# 67865 - כלים מתמטיים

7 בינואר 2014

מרצה: מיכאל בן אור
מתרגל: צור לוריא

איני לוקחת אחריות על מה שכתוב כאן, so tread lightly
אין המרצה קשור לסיכום זה בשום דרך.
הערות יתקבלו בברכה - *noga.rotman@gmail.com*. אהבתם? יש עוד!
*www.bit.ly/integrali*

# תוכן עניינים

## רשימת אלגוריתמים

## 0.1 הקדמה

15.10.2013

מה נלמד? "דברים שצריכים להיות בקצות אצבעותיכם בכל תחומי מדעי המחשב".
כל מה שנלמד היום אמור להיות לכולנו חזרה ולא יותר מזה. מכיוון וזה קורס יותר מתקדם, נתקדם יותר מהר, הדוגמאות יהיו יותר מורכבות ממה שראינו בעבר, וכו'.

## 0.2 מנהלות

לקורס יש אתר שהוא כרגע ריק - באתר בשנה שעברה יש את כל החומר. בפרט יש שם הפניה לסיכומי הרצאות משנים קודמות.
מבחינה האדמיניסטרטיבית - ישנו תרגול שבועי.
דרישות: בסיום כל פרק נעשה בוחן קטן (בערך 10 דקות) שכל אחד שקרא ויודע אמור לעשות אותו בלי בעיה. ברגע זה מתוכננת בחינה סופית. לקבוצות קטנות יותר המרצה מעדיף לתת עבודה, אבל זה עלול להיות מסורבל ועל כן רב הסיכויים שתהיה בחינה :(

אתר הקורס:

$$www.cs.huji.ac.il/\sim mathtool2$$

ותיבת הדואר של הקורס להגשת תרגילים:

$$mathtools.huji@gmail.com$$

תרגיל בכל שבוע להגשה ביום חמישי. תא להגשת תרגילים ברוס 1- או הגשה אלקטרונית לאימייל של הקורס. התרגילים לא יבדקו, אולם בסוף כל נושא (יהיו שלושה נושאים) יערך סבב ראיונות - רישום דרך האתר של הקורס. הראיונות האלו יהיו $20\%$ מהציון הסופי.
בנוסף יהיו בחנים בסוף כל נושא, שיהוו $10\%$ מהציון הסופי[1].
שעות קבלה של המתרגל: ימי שלישי $16:00-17:00$ ברוס $-1$, חדר 36.
ספר מומלץ:

The Probabilistic Method - Alon &Spencer

[1] שאלות פשוטות - "נסח את אי שיוויון צ'ביצ'ב" ולא "הוכח את אי שיוויון צ'ביצ'ב".

# 1 הסתברות

השיעור נדבר בעיקר על הסתברות בדידה.

## 1.1 הסתברות בדידה

### 1.1.1 הגדרות בסיסיות

**הגדרה 1.1** מרחב הסתברות דיסקרטי (סופי או בן מניה) מורכב מקבוצה $\Omega$ ופונקציה $Pr$ : $\Omega \to \mathbb{R}_+ = \{\, x \geq 0 | \, x \in \mathbb{R}\}$ לממשיים החיוביים כך ש:

$$\sum_{\omega \in \Omega} Pr\left[\omega\right] = 1$$

בהמשך נכליל המושג להסתברות רציפה - למשל הגדרה זו אינה מתאימה להגדרת הסתברות על הקטע בין 0 ל-1.

**הגדרה 1.2** מאורע $(Event)$ הוא קבוצה $A \supseteq \Omega$ כך ש:

$$Pr\left[A\right] = \sum_{\omega \in A} Pr\left[\omega\right]$$

כאשר $Pr\left[A\right]$ היא ההסתברות של המאורע $A$.

#### אי תלות

**הגדרה 1.3** שני מאורעות $A, B \supseteq \Omega$ נקראים בלתי תלויים $(Independent)$ אם:

$$Pr\left[A \cap B\right] = Pr\left[A\right] \cdot Pr\left[B\right]$$

**לדוגמא:** ניקח את מרחב ההסתברות של $n$ הטלות מטבע (הוגן) - $\Omega = \{0,1\}^n$ כאשר $Pr\left[\omega\right] = \frac{1}{2^n} \; \forall \omega \in \{0,1\}^n$, ונגדיר את שני המאורעות:

$$\begin{aligned}
A &= \{\, x = (x_1, ..., x_n) \in \{0,1\}^n | \, x_1 = 0\} \\
B &= \{\, x = (x_1, ..., x_n) \in \{0,1\}^n | \, x_2 = 0\} \\
&\Rightarrow Pr\left[A\right] = \frac{|A|}{|\Omega|} = \frac{2^{n-1}}{2^n} = \frac{1}{2} = Pr\left[B\right] \\
&\Rightarrow Pr\left[A \cap B\right] = \frac{2^{n-2}}{2^n} = \frac{1}{4} = \frac{1}{2} \cdot \frac{1}{2}
\end{aligned}$$

**הגדרה 1.4** $A_1, ..., A_k$ הם מאורעות בלתי תלויים, אם לכל תת קבוצה של אינדקסים $S \supseteq \{1, ..., k\}$, $S = \{i_1, ..., i_t\}$ מתקיים:

$$Pr\left[A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_t}\right] = Pr\left[A_{i_1}\right] \cdot ... \cdot Pr\left[A_{i_t}\right]$$

**הגדרה 1.5** מאורעות אלו נקראים בלתי תלויים בזוגות, אם כל שני מאורעות מתוכם בלתי תלויים.

במדעי המחשב רואים הרבה מאוד מאורעות שהם בלתי תלויים בזוגות או בשלשות, אך לא בלתי תלויים.

**הסתברות מותנית** $(Conditional\ Prob.)$

**הגדרה 1.6** בהנתן $A, B$ מאורעות, כאשר $Pr[B] \neq 0$, ההסתברות המותנית של $A$ בהנתן $B$ מוגדרת להיות:

$$Pr[A|B] = \frac{Pr[A \cap B]}{Pr[B]}$$

**לדוגמא:** נביט במרחב מהדוגמא הקודמת. ללא ידע אנו רק יודעים שיש הסתברות אחידה לכל סדרה.
נגיד ואנו יודעים כי מאורע $B$ קרה. בהנתן הידע הזה, מה אנחנו יודעים על ההסתברות של המאורע הראשון? האם הידע שלנו השתנה? מכיוון ו־$A, B$ בלתי תלויים:

$$Pr[A|B] = \frac{Pr[A \cap B]}{Pr[B]} = \frac{Pr[A] \cdot Pr[B]}{Pr[B]} = Pr[A]$$

כלומר, הידע שלנו לא משתנה אמ"מ המשתנים הם בלתי תלויים.

**משתנים מקריים ממשיים** $(Random\ Variables)$

**הגדרה 1.7** משתנה מקרי ממשי הוא פונקציה $f : \Omega \to \mathbb{R}$.

**לדוגמא:**

- בהנתן קבוצה $W \subseteq \mathbb{R}$, ניתן לדוגמא להגדיר את המאורע:

$$A = \{\omega \in \Omega | f(\omega) \in W\}$$

- בהנתן מאורע $\Omega \supseteq A$, ניתן להגדיר את **הפונקציה המציינת** $(Indicator\ Function)$:

$$I_A(\omega) := \begin{cases} 1 & \omega \in A \\ 0 & otherwise \end{cases}$$

**הגדרה 1.8** הערך הממוצע של $f$ על מרחב ההסתברות, או **התוחלת** $(Expectation)$ של $f$ היא:

$$\mathbb{E}[f] = \sum_{\omega \in \Omega} Pr[\omega] \cdot f(\omega)$$

נשים לב כי לא תמיד התוחלת קיימת ־ הטור לא תמיד מתכנס! במקרים שאנחנו נתעסק בהם, התוחלת תהיה לפחות קיימת (אם כי יתכן ותהיה אינסופית).

**לדוגמא:**

$$\Omega = \{1, 2, ..., n, ...\}$$
$$Pr[k] = \frac{1}{2^k},\ \sum_{k=1}^{\infty} \frac{1}{2^k} = 1$$
$$f(k) = 2^k \Rightarrow \mathbb{E}[f] = 1$$
$$f(k) = 2^k \cdot (-1)^k \Rightarrow \mathbb{E}[f]\ \ does\ not\ exist$$
$$\overbrace{\sum_{k=1}^{\infty} \frac{k}{2^k}}^{=a} = \sum_{k=1}^{\infty} \frac{1}{2^k} + \sum_{k=1}^{\infty} \frac{k-1}{2^k} = 1 + \frac{1}{2} \cdot \sum_{k=1}^{\infty} \frac{k-1}{2^{k-1}} = 1 + \frac{1}{2} \cdot \sum_{k=1}^{\infty} \frac{k}{2^k}$$
$$\Rightarrow a = 1 + \frac{1}{2}a \Rightarrow \frac{1}{2}a = 1 \Rightarrow a = 2$$

**התוחלת של משתנה גיאומטרי** מטילים מטבע $\{0, 1\}$, ונסמן:

$$Pr[1] = p,\ Pr[0] = 1 - p$$

כמה פעמים יש להטיל את המטבע על ל"הצלחה" הראשונה?
לכל $n$, מגדירים מ"מ על $\{1, 2, ..., n, ...\}$ כך ש:

$$Pr[n] = (1-p)^{n-1} \cdot p$$

כלומר, הפסד בכל ההטלות עד ל־$n$ ואז הצלחה. נגדיר $f(n) = n$.
אזי, תוחלת מספר הטלות המטבע עם הסתברות הצלחה $p$ הינה $\mathbb{E}[f]$, וכפי שראינו בקורסים קודמים היא שווה ל־$\frac{1}{p}$.

**מרחב המ"מ** אם מתבוננים על מרחב של הפונקציות:

$$f : \Omega \to \mathbb{R}$$

זהו מרחב לינארי מעל $\mathbb{R}$־ בהנתן $g, f : \Omega \to \mathbb{R}$ וכן $\alpha, \beta \in \mathbb{R}$, מתקיים:

$$h = (\alpha \cdot g + \beta \cdot f) : \Omega \to \mathbb{R} \Rightarrow (\alpha \cdot g + \beta \cdot f)(\omega) = \alpha \cdot g(\omega) + \beta \cdot f(\omega)$$

**הערה 1.9** התוחלת היא לינארית:

$$\mathbb{E}\left[\alpha g + \dot{\beta} \cdot f\right] = \alpha \cdot \mathbb{E}[g] + \beta \cdot \mathbb{E}[f]$$

**משתנים מקריים בלתי תלויים**

**הגדרה 1.10** שני משתנים מקריים הם בלתי תלויים, אם לכל שני ערכים $s,t \ni \mathbb{R}$, המאורעות $f(\omega)=s$ ו־$g(\omega)=t$ הם בלתי תלויים.

**השונות** $(Varience)$

**הגדרה 1.11** נסמן את התוחלת של משתנה מקרי $X:\Omega\to\mathbb{R}$ ב־$\mathbb{E}[X]=\eta$. השונות היא ההבדל בין המ"מ לתוחלת:

$$Var(X)=V=\mathbb{E}\left[(X-\mathbb{E}[X])^2\right]$$

**הגדרה 1.12** סטיית התקן $\sigma$ של המ"מ הנ"ל הינה $\sigma^2=V$.

ומקבלים מחישוב קצר:

$$V=\mathbb{E}\left[X^2\right]-(\mathbb{E}[X])^2:=Var[X]$$

### 1.1.2 אי שיוויונות פשוטים בהסתברות

כדי להעריך הסתברויות שונות עלינו להשתמש בחסמים.

**חסם האיחוד** אם $\{A_i\}_{i\in I}$ אוסף של מאורעות, $A=\bigcup_{i\in I}A_i$, אזי:

$$Pr[A]\le\sum_{i\in I}Pr[A_i]$$

**הוכחה:** נובעת ישירות מההגדרה של $Pr[A]$ כסכום ההסתברויות של אברי $A$. ■

**אי שיוויון מרקוב** $(Markov)$ יהי $0\le X$ מ"מ לא שלילי, ו־$1\le c$ קבוע כלשהוא. אזי:

$$Pr[X>c\cdot\mathbb{E}[X]]\le\frac{1}{c}$$

**הוכחה:** מקורס הסתברות. ■

**אי שיוויון צ'ביצ'ב** $(Chebychev)$ יהי $X$ מ"מ עם תוחלת $\mathbb{E}[X]=\mu$ ושונות $V=Var[X]$ וסטיית תקן $\sigma$, $\sigma^2=V$. אזי לכל קבוע $1\le c$:

$$Pr[|X-\mu|>c\cdot\sigma]\le\frac{1}{c^2}$$

ההוכחה מוכחת מתוך אי שיוויון מרקוב (ניתן לראות בקורס הסתברות).

אנחנו נשתמש ונוכיח בהמשך אי שיוויונות יותר מסובכים.

**דוגמא** נתבונן באוסף הפרמוטציות על $n$ איברים:

$$S_n = \{\pi | \, \pi : [n] \to [n] \, , \ \pi \ is \ ...\} \, , \ [n] = \{1, ..., n\}$$

אנו יודעים כי $|S_n| = n!$, נסמן $\Omega = S_n$ עם התפלגות אחידה:

$$Pr\left[\pi\right] = \frac{1}{n!}$$

בהנתן פרמוטציה מקרית, מהי תוחלת מספר האיברים שנשארים במקום?
יהי $X$ המ"מ:

$$X\left(\pi\right) = \#\left\{i | \, \pi\left(i\right) = i\right\}$$

מהי התוחלת $\mathbb{E}\left[X\right]$?

**טענה 1.13**

$$\mathbb{E}\left[X\right] = 1$$

**הוכחה:** בעזרת הלינאריות של פונקציית התוחלת: נתבונן במ"מ:

$$X_i\left(\pi\right) = \begin{cases} 1 & \pi\left(i\right) = i \\ 0 & otherwise \end{cases}$$

נשים לב כי $X_i$ היא הפונקציה המציינת של המאורע "$i$ נשאר במקום". כעת:

$$X = \sum_{i=1}^{n} X_i$$

נחשב - המאורע הזה מקבע רק איבר אחד במקום ספציפי, ושאר האיברים האחרים יכולים לעבור לכל מקום אחר. על כן:

$$\mathbb{E}\left[X_i\right] = \frac{|S_{n-1}|}{|S_n|} = \frac{(n-1)!}{n!} = \frac{1}{n}$$

$$\Rightarrow \mathbb{E}\left[X\right] = \sum_{i=1}^{n} \mathbb{E}\left[X_i\right] = n \cdot \frac{1}{n} = 1$$

■

**עוד דוגמא!** כל פרמוטציה $\pi \in S_n$ ניתן לפרק לאוסף של ציקלים $(Cycles)$/מעגלים זרים באופן הבא:

$$1 \to \pi\left(1\right) \to \pi\left(\pi\left(1\right)\right) \to ... \to 1$$

מעגל באורך אחד הוא איבר שנשאר במקום.
$(i, j)$ הוא מעגל באורך 2 אם $\pi\left(i\right) = j \ \pi\left(j\right) = i$.
מעגל באורך $k$ ב-$\pi$ הוא אוסף של איברים שונים $i_1, ..., i_k$ כך ש:

$$\pi\left(i_1\right) = i_2, \ \pi\left(i_2\right) = i_3, ..., \pi\left(i_{k-1}\right) = i_k, \ \pi\left(i_k\right) = i_1$$

ונסמן $(i_1, ..., i_k)$.

**למה 1.14** יהי $X_k : S_n \to \mathbb{N}$ פונקציה הסופרת את מספר המעגלים באורך $k$ המופיעים בפרמוטציה. אזי, כאשר בוחרים $S_n \ni \pi$ בהתפלגות אחידה:

$$\mathbb{E}[X] = \frac{1}{k}$$

נשים לב כי עבור $k = 1$ מקבלים 1, ועבור $k = n$ יש $(n-1)!$ פרמוטציות שמקיימות זאת (כל האיברים על מעגל), והתוחלת המתקבלת במקרה זה היא $\frac{(n-1)!}{n!} + 0 = \frac{1}{n}$. **הוכחה:** תהי $\mathcal{F}_k$ אוסף המעגלים השונים באורך $k$ על $n$ איברים. נגדיר יחס שקילות על סדרות של $k$ איברים מתוך $\{1, ..., n\}$:

$$(i_1, ..., i_k) \sim (i_k, i_1, ..., i_{k-1}) \sim (i_{k-1}, i_k, i_1, ..., i_{k-2}) \sim ...$$

אזי:

$$|\mathcal{F}_k| = \begin{pmatrix} n \\ k \end{pmatrix} \cdot (k-1)!$$

בהנתן $\mathcal{F}_k \ni (i_1, ..., i_k)$, נגדיר:

$$X_{(i_1,...,i_k)}(\pi) = \begin{cases} 1 & (i_1, ..., i_k) \in \pi \\ 0 & otherwise \end{cases}$$

אזי:

$$X_k = \sum_{(i_1,...,i_k) \in \mathcal{F}_k} X_{(i_1,...,i_k)}$$

נחשב את התוחלת של $X_{(i_1,...,i_k)}$ :

$$\mathbb{E}\left(X_{(i_1,...,i_k)}\right) = \frac{(n-k)!}{n!}$$

ומלינאריות התוחלת:

$$\mathbb{E}[X_k] = |\mathcal{F}_k| \cdot \frac{(n-k)!}{n!} = \frac{n!\,(k-1)!\,(n-k)!}{k!\,(n-k)!n!} = \frac{1}{k}$$

■

**דוגמא מתורת** $Ramsey$ ישנה תופעה קומבינטורית מעניינת - כשלוקחים דברים "גדולים", קשה מאוד שלא יהיה בהם איזשהוא סדר - איזה מבנה מאוד יפה, או דברים דומים. בתופעה זו עוסקת תורת רמזי.

נתבונן בגרף המלא $G = (V, E)$ על $n$ קודקודים - $K_n$; נסמן $V = \{1, ..., n\}$, ו-$E$ היא קבוצת כל הקשתות. נבחר צביעת קשתות $f : E \to \{B, R\}$ .

אזי, לכל $k, l$ טבעיים קיים $R(k,l)$[2] כך שלכל צביעה של קשתות $K_n$, $R(k,l) \leq n$ בשני צבעים אדום וכחול, או שיש קליקה אדומה בגודל $\geq l$, או שיש קליקה כחולה בגודל $\geq k$.

[2] כאשר $R$ הוא מספר הנקרא "מספר רמזי", התלוי ב-$k$ ו-$l$.

**הערה 1.15** ההוכחה הסטנדרטית נותנת חסם:

$$R(k,l) \leq \left( \begin{array}{c} k+l-2 \\ k-1 \end{array} \right)$$

ועבור $k = l$:

$$R(k,k) \leq 2^{2k} = 4^k$$

במילים אחרות, בכל גרף על $n$ קודקודים או שיש קליקה בגודל $\frac{1}{2}\log_2 n$, או שיש אנטי־קליקה בגודל $\frac{1}{2}\log_2 n$ (כלומר הצביעה בשני הצבעים קובעת אם קיימת או לא קיימת קליקה).

**טענה 1.16** מתקיים:

$$R(k,k) \geq 2^{k/2}$$

או במילים אחרות, קיימים גרפים בגודל $n$ שבהם אין קליקה או אנטי־קליקה בגודל $2\log_2 n$.

**הוכחה:** נתבונן במודל של גרף הסתברותי $G(n,p)$: זהו גרף על $n$ קודקודים שכל קשת קיימת בהסתברות $p$, וקשתות שונות הן בלתי תלויות. עבור $p = \frac{1}{2}$ מקבלים התפלגות אחידה על כל הגרפים. נשתמש בערך זה (ההוכחה נובעת מכך!), ונגדיר משתנה מקרי $X(G)$ = מספר הקליקות בגודל $k = 2 \cdot \log_2 n$, ומשתנה מקרי נוסף $Y(G)$ = מספר האנטי־קליקות בגודל $k$. כמו כן, נגדיר מ"מ:

$$X_S = \begin{cases} 1 & S \text{ is a clique in } G \\ 0 & otherwise \end{cases} \Rightarrow X = \sum_{|S|=k} X_S$$

וכנ"ל עבור $Y_S$. אזי:

$$\mathbb{E}[X_S] = Pr[S \text{ is a clique in } G] = \left(\frac{1}{2}\right)^{\frac{k(k-1)}{2}}$$

כדי להוכיח את הטענה על מספר $Ramsey$, נראה שעבור ה־$k$ שבחרנו מתקיים:

$$\mathbb{E}[X+Y] < 1$$

שכן התוחלת הזו היא מספר הקליקות ועוד מספר האנטי־קליקות, ואם זה מתקיים אז חייב להיות קיים גרף עבורו המספר הזה שווה לאפס (אחרת הממוצע היה גדול או שווה מ־1), כלומר קיים גרף $G$ עבורו:

$$X(G) = Y(G) = 0$$

נשים לב:

$$\mathbb{E}[X] = \mathbb{E}[Y]$$

איך נחשב את התוחלת הזו?

$$\mathbb{E}[X] = \sum_{|S|=k} \mathbb{E}[X_S] = \left( \begin{array}{c} n \\ k \end{array} \right) \cdot 2^{-\frac{k(k-1)}{2}} \leq \frac{n^k}{k!} \cdot \left(2^{-\frac{k-1}{2}}\right)^k$$

בסיכום מופיע שימוש בנוסחאת סטרלינג, לאחריה מתקבל:

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

וכאשר בוחרים $k \geq 2 \cdot \log_2 n$ מקבלים:

$$\leq \frac{2^{k/2}}{k!} \overset{k\to\infty}{\longrightarrow} 0$$

■

22.10.2013

נזכור כי בסוף ההוכחה מעלה קיבלנו מ"מ $0 \leq X$, כאשר $X(\omega)$ לכל $\omega \in \Omega$ הוא מספר שלם. אם כך, כאשר קיבלנו כי $\mathbb{E}[X] < 1$, המשמעות היא כי קיים $\omega \in \Omega$ כך ש: $X(\omega) = 0$[3]. למעשה, הראנו כי $\mathbb{E}[X_n] \overset{n\to\infty}{\longrightarrow} 0$.

עולה השאלה, מה קורה כאשר דוגמים במרחב? אולי לפעמים המספר מאוד גדול, אולי המספר מאוד קטן... מעניין אותנו לדעת אינפורמציה יותר טובה רק מהתוחלת. נשאל, מה קורה עם $Pr(X_n = 0)$? נטען כי הסתברות זו שואפת ל־1. אחרת, קיימת תת סדרה עבורה $Pr(X_n \geq 1) \to \varepsilon > 0$. מכאן, $\mathbb{E}[X] \geq \varepsilon > 0$, בסתירה למה שהוכחנו.

קיבלנו אם כך טענה הרבה יותר חזקה ־ כמעט כל גרף שנבחר יקיים זאת. לכך מתכוונים כשאומרים שכמעט בוודאות $X_n = 0$ (almost surely).

**הגדרה 1.17** $A_n$ סדרה של מאורעות מתרחשת כמעט בוודאות (או כמעט בבטחה) אם $Pr(A_n) \to 1$.

בתרגיל שניתן לנו (בשאלה על מעגלים המילטוניים), רואים כי גם אם התוחלת לא שואפת לאפס (ולמעשה, במקרה של מעגלים המילטוניים שואפת לאינסוף) כמעט תמיד מקבלים אפס, כלומר: $Pr(X_n = 0) \overset{n\to\infty}{\longrightarrow} 1$.

במקרה שלנו, אנחנו יודעים מה קורה בהסתברות ־ הרב מרוכז סביב 1. אפשר לדעת הרבה יותר על ההסתברות במקרה הכללי אם יודעים את התוחלת של $X_n^2$, או בדרגות הרבה יותר גבוהות (וגם זה לעיתים לא מספיק) ־ ככל שמוסיפים ממונטים יותר גבוהים, יש יותר מידע. הסיבה ־ במקרה שיש מומנט שני אפשר לחשב את השונות, ואז אפשר להשתמש באי"ש צ'בישב ולקבל תוצאות יותר טובות מאי"ש מרקוב (וכמובן ויש אי"ש מתאימים ומדוייקים יותר למומנטים גבוהים יותר).

מטרתנו הינה לדעת איך מתנהג באמת $X_n$. אבל זה מאוד קשה, על כן נתמקד בלפחות לענות על השאלה האם $X_n$ באמת מרוכז סביב התוחלת?

בהנתן $X \geq 0$, מאי"ש מרקוב נקבל:

$$Pr[X \geq a] \leq \frac{\mathbb{E}[X]}{a}$$

ומכאן אנחנו לא יודעים איך ההסתברות "זזה". אם מסתכלים על אי"ש צ'בישב:

$$Pr[|X - \mathbb{E}[X]| \geq a] \leq \frac{Var[X]}{a^2}$$

וזה כבר אומר ש"אי אפשר לזוז פה הרבה", וזה בתנאי שהשונות קטנה מהתוחלת בריבוע. לשימוש הזה בצ'בישב או בשימוש התוחלת בריבוע נקרא שיטת המומנט בריבוע, ואותה נראה בשיעור זה:

[3] למעשה המ"מ שלנו היה $X + Y$.

### 1.1.3 שימושים במומנט שני $\mathbb{E}\left[X^2\right]$

- בהנתן סדרה של משתנים $X_n \geq 0$, $\mathbb{E}[X_n] \to \infty$, והשונות $Var[X_n]$ "לא גדולה מידי" (כלומר קטנה מהתוחלת בריבוע - בהמשך טענה שמפרטת זאת), נוכל להסיק כי משתנה באמת יהיה מרוכז סביב התוחלת שלו, דהיינו כמעט בוודאות $X_n > 0$.
מדוע? אם לוקחים $a = \mathbb{E}[X]$ למשל, לא מקבלים כלום מא"ש צ'בישב. אולם, ברגע ש- $Var[X]$ קצת יותר קטן מהתוחלת, כבר מקבלים משהו.

**טענה 1.18**

$$Pr[X = 0] \leq \frac{Var(X)}{\mathbb{E}[X]^2}$$

**הוכחה:** נתבונן במאורעות:

$$A = \{\omega \,|X(\omega) = 0\}, \; B = \{\omega \,||X(\omega) - \mathbb{E}[X]| \geq \mathbb{E}[X]\}$$

מא"ש צ'בישב:

$$Pr[B] \leq \frac{Var[X]}{\mathbb{E}[X]^2}, \; Pr[A] \leq Pr[B]$$

כי $A \subseteq B$. ■

**דוגמא לשימוש** נתבונן בגרף מקרי $G_n = G(n, p_n)$ גרף מקרי על $n$ קודקודים; ההסתברות לכל צלע היא $p$.
נתבונן במאורע: "יש קליקה בגודל 4 בגרף $G$". למרבית התופעות האלו בגרפים (במיוחד לתכונות מונוטוניות - ככל שיש יותר צלעות ההסתברות תעלה לקיום קליקה, למשל) יש סף ספציפי של $p$ - כמעט תמיד מעל הסף התכונה מתרחשת, וכמעט תמיד מתחת לסף התכונה לא מתקיימת.

**טענה 1.19** 1. אם $p_n = o\left(n^{-\frac{2}{3}}\right)$[4], אזי כמעט בוודאות $G$ לא מכיל $K_4$[5].
2. אם $p_n = \omega\left(n^{-\frac{2}{3}}\right)$ אזי כמעט בוודאות יש $K_4$ ב-$G$.

**הוכחה:** את 1 ניתן להוכיח בשיטות של שבוע שעבר - יהי $X$ מ"מ המציין את מספר הקליקות בגודל 4 ב-$G$. אזי ניתן לסמן:

$$X = \sum_{|T|=4;\; T \subset \{1,\ldots,n\}} X_T$$

כאשר $X_T$ מ"מ המציין האם $T$ הוא קליקה ב-$G$:

$$X_T(G) = \begin{cases} 1 & T \text{ is a clique in } G \\ 0 & otherwise \end{cases}$$

---

[4] כלומר $\frac{p_n}{n^{-\frac{2}{3}}} \xrightarrow{n\to\infty} 0$

[5] כמובן שאנחנו מדברים כאן על סדרה של $p_n$ - אם $p$ קבוע, לשאיפה אסימפטוטית אין משמעות

אזי, התוחלת $\mathbb{E}[X_T] = p^6$ (אם קיימות כל הצלעות בגרף בן 4 קודקודים). על כן:

$$\mathbb{E}[X] = \begin{pmatrix} n \\ 4 \end{pmatrix} \cdot p^6 \leq n^4 \cdot p^6$$

במקרה הראשון, כלומר אם $p = o\left(n^{-\frac{2}{3}}\right)$, אזי:

$$n^4 \cdot p^6 \overset{n\to\infty}{\longrightarrow} 0$$

ההוכחה של 2 תדרוש מאיתנו קצת יותר - את חישוב השונות: נרצה להוכיח כי ההסתברות שלא קיימת $K_4$ בגרף שואפת לאפס. במקרה 2 מתקיים:

$$\mathbb{E}[X] \geq \frac{(n-3)^4}{4!} \cdot p^6 \overset{n\to\infty}{\longrightarrow} \infty$$

זה טוב ויפה, אבל איך נראה שכמעט תמיד באמת קיימת קליקה, הרי ייתכן שהרבה פעמים ההסתברות היא אפס, למרות השאיפה הנ"ל. נרצה להראות כי $\frac{Var(X)}{\mathbb{E}[X]^2} \to 0$. לשם כך, נחשב את השונות:

$$\begin{aligned} Var(X) &= \mathbb{E}\left[\left(\sum_{|T|=4} X_T\right)^2\right] - \left(\mathbb{E}\left[\sum_{|T|=4} X_T\right]\right)^2 \\ &= \sum_{T,S;\ |T|=|S|=4} \mathbb{E}[X_T \cdot X_S] - \sum_{T,S;\ |T|=|S|=4} \mathbb{E}[X_T] \cdot \mathbb{E}[X_S] \\ &= \overbrace{\sum_{|T|=4} \mathbb{E}\left[X_T^2\right] - \mathbb{E}[X_T]^2}^{(*)} + \overbrace{\sum_{T\neq S;\ |T|=|S|=4} \mathbb{E}[X_T \cdot X_S] - \mathbb{E}[X_T] \cdot \mathbb{E}[X_S]}^{(**)} \end{aligned}$$

מכיוון ו-$X_T$ הוא מ"מ מציין, דהיינו ערכיו הם אפס או 1, אז נוכל לוותר על הריבוע בביטוי השמאלי ביותר ב-$(*)$. אזי מחישובים קודמים נקבל:

$$(*) \leq \sum_{|T|=4} \mathbb{E}[X_T] \leq n^4 \cdot p^6 << n^8 \cdot p^{12}$$

$X_T, X_S$ הם מ"מ בלתי תלויים אלא אם כן $|T \cap S| = 2, 3$ (במקרה בו $T \neq S$). נזכיר כי אם $U, V$ מ"מ,

$$cov(U, V) = \mathbb{E}[U \cdot V] - \mathbb{E}[U] \cdot \mathbb{E}[V]$$

הוא ה-*coveriance*.

אם $X_T$ ב"ת ב-$X_S$, אזי האיבר בסכום $(**)$ הוא אפס. נותר אם כך לבדוק מה קורה במקרה בו החיתוך שווה ל-2 ובמקרה בו החיתוך שווה ל-3:

$$V \leq n^4 \cdot p^6 + \sum_{|T\cap S|=2,\ |T|=|S|=4} cov(X_T, X_S) + \sum_{|T\cap S|=3,\ |T|=|S|=4} cov(X_T, X_S)$$

איך מקרה התלות נראה? במקרה ש:$|T \cap S| = 2$ *באיור*, צריך ש־11 הצלעות שבין 6 הקודקודים יתקיימו:

$$\sum_{|T\cap S|=2} \mathbb{E}\left[X_T \cdot X_S\right] = \left(\begin{array}{c} n \\ 4 \end{array}\right) \cdot \left(\begin{array}{c} 4 \\ 2 \end{array}\right) \cdot \left(\begin{array}{c} n-4 \\ 2 \end{array}\right) \cdot p^{11}$$

כאשר בימני ביותר בוחרים $T$, בשני בוחרים מתוך $T$ חיתוך עם $S$, ולאחר מכן בוחרים השלמה ל־$S$ (בבחירה למעשה מגדירים את $S$). כל המספר שקיבלנו $= O\left(n^6 \cdot p^{11}\right)$. באופן דומה:

$$\sum_{|T\cap S|=3} \mathbb{E}\left[X_T \cdot X_S\right] = \left(\begin{array}{c} n \\ 4 \end{array}\right) \cdot \left(\begin{array}{c} 4 \\ 3 \end{array}\right) \cdot \left(\begin{array}{c} n-4 \\ 21 \end{array}\right) \cdot p^9 = O\left(n^5 \cdot p^9\right)$$

ואם נסכם את הכל, נקבל את הביטוי הבא:

$$V \leq n^4 \cdot p^6 + n^4 \cdot p^{11} + n^5 \cdot p^9$$

ובמקרה בו $p >> n^{-\frac{2}{3}}$ נקבל כי הביטוי הזה שווה ל:

$$= o\left(n^8 \cdot p^{12}\right) \Rightarrow \frac{Var\left(X\right)}{\mathbb{E}\left[X\right]^2} \to 0$$

■

### 1.1.4 בעיה מעניינת ושימושית ־ כדורים ותיבות Balls and Bins

1. פרדוקס יום ההולדת:
זורקים כדורים ל־$n$ תיבות. אזי אחרי בערך $\sqrt{n}$ כדורים, סביר שתהיה תיבה עם יותר מכדור אחד[6].

2. בעיית איסוף הקופונים:
כמה כדורים יש לזרוק עד שכמעט בוודאות אין תיבה ריקה?

**פרדוקס יום ההולדת** מהי ההסתברות שאין חזרות כאשר זורקים $r$ כדורים ל־$n$ תיבות?

$$P_{n,r} = 1 \cdot \frac{n-1}{n} \cdot \frac{n-2}{n} \cdot ... \cdot \frac{n-(r-1)}{n} = 1 \cdot \left(1 - \frac{1}{n}\right) \cdot ... \cdot \left(1 - \frac{r-1}{n}\right)$$

כל עוד $r$ לא יותר מידי גדול, אפשר להשתמש בהערכה שאנחנו כבר מכירים: $1 - x \sim e^{-x}$ (עד כדי הקבוע), ואז נקבל כי הביטוי

$$\sim e^{-\sum_{i=1}^{r-1} \frac{i}{n}} = e^{-\frac{r\cdot(r-1)}{2n}}$$

אם $r = \omega\left(\sqrt{n}\right)$:

$$\overset{\frac{r^2}{n}\to\infty}{\longrightarrow} 0$$

[6] כלומר, מספר הכדורים חלקי $\sqrt{n}$ שואף לאינסוף ־ ניסוח מסודר בהמשך.

