{P}(f(x,y)=1 \wedge (x,y)\in R_t)\right| \leq$$

$$\leq \sum_t \underset{\mu}{Disc}(R_t,f) \leq$$

$$\leq 2^c \cdot \underset{\mu}{Disc}(f)$$ (c = מספר המלבנים.)

$$\Downarrow$$

$$\underset{\mu}{Disc}(f)\cdot 2^c \geq 2\varepsilon$$
$$c \geq \log\left(\frac{2\varepsilon}{\underset{\mu}{Disc}(f)}\right)$$

דוגמא: IP: $IP(x,y) = \langle x,y\rangle \bmod 2$.

נראה ש- $\underset{U}{Disc}(IP) \le 2^{-\frac{n}{2}}$, כאשר U התפלגות האחידה.

נשתמש בהגדרה $IP(x,y) = (-1)^{\langle x,y\rangle \bmod 2}$ (לשם נוחות).

יהי $S\times T$ מלבן.

$$\underset{U}{Disc}(S\times T, IP) = \frac{1}{2^{2n}} \cdot \left|\sum_{\substack{x\in S\\ y\in T}} IP(x,y)\right| =$$

זה שקול להגדרה, כי $IP(x,y)$
הוא 1 אם 1-
ו -1 אם 1.

$$= \frac{1_S^t \cdot IP \cdot 1_T}{2^{2n}} = \textcircled{*}$$

כאשר 1_P הוא
מטריצה שיש בה
1 ב- $i\in P$
0 ב- $i\notin P$
לכל שורה i.

נשתמש בעובדות הבאות:

(*) נורמה של מטריצה: $\|A\| = \max_{v:\|v\|_2=1} \|Av\|_2$

(*) $\|A\| = \max\{\sqrt{\lambda} \mid \lambda \text{ ערך עצמי של } AA^t\}$

(*) $vAw \le \|v\|_2 \|A\|_2 \|w\|_2$ למטריצה A וקטורים v,w.

נגיע להוכחה עצמה:

$$\|1_S^t\|_2 = \sqrt{|S|}, \quad \|1_T\| \le \sqrt{|T|}$$

(המטריצה) $(IP\cdot IP^t)_{x,y} = \sum_z \langle x, z\rangle \cdot \langle z,y\rangle$

$$IP\cdot IP^t = 2^n\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1\end{pmatrix} = 2^n \cdot I$$

$$\Downarrow$$

$$\|IP\| = 2^{\frac{n}{2}}$$

$$\textcircled{*} \le 2^{\frac{n}{2}} \cdot 2^{\frac{n}{2}} \cdot 2^{\frac{n}{2}} \cdot \frac{1}{2^{2n}} = 2^{-\frac{n}{2}}$$

ראינו בתרגיל בית ש- $\underset{\mu}{Disc}(disj) \approx \frac{1}{n}$ לכל μ.

ראינו היום ש- $\Omega(\sqrt{n})$, אפשר להראות $\Omega(n)$, אבל יותר מסובך.

Corruption: (1-sided discrepancy).

μ התפלגות מעל $X\times Y$. α,ρ פרמטרים, ε שגיאה של הפרוטוקול.

נניח שלכל מלבן R עם $\mu(R)>\rho$ מתקיים:

$$\mu(R\cap f^{-1}(1)) > \alpha\cdot\mu(R\cap f^{-1}(0)),$$

אזי $R_\varepsilon(f)\ge\log\left(\frac{1}{\rho}\cdot\mu(f^{-1}(0))-\frac{\varepsilon}{\mu}\right)$.

הערה: לפעמים קוראים corruption לשיטה הזאת.

הוכחה: יהי Π פרוטוקול c' עם שגיאה $\le\varepsilon$ מעל μ.

נתבונן במלבנים $R_1,\dots,R_t$ שמושרים ע"י Π כך ש-

(*) הפלט הוא 0.

