ind k-wise

מה גודל מרחב המדגם הדרוש ל X_1,X_2,X_3 מקריים (ב״ת)

אוניפורמיים וב״ת - ביטים יחד

X	X_1	X_2	X_3
	0	0	0
	0	0	1
		⋮	
	1	1	1

$|supp(X)| = 8$

מה גודל מרחב המדגם הנדרש לאי-תלות בזוגות

X	X_1	X_2	X_3
	0	0	0
	1	1	0
	0	1	1
	1	0	1

$|supp(X)| = 4$ בזוגות

<u>הגדרה</u> $X_1 \ldots X_n$ על Σ הם בזוגות

אם לכל $1 \le i \ne j \le n$

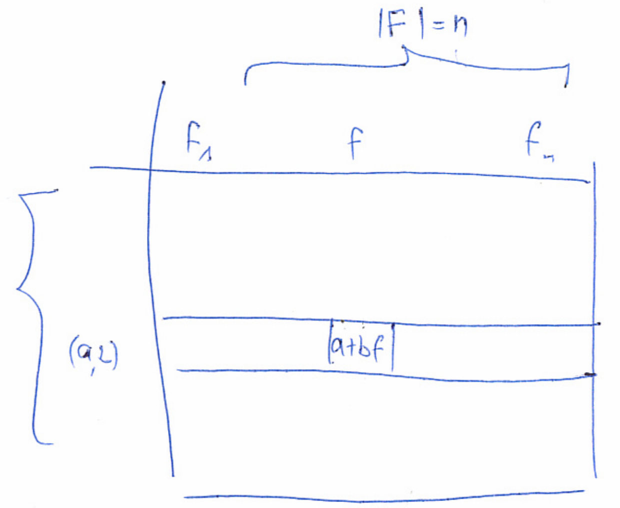
ולכל $\sigma_1, \sigma_2 \in \Sigma$

$$\Pr(X_i = \sigma_1 \wedge X_j = \sigma_2) = \frac{1}{|\Sigma|^2}$$

תזכורת: יהי n חזקה של ראשוני.

אז $\Sigma = F_n$ שדה בן n איברים.

בנייה: $X = X_1,\dots,X_n$ ב"ת בזוגות מעל $\Sigma = F_n$



$n^2 = |F|^2$

$X_f = a + bf$

נבחר $(a,b) \in F^2$

ונגדיר

טענה: $X_1,\dots,X_n$ ב"ת בזוגות.

יהי $1 \le i < j \le n$

$\alpha, \beta \in F$

$$\Pr_{a,b\in F}\left[X_i(a,b)=\alpha \wedge X_j(a,b)=\beta\right] = \Pr_{a,b\in F}\left[\underbrace{\begin{pmatrix}1 & i\\ 1 & j\end{pmatrix}}_{M}\begin{pmatrix}a\\ b\end{pmatrix} = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}\right]$$

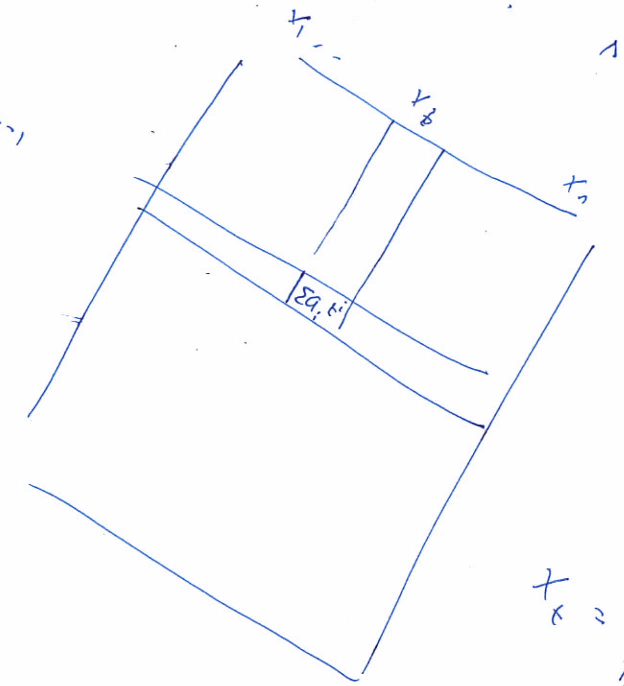
$$= \Pr_{a,b\in F}\left(M^{-1}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}a\\ b\end{pmatrix}\right) = \frac{1}{|F|^2}$$

M הפיכה כי

$\begin{vmatrix}1 & i\\ 1 & j\end{vmatrix} = j - i \neq 0$

תזכורת: $X_1,\dots,X_n$ הם k-wise ind. אם לכל $i_1 < \dots < i_k \le n$ ולכל $a_1,\dots,a_k \in \Sigma$