כלומר, כמעט בוודאות יש תיבה שיש בה יותר מכדור אחד.
בכיוון השני, אם $r = o\left(\sqrt{n}\right)$:

$$\frac{r^2}{n} \to 0 \Rightarrow P_{n,r} \to 1$$

כלומר, כמעט בוודאות אין תיבה שיש בה יותר מכדור אחד.
באופן דומה נקבל הכללה: בוחרים שתי קבוצות מקריות $A, B \subseteq \{1, ..., n\}$ כך ש־ $|A| = k,\ |B| = l$ באופן ב"ת, וניח $k \geq l$. נשאל, מהי ההסתברות שהחיתוך של הקבוצות ריק\לא ריק? בה"כ אפשר להניח ש־$A = \{1, ..., k\}$, ובוחרים $B$ מקרית בגודל $l$ מתוך $\{1, ..., n\}$.

$$\begin{aligned} Pr\left(A \cap B = \phi\right) &= \frac{\left(\begin{array}{c} n-k \\ l \end{array}\right)}{\left(\begin{array}{c} n \\ l \end{array}\right)} = \frac{(n-k)\left(n-k-1\right)...\left(n-k-l+1\right) \cdot l!}{l! \cdot n\left(n-1\right)...\left(n-l+1\right)} \\ &= \left(1-\frac{n}{k}\right)\left(1-\frac{k}{n-1}\right)\left(1-\frac{k}{n-2}\right)...\left(1-\frac{k}{n-l+1}\right) \\ &\sim e^{-\sum_{i=0}^{l-1}\frac{k}{n-i}} \leq e^{-\frac{l \cdot k}{n}} \\ e^{-\sum_{i=0}^{l-1}\frac{k}{n-i}} &\geq e^{-\frac{k \cdot l}{n-l}} \end{aligned}$$

אם $n >> k \cdot l$, החסם התחתון $e^{-\frac{k \cdot l}{(n-l)}} \leftarrow 1$. לעומת זאת, אם $l \cdot k >> n$, החסם העליון $e^{-\frac{l \cdot k}{n}} \leftarrow 0$, דהיינו החיתוך ריק.

**בעיית איסוף הקופונים**

**טענה 1.20** 1. אם בוחרים $m$ פעמים מתוך $n$ איברים באופן בלתי תלוי, ו־$m >> n \cdot \log n$, אזי כמעט בוודאות נבחרו כל האיברים.
2. תוחלת הזמן עד שנבחר נציג מכל האיברים הוא $n \cdot \log_e n + O\left(n\right)$.

בהמשך נראה תוצאה הרבה יותר חזקה ־ לא צריך לבחור כל כך הרבה באופן אסימפטוטי.
**הוכחה:** 1. יהי $X$ מ"מ הסופר את מספר התאים הריקים. נרצה להוכיח שכמעט בוודאות $X = 0$. ניתן לרשום:

$$X = \sum_{i=0}^{n} X_i$$

כאשר $X_i$ מ"מ המציין אם האיבר ה־$i$אי נבחר או לא (1 אם $i$ לא נבחר, 0 אם נבחר).

$$\mathbb{E}\left[X_i\right] = \left(1-\frac{1}{n}\right)^m \Rightarrow \mathbb{E}\left[X\right] = n \cdot \left(1-\frac{1}{n}\right)^m$$

נבחר $m = n\left(\log n + \Delta_n\right)$, כאשר $\Delta_n \leftarrow \infty$[7]. במקרה זה:

$$\mathbb{E}\left[X\right] \approx n \cdot \left[\left(1-\frac{1}{n}\right)^n\right]^{(\log n + \Delta_n)} = n \cdot e^{-\log_e n - \Delta_n} = e^{-\Delta_n} \to 0$$

[7] למעשה אנחנו מוכיחים כאן טענה חזקה יותר מהמבוקש.

2. יהי $Y$ מ"מ הסופר כמה בחירות היו עד שכולם נבחרו. נסמן:

$$Y = \sum_{i=1}^{n} Y_i$$

כאשר $Y_i$ הוא מ"מ הסופר את מספר הבחירות מהרגע שנבחר האיבר ה־$(i-1)$ ועד לבחירת האיבר ה־$i$־אי (האיבר $Y_1$ הוא זהותית 1). נשים לב כי המשתנים המקריים $Y_i$ הם בלתי תלויים; $Y_{17}$ הוא מ"מ גיאומטרי עם הסתברות הצלחה $p_{17} = \frac{n-16}{n}$.
בהנתן $Y_k$ מ"מ מפולג גיאומטרית עם הסתברות הצלחה $\frac{n-k+1}{n}$:

$$\mathbb{E}[Y_k] = \frac{n}{n-k+1}$$

$$\Rightarrow \mathbb{E}[Y] = \sum_{k=1}^{n} \frac{n}{n-k+1} = n \cdot \overbrace{\sum_{k=1}^{n} \frac{1}{k}}^{H_n} \approx n \log_e n + O(n)$$

מכאן בעזרת מרקוב נקבל:

$$Pr(Y > 10n \log_e n) < \frac{1}{10}$$

נרצה להוכיח כי הריכוז של ההסתברות היא באמת סביב התוחלת הזו. נחשב את השונות:

$$Var(Y) \overset{independance}{=} \sum_{k=1}^{n} Var(Y_k) = (*)$$

נזכור כי אם $Z$ מפולגת גיאומטרית עם הסתברות הצלחה $p$, אז:

$$Var(Z) = \frac{1-p}{p^2} \leq \frac{1}{p^2}$$

ולכן:

$$(*) \leq \sum_{k=1}^{n} \left( \frac{n}{n-k+1} \right)^2 = n^2 \cdot \sum_{k=1}^{n} \frac{1}{k^2} \leq n^2 \cdot \sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{n^2 \cdot \pi^2}{6}$$

נשתמש באי"ש צ'בישב ונקבל:

$$Pr\left( Y > n \cdot H_n + c \cdot \frac{n\pi}{\sqrt{6}} \right) < \frac{1}{c^2}$$

ואם נבחר $c = \sqrt{\log n}$ נקבל שאיפה לאפס, ולכן ההסתברות ממש מרוכזת סביב התוחלת. ■

29.10.2013

נמשיך עם הסתברות, ונראה משפטי ריכוז - עד כה ראינו את א"ש מרקוב וצ'בישב. קיימות דוגמאות בהן הא"ש הללו הם הטובים ביותר, אולם עבור מקרים רבים אפשר להוכיח משפטי ריכוז חזקים יותר.

### 1.1.5 הליכה מקרית על הישר

מתחילים ב־$0$, ובכל צעד מטילם מטבע: בהסתברות $\frac{1}{2}$ זזים צעד אחד ימינה ־ $(+1)$, ובהסתברות $\frac{1}{2}$ זזים אחד שמאלה ־ $(-1)$. כלומר:

$$X_i = \begin{cases} 1 & p = \frac{1}{2} \\ -1 & p = \frac{1}{2} \end{cases}$$

אחרי $n$ צעדים נגיע לנקודה $X = \sum_{i=1}^{n} X_i$. יש הרבה תהליכים שקרובים לתהליך אך הרבה יותר מסובכים לניתוח. לכן המקרה הזה מאוד מעניין, שכן הוא מאוד פשוט.

בהנתן $l \in \mathbb{Z}^+$, ההסתברות $Pr\left(X = l\right)$ מתרחשת אם הלכנו $t$ צעדים $(-1)$ ו־$(n-t)$ צעדים $(+1)$. עלינו למצוא את $t$. מתקיים:

$$n - t - t = n - 2t = l$$

ולכן נכיע ל־$l$ אם $t = \frac{n-l}{2}$. על כן ההסתברות היא:

$$Pr\left(X = l\right) = \frac{\binom{n}{t}}{2^n} = \frac{\binom{n}{\frac{n-l}{2}}}{2^n}$$

$$Pr\left(X \geq a\right) = \sum_{l=a}^{n} \frac{\binom{n}{\frac{n-l}{2}}}{2^n}$$

כאשר ההסתברות מעלה קיימת כאשר האיבר העליון זוגי (כמעט חצי מהביטויים מעלה הם אפס). כדברי המרצה, "אפשר להסתכל על הביטוי הזה והוא פשוט יסתכל עלינו חזרה" ־ כלומר, לא מיידי ואפילו קשה להעריך כמה הביטוי מעלה קטן עבור $l$־אים גדולים. עם זאת, ישנם כלים שיעזרו לנו במשימת ההערכה:

נבחר פרמטר $t > 0$ כלשהוא (נמצא את הבחירה הטובה ביותר מאוחר יותר). $X \geq a \Leftrightarrow tX \geq ta \overset{*}{\Leftrightarrow} e^{tX} \geq e^{ta}$. הסיבה לשימוש במעבר $(*)$ לא ברורה, אך תדבהר בעתיד, ונובעת פשוט ממונוטוניות $e$. לכן נקבל:

$$Pr\left(X \geq a\right) = Pr\left(e^{tX} \geq e^{ta}\right) \overset{Markov}{\leq} \frac{\mathbb{E}\left[e^{tX}\right]}{e^{ta}}$$

כעת נעשה אנליזה של המונה ושל המכנה, כאשר מעבר $(*)$ נובע מכך כי $X_i$ ב"ת:

$$\mathbb{E}\left[e^{tX}\right] = \mathbb{E}\left[e^{\sum_{i=1}^{n} tX_i}\right] = \mathbb{E}\left[\prod_{i=1}^{n} e^{tX}\right] \overset{(*)}{=} \prod_{i=1}^{n} \mathbb{E}\left[e^{tX_i}\right]$$

$$\Rightarrow \mathbb{E}\left[e^{tX_i}\right] = \frac{1}{2} \cdot e^{t} + \frac{1}{2} \cdot e^{-t} = \frac{1}{2}\left[\sum_{k=0}^{\infty} \frac{t^k}{k!} + \sum_{k=0}^{\infty} \frac{(-t)^k}{k!}\right]$$

כאן נחלק לערכים זוגיים ולא זוגיים ־ כאשר האיברים אי זוגי מקבלים ביטול, כאשר הערך זוגי מקבלים את אותו ערך פעמיים (אפשר לשנות את סדר הסכימה שכן הטור מתכנס

בהחלט). על כן:

$$= \sum_{k=0}^{\infty} \frac{t^{2k}}{(2k)!} \overset{(2k)!\geq 2^k \cdot k!}{\leq} \sum_{k=0}^{\infty} \frac{\left(t^2\right)^k}{2^k \cdot k!} = \sum_{k=0}^{\infty} \frac{\left(\frac{t^2}{2}\right)^k}{k!} = e^{\frac{t^2}{2}}$$

$$\Rightarrow \mathbb{E}\left[e^{tx}\right] \leq \prod_{i=1}^{n} e^{\frac{t^2}{2}} = e^{\frac{nt^2}{2}}$$

$$\Rightarrow P\left(X \geq a\right) \leq e^{\frac{nt^2}{2} - ta}$$

קיבלנו פרבולה בעלת מרכז חיובי.לאחר גזירה והשוואה לאפס נקבל כי המינימום מתקבל עבור:

$$t = \frac{a}{n}$$

ערך זה יתן לנו את החסם הכי טוב. כעת נציב ונקבל:

$$\leq e^{n \cdot \frac{a^2}{2n^2} - \frac{a^2}{n}} = e^{-\frac{a^2}{2n}}$$

$$\Rightarrow Pr\left(X \geq a\right) \leq e^{-\frac{a^2}{2n}}$$

ובאופן סימטרי:

$$Pr\left(X \leq -a\right) \leq e^{-\frac{a^2}{2n}}$$

$$\Rightarrow Pr\left(|X| \geq a\right) \leq 2 \cdot e^{-\frac{a^2}{2n}}$$

עבור מספרים גדולים, אם בוחרים למשל $a = n$, נקבל $2 \cdot e^{-\frac{n}{2}}$, כלומר ביטוי אקספוננציאלי קטן, כלומר "לא מצפים לראות מופע כזה", כלומר קיבלנו חסם "אמיתי".
אם לדוגמא בוחרים $a = O\left(n\right)$, כלומר $a = \frac{n}{1100},\ a = \frac{n}{4}$ החסם הוא אקספוננציאלי קטן במספר הצעדים, ואם בוחרים $a = O\left(\sqrt{n \log_e n}\right)$, למשל $a = b \cdot \sqrt{n \log_e n}$, מקבלים:

$$e^{\frac{b \cdot n \log n}{n}} \approx \frac{1}{n^b},\ \sigma = \sqrt{n},\ V = n$$

נרחיב את מה שעשינו מעלה למשפטים יותר כללים. המשפטים הללו מופיעים בשמות רבים ושונים בספרות.

### 1.1.6 א"ש צ'רנוף $(Hoeffeding)$

**משפט 1.21** יהיו $X_1, ..., X_n$ מ"מ ב"ת כך שכל $X_i$ הוא מציין של אירוע (מקבל ערכי $0, 1$). נסמן $X = \sum_{i=1}^{n} X_i$, $\mu = \mathbb{E}\left[X\right]$. אזי:

$$\forall \delta > 0 \qquad Pr\left(X \geq (1+\delta)\,\mu\right) \leq \left(\frac{e^{\delta}}{(1+\delta)^{1+\delta}}\right)^{\mu} \tag{1}$$

$$\forall 1 > \delta > 0 \qquad Pr\left(X \leq (1-\delta)\,\mu\right) \leq \left(\frac{e^{-\delta}}{(1-\delta)^{1-\delta}}\right)^{\mu} \tag{2}$$

**הוכחה:** נוכיח את אי השיוויון הראשון, השני מוכח באופן דומה.
שוב נבחר פרמטר $t > 0$.

$$(*)\, Pr\left(X \geq a\right) = Pr\left(e^{tX} \geq e^{ta}\right) \overset{Markov}{\leq} \frac{\mathbb{E}\left[e^{tX}\right]}{e^{ta}},\ a = (1+\delta)\,\mu$$

באופן דומה למקרה של ההליכה המקרית, $X_i$ ב"ת, ולכן:

$$\mathbb{E}\left[e^{tX}\right] = \prod_{i=1}^{n} \mathbb{E}\left[e^{tX_i}\right]$$

אם $X_i$ מציין של מאורע המתרחש בהסתברות $p_i$:

$$\mathbb{E}\left[e^{tX_i}\right] = p_i e^t + (1-p_i)\cdot e^0 = 1 + p_i\left(e^t - 1\right)$$

כפי שהביטוי כתוב קשה להעריכו, על כן נשתמש בעובדה כי לכל $x$, $1 + x \leq e^x$, ונקבל:

$$\begin{aligned}
&\mathbb{E}\left[e^{tX_i}\right] \leq e^{p_i\left(e^t-1\right)} \\
&\Rightarrow \mathbb{E}\left[e^{tX}\right] = \prod_{i=1}^{n} \mathbb{E}\left[e^{tX_i}\right] \leq \prod_{i=1}^{n} e^{p_i\left(e^t-1\right)} = e^{\left(\sum_{i=1}^{n} p_i\right)\left(e^t-1\right)} \\
&(**)\, \mathbb{E}\left[X_i\right] = p_i \Rightarrow \mathbb{E}\left[X\right] = \mu = \sum_{i=1}^{n} p_i \\
&\Rightarrow \mathbb{E}\left[e^{tX}\right] \leq e^{\mu\cdot\left(e^t-1\right)} \\
(*)+(**) &\Rightarrow Pr\left(X \geq (1+\delta)\,\mu\right) \leq e^{\mu\left(e^t-1\right)-t+(1+\delta)\mu} \\
&= e^{\mu\left(e^t-1-t(1+\delta)\right)}
\end{aligned}$$

והמינימום מתקבל בנקודה $t = \ln(1+\delta)$. נציב ונקבל:

$$Pr\left(X \geq \mu\left(1+\delta\right)\right) \leq e^{\mu\cdot[\delta-\ln(1+\delta)\cdot(1+\delta)]} = \left(\frac{e^{\delta}}{(1+\delta)^{1+\delta}}\right)^{\delta}$$

■

הביטוי שקיבלנו הוא שבר עבור כל $\delta$ והולך וקטן אקספוננציאלית.

**הערה 1.22** ישנו אוסף שלם של משפטים למקרים פרטיים של המשפט הנ"ל, כאשר הטריק המרכזי נשאר - המעבר בין ההסתברות $Pr\left(X \geq a\right)$ להסתברות $Pr\left(e^{tX} \geq e^{ta}\right)$, ואי השיוויון המתקבל כתוצאה ממרקוב - $\frac{\mathbb{E}\left[e^{tx}\right]}{e^{ta}}$, והוא מפתיע בכוחו! יש סיבה שהטריק הזה חזק כל כך:

$$\begin{aligned}
e^{tX} &= \sum_{k=1}^{\infty} \frac{(tX)^k}{k!} \\
\Rightarrow \mathbb{E}\left[e^{tX}\right] &= \sum_{k=1}^{\infty} \frac{t^k \cdot \mathbb{E}\left[X^k\right]}{k!}
\end{aligned}$$

למעשה הביטוי הזה משקלל מומנטים יותר גבוהים באיזושהיא צורה שטובה לנו בתחום הזה - שכן ראינו שככל שהמומנט גדול יותר אנו מקבלים דיוק גדול יותר (המעבר ממרקוב לצ'בישב למשל).

ננסח (לפחות חלק) מהמשפטים הנ"ל, אך לא נעבור על ההוכחות שלהם.
בתנאים דומים לתנאי המשפט נקבל:

$$1.\forall 0<\delta<1\ Pr\left(X\geq(1+\delta)\mu\right)\leq e^{-\frac{\mu\delta^2}{2}}$$
$$2.\forall 0<\delta<1\ Pr\left(X\leq(1-\delta)\mu\right)\leq e^{-\frac{\mu\delta^2}{2}}$$
$$3.\forall R\geq 6\mu\ Pr\left(X\geq R\right)\leq 2^{-R}$$

לצורך אי שיוויון נוסף, נתבונן בהליכה המקרית המורכבת מ"מ $X_1,...,X_n$ ב"ת המקבלים בהסתברות $\frac{1}{2}$ את הערכים $(\pm 1)$, ונגדיר $F_k=\sum_{i=1}^{k}X_i$. נתבונן בסדרת המ"מ $F_k$ $k=1,...,n$, ונוסיף $F_0=0$.

$$\mathbb{E}\left[F_k|F_{k-1},...,F_0\right]=F_{k-1}$$

סדרת משתנים מקריים כזו נקראת Martingale. אם למרטינגייל $\{F_k\}_{k=1}^{n}$ מתקיים:

$$|F_k-F_{k-1}|\leq c_k$$

(כמעט בוודאות), כאשר בדוגמא שלנו $c_k=1$, אזי **הלמה של** $Azuma$ נותנת חסם על הריכוז של $F_n$:

$$Pr\left(F_n-F_0\geq t\right)\leq e^{\frac{-t^2}{2\left(\Sigma_{k=1}^{n}c_k^2\right)}}$$

עבור ההליכה המקרית,

$$n=\sum_{k=1}^{n}c_k^2\leq e^{-\frac{t^2}{2n}}$$

אי שיוויון דומה:

$$Pr\left(F_n-F_0\leq -t\right)\leq e^{\frac{-t^2}{2\left(\Sigma_{k=1}^{n}c_k^2\right)}}$$

## 1.2 מרחבי הסתברות אחרים

נביט במשתנה גיאומטרי, ונטיל אינסוף מטבעות. נרצה לטעון למשל כי בהסתברות 1 נראה 1 - די קל לראות כי נקבל שאיפה לאפס מהר מאוד.
בתהליך הסתברותי נמשך רוצים לטעון שתכונה מסויימת מתקיימת בהסתברות כלשהיא (נניח $0,1$).
לדוגמא $\Omega=\{0,1\}^{\mathbb{N}}$ - המרחב של סדרה איסופית של הטלות מטבע.

בוחרים קבוצה חלקית $A \subset [0,1]$. מהי ההסתברות שבחירת $X$ באופן אחיד בקטע $[0,1]$ נמצאת ב־$A$? מתברר[8] כי לא ניתן להגדיר את ההסתברות הזו. מה אם נרצה להגדיר הזזה צפידה של $A$, כלומר:

$$B = A + \varepsilon = \{a + \varepsilon \,|a \in A\}$$

מה כן קורה? אפשר לחלק את הפנים של כדור תלת מימדי לשלוש קבוצות זרות[9], כך שבסיבוב כל זוג קבוצות ירכיבו את כל פני הכדור. עוד על דוגמא זו ־ בוויקיפדיה: "יש באינסוף דברים מפתיעים".

**הגדרה 1.23** תהי $\Omega$ קבוצה כלשהיא. משפחה $\mathcal{F}$ תת קבוצות של $\Omega$ (כלומר $\mathcal{F} \subset 2^{\Omega}$) נקראת $\sigma$־אלגברה מעל $\Omega$ אם:

$$1.\phi \in \mathcal{F}$$
$$2.A \in \mathcal{F} \Rightarrow \mathcal{F} \ni (\Omega \backslash A)$$
$$3.A_1, A_2, ... \in \mathcal{F} \Rightarrow \bigcup A_i \in \mathcal{F}$$

**הגדרה 1.24** מידה על $\sigma$־אלגברה $\mathcal{F}$ היא פונקציה:

$$\mu : \mathcal{F} \to \mathbb{R}^+$$

כך ש:

1. $\mu(\phi) = 0$.
2. אם $\mathcal{F} \ni A_1, ..., A_n, ...$ קבוצות זרות אזי:

$$\mu\left(\bigcup_i A_i\right) = \sum_i \mu(A_i)$$

**הגדרה 1.25** המידה נקראת מידת הסתברות אם $\mu(\Omega) = 1$.

ניתן להגדיר $\sigma$־אלגברה בעזרת **בסיס**, כלומר אוסף $E$ של קבוצות חלקיות ל־$\Omega$ כך ש־$\sigma$־אלגברה הקטנה ביותר המכילה את $E$ נותנת את ה־$\sigma$־אלגברה המקורית.
למשל, דרך להגדיר מידת הסתברות (**ההסתברות האחידה**) על הקטע $[a,b]$:

$$E = \{(c,d) \,|a \le c < d \le b\}$$

---

[8] עוד על כך בתורת המידה

[9] אפשר להראות קיום של קבוצות אלו בעזרת אקסיומת הבחירה, זוהי לא בניה קונטרוקטיבית.

בתור בסיס. אפשר להגדיר מידה על ה־$\sigma$־אלגברה הנוצרת באופן הבא ־ תחילה, נותנים מידה לכל קטע:

$$\mu\left((c,d)\right)=\frac{d-c}{b-a}$$

לכל קבוצה ב־$\sigma$־אלגברה אפשר להגדיר מידה חיצונית:

$$\mu^{*}\left(A\right)=inf\left\{\sum_{i=1}^{\infty}\mu\left(E_i\right)\middle|E_i\text{ basis groups, }A\subset\bigcup_{i=1}^{\infty}E_i\right\}$$

ובאופן דומה מידה פנימית:

$$\mu_{*}\left(A\right)=sup\left\{\sum_{i=1}^{\infty}\mu\left(E_i\right)\middle|E_i\text{ foreign basis groups, }A\subset\bigcup_{i=1}^{\infty}E_i\right\}$$

קבוצה $A$ נקראת מדידה אם:

$$\mu_{*}\left(A\right)=\mu^{*}\left(A\right)$$

ראינו שתי דוגמאות ־ קטע על הישר, ואוסף הסדרות האינסופיות. "כל הקבוצות היפות הן מדידות". לא נביא דוגמא לקבוצה לא מדידה, אולם ניתן להוכיח קיום קבוצה שכזו.
נגדיר קבוצות בסיס למרחב $\{0,1\}^{\mathbb{N}}$ ־ נביט בקבוצות מהצורה:

$$\{0,1\}^{k}\ni a_1,...,a_k,\ E_{a_1,...,a_k}=\{(x_1,...,x_k,x_{k+1},...,x_n,...)\,|x_1=a_1,x_2=a_2,...,x_k=a_k\}$$

כדי לקבל מרחב מידה, יש לקבוע על כל קבוצת בסיס את המידה הבאה:

$$\mu\left(E_{a_1,...,a_k}\right)=\frac{1}{2^k}$$

כאשר הבסיס למרחב הוא אוסף כל הקבוצות $E_{a_1,...,a_k}$ לכל $k\geq 0$, $\{0,1\}^{k}\ni a_1,...,a_k$.

בדרך דומה, בהנתן שני מרחבי הסתברות $(\Omega_1,\mu_1)$ , $(\Omega_2,\mu_2)$, ניתן להרחיב מרחב הסתברות על המכפלה $\Omega_1\times\Omega_2$ בעזרת **מידת המכפלה**:
קבוצות הבסיס תהיינה $E_1\times E_2$, כאשר $E_i$ קבוצות בסיס ב־$\Omega_i$ (או סתם קבוצה מדידה כלשהיא), וכן:

$$\mu\left(E_1\times E_2\right)=\mu_1\left(E_1\right)\times\mu\left(E_2\right)$$

לדוגמא:

$$[0,1]^{n}\Rightarrow[a,b]\times[c,d]$$

### 1.2.1 דוגמא אחרונה למשפט ריכוז - משפט הגבול המרכזי

אפשר להגדיר מידת הסתברות על $\mathbb{R}$:

$$g:\mathbb{R}\to\mathbb{R},\ g(x)\geq 0,\ \int_{-\infty}^{\infty} g(x)\,dx=1$$

$g$ מגדירה מידת הסתברות הניתנת לקטע $[a,b]$ את המידה:

$$\mu([a,b])=\int_a^b g(x)\,dx$$

כאשר $g$ נקראת פונקציית הצפיפות של $\mu$.
פונקציית צפיפות מעניינת היא הפונקציה הבאה:

$$\varphi(x)=\frac{1}{\sqrt{2\pi}}\cdot e^{-\frac{1}{2}x^2}$$

תרגיל לא קל באינפי הוא להוכיח כי $\int_{-\infty}^{\infty}\varphi(x)=1$. למידת ההסתברות הזו קוראית התפלגות נורמלית\גאוסיאנית. למה קוראים לה נורמלית? כי היא מופיעה בכל מקום! בתור דוגמא לכך:

**משפט 1.26** אם .. סדרה אינסופית של מ"מ ב"ת, ונסמן $\mathbb{E}[X_i]=\mu,\ Var(X_i)=\sigma^2$, אזי אם נגדיר $Y_n=\sum_{i=1}^n X_i$, $Z_n=\frac{Y_n-n\mu}{\sigma\cdot\sqrt{n}}$[10], אזי:

$$\lim_{n\to\infty} Pr[Z_n<a]=\int_{-\infty}^{\infty}\varphi(x)\,dx=:\Phi(a)$$

**מסקנה 1.27**

$$\lim_{n\to\infty} Pr[a<Z_n<b]=\int_a^b\varphi(x)\,dx$$

### 1.2.2 דוגמא לשמוש במשפט הריכוז של $Azuma$

5.11.2013

נשלים עוד דבר קטן לפני שנמשיך לנושא הבא - שימוש נוסף בלמה של אזומה. יש הרבה שימושים ללמה הזו, ולכן הניסוח המסורבל שלה.

תזכורת: נתון מרטינגייל, דהיינו ... $X_0,X_1,...,X_n,...$ סדרה של מ"מ כך שמתקיים:

$$\mathbb{E}[X_{k+1}|X_k,...,X_0]=X_k$$

נשים לב שתוחלת שווה למשתנה. מה זה אומר? לכל השמה של משתנים בצד שמאל, אפשר להסתכל על התוחלת, והיא שווה למספר $X_k$ (זה כאמור נכון לכל המספרים האפשריים).

[10] למעשה ההגדרה של $Z_n$ היא נירמול של $Y_n$ כך שהתוחלת של $Z_n$ היא 0 והשונות היא 1.

המקרים המעניינים במשפט הזה מתרחשות כאשר המשתנים תלויים לינארית (אין חובה על המ"מ להיות בת"ל).

דוגמא: נתונה פונקציה:

$$F : \Omega_1 \times ... \times \Omega_n \to \mathbb{R}$$

ונתונה התפלגות על המרחב הזה; נסמן $F(x_1, ..., x_n)$. אפשר להגדיר את המ"מ $Y_0 = \mathbb{E}[F]$. כמו כן, אפשר להגדיר משתנים חדשים:

$$\begin{aligned} &Y_1(a_1) = \mathbb{E}[F|x_1 = a_1] \\ &Y_2(a_1, a_2) = \mathbb{E}[F|x_1 = a_1, x_2 = a_2] \\ &\vdots \\ &Y_n = F \end{aligned}$$

בצורה ברורה הסדרה $Y_0, Y_1, ..., Y_n$ היא מרטינגייל. למשל:

$$\mathbb{E}[Y_1|Y_0] = Y_0$$

כי $Y_0$ קבוע, וממוצע של ממוצעים שווה לעצמו[11].

אם ידוע כי $|Y_k - Y_{k-1}| \leq c_k$ עבור $k = 1, ..., n$, אזי:

$$Pr(|Y_n - Y_0| \geq t) \leq 2e^{-\left(\frac{t^2}{2\left(\sum_{k=1}^n c_k^2\right)}\right)}$$

זו דוגמא נחמדה, אבל נרצה דוגמא מעניינת יותר. נתבונן בגרף $G\left(n, \frac{1}{2}\right)$ (באותה צורה אפשר גם $G(n, p)$).

בהנתן גרף $G$, מספר הצביעה $\chi(G)$ הוא מספר הצבעים המינימלי שבו אפשר לצבוע את קודקודי $G$ כך שכל שני קודקודים עם צלע ביניהם אינם צבועים באותו צבע. אפשר לשאול כמה מרוכז $\chi(G)$.

אם לוקחים קבוצה של קודקודים שצבועים באותו צבע, אז בין כל שניים מהם אין צלע בגרף. נתבונן בקבוצה הצבועה בצבע כלשהוא -היא אנטי קליקה בגרף המשלים! חישבנו כבר מהו גודל הקליקה המקסימלית - כבר הראינו שאין קליקה בגודל יותר מ־$\log n$ (כפול קבוע כלשהוא) כמעט בוודאות בגרף המקורי. לכן עבור $p$ קבוע, מספר הצבעים הדרוש הוא $\Omega\left(\frac{n}{\log n}\right)$ כמעט בוודאות.

נראה שמספר הצביעה בגרף הוא אכן מרוכז - נראה סדר של $\sqrt{n}$. מתקיים:

$$\chi : \text{Graph collection} \to \mathbb{R}$$

וזו פונקציה $\chi : \{0,1\}^{\binom{n}{2}} \to \mathbb{R}$, כאשר הנתון הוא וקטור מציין של צלעות הגרף (כך ניתן להגדיר את הגרף). נגדיר:

$$Y_0, ..., Y_{\binom{n}{2}}$$

[11] אפשר לבצע את החישובים במדויק בכדי להיווכח.

כאשר $Y_0$ הוא התוחלת של $\chi(G)$, והסדרה מהווה מרטינגייל כפי שכבר ראינו.
נשים לב כי $|Y_{k+1} - Y_k| \geq 1$ כי כל צלע נוגעת רק בשני קודקודים שונים, ואת אחד מהם ניתן תמיד לצבוע בצבע נוסף מיוחד.
לכן נקבל:

$$Pr\left(\left|\overbrace{\chi(G)}^{Y_n} - \overbrace{\mathbb{E}[\chi(G)]}^{Y_0}\right| \geq t\right) \leq 2e^{-\left(\frac{t^2}{2\binom{n}{2}}\right)}$$

ולכן $t = \omega(n)$ נקבל הסתברות שואפת לאפס.
הצעה לשיפור - נגדיר את המרטינגייל בצורה יותר קצרה - בכל שלב לא נגלה רק את הצלע, אלא נבחר קודקוד ונגלה את כל הצלעות המחוברות אליו שלא התגלו עד עכשיו.
**תרגיל**: הראו כי מרטינגייל דומה (כנתון בהסבר) באורך $n$ יתן ריכוז טוב יותר - נקבל $t = \omega(\sqrt{n})$ - ההסתברות זניחה (כיוון שהתוחלת היא גדולה - $\Omega\left(\frac{n}{\log n}\right)$, הסבירות שנסטה היא קטנה, כלומר הריכוז הוא באמת סביב התוחלת).
אם $p$ קטן, למשל $p = \frac{1}{n^\alpha}$ עבור $\alpha < 1$, מתברר משהו די מדהים - לא רק שיש ריכוז, $\chi(G)$ הוא כמעט בוודאות למספר אחד[12].

## 1.3 תרגולים

15.10.2013 תרגול

**דוגמא - משתנה מקרי גיאומטרי**

יהי פלוני תלמיד מאסטר. ע"מ לסיים את התואר, פלוני צריך לכתוב תזה, ועל מנת לעשות זאת הוא זקוק להשראה. נניח שבכל יום הסיכוי של פלוני לקבל השראה היא $p = \frac{1}{300}$.

1. מה תוחלת מספר הימים עד שפלוני מקבל השראה?
2. מה הסיכוי שזה יקרה עד תום שנתיים (730 ימים)?

נגדיר את מרחב ההסתברות, כאשר $s$ משמעו inspiration has Struck:

$$\Omega = \left\{ n^k s \middle| \, k \in \mathbb{N} \cup \{0\} \right\}, \; Pr\left(n^k s\right) = (1-p)^k p$$

נגדיר מ"מ $X$ = מספר הימים עד לקבלת השראה.

$$Pr(X = i) = (1-p)^{i-1} \cdot p$$
$$\Rightarrow \mathbb{E}[X] = \sum_{i=1}^{\infty} i(1-p)^{i-1} \cdot p = p \cdot \sum_{i=1}^{\infty} i \cdot (1-p)^{i-1}$$

נסמן $t = 1 - p$. אזי:

$$\left(\sum_{i=1}^{\infty} i \cdot t^{i-1}\right) = \left(\sum_{i=1}^{\infty} t^i\right)' = \left(\frac{t}{1-t}\right)' = \left(\frac{1}{(1-t)^2}\right)$$
$$\Rightarrow \mathbb{E}[X] = p \cdot \frac{1}{p^2} = \frac{1}{p}$$

[12] מספר כלשהוא, כלומר $\pm 1$ מהמספר הזה.

