tail inequalities

א"ש מרקוב : Markov

אם $X \geq 0$, אז

$$pr(X \geq A) \leq \frac{E(X)}{A}$$

הוכחה

$$E(X) = \sum_k pr(X=k)\cdot k$$

$$\geq A \cdot pr(X \geq A)$$

ע"י השמטת חיוביים.

א"ש צ'בישב Chebychev

עבור X ממ"מ , $\mu = E(X)$

$$pr(|X-\mu| \geq A) \leq \frac{Var(X)}{A^2}$$

הוכחה

$$pr(|X-\mu| \geq A) = pr(|X-\mu|^2 \geq A^2) \underset{\text{מרקוב}}{\leq} \frac{E(|X-\mu|^2)}{A^2} = \frac{Var(X)}{A^2}$$

דוגמה: $X_1, \ldots, X_n$ ממ"מ בלתי תלויים , (מקבלים ערכים $\{0,1\}$)

נניח $pr(X_i = 1) = p = \frac{1}{2}$. $X = \sum_{i=1}^{n} X_i$

לפי:

$$pr\left(X \geq \tfrac{2}{3}n\right) \leq \frac{E(X)}{\frac{2}{3}n} = \frac{\frac{n}{2}}{\frac{2}{3}n} = \boxed{\frac{3}{4}}$$

לעומת: אם

	X_1		X_n
$\frac{1}{2}$:	0	...	0
$\frac{1}{2}$	1	...	1

אז $pr(X=n) = \frac{1}{2}$

אם נגדיר נניח $X_1 \dots X_n$ ב״ת <u>בזוגות</u>

אז $\mathrm{Var}(X) = \sum_{i=1}^{n} \mathrm{Var}(X_i) = n \cdot p(1-p) = \frac{n}{4}$

ב״ת

ולכן: $\Pr\left(X \geq \frac{2}{3}n\right) \leq \Pr\left(|X - E(X)| \geq \frac{n}{6}\right) \leq \frac{\mathrm{Var}(X)}{\left(\frac{n}{6}\right)^2} = \frac{\frac{n}{4}}{\frac{n^2}{36}} = \boxed{\frac{9}{n}}$

<u>תכונות</u>:

1. $\mathrm{Var}(X) \overset{def}{=} E\left((X - E(X))^2\right) = E(X^2) - (E(X))^2$

2. אם X מציין, $\Pr(X=1)$, אז $\mathrm{Var}(X) = p(1-p)$

3. אם $X_1 \sim X_n$ ב״ת <u>בזוגות</u> אז $\mathrm{Var}\left(\sum X_i\right) = \sum \mathrm{Var}(X_i)$

~~<u>הכללה</u>: יהיו $X_1 \dots X_n$ ב״ת בהינתן k-wise, k <u>זוגי</u>~~

~~נסמן $X = \sum_{i=1}^{n} X_i$, $\mu = E(X)$~~

~~הוכחנו $\Pr(|X - \mu| \geq A) \leq \frac{E(|X-\mu|^k)}{A^k} \leq \left(k n\right)^{k/2} \cdot \frac{1}{A^k}$~~

~~עבור $k=4$ $\leq \frac{3n^2}{A^4}$~~

מה קורה כשיש לנו אי-תלות מותנית ?

$Pr(X_i=1)=p_i$ $\qquad$ $X_1,\dots,X_n$ מ"מ-פואסוניים ב-$\{0,1\}$

$X_1 \dots X_n$ ב"ת שמקיים: $\quad X=\sum_{i=1}^n X_i, \quad \mu=E(X)=\sum p_i$.

טענה:

$$Pr(X<(1-\delta)\mu) \le \left(\frac{e^{-\delta}}{(1-\delta)^{1-\delta}}\right)^{\mu} \le e^{-\mu\delta^2/2}$$

(מה שצריך.) $\qquad$ נובע מ- $(1-\delta)^{1-\delta} > e^{-\delta+\delta^2/2}$

הוכחה:

$$Pr(X<(1-\delta)\mu) \underset{t>0\ \text{נבחר אותו יותר}}{=} Pr\left(e^{-tX} > e^{-t(1-\delta)\mu}\right) \underset{\text{מרקוב}}{\le} \frac{E(e^{-tX})}{e^{-t(1-\delta)\mu}}$$

$$E(e^{-tX}) = E(e^{-t\sum X_i}) = E\left(\prod_{i=1}^n e^{-tX_i}\right) \underset{\text{בגלל אי-תלות}}{=} \prod_{i=1}^n E(e^{-tX_i}) = \prod_{i=1}^n \left(p_i e^{-t}+1-p_i\right)$$

$$= \prod_{i=1}^n \left(1-p_i(1-e^{-t})\right) \underset{1-x<e^{-x}}{<} \prod_{i=1}^n e^{p_i(e^{-t}-1)} = e^{(e^{-t}-1)\sum p_i} = e^{(e^{-t}-1)\mu}$$