(*) $\mu(R_i)>\rho_t$.

$$P(\Pi=0 \wedge f=1) \ge \mu\left(\bigcup_{i=1}^{t} R_i\cap f^{-1}(1)\right) =$$

$$=\sum_{i=1}^{t}\mu(R_i\cap f^{-1}(1)) \ge$$

$$\ge\sum_{i=1}^{t}\alpha\cdot\mu(R_i\cap f^{-1}(0))$$

$$\sum_{i=1}^{t}\mu(R_i\cap f^{-1}(0)) \le \frac{1}{\alpha}\cdot P(\text{0 במקום 1})$$

$$\mu(f^{-1}(0)) = \sum_{i=1}^{t}\mu(R_i\cap f^{-1}(0)) + \overbrace{\rho\cdot 2^c}^{\text{"מלבנים קטנים"}} + P(\text{1 במקום 0}) \le$$

$$\le\sum_{i=1}^{t}\mu(R_i\cap f^{-1}(0)) + \rho\cdot 2^c + \frac{1}{\alpha}\cdot P(\text{1 במקום 0}) \le$$

$$\le\frac{1}{\alpha}P(\text{0 במקום 1}) + \rho\cdot 2^c + \frac{1}{\alpha}\cdot P(\text{1 במקום 0}) \le$$

$$\le \rho\cdot 2^c + \frac{\varepsilon}{\alpha}$$

$$\overset{\Downarrow}{c} \ge \log\left(\frac{1}{\rho}\cdot\left(\mu(f^{-1}(0)) - \frac{\varepsilon}{\alpha}\right)\right)$$

תזכורת: disj תחת התפלגות מכפלה.

אינטואיציה: לכל i, $i\in X$, $i\in Y$ באופן בלתי תלוי בהסתברות p.

$$E[|X\cap Y|]=\sum_{i=1}^{n}p^2=n\cdot p^2$$

עבור $p\approx\frac{1}{\sqrt{n}}$, ונקבל $|X|\approx|Y|\approx\frac{1}{\sqrt{n}}$.

מסיבות טכניות לא נעבוד עם ההתפלגות הזאת.

נגדיר התפלגות μ: אחידה מעל X,Y כך ש- $|X|=|Y|=\sqrt{n}$.

אז מתקיים-

$$P(X\cap Y=0)\approx\frac{1}{e}$$

קירוב סטירלינג- $n!\approx\sqrt{2\pi n}\cdot\left(\frac{n}{e}\right)^n$

צריך לעשות קירובים עם מקדמים בינומיים, אנחנו לא עושים את זה.

רוצים להוכיח שקיים קבוע c כך שעבור n גדול דיו (ו-α קטן מספיק) אם R מקיים

$$\underset{(x,y)\sim\mu}{P}\left(disj(x,y)=0\mid(x,y)\in R\right)\le\alpha$$

אז או ש- $|S|\le 2^{-c\sqrt{n}}\cdot\binom{n}{\sqrt{n}}$ או $|T|\le 2^{-c\sqrt{n}}\cdot\binom{n}{\sqrt{n}}$.

אם S וגם T "קטנים": נניח בה"כ $|S|<|T|$. אז:

$$\mu(S\times T)=\sum_{(s,t)\in S\times T}\mu(s,t)=\underbrace{\mu(S)}_{\le1}\cdot\mu(T)\le\mu(T)\le\frac{1}{\binom{n}{\sqrt{n}}}\cdot|T|\le$$

$$\le 2^{-c\sqrt{n}}\cdot\binom{n}{\sqrt{n}}\cdot\frac{1}{\binom{n}{\sqrt{n}}}=2^{-c\sqrt{n}}$$

בניית ה- hard core: נניח ש- $|S|\ge 2^{-c\sqrt{n}}\cdot\binom{n}{\sqrt{n}}$ (אחרת סיימנו).

$S':=\{x\in S$ | x נחתך עם לכל היותר 2α מהאיברים/קבוצ' ב-$T\}$

לפי מרקוב: $|S'|\ge\frac{|S|}{2}$

טענה: קיימת קבוצה $S''\subseteq S'$,

$S''=\{x_1,\dots,x_{\frac{\sqrt{n}}{3}}\}$, כך שלכל $i<\frac{\sqrt{n}}{3}$,

$$\left|x_{i+1}\cap\left(\bigcup_{j\le i}x_i\right)\right|<\frac{\sqrt{n}}{2}.$$

בניית S'' באינדוקציה על i: נניח שבחרנו $x_1,\dots,x_i$ עבור $i<\frac{\sqrt{n}}{3}$,

אז $\bigcup_{i<j}x_j<\frac{n}{3}$. כמה קבוצות "רעות" יש? (שאי אפשר לבחור).

$$\sum_{l=\frac{\sqrt{n}}{2}}^{\sqrt{n}}\binom{\frac{n}{3}}{l}\cdot\binom{\frac{2n}{3}}{\sqrt{n}-l}\underset{\text{סטירלינג.}}{\le}\underset{(c'<c\text{ קבוע, }c')}{2^{-c'\sqrt{n}-1}}\cdot\binom{n}{\sqrt{n}}$$

$\Leftarrow$ ב-S' יש קבוצה טובה, אותה נבחר.