אפשר לעשות זאת ישירות מההגדרה, אבל בשביל הדגמה נראה איך נותנים את התשובה לשאלה השניה מאי שיוויון צ'בישב- נחשב תחילה את השונות של $X$:

$$Var\left[X\right]=\mathbb{E}\left[X^2\right]-\overbrace{\left(\mathbb{E}\left[X\right]\right)^2}^{\left(\frac{1}{p}\right)^2}$$

חוק הסטטיסטיקאי חסר ההכרה קובע:

$$\mathbb{E}\left[f\left(X\right)\right]=\sum_x f\left(x\right)Pr\left(X=x\right)$$

ומכאן נקבל:

$$\mathbb{E}\left[X^2\right]=\sum_{i=1}^{\infty}i^2\cdot\left(1-p\right)^{i-1}\cdot p=p\cdot\overbrace{\sum_{i=1}^{\infty}i^2\cdot t^{i-1}}^{=*}$$

נזכר בזהות הבאה:

$$i^2=1+3+5+...+\left(2i-1\right)$$

ומכאן[13]:

$$*=\sum_{i=1}^{\infty}\left(\sum_{j=1}^{i}\left(2j-1\right)\right)\cdot t^{i-1}=\sum_{i=1}^{\infty}\sum_{j=1}^{i}\left(\left(2j-1\right)\cdot t^{i-1}\right)=\sum_{j=1}^{\infty}\sum_{i=j}^{\infty}\left(2j-1\right)t^{i-1}$$

$$=\sum_{j=1}^{\infty}\left(2j-1\right)\sum_{i=j}^{\infty}t^{i-1}=\frac{1}{1-t}\cdot\sum_{j=1}^{\infty}\left(2j-1\right)t^{j-1}=\frac{1}{1-t}\left(2\cdot\overbrace{\sum_{j=1}^{\infty}j\cdot t^{j-1}}^{\frac{1}{\left(1-t\right)^2}}-\overbrace{\sum_{j=1}^{\infty}t^{j-1}}^{\frac{1}{1-t}}\right)=\frac{2-\left(1-t\right)}{\left(1-t\right)^3}$$

$$\Rightarrow\mathbb{E}\left[X\right]=\frac{2-p}{p^2}$$

$$\Rightarrow Var\left[X\right]=\frac{2-p}{p^2}-\frac{1}{p^2}=\frac{1-p}{p^2}$$

ואם נציב את המספרים נקבל:

$$Var\left[X\right]=\frac{1-p}{p^2}=\frac{1-\frac{1}{300}}{\frac{1}{90000}}=89700$$

נשתמש בא"ש צ'בישב על מנת להעריך הם לפלוני תהיה השראה לפני תום השנתיים:

$$Pr\left(X\geq 730\right)=Pr\left(\left|X-300\right|\geq 430\right)\leq\frac{89700}{\left(430\right)^2}\sim 0.48...$$

[13] עצה מצור: כשרוצים להעריך טור, נסו להחליף את סדר הסכימה, "זה בדר"כ עוזר".

כלומר, החסם לא משהו.
ננסה להשתמש באי"ש מרקוב:

$$Pr\left(X \geq 730\right) \leq \frac{\mathbb{E}\left[X\right]}{730} = \frac{300}{730}$$

וזה כבר יותר טוב.
נחשב ישירות:

$$Pr\left[X \geq 730\right] = \sum_{i=730}^{\infty} Pr\left(X = i\right) = \sum_{i=730}^{\infty} \left(1-p\right)^{i-1} \cdot p = p \cdot \sum_{i=730}^{\infty} \left(1-p\right)^{i-1}$$
$$= p \cdot \frac{\left(1-p\right)^{730}}{1-\left(1-p\right)} = \left(1-p\right)^{730}$$

ומקירוב טיילור נקבל תוצאה שאנחנו מכירים:

$$\left(1 - \frac{1}{300}\right)^{730} \simeq e^{-\frac{730}{300}} = 0.087...$$

22.10.2013 תרגול דהיינו הסיכוי לא להצליח מאוד נמוך, ועל כן הסיכוי להצליח גדול!

**הגדרה 1.28** מספר רמזי $R\left(s,t\right)$ הוא המספר המינימלי $n$ כך שכל צביעה של צלעות הגרף המלא $K_n$ באדום ובכחול מכילה קליקה אדומה בגודל $s$ או קליקה כחולה בגודל $t$.

**טענה 1.29**

$$R\left(3,3\right) = 6$$

**הוכחה:** נראה צביעה של $K_5$ בלי משולש: *איור*
צביעה של $K_6$ - הסבר בעל פה ובציור - מ־$x$ יוצאות שלוש צלעות (בה"כ) כחולות לפחות. אם אחת מהצלעות בין הקודקודים היא כחולה, אז מצאנו משולש כחול. אחרת כל הצלעות אדומות, ואז נוצר משולש אדום. ■

ידוע כי $R\left(4,4\right) = 18$. שאלה פתוחה: $R\left(5,5\right) =?$. ידוע כי:

$$43 \leq R\left(s,s\right) \leq 49$$

בכיתה הגדרנו את $X$ להיות מספר ה־$K_4$ ב־$G$, וראינו כי אם $p$ קטן המספר הוא 0. נפרמל את השיטות בהן השתמשנו:

**טענה 1.30** יהי $X_n$ מ"מ שלם ואי שלילי. אז אם $\mathbb{E}\left[X\right] \to 0$, אז $Pr\left(X=0\right) \to 1$.

**הוכחה:**

$$Pr\left(X > 0\right) = Pr\left(X \geq 1\right) \leq \frac{\mathbb{E}\left[X\right]}{1} \to 0$$

■

**טענה 1.31** אם $\frac{Var(X)}{(\mathbb{E}[X])^2} \to 0$, אז לכל $\varepsilon > 0$:

$$Pr\left((1-\varepsilon)\,\mathbb{E}\left[X\right] \le X \le (1+\varepsilon)\,\mathbb{E}\left[X\right]\right) \to 1$$

**הוכחה:** לפי מרקוב:

$$Pr\left(\left|X - \mathbb{E}\left[X\right]\right| \ge \varepsilon \cdot \mathbb{E}\left[X\right]\right) \le \frac{Var\left(X\right)}{\varepsilon^2 \cdot \mathbb{E}\left[X\right]^2} \to 0$$

■

### 1.3.1 חסמים על $\binom{2m}{m}$

**טענה 1.32**

$$\frac{2^{2m}}{4\sqrt{m}} \le \binom{2m}{m} \le 2^{2m}$$

**הוכחה:** הצד הימני טריוויאלי:

$$(1+1)^{2m} = \sum_{k=0}^{2m} \binom{2m}{k} = 2^{2m} \Rightarrow \binom{2m}{m} \le 2^{2m}$$

נוכיח את הצד השמאלי: נראה ש־$\binom{2m}{m} \ge \binom{2m}{k}$:

$$\frac{(2m)!}{m!m!} \overset{?}{\ge} \frac{(2m)!}{k!\,(2m-k)!}$$

נניח בה"כ כי $k < m$. לאחר צמצום צ"ל:

$$\frac{1}{m \cdot (m-1) \cdot \ldots \cdot (k+1)} \overset{?}{\ge} \frac{1}{(2m-k) \cdot \ldots \cdot (m+1)}$$

כל הגורמים בצד ימין גדולים מהגורמים בצד שמאל, ולכן אי השיוויון מתקיים. כעת:

$$\sum_{k=0}^{2m} \binom{2m}{k} \le (2m+1)\binom{2m}{m} \Rightarrow \binom{2m}{m} \ge \frac{2^{2m}}{m+1}$$

נשתמש בהתפלגות של משתנה בינומי:

$$X \sim B\left(n,p\right) \Rightarrow \mathbb{E}\left[X\right] = n{\cdot}p,\ Var\left(X\right) = n{\cdot}p\left(1-p\right),\ Pr\left(X=k\right) = \binom{n}{k} p^k \left(1-p\right)^{n-k}$$

נביט ב־$X \sim B\left(2m, \frac{1}{2}\right)$:

$$\mathbb{E}[X] = m,\ Var(X) = 2m \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{m}{2},\ Pr(X = k) = \binom{2m}{k} \left(\frac{1}{2}\right)^{2m}$$

מאי שיוויון צ'בישב:

$$Pr\left(|X - m| \geq \sqrt{m}\right) \leq \frac{\frac{m}{2}}{m} = \frac{1}{2}$$

כעת:

$$\sum_{k=m-\sqrt{m}+1}^{m+\sqrt{m}} \binom{2m}{k} \left(\frac{1}{2}\right)^{2m} = Pr\left(m - \sqrt{m} < X < m + \sqrt{m}\right) \overset{Chevichev}{\geq} \frac{1}{2}$$

$$\Rightarrow \left(\frac{1}{2}\right)^{2m} \left(2\sqrt{m} - 1\right) \binom{2m}{m} \geq \sum_{k=m-\sqrt{m}}^{m+\sqrt{m}} \binom{2m}{k} \left(\frac{1}{2}\right)^{2m} \geq .. \geq \frac{1}{2}$$

$$\Rightarrow \binom{2m}{m} \geq \frac{2^{2m}}{2\left(2\sqrt{m} - 1\right)} \geq \frac{2m}{4\sqrt{m}}$$

■

"האמת היא שהחישוב למעלה קצת מטופש - כי אפשר פשוט להציב בנוסחאת שטרלינג":

$$n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n \Rightarrow \frac{2^{2m}}{\sqrt{\pi m}}$$

29.10.2013 תרגול

אבל המתרגל רצה להראות שימוש בחומר, כי נצטרך להשתמש בו בתרגיל.
בשבוע הבא בסוף התרגול יהיו שתי שאלות - ניסוח משפט מהרצאה או תרגול, או הגדרת מושג.

### 1.3.2 שימוש קומבינטורי לא"ש צ'רנוף

**משפט 1.33** כמעט לכל הגרפים יש קוטר 2, כלומר, אם $G$ נדגם באופן מקרי (כלומר הסתברות אחידה) מקבוצת כל הגרפים על $n$ קודקודים, אז:

$$Pr(diam(G)) = 2 \overset{n\to\infty}{\longrightarrow} 1$$

**הגדרה 1.34** קוטר של גרף זה המרחק המקסימלי בין שני קודקודים בגרף (אם הגרף לא קשיר, הקוטר מוגדר להיות אינסופי).

**הוכחה:** אינטואיציה: נסתכל על שני קודקודים: בהסתברות $\frac{1}{2}$ אין ביניהם צלע. נסתכל על קודקודי הביניים (בין שני הקודקודים המקוריים). כדי שיהיה מסלול דרך אחד מהם, צריך ששתי הצלעות המתאימות יתקיימו, וזה מתרחש בהסתברות $\frac{1}{4}$ לכל קודקוד ביניים. באמצעות חסם צרנוף נחסום את האפשרות שלא קיים כזהץ

**הערה 1.35** $G_{n,\frac{1}{2}}$ זו התפלגות אחידה על פני כל הגרפים עם $n$, קודקודים, וכן:

$$Pr\left(G\right)=\left(\frac{1}{2}\right)^{\left(\begin{array}{c}n\\2\end{array}\right)}$$

נתחיל מבחינת ההסתברות שהקוטר שווה לאחד:

$$Pr\left(diam\left(G\right)=1\right)=Pr\left(G=K_n\right)=\left(\frac{1}{2}\right)^{\left(\begin{array}{c}n\\2\end{array}\right)}\to 0$$

כעת, נראה כי ההסתברות שהקוטר גדול מ־2 שואפת לאפס:
נקבע שני קודקודים $u,v$. נגדיר מ"מ $X_{u,v}$ להיות מספר המסלולים באורך 2 בין $u$ ל־$v$.
לכל קודקוד אחר $w\in V\backslash\left\{u,v\right\}$ נגדיר מ"מ מציין $X_{u,v}^{w}$ באופן הבא:

$$X_{u,v}^{w}=\begin{cases}1 & \left\{u,w\right\},\left\{v,w\right\}\in E\\0 & otherwise\end{cases}$$

נשים לב כי ל־$u,v$ קבועים, $\left\{X_{u,v}^{w}\right\}_{w\in V\backslash\left\{u,v\right\}}$ הם ב"ת. כמו כן, מ"מ אלו הם שווי התפלגות:

$$Pr\left(X_{u,v}^{w}=1\right)=\frac{1}{4}\Rightarrow\mathbb{E}\left[X_{u,v}^{w}\right]=\frac{1}{4}$$

יתרה על כן,

$$X_{u,v}=\sum_{w}X_{u,v}^{w},\ \mathbb{E}\left[X_{u,v}\right]=\sum_{w}\mathbb{E}\left[X_{u,v}^{w}\right]=\frac{n-2}{4}$$

נזכר באי"ש צ'רנוף בניסוח האהוב על המתרגל:
אם $X=\sum_i X_i$, $X_i$ מ"מ מציינים וב"ת, וכן נסמן $\mathbb{E}\left[X\right]=\mu$, אזי:

$$1.Pr\left(X\geq\left(1+\delta\right)\mu\right)\leq e^{-\frac{\delta^2\mu}{3}}$$
$$2.Pr\left(X\geq\left(1-\delta\right)\mu\right)\leq e^{-\frac{\delta^2\mu}{2}}$$

במקרה שלנו, לכל $0<\delta<1$:

$$Pr\left(X_{u,v}=0\right)\leq Pr\left(X_{u,v}\leq\left(1-\delta\right)\cdot\frac{n-2}{4}\right)\leq e^{\frac{-\delta^2(n-2)}{8}}$$
$$\Rightarrow Pr\left(X_{u,v}=0\right)\leq e^{\frac{-(n-2)}{8}}$$

עם א"ש צ'בישב, היינו יכולים לעשות חישוב דומה אך היינו מקבלים פונקציה השואפת לאפס בצורה פולינומית, ואז מה שנעשה הלאה - חסם על האיחוד לא היה עובד. בעזרת צ'רנוף לעומת זאת קיבלת שאיפה אקספוננציאלית, שתאפשר לנו את הצעד שאנו צריכים.

$$Pr\left(diamG>2\right)=Pr\left(\bigcup_{\left\{u,v\right\}}\left\{X_{u,v}=0\right\}\right)\leq\sum_{\left\{u,v\right\}}Pr\left(X_{u,v}=0\right)\leq\left(\begin{array}{c}n\\2\end{array}\right)\cdot e^{-\frac{(n-2)}{8}}\overset{n\to\infty}{\longrightarrow}0$$

■

בתרגיל נוכיח את הסף ב־$G_{n,p}$ לקשירות. הרעיון: אם $p$ גדול, לעבור על כל $S \subseteq V$ עבור $|S| \leq \frac{n}{2}$ ולהראות בעזרת צ'רנוף כי ההסתברות שאין מ־$S$ צלעות יוצאות נורא קטנה. אז צריך לעשות חסם איחוד (כמו למעלה) על פני כל ה־$S$־אים.

### 1.3.3 משתנים מקריים רציפים

לא כל המ"מ הם רציפים או בדידים; יש כאלה שלא זה ולא זה, "וזה בסדר".

**הגדרה 1.36** מ"מ $X : \Omega \to \mathbb{R}$ נקרא רציף אם יש פונקציה (פונקציית צפיפות):

$$f : \mathbb{R} \to \mathbb{R}^+ \cup \{0\}$$

מגדירים:

$$Pr\left(X \in [a,b]\right) = \int_a^b f\left(x\right) dx$$

והתוחלת:

$$\mathbb{E}\left[X\right] = \int_{-\infty}^{\infty} x f\left(x\right) dx$$

**דוגמא - מ"מ אוניפורמי** מ"מ אוניפורמי הוא מ"מ רציף שפונקציית הצפיפות שלו היא:

$$f\left(x\right) = \begin{cases} \frac{1}{b-a} & a \leq x \leq b \\ 0 & otherwise \end{cases}$$

ונסמן: $X \sim U\left([a,b]\right)$.
נחשב את התוחלת ואת השונות של מ"מ שכזה:

$$\mathbb{E}\left[X\right] = \int_{-\infty}^{\infty} x f\left(x\right) = \int_a^b \frac{x}{b-a} = \frac{1}{b-a}\left(\frac{x^2}{2}\right)\Big|_a^b = \frac{b^2-a^2}{2\left(b-a\right)} = \frac{a+b}{2}$$

$$Var\left(X\right) = \mathbb{E}\left[\left(X - \mathbb{E}\left[X\right]\right)^2\right] = \mathbb{E}\left[X^2\right] - \mathbb{E}\left[X\right]^2$$

$$\mathbb{E}\left[X^2\right] = \int_{-\infty}^{\infty} x^2 f\left(x\right) = \int_a^b \frac{x^2}{b-a} = \frac{1}{b-a}\left(\frac{x^3}{3}\right)\Big|_a^b = \frac{b^3-a^3}{3\left(b-a\right)} = \frac{b^2+ab+a^3}{3}$$

$$\Rightarrow Var\left(X\right) = \frac{b^2+ab+a^3}{3} - \frac{\left(a+b\right)^2}{4} = ... = \frac{\left(b-a\right)^2}{12}$$

# 2 אלגברה לינארית ושימושיה

## 2.1 תזכורות מהעבר

### 2.1.1 הגדרות בסיסיות

**הגדרה 2.1** נתון שדה $F$, לדוגמא $F=\mathbb{R}$, $F=\mathbb{C}$, $F=\mathbb{Z}_p$ - השדה מודולו $p$.
מרחב וקטורי $V$ מעל שדה $F$ הוא מבנה עם פעולות חיבור $+$ וכפל בקבועים $\cdot$ ב-$F$ שמקיים אוסף של אקסיומות.

**דוגמאות סטנדרטיות**

1. $V=F^n$ עם חיבור בכל קואורדינטה וכפל בסקלר מתוך $F$ - מכפיל את כל האיברים.
2. נתונה קבוצה $\Omega$, $V=F^\Omega$ הינו אוסף כל הפונקציות מ-$\Omega$ ל-$F$. אם $\Omega=\{1,...,n$, אזי

$$F^\Omega \cong F^n$$

3. אוסף הפונקציות הממשיות הרציפות על הקטע $[0,1]$ הוא מרחב וקטורי מעל $\mathbb{R}$.

**הגדרה 2.2** בהנתן אוסף של וקטורים $A=\{v_i\}_{i\in I}$:

$$A\subseteq W=Span\{A\}=\left\{\sum_{k=1}^{m}a_kv_{i_k}\middle|\ v_{i_k}\in A,\ a_k\in F\ \forall m\right\}$$

כאשר $W$ בעצמו שדה וקטורי. אזי $V\supseteq W$ הוא תת מרחב הנפרש ע"י קבוצת הוקטורים $A$ והוא זהה לתת המרחב הוקטורי המינימלי המכיל את $A$.

**הערה 2.3** אם $A$ אוסף סופי ההגדרה יותר פשוטה:

$$A=\{v_1,...,v_m\},\ I=\{1,...,m\}\Rightarrow Span(A)=\left\{\sum_{i=1}^{m}a_iv_i\middle|\ a_i\in F\right\}$$

**הגדרה 2.4** המימד של מרחב וקטורי $V$, המסומן ב- $dim(V)$, הוא המספר המינימלי של וקטורים הפורשים את כל המרחב.

קל לראות: $dim(F^n)=n$. ע"מ שיהיה באמת קל לראות זאת, נשתמש בכמה כלים שהכרנו בקורס אלגברה לינארית.

**הגדרה 2.5** קבוצת וקטורים $v_1,...,v_m$ נקראת בלתי תלויה מעל $F$ אם (וקטור האפס)$=a_1,...,a_m$ $\sum_{i=1}^{m}a_iv_i=0\Leftrightarrow 0$, ואחרת הקבוצה נקראת תלויה לינארית מעל $F$.

**למה 2.6** אם $dim(V)=n$ אזי התנאים הבאים שקולים:

1. $Span(v_1,...,v_n)=V$.

2. $v_1, ..., v_n$ בלתי תלויה לינארית.

**הוכחה:** תרגיל פשוט באלגברה לינארית. ■

**הגדרה 2.7** ל־$v_1, ..., v_n$ מהלמה מעלה קוראים בסיס למרחב $V$.

**מסקנה 2.8** לכל $v \in V$ יש הצגה יחידה:

$$v = \sum_{i=1}^{n} a_i v_i, \ a_i \in F$$

### 2.1.2 העתקות לינאריות (Linear Transformations)

**הגדרה 2.9** יהיו $V, W$ מרחבים וקטורים מעל שדה $F$.

$$T : V \to W$$

היא העתקה לינארית אם:

$$\forall v_1, v_2 \in V T(v_1 + v_2) = T(v_1) + T(v_2)$$
$$\forall v \in V \ \forall a \in F T(av) = aT(v)$$

**דוגמא להעתקה לינארית**

נתון $V$ ממימד $n$. $v_1, ..., v_n$ בסיס ל־$V$ אם $v = \sum_{i=1}^{n} a_i v_i$. אזי ההעתקה הבאה:

$$T : V \to F^n, \ T(v) = (a_1, ..., a_n)$$

היא בבירור העתקה לינארית.

בהנתן בסיס $v_1, ..., v_n$ למרחב $V$, כדי להגדיר העתקה לינארית $T$, די להגדיר מה $T$ עושה לאיברי הבסיס:

$$i = 1, ..., n \ T(v_i) = w_i$$

ואז הרחבה לינארית היא יחידה ־ אם $v = \sum_{i=1}^{n} a_i v_i$, $a_i$ הם יחידים, ולכן:

$$T(v) = \sum_{i=1}^{n} a_i w_i$$

ואין כל דרישה לתכונות נוספות על הקבוצה $w_1, ..., w_n$ חוץ מכך שהם וקטורים ב־$W$.

**דוגמא נוספת להעתקה לינארית**

יהי $V_n$ אוסף הפולינומים ממעלה $\leq n-1$ מעל הממשיים.
פולינום נקבע ע"פ מקדמיו:

$$p(x) = a_0 + a_1 x + ... + a_n x^{n-1}$$

ולכן $dim(V_n) = n$.
אם נסתכל על פונקציית הגזירה הסטנדרטית מעל הממשיים:

$$D(p(x)) = p'(x)$$

כללי הגזירה אומרים לנו כי $D : V_n \to V_{n-1}$ העתקה לינארית, כאשר $D\left(x^k\right) = kx^{k-1}$ עבור $k = 0, ..., n-1$ מגדיר את הפעולה על $V_n$.

אם בוחרים בסיס $v_1, ..., v_n$ למרחב ממימד $n$ ־ $V$, ובסיס $w_1, ..., w_m$ למרחב $W$, אזי אם $T : V \to W$ טרנספורמציה לינארית:

$$V \cong F^n,\ W \cong F^m$$
$$\Rightarrow T = \sum_{i=1}^{m} a_{ik} w_i$$

נביט במטריצה הבאה:

$$\begin{pmatrix} \overbrace{a_{11}}^{T(v_1)} & \cdots & \overbrace{a_{1n}}^{T(v_n)} \\ \vdots & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} = A$$

אז הוקטור $A \begin{pmatrix} \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \end{pmatrix} = \begin{pmatrix} a_{1k} \\ \vdots \\ a_{mk} \end{pmatrix} = T(v_k)$, ובאופן כללי $A$ מגדירה העתקה ע"י כפל מטריצה בוקטור $A : F^n \to F^m$, וזו העתקה המתאימה ל־$T$ עבור $v_1, ..., v_n$ ו־$w_1, ..., w_m$, ולהפך ־ $A$ כזאת קובעת $T$.

**הגדרה 2.10** תהי $T : V \to W$ טרנספורמציה לינארית. הגרעין של $T$, או הקרנל (Kernel) מוגדר להיות:

$$Ker(T) := \{ v \in V | \, T(v) = 0 \}$$

וזהו תת מרחב של $V$.
הטווח של $T$ מוגדר להיות:

$$Im(T) := \{ w \in W | \, \exists v \in V \ T(v) = w \}$$

וזהו תת מרחב של $W$.

**הגדרה 2.11** הדרגה של הטרנספורמציה $T$ הינה:

$$Rank\left(T\right)=dim\left(Im\left(T\right)\right)$$

וידוע:

$$dim\left(Ker\left(T\right)\right)+Rank\left(T\right)=dim\left(V\right)$$

**הגדרה 2.12** אם בוחרים בסיסים ב־$V$ ו־$W$, אזי הדרגה של המטריצה $A$ המתאימה ל־$T$ היא דרגת $T$.

זו דרך אחת להגדיר את הדרגה של מטריצה. דרכים שקולות אחרות להגדרת דרגת מטריצה $A$ (מסדר $m\times n$):

1. מספר מקסימלי של שורות בלתי תלויות לינארית.
2. מספר מקסימלי של עמודות בלתי תלויות לינארית.
3. בהנתן שני וקטורים $x=\begin{pmatrix}x_1\\ \vdots\\ x_m\end{pmatrix}$, $y=\begin{pmatrix}y_1\\ \vdots\\ y_n\end{pmatrix}$, ומטריצה מדרגה 1:

$$B=x\cdot y^T=\begin{pmatrix}x_1\\ \vdots\\ x_m\end{pmatrix}(y_1,...,y_n)$$

וכל מטריצה מדרגה 1 מתקבלת כך. מסמנים גם $B=x\otimes y$ "המכפלה הטנזורית של $x$ ו־$y$". אזי הדרגה של $A$ הוא המספר המינימלי של מטריצות $B_1,...,B_r$ מדרגה 1 כך שסכומם שווה ל־$A$:

$$A=B_1+...+B_r$$

### 2.1.3 מטריצות וערכים עצמיים

כאן נדון בשדות $F=\mathbb{R},\mathbb{C}$.
תהי $A\in M_n\left(\mathbb{C}\right)$ מטריצה מסדר $n\times n$ מעל המרוכבים. אפשר לחשוב על $A$ כעל טרנספורמציה לינארית מ־$\mathbb{C}^n$ אל עצמו (בוחרים בסיס סטנדרטי).
איך נראית טרנספורמציה לינארית? מה היא עושה? אולי מעל המרוכבים זה פחות טבעי (יותר "הגיוני" מעל הממשיים), אולם לצורך זה נשתמש בכלי שאנו כבר מכירים:

**הגדרה 2.13** נאמר שוקטור $x\neq 0\in\mathbb{C}^n$ הוא וקטור עצמי של $A$ עם ערך עצמי $\lambda\in\mathbb{C}$ אם $Ax=\lambda x$.

המשמעות הגיאומטרית כאן היא שכפל במטריצה $A$ היא למעשה מותחת\מכווצת ו\או מסובבת את הו"ע במרחב (שכן כל רכיבי הוקטור מוכפלים באותו גורם $\lambda$שהוא הע"ע). במרוכבים יכול להיות שמסובבים את הוקטור סביב כל המעגל (מעל הממשיים אפשר לסובב לכיוון ההפוך ע"י הכפלה ב־$-1$).

נרצה למצוא את הע"ע של מטריצה. נסמן את מטריצת היחידה ב־ $I = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$.

מתקיים:

$$Ax = \lambda x \Leftrightarrow (A - \lambda \cdot I)\, x = 0$$

כלומר בקרנל של המטריצה $(A - \lambda \cdot I)$ יש וקטור שאיננו אפס, ועל כן היא איננה מדרגה מלאה. אזי:

$$\Leftrightarrow det\,(A - \lambda I) = 0$$

אם נתבונן ב־$\lambda$ כמשתנה, אזי:

$$det\,(A - \lambda \cdot I) = p_A\,(\lambda)$$

כאשר הפולינום שהתקבל הוא מדרגה $n$ תמיד (האלכסון מלא ־ אין בו אפסים), ולכן $\lambda$ ע"ע של $A \Leftrightarrow p_A\,(\lambda) = 0$.

**הגדרה 2.14** $p_A\,(\lambda)$ הינו הפולינום האופייני של $A$ (Characteristic Poly).

לאחר שמצאנו את הע"ע, אפשר להציב במערכת המשוואות הלינאריות $(A - \lambda \cdot I)\, x = 0$ ולקבל את הו"ע $x$.

**מסקנה 2.15** כיוון שדרגת הפולינום האופייני $= n$, יש לכל היותר $n$ ערכים עצמיים שונים.

**מסקנה 2.16** ל־$A$ ול־$A^T$ יש אותם ע"ע.

**הערה 2.17** זאת מכיוון ו־$det\,(B) = det\left(B^T\right)$, כלומר הפולינום האופייני הוא זהה.

המקרה בו יש פחות מ־$n$ ע"ע שונים הוא מאוד מיוחד (מגביל למרחב מסויים מאוד של מטריצות), ובדר"כ לרב המטריצות יש $n$ ערכים עצמיים שונים.

**טענה 2.18** יהיו $v_1, ..., v_r$ וקטורים עצמיים של $A$ עם ערכים עצמיים $\lambda_1, ..., \lambda_r$, כאשר ה־$\lambda_i$ שונים זה מזה. אזי $v_1, ..., v_r$ בלתי תלויים לינארית.

**הוכחה:** בה"כ נניח בשלילה כי $v_1, ..., v_k$ הקבוצה הקטנה ביותר מתוך $v_1, ..., v_r$ שהיא תלויה לינארית. לכן, קיימים קבועים $c_1, ..., c_k$ כולם $\neq 0$ כך ש:

$$(1) \sum_{i=1}^{k} c_i v_i = 0$$

$$(2) \Rightarrow A\,(0) = 0 = \sum_{i=1}^{k} c_i A v_i = \sum_{i=1}^{k} c_i \lambda_i v_i$$

בה"כ $\lambda_1 \neq 0$. נכפיל ב־$\lambda_1^{-1}$ את 2 ונחסיר מ־1 ונקבל תלות קצרה יותר מ־$k$:

$$0 = \sum_{i=1}^{k} c_i \lambda_i v_i \cdot \lambda_1^{-1} = c_1 v_1 + \sum_{i=2}^{k} c_i \lambda_i \lambda_1^{-1} v_i$$
$$\Rightarrow 0 = \sum_{i=1}^{k} c_i v_i - c_1 v_1 + \sum_{i=2}^{k} c_i \lambda_i \lambda_1^{-1} v_i = \sum_{i=2}^{k} c_i \lambda_i \lambda_1^{-1} v_i$$

בסתירה מהנחת המינימליות. ■

כאמור במקרה הגנרי יש $n$ ערכים שונים, ולכן קיים בסיס למרחב המרוכב מוקטורים עצמיים.
כאמור וקטורים עצמיים מגדירים לנו סיבוב במרחב והגדלה\הקטנה. בשיעור הבא נגדיר את המושג של מרחק (כמובן ויש הרבה מאוד דרכים לעשות זאת) ונראה מה נקבל.

## 2.2 פולינומים מעל שדות סופיים

12.11.2013

**הגדרה 2.19** חוג הוא מבנה הכולל קבוצה עם פעולות חיבור וכפל, כאשר:

- שתי הפעולות אסוציאטיביות.
- פעולת החיבור היא קמוטטיבית.
- קיים איבר יחידה לגבי פעולת החיבורץ
- קיים איבר נגדי לכל איבר ביחס לפעולת החיבור.
- מתקיים חוק הפילוג (דיסטריביוטיביות).

**הערה 2.20** ההגדרה מעלה אינה סטנדרט - לעיתים מגדירים חוג כך שיש בו גם איבר יחידה כפלי. במידה וקיים כזה, אנחנו נגיד שהחוג עם יחידה.

**הערה 2.21** אם גם פעולת הכפל היא קמוטטיבית, נגיד שהחוג קמוטטיבי.

**הגדרה 2.22** בהנתן שדה $F$, חוג הפולינומים מעליו מוגדר להיות:

$$R = F[x] = \left\{ \sum_{i=0}^{d} a_i x^i \middle| a_i \in F,\ d \geq 0 \right\}$$

החוג הזה, שהוא קמוטטיבי עם יחידה, הוא ממימד אינסופי, כאשר פעולות החיבור והכפל הן כמצופה.

"מה שנחמד בחוג הזה" הוא שקיים חילוק עם שארית מעל השדה:

**הגדרה 2.23** בהנתן שני פולינומים $R \ni f(x), g(x)$, פעולת החילוק עם שארית מעל השדה $F$ מוגדרת להיות:

$$f(x) = q(x) \cdot g(x) + r(x)$$

כאשר $deg(f(x))$ היא החזקה הגבוהה ביותר של $x$ עם מקדם $\neq 0$ ב־$f(x)$, ומתקיים: $deg(g(x)) > deg(r(x))$.

**הגדרה 2.24** אם $r(x)=0$, אזי נסמן $g(x)\,|\,f(x)$ ונאמר ש־$g(x)$ מחלק את $f(x)$.

אם ל־$f(x)$ ו־$g(x)$ אין מחלק משותף מדרגה $\geq 1$[14], אם נמשיך כמו באלגוריתם של אוקלידס נוכל למצוא פולינומים $u(x),v(x)$ כך ש:

$$u(x)\cdot f(x)+v(x)\cdot g(x)=1$$

**הגדרה 2.25** פולינום $f(x)$ נקרא פולינום ראשוני אם אין לו מחלקים לא טריוויאלים מדרגה נמוכה יותר.

**הגדרה 2.26** בהנתן $p(x)$ פולינום ראשוני ב־$R=F[x]$, ונסמן $d=deg(p(x))$, נגדיר:

$$R/_{(p)}:=\left\{a_0+a_1x+...+a_{d-1}x^{d-1}\,\middle|\,a_i\in F\right\}$$

עם פעולות מודולו $p(x)$, כלומר מבצעים פעולות חיבור וכפל, ואם התוצאה דרגתה $\geq d$, לוקחים את השארית בחלוקה ב־$p(x)$.

**טענה 2.27** מכיוון ו־$p(x)$ פולינום ראשוני, נקבל כי $R/_{(p)}$ עם פעולות חישוב מודולו $p(x)$ הינו שדה[15].

**הוכחה:** על מנת שחוג יהיה שדה, יש להוכיח כי הכפל קמוטטיבי, וכי קיים איבר יחידה כפלי. העובדה שהכפל הוא קמוטטיבי היא טריוויאלית. נותר אם כך להראות כי בחוג שהגדרנו מעלה קיים איבר יחידה.