ולכן:

$$Pr(X<(1-\delta)\mu) \le \frac{e^{(e^{-t}-1)\mu}}{e^{-t(1-\delta)\mu}} = e^{\mu\left[e^{-t}-1+t(1-\delta)\right]}$$

$t=\ln\frac{1}{1-\delta}$ $\qquad$ רוצים הכי קטן אפשר, ומסתבר שצריך לבחור

$$\le e^{\mu\left[\cancel{1}-\delta-\cancel{1}+(1-\delta)\ln\left(\frac{1}{1-\delta}\right)\right]} = \left[\frac{e^{-\delta}}{1-\delta}\right]^{\mu}$$

וכך מקבלים

$e^{-t}=(1-\delta)$ $\qquad$ $e^{\ln\frac{1}{1-\delta}} = \frac{1}{1-\delta}$

$$\Pr\left(X > (1+\delta)\mu\right) < \left(\frac{e^{\delta}}{(1+\delta)^{1+\delta}}\right)^{\mu}$$ גרסה 1:

גרסה 2: אם $\delta \geq 2e-1$ אז $1+\delta \geq 2e$

$e = 2.7\ldots$

$$\Pr\left(X > (1+\delta)\mu\right) \leq 2^{-\delta\mu}$$

~~proof~~

$$\Pr\left(X \geq (1+\delta)\mu\right) < e^{-\mu\frac{\delta^2}{4}}$$ גרסה 3: אם $\delta < 2e-1$

$$\Pr\left(|X-\mu| \geq \delta\mu\right) \leq e^{-\mu\frac{\delta^2}{4}}$$ ומכאן

טענה: יהיו $X_1 \dots X_n$ מ"מ $0 \le X_i \le 1$

k-wise ind לכל k זוגי:

$$X = \sum_{i=1}^{n} X_i \qquad \mu = E(X), \qquad \mu_i = E(X_i)$$

$$\Pr\left[\left|\sum_{i=1}^{n} X_i - \mu\right| \ge \varepsilon\mu\right] \le \left(\frac{k^2}{4\varepsilon^2} \cdot \frac{n}{\mu^2}\right)^{k/2}$$

הוכחה:
$$\Pr\left[\left|\sum_{i=1}^{n} X_i - \mu\right| \ge A\right] = \Pr\left(\left(\sum_{i=1}^{n} X_i - \mu\right)^k \ge A^k\right) \le \frac{E\left(\left(\sum_{i=1}^{n}(X_i - \mu_i)\right)^k\right)}{A^k}$$

נסמן $Z_i = X_i - \mu_i$

$$E\left(\left(\sum_{i=1}^{n} Z_i\right)^k\right)$$
$$= \sum_{i_1 \dots i_k = 1}^{n} E\left(Z_{i_1} \cdots Z_{i_k}\right)$$

כל מכפלה $Z_{i_1} \cdots Z_{i_k}$

נראית כך: $Z_1^{m_1} \cdots Z_n^{m_n}$

כאשר $0 \le m_i$ וגם, $\sum_{i=1}^{n} m_i = k$.

- מכפלה שבה יש $m_i = 1$

$$E\left(Z_1^{m_1} \cdots Z_n^{m_n}\right) = \underbrace{E\left(Z_i^{m_i}\right)}_{0} \cdot E(\text{שאר}) = 0$$

יש לכל היותר k משתנים

ולכן הם k-wise ind

לכן במקרה הזה מופיעים לכל היותר מ $\frac{k}{2}$ $m_i > 0$

ח"כ יהיה $m_i = 1$ $\exists_{k \neq i}$

ערכים אחרים ואפס

- כל גורם שאינו, תורם לכל היותר 1.