$\Pr(X_{i_1} = a_1 \wedge \dots \wedge X_{i_k} = a_k) = \frac{1}{|\Sigma|^k}$



בנייה: נניח $|\Sigma| \le |F|$ שדה

נבחר $\vec{a} = a_0,\dots,a_{k-1} \in F$

ונגדיר $X_i = \sum_{j=0}^{k-1} a_j i^j$

$|supp(X)| = |F|^k$

טענה: X הוא k-wise

הוכחה: יהי $i_1,\dots,i_k$ ו-$a_1,\dots,a_k$

$$\Pr(X_{i_1}=a_1 \wedge \dots \wedge X_{i_k}=a_k) = \Pr\left(\underbrace{\begin{pmatrix} f_1^0 & f_1^1 & \cdots & f_1^{k-1}\\ f_2^0 & f_2^1 & & \\ \vdots & & & \\ f_k^0 & & \cdots & f_k^{k-1}\end{pmatrix}}_{M}\begin{pmatrix}a_0\\ \vdots\\ a_{k-1}\end{pmatrix} = \begin{pmatrix}a_1\\ \vdots\\ a_k\end{pmatrix}\right) = \frac{1}{|\Sigma|^k}$$

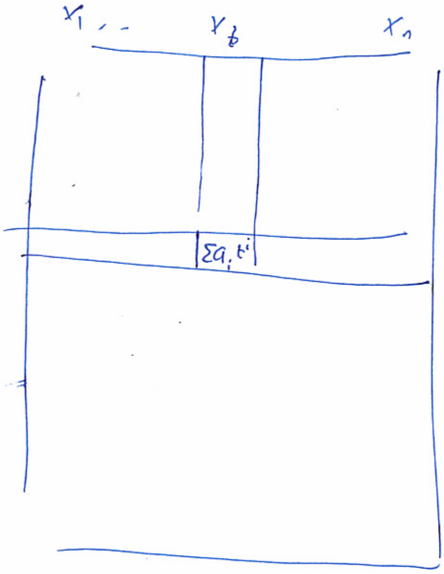
הגדרה: k-wise ind

$X_1, \dots, X_n$ על Σ הם k-wise ind אם

לכל $1 \le i_1 < i_2 < \dots < i_k \le n$

ולכל $\sigma_1, \dots, \sigma_k \in \Sigma$

$$\Pr(X_{i_1} = \sigma_1 \wedge \dots \wedge X_{i_k} = \sigma_k) = \frac{1}{|\Sigma|^k}$$



בנייה: נקח שדה $F \geq |\Sigma|$ איברים.

נבחר את מרחב ההסתברות:

נבחר $\bar{a} = a_0, \dots, a_{k-1} \in F$

בהינתן $\bar{a}$ נגדיר

$$X_t = \sum_{i=0}^{k-1} a_i t^i$$

$$|supp(X)| = |F|^k$$

טענה: הם ב"ת k-wise.

הוכחה: לכל $i_1, \dots, i_k$, $\sigma_1, \dots, \sigma_k$

$$\Pr(X_1 = \sigma_1 \wedge \dots \wedge X_k = \sigma_k) = \Pr_{\bar{a}}\left(\underbrace{\begin{pmatrix} f_{i_1}^0 & f_{i_1}^1 & \dots & f_{i_1}^{k-1} \\ f_{i_2}^0 & f_{i_2}^1 & & f_{i_2}^{k-1} \\ & & \vdots & \\ f_{i_k}^0 & & & f_{i_k}^{k-1} \end{pmatrix}}_{M} \begin{pmatrix} a_0 \\ \vdots \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} \sigma_1 \\ \vdots \\ \sigma_k \end{pmatrix} \right)$$

M הפיכה כי

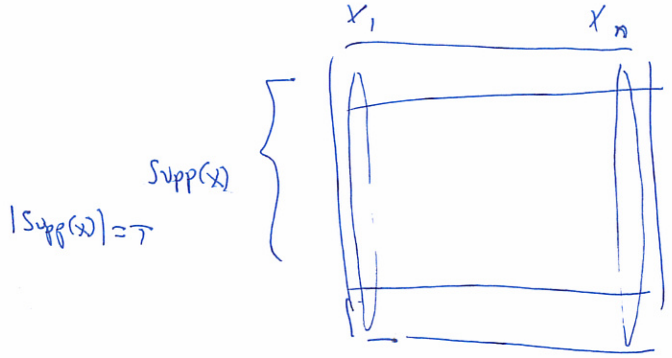
$$\det(M) = \prod_{1 \le j_1 < j_2 \le k} (f_{i_{j_1}} - f_{i_{j_2}}) \ne 0$$

$$= \Pr_{\bar{a}}\left(M^{-1} \begin{pmatrix} \sigma_1 \\ \vdots \\ \sigma_k \end{pmatrix} = \begin{pmatrix} a_0 \\ \vdots \\ a_{k-1} \end{pmatrix} \right) = \frac{1}{|\Sigma|^k}$$

טענה: אם $X = X_1 \dots X_n$ מפולגים על $\{0,1\}$ ובת"ז זוגית

אז $|supp(X)| \geq n$

הוכחה: תהי X מפולג על $\{0,1\}^n$, בת"ז זוגית עם תומך מינימלי.