יהי $f\in R/_{(p)}$. בהכרח $deg(f)<deg(p)$. נסמן:

$$\sum_{i=0}^{d-1}a_ix^i=f(x)$$

אזי $(f(x),p(x))=1$ הוא המחלק המשותף המקסימלי ($f$ דרגתו קטנה מ־$p$, ולכן אם היה כזה שאינו קבוע אזי $p$ לא היה ראשוני).

על כן, קיימים $v(x),u(x)$ כך ש:

$$u(x)\cdot f(x)+v(x)\cdot p(x)=1$$

לאחר ביצוע $((modp(x)))$נקבל:

$$\Rightarrow u(x)\cdot f(x)+0\equiv 1\,(mod\,(p(x)))$$

כעת, $f(x)\,(mod\,(p(x)))=f(x)$. על כן (לאחר בדיקה כי בעת ביצוע מודולו $p$ "הפעולות בסדר" - כלומר החיבור והכפל נשמרות) ניתן לקבל ש:

$$\Rightarrow[u(x)\,(mod\,(p(x)))]\cdot f(x)\equiv 1\,(mod\,(p(x)))$$

דהיינו מצאנו ל־$f(x)$ הופכי כפלי, כנדרש. ■

[14] קבועים, שהם מדרגה 0, מחלקים כל דבר.

[15] אם לא היה ראשוני, היינו מקבלים עוד חוג.

### 2.2.1 כמה דוגמאות לשימושים של פולינומים מעל שדה

**שימוש ראשון - מציאת שדה ממימד כלשהוא**

אם מתחילים מ־$F=\mathbb{Z}_2$ שדה השאריות מודולו 2, ו־$p(x)$ פולינום אי פריק מדרגה $d$, נקבל שדה:

$$F[x]/p(x)$$

בשדה הזה יש $2^d$ איברים, כי יש בדיוק $2^d$ פולינומים מדרגה $\geq d-1$ עם מקדמים 0 או 1, כלומר $\{0,1\} \ni a_0, a_1, ..., a_{d-1}$.

ידוע כי לכל שדה סופי $F$ (בפרט $F=\mathbb{Z}_q$, שדה השאריות מודולו $q$ ראשוני) יש לכל קבוע $d$ פולינומים ראשוניים מדרגה $d$.

למשל, הפולינום $x^2+x+1$ הוא פולינום אי פריק מעל $F_2=\mathbb{Z}_2$.

**מסקנה 2.28** לכל ראשוני $q$ ולכל $d$ טבעי יש שדה עם $q^d$ איברים.

**דוגמא לפולינום שהינו אי פריק מעל שדה אחד, אך פריק מעל שדה אחר**

נביט בפולינום $x^2+x+1$: כפי שציינו מעלה, הוא אי פריק מעל $\mathbb{Z}_2$, אבל אם נסתכל על $F=\mathbb{Z}_2[x]/(x^2+x+1)$, $F[y] \ni y^2+y+1$ - המשמעות כאן היא שהאיברים הם מהצורה $a+bx$, $a,b \in \{0,1\}$, וכל פעם שמכפילים ומקבלים $x^2$ אזי $x^2=x+1$, דהיינו פעולת הכפל היא מהצורה:

$$\begin{aligned}(a+bx)(c+dx) &= ac+(bc+ad)x+bd\cdot x^2 \\ &= (ac+bd)+(bc+ad+bd)x\end{aligned}$$

כאשר $a,b,c,d \in \mathbb{Z}_2$.

נשים לב כי אם נציב בפולינום הזה $x$, נקבל כי פולינום פריק (ואפילו כל השורשים שלו בשדה - זה לא דבר טריוויאלי ודורש הוכחה):

$$\begin{aligned}(y+x)(y+x+1) &= y^2+(x+x+1)y+x(x+1) \\ &= y^2+y+1\end{aligned}$$

**שימוש שני - בניית פונקציות ערבול** $(Hash)$

יהי $F=F_{p^n}$ עבור $p$ ראשוני כלשהוא, ונסמן $|F|=p^n=q$. אפשר להציג פולינום:

$$f(x)=a_0+a_1x+...+a_tx^t,\ a_i \in F$$

דרך שניה להציג את הפולינום $f(x)$ היא ע"י בחירת $\alpha_0,\alpha_1,...,\alpha_t$ <u>איברים שונים</u> בשדה $F$, ולחשב את:

$$f(\alpha_0), f(\alpha_1), ..., f(\alpha_t)$$

ונסמן $\beta_k = f(\alpha_k)$. איך מחשבים זאת?

$$\begin{pmatrix} 1 & \alpha_0 & \alpha_0^2 & \cdots & \alpha_0^t \\ 1 & \alpha_1 & \alpha_{01}^2 & \cdots & \alpha_1^t \\ \vdots & & & & \\ 1 & \alpha_t & \alpha_t^2 & \cdots & \alpha_t^t \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_t \end{pmatrix} = \begin{pmatrix} f(\alpha_1) \\ f(\alpha_1) \\ \vdots \\ f(\alpha_t) \end{pmatrix}$$

המטריצה מצד שמאל $V$ היא מטריצת ון־דר־מונדה, והיא הפיכה, ונקבל:

$$det(V) = \prod_{i<j} (\alpha_i - \alpha_j) \neq 0$$

$$V \cdot \begin{pmatrix} a_0 \\ \vdots \\ a_t \end{pmatrix} = \begin{pmatrix} f(\alpha_1) \\ \vdots \\ f(\alpha_t) \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} a_0 \\ \vdots \\ a_t \end{pmatrix} = V^{-1} \cdot \begin{pmatrix} f(\alpha_1) \\ \vdots \\ f(\alpha_t) \end{pmatrix}$$

כיוון והמטריצה $V$ הפיכה, אפשר מכל בחירה של $\beta_0, ..., \beta_t$ לקבל מקדמי פולינום $f(x) = a_0 + ... + a_t x^t$ כך ש: $f(\alpha_k) = \beta_k$.

**בפרט**, כאשר קובעים את $F \ni \alpha_0, \alpha_1, ..., \alpha_t$ (איברים שונים זה מזה), אזי אם בוחרים את מקדמי $f(x) = a_0 + a_1 x + ... + a_t x^t$ בהתפלגות אחידה על $F^{t+1}$, אזי גם ה־$\beta_0, ..., \beta_t$ המתקבלים מפולגים גם הם בהתפלגות אחידה על $F^{t+1}$, $\beta_k = f(\alpha_k)$.

וכך להיפך - אם $\beta_0, ..., \beta_t$ נבחרים בהתפלגות אחידה, אזי מקדמי פולינום האינטרפולציה $a_0, ..., a_t$ מפולגים בהתפלגות אחידה על $F^{t+1}$.

בוחרים $f = a_0 + a_1 x + ... + a_t x^t$ באופן אחיד, אבל בוחרים יותר מ־$(t+1)$ נקודות הערכה: נבחר $\alpha_0, ..., \alpha_n$, כאשר $\alpha_i$ שונים זה מזה, $t+1 \leq n$. נקבל:

$$\beta_0(f(\alpha_0)), ..., \beta_n(f(\alpha_n))$$

סדרה של משתנים מקריים כך שכל אחד מהם מפולג באופן אחיד על $F$, וכל קבוצה של $t+1$ מה־$\beta$־אים הם משתנים מקריים בלתי תלויים (זה לא נכון שהם כולם בלתי תלויים - אם ניקח $t+2$, $t+1$ יקבע את הפולינום, וזה יקבע את הערך הנוסף $f(\alpha_{t+2})$).

במשל, במקרה בו $t=1$, מסתכלים על פולינום:

$$f = a_0 + a_1 x$$

עכשיו בוחרים:

$$\alpha_0, \alpha_1, ..., \alpha_N \ \ (N = 2^n)$$

כל האיברים השונים בשדה $F$.$f(\alpha_i), f(\alpha_j)$ עבור $i \neq j$ ב"ת ומפולגים באופן אחיד כאשר $a_0, a_1$ נבחרים בהתפלגות אחידה (כל אחד מהם בעל $n$ סיביות).

אם $F = F_{2^n}$, אזי אוסף הפונקציות:

$$H = \{ f(x) = a_0 + a_1 x \mid a_i \in F \}$$

הוא אוסף פונקציות מ־$F$ ל־$F$ שהוא 2־אוניברסלי.

**הגדרה 2.29** אוסף $H$ של פונקציות $H=\{h\},\ h:X\to Y$ הוא $k$־אוניברסלי אם לכל $x_1,...,x_k$ שונים ב־$X$, המשתנים המקריים $h(x_1),...,h(x_k)$ עבור $h$ מקרי ב־$H$, כל אחד מפולג באופן אחיד על $Y$ והם בלתי תלויים.

במקרה של פונקציות $Hashing$ התחום $X$ הוא גדול ו־$Y$ הוא קטן, וזה המקרה המעניין. במקרה שלנו הפונקציות הן מהתחום לעצמו, וזה "לא מעניין". כדי להצליח לעשות $Hashing$ למספרים יותר קטנים, משתמשים במה שעשינו עד כה עם שינוי קטן.

**הערה 2.30** אם $X,Y$ מ"מ בלתי תלויים על תחום $\Omega_1$, אזי לכל פונקציה:

$$f:\Omega_1\to\Omega_2$$

גם המשתנים המקריים $f(X)$ ו־$f(Y)$ הם בלתי תלויים.

אם $F=F_{2^n}$, אזי לכל איבר יש ייצוג בתור וקטור של 0 ו־1 באורך $n$:

$$\pi:\{0,1\}^n\to\{0,1\}^k,\ (x_1,...,x_n)\to(x_1,...,x_k)$$

אזי התפלגות אחידה על $\{0,1\}^n$ ואח"כ הפעלת $\pi$ מגדירה התפלגות אחידה על $\{0,1\}^k$.
פונקצית ערבול $(Hash)$ $\overline{h}:\{0,1\}^n\to\{0,1\}^k$, כאשר $k\geq n$: נתבונן על $\{0,1\}^n$ כשדה סופי. נבחר פולינום מקרי $h(x)=a_0+a_1x$ עם מקדמים מקריים בשדה.

$$\overline{h}(x)=\pi(h(x))$$

בקורסים במבני נתונים, ע"מ לא להשתמש בפולינומים, משתמשים במשהו שהוא "כמעט" נכון:
$F=\mathbb{Z}_p$, $2^n<p$,

$$H=\{a+bx|\leq a,b<p\}$$

עם חשבון מודולו $p$. $\alpha_0=0,\alpha_1=1,...,\alpha_{p-1}=p-1$, אזי $h(\alpha_i)$ נותנים $hashing$ לתוך תחום גדול. אם $p<2^{n+1}$ ניתן להציג את המספרים הללו בתור $(x_0,...,x_n)\in\{0,1\}^{n+1}$.
אם לוקחים את $k$ הביטים הראשונים:

$$\pi:\mathbb{Z}_p\to\{0,1\}^k$$

הבעיה פה היא שלא מתקבלת התפלגות אחידה - לא כל האיברים מקבלים פה באותו מספר (מקודם בדיוק מספר המקורות היה קבוע לכולם). ההפרש יהיה קטן מאוד (1 יותר מהאחרים נגיד), אבל "באופן יחסי" זה מתנהג אותו דבר, ולכן מראים את הפונקציה הזו.

**שימוש שלישי - תיקון שגיאות**

יהי $F$ שדה, ונתונה הודעה בת $k$ איברים בשדה: $(a_0,...,a_{k-1})\in F^k$. נרצה להיות מסוגלים לספוג שגיאות בחלק ממהקואורדינטות.
למשל, אם מעתיקים את האינפורמציה כולה 3פעמים, כלומר $k$ איברים ל־$3k$ איברים, נוכל לשחזר את האינפורמציה המקורית גם אם מישהו ישנה את אחת מ־$3k$ הקואורדינטות. זוהי דרך מאוד גרועה לעשות זאת, כי הכפלנו את המידע פי 3, אבל קיבלנו רק יכולת לספוג טעות יחידה.

המטרה שלנו היא להעתיק את המידע כמה שפחות פעמים, ולקבל יכולת לספוג כמה שיותר טעויות בו זמנית. נראה דרך אחת לעשות זאת בעזרת פולינומים:

כדי להגן על הוקטור $(a_0, ..., a_{k-1})$ בצורה יותר יעילה ויותר עמידה, נתבונן על הוקטור כמקדמי פולינום ממעלה $k-1$:

$$f(x) = a_0 + a_1 x + ... + a_{k-1} x^{k-1}$$

ונבחר $n$ נקודות שונות בשדה $F$ $\alpha_1, ..., \alpha_n$, ונחשב את:

$$(f(\alpha_1), ..., f(\alpha_n))$$

כאשר $k \leq n$.

קודם כל, לא איבדנו את האינפורמציה - יש $k$ קואורדינטות הקובעות את הפולינום. הטענה היא שזה עמיד בפני שגיאות.

נניח ש-$t$ קואורדינטות שגויות (ולא יודעים היכן). $f(x)$ המקורית עוברת דרך לפחות $n-t$ נקודות. אם גם $g(x)$ עוברת דרך $n-t$ נקודות ו-$deg(g(x)) \leq (k-1)$, עדיין יש $n-2t$ נקודות $\alpha_i$ כך ש: $f(\alpha_i) = g(\alpha_i)$. אם $n - 2t \geq k$, אזי $g(x) = f(x)$, כי שני פולינומים מדרגה קטנה מ-$k$ המתלכדים על $k$ נקודות זהים.

לכן, אם $t \leq \frac{n-k}{2}$, אפשר לתקן עד $t$ שגיאות: יש פולינום אחד כזה $f(x)$, נעבור על הפולינומים האפשריים ונבדוק "מי מהם בסדר". זה מאוד לא יעיל, כי המספר יכול להיות אקספוננציאלי, "וזה לא מוצלח במיוחד". לדוגמא, אם $n = 3k$, אז הכפלנו את האינפורמציה פי שלוש (כמו בנסיון הראשון שלנו), ונוכל לתקן:

$$t \leq \frac{3k-k}{2} = \frac{2k}{2} = k$$

אכן שיפרנו את העמידות, אבל קיבלנו כאמור אלגוריתם לא יעיל. ננפנף בידיים כדי להסביר איך עושים זאת בצורה יעילה, בעזרת אלגוריתם בסיסי שלומדים בכל קורס על קודים מתקני

שגיאות[16]:

$$\begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{k-1} & \cdots & \alpha_1^{n-1} \\ & & & & & \\ 1 & \alpha_n & & & & \alpha_n^{n-1} \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_{k-1} \\ 0 \\ \vdots \end{pmatrix} = \begin{pmatrix} f(\alpha_1) \\ \vdots \\ \vdots \\ \vdots \\ f(\alpha_n) \end{pmatrix}$$

$$\Rightarrow V \cdot \begin{pmatrix} a_0 \\ \vdots \\ a_{k-1} \\ 0 \\ \vdots \end{pmatrix} = \begin{pmatrix} f(\alpha_1) \\ \vdots \\ \vdots \\ \vdots \\ f(\alpha_n) \end{pmatrix}$$

$$\begin{pmatrix} a_0 \\ \vdots \\ a_{k-1} \\ 0 \\ \vdots \end{pmatrix} = V^{-1} \begin{pmatrix} f(\alpha_1) \\ \vdots \\ \vdots \\ \vdots \\ f(\alpha_n) \end{pmatrix}$$

כאשר הקואורדינטות האפס הן $n-k$ הקואורדינטות האחרונות. זהו דרך לחשב את פולינום האינטרפולציה. מה אם נוסיף לזה שגיאות?

$$\begin{pmatrix} a_0 \\ \vdots \\ a_{k-1} \\ 0 \\ \vdots \end{pmatrix} = V^{-1} \left[ \begin{pmatrix} f(\alpha_1) \\ \vdots \\ \vdots \\ \vdots \\ f(\alpha_n) \end{pmatrix} + \begin{pmatrix} e_1 \\ \vdots \\ \vdots \\ \vdots \\ e_n \end{pmatrix} \right]$$

כאשר לכל היותר $t$ מ־$e_i \neq 0$. נסתכל בשורות שאינן אפס:

$$n-k \; last \; rows \; of \; V^{-1} \left[ \begin{pmatrix} f(\alpha_1) \\ \vdots \\ \vdots \\ \vdots \\ f(\alpha_n) \end{pmatrix} + \begin{pmatrix} e_1 \\ \vdots \\ \vdots \\ \vdots \\ e_n \end{pmatrix} \right] = same \; n-k \; rows \cdot \begin{pmatrix} e_1 \\ \vdots \\ \vdots \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} s_1 \\ \vdots \\ \vdots \\ \vdots \\ s_{n-k} \end{pmatrix}$$

יודעים כי $n-k \geq 2t$. נטען כי יש פה $2t$ נעלמים. "בשיטה של פיזיקאים" נראה איך פותרים זאת - כלומר ננפנף בידיים: לכל קואורדינטה נתאים איבר בשדה - ל־$i$ מתאים $\alpha_i$, כלומר

[16] הקורסים האלו תחת אשכול מתמטיקה בעברית אבל גם תלמידי מדמ"ח בדר"כ מקבלים אישור לקחת אותם.

נסתכל על המיקום כאל איבר בשדה. יש לנו לפחות $2t$: מתוכם $t$ נעלמים בהם מתרחשת הטעות, ועוד $t$ נעלמים המייצגים מהי הטעות. "אם יש צדק" אפשר גם לחשב את מיקום השגיאה ומהו הגודל של ה־$e_i$ הזה מתוך $2t$ המשתנים.

נקבל כי אנחנו יכולים לתקן הרבה מאוד שגיאות בעוד שניפחנו את המידע רק פי קבוע, בעוד שאם משתמשים בחזרה כמו בדוגמא הראשונה מקבלים תוצאה הרבה פחות טובה.

## 2.3 נורמות ומרחבים מטריים

19.11.2013

מיכאל חולה ־ שיעור השלמה עם נתי ליניאל!

כשמלמדים אלגברה לינארית בתואר ראשון, יש אספקט גיאומטרי שלא רואים ־ אותו נראה בקורס הזה.

המושג הכי בסיסי שרואים באינפי בתואר ראשון הוא התכנסות. אולי ראינו כבר במקומות אחרים שאין בעיה להסתכל על סדרות מתכנסות לא של מספרים, אלא של נקודות במישור. מה דרוש לכך? מעט מאוד. מה שבעצם צריך הוא מושג של מרחק. זאת מכיוון והתשובה לשאלה מתי $x_n \to x$ היא "כשאתה מספיק רחוק בסדרה, אתה מאוד קרוב ל־$x$": $|x_n - x| < \varepsilon$ ־ וזהו מרחק! מרחק יכול להיות הרבה דברים ־ מרחק גיאוגרפי, מרחק נסיעה, ועוד ועוד. מכאן אנחנו מגיעים להגדרה של מרחב מטרי[17]:

**הגדרה 2.31** תהי $X$ קבוצה. העתקה $d : X \times X \to \mathbb{R}$ המקיימת את התנאים הבאים נקראת מטריקה (על $X$):

1.
$$\forall x, y \in X \; d(x, y) \geq 0$$
ושיוויון אמ"מ $x = y$.

2.
$$\forall x, y \in X \; d(x, y) = d(y, x)$$

3. א"ש המשולש:
$$\forall x, y, z \in X \; d(x, y) + d(y, z) \geq d(x, z)$$

פחות או יותר כל האינפי הבסיסי אפשר לעשות (ויש ספרים וקורסים שעושים את זה) בתוך המסגרת של מרחבים מטריים וההגדרה מעלה. אנחנו מכירים עוד הרבה מטריקות פשוטות שראינו כבר פעמים רבות, ונוסיף עוד עושר עליהן:

[17] יש מספר וריאציות קלות להגדרה הזו, ואולי נראה בהמשך הדרך האקדמית שלנו הגדרות אחרות.

**דוגמאות**

- המטריקה הפשוטה ביותר נגיד על הישר: $X = \mathbb{R}$, $d(x,y) = |x-y|$.
- המרחק במישור $X = \mathbb{R}^2$:

$$d\left((x_1,x_2),(y_1,y_2)\right) = \sqrt{(x_1-y_1)^2 + (x_2-y_2)^2}$$

- דוגמא אחרת לגמרי - למשל בביוינפורמטיקה, אם מסתכלים על גן בכל מיני יצורים, ורוצים להבין מי קרוב ומי רחוק ממי, ואולי לשחזר את ההתפתחות האבולוציונית, צריך מדד שיגיד עד כמה שני רצפים של $DNA$ דומים זה לזה. לצורך זה מוגדר מרחק עריכה $edit\ distance$ בין סדרות (מחרוזת של אותיות) שרואים למשל בקורס אלגוריתמים: גם זוהי מטריקה.

למה יש למטריקות תפקיד כל כך חשוב? בתחום המעשי, למשל בדוגמא האחרונה, כי בעזרתן פותרים הרבה דברים חשובים. בתחום התיאורטי כי כפי שציינו כל הדברים של אינפי אפשר לעשות בתנאי שמוגדרת לנו מטריקה.

אנחנו עובדים בעיקר במרחב $\mathbb{R}^n$. היינו רוצים מטריקות "יפות" - נחפש מבנה מטרי על $\mathbb{R}^n$ כזה שישקף היטב את הגיאומטריה של מרחב זה.

ב-$\mathbb{R}^n$ יש שתי פעולות ברורות: חיבור וקטורי וכפל בסקלר.

בחיבור וקטורי יוצאים מהראשית בעזרת שני וקטורים ומגיעים ליעד. למעשה הציור הזה וא"ש המשולש הוא אותו הדבר - עוברים דרך נקודה נוספת כדי להגיע מהמקור ליעד.

האופן שבו נממש את הרעיון הזה (והוא קונספט חשוב ומאוד מרכזי): במקום להתחיל מהגדרה של מרחק, נתחיל מהגדרה של מושג "אורך" (או גודל) של וקטור - נורמה $\|\cdot\|$.

ברור איך שני הדברים האלה הולכים להתקשר ביחד: האורך של הוקטור מהמקור ליעד הוא קטן או שווה מהאורך של שני הוקטורים. נרצה:

$$\forall u,v \in \mathbb{R}^n \ \ \|u\| + \|v\| \geq \|w\|$$

נטען כי אם יש מושג של אורך, מקבלים באופן מיידי גם מושג של מרחק באופן הבא:

$$d(x,y) := \|y-x\|$$

נראה זאת, אבל תחילה נפרמל את מה שאמרנו עד כה:

**הגדרה 2.32** נורמה על $\mathbb{R}^n$ זו העתקה $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}$ בעלת התכונות הבאות:

1. חיוביות:

$$\forall u \in \mathbb{R}^n, \ \ \|u\| \geq 0$$

ויש שיוויון $u = \vec{0} \Leftrightarrow$.

2. אי שיוויון המשולש:

$$\forall u,v \in \mathbb{R}^n \ \ \|u\| + \|v\| \geq \|u+v\|$$

3. הומוגניות: לכל $u \in \mathbb{R}^n$ ולכל $\alpha \in \mathbb{R}$ מתקיים:

$$\|\alpha u\| = |\alpha| \cdot \|u\|$$

**הערה 2.33** כל נורמה משרה גם מטריקה על $\mathbb{R}^n$ באמצעות:

$$d(x,y) := \|x - y\|$$

למה הדבר הזה כל כך חשוב? מוטיב בסיסי שלא רואים כמעט בקורסים היסודיים הוא שהמושג של חישוב מקורב התבגר לנקודה שהמון דברים לא ניתן לחשב בחישוב מוחלט. זאת בשל מספר סיבות: זה $NP$-קשה, מגבלות של חומרה, וכו', ולכן הקונספט של לעשות משהו בצורה מקורבת הוא מאוד רלוונטי כבר הרבה שנים. לכן צריך למצוא פתרון מקורב - יש הרבה דרכים כאלה, מהי הדרך הכי טובה? כל המושגים שנדבר עליהם היום נכנסים שם בצורה מאוד חזקה: $x$ הוא הפתרון האידאלי, ו-$y$ הפתרון שמצאנו. השיטה הטובה ביותר תיתן את המרחק הקטן ביותר בין הפתרונות. על מנת להעריך זאת יש צורך במטריקה.

**דוגמא 0**: עבור $n = 1$ על $\mathbb{R}$, הנורמה $\|x\| = |x|$ היא הנורמה היחידה.

כשהמימד עולה, מרחב האפשרויות הוא עצום: יש אינסוף נורמות, ויש הרבה שמעניינות אותנו באופן מעשי. כעת נכיר חלק מהן ונלמד איך לעבוד איתן.

ידענו למדוד גודל של מספרים ממשיים, וכעת נדבר על מדידת גודל של וקטורים. נרצה למדוד גודל להרבה דברים אחרים: גודל של מטריצות, של העתקות... כל אלה דברים מאוד חשובים.

### 2.3.1 דוגמאות מאוד חשובות של נורמות

**נורמה אוקלידית, נורמה** $l_2$ על $\mathbb{R}^n$:

$$\|(x_1, ..., x_n)\| = \sqrt{\sum x_i^2}$$

יש משפחה שלמה של נורמות שזו אחת מביניהן - נורמות $l_p$:

$$x \in \mathbb{R}^n \quad \|x\|_{p:} = \left(\sum |x_i|^p\right)^{\frac{1}{p}}$$

נראה במהרה כי זוהי באמת נורמה:

אי שלילי ושיוויון רק ב-$x = 0$ טריוויאלי. לינאריות גם מתקבלת באופן מאוד מהיר. הדבר היחיד שבאמת צריך להוכיח את א"ש המשולש:

$$\|x + y\|_p \leq \|x\|_p + \|y\|_p$$

נוכיח זאת בהמשך.

מה מיוחד בנורמת $l_2$? כרגע לא נוכיח זאת, אבל נחזור לכך אחר כך - נורמה זו היא אינווריאנטית לסיבובים של המרחב. מה זה אומר? בצורה אינטואיטיבית אנו מבינים מה זה אומר לסובב את המישור. אם $T$ היא טרנספורמציית סיבוב של המרחב $\mathbb{R}^n$, אזי אינווריאנטיות לסיבוב אומרת כי לכל $x \in \mathbb{R}^n$ מתקיים:

$$\|Tx\|_2 = \|x\|_2$$

וזוהי תכונה מאוד יחודית.
שתי הנורמות החשובות הנוספות הן $l_1, l_\infty$:

$$l_1 : x \in \mathbb{R}^n,\ \|x\|_1 := \sum |x_i|$$

לנורמה זו קוראים גם נורמת מנהטן, זאת מכיוון ומנהטן מורכבת מגריד - רשת של רחובות.

$$l_\infty = max\,|x_i|$$

**הערה 2.34** תרגיל מאוד פשוט:

$$\lim_{p\to\infty} \|x\|_p = \|x\|_\infty$$

איך מעריכים טעות? כביכול נורמת $l_1$ היא מאוד אינטואיטיבית ונכונה - לכל טעות אותו משקל. אולם, יש הרבה סיטואציות, ואולי לא תמיד נרצה לתת את אותו משקל, אולי נרצה לייחס חשיבות גדולה יותר או פחותה יותר לטעויות גדולות או קטנות. ככל שמעלים את $p$, הקואורדינטה הכי גדולה מתחילה לתפוס משקל יותר ויותר גדול, ושאר הקואורדינטות מתגמדות. על כן השאלה באיזו נורמה להשתמש היא לא שאלה מתמטית טהורה, אלא צריכה לשקף את הצרכים. אפשר גם "לתפור" נורמות שונות מאלו שראינו - לא לייחס משקל כלל לקואורדינטות מסויימות, ועוד.

**הערה 2.35** נשים לב כי בהמשך, ובעצם כבר למעלה, במקום לכתוב $\|\cdot\|_{l_p}$ נרשום בקיצור $\|\cdot\|_p$, ונדון בעיקר בנורמות אלו.

### 2.3.2 פרספקטיבה גיאומטרית של נורמות

**הגדרה 2.36** אם $\|\cdot\|$ נורמה על $\mathbb{R}^n$, אנו מגדירים את הקבוצה:

$$\mathbb{R}^n \supseteq B = B_{\|\cdot\|} := \{x \in \mathbb{R}^n |\, \|x\| \leq 1\}$$

להיות "כדור היחידה של הנורמה $\|\cdot\|$".

*איורים - כדורי היחידה*
ב-$l_2$ כדור היחידה הוא עיגול.
ב-$l_1$ כדור היחידה הוא מעויין.
ב-$\mathbb{R}^n$ זה פאון - *polytope*. סוג אחד של פאונים אנחנו מכירים - במישור זה מצולע. נראה הגדרה פורמלית בהמשך הקורס בנושא אחר. יש חמישה פאונים משוכללים בשלושה מימדים (אחד ההישגים הגדולים ביותר של הגיאומטריה היוונית: קוביה, סימפלקס (ארבעון), אוקטהדר, ועוד שניים מופלאים: 12 ו-20 דפנות. פאון בעל $n$ צדדים נקרא גם $n-gon$.
איך מתארים פאון?

- באמצעות קודקודיו - הפאון הוא הקמור $convex\ hull$ של קודקודיו.
- על ידי אי שיוויונים לינאריים.

כדור היחידה של $l_1$ ב־$\mathbb{R}^n$ הוא האוקטהדר או *cross polytope*. נתאר בשתי הדרכים שציינו:

- תיאור ע"י קודקודים: זהו הקמור של $2n$ הנקודות $Ie_1, Ie_2, ..., Ie_n$.
- אי השיוויונים הם $\sum |x_i| \leq 1$. כאי שיוויונים לינאריים באופן כללי: לכל $\varepsilon_1, ..., \varepsilon_n$ כאשר $\varepsilon_i \in \{-1, 1\}$, נכתוב $\sum \varepsilon_i x_i \leq 1$.

כדור היחידה של $l_\infty$ הוא הקוביה (או היפר־קוביה לפעמים):

- הקודקודים: כל $2^n$ קודקודי הסימנים.
- אי השיוויונים:

$$\forall i \ -1 \leq x_i \leq 1$$

נשים לב כי קיבלנו רשימה מאוד קצרה של אי שיוויונים כאן והרבה קודקודים, לעומת הדוגמא הקודמת ־ נראה בהמשך כי זה לא במקרה, וה־$tradeoff$ הזה מאוד חשוב בחישוב לינארי.

עוד דבר אחד כדי לקשור את הקצוות הגיאומטריים: לא קשה להוכיח שלכל נורמה $\|\cdot\|$ יש לכדור היחידה $B = B_{\|\cdot\|}$ התכונות הבאות:

- $B$ קבוצה קמורה (זו מסקנה קלה מאי שיוויון המשולש).
- $B$ סימטרית יחסית לראשית (או סימטרי מרכזית), ז"א אם $x \in B$ אז גם $-x \in B$.

זה לא מקרה שכל הדברים שציירנו יש להם את התכונות האלו. עובדה מעניינת (וקלה) שלא נפתח אלא רק נזכיר בקצרה (וכדאי לזכור אם צריך להגדיר מדד גודל כלשהוא בהמשך) היא שכל גוף קמור סימטרי מרכזית הוא כדור היחידה של נורמה.

התעסקנו עד כה רק ב־$\mathbb{R}^n$ (ונעשה זאת גם בהמשך), אך נורמות מופיעות גם במרחבים לינאריים גדולים יותר, למשל $C[0,1]$ ־ מרחב הפונקציות הממשיות הרציפות על הקטע $[0,1]$. כל הדברים שעשינו עד כה אפשר לפתח גם במרחב זה:

אם $f \in C[0,1]$, אפשר למשל להגדיר:

$$\begin{aligned} \|f\|_1 &:= \int_0^1 |f(x)|\, dx \\ \|f\|_p &:= \left( \int_0^1 |f(x)^p|\, dx \right)^{\frac{1}{p}} \end{aligned}$$

מלבד מתמטיקה יפה ושימושים פרקטיים, יש כאן אינטראקציה מאוד יפה בין המושגים למשמעות הגיאומטרית.

עוד דבר שמקבלים מיד "בתור בונוס" כשיש לנו מושג של "אורך של וקטור": אם $X, Z$ הם שני מרחבים נורמיים, ונסמן את הנורמות שלהם באופן הבא: $\|\cdot\|_X$ , $\|\cdot\|_Z$ בהתאמה, ואם $f : X \to Z$ העתקה ביניהם, אז ניתן לייחס "גודל" גם ל־$f$. זהו רעיון מאוד חשוב. כלומר, ברגע שיודעים למדוד גודל של עצמים במרחב, יש צורה מאוד מתבקשת למדוד גודל של העתקות. זה כבר נשמע מאוד לא צפוי. נראה את המושג הזה במהלך הקורס מספר פעמים. נוכל לדבר על האספקט של מתיחה וכיווץ: לוקחים מישהו ב־$X$ ומעתיקים אותו

ל־$Y$: היה לו גודל ב־$X$ ויש לו גם גודל ב־$Z$: יתכן שההעתקה כיווצה, הרחיבה או השאירה את הגודל אותו דבר. הגודל שנרצה לייחס ל־$f$ היא מידת המתיחה המירבית של $f$, כלומר:

$$\|f\|_{X\to Z} := \max_{x\in X,\|x\|_X\neq 0, z\in Z} \frac{\|f(x)\|_Z}{\|x\|_X}$$

זוהי רק "הצעת הגשה", יש צורך לפרמל כדי שנוכל לעבוד עם זה (עוד על כך בקורס "שיטות גיאומטריות בתורת האלגוריתמים").

נביט ב־$X = Y = \mathbb{R}^n$. אפשר לחשוב על איברי $y \in Y$ לא כוקטורים, אלא כפונקציונלים לינאריים על $X$; מה פירוש הדבר? רוצים לחשוב על $y \in Y$ בתור ההעתקה $x \to \langle x, y\rangle$. העתקה כזו נקראת פונקציונל לינארי, שתכונותיה הינן:

$$\langle \alpha x, y\rangle = \alpha \langle x, y\rangle$$
$$\langle x_1 + x_2, y\rangle = \langle x_1, y\rangle + \langle x_2, y\rangle$$

עכשיו נרצה למדוד את הגודל של $y$ במונחי המושג שהגדרנו קודם, כלומר במושגי מידת המתיחה המירבית.

תהיה $\|\cdot\|$ נורמה על $\mathbb{R}^n$, ונרצה לראות איך מערכת המושגים הזו משתקפת כשאנו חושבים על $Y = \mathbb{R}^n$ כמרחב של פונקציונלים לינאריים על $\mathbb{R}^n$.