כי $0 \le X_i \le 1$ וגם $1 \ge \mu_i \le 1$

$$X_i - \mu_i \le 1$$

$$(X_i - \mu_k)^{m_i} \le 1$$

$$E(Z_1^{m_1} \cdots Z_n^{m_n}) \le 1$$

~~לבסוף~~

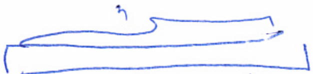
כמה גורמים שונים ≥ 1 ?

k

כל כניסה מסומנת $1 .. \frac{k}{2}$

לומר איזה מה $\frac{k}{2}$ נמסו זה

$\left(\frac{k}{2}\right)^k$ אפשרויות



n

איזה $\frac{k}{2}$ בחרנו?

$$\binom{n}{\frac{k}{2}} \le n^{k/2}$$

ובסה"כ

$$\le \frac{n^{\frac{k}{2}} \left(\frac{k}{2}\right)^k}{(\varepsilon\mu)^k} = \left[\frac{k^2 \; n}{4 \; \varepsilon^2 \mu^2}\right]^{k/2}$$

מ.ש.

The sampling problem

בעיית הדגימה

נתון קבוצה Σ (בד״כ $\Sigma=\{0,1\}^n$)

ותת-קבוצה $A \subseteq \Sigma$.

אנחנו רוצים להעריך את $P(A)=\frac{|A|}{|\Sigma|}$

עד כדי טעות אדיטיבית ε

בהסתברות הצלחה $\geq 1-\delta$

$$\Pr\left(\left| \text{התשובה שלנו} - P(A) \right| \geq \varepsilon \right) \leq \delta$$

מדדי סיבוכיות שלנו:

- מס. קריאות
- זמן ריצה.

לצורך, אנו עובדים בצורת black-box דרכו אנחנו יכולים

לשאול שאילתות $x \overset{?}{\in} A$, ואין מידע נוסף מלבד:

- מס. של קריאות — אנו משתמשים
- מס. שאילתות...

שאלה 1:

נבחר $a_1,\dots,a_T \in_R \{0,1\}^n$

נבדוק $a_i \overset{?}{\in} A$ $\quad i=1..T$

ונחזיר את אחוז הפגיעות.

נסמן $X_i=1$, אם קיבלנו כן בבדיקה ה-i, 0 אחרת...

אז לפי צ'רנוף

$$pr\left(\left|\frac{1}{T}\sum_{i=1}^{T}X_i - P(A)\right| \ge \varepsilon\right) = pr\left(\left|\frac{1}{T}\sum_{i=1}^{T}x_i - P(A)\right| \ge \frac{\varepsilon}{P(A)}\cdot P(A)\right) \le 2^{-\frac{\varepsilon^2 T}{4P(A)}} \le 2^{-\frac{\varepsilon^2 T}{4}} = \delta$$

עבור $\boxed{T=O\left(\frac{\lg\frac{1}{\delta}}{\varepsilon^2}\right)}$ ($P(A)$ קבוע)

רנדום: סה"כ ביטים: $T\cdot\lg|\Sigma| = O\left(\frac{n\cdot\lg\frac{1}{\delta}}{\varepsilon^2}\right)$

סה"כ שאילתות: $T = O\left(\frac{\lg\frac{1}{\delta}}{\varepsilon^2}\right)$

וניתן לראות שאין תלות בגודל (זה כמו קבוע) לכל משנה תלויה

אלגוריתם לא משתמש.

דוגמא 2:

נגריל $X_1 \ldots X_T$, $X_i \in \Sigma = \{0,1\}^n$ p.i. , $T \le 2^n$

נשאל $X_i \overset{?}{\in} A$ ונחזיר $\frac{1}{T}\sum_{i=1}^{T} X_i$.

$$\Pr\left(\left| \frac{1}{T}\sum X_i - P(A) \right| \ge \varepsilon \right) \le \frac{V\left(\frac{1}{T}\sum X_i\right)}{\varepsilon^2} = \frac{Var(X_1)}{\varepsilon^2 T} = \frac{P(A)(1-P(A))}{\varepsilon^2 T} \le \frac{1}{\varepsilon^2 T} = \delta$$

$$\boxed{T = \frac{1}{\varepsilon^2 \delta}}$$

מס' ביטים: $O(n + \lg T) = O\left(n + \lg \frac{1}{\varepsilon\delta}\right)$

מס' שאלות: $T = O\left(\frac{1}{\varepsilon^2 \delta}\right)$

	מס' ביטים	מס' שאלות
בלתי תלויים:	$O\left(\frac{n \cdot \lg \frac{1}{\delta}}{\varepsilon^2}\right)$	$O\left(\frac{\lg \frac{1}{\delta}}{\varepsilon^2}\right)$
p.i.	$O\left(n + \lg \frac{1}{\varepsilon\delta}\right)$	$O\left(\frac{1}{\varepsilon^2 \delta}\right)$

הערה: אם δ קבוע (נניח $\delta = \frac{1}{100}$)

בפועל מספר השאלות הוא $O\left(\frac{1}{\varepsilon^2}\right)$

אבל מס' הביטים יורד מ $O\left(\frac{n}{\varepsilon^2}\right)$ ל $O\left(n + \lg \frac{1}{\varepsilon}\right)$!