נסמן $T = |supp(X)|$

$Supp(X) = \{ w^{(1)}, \dots, w^{(T)} \}$

$w^{(\ell)} \in \{0,1\}^n$.

$\Pr_{x \in X} (x = w^{(\ell)}) = p_\ell$

בה"כ נניח שאנחנו מפולגים על $\{1,-1\}^n$.

נגדיר וקטורים $V_1, \dots, V_n \in \mathbb{R}^T$

$$V_1 = \left(\sqrt{p_1}\, w^{(1)}_1, \dots, \sqrt{p_\ell} \cdot w^{(\ell)}_1, \dots, \sqrt{p_T}\, w^{(T)}_1 \right)$$

$$V_2 = \left(\sqrt{p_1}\, w^{(1)}_2, \dots, \sqrt{p_\ell}\, w^{(\ell)}_2, \dots, \sqrt{p_T}\, w^{(T)}_2 \right)$$

$$\vdots$$

$$V_n = \left(\sqrt{p_1}\, w^{(1)}_n, \dots, \sqrt{p_\ell}\, w^{(\ell)}_n, \dots, \sqrt{p_T}\, w^{(T)}_n \right)$$

אז לכל $i \neq j$ מתקיים ש

$$\langle V_i, V_j \rangle = \sum_{\ell=1}^{n} p_\ell \cdot \underbrace{w^{(\ell)}_i\, w^{(\ell)}_j}_{\substack{1 \text{ אם } w^\ell_{(i)} = w^\ell_{(j)} \\ -1 \text{ אם } w^\ell_{(i)} \neq w^\ell_{(j)}}} = \Pr[X_i = X_j] - \Pr[X_i \neq X_j] = 0$$

בגלל הבת"ז הזוגית

לכן כל ה-$\{V_i\}_{i=1}^n$ בת"ז, ולכן $\dim(\mathbb{R}^T) \geq n$ ולכן $n \leq T$.

תרגיל: יהיו $X_1 \dots X_n$ מפולגים אחיד על $\{0,1\}$, k-wise ind, אז $|Supp(X)| \geq \binom{n}{k/2}$

<u>תרגיל:</u> לאלגוריתם ל maximal-IS

נתחיל בכינוי א המשתנים- $X_1, \dots, X_n$ $n=|V|$

כך שלכל i X_i מפולג אחיד על $\{1,\dots,2d(n)\}$

ולכל $i \neq j$, X_i ב"ת ב- j.

הראנו כי ניתן לבנות מ"ה מקבילית $\breve{A}$ עם $|supp(\breve{A})| = poly(n)$

וכך גם A שעבורו $|A-\breve{A}|_1 \leq o(\frac{1}{n})$

ו A מקבל_ את ~~[illegible]~~

הסק ש maximal-IS $\in NC$.

tail inequal

אי״ש מרקוב : Markov

אם $X \geq 0$, אז

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

הוכחה

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

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

כי הערכים חיו״ב.

אי שוויון צ׳בישב Chebychev

לכל X מ״מ , $\mu = E(X)$

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

הוכחה

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

דוגמא: $X_1, \ldots, X_n$ מ״מ בלתי תלויים , (מתפלגים על $\{0,1\}$)

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

לכן:

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

לעומת: אם אז $pr(X=n) = \frac{1}{2}$.

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

אם נוסף נניח $X_1 \dots X_n$ ב"ת בזוגות

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

ב"ת

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

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

2. אם X מ"מ, $pr(X)=1$, אז $Var(X) = p(1-p)$

3. אם $X_1 \sim X_n$ ב"ת בזוגות אז

$Var\left(\sum X_i\right) = \sum Var(X_i)$

תרגיל: יהיו $X_1 \dots X_n$ מ"מ בלתי תלויים k-wise, k זוגי.

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

הוכיחו $pr\left(|X - \mu| \geq A\right) \leq \frac{E(|X-\mu|^k)}{A^k} \leq (kn)^{k/2} \cdot \frac{1}{A^k}$

עבור $k=4$ $\leq \frac{3n^2}{A^4}$

מה קורה כשיש לנו אי-תלות מוחלטת ?

$X_1,\dots,X_n$ מתפלגים ב-$\{0,1\}$, $Pr(X_i=1)=p_i$

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

טענה:

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

זה מה שנוכיח.

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

הוכחה:

$$Pr\left(X<(1-\delta)\mu\right) = Pr\left(e^{-tX} > e^{-t(1-\delta)\mu}\right) \le \frac{E(e^{-tX})}{e^{-t(1-\delta)\mu}}$$

לכל $t>0$ כי הפונק' מונו' יורד.

מרקוב

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

מאי התלות

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

$1-x<e^{-x}$

ולכן:

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

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

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

וכך מקבלים

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

גרסה 1:

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

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

$e = 2.7\ldots$

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

~~pr(Ax~~

גרסה 3: אם $\delta < 2e-1$

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

למה:

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