**הגדרה 2.37** נסמן את **הנורמה הדואלית** באופן הבא:

$$\|y\|^* := max \frac{|\langle x, y\rangle|}{\|x\|_X}$$

לא קשה להראות שאכן $\|\|^*$ הוא נורמה. הלינאריות פשוטה:

$$\|\beta y\|^* := |\beta| \cdot \|y\|^*$$

נוכיח את א"ש המשולש, כלומר:

$$\|y_1\|^* + \|y_2\|^* \geq \|y_1 + y_2\|^*$$

נגיד במילים ־ נביט בהגדרה: אם נכפיל את $x$ בשבר דבר לא ישתנה. לכן יהיה לנו מאוד נוח לסלק את המכנה. בגלל הלינאריות, אפשר להסתכל רק על $x$ בעלי נורמה 1[18]. אגף ימין:

$$\|y_1 + y_2\|^* = \max_{\|z\|_X=1} |\langle y_1 + y_2, z\rangle|$$

יהי $z = x$ הוקטור המשיג את המקסימום. על כן:

$$\|y_1\|^* \geq |\langle y_1, z\rangle|$$

וכנ"ל לגבי $y_2$, ובגלל הלינאריות מקבלים את אי השיוויון המבוקש.

כעת עולות כמה שאלות:

- בהנתן $B_{\|\cdot\|}$, איך נראה $B_{\|\cdot\|^*}$?

[18] חלקנו ראינו זאת בקורס אלגברה לינארית 2.

- ספציפית: מהי הנורמה הדואלית של $l_p, l_2, l_1, l_\infty$?

נראה את המשפט הכללי בנושא:

**משפט 2.38** הנורמה הדואלית לנורמת $l_p$ היא נורמת $l_q$ כאשר:

$$\frac{1}{p}+\frac{1}{q}=1$$

בפרט נורמת $l_2$ דואלית לעצמה, ונורמות $l_1, l_\infty$ דואליות זו לזו.

26.11.2013

בשיעור הקודם הגדרנו את נורמה $p$. על מנת להוכיח כי היא אכן נורמה, יש להוכיח את א"ש המשולש - אי השיוויון במקרה זה נקרה **אי שיוויון** $Minkowski$**:**

**טענה 2.39**

$$\|x\|_p + \|y\|_p \geq \|x+y\|_p$$

כמו כן, דיברנו על כדור היחידה:

$$B = \{\, x \in \mathbb{R}^n | \, \|x\| \leq 1\}$$

**תכונות כדור היחידה**

1. $B$ הוא קבוצה קמורה:

$$\forall x, y \in B,\ \forall 0 \leq \lambda \leq 1\ \lambda x + (1-\lambda)\, y \in B$$

2. $B$ הוא קבוצה סימטרית מסביב לראשית:

$$x \in B \Leftrightarrow -x \in B$$

3. $B$ מכיל סביבה פתוחה סביב לראשית (לפי נורמה אוקלידית למשל).

תהי $B \subseteq \mathbb{R}^d$ קבוצה קמורה, סימטרית (סביב הראשית) ומכילה סביבה פתוחה של הראשית. נגדיר מהקבוצה הזו נורמה:

$$\|x\|_B := \frac{1}{max\,\{\,\lambda |\, \lambda x \in B\}}$$

קל לראות כי אכן הפעולה מקיימת את התנאים הדרושים.

המכפלה הפנימית הסטנדרטית מוגדרת באופן הבא - עבור $x, v \in \mathbb{C}^d$:

$$\langle x, v \rangle := \sum_{i=1}^{d} \overline{x}_i v_i = x^* v$$

כאשר $x^*$ הוא טרנספוז צמוד. אזי:

$$\langle x, x \rangle = \sum_{i=1}^{d} \overline{x}_i x_i = \sum_{i=1}^{d} |x_i|^2 = \|x\|_2^2$$

תהי $\|\cdot\|$ נורמה ו־$B$ כדור היחידה שלה. אזי ניתן להגדיר את הנורמה הדואלית שראינו בשיעור הקודם:

**הגדרה 2.40** נסמן את **הנורמה הדואלית** באופן הבא:

$$\|x\|^* := max \frac{|\langle x, v \rangle|}{\|v\|} = \max_{\|v\|=1} |\langle x, v \rangle|$$

בפעם הקודמת הוכחנו ב"נפנופי ידיים" כי זוהי אכן נורמה. הפעם נעשה זאת באופן מסודר:

**למה 2.41** $\|x\|^*$ היא נורמה.

**הוכחה:** נוכיח את התנאים:

- הלינאריות טריוויאלית.
- א"ש המשולש:

$$\begin{aligned} \|x_1 + x_2\|^* &= \max_{\|v\|=1} |\langle x_1 + x_2, v \rangle| = \max_{\|v\|=1} |\langle x_1, v \rangle + \langle x_2, v \rangle| \\ &\leq \max_{\|v\|=1} \left( |\langle x_1, v \rangle| + |\langle x_2, v \rangle| \right) \\ &\leq \max_{\|v\|=1} |\langle x_1, v \rangle| + \max_{\|v\|=1} |\langle x_2, v \rangle| = \|x_1\|^* + \|x_2\|^* \end{aligned}$$

- חיוביות חזקה: נובעת מכך שלכל $x \neq 0$, עבור $v = \frac{x}{\|x\|}$ נקבל:

$$\|x\|^* \geq |\langle x, v \rangle| = \|x\| > 0$$

■

**טענה 2.42** כדור היחידה של $\|x\|^*$ הוא:

$$B^* := \left\{ x \in \mathbb{R}^d \middle| \forall v \in B \ \ \langle x, v \rangle \leq 1 \right\}$$

**הוכחה:** נראה כי אם $x \in B^*$, אזי $x$ בכדור היחידה של $\|\cdot\|^*$, ונראה כי אם $x \notin B^*$, הוא גם אינו בכדור היחידה הנ"ל.
בכיוון ראשון, נניח $x \in B^*$. אזי לכל $v \in B$ מתקיים $\langle x, v\rangle \leq 1$. בפרט זה מתקיים לכל $\|v\| = 1$, ולכן:

$$\|x\|^* = \max_{\|v\|=1} |\langle x, v\rangle| \leq 1$$

ולכן $x$ בכדור היחידה של $\|\cdot\|^*$.
בכיוון השני, אם $x \notin B^*$, קיים $v \in B$ כך ש:

$$\langle x, v\rangle = a > 1$$

אם $\|v\| < 1$, אזי ניתן להכפיל את $v$ ב־$\frac{1}{\|v\|} > 1$, וקטור בעל נורמה 1 ו־$a$ יותר גדול. לכן נוכל להניח כי $\|v\| = 1$. אזי:

$$\|x\|^* = \max_{\|v\|=1} |\langle x, v\rangle| > 1$$

ועל כן $x$ איננו בכדור היחידה של $\|\cdot\|^*$. ■

### 2.3.3 אי שיוויונים

נראה הכללה של אי שיוויון קושי־שוורץ:

**אי שיוויון הולדר**

**למה 2.43** תהי $\|\cdot\|$ נורמה, ו־$\|\cdot\|^*$ הנורמה הדואלית שלה. אזי לכל שני וקטורים $x, v$ מתקיים:

$$|\langle x, v\rangle| \leq \|x\| \cdot \|v\|^*$$

**הוכחה:** יהיו $B, B^*$ כדורי היחידה המתאימים לנורמות $\|\cdot\|^*, \|\cdot\|$ בהתאמה. מתקיים $\frac{x}{\|x\|} \in B$ וכן $\frac{v}{\|v\|^*} \in B^*$. מהגדרת $B^*$(כפי שהוכחנו בטענה הקודמת):

$$1 \geq \left\langle \frac{x}{\|x\|}, \frac{v}{\|v\|} \right\rangle = \frac{\langle x, v\rangle}{\|x\| \, \|v\|^*}$$

וקיבלנו את הנדרש. ■

**טענה 2.44** יהי $B_p$ כדור היחידה בנורמה $\|\cdot\|_p$, ויהי $q$ כך ש־$\frac{1}{p} + \frac{1}{q} = 1$. אזי:

$$B_q = B_p^*$$

באופן שקול אפשר לטעון כי $\|\cdot\|_q$ היא הנורמה הדואלית של $\|\cdot\|_p$.

לפני הוכחת הטענה, נוכיח שני אי שיוויונות נוספים:

**אי שיוויון** $Young$

**למה 2.45** יהיו $\mathbb{R} \ni p,q > 0$ כך ש־$\frac{1}{p}+\frac{1}{q}=1$. אזי לכל $a,b \in \mathbb{R}$ מתקיים:

$$a \cdot b \leq \frac{1}{p}a^p + \frac{1}{q}a^q$$

**הוכחה:** אם $a=0$ או $b=0$, ברור.
אחרת $b,a>0$. חלקנו ראינו בקורסים קודמים כי פונקציית ה־$log$ היא פונקציה קעורה, כלומר לכל $x,y>0$, $0 \leq \lambda \leq 1$ מתקיים:

$$\log\left(\lambda x + (1-\lambda)\, y\right) \geq \lambda \log x + (1-\lambda)\log y$$

ולכן:

$$\begin{array}{ccc} & \lambda = \frac{1}{p} \Rightarrow (1-\lambda) = \frac{1}{q} & \\ & x = a^p,\ y = b^q & \\ \log(ab) = \frac{1}{p}\log a^p + \frac{1}{q}\log b^q & \leq & \log\left(\frac{1}{p}a^p + \frac{1}{q}b^q\right) \end{array}$$

ומכך ש־$log$ מונוטונית עולה ניתן להוציא את הלוג בשני הכיוונים תוך כדי שמירה על אי השיוויון, ונקבל את הנדרש. ■

**אי שיוויון הולדר "המוכר"**

**למה 2.46** יהיו $\mathbb{R} \ni p,q > 0$. אזי לכל $x,v \in \mathbb{R}^d$ מתקיים:

$$|\langle x,v\rangle| \leq \|x\|_p \|v\|_q$$

**הוכחה:** אם $x=0$ או $v=0$ ברור. אחרת, נוכל לחלק בכפל הנורמות, ונקבל:

$$\begin{aligned} \frac{|\langle x,v\rangle|}{\|x\|_p\|v\|_q} &= \frac{\left|\sum_{k=1}^d x_k v_k\right|}{\|x\|_p\|v\|_q} \leq \frac{\sum_{k=1}^d |x_k|\,|v_k|}{\|x\|_p\|v\|_q} = \sum_{k=1}^d \frac{|x_k|}{\|x\|_p}\frac{v_k}{\|v\|_q} \\ &\leq \sum_{k=1}^d \left(\frac{1}{p}\cdot\frac{|x_k|^p}{\|x\|_p^p} + \frac{1}{q}\cdot\frac{|v_k|^q}{\|v\|_q^q}\right) = \frac{1}{p}\cdot\frac{\sum_{k=1}^d |x_k|^p}{\|x\|_p^p} + \frac{1}{q}\cdot\frac{\sum_{k=1}^d |v_k|^q}{\|v\|_q^q} \\ &= \frac{1}{p}\cdot 1 + \frac{1}{q}\cdot 1 = 1 \end{aligned}$$

■

כעת, נוכל להוכיח את הטענה המקורית ־ כלומר כי כדור היחידה של הנורמה $l_q$ היא כדור היחידה של הנורמה הדואלית של $l_p$. **הוכחה:** תחילה, נניח כי $x \in B_q$, ונראה כי $x \in B_p^*$. מאי שיוויון הולדר, לכל $v$ מתקיים:

$$|\langle x,v\rangle| \leq \|x\|_p\|v\|_q \overset{\|x\|_p \leq 1}{\leq} \|v\|_q$$

ולכן לכל $v \in B_q$ נקבל כי $|\langle x,v\rangle| \leq \|v\|_q \leq 1$, כלומר $x \in B_p^*$ מההגדרה.
שנית, נניח כי $x \in B_p^*$, ונראה כי $x \in B_q$. מהגדרת $B_p^*$, לכל $v$ כך ש־$\|v\|_p \leq 1$ (כלומר $v \in B_p$) מתקיים:

$$\langle x,v\rangle \leq 1$$

נגדיר $v \in \mathbb{R}^d$ באופן הבא:

$$v_k = \frac{sgn\left(x_k\right) \cdot |x_k|^{q-1}}{\|x\|_q^{\frac{q}{p}}}$$

נשים לב כי מהגדרתם, $p \cdot q = p + q$. לכן:

$$\|v\|_p^p = \frac{1}{\|x\|_q^q} \sum_{k=1}^{d} |x_k|^{(q-1)p} = \frac{1}{\|x\|_q^q} \sum_{k=1}^{d} |x_k|^q = 1$$

ולכן:

$$\begin{aligned} 1 \geq \langle x,v\rangle &= \frac{1}{\|x\|_q^{\frac{q}{p}}} \sum_{k=1}^{d} sgn\left(x_k\right) x_k \left|x_k\right|^{q-1} = \frac{1}{\|x\|_q^{\frac{p}{q}}} \sum_{k=1}^{d} |x_k|^q \\ &= \|x\|_q^{q-\frac{p}{q}} = \|x\|_q^{q\left(1-\frac{1}{p}\right)} = \|x\|_q^{q\cdot\frac{1}{q}} = \|x\|_q \end{aligned}$$

ולכן $x \in B_q$, כנדרש. ■

**מסקנה 2.47** עבור $\mathbb{R} \ni p,q > 0$ כאשר $\frac{1}{p} + \frac{1}{q} = 1$, נורמה ה־$p$־אית והנורמה ה־$q$־אית הן נורמות דואליות.

### 2.3.4 מטריצות ופרספקטיבה גיאומטרית

**הגדרה 2.48** מטריצה $U$ מסדר $n \times n$ מעל המרוכבים נקראת אוניטרית $(Unitary)$ אם:

$$U^*U = I$$

כאשר אם $U = (u_{ij})$ מגדירים: $U^* = (\overline{u}_{ij})$.

**הגדרה 2.49** מעל הממשיים, $O$ מסדר $n \times n$ המקיימת:

$$O^TO = I$$

נקראת מטריצה אורתוגונלית.

**הערה 2.50** מטריצה אורתוגונלית היא בפרט אוניטרית מעל המרוכבים.

**הגדרה 2.51** מטריצה $A$ היא איזומטריה / שומרת מרחק / שומרת אורך אם לכל $x \in \mathbb{C}^n$ מתקיים $\|Ax\|_2 = \|x\|_2$.

**טענה 2.52** בנורמת $l_2$, העתקה לינארית מהמרחב אל עצמו היא שומרת אורכים אמ"מ היא מטריצה אוניטרית (אורתוגונלית בממשיים).

**דוגמא** ב־$\mathbb{R}^2$, אלו מטריצות מהצורה:

$$\begin{pmatrix} cos\alpha & sin\alpha \\ -sin\alpha & cos\alpha \end{pmatrix}$$

מה המטריצה הזו עושה? מסובבת וקטור בזווית $\alpha$. זה מתקשר למשהו שכבר הזכרנו בעבר ־ ב־$L_2$ ($l_2$ עם הנורמה $\mathbb{R}^2$) סיבוב שומר על האורך.

נוכיח את הטענה: **הוכחה:** בכיוון הראשון, נניח כי $U$ אוניטרית, ונראה כי היא שומרת מרחק. לכל $u, v$ מתקיים:

$$\langle u, Av \rangle = \langle A^* u, v \rangle$$

ולכל לכל $x$:

$$\|Ux\|_2^2 = \langle Ux, Ux \rangle = \langle U^*Ux, x \rangle = \langle Ix, x \rangle = \langle x, x \rangle = \|x\|_2^2$$

בכיוון השני, נניח כי $U$ שומרת מרחק, ונוכיח כי היא אוניטרית.

$$\begin{aligned} \|x+y\|^2 &= \langle x+y, x+y \rangle = \langle x, x \rangle + \langle x, y \rangle + \langle y, x \rangle + \langle y, y \rangle \\ &= \langle x, x \rangle + \langle x, y \rangle + \overline{\langle x, y \rangle} + \langle y, y \rangle = \|x\|^2 + 2Re\left(\langle x, y \rangle\right) + \|y\|^2 \end{aligned}$$

מצד שני, באופן דומה ובשימוש בהנחה:

$$\begin{aligned} \|x+y\|^2 &= \|U\left(x+y\right)\|^2 = \|Ux+Uy\|^2 = \|Ux\|^2 + 2Re\left(\langle Ux, Uy \rangle\right) + \|Uy\|^2 \\ &= \|x\|^2 + 2Re\left(\langle U^*Ux, y \rangle\right) + \|y\|^2 \end{aligned}$$

ולכן:

$$\begin{aligned} &Re\left(\langle x, y \rangle\right) = Re\left(\langle U^*Ux, y \rangle\right) \\ &\Rightarrow 0 = Re\left(\langle x, y \rangle\right) - Re\left(\langle U^*Ux, y \rangle\right) = Re\left(\langle x - U^*Ux, y \rangle\right) \end{aligned}$$

לכל $x, y$. נקבע את $x$, ונבחר $y = x - U^*Ux$. נקבל:

$$\|x - U^*Ux\|^2 = \langle x - U^*Ux, x - U^*Ux \rangle = Re\left(\langle x - U^*Ux, x - U^*Ux \rangle\right) = 0$$

ולכן בהכרח $x - U^*Ux = 0$, כלומר $x = U^*Ux$. זה כאמור נכון לכל $x$, ועל כן $U^*U = I$, כנדרש. ■

**הערה 2.53** נשים לב כי מההגדרה, מטריצה $U$ היא אוניטרית (אורתוגונלית) אמ"מ עמודות המטריצה $U = [U_1 \cdots U_n]$ הם וקטורי יחידה ניצבים זה לזה (בסיס אורתונורמלי).

תהי $A : \mathbb{R}^n \to \mathbb{R}^n$. אם ל־$A$ יש בסיס של וקטורים עצמיים $v_1, ..., v_n$ עם ע"ע $\lambda_1, ..., \lambda_n$, אזי ברור מה ההעתקה עושה ־ היא מנפחת ב־$\lambda_i$ בכיוון $v_i$.

אולם, לא תמיד יש בסיס כזה. למשל:

$$C = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

הוקטור $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ פורש את אוסף הוקטורים עם ע"ע 0, שהוא הערך העצמי היחיד.

בוודאי שאין בסיס כזה אם המטריצה $A$ אינה ריבועית (שם ערכים עצמיים כלל לא מוגדרים). עם זאת, המטריצה $A^*A$ היא מטריצה סימטרית, ויש לה ערכים עצמיים ממשיים $\geq 1$ ובסיס של וקטורים עצמיים. בשיעור הבא נראה כיצד "מפרקים" מטריצות שכאלו.

## 2.4 פירוק $SVD$ של מטריצות

3.12.2013

$SVD - Singular\,Value\,Dexomposition$.

**שיעורי בית**: לקרוא את סיכום הרצאה 6 מהשנה שעברה - יש שם הצגה קצת שונה מזו שנראה בכיתה.

ההצגה שאנחנו נראה יותר אפליקטיבית במדעי המחשב, ונראה דוגמא לשימוש בשיעורי הבית.

**הגדרה 2.54** מטריצה ריבועית $A$ (ממשית\מרוכבת) המקיימת: $AA^* = A^*A$ נקראת מטריצה נורמלית.

ידוע שאם $A$ מטריצה נורמלית, אזי קיימת מטריצה $U$ כך ש-$UU^* = I$, כאשר $U$ ממשית כזאת נקראת אורתוגונלית, ומרוכבת נקראת אוניטרית $(Unitary)$, כך ש:

$$A = UDU^*$$

כאשר $D$ מטריצה אלכסונית:

$$D = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$$

**משפט 2.55** $A$ נורמלית $\Leftrightarrow$ קיימת $U$ כזו.

הוכחנו משפט זה בקורס אלגברה לינארית 2.

בתנאים הללו:

$$\Rightarrow AU = UD$$

כלומר אפשר לבחור בסיס של וקטורים עצמיים עם ע"ע $d_1, ..., d_n$ שיבנה את $U$, ובצד ימין מקבלים הכפלה בע"ע.

מטריצות כאלו אנחנו מבינים - כשמכפילים במטריצה אורתוגונלית מקבלים סיבוב. אבל, לא כל המטריצות ניתנות ללכסון אורתוגונלי. יתרה מזו, אם המטריצה לא ריבועית, בוודאי שאי אפשר לכתוב אותה ככה. נרצה אם כך למצוא פירוק שיסביר לנו איך גיאומטרית פועלת מטריצה כלשהיא. לשם כך נוכיח את המשפט הבא:

**משפט $SVD$**

**משפט 2.56** תהי $A$ מטריצה (ממשית) מסדר $m \times n$, $m \geq n$ ודרגה $n \geq r$. אזי קיימות מטריצות אורתוגונליות $U$ מסדר $m \times m$ ו-$V$ מסדר $n \times n$ ומטריצה אלכסונית $D$ מסדר $m \times n$ כך ש:

$$A = UDV^T$$

כאשר

$$D = \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_r & \\ & & & 0 \end{pmatrix},\ d_1 \geq d_2 \geq ... \geq d_r > 0$$

מה המטריצה $A$ עושה מבחינה גיאומטרית אם כך? בתור אופרטור היא פועלת באופן הבא:

$$A : \mathbb{R}^n \to \mathbb{R}^m$$
$$\mathbb{R}^n \overset{V^T}{\to} \mathbb{R}^n \overset{D}{\to} \mathbb{R}^m \overset{U}{\to} \mathbb{R}^m$$

מה קורה לוקטור לאורך הדרך הזו?
הכפלה ב־$V^T$ מבצעת סיבוב. לאחר מכן ההכפלה ב־$D$ מעבירה את $e_i^n$ ל־$d_i e_1^m$ עבור $1 \leq i \leq r$, והשאר $e_k$ עוברים ל־0, כלומר גיאומטרית רק מתחתנו או כיווצנו. לבסוף לוקחים את הקואורדינטות הסטנדרטיות ומסובבים אותם עד שמגיעים ל"מה שרצינו".

**הבעיה**: בהנתן $m$ נקודות ב־$\mathbb{R}^n$ רוצים למצוא ישר (או במקרה הכללי, תת מרחב ממימד $k$ כלשהוא) העובר דרך הראשית כך שהנקודות הנתונות הן הכי קרובות לישר זה.
כמובן שיש להגדיר את המושג "הכי קרובות": לסכום את המרחקים עלול להיות קשה מידי. לכן מחפשים ישר (במקרה של $n = 2$) עם $\sum d_i^2$ מינימלי, כאשר $d_i$ מרחק הנקודה $i$ מהישר. אחת הסיבות שמחפשים את המינימום הזה ־ מאוד קל למצוא אותו. אם $v$ וקטור יחידה הפורש את הישר $l$ הנתון, ונסמן את שורות המטריצה ב־$a_1, ..., a_k, ..., a_m$, אזי:

$$\|a_k\|_2^2 = \|b_k\|_2^2 + \|l_k\|_2^2$$

כאשר $b_k$ הוא ההיטל של $a_k$ על הישר הנתון (החלק של $l$ מהראשית ועד ל־$d_k$).
$a_k$ נתונים, ולכן המינימום של $\sum \|l_k\|^2$ יתקבל כאשר נקבל את המקסימום של $\sum \|b_k\|^2$.
$b_k$ מתקבל כך:

$$b_k = \langle v, a_k \rangle \cdot v$$
$$\Rightarrow \|b_k\|^2 = \langle v, a_k \rangle^2$$

אזי:

$$Av = \begin{bmatrix} \langle a_1, v \rangle \\ \vdots \\ \langle a_m, v \rangle \end{bmatrix}$$

ולכן אנו מחפשים $v \ni \mathbb{R}^n$ כך ש:

$$\|Av\| = \max_{\|v\|=1} \|Av\|_2$$

כלומר, מחפשים את הכיוון של ההיטל על $l$ שימקסם את הערך.
עבור ישר, פשוט נמצא וקטור $v_1$ כך שעבורו מתקבל המקסימום הזה.
אם רוצים מישור כך שסכום ריבועי המרחקים למישור (העובר דרך הראשית) הוא מינימלי, נבחר וקטור $v_1$ כנ"ל, ווקטור ניצב $v_2$ (דהיינו $v_1 \perp v_2$) כך שעבורו מתקבל המקסימום:

$$\max_{v \perp v_1,\ \|v\|=1} \|Av\|_2$$

וכן הלאה למימדים גבוהים יותר.
כמובן ויש להראות כי שיטה חמדנית זו באמת עובדת ־ נעשה זאת.
נגדיר את הערכים הסינגולריים ואת הוקטורים הסינגולריים של $A$ באופן הבא:

- $v_1$ נותן את $\sigma_1(A) = \max_{\|v\|=1} \|Av\|$.
- $v_2$ נותן את $\sigma_2(A) = \max_{v \perp v_1, \|v\|=1} \|Av\|$.
- $\vdots$
- $v_r$ נותן את $\sigma_r(A) = \max_{v \perp v_1 \dots v_{r-1}, \|v\|=1} \|Av\|$.

וכמובן מקבלים כי $\sigma_1(A) \geq \sigma_2(A) \geq \dots \geq \sigma_r(A) > 0$, $\sigma_{r+1}(A) = \dots = \sigma_n(A) = 0$.
$v_1, \dots, v_r$ נקראים הערכים הסינגולריים (הימניים) של $A$, $\sigma_1(A) \geq \sigma_r(A) > 0$ הם הערכים הסינגולריים.
כדי להוכיח שהשיטה אכן עובדת, נוכיח:

**טענה 2.57** יהיו $v_1, \dots, v_r$ הוקטורים הסינגולריים. אזי לכל $k$, $1 \leq k \leq r$, המרחב $V_k = Span(v_1, \dots, v_k)$ הוא המרחב הקרוב ביותר (במובן של סכום ריבועי ההיטלים עליו מקסימלי) לשורות של $A$.

**הוכחה:** באינדוקציה על $k$.
$k = 1$: ברור מהבניה.
$k = 2$: יהי $W$ מרחב ממימד 2 כך שסכום ריבועי ההיטלים של שורות $A$ על $W$ מקסימלי. אם $W$ נפרש ע"י שני וקטורי יחידה אורתוגונליים $w_1, w_2$, אזי סכום ריבועי ההיטלים של שורות $A$ הוא בדיוק $\|Aw_1\|^2 + \|Aw_2\|^2$. בה"כ $w_2$ ניצב ל־$v_1$.
מהגדרת $v_1$ אנו יודעים כי:

$$\|Aw_1\|^2 \leq \|Av_1\|^2$$

מכיוון ו־$v_2$ ניצב ל־$v_1$:

$$\|Aw_2\|^2 \leq \|Av_2\|^2$$

אזי:

$$\|Aw_1\|^2 + \|Aw_2\|^2 \leq \|Av_1\|^2 + \|Av_2\|^2$$

עבור $k$ כללי: נניח ל־$(k-1)$, ולכן $Span(v_1, \dots, v_{k-1}) = V_{k-1}$ הוא הטוב ביותר ממימד $k-1$. נניח $W$ אופטימלי ממימד $k$. ב־$W$ אפשר לבחור וקטור יחידה $w_k$ שניצב ל־$v_1, \dots, v_{k-1}$, ונשלים $w_1, w_2, \dots, w_k$ לבסיס אורתוגונלי של $W$. סכום ריבועי ההיטלים על $W$ הוא:

$$\|Aw_1\|^2 + \dots + \|Aw_{k-1}\|^2 + \|Aw_k\|^2$$

מאופטימליות $V_{k-1}$:

$$\|Aw_1\|^2 + \dots + \|Aw_{k-1}\|^2 \leq \|Av_1\|^2 + \dots + \|Av_{k-1}\|^2$$

אבל אז מהגדרת $v_k$:

$$\|Aw_k\|^2 \leq \|Av_k\|^2$$

מסכמים וסיימנו. ■

**מסקנה 2.58** $r = rank\,(A)$.

**הוכחה:** מההגדרה, לכל $i \geq r+1$, $\sigma_{r+1}\,(A) = 0$, כלומר כל וקטור הניצב ל־$v_1, ..., v_r$ ניצב לכל השורות של $A$. לכן קיבלנו שהמרחב הנפרש ע"י $v_1, ..., v_r$ מכיל את כל השורות של $A$. מצד שני אין תת מרחב ממימד קטן מ־$r$ שיתן לנו תוצאה מקסימלית, אחרת $\sigma_r\,(A) = 0$ בסתירה.
לכן $rank\,(A) = r$, ויתרה מזו, $Span\,(a_i) = Span\,(v_1, ..., v_r)$. ■

נרצה להסתכל על הוקטורים שקיבלנו:
$Av_k$ היה וקטור $m$ מימדי בעל הנורמה $\sigma_k$. נגדיר וקטורי יחידה $u_k = \frac{Av_k}{\sigma_k}$ עבור $k = 1, ..., r$.
נוכיח:

**טענה 2.59** $u_1, ..., u_r$ הם וקטורי יחידה אורתוגונליים, ו:

$$A = \sum_{k=1}^{r} \sigma_k u_k \cdot v_k^T$$

**הערה 2.60** אם משלימים את $u_1, ..., u_r, u_{r+1}, ..., u_m$ לבסיס אורתונורמלי, ואת $v_1, ..., v_r, v_{r+1}, ..., v_n$, מקבלים מהטענה:

$$A = U \begin{pmatrix} \sigma_1 & & & & & \\ & \ddots & & & 0 & \\ & & \sigma_r & & & \\ & & & 0 & & \\ & 0 & & & \ddots & \\ & & & & & 0 \end{pmatrix} V^T$$

כאשר $U = (u_1|...|u_m)$, $V = (v_1|...|v_n)$, ובזה למעשה סיימנו את הוכחת משפט ה־$SVD$.

נוכיח את הטענה: **הוכחה:** הוכחת האורתוגונליות:
באינדוקציה על $r$:
בסיס: $r = 1$ - אין מה להוכיח.
צעד האינדוקציה: נגדיר:

$$B = A - \sigma_1 u_1 \cdot v_1^T$$

$$\Rightarrow Bv_1 = Av_1 - \sigma_1 u_1 \cdot \overbrace{v_1^T \cdot v_1}^{=1} = 0$$

נריץ את האלגוריתם למציאת הוקטורים והערכים הסינגולריים ל־$B$.
יהי $z$ הוקטור הסינגולרי הראשון של $B$.

**טענה 2.61** $z$ ניצב ל־$v_1$.

**הוכחה:** אם לא, יהי $z_1$ ההיטל של $z$ על $v_1$ (היטל זה אינו אפס מההנחה בשלילה). אם $z_1 \neq 0$, אזי $\|z - z_1\| < 1$. נקבל:

$$B \cdot \frac{z - z_1}{\|z - z_1\|} \overset{Bz_1=0}{=} \frac{Bz}{\|z - z_1\|}$$
$$\Rightarrow \left\| B \cdot \frac{z - z_1}{\|z - z_1\|} \right\| = \left\| \frac{Bz}{\|z - z_1\|} \right\| > \|Bz\|$$

בסתירה למקסימליות $z$. ■

מטענת העזר $z$ ניצב ל־$v_1$, אבל אם כך:

$$Bz = Az - \sigma_1 u_1 \overbrace{v_1^T \cdot z}^{=0} = Az$$

ולכן נקבל את $v_2$ כמקסימום על $\underset{\|z\|=1}{max} \|Bz\|$, וכן הלאה. קל לראות שנקבל בתהליך את $v_2, ..., v_r$ ואת $\sigma_2, ..., \sigma_r$, ועל כל אלה:

$$k = 2, ..., r : Bv_k = Av_k$$

ולכן נקבל גם את הוקטורים $u_2, ..., u_r$ (שמוגדרים להיות $u_i = \frac{Av_i}{\|Av_i\|}$), ומהנחת האינדוקציה:

$$B = \sum_{k=2}^{r} \sigma_k u_k v_k^T$$

וכן $u_2, ..., u_r$ אורתוגונליים.
קיבלנו:

$$A = \sum_{k=1}^{r} \sigma_k u_k v_k^T$$

כמו כן אנו יודעים כי $u_2, ..., u_r$ אורתוגונליים. כדי לסיים את ההוכחה, נותר להוכיח כי $u_1$ ניצב ל־$u_2, ..., u_r$.

נניח שלא, ונגיע לסתירה למקסימליות של $v_1$. אם $u_1$ איננו ניצב ל־$u_i$, אזי בה"כ $u_i^T \cdot u_1 > 0$ (ההוכחה למקרה ש־$u_i^T \cdot u_1 < 0$ דומה). נתבונן בוקטור:

$$\frac{v_1 + \varepsilon v_i}{\|v_1 + \varepsilon v_i\|} = \frac{v_1 + \varepsilon v_i}{\sqrt{1 + \varepsilon^2}}$$

נשתמש בקירוב לפי טור טיילור:

$$\frac{1}{\sqrt{1 + \varepsilon^2}} \sim 1 - \frac{\varepsilon^2}{2} + O\left(\varepsilon^4\right)$$

ונקבל:

$$A\left(\frac{v_1 + \varepsilon v_i}{\sqrt{1 + \varepsilon^2}}\right) = \frac{\sigma_1 u_1 + \varepsilon \sigma_i u_i}{\sqrt{1 + \varepsilon^2}}$$

נראה שההיטל של הווקטור הזה על וקטור היחידה $u_1$ כבר גדול מ־$\sigma_1$, ולכן אורכו גדול ממש מ־$\sigma_1$, בסתירה לאופטימליות $\sigma_1$.

$$u_1^T \cdot \left( \frac{\sigma_1 u_1 + \varepsilon \sigma_i u_i}{\sqrt{1+\varepsilon^2}} \right) = \left( \sigma_1 + \varepsilon \sigma_i \cdot u_1^T u_i \right) \left( 1 - \frac{\varepsilon^2}{2} + O\left(\varepsilon^4\right) \right)$$
$$= \sigma_1 + \varepsilon \sigma_i u_1^T u_i + O\left(\varepsilon^2\right) > \sigma_1$$

וזה מסיים את ההוכחה. ■

בסה"כ קיבלנו כי אם $A$ מטריצה מסדר $m \times n$ ודרגה $r$:

$$A = \begin{bmatrix} \\ \underset{m \times r}{U} \\ \\ \end{bmatrix} \begin{bmatrix} \sigma_1 & & \\ & \ddots & \\ & & \sigma_r \end{bmatrix} \left[ r \times n \; V^T \right] = U \cdot D \cdot V^T$$

"למה זה כל כך מעניין?" אם אנחנו יודעים את $r$ מה טוב. אם למשל בנתונים שלנו יש רעש, ואנחנו יודעים כמה אי דיוק אנחנו מוכנים לסבול, אפשר לחשב ו"לזרוק" סיגמאות בהתאם.