המשך דוגמה: נחסום את $|T|$: נגדיר -

$$T'=\{y\in T \mid y \text{ נחתך עם לכל היותר } 4\alpha \text{ מהקבוצות ב-}S\}$$

$|T'|\ge\frac{|T|}{2}$.

נבחין ש- $\left|\bigcup_{i=1}^{\frac{\sqrt{n}}{3}} x_i\right| \ge \frac{\sqrt{n}}{2}\cdot\frac{\sqrt{n}}{3}=\frac{n}{6}$.

לכל $y\in T'$: יש $\le 4\alpha\cdot\frac{\sqrt{n}}{3}$ קבוצות ב-S אותן y חותך,

לכן יש $(1-4\alpha)\cdot\frac{\sqrt{n}}{3}$ קבוצות שלא חותך אותן, נסמן $x_{i_1},\dots,x_{i_{(1-4\alpha)\frac{\sqrt{n}}{3}}}$.

$$\left|\{1,\dots,n\}\setminus\bigcup_{j=1}^{(1-4\alpha)\cdot\frac{\sqrt{n}}{3}} x_j\right| \le n-(1-4\alpha)\cdot\frac{\sqrt{n}}{3}\cdot\frac{\sqrt{n}}{2} < \frac{8}{9}n$$

עבור $\alpha<\frac{1}{100}$.

$$|T'|\le \underbrace{\binom{\frac{\sqrt{n}}{3}}{4\alpha\cdot\frac{\sqrt{n}}{3}}}_{\text{בחירת קבוצות שאותן אינו חותך } y}\cdot\binom{\frac{8}{9}n}{\sqrt{n}} \le \dots < 2^{-c''\cdot\sqrt{n}-1}\cdot\binom{n}{\sqrt{n}}$$

סטירלינג ועוד. עבור c'' שבחרנו מתאים.

$$\Downarrow$$

$|T|<2^{-c\cdot\sqrt{n}}\cdot\binom{n}{\sqrt{n}}$.

הבעיה: עם התפלגות מכפלה: $\mu(x,y)=\mu_1(x)\cdot\mu_2(y)$.

טענה: $D^{\mu}_{\frac{1}{3}}(disj)=O(\sqrt{n}\cdot\log n)$ כש-μ מכפלה.

כלומר, אי אפשר לקבל חסם טוב עם מכפלה.

שימוש - Streaming Alg.:

$s_i\in\{1,\dots,n\}$

קלט - $s=s_1s_2\dots s_m$ stream, מאוד ארוך, כך שאי אפשר לשמור את כולו בזכרון. האלגו' עובר על ה-stream לפי הסדר, כשבכל רגע הוא רואה רק חלק וצריך לשמור פחות, וצריך לחשב משהו.

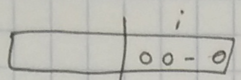
דוגמאות מעניינות - frequency moments: f_i = מספר הפעמים ש-i הופיע ב-S.

$$F_k=\sum_{i=1}^{n}(f_i)^k \quad , \quad F_\infty=\max_i f_i$$

F_0 = מספר האיברים השונים.

$F_1=m$.

המשך:



אלגוריתם ל-F_0: אם ב-S היו r איברים שונים,

נצפה לראות $\frac{r}{2^i}$ פעמים ערך שמסתיים ב-0^i.

משתמשים ב-hash ובסופו. לא נכנס לפרטים.

$\log n$ מקום.

חסם תחתון על המקום הנדרש לקירוב F_0:

נגדיר:

$$GEq = \begin{cases} x=y \Rightarrow 1 \\ \Delta(x,y) \geq \frac{n}{100} \Rightarrow 0 \end{cases} \quad (gap-eq)$$

$$|X| = |Y| = \frac{n}{50}$$

(x,y קבוצות בנות $\frac{n}{50}$ איברים.)

אפשר להראות:

$D = \Omega(n)$.

$R = \Omega(\log n)$.

רדוקציה מ-GEq ל-F_0: בהינתן X,Y, נבנה stream: $S = XY$,

כלומר, האיברים של אליס, ואז של בוב.

אם $x=y$, אז $F_0(S) = \frac{n}{50}$.

אם $\Delta(x,y) \geq \frac{n}{100}$, אז $F_0(S) \geq \frac{3n}{100}$.

נניח שנתון אלג' F_0 עם מקום $< B$, ושגיאה $\frac{1}{1000}$.

אז $\Omega(\log n) \leq R(GEq) \leq B$.

לכן צריך $\Omega(\log n)$ מקום.