בהמשך: נראה מה זה k-wise ind.

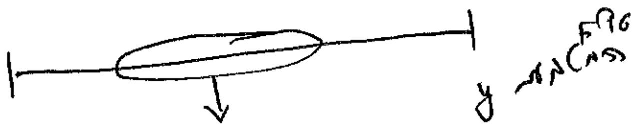
אמפליפיקציה של BPP — Deterministic amplification

נניח כי מכונת $BPP(\frac{1}{2}-\varepsilon, \frac{1}{2}+\varepsilon)$

[תזכורת: $BPP(\alpha,\beta)$. שפה L, קיים מ"ט $M(x,y)$, $|y|=poly(|x|)$ כך ש:

$$x\in L \Rightarrow Pr_y[M(x,y)=1] \geq \beta$$
$$x\notin L \Rightarrow Pr_y[M(x,y)=1] \leq \alpha$$
]

בהינתן x:



ה y כך ש $M(x,y)=1$

אם נקבע את $x\in L$ אז נרצה לדגום את $|\{y \mid M(x,y)=1\}|$ שהוא $\geq \frac{1}{2}+\varepsilon$ או $\leq \frac{1}{2}-\varepsilon$.

אז כי ניקח Sampler לדיוק ε והסתברות δ, ...

הכרה: $BPP(\frac{1}{2}-\varepsilon, \frac{1}{2}+\varepsilon) \rightarrow BPP(\delta, 1-\delta)$

עם $O(\lg\frac{1}{\delta}/\varepsilon^2)$ הגרלות ... [כי $\frac{\lg\frac{1}{\delta}}{\varepsilon^2}$ הגרלות]

או עם $O(\frac{1}{\varepsilon^2\delta})$ הגרלות ... <u>בזוגות</u>. [כי 2 הגרלות]

מדגמים ... הסתברות ... $\frac{\lg\frac{1}{\delta}}{\varepsilon^2}$ הגרלות <u>...</u> ...

הכרעה עבור שגיאה חד כיוונית!

$y \in \{0,1\}^m$ M(x,y) מכונה הסתברותית

$$x \in L \Rightarrow \Pr_y(M(x,y)=1) \ge \alpha$$

$$x \notin L \Rightarrow \Pr_y(M(x,y)=1) = 0$$

נעשה T הרצות (כנ"ל / ב"ת בלתי תלויות) ונקבל ⟺ אם יש קבל.

$x \notin L$, תמיד נדחה.

$x \in L$

$$\Pr_{\text{הכרעה}}(\text{נדחה}) \le (1-\alpha)^T \approx e^{-\alpha T} \le \delta \qquad \boxed{T = O\left(\frac{\lg\frac{1}{\delta}}{\alpha}\right)}$$

$$\Pr_{\text{הכרעה}}(\text{נדחה}) \le \Pr\left(\left|\sum_{i=1}^{T} X_i - \underset{E(X)}{\alpha T}\right| \ge \alpha T\right) \le \frac{V(X)}{(\alpha T)^2} = \frac{T\alpha(1-\alpha)}{(\alpha T)^2} \le \frac{1}{\alpha T} \le \delta \qquad \boxed{T = O\left(\frac{1}{\delta\alpha}\right)}$$

מעבר אמפליפיקציה n $(0,\frac{1}{n}) \to (0,\frac{1}{2})$

	מס' ביטים	מס' הרצות
הכרעה חד	$O(n \cdot m)$	$O(n) = T$
״ ״ כיווני	$2m = O(n^2 m)$	$T = O(n)$

למדנו!

אבל אמפליפיקציה n $(0,\frac{1}{2}) \to (0, 1-2^{-n})$

	מס' ביטים	מס' הרצות
הכרעה חד	$O(n^2 \cdot m)$	$O(n^2)$
הכרעה חד כיווני	רע $O(2^n \cdot m)$	$O(2^n)$

הכרעה חד כיווני - ממש רע.