על פי הפיתוח עד כה, $k$ השורות הראשונות ב־$V^T$ פורשות את המרחב הטוב ביותר ממימד $k$ במובן של סכום ריבועי המרחקים של שורות $A$ למרחב ממימד $k$. נשתמש בעובדה זו בהוכחה מיד. אבל, יש עוד מושגים של מרחק של מטריצות.

בהנתן $A$ מסדר $m \times n$, אנו רוצים לחפש קירוב למטריצה $A$ מדרגה קטנה $k$. דהיינו, מחפשים את הדבר הבא:

נגדיר אוסף של נורמות על מטריצות ־

- נורמה אחת: מתבוננים על המטריצה כוקטור באורך $m \times n$:

$$\|A\|_F = \left( \sum_{i,j} |a_{i,j}|^2 \right)^{\frac{1}{2}}$$

נורמה זו נקראת נורמת הילברט־שמידט או נורמת פרובניוס.

- נורמה שניה: מתבוננים על $A$ כאופרטור:

$$\|A\|_2 = \max_{\|v\|_2=1} \|Av\| = \sigma_1(A)$$

**טענה 2.62** תהי $A$ כנ"ל עם פירוק $SVD$ $(\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_r > 0)$:

$$A = \sum_{i=1}^{r} \sigma_i u_i v_i^T$$

ונגדיר:

$$B_k = \sum_{i=1}^{k} \sigma_i u_i v_i^T$$

אזי, $B$ היא מטריצה מדרגה $k$, והיא המטריצה הכי קרובה ל־$A$ במובן הבא:

$$\|A-B\|_F = \min_{B,\ rank(B)=k} \|A-B\|_F$$

וכן:

$$\|A-B\|_2 = \min_{B,\ rank(B)=k} \|A-B\|_2$$

**הוכחה:** נוכיח את השיוויון הראשון (ההוכחה לשני מופיעה בסיכומים משנה שעברה): תהי $\overline{B}$ מטריצה מדרגה $k$ הנותנת את $min\|A-B\|_F$ (יש כאן קצת $abuse$ לסימנים), ויהי $V$ המרחב מימד $k \geq$ הנפרש ע"י שורות $\overline{B}$. כל שורה של $\overline{B}$ חייבת להיות שווה להיטל של השורה המתאימה של $A$ על המרחב $V$, אחרת נחליף את השורה של $B$ בהיטל הזה, וזה יקטין את המרחק ולא יגדיל את מימד השורות. אבל אז $\left\|A-\overline{B}\right\|_F^2$ = סכום ריבועי המרחקים של שורות $A$ למרחב $V$, ולכן זה שווה לסכום ריבועי המרחקים למרחב $V_k$ שנפרש ע"י $v_1,...,v_k$ (כי $V_k$ אופטימלי).

מצד שני, נראה כי $\|A-B_k\|_F^2$ שווה למינימום הזה. זה שקול לטענת העזר הבאה:

**טענה 2.63** השורות של $B_k$ הן ההיטל של שורות $A$ על המרחב $V_k$.

**הוכחה:** אם $a$ שורה כלשהיא, ההיטל של $a$ על $V_k$ נראה כך:

$$\sum_{i=1}^{k} (a \cdot v_i) \cdot v_i^T$$

ולכן מטריצת ההטלים נראית כך:

$$\sum_{i=1}^{k} Av_i \cdot v_i^T = \sum_{i=1}^{k} \sigma_i u_i \cdot v_i^T = B_k$$

■

מכיוון וההיטל הוא הערך הגדול ביותר, $\|A-B_k\|_F^2$ הוא הקטן ביותר, וסיימנו. ■

10.12.2013

נשלים את התוצאות לגבי פירוק $SVD$:

נתונה מטריצה $A$ מסדר $m \times n$, וראינו שאפשר למצוא מטריצה $U$ עם עמודות אורתוגונליות מסדר $m \times r$, לכפול אותה במטריצה אלכסונית $D$ שערכיה על האלכסון הם $\sigma_1,...,\sigma_r$ מסדר $r \times r$ ומטריצה $V^T$ אורתוגונלית מסדר $r \times n$ כך ש:

$$A = UDV^T$$

נשים לב כי כאן מדובר בהצגה המצומצמת. מתקיים:

$$\sigma_1 \geq ... \geq \sigma_r > 0$$

וכן $Rank\,(A) = r$, ומתקיים:

$$A = \sum_{k=1}^{r} \sigma_1 u_k \cdot v_k^T$$

אנו מסתכלים כאן על וקטורי עמודה. זוהי קונבנציה של פיסיקאים, מהמאה העשרים מתמטיקאים בדר"כ משתמשים בוקטורי שורה. אנחנו נראה זאת בהמשך בתהליכים סטוכסטיים.
הוכחנו כי:

$$Span\left(v_1, ..., v_k\right)$$

הוא המרחב שאליו השורות של $A$ קרובות ביותר (במובן של סכום ריבועי המרחקים).
לקראת סוף השיעור הגדרנו שתי דרכים להערכת המרחק מ־$A$:

- נורמת פרוביניוס:

$$\|A\|_F = \left(\sum_{i,j} a_{ij}^2\right)^{\frac{1}{2}}$$

- 

$$\|A\|_2 = \max_{\substack{x \in \mathbb{R}^n \\ \|x\|_2 = 1}} \|Ax\|_2$$

וטענו:

**טענה 2.64** אם מחפשים מטריצה $B$ מדרגה $k \geq$ כך שהיא הכי קרובה ל־$A$ באחת משתי הנורמות $\|\cdot\|_F$ או $\|\cdot\|_2$, אזי:

$$B_k = \sum_{i=1}^{k} \sigma_i u_i \cdot v_i^T$$

היא מטריצה קרובה ביותר כזו.

נוכיח שוב בקצרה לגבי נורמת פרוביניוס ־ ההוכחה לגבי הנורמה השניה מופיעה בסיכומי הקורס בשנה שעברה. **הוכחה:** תהי $B$ מטריצה קרובה ביותר ל־$A$ כך ש:

$$\|A - B\|_F = \min_{C \ s.t. \ rank(C)=k} \|A - C\|_F$$

יהי $V = Span\{rows\ of\ B\}$. אזי $dim\left(V\right) \leq k$. אם השורה ב־ $B$ המתאימה לשורה ב־$A$ אינה שווה בדיוק לנקודה הקרובה ביותר ב־$V$ לשורה של $A$, אפשר להחליף את השורה בשורה ב־$B$ בהיטל של השורה של $A$ על תת המרחב של $V$, ולהקטין את המרחק בין המטריצות בנורמת פרובניוס. לכן כל שורה היא היטל של $V$ על השורה המתאימה של $A$. על כן $\|A - B\|^2$ הוא סכום ריבועי המרחקים של שורות $A$ מתת המרחב $V$, אבל $B_k$ היתה אופטימלית במקרה הזה, ולכן:

$$\|A - B_k\| \leq \|A - B\|_F$$

■

לצורך ההוכחה הזו הוכחנו למה:

**למה 2.65** תהי $B_k = \sum_{i=1}^{k} \sigma_i u_i v_i^T$. אזי השורות של $B_k$ הן ההיטל של שורות $A$ על המרחב $Span\,(v_1, ..., v_k)$.

נוכיח כעת עבור הנורמה השניה. אין מה להוכיח אם $k = r$. אחרת, נזדקק ללמות:

**למה 2.66**

$$\|A - B_k\|_2 = \sigma_{k+1}$$

**הוכחה:**

$$A - B_k = \sum_{i=k+1}^{r} \sigma_i u_i v_i^T$$

יהיה $v$ הוקטור הסינגולרי הראשון של $A - B_k$. אזי אפשר לרשום אותו באופן הבא:

$$v = \sum_{i=1}^{n} \alpha_i v_i, \ \|v\|_2 = 1$$

אזי:

$$\|(A - B_k)\, v\|^2 = \left\| \left( \sum_{i=k+1}^{r} \sigma_i u_i v_i^T \right) \cdot \left( \sum_{j=1}^{n} \alpha_j v_j \right) \right\|$$

נשים לב כי במכפלה אנו מקבלים בעצם את המכפלה הטנזורית של $v_i$ ו־$v_j$, מכיוון והוקטורים הם אורתוגונליים, אזי אם $i \neq j$, $\langle v_i, v_j \rangle = 0'$, ועל כן:

$$= \left\| \sum_{i=k+1}^{r} \alpha_i \sigma_i u_i \right\|^2 = \sum_{i=k+1}^{r} \alpha_i^2 \sigma_i^2$$

נשים לב כי $\sum_{i=1}^{n} \alpha_i^2 = 1$ (כי $\|v\|_2 = 1$), והמקסימום מתקבל עבור $\alpha_{k+1} = 1$ והשאר $0$ (שכן הערכים הסינגלריים האחרים רק קטנים או שווים לו). ■

כדי להשלים את ההוכחה עבור הנורמה השניה, נוכיח את הלמה הבאה:

**למה 2.67** לכל מטריצה $B$ מדרגה $\geq k$ מתקיים:

$$\|A - B\|_2 \geq \sigma_{k+1}$$

**הוכחה:** יהי:

$$\{ v \in \mathbb{R}^n | \, Bv = 0 \} = N\,(B)$$

מרחב האפס של $B$. אזי $dim\,(N\,(b)) \geq n - k$. על כן:

$$N\,(B) \cap Span\,(v_1, ..., v_{k+1}) \neq 0$$

משיקולי מימדים, ולכן יש וקטור $z$ שאיננו אפס בחיתוך. נבחר $\|z\|_2 = 1$. נחשב:

$$(A-B)\,z = Az$$

כי $z \in N(B)$. מצד שני, $z$ נפרש על ידי הוקטורים $v_1, ..., v_{k+1}$, ועל כן ניתן לרשום אותו כצ"ל שלהם:

$$z = \sum_{i=1}^{k+1} \alpha_i v_i$$

כאשר מכיוון ו־$\|z\|_2 = 1$, אזי $\sum \alpha_i^2 = 1$. לכן:

$$\begin{aligned}\|Az\|^2 &= \left\| \left( (\sum_{i=1}^{n} \sigma_i u_i v_i^T) \left( \sum_{j=1}^{k+1} \alpha_j v_j \right) \right\|^2 = \left\| \left( \sum_{i=1}^{r} \sigma_i u_i v_i^T \right) \left( \sum_{j=1}^{k+1} \alpha_j v_j \right) \right\| \\ &= \left\| \sum_{i=1}^{k+1} \alpha_i \sigma_i u_i \right\|^2\end{aligned}$$

ובדומה ללמה הקודמת, מכיוון ו־$u_i$ אורתוגונלים זה לזה:

$$= \left\| \sum_{i=1}^{k+1} \alpha_i^2 \sigma_i^2 \right\| \geq \sigma_{k+1}^2 \cdot \sum_{i=1}^{k+1} \alpha_i^2 = \sigma_{k+1}^2$$

כנדרש. ■

וכאן סיימנו את ההוכחה לגבי הנורמה השניה!
נבהיר נקודה נוספת לבקשת הקהל:

**למה 2.68** יהיו $v_1, ..., v_k$ הווקטורים הסינגולריים, $\sigma_1, ..., \sigma_r$ הערכים הסינגולריים, ויהיו:

$$A = \sum_{i=1}^{n} \sigma_i u_i v_i^T,\ B_k = \sum_{i=1}^{k} \sigma_i u_i v_i^T$$

אזי שורות $B_k$ הן ההיטלים של שורות $A$ על $V_k = Span(v_1, ..., v_k)$.

**הוכחה:** תהי $a$ שורה של $A$. ההיטל של $a$ על $V_k$ הינו:

$$\sum_{i=1}^{k} (a \cdot v_i)\, v_i^T$$

ולכן ההיטלים של כל שורות המטריצה $A$ הם:

$$\sum_{i=1}^{k} A v_i v_i^T = \sum_{i=1}^{k} \left( \sum_{j=1}^{k} \sigma_j u_j v_j^T \right) v_i v_i^T = \sum_{i=1}^{k} \sigma_i u_i v_i^T = B_k$$

■

## 2.5 מטריצות סימטריות ממשיות ושרשראות מרקוב

נעבור כעת למטריצות סימטריות ממשיות. אלו מטריצות "יפות", שיש להן תכונות מיוחדות. למשל, יש להן יציבות נומרית - אם משנים את הערכים ב$\varepsilon$ מסויים ההתנהגות הכללית שלהם נשמרת. כמו כן הן גם שימושיות, ונראה לא מעט שימושים המרכזיים למטריצות אלו ולע"ע שלהם. שימוש אחד כזה - נביט במטריצת שכינויות של גרף לא מכוון - היא מטריצה סימטרית, שכן אם יש צלע מקודקוד אחד לשני אז היא גם צלע מהקודקוד השני לראשון. מסתבר שיש כאן הרבה שימושים לע"ע של המטריצה.

מטריצות סימטריות ממשיות מקיימות (זו למעשה ההגדרה של מטריצה סימטרית):

$$A = A^T$$

ונשתמש בתכונה הזו[19].

**משפט 2.69** תהי $A$ מטריצה סימטרית ממשית מסדר $n \times n$. אזי קיימת מטריצה אורתוגונלית $U$ כך ש:

$$A = UDU^T$$

כך ש-$D$ מטריצה אלכסונית, ועל האלכסון מופיעים הערכים העצמיים של $A$ - נסמנם ב-$d_1, ..., d_n$, ו-$d_i$ ממשיים.

או בדרך אחרת:

ל-$A$ יש בסיס אורתוגונלי של ווקטורים עצמיים, והע"ע הם $d_1, ..., d_n$ ממשיים.

**הגדרה 2.70** מטריצה סימטרית $A$ נקראת מוגדרת חיובית למחצה (מוגדרת אי שלילית - PSD=Positive semi definite) אם לכל ווקטור $x \ni \mathbb{R}^n$:

$$x^T Ax \geq 0$$

**טענה 2.71** התנאים הבאים שקולים:

1. $A$ היא $PSD$.
2. $A = M \cdot M^T$ עבור מטריצה ממשית $M$.
3. כל הערכים העצמיים של $A \geq 0$.

**הוכחה:** $2 \Leftarrow 3$: אם כל הע"ע של $A \geq 0$, אזי מהמשפט מעלה קיים פירוק:

$$A = UDU^T$$

וכן $d_i \geq 0$. נגדיר:

$$M = U\sqrt{D}$$

[19] נשים לב שכל מה שנדבר ספה גם נכון למטריצות הרמיטיות, שאלו מטריצות המקיימות $A = A^*$, אבל לא נדון בהן במסגרת הקורס הזה.

כאשר:

$$\sqrt{D} = \begin{pmatrix} \sqrt{d_1} & & \\ & \ddots & \\ & & \sqrt{d_n} \end{pmatrix}$$

ונקבל:

$$A = \overbrace{U\sqrt{D}}^{M} \cdot \overbrace{\sqrt{D}U^T}^{M^T}$$

$2 \Leftarrow 1$: מהנתון, נחשב:

$$x^T Ax = x^T MM^T x = \left(M^T x\right)^T M^T x = \left\langle M^T x, M^T x \right\rangle = \left\| M^T x \right\|^2 \geq 0$$

$3 \Leftarrow 1$: יהיו $d_i$ הע"ע של המטריצה. ניתן לסמן:

$$x = \sum_{i=1}^{n} \alpha_i u_i$$

כאשר $u_i$ הם הוקטורים העצמיים. אזי:

$$x^T Ax = \left(\sum \alpha_i u_i^T\right)\left(\sum \alpha_j Au_j\right) = \left(\sum \alpha_i u_i^T\right)\left(\sum \alpha_j d_j u_j\right) = \sum_{i=1}^{n} \alpha_i^2 d_i \geq 0$$

$3 \Leftarrow 1$: נתון כי לכל $x \in \mathbb{R}^n$ מתקיים: $x^T AX \geq 0$, בפרט עבור וקטור עצמי $v$ עם ע"ע $\lambda$. אזי:

$$\begin{aligned} &0 \leq v^T Av = v^T \cdot (\lambda v) = \lambda v v^T = \lambda \left\| v \right\|^2 \\ &\Rightarrow \lambda \geq 0 \end{aligned}$$

■

**טענה 2.72** מתקיים:

1. אם $A$ חיובית למחצה אז גם $\lambda A$ עבור $\lambda \geq 0$ חיובית למחצה.
2. אם $A, B \in PSD$ אז גם $A + B \in PSD$.

**הוכחה:** הראשון פשוט, השני:

$$x^T \left(A + B\right) x = x^T Ax + x^T Bx \geq 0$$

■

מה הטענה הזו בעצם אומרת? אוסף המטריצות $PSD$ לא מהווה תת מרחב, אולם אפשר לכפול בסקלר חיובי. מתקיים:

$$\lambda A + (1-\lambda) B \in PSD \; \lambda \in [0,1]$$

קבוצה כזו היא קבוצה קמורה. היא קונוס $Cone$ במרחב.
זוהי תכונה אחת ש"נוח" במטריצות סימטריות.

דבר נוסף שהוא נוח - היכולת להגדיר את הערכים העצמיים. במטריצות כלליות השתמשנו בערכים סינוגלריים, כי לאו דווקא היתה הגדרה לע"ע. כאן לעומת זאת יש לנו יותר חופש:

**משפט** $Rayleigh - Ritz$

**משפט 2.73** תהי $A$ מטריצה מסדר $n \times n$ סימטרית ממשית עם ע"ע $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n$. אזי:

$$\lambda_1 = \max_{0 \neq x \in \mathbb{R}^n} \frac{x^T A x}{\|x\|^2} = \max_{\|x\|=1} x^T A x$$

והמקסימום מתקבל עבור וקטור עצמי $v_1$ עם ערך עצמי $\lambda_1$. באופן כללי אם $v_1, ..., v_k$ וקטורים עצמיים המתאימים לערכים העצמיים $\lambda_1, ..., \lambda_k$, אזי:

$$\lambda_{k+1} = \max_{x \in V_k^{\perp}} \frac{x^T A x}{\|x\|^2} = \max_{\substack{\|x\|=1 \\ x \in V_k^{\perp}}} x^T A x$$

כאשר $V_k^{\perp}$ הוא המרחב הניצב לכל הוקטורים $v_1, ..., v_k$.

**הוכחה:** מתקיים:

$$A = V D V^T$$

כאשר $D$ אלכסונית ו-$V$ אורתוגונלית, ונסמן את הע"ע על האלכסון של $D$ ב-$\lambda_1, ..., \lambda_n$. נחשב:

$$\begin{aligned} x^T A x = x^T V D V^T x \overset{V \; ortho.}{=} \sum_{i=1}^{n} \lambda_i \left(V^T x\right)_i^2 \leq \max_i \{\lambda_i\} \cdot \sum_{i=1}^{n} \left(V^T x\right)_i^2 \\ = max\{\lambda_i\} \cdot \left\|V^T x\right\|^2 \overset{V \; ortho.}{=} max\{\lambda_i\} \cdot \|x\|^2 \\ \Rightarrow \frac{x^T A x}{\|x\|^2} \leq max\{\lambda_i\} = \lambda_1 \end{aligned}$$

ומצד שני, עבור ו"ע $v_1$ המתאים לע"ע $\lambda_1$ מתקיים $\|v_1\| = 1$ (שכן מהמשפט הראשון בפרק זה, ל-$A$ יש בסיס אורתוגונלי של וקטורים עצמיים), ואז:

$$v_1^T A v_1 = v_1^T \lambda_1 v_1 = \lambda_1 v_1^T v_1 = \lambda_1$$

כאשר ממשיכים ומתבוננים בווקטורים ב־$V_k^{\perp}$, אזי נמצא שם $V_{k+1}$ המקבל ערך $\lambda_{k+1}$, ובדרך דומה אפשר להוכיח שזה המקסימום על $V_k^{\perp}$. ■

באופן דואלי אפשר להתחיל מן המינימום:

$$\lambda_n = \min_{\|x\|=1} x^T A x$$

והמינימום מתקבל על וקטור עצמי $v_n$ עם ערך עצמי $\lambda_n$.
אם $v_k, ..., v_n$ וקטורים עצמיים עם ערכים עצמיים $\lambda_n$. $\lambda_1, ..., \lambda_n$. אזי:

$$\lambda_{k-1} = \begin{array}{ll} min & x^T A x \\ \|x\| = 1 & \\ x \in W_k^{\perp} & \end{array}$$

כאשר:

$$W_k^{\perp} = \{w \,|w \perp v_k, ..., v_n\}$$

והמינימום מתקבל על וקטור עצמי $v_{k-1}$ עם ערך עצמי $\lambda_{k-1}$.
באופן דומה, ננסח את :

**משפט** $Courrant - Fischer$

**משפט 2.74**

$$\begin{array}{ll} \min & \max \quad x^T A x = \lambda_2 \\ V & \|x\| = 1 \\ dim\,(V) = n-1 & x \in V \end{array}$$

ובאופן כללי:

$$\begin{array}{ll} \min & \max \quad x^T A x = \lambda_k \\ V & \|x\| = 1 \\ dim\,(V) = n-k+1 & x \in V \end{array}$$

וכמו כן:

$$\begin{array}{ll} max & min \quad x^T A x = \lambda_k \\ V & \|x\| = 1 \\ dim\,(V) = k & x \in V \end{array}$$

ההוכחה די דומה למה שראינו, אבל לא נראה אותה.
בתור הכנה לשיעור הבא, נסתכל על מטריצות ממשיות שכל הערכים בהם חיוביים. מטריצות אלו מופיעות כמטריצות מעבר בתהליכי מרקוב בין מצב אחד לשני - נראה זאת בשיעור הבא. מכיוון ואנו חותרים לשימוש הזה, מטריצות שהערכים שלהם לא חיוביים לא מעניינים אותנו (כל תא במטריצה יהיה ההסתברות לעבור ממצב אחד לשני).
בינתיים, קצת תיאוריה לפני השימוש:

**מקרה פרטי של משפט** $Perrron-Frobenius$

**טענה 2.75** תהי $M$ מטריצה סימטרית ממשית, ונסמן $M=(m_{ij})$, וננית $m_{ij}>0$. יהי $v$ וקטור עצמי המתאים לערך העצמי $\lambda_1$ = הערך העצמי הגדול ביותר של $M$. אזי $\lambda_1>0$, וכן ניתן לבחור לו ו"ע $v>0$, כלומר אם $v=(v_1,...,v_n)$, אזי $v_i>0$ לכל $i$.

**הוכחה:** $\lambda_1>0$ ברור, כי זה המקסימום של $x^TMx$ ואפשר לקבל $0<$.
ממשפט ה־$SVD$, אם $v$הוא הווקטור העצמי המתאים הגדול ביותר, אזי $v$ נותן את המינימום:

$$\left\|M-\lambda vv^T\right\|_F$$

והווקטור $v$ פורש ישר שעליו ההטלות הן מקסימליות. גיאומטרית, מכיוון וכל ערכי $M$ ברבע הימני העליון, הוקטור $v$ חייב גם לעבור שם ע"מ לתת את המינימום (אם קואורדינטה שלילית, אם נעביר לערך המוחלט נקרב), ולכן כל הקואורדינטות של $v$ הן חיוביות ממש. ■

**הגדרה 2.76** אם $A$ מטריצה סימטרית, אזי הרדיוס הספקטרלי של $A$ הינו:

$$\rho(A):=max\{|\lambda|\,|\lambda\ eighnvalue\ of\ A\}$$

מכאן ועד סוף הפרק נניח כי $M$ כפי שציינו מעלה, כלומר כלומר ממשית סימטרית וכן $m_{ij}>0$, אלא אם כן נאמר אחרת.

**טענה 2.77** מתקיים $\lambda_1>|\lambda_n|$.

וטענה נוספת:

**טענה 2.78** $\lambda_1>\lambda_2$.

משתי הטענות האלו נקבל:

**מסקנה 2.79**

$$\rho(A)=\lambda_1>max\{|\lambda_i|\,|i=2,...,n\}$$

נוכיח תחילה את הטענה האחרונה: **הוכחה:** נשים לב כי:

$$\lambda_2=\begin{array}{c}max\\ x\perp v_1\\ \|x\|=1\end{array}\quad x^TMx$$

יהי $x$ הוקטור הממקסם את הביטוי מעלה. מכיוון ש־$x\perp v_1$, לא לכל הקואורדינטות של $x$ יש אותו סימן (כי $v_1$ חיובי כולו). אזי:

$$x^TMx=\sum_{i,j}m_{ij}x_ix_j$$

נסמן: $\overline{x} = (|x_1|, ..., |x_n|)$, כאשר $x = (x_1, ..., x_n)$, ונקבל עבור $\|x\| = 1$ כאשר $x \perp v_1$ כי:

$$x^T M x < \overline{x}^T M \overline{x} \leq \lambda_1$$

ולכן עבור $v_2$ המתאים ל־$\lambda_2$ נקבל:

$$\lambda_2 < \lambda_1$$

■

אותה הוכחה בדיוק עובדת עבור טענה 2.77: **הוכחה:** באותו אופן:

$$\lambda_n = \min_{\|x\|=1} x^T M x$$

והמינימום מתקבל על $v_n$, ו־$v_n \perp v_1$. לכן ב־$v_n$ גם יש קואורדינטות חיוביות ושליליות, שכן אחרת לא יוכל להיות ניצב לוקטור $v_1$ אשר הוא חיובי ממש. אזי ב־$min \sum m_{ij} x_i x_j$ לא כל המכפלות יכולות להיות בסימן זהה, כי $x_i^2 \geq 0$, ולפחות חלקם חיוביים ממש.

מכאן קל להסיק כי:

$$\lambda_1 > |\lambda_n|$$

שכן:

$$|\lambda_n| = \left| \sum m_{ij} x_i x_j \right| < \sum m_{ij} |x_i| |x_j| \leq \lambda_1$$

■

24/12/2013

אדמיניסטרטיבית - לגבי המבחן, מלבד התרגילים והראיונות נקבל עבודת בית. המטרה היא כמובן שנדע את החומר ולא לתת ציונים. יכול להיות שזה יהיה במסגרת זמן קצרה כמו בשנים שעברו, או עבודה מסובכת יותר לזמן ארוך יותר, הפורמט יוחלט מאוחר יותר.

נחזור בקצרה על מה שדיברנו עליו בשיעור הקודם - ראינו את מקרה פרטי של משפט Perron Forbenious (את המקרה הכללי בתקווה נראה לקראת סוף החומר):

תהי $M$ מטריצה מסדר $n \times n$ סימטרית ממשית, ונסמן $M = (m_{ij})$, ונניח $m_{ij} > 0$. הוכחנו את הלמה:

**למה 2.80** יהי $V$ וקטור עצמי של הערך העצמי הגדול ביותר של $M$. אזי $V = (v_1, ..., v_n)$, $v_i > 0$.

הוכחנו את הלמה באמצעות הפירוק $M = UDU^T$, כאשר $D$ אלכסונית המכילה את הע"ע שהינם ממשיים, ומניחים שהסידור עליה הוא $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n$, ו־$U$ מטריצה אורתוגונלית.

השורה הראשונה של $U$ מגדירה כיוון במרחב $\mathbb{R}^n$ כך שהנקודות ב־$\mathbb{R}^n$ המתאימות לשורות של $M$ קרובות ביותר לישר הזה. $v_i > 0$, כי (הכי קל לראות זאת בציור) אם יש ב־$v$ קואורדינטות שליליות, אזי הערך החיובי של אותה קואורדינטה יהיה קרוב יותר לנקודות.

הראנו גם $\lambda_1 > |\lambda_i|$ עבור $i = 2, ..., n$, $\lambda_1 = \max_{\|v\|=1} v^T M v$:

אם $u$ וקטור עצמי המתאים ל־$\lambda_i$, $i \geq 2$, כאשר $\langle u, v \rangle = 0$, נקבל כי ב־$u$ יש קואורדינטות שליליות (אחרת המכפלה הפנימית לא היתה 0). כעת $\lambda_i = u^T M u$ ־ נגדיר וקטור:

$$\overline{u} = (|u_1|, ..., |u_n|), \ 1 = \|\overline{u}\| = \|u\|$$

וכעת נקבל:

$$\begin{aligned} &\lambda_1 \geq \overline{u}^T M \overline{u} > u^T M u = \lambda_i \\ &\Rightarrow \lambda_1 \left|\overline{u}^T M \overline{u}\right| > \left|u^T M u\right| = |\lambda_i| \\ &\Rightarrow \left|\sum |u_i| \, |u_j| \, m_{i,j}\right| > \left|\sum u_i u_j m_{i,j}\right| \end{aligned}$$

כאשר בביטוי האחרון בצד ימין חלק מהביטויים שליליים וחלקם חיוביים.

**לסיכום**: אם $M = (m_{ij})$ מטריצה $n \times n$, $m_{i,j} > 0$ לכל $i, j$, אזי הווקטור עצמי $v$ המתאים לערך העצמי הגדול ביותר $\lambda_1$ הוא וקטור שכל הקואורדינטות שלו חיוביות, ובנוסף $|\lambda_i| < \lambda_1$ עבור $i = 2, ..., n$, כאשר $\lambda_i$ הערכים העצמיים האחרים.

נשתמש במשפט הזה על מנת להסיק מסקנות לגבי העלאה בחזקה של מטריצה שכזו:

$$M^k = \left(UDU^T\right)^k = UD^kU^T$$

כאשר:

$$D^k = \begin{pmatrix} \lambda_1^k & & \\ & \ddots & \\ & & \lambda_n^k \end{pmatrix}$$

ולכן:

$$\left(\frac{M^k}{\lambda_1}\right) = \left(U\frac{D}{\lambda_1}U^T\right)^k = ... = U \begin{pmatrix} 1 & & & \\ & \left(\frac{\lambda_2}{\lambda_1}\right)^k & & \\ & & \ddots & \\ & & & \left(\frac{\lambda_n}{\lambda_1}\right)^k \end{pmatrix} U^T$$

$$\overset{k\to\infty}{\longrightarrow} U \begin{pmatrix} 1 & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{pmatrix} U^T = v \cdot v^T$$

כלומר, אם $M$ חיובית ממש וסימטרית, ו־$v$ וקטור עצמי המתאים לערך העצמי הגדול ביותר $\lambda_1$, אזי:

$$\lim_{k\to\infty} \left(\frac{M}{\lambda_1}\right)^k = v \cdot v^T$$

המשפט הזה גם נכון גם אם $M$ לא חיובית ממש עבור ערכים מסויימים, נראה זאת ־ מקרה פרטי נוסף:

**מסקנה 2.81** תהי $M$ סימטרית וחיובית, כלומר $m_{i,j} \geq 0$. אם קיים $k_0$ כך ש־$M^{k_0}$ חיובית ממש (כלומר כל איברי $M^{k_0}$ חיוביים ממש), אזי הגבול הנ"ל עדיין מתקיים:

$$\lim_{k\to\infty}\left(\frac{M}{\lambda_1}\right)^k = v\cdot v^T$$

**הוכחה:** בנפנוף ידיים - ממשפט ה־$SVD$: $M = UDU^T$. מתקיים:

$$M^{k_0} = UD^{k_0}U^T \Rightarrow \frac{M^{k_0 k}}{\lambda_1^{k_0 k}} = \left(\frac{M^{k_0}}{\lambda_1^{k_0}}\right)^k \to v\cdot v^T$$

אבל זו רק תת סדרה אחת (ויכול להיות שהיא מחזורית אבל "באמצע" דברים משתגעים). אבל מהמשפט על $M^{k_0}$ אנו יודעים כי:

$$1 > \left|\left(\frac{\lambda_i}{\lambda_1}\right)^k\right|$$

ולכן כאשר $k \to \infty$ זה שואף לאפס, ונקבל:

$$\left(\frac{M}{\lambda_1}\right)^k \to v\cdot v^T$$

■

### 2.5.1 תהליכים מקריים ושרשראות מרקוב

למה בכלל אנחנו מתעניינים במטריצות חיוביות?

הסיבה היא שהמטריצות האלה מופיעות ב**תהליכים מקריים**: אם נתבונן בתהליך מקרי על $n$ מצבים $V = \{1, ..., n\}$. בהתחלה מתחילים בהתפלגות נתונה:

$$Pr\left(X_0 = i\right) = p_i,\ 1 \leq i \leq n,\ \pi_0 = (p_1, ..., p_n)$$

בכל צעד אם נמצאים במצב $i$ עוברים בצעד הבא למצב $j$ ההסתברות $p_{i,j}$, כלומר:

$$Pr\left(X_{t+1} = j | X_t = i\right) = p_{i,j}$$

ונגדיר $P = (p_{i,j})$. מטריצה זו הינה מטריצת המעבר של התהליך המקרי. מטריצה זו היא חיובית (לאו דווקא ממש) וסימטרית!

דוגמא לתהליך כזה - נתון גרף בו לכל קודקוד אותה דרגה (גרף $d$־רגולרי), ועוברים בכל צעד לאחד השכנים בהתפלגות אחידה, אזי נקבל $P$ חיובית וסימטרית.

נמשיך בניתוח:

$$\pi_0 = \left(p_1^0, ..., p_n^0\right)$$
$$\pi_1 = \left(p_1^1, ..., p_n^1\right)$$
$$p_j^1 = \sum_{i=1}^{n} p_i \cdot p_{i,j} \Rightarrow \pi_1 = \pi_0 \cdot P,\ \pi_t = \pi_0 P^T$$

נשים לב כי אין זה אומר בוודאות שכל התהליך הזה מתכנס.

בהנתן מטריצה אי שלילית $M=(m_{i,j})$ מסדר $n\times n$, נתאים ל־$M$ גרף מכוון $G=(V,E)$ באופן הבא: $V=\{1,...,n\}$, $(i,j)\in E$ אמ"מ $m_{i,j}>0$.
נרצה להגדיר בדיוק את המקרים בהם יש "דברים מחזוריים" - כלומר מתי אנחנו יודעים בוודאות שההסתברות לא תתכנס לאיזשהוא ערך קבוע:

**הגדרה 2.82** יהי $G$ גרף מכוון קשיר חזק (כלומר, ישנו מסלול מכוון בין כל שני קודקודים). נאמר ש־$G$ מחזורי עם מחזור $k\geq 2$ אם ניתן לחלק את קודקודי הגרף לקבוצות זרות $S_1,...,S_k$, כך ש: $V=S_1\cup...\cup S_k$

$$E\subseteq S_1\times S_2\cup S_2\times S_3\cup...\cup S_k\times S_1$$

גרף קשיר חזק איננו מחזורי אם אין פירוק כזה.

קצת אינטואיציה גיאומטרית - גרף קשיר חזק מחזורי בעצם "מתחלק" כך שהצלעות הן מקבוצה $i$ לקבוצה $i+1$ ומ־$n$ ל־$1$ בלבד - נראה כמו מעגל.
תחת ההגדרה הזו קל לנסח את משפט Perron-Frobenious (גרסא יותר כללית - קיימות גרסאות אף יותר כלליות אך הן אינן רלוונטיות לנו):

**משפט 2.83** תהי $M$ מטריצה אי שלילית, ויהי $\rho(M)$ הערך הסינגולרי הגדול ביותר של $M$, ונניח שהגרף המתאים ל־$M$ קשיר חזק ואיננו מחזורי.
אזי $\rho(M)$ הוא ערך עצמי פשוט גם מצד ימין ומצד שמאל, כלומר קיימים וקטורים $x_l,x_r$ כך ש:

$$Mx_r=\rho(M)\,x_r,\ \ x_l^TM=\rho(M)\,x_l^T$$

וכל וקטור עצמי אחר עם ע"ע $\rho(M)$ הוא כפולה של $x_r$ או $x_l$ בהתאם לצד המתאים, ומתקיים:

$$\left(\frac{M}{\rho(M)}\right)^k\xrightarrow{k\to\infty}\frac{x_r\cdot x_l^T}{\langle x_r,x_l\rangle}$$

הוכחת היחידות דורשת להוכיח את העובדה שכל הערכים העצמיים האחרים קטנים ממש בערך מוחלט מ־$\rho(M)$ - זה דורש מעט עבודה שלא נעשה. במקרה הסימטרי זה יותר קל.

**הערה 2.84** במקרה הסימטרי $x_r=x_l=v$, ובחרנו $\|v\|=1$.

**הגדרה 2.85** תהליך מקרי על $n$ מצבים עם מטריצת מעבר $(p_{i,j})=P$ נקרא שרשרת מרקוב סופית.

במקרה הזה, אם הגרף המתאים ל־$P$ קשיר חזק ואיננו מחזורי, אזי קל להצביע על וקטור שמאלי $x_r=(1,1,...,1)=\overline{1}$:

$$(p_{i,j})\begin{pmatrix}1\\\vdots\\1\end{pmatrix}=\begin{pmatrix}\sum_{j=1}^m p_{i,j}\end{pmatrix}=\begin{pmatrix}1\\\vdots\\1\end{pmatrix}$$

לכן $\overline{1}$ הוא וקטור עצמי שמאלי עם ערך עצמי 1, וקל לראות שהרדיוס הספקטרלי גם הוא $\rho(P)=1$.

יהי $x_l=\pi$ וקטור עצמי שמאלי המתאים לערך העצמי 1, $\pi=\left(\pi^1,...,\pi^n\right)$, $\sum_{i=1}^n \pi^1=$ 1 ואז ממשפט $P-F$:

$$\lim_{t\to\infty} P^t=\overline{1}\cdot\pi^T\left(=\frac{\overline{1}\cdot\pi^T}{\langle 1,\pi\rangle}\right)=\begin{pmatrix}\pi^1 & \cdots & \pi^n\\ \pi^1 & \cdots & \pi^n\\ \vdots & \ddots & \vdots\\ \pi^1 & \cdots & \pi^n\end{pmatrix}$$

אם מתחילים בהתפלגות כלשהיא $u=(u_1,...,u_n)$, $u_i\geq 0$, $\sum_{i=1}^n u_i=1$.

$$u\cdot P^t\overset{t\to\infty}{\longrightarrow}(u_1,...,u_n)\begin{pmatrix}\pi^T\\ \pi^T\\ \vdots\\ \pi^T\end{pmatrix}=\left(\sum u_i\right)\pi^T=\pi^T$$

כלומר, לא משנה מאיפה התחלנו, "לאחר הרבה זמן" אנחנו מגיעים להתפלגות שאיננה תלויה בנקודת ההתחלה שלנו, אלא במטריצה $P$ בלבד.

נקבל כי אפשר לחלק את הגרף לרכיבי קשירות חזקים, והגרף של רכיבי הקשירות הללו איננו מחזורי (וכל הדרכים מובילות לבסוף לרכיב סופי במקרה של רכיבים חזקים - במקרה הכללי יכולים להיות כמה רכיבים כמצב סופי, אבל אז כמובן יש חשיבות לנקודת ההתחלה. לא נתעסק במקרים אלו). עולות כאן שאלות כמובן כגון תוך כמה זמן מתכנסים וכו', אבל בכל אופן התוצאה הסופית נותרת בעינה.

יהי $G$ גרף לא מכוון עם משקולות $0\leq w_{i,j}$ על הצלעות. נתבונן בתהליך מרקוב הבא: אם אני בקודקוד $i$, אזי עוברים לקודקוד $j$ בהסתברות $\frac{w_{i,j}}{\sum_{j=1}^n w_{i,j}}$. אם $G$ קשיר, אזי מטריצת המהלך $P$ קשירה חזק.

כיוון שהגרף $G$ לא מכוון, $P$ יכולה להיות מחזורית רק עבור $k=2$, וזה קורה אם הגרף $G$ הוא דו צדדי (bipartite), כלומר יש חלוקה של הקודקודים $V=L\cup R$ כך ש-$L\cap R=\phi$, וכן $E\subset L\times R$ (כלומר אין צלעות בתוך הקבוצות, רק מקודקוד בקבוצה אחת לקודקוד בקבוצה השניה). לכן, אם הגרף $G$ איננו דו-צדדי, ההליכה המקרית על $G$ מתכנסת להתפלגות קבועה. נגדיר:

$$0<w_i=\sum_{j=1}^n w_{i,j}$$

$$w=\sum_{i=1}^n w_i$$

נגדיר וקטור הסתברות:

$$\pi=\frac{(w_1,w_2,...,w_n)}{w}$$

**טענה 2.86** $\pi$ הוא וקטור עצמי שמאלי עם ערך עצמי 1.

**הוכחה:** נחשב:

$$(\pi P)_j = \sum_{i=1}^{n} \pi_i p_{i,j} = \sum_{i=1}^{n} \frac{w_i}{w} \cdot \frac{w_{i,j}}{w_i} = \frac{\sum_{i=1}^{n} w_{i,j}}{w} = \frac{w_j}{w} = \pi_j$$

■

נקבל כי אם הגרף קשיר חזק ואינו דו צדדי, מקבלים "לאחר הרבה זמן" כי התפלגות אחידה מתכנסת להתפלגות אחידה על הצלעות.

כאמור עולה השאלה, באיזה קצב ההתכנסות מתרחשת? **אם $\lambda_1$ גדול בהרבה מהע"ע האחרים, ההתכנסות תהיה מהירה מאוד**, כלומר אחרי מעט מאוד זמן "שוכחים" איפה היינו.

**הגדרה 2.87** גרף (לא מכוון) נקרא $d$-רגולרי אם לכל קודקוד יש $d$ שכנים.

**מסקנה 2.88** אם $G$ גרף $d$-רגולרי שאיננו דו צדדי, אזי למטריצת המעבר שלו יש וקטור עצמי $\overline{1}$ גם מימין וגם משמאל, ולכן ממשפט $P-F$ ההתפלגות של ההליכה המקרית על קודקודי הגרף שואפת להתפלגות:

$$\frac{1}{n}\overline{1} = \left(\frac{1}{n}, ..., \frac{1}{n}\right)$$

**דוגמא לגרף בו ההתכנסות לא תהיה מהירה:** מעגל. בגרף כזה דרושים לפחות $O\left(n^2\right)$ צעדים עד שנגיע להתפלגות אחידה.

איזה פונקציות מרחק "טבעי" לבחור בין וקטורי הסתברות? נטען כי הדבר ה"טבעי" ביותר הוא $l_1$. בהנתן $\pi_0$ ו-$\pi_1$ התפלגויות על $1, ..., n$, יהי $A \supset \{1, ..., n\}$ מאורע (מאורע הוא קבוצה חלקית של קודקודים במרחב ההסתברות הזה). אפשר לשאול מהו:

$$\max_A |\pi_0(A) - \pi_1(A)|$$

למעשה אנחנו מחפשים את הנקודה בה סכימה עד לנקודה הזו תוסיף לסכום ההפרשים, ומאותה נקודה כל תוספת רק תחסיר מסכום זה. אבל מניתוח גיאומטרי:

$$\max_A |\pi_0(A) - \pi_1(A)| = \frac{1}{2}|\pi_0 - \pi_1|$$

יתרה מזאת - הוכחנו את השיוויון בין שתי ההגדרות בתרגיל 9.

דוגמא נוספת לגרף - $\{0, 1, ..., p-1\}$, עם הצלעות:

$$x \to x \pm 1 \,(mod p)$$
$$x \leftrightarrow \frac{-1}{x} \,(mod p)$$

זהו גרף 3 רגולרי (כל עוד מרשים שלוש צלעות). זה מתכנס "נורא מהר" להתפלגות אחידה - בסדר של $O(\log p)$ צעדים[20]; לא נראה זאת, שכן ההוכחה דורשת מתמטיקה מאוד מאוד מתקדמת.

[20] חייבים מינימום של $\log p$ כדי ש"יהיה סיכוי" שיעברו על כל המצבים האפשריים.

### 2.5.2 גרפים מרחיבים

תחילה, סימונים:

- יהי $G=(V,E)$ גרף לא מכוון. אם $A,B\supseteq V$ נסמן:

$$e\left(A,B\right):=\#\left\{e=(v,w)\in E|\,v\in A,w\in B\right\},\ e\left(A,A\right):=e\left(A\right)$$

- אם $S\supseteq V$ נסמן ב־$\overline{S}$ את המשלים ב־$V$: $\overline{S}=V\backslash S$.

**הגדרה 2.89** יהי $\delta>0$. נאמר שהגרף $G$ הוא $\delta$־מרחיב (בצלעות) ־ $\delta-(edge)\ expander$ אם לכל קבוצת קודקודים $S\supset V$ כך ש־$|S|\geq\frac{|V|}{2}$ מתקיים:

$$e\left(S,\overline{S}\right)\geq\delta\left|S\right|$$

נסמן:

$$N\left(S\right):=\#\left\{v\in V|\,v\in\overline{S},\ \exists w\in S\ s.t.\ (w,v)\in E\right\}$$

(כלומר מספר הקודקודים ב־$\overline{S}$ להם קיימים שכנים ב־$S$).
מההגדרה, אם הגרף הוא $d$־רגולרי והוא גם $\delta$־מרחיב, אזי לכל קבוצה $S\supseteq V$ כך ש־$|S|\geq\frac{|V|}{2}$ , מתקיים $N\left(S\right)\geq\frac{\delta}{d}\left|S\right|$.
אם נמצאים בקבוצה בגודל $|S|$, אזי אם מוסיפים את השכנים עוברים לקבוצה בגודל $|S\cup N\left(S\right)|\geq|S|\left(1+\epsilon\right)$. אחרי $k$ פעמים הגודל הוא לפחות:

$$|S|\left(1+\epsilon\right)^{k}$$

ולכן אחרי $log_{\epsilon+1}n$ "רואים" כבר מחצית מהגרף.
השאלה היא מהי ה־$\delta$ הזו. קל לראות שכל גרף קשיר הוא $\frac{1}{|V|}$־מרחיב. גרף $d$־רגולרי מקרי הוא בהסתברות גבוהה מאוד הוא מרחיב. ניתן לדעת אם גרף הינו מרחיב לפי הערכים העצמיים שלו.

**משפט 2.90** יהי $G=(V,E)$ גרף לא מכוון $d$־רגולרי שאיננו דו צדדי[21], תהי $A$ מטריצת השכינויות של $G$, ויהיו $\lambda_1\geq|\lambda_2|\geq...\geq|\lambda_n|$ הע"ע של $A$.

**הערה 2.91** נשים לב כי $A$ איננה מטריצת הסתברות ־ היא תהיה כזו אם נחלקה ב־$d$; מטריצת המעבר של ההליכה המקרית על $G$ היא $P=\frac{1}{d}A$.

ידוע כי $\lambda_1=d$, וכן $|\lambda_i|<d$ עבור $i=2,...,n$ (ב־$P$ אנו יודעים כי הע"ע הגדול ביותר הוא 1, וכשמכפילים ב־$d$ מקבלים את ע"ע זה).
אזי, $G$ הוא $\delta$־מרחיב בצלעות עבור $\delta=\frac{d-|\lambda_2|}{2}$.

[21] ללא לולאות וצלעות כפולות כמו בדוגמא שראינו קודם.

ההוכחה של משפט זה היא בעזרת אלגברה לינארית מאוד פשוטה (נמצאת בסיכומים של שנה שעברה למתעניינים), ונראה אותה בשיעור הבא. הרעיון:
הוקטור המתאים לע"ע $d$ הוא $(1,...,1)$. בהנתן קבוצה $S$, נתאים את הוקטור $x = (x_1,...,x_n)$:

$$x_i = \begin{cases} |\overline{S}| & i \in S \\ -|S| & i \notin S \end{cases}$$

כיוון שהוא ניצב לוקטור $(1,...,1)$, אפשר לחשב את $x^T Ax$ בצורה פשוטה (כפי שהוא מוגדר) ובדרך נוספת - לפתח את $x$ לפי הע"ע. כאשר משווים את שני הביטויים המתקבלים משתי דרכי הפיתוח השונות מוכיחים את הנדרש.

**תוצאות ידועות** אנו יודעים כבר ממסקנה קודמת לאיזו הסתברות סטציונרית גרף $\delta$-מרחיב $d$-רגולרי שאיננו דו צדדי מתכנס. כאן עולה השאלה - כמה מהירה היא ההתכנסות הזו? ההתכנסות תהיה מהירה ככל ש-$\delta$ יהיה קטן יותר.
כמה אפשר לצפות ש-$\delta$ יהיה קטן? ככל ש-$|\lambda_2|$ קטן יותר (שכן $\lambda_1$ ידוע כי הוא תמיד $d$, אזי זהו הערך הגדול ביותר הבא בתור, והוא לא קבוע).
**ידוע**: עבור גרפים גדולים $2\sqrt{d-1} \leq |\lambda_2| \leq 2\sqrt{d-1}\,(1+o\,(1))$. עבור גרפים קטנים $|\lambda_2|$.
אם היינו מצליחים לקבל את הערך הזה, היינו מקבלים מרחיב מאוד גדול - אי אפשר לצפות לקבל משהו טוב מזה (דהיינו $\delta$ קטנה יותר), אבל האם אפשר לקבל ממש את הערך הזה? כן, ידועה בניה מפורשת עם:

$$|\lambda_2| = 2\sqrt{d+1}$$

כאשר $d$ הוא חזקה של ראשוני + 1 $\left(d = p^k + 1\right)$: גרפים אלו נקראים גרפי רמנוג'אן.
תוצאה נוספת - גרף $d$-רגולרי מקרי מקיים בהסתברות גבוהה:

$$2\sqrt{d-1}\,(1+o\,(1)) = |\lambda_2|$$

כלומר "גרף מקרי הוא טוב".
עם זאת, ידועות בניות מפורשות, וידועה לכל $d$ בניה מפורשת המקיימת:

$$|\lambda_2| = d^{\frac{3}{4}}$$

בגרפים כאלה הליכה מקרית מתכנסת מאוד מהר (אחרי $\log n$ צעדים).
אפשר לשאול את השאלה הבאה: ישנו אלגוריתם הסתברותי המטיל $n$ מטבעות, בהסתברות $\frac{2}{3}$ מקבלים את התשובה הנכונה. כיצד ניתן להוריד את הסתברות הטעות?
אפשר לחזור על הניסויים שוב ושוב (לפי צ'רנוף) ולקבל הסתברות יותר טובה, אבל אז הטלנו הרבה מהביטים המקריים לצורך הרצת האלגוריתם. איך ניתן לשפר את התהליך הזה?
בונים גרף מרחיב $d$ רגולרי, בוחרים שכן אחד מקרי, מבצעים הילוך מקרי על הגרף, ומשתמשים בביטים של כל שכן לצורך הרצת האלגוריתם (שכן אפשר לייצג כל קודקוד ע"י $m$ ביטים - פשוט ממספרים את $2^m$ הקודקודים בינארית). למעשה מכיוון וההתפלגות על המהלך מתכנסת כל כך מהר להתפלגות אוניפורמית, אפשר לקבל הרבה ביטים מקריים ממעט מאוד. סה"כ מספר הביטים בתהליך החדש הוא $n$ ביטים עבור בחירת הקודקוד

הראשון, ולאחר מכן לכל היותר $n$ צעדים. לכן כשעושים את החשבון הליכה באורך $n$ מקבלים הסתברות שגיאה שמתנהגת "מאוד טוב".

לכן גם לא רוצים לייצר גרף מקרי - רק לתאר גרף כזה יקח לנו הרבה מאוד ביטים. מסיבה זו יש צורך בבניה מפורשת של גרף מרחיב כנ"ל[22]. 31/12/2014

אם $G$ גרף $d$-רגולרי (כלומר כל הקודקודים מדרגה $d$) אזי $\delta$-מרחיב בצלעות $\Leftarrow$ $\frac{\delta}{d}$ מרחיב בקודקודים (לא נתנו הגדרה פורמלית אבל אפשר להבין מהי - על פי המרצה "זהו תרגיל טוב לכתוב").

בשבוע שעבר ניסחנו משפט אותו נרצה להוכיח:

**משפט 2.92** יהי $G=(V,E)$ גרף לא מכוון $d$-רגולרי שאיננו דו צדדי (וללא לולאות וצלעות מקבילות), תהי $A$ מטריצת השכינויות של $G$ ($A$ סימטרית עם איברים $0,1$ ו-$0$ על האלכסון), ויהיו $d=\lambda_1 \geq |\lambda_2| \geq ... \geq |\lambda_n|$ הע"ע של $A$.

אזי, $G$ הוא $\delta$-מרחיב בצלעות עבור $\delta = \frac{d-\lambda_2}{2}$.

**הערה 2.93** ראינו כי כיוון ו-$G$ רגולרי, הוקטור $\overline{1}=(1,...,1)$ הוא וקטור עצמי ימני ושמאלי של $A$ עם ע"ע $d$ (ממשפט $P-F$).

**הערה 2.94** $\lambda_2 = d \Leftrightarrow$ הגרף איננו קשיר, אחרת $d > |\lambda_2|$ אם הגרף איננו דו צדדי.

**הוכחה:** הוקטור העצמי המתאים ל-$\lambda_1$ הוא $\overline{1}=(1,...,)$. לכן:

$$\lambda_2 = \underset{x \perp \overline{1}}{max} \frac{x^T A x}{\|x\|^2}$$

תהי $V \supseteq S$ כך ש-$S \geq \frac{|V|}{2}$. נגדיר את הוקטור הבא:

$$x: \ x_i = \begin{cases} \left|\overline{S}\right| & i \in S \\ -|S| & i \notin S \end{cases}$$

נסמן $|V|=n$. אזי:

$$\sum_{i=1}^{n} x_i = \sum_{i \in S} \left|\overline{S}\right| - \sum_{i \notin S} |S| = |S| \cdot \left|\overline{S}\right| - \left|\overline{S}\right| \cdot |S| = 0$$

נחשב את $\frac{x^T A x}{\|x\|^2}$ בשני אופנים:

$$\|x\|^2 = |S| \cdot \left|\overline{S}\right|^2 + \left|\overline{S}\right| \cdot |S|^2 = |S| \cdot \left|\overline{S}\right| \left(\left|\overline{S}\right| + |S|\right) = |S| \cdot \left|\overline{S}\right| \cdot n$$
$$x^T A x = \sum_{i,j} x_i x_j A_{ij}$$

נחלק את הסכום הזה לשלוש קבוצות:

1. $(i,j) \in E$, $i,j \in S$: במקרה זה $x_i x_j = \left|\overline{S}\right|^2$, ולכן הסכום יהיה $2e(S) \cdot \left|\overline{S}\right|^2$.

[22] עוד על השימוש המעניין הזה, למשל, בנושאים מתקדמים בחישוביות. החומר הזה מופיע בצורה יפה בספר של אורורה וברק.

2. $(i,j) \in E$, $i,j \in \overline{S}$: במקרה זה $x_i x_j = |S|^2$, ולכן הסכום יהיה $2e\left(\overline{S}\right) \cdot |S|^2$.

3. $i,j \in E$, אחד מ־$i,j$ נמצא ב־$S$ והשני ב־$\overline{S}$: במקרה זה $x_i x_j = -|S|\left|\overline{S}\right|$, ולכן הסכום יהיה $-2e\left(S,\overline{S}\right) \cdot \left|\overline{S}\right| |S|$.

על כן בסה"כ:

$$x^T A x = 2\left(e\left(S\right) \cdot \left|\overline{S}\right|^2 + e\left(\overline{S}\right) \cdot |S|^2 - e\left(S,\overline{S}\right) \cdot |S| \left|\overline{S}\right|\right)$$

מצד שני, נתון כי הגרף $d$־רגולרי, לכן:

$$\begin{aligned} d\,|S| &= 2e\left(S\right) + e\left(S,\overline{S}\right) \\ d\left|\overline{S}\right| &= 2e\left(\overline{S}\right) + e\left(S,\overline{S}\right) \end{aligned}$$

נסמן $n_e = e\left(S,\overline{S}\right)$. נציב ונקבל:

$$\begin{aligned} x^T A x &= 2\left(\frac{1}{2}\left(d\,|S| - n_e\right)\left|\overline{S}\right|^2 + \frac{1}{2}\left(d\left(\overline{S}\right) - n_e\right)|S|^2 - n_e \cdot |S|\left|\overline{S}\right|\right) \\ &= d\,|S|\left|\overline{S}\right|\left(\left|\overline{S}\right| + |S|\right) - n_e\left(\left|\overline{S}\right|^2 + 2\,|S|\left|\overline{S}\right| + |S|^2\right) \\ &= d\,|S|\left|\overline{S}\right| \cdot n - n_e \cdot n^2 \\ \Rightarrow \lambda_2 \geq \frac{x^T A x}{\|x\|^2} &= \frac{d\,|S|\left|\overline{S}\right| \cdot n - n_e n^2}{|S| \cdot \left|\overline{S}\right| \cdot n} = d - n_e \cdot \frac{n}{|S| \cdot \left|\overline{S}\right|} \overset{|\overline{S}| \geq \frac{n}{2} \Rightarrow 2 \geq \frac{n}{|\overline{S}|}}{\geq} d - n_e \cdot \frac{2}{|S|} \end{aligned}$$

ומכאן ע"י העברת אגפים:

$$\frac{n_e}{|S|} = \frac{e\left(S,\overline{S}\right)}{|S|} \geq \frac{d - \lambda_2}{2}$$

■

תוצאה שניה שנרצה להוכיח, שגם היא נובעת מ"טריק אלגברי" כמו מעלה, היא העובדה כי מספר הצלעות בגרף מרחיב בין קבוצות לא קטנות מידי מתנהג כמו בגרף מקרי. ובאופן פורמלי:

### Expander Mixing Lemma

**משפט 2.95** יהי $G = (V,E)$ גרף $d$־רגולרי. אזי לכל שתי קבוצות $A, B \subseteq V$:

$$\left|\frac{|A \times B \cap E|}{2\,|S|} - \frac{|A|}{|V|} \cdot \frac{|B|}{|V|}\right| \leq \frac{\lambda_2\left(G\right) \cdot \sqrt{|A| \cdot |B|}}{d \cdot |V|} \leq \frac{\lambda_2\left(G\right)}{d}$$

**הערה 2.96** נשים לב כי הביטוי מצד שמאל הוא בעצם ההפרש ההסתברות לקבל את מספר הצלעות האמיתי לבין מספר הצלעות בגרף מקרי.

**סימון:** נסמן $\rho(A) = \frac{|A|}{|V|}$.

**מסקנה 2.97**

$$|A \times A \cap E| = (\rho(A) \cdot d \pm \lambda_2(G)) \cdot |A|$$

**הוכחה:** נסמן $|V| = n$, וכן $\lambda_2(G) = \lambda$, ידוע $\lambda_1 = d$ הערכים העצמיים השני והראשון של מטריצות השכינויות של $G$. צריך להוכיח:

$$\left| \frac{|A \times B \cap E|}{d \cdot n} - \rho(A) \cdot \rho(B) \right| \leq \frac{\lambda}{d} \cdot \sqrt{\rho(A) \cdot \rho(B)}$$

נבחר ווקטור:

$$\overline{a}: \ \overline{a}_i = \begin{cases} 1 & i \in A \\ 0 & otherwise \end{cases}$$

ובאופן דומה:

$$\overline{b} := \overline{b}_i = \begin{cases} 1 & i \in B \\ 0 & otherwise \end{cases}$$

נשים לב:

$$|A \times B \cap E| = \overline{a}^T A \overline{b} = \sum_{i,j} a_i b_j A_{ij}$$

נבחר בסיס אורתוגונלי של וקטורים עצמיים למטריצה $A$: $\overline{e}_1, ..., \overline{e}_n$, כאשר $\overline{e}_1 = (1, ...., 1)$ עם ע"ע $d$, $\overline{e}_i$ עם ע"ע $\lambda_i$, כאשר $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n$, ונבחר את $\overline{e}_i$ כך ש:

$$\|\overline{e}_i\|^2 = \overline{e}_i^T \overline{e}_i = n$$

נסמן ב־$a_i$ את המקדם של הוקטור $\overline{a}$ בבסיס $\{\overline{e}_i\}$. אזי:

$$a_i = \frac{\overline{a}^T \cdot \overline{e}_i}{n}, \ \overline{a} = \sum_{i=1}^{n} a_i \cdot \overline{e}_i \Rightarrow a_1 = \frac{\overline{a}^T \cdot \overline{e}_1}{n} = \rho(A)$$

$$\Rightarrow \sum_{i=1}^{n} a_i^2 = \frac{\overline{a}^T \cdot \overline{a}}{n} = \frac{|A|}{n} = \rho(A), \ \sum_{i=1}^{n} b_i^2 = \rho(B)$$

$$\Rightarrow |A \times B \cap E| = \overline{a}^T A b = \overline{a}^T A \cdot \sum_{i=1}^{n} b_i \overline{e}_i = \sum \lambda_i b_i \overline{a}^T \cdot \overline{e}_i = \sum_{i=1}^{n} \lambda_i b_i \cdot (a_i n)$$

$$\Rightarrow \frac{|A \times B \cap E|}{d \cdot n} = \sum_{i=1}^{n} \frac{\lambda_i b_i a_i}{d} = a_1 b_1 + \sum_{i=2}^{n} \frac{\lambda_i a_i b_i}{d}$$

$$(*) = \rho(A) \cdot \rho(B) \pm \frac{\lambda}{2} \sum_{i=2}^{n} a_i b_i$$

$$\sum_{i=1}^{n} |a_i| |b_i| \leq \left( \sum_{i=1}^{n} a_i^2 \cdot \sum_{i=1}^{n} b_i^2 \right)^{\frac{1}{2}} \leq \sqrt{\rho(A) \cdot \rho(B)} = \rho(A) \cdot \rho(B) \pm \frac{\lambda}{2} \sqrt{\rho(A) \cdot \rho(B)}$$

כנדרש.

**הערה 2.98** נשים לב כי $(*)$ למעשה אינו באמת שווה אלא הטענה כי הביטוי מוכל באינטרוול הזה (כתבנו פלוס מינוס הרי), אבל "אף אחד לא באמת משתמש בסימון הזה", ולכן נשאיר את הסימון המקובל, אם כי לא נכון באמת.

■

## 2.6 תרגולים

5.11.2013

### 2.6.1 שיטת החזקה לחישוב ע"ע - Power iteration

**שאלה:** בהנתן מטריצה $A$, איך ניתן למצוא את הע"ע שלה ואת הו"ע שלה?

**הערה 2.99**

1. אם אנחנו יודעים את הו"ע, קל למצוא את הע"ע.
2. אם אנחנו יודעים ש-$\lambda$ ע"ע של $A$, אפשר למצוא את הו"ע המתאים ע"י פתרון המערכת $Av = \lambda v$.

**רעיון 1**: בהנתן $A$, נחשב את $p(\lambda) = det(A - I\lambda)$, נמצא את שורשי $p$, ואלה הע"ע.
**בעיות**:

1. אין נוסחא סגורה למציאת שורשי פולינום. אפשר לפתור את בעיה זו עם אלגוריתמים נומריים למציאת שורשים.
2. אם משנים מקדם של פולינום במעט מאוד, זה יכול להזיז את השורשים בהרבה, ולכן השיטה לא יציבה נומרית.
   **דוגמא**: $x^{100}$ כל שורשיו אפס. אבל עקב חסם על דיוק המחשב למשל נקבל במקומו את הפולינום $x^{100} - \frac{1}{2^{100}}$, אשר שורשיו הם $\frac{1}{2}$·כל שורשי היחידה מסדר $100$.

היום נדבר על שיטה אחרת - שיטת החזקה!
נתחיל עם ניסוח למטריצות סימטריות, המשתמשת בתכונה הבאה:

**משפט 2.100** תהי $A$ מטריצה סימטרית $n \times n$ ממשית. אזי ל-$A$ יש בסיס אורתונורמלי $v_1, ..., v_n$ של ו"ע עם ע"ע ממשיים $\lambda_1, ..., \lambda_n$.

**הגדרה 2.101** וקטורים $v_1, ..., v_n$ הם אורתונורמליים אם:

1. $\|v_i\|_2 = 1$ לכל $i$.
2. לכל $i \neq j$, $\langle v_i, v_j \rangle = 0$ כאשר זוהי המכפלה הפנימית הסטנדרטית: $\sum_{k=1}^{n} v_i^k \cdot v_j^k$.

**השיטה** תהי $A$ מטריצה סימטרית, ונניח:

$$|\lambda_1| > |\lambda_2| > ... > |\lambda_n|$$

הם הע"ע של $A$, ונרצה למצוא את $\lambda_1, ..., \lambda_n$.
תחילה אנו מחפשים וקטור בכיוון של $v_1$, למרות שאנחנו לא יודעים מיהו. איך נמצא את הכיוון?
נגריל $v$ מתוך הקוביה ה־$n$ מימדית $[0,1]^n$.

**הערה 2.102** בהסתברות 1 יש ל־$v$ רכיב $0 \neq$ בכיוון $v_1$, כי וקטורים שאין להם את התכונה הזו הם תת־מרחב וקטורי ממימד $n-1$, ולכן לחיתוך שלו עם הקוביה הוא בעל מידה 0.

נתבונן בוקטור $v_k^* = \frac{A^k v}{\|A^k v\|_2}$.

**טענה 2.103** $v_k^* \to v_1$.

**הוכחה:** נרשום את $v$ כצ"ל של איברי הבסיס:

$$(a_i \neq 0)\, v = \sum_{i=1}^{n} a_i v_i$$

נתבונן ב־$A^k \cdot v$:

$$A^k v = \sum a_i A^k v_i = \sum a_i \lambda_i^k v_i = a_1 \lambda_1^k \left( v_1 + \sum_{i=2}^{n} \frac{a_i}{a_1} \left( \frac{\lambda_i}{\lambda_1} \right)^k v_i \right)$$

נשים לב:

$$\left\| A^k v \right\|_2 \geq \left| a_1 \lambda_1^k \right|$$

זה נובע מכך ש־$v_i$ אורתונורמליים ובפרט ניצבים, ו־$a_1 \lambda_1^k$ הוא הרכיב של $A^k v$ בכיוון $v_1$, ולכן הנ"ל מתקבל ממשפט פיתגורס המוכלל.
נסמן $\alpha_k = \frac{a_1 \lambda_1^k}{\|A^k v\|_2}$. אנו יודעים כי $|\alpha| \leq 1$.

$$v_k^* = \frac{A^k v}{\|A^k v\|_2} = \alpha v_1 + \sum_{i=2}^{n} \alpha_k \frac{a_i}{a_1} \left( \frac{\lambda_i}{\lambda_1} \right)^k v_i$$

הסכום שואף לאפס כי $|\lambda_1| >$ משאר הוקטורים, ולכן:

$$v_k^* \to \alpha v_1$$

$v_1, v_k^*$ הם וקטורי יחידה, ולכן $\alpha = \pm 1$, דהיינו:

$$v_k^* \to \pm v_1$$

■

איך נמצא את $v_2, v_3, ...$?

אם ל־$v$ לא היה רכיב בכיוון $v_1$, אותו תהליך היה נותן את $v_2$. לכן, נגריל את $v$ כמקודם, ונגדיר:

$$v' = v - \langle v, v_1 \rangle v_1$$

נעשה את התהליך על $v'$.

**הערה 2.104** אפילו אם יש רכיב קטן של $v_1$, כל התהליך יתפוצץ לנו (וזה יקרה שכן עוצרים לאחר מספר סופי של איטרציות). לכן, כשנעשה זאת בפועל, בכל שלב של הכפלה ב־$A$ נסלק את הרכיב בכיוון $v_1$ (ובאופן דומה עבור $v_3$ נסלק בכל שלב את הרכיבים בכיוונים $v_1$ ו־$v_2$, וכו').

האלגוריתם הזה מתקשר ל־Google pagerank:
נייצג את האינטרנט כגרף מכוון, כאשר הקודקודים הם האתרים, וקיימת צלע $(u, v)$ בגרף אם יש לינק מ־$u$ ל־$v$.
תהי $A$ מטריצת השכינויות של הגרף מנורמלת כך שסכום כל עמודה הוא 1. נסמן את $A$ מטריצה $n \times n$, כאשר $n$ מספר האתרים. תהי $v$ התפלגות על האתרים.
אזי $Av$ תיתן את ההתפלגות על האתרים אם מתחילים ועושים צעד אחד מקרי. מה שמעניין היא ההתפלגות הסטציונרית אליה מגיעים בגבול. מסתבר שההתפלגות הסטציונרית הזו היא הו"ע עם הע"ע המקסימלי של $A$.
איך מחשבים את זה? $A$ מטריצה גדולה, אולם היא דלילה, וכמו כן את גוגל לא מעניין הדירוג המדוייק, אלא קירוב. לכן הרצה של שיטת החזקה מספר פעמים תיתן קירוב "מספיק טוב" ל־$v_1$.

### 2.6.2 אי שיוויון קושי שוורץ

12.11.2013

**הגדרה 2.105** יהי $\mathbb{R}^n = V$. נורמה היא פונקציה $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}$ המקיימת:

1. חיוביות: $\|x\| \geq 0$, ושיוויון $\Leftrightarrow \overline{x} = \overline{0}$.
2. הומוגניות:

$$\forall \lambda \in \mathbb{R}, x \in \mathbb{R}^n \quad \|\lambda \cdot x\| = |\lambda| \cdot \|x\|$$

3. א"ש המשולש:

$$\forall x, y \in \mathbb{R}^n \quad \|x + y\| \leq \|x\| + \|y\|$$

**הגדרה 2.106** מרחב נורמי הוא זוג $(V, \|\cdot\|)$.

**הגדרה 2.107** יהי $V = \mathbb{R}^n$. פונקציה:

$$\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}$$

נקראת מ"פ אם היא מקיימת:

1. סימטריות:

$$\langle x, y\rangle = \langle y, x\rangle$$

2. לינאריות:

(א) חיבורית:

$$\langle x + y, z\rangle = \langle x, z\rangle + \langle y, z\rangle$$

(ב) כפלית:

$$\forall \lambda \in \mathbb{R} \ \ \langle \lambda x, y\rangle = \lambda \langle x, y\rangle$$

3. חיוביות: לכל $x \in \mathbb{R}^n$ $\langle x, x\rangle \geq 0$ ושיוויון$\Leftrightarrow x = 0$.

**הגדרה 2.108** באופן דומה, מרחב מכפלה פנימית הוא המרחב עם מ"פ.

התכונות של מ"פ מזכירות נורמה, ובאמת נורמה משרה מ"פ:

**טענה 2.109** מרחב מ"פ משרה נורמה על $\mathbb{R}^n$ ע"י:

$$\|x\| := \sqrt{\langle x, x\rangle}$$

**הערה 2.110** לא נוכיח הטענה הזו כאן, אלא נתייחס אליה כמובנת מאליו - מוכחת במספר קורסים בסיסיים במתמטיקה.

**מכפלה פנימית סטנדרטית:**

$$\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i$$

**הערה 2.111** הנורמה המושרה מהמ"פ הסטנדרטית היא:

$$\|x\| = \sqrt{\sum x_i^2}$$

נורמה זו נקראת נורמת $l_2$.

באופן כללי:

**הגדרה 2.112** נורמת $l_p$ של וקטור $x \in \mathbb{R}^n$ עבור $p \geq 1$ מוגדרת להיות:

$$\|x\|_{l_p} := \left(\sum |x_i|^p\right)^{\frac{1}{p}}$$

**דוגמאות:**

- $p = 1$:

$$\|x\|_1 = \sum |x_i|$$

פשוט סכום הקואורדינטות.

- $p = \infty$:

$$\|x\|_\infty = \lim_{p\to\infty} \|x\|_p = \max_i \{|x_i|\}$$

**תרגיל**: לכל $x \in \mathbb{R}^n$:

$$\|x\|_1 \geq \|x\|_2 \geq \|x\|_\infty$$

כאן עולה השערה - ככל שמעלים את ה־$p$ מקטינים את הנורמה. בעוד התרגיל מעלה פשוט, הוכחת ההשערה הזו קצת יותר מסובכת.

**הגדרה 2.113** יהי $(\mathbb{R}^n, \|\cdot\|)$ מרחב נורמי. נגדיר את הנורמה הדואלית ל־$\|\cdot\|$ באופן הבא:

$$\|x\|^* := \max_{v|\|v\|=1} \langle x, v\rangle$$

כאשר המ"פ היא המ"פ הסטנדרטית.

בשיעור נראה כמה תכונות לנורמה הדואלית, למשל, ב־$l_2$ הנורמה הדואלית היא אותה הנורמה.
עוד תכונה:

$$\|x\|_p^* = \|x\|_q$$

כאשר

$$\frac{1}{p} + \frac{1}{q} = 1$$

**אי שיוויון קושי שוורץ**

**משפט 2.114** יהיו $a, b \in \mathbb{R}^n$. אז:

$$\sum a_i b_i \leq \sqrt{\sum a_i^2} \cdot \sqrt{\sum b_i^2}$$

כלומר, במקרה של המ"פ הסטנדרטית:

$$\langle a, b\rangle \leq \langle a, a\rangle^{\frac{1}{2}} \langle b, b\rangle^{\frac{1}{2}}$$

**הערה 2.115** יש הרבה הכללות למשפט הזה, אבל "איכשהוא הגרסאות הכי פשוטות הן הכי שימושיות".

**הכללות**

1. לכל מ"פ מתקיים:

$$\langle a,b\rangle \leq \langle a,a\rangle^{\frac{1}{2}} \langle b,b\rangle^{\frac{1}{2}}$$

2. **אי שיוויון הולדר:**
יהיו $a,b \in \mathbb{R}^n$. אזי:

$$\sum_{i=1}^{n} a_i b_i \leq \|a\| \cdot \|b\|^*$$

לכל נורמה $\|\cdot\|$.

**שימושים בא"ש קושי שוורץ** נשתמש במקרה פרטי של א"ש זה:

**טענה 2.116** יהי $a \in \mathbb{R}^n$. אזי:

$$\sum_{i=1}^{n} |a_i| \leq \sqrt{n} \cdot \left(\sum a_i^2\right)^{\frac{1}{2}}$$

**הוכחה:**

$$\sum_{i=1}^{n} |a_i| = \sum 1 \cdot |a_i| = \left\langle \overrightarrow{1}, a \right\rangle \overset{C-S}{\leq} \left\| \overrightarrow{1} \right\|_2 \cdot \|a\|_2 = \sqrt{n} \cdot \|a\|_2$$

■

**מסקנה 2.117** אנחנו אמרנו:

$$\|x\|_2 \leq \|x\|_1$$

למעשה הראנו מעלה:

$$\|x\|_2 \leq \|x\|_1 \leq \sqrt{n} \cdot \|x\|_2$$

א"ש קושי שוורץ נוטה להופיע הרבה במתמטיקה, שכן הרבה פעמים אנחנו מגיעים לאיזה טור:

$$\left(\sum a_i\right)^2$$

ורוצים לחסום אותו, ואז פשוט מציבים בא"ש קושי שוורץ, ומקבלים:

$$\leq n \cdot \sum a_i^2$$

**שימוש ראשון לקושי שוורץ** תהי $P = \{p_1, ..., p_n\}$ קבוצה של $n$ נקודות שונות במישור, ותהי $L = \{l_1, ..., l_n\}$ קבוצה של $n$ ישרים שונים במישור.
נגדיר:

$$I = \{\, (p,l) | \, p \in P,\ l \in L,\ p\ is\ on\ l \}$$

שאלה: עד כמה גדול יכולה להיות הקבוצה $I$?
**הערה:** $|I| \leq n^2$ (ישירות מההגדרה).
משפט $Szemerdi - Trotter$, שהוא משפט הדוק, אומר:

**משפט 2.118** $|I| \leq n^{\frac{3}{4}}$.

אנחנו נראה:

**טענה 2.119** $|I| \leq \sqrt{2} n^{\frac{2}{3}}$.

**הוכחה:** לכל נקודה $p$ וישר $l$ נגדיר:

$$\delta_{p,l} = \begin{cases} 1 & p\ is\ on\ l \\ 0 & otherwise \end{cases}$$

נחשב:

$$|I| = \sum_p \sum_l \delta_{p,l}$$

נרצה להשתמש באי"ש קושי שוורץ, ועל כן נתבונן ב-$|I|^2$:

$$|I|^2 = \left( \sum_p \left( \sum_l \delta_{p,l} \right) \right)^2 \overset{C-S}{\leq} n \cdot \left( \sum_p \left( \sum_l \delta_{p,l} \right)^2 \right) = (*)$$

$$\left( \sum_l \delta_{p,l} \right)^2 = \left( \sum_l \delta_{p,l} \right) \cdot \left( \sum_l \delta_{p,l} \right) = \left( \sum_{l_2} \delta_{p,l} \right) \cdot \left( \sum_{l_1} \delta_{p,l} \right) = \sum_{l_1, l_2 \in L} \delta_{p,l_1} \cdot \delta_{p,l_2}$$

$$\Rightarrow (*) = n \cdot \left( \sum_p \sum_{l_1, l_2 \in L} \delta_{p,l_1} \cdot \delta_{p,l_2} \right) = n \cdot \sum_{l_1, l_2 \in L} \left( \sum_p \delta_{p,l_1} \cdot \delta_{p,l_2} \right)$$

$$= n \cdot \left( \sum_{l \in L} \left( \sum_p \delta_{p,l}^2 \right) + \sum_{l_1 \neq l_2 \in L} \overbrace{\sum_p \delta_{p,l_1} \cdot \delta_{p,l_2}}^{\leq 1} \right)$$

$$\leq n \cdot |I| + n \cdot n^2 \leq 2n^3$$

$$\Rightarrow |I|^2 \leq 2n^3$$

■

### 2.6.3 גיאומטריה

**הגדרה 2.120** קוביית יחידה מוגדרת באופן הבא:

$$C := \{ x \in \mathbb{R}^n | \, 0 \leq x_i \leq 1 \}$$

**הגדרה 2.121** כדור יחידה מוגדר באופן הבא:

$$B := \{ x \in \mathbb{R}^n | \, \|x\|_2 \leq 1 \}$$

נרצה לדבר על הנפח של הדברים האלה - הנפח של קוביית היחידה הוא איכשהוא תמיד $1$, גם במימדים גבוהים: נפח של תיבה הוא מכפלה של אורכי הצלעות.

בשני מימדים קל לראות שהכדור יותר גדול מהקוביה - הנפח של הכדור הוא $\pi$ ושל הקוביה - $1$. ב-$\mathbb{R}^3$ ניתן להוכיח שנפח הכדור הוא $\frac{4}{3}\pi$: כלומר הנפח של הקוביה היא קבועה, והנפח של הכדור הולך וגדל. איך מחשבים את זה? מחשבים אינטגרל בקואורדינטות פולאריות, ואפילו אז זה לא כל כך פשוט. מקבלים:

$$V_n \sim \left( \frac{2\pi e}{n} \right)^{\frac{n}{3}}$$

ב-$n = 5$ הנפח של הכדור הוא הגדול ביותר, והחל מ-$n = 13$ הנפח של הכדור שואף לאפס מאוד מהר.

### 2.6.4 טרנספורם פוריה

19.11.2013

היום נדבר על אפליקציה של מרחבים נורמיים וכו' - טרנספורם פורייה, ועל הקוביה הדיסקרטית.

**הגדרה 2.122** פונקציה בוליאנית $f$ היא פונקציה:

$$f : \{0,1\}^n \to \{0,1\}$$

רואים אותן בכל מקום: למשל אם רוצים לדעת אם גרף בעל $n$ קודקודים הוא 2-צביע, מסתכלים על:

$$f : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$$

כי כל $x \in \{0,1\}^{\binom{n}{2}}$ מקודד גרף על $n$ קודקודים. נקבל כי:

$$f(x) = \begin{cases} 1 & G \text{ is connexted} \\ 0 & otherwise \end{cases}$$

היום נתבונן בפונקציות:

$$f : \{-1,1\}^n \to \{-1,1\}$$

ונחשוב על $-1,1$ כעל מספרים ממשיים ב־$\mathbb{R}$ (בניגוד למה שאנחנו בדר"כ עושים עם פונקציות בוליאניות - אינדיקציה ל־$true$ או $false$)/

**הגדרה 2.123** טרנספורם פורייה של:

$$f : \{-1,1\}^n \to \mathbb{R}$$

הוא הצגה של $f$ כפולינום מולטי־לינארי.

מה פולינום מולטי־לינארי? למשל:

$$x_1 x_5 x_{17}$$

הוא פולינום מולטי לינארי, כלומר צירוף של מונומים של הרבה משתנים, כאשר אין לאף משתנה חזקה גדולה מ־1.

**דוגמא לטרנספורם פורייה:**

$$max_2 : \{-1,1\}^2 \to \{-1,1\}\,,\ max_2(x_1,x_2) = max(x_1,x_2)\,,\ x_1,x_2 \in \{-1,1\}$$

נשים לב כי כאן מתקיים:

$$(1,1) \to 1,\ (-1,1) \to 1,\ (1,-1) \to 1,\ (-1,-1) \to -1$$

**טענה 2.124**

$$max_2(x_1,x_2) = \frac{1}{2} + \frac{1}{2}x_1 + \frac{1}{2}x_2 - \frac{1}{2}x_1x_2$$

**הוכחה:** ע"י הצבה. נראה הצבה אחת:

$$(1,-1) \Rightarrow \frac{1}{2} + \frac{1}{2}\cdot(1) + \frac{1}{2}\cdot(-1) - \frac{1}{2} = 1$$

■

זה נראה קצת כמו נס - מאיפה זה הגיע? נטען כי תמיד (בתנאים מסויימים) קיימת הצגה כזו. איך אפשר למצוא הצגה כזו? בעזרת אינטרפולציה:

נפעל על הדוגמא שלנו - נגדיר $4$ פולינומים, אחד לכל נקודה אפשרית בדוגמא שלנו - כאשר כל פולינום שכזה יתן $1$ עבור הנקודה אליה הוא מתייחס, ו־$0$ לכל שאר הנקודות:

$$P_{1,1} = \left(\frac{1+x_1}{2}\right)\left(\frac{1+x_2}{2}\right)$$
$$P_{1,-1} = \left(\frac{1+x_1}{2}\right)\left(\frac{1-x_2}{2}\right)$$
$$P_{-1,-1} = \left(\frac{1-x_1}{2}\right)\left(\frac{1-x_2}{2}\right)$$

אז:

$$max_2 = 1 \cdot P_{1,1} + 1 \cdot P_{1,-1} + 1 \cdot P_{-1,1} + (-1) \cdot P_{-1,-1}$$

וזה נכון, כי כפלנו את הערך של $max_2$ בכל נקודה, בפולינום המתאים לה.

**הערה 2.125** הבניה הזו תעבוד לכל פונקציה:

$$f : \{-1,1\}^n \to \mathbb{R}$$

נוכיח בהמשך שיש לכל פונקציה כזאת יצוג יחיד כפולינום מולטי־לינארי.
כמה מונומים אפשריים ישׁ? $2^n$, כי יש התאמה בין $S \subseteq \{1,...,n\}$ לבין מונומים ע"י:

$$\prod_{i \in S} x_i$$

אז לכל פונקציה כזו יש ייצוג באופן הבא:

$$f(x) = \sum_{S \subseteq \{1,...,n\}} \overbrace{c_S}^{\in \mathbb{R}} \prod_{i \in S} x_i$$

נסמן:

1. $\{1,...,n\} = [n]$
2. $x^S = \prod_{i \in S} x_i$.
3. $\hat{f}(S) = c_S$.

כלומר, בסימונים הללו אפשר לרשום:

$$f(x) = \sum_{S \subseteq [n]} \hat{f}(S)\, x^S$$

נוכיח בהמשך כי $\hat{f}(S)$ הם יחידים, ולכן $f$ בהצגה הנ"ל מוגדרת היטב.

**הערה 2.126** כל מונום $x^S$ הוא פונקציה בוליאנית:

$$S \subseteq [n]\,,\ x^S : \{-1,1\}^n \to \{-1,1\}$$

למשל: $S = \{1,3\}$, אזי $x^S = x_1 \cdot x_3$.
נוסיף סימון נוסף:

$$\chi_S(x) := x^S$$

למשל:

$$n = 3,\ \chi_{\{1,2\}}(-1,1,-1) = x_1 \cdot x_2 = -1$$

ועכשיו - נקשר את מה שעשינו לאלגברה לינארית:

**הערה 2.127** מרחב הפונקציות:

$$\{f : \{-1,1\}^n \to \mathbb{R}\}$$

הוא מרחב וקטורי ממשי במימד $2^n$, כי אפשר לזהות כל אחת לפי טבלת האמת שלה ולהפך, דהיינו $\mathbb{R}^{2^n} \simeq$.

ראינו: לכל פונקציה $f : \{-1,1\}^n \to \mathbb{R}$ יש ייצוג:

$$f(x) = \sum_{S \subseteq [n]} \hat{f}(S)\, \chi_S(x)$$

כלומר לכל פונקציה יש ייצוג כצ"ל של הפונקציות $\{\chi_S\}_{S\subseteq[n]}$, כלומר $\{\chi_S\}$ היא קבוצה פורשת בגודל $2^n$, ולכן זה בסיס, וזה מוכיח את היחידות - כי לכל וקטור יש יצוג לינארי יחיד באיברי הבסיס.
נגדיר מכפלה פנימית על המרחב הוקטורי שלנו $V = \{f : \{-1,1\}^n \to \mathbb{R}\}$, כך שתהיה כמו הסטנדרטית עם נרמול:

$$\langle f, g \rangle = \frac{1}{2^n} \sum_{x \in \{-1,1\}^{2^n}} f(x)\, g(x)$$

למכפלה הפנימית הזו יש פרשנות הסתברותית שהיא גם חשובה:

$$\langle f, g \rangle = \mathbb{E}_{x \sim U\{-1,1\}^n} [f(x) \cdot g(x)]$$

"תדגום נקודה מהקוביה הדיסקרטית באופן אקראי, ואז תיקח את התוחלת של התהליך הזה".

**משפט 2.128** $\{\chi_S\}_S$ הוא בסיס אורתונורמלי, כאשר הנורמה היא הנורמה המושרה:

$$\|f\| = \sqrt{\langle f, f \rangle}$$

**הוכחה:**

$$\langle \chi_S, \chi_T \rangle = \mathbb{E}_{x\sim U\{-1,1\}^n} [\chi_S \cdot \chi_T] = \mathbb{E}_{x\sim U\{-1,1\}^n} \left[ \prod_{i\in S} x_i \cdot \prod_{i\in T} x_i \right]$$

$$\mathbb{E}_{x\sim U\{-1,1\}^n} \left[ \prod_{S\cap T} \overbrace{x_i^2}^{=1} \cdot \prod_{S\triangle T} x_i \right] (*)$$

הערה: אם $x \in \{-1,1\}^n$, אז:

$$x_i = \begin{cases} 1 & w.\ prob.\ \frac{1}{2} \\ -1 & -"- \end{cases}$$

באופן בלתי תלוי. על כן נקבל:

$$(*) = \prod_{S\triangle T} \mathbb{E}[x_i] = \begin{cases} 1 & S = T \\ 0 & S \neq T \end{cases}$$

■

**תכונות:**

1. משפט פלנצ'רל:

$$\langle f, g \rangle = \sum_{S\subseteq[n]} \hat{f}(S) \cdot \hat{g}(S)$$

**הוכחה:**

$$\langle f, g \rangle = \left\langle \sum_{S\subseteq[n]} \hat{f}(S) \cdot \chi_S, \sum_{T\subseteq[n]} \hat{g}(T) \chi_T \right\rangle$$
$$= \sum_{S\subseteq[n]} \sum_{T\subseteq[n]} \hat{f}(S) \cdot \hat{g}(T) \langle \chi_S, \chi_T \rangle = \sum_{S\subseteq[n]} \hat{f}(S) \cdot \hat{g}(S)$$

■

מסקנה נחמדה: עבור פונקציה בוליאנית $f : \{-1,1\}^n \to \{-1,1\}$:

$$\overbrace{\langle f, f \rangle}^{\mathbb{E}[f^2(x)]=1} = \sum_{S\subseteq[n]} \hat{f}(S)^2$$

"בשביל מה כל זה טוב?" - לא נראה שימוש לזה, אז זה קצת מתמיה. כשעושים את הדבר הזה, אפשר להסיק אינפורמציה על הפונקציה ממקדמי פוריה האלה. דוגמא אחת ממש טריוויאלית לכך:

נסתכל על מקדם הפוריה של הקבוצה הריקה:

$$\hat{f}(\phi) = \left\langle f, \overbrace{\chi_\phi}^{=1} \right\rangle = \mathbb{E}[f]$$

אז אם יודעים את מקדם הפוריה של הקבוצה הריקה, יודעים את התוחלת של הפונקציה. הדברים האלה היו שימושיים בעבר, אבל אין לנו זמן להראות שימוש שירגש אותנו.

### 2.6.5 משפט ה־$SVD$

3.12.2013

הבוחן בשבוע הבא - כמו הפעם הקודמת. כמו כן, המקום של שעת הקבלה השתנה - כעת בבניין החדש בחדר $422A$.

#### משפט ה־$SVD$

**משפט 2.129** כל מטריצה ממשית $A$ מסדר $m \times n$ ניתנת לפירוק:

$$A = UDV^T$$

כאשר $U$ מסדר $m \times m$ אורתוגונלית, $V$ מסדר $n \times n$ אורתוגונלית, ו־$D$ מסדר $m \times n$ אלכסונית, כלומר $d_{i,j} = 0$, אם $i \neq j$.

**הגדרה 2.130** מטריצה $U$ נקראת אורתוגונלית אם:

1. העמודות של $U$ הן בסיס אורתונורמלי.
2. השורות של $U$ הן בסיס אורתונורמלי.
3. $U^TU = UU^T = I$.

נשים לב כי התנאים מעלה שקולים (לכן מספיק ידיעה שאחד מתקיים).

**הערה 2.131**

1. איברי האלכסון של $D$ הם השורשים של הע"ע של $AA^T$ ושל $A^TA$ (אפשר למצוא $D$ שכזו כך שהערכים אכן חיוביים, ולא השליליים).

$$A^TA = \left(UDV^T\right)^T \left(UDV^T\right) = VD^TU^TUDV^T = VD^TDV^T$$

   אם $m \geq n$, אזי $D^TD$ היא מטריצה ריבועית "קטנה" מסדר $n \times n$, נסמנה ב־$W$, כאשר איבריה על האלכסון הם $d_i^2$ (והשאר אפסים).

2. זה מניב אלגוריתם (לא הכי יעיל) לחישוב ה־$SVD$: מלכסנים את $A^TA$ ואת $AA^T$ ומוצאים את הע"ע שלהם. המטריצה המלכסנת תהיה זו עם הע"ע, ולכן בפרט אפשר למצוא את $W$, ממנה את $D$, וכן מצאנו את $V$.

3. המטריצה $B$ מדרגה $k \geq$ שנותנת מינימום ל־$\|A - B\|_{F:2\to 2}$ היא אותה מטריצה מהלכסון!

4. הייצוג הוא בזבזני: $D$ היא כמעט בכל מקום אפסים, לכן גם ב־$m-n$ $U$ העמודות האחרונות יכולות להיות אפס, כי הן לא ישפיעו על התוצאה, על כן אפשר עבור $U$ לשמור רק את $n$ העמודות הראשונות ואת $n$ השורות הראשונות של $D$; ליצוג הזה קוראים לפעמים "ייצוג מצומצם".

5. אם $A$ מטריצה ריבועית סימטרית, אז ל־$A$ יש בסיס א"ת של ו"ע, אז הלכסון של $A$ הוא גם ה־$SVD$ שלה: $A=UDU^T$.

**שימוש ראשון: פסאודו הופכי** נניח ש־$Ax=b$ היא מערכת של שיוויונות, $A$ מסדר $n\times n$ הפיכה.

אנחנו יודעים לפתור מערכת כזאת. נניח שאנחנו מחפשים את הפתרון עבור $x$. הפתרון נתון ע"י:

$$x=A^{-1}b$$

**הערה 2.132** אם אנחנו יודעים את ה־$SVD$ של $A$, קל מאוד למצוא את ההופכי שלה (נשים לב שהמטריצה ההופכית של $D$ היא האלכסונית כך שאיברי האלכסון שלה הם $\frac{1}{d_{ii}}$):

$$A=UDV^T \Rightarrow A^{-1}=\left(UDV^T\right)^{-1}=VD^{-1}U^T$$

נניח שרוצים פתרון מקורב ל־$Ax=b$, כאשר ל־$A$ יש יותר שורות מעמודות. זה מצב קצת משונה, כי יש יותר שורות מעמודות, ולכן לא יהיה פתרון למערכת המשוואות. עם זאת, מסתבר שבעיה זו מופיעה הרבה בתחומים מדעיים: למשל אם יש ניסוי שהניב תוצאות שונות $(y_1,...,y_n)$ לנקודות מדגם $(x_1,...,x_n)$ שאנו יודעים שצריכות לתת קו ישר בגרף, אבל עקב בעיות שונות, כגון כיול המכשירים וכו', התוצאה עצמה אינה נותנת ישר, יש צורך למצוא את הקירוב הכי טוב לישר הזה: $ax+b$.

דהיינו, אנחנו רוצים למזער את $\|Ax-b\|_2^2$. מסתבר שה־$x$ שממזער הוא:

$$x=A^+b$$

כאשר $A^+$ נקרא הפסאודו־הופכי של $A$, כאשר מתקיים:

$$A^+=VD^{"-1"}U^T$$

**שימוש שני: כיווץ תמונות** נביט במטריצה $Im$ המכילה את ערכי האפור של הפיקסלים בתמונה כלשהיא, ואנו רוצים לכווץ אותה.כיצד נעשה זאת?

$$Im=UDV^T$$

כאשר $Im$ היא מסדר $m\times n$, ונניח $m\geq n$. ה־$SVD$ רק מגדיל לנו את המקום שהתמונה תופסת, כי קיבלנו $m^2+m\cdot n+n^2$.

אבל, למעשה לא צריך להחזיק את כל $D$, אלא רק את האלכסון, כלומר נחזיק $m^2+n+n^2$.

אבל כפי שציינו, זה ייצוג בזבזני, ומספיק להחזיק רק את $n$ העמודות הראשונות של $U$, דהיינו דורש מקום של $m \cdot n + n + n^2$.

לא חסכנו עדיין. גם ב־$V$ אפשר להעיף שורות: כל שורה אחרי השורה ב־$k$, כאשר $k$ נבחר לפי הטעות שאנחנו מוכנים לסבול. לכן אפשר לחתוך גם את שתי המטריצות האחרות ־ $U$ תהיה $m$ שורות ו־$k$ עמודות, ו־$D$ תהיה מגודל $k \times k$, וצריך לשמו רק את $k$ האיברים על האלכסון. לכן בסה"כ מתקבל גודל של: $m \cdot k + k + n \cdot k$.

עוד על כך בסיכום באתר הקורס עם דוגמאות.

### 2.6.6 הילוכים מקריים ושרשראות מרקוב

10.12.2013

הראיון על תרגילי 8־4.

**הגדרה 2.133** תהליך מקרי (random process) הוא שרשרת של משתנים מקריים:

$$X_1, X_2, ....$$

**הגדרה 2.134** שרשרת מרקוב היא תהליך מקרי כך ש:

$$Pr\left(X_n = x \,|X_{n-1} = x_{n-1}, ..., X_1 = x_1\right) = Pr\left(X_n = x \,|X_{n-1} = x_{n-1}\right)$$

ותכונה זו נקראת תכונת המרקוביות.

מה המשמעות של התכונה? לא מעניין אותנו מה קרה במהלכים הקודמים, ע"מ לדעת מה ההסתברות בצעד ה־$n$־י מספיק לנו לדעת מה קורה בצעד שקדם לו. נשים לב כי אין זה אומר בהכרח שהמ"מ בת"ל.

**דוגמאות**

1. הילוך מקרי על $\mathbb{Z}^2$: מתחילים מראשית הצירים:

$$X_1 = (0, 0)$$

ומשם הולכים באופן מקרי על השריג, כאשר $X_n$ הוא המיקום בצעד ה־$n$־אי.

2. Self avoiding random walk: גם על $\mathbb{Z}^2$, בכל צעד בוחרים כיוון מקרי מבין הכיוונים המותרים, כאשר כיוון הוא מותר אם לא היינו בנקודה אליו הכיוון מוביל. משתמשים במודל זה למידול של תהליכים של חלבונים. זהו הילוך מקרי אך הוא אינו מרקובי, שכן הכיוונים המותרים תלויים בכל המצבים בהם היינו בהם קודם לכן.

**הגדרה 2.135** שרשרת מרקוב היא סופית אם $X_i \in \Omega$ כאשר $\Omega$ סופית.

**הגדרה 2.136** שרשרת מרקוב היא הומוגנית ביחס לזמן, אם:

$$Pr\left(X_{n+1} = y \,|X_n = x\right) = Pr\left(X_2 = y \,|X_1 = x\right)$$

**הגדרה 2.137** במקרה מעלה, להסתברות:

$$Pr\left(X_2 = y \,|X_1 = x\right)$$

קוראים הסתברות מעבר $p\left(x,y\right)$, ול־$\Omega$ קוראים מרחב המצבים.

**הגדרה 2.138** מטריצת המעבר $P$ היא מטריצה מסדר $|\Omega| \times |\Omega|$ המוגדרת באופן הבא:

$$P := \left(p\left(x,y\right)\right)$$

**הערה 2.139** נוח לייצג שרשרת מרקוב כזאת ע"י גרף מכוון המוגדר באופן הבא: $V = \Omega$, ו־$(x,y) \in E$ אם $p\left(x,y\right) > 0$, וכן $p\left(x,y\right)$ הן משקלות על הצלעות.

**דוגמא - צפרדע באגם** לצפרדע יש שני עלים מהם הוא יכול לקפוץ - בהסתברות מסויימת הוא נשאר, בהסתברות אחרת הוא עובר לעלה האחר. *איור*. מטריצת המעבר המתאימה היא:

$$P = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix}$$

**תכונות מטריצת המעבר:**

1. סכום כל שורה ב־$P$ $= 1$.
2. תהי $\mu$ התפלגות על $\Omega$. אזי: $(\mu P)$ היא ההתפלגות על $\Omega$ שמתקבלת אם דוגמים מצב ב־$\Omega$ ע"פ $\mu$, ועושים צעד אחד (ממנו) לפי הסתברויות המעבר.

למה?

$$\left(\mu P\right)_y = \sum_{x \in \Omega} \mu_x p\left(x,y\right)$$

נסמן $X_1 \sim \mu,\ X_2 \sim \mu P$, אזי $X_n \sim \mu P^{n-1}$.
תחת תנאים די נרחבים, $X_n$ מתכנס להתכנסות גבולית. זה לא כל כך מפתיע, שכן ראינו את שיטת החזקה בה התכנסנו לערך הגבוה ביותר של המטריצה. כאן המצב דומה.

**הגדרה 2.140** התפלגות סטציונרית היא התפלגות $\pi$ על $\Omega$ כך ש־$\pi P = \pi$.

**דוגמא - שוב הצפרדע באגם** נרצה למצוא התפלגות סטציונרית $\pi = (x,y)$ כלומר:

$$(x,y) \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix} = (x,y)$$

לא נוכיח זאת, אבל ל־$P$ ו"ע עם ע"ע 1. נפתור את מערכת המשוואות הלינאריות שקיבלנו:

$$\begin{cases} \frac{1}{2}x + \frac{1}{3}y &= x \\ \frac{1}{2}x + \frac{2}{3}y &= y \end{cases} \Rightarrow \begin{cases} -3x + 2y &= 0 \\ 3x - 2y &= 0 \end{cases} \Rightarrow x = 2, y = 3$$
$$\Rightarrow \pi = \left(\frac{2}{5}, \frac{3}{5}\right)$$

נטען כי אם נתחיל במקום מסויים, לאחר זמן כלשהו תחת תנאים מסויימים ההתפלגות תשאף להתפלגות הסטציונארית. מתי זה לא קורה?

- המצבים הם גרף לא קשיר ־ במקרה זה אין אפילו יחידות למצב סטציונארי.
- יודעים בוודאות איפה נמצאים בכל זמן.

ואלו שני המקרים היחידים בהם זה לא קורה. על מנת לפרמל זאת, נצטרך הגדרות נוספות:

**הגדרה 2.141** תהיינה $\mu_1, \mu_2$ התפלגויות על $\Omega$. אזי המרחק על ההתפלגויות הללו מוגדר להיות:

$$d_{TV}(\mu_1, \mu_2) := \frac{1}{2} \sum_{x \in \Omega} |\mu_1(x) - \mu_2(x)|$$

מטריקה זו ידועה בשם Total Variation Distance.

למרחק זה יש כמה הגדרות שקולות, שאולי נראה בתרגיל. כאשר נדבר על התכנסות של התפלגות נדבר במונח הזה.

**הגדרה 2.142** שרשרת מרקוב נקראת אי פריקה אם הגרף המכוון המתאר אותה קשיר חזק (כלומר אפשר להגיע מכל מצב לכל מצב אחר).

הגדרה זו מתאימה לתכונה הראשונה שתיארנו ־ הגרף המכוון המתאר את השרשרת מאוד מאוד קשיר.

**הגדרה 2.143** שרשרת מרקוב נקראת א־פריודית אם לכל $i \in \Omega$:

$$1 = gcd\left(n \,|Pr\left(X_n = i \,|X_0 = i\right) > 0\right)$$

הגדרה זו מתאימה לתכונה השניה שתיארנו ־ אם ה־ $gcd = 1$, אזי אין מחזוריות, שכן ה־$n$־אים אינם כפילויות אחד של השני, ועל כן אנחנו יכולים לדעת תמיד היכן אנחנו בדיוק (אם היו מחזורים, יכולנו לדעת איפה אנחנו במחזור, אבל לא את מספר המחזור).

**משפט 2.144** :

1. לכל שרשרת מרקוב סופית והומוגנית יש התפלגות סטציונרית $\pi$.
2. אם בנוסף השרשרת אי פריקה, אז $\pi$ יחיד.

3. אם בנוסף השרשרת א־פריודית, אז:

$$d_{TV} = \left(\mu P^t, \pi\right) \overset{t\to\infty}{\longrightarrow} 0$$

לכל התפלגות $\mu$.

24/12/2013

יהי $\Omega$ מרחב המצבים (אנחנו נדבר רק על מרחב סופי), $P$ מטריצת מעבר כך ש־$P_{ij}$ היא ההסתברות לעבור מ־$i$ ל־$j$. אזי $P$ היא מטריצה סטוכסטית.

**הגדרה 2.145** מטריצה סטוכסטית מטריצה ריבועית אשר כל איבריה הם אי שליליים, וסכום כל שורה בה הוא 1.

ראינו בפעם הקודמת הסתברות סטציונרית:

$$\pi P = \pi$$

.

וכן ראינו משפט התכנסות: אם הילוך מקרי הוא קשיר ולא מעגלי\דו"צ, הוא מתכנס להסתברות סטציונרית.

מה זה אומר מתכנס? בהתייחס למרחק שהגדרנו:

$$d_{TV}\left(\mu_1, \mu_2\right) = \frac{1}{2}\sum_{x\in\Omega}\left|\mu_1\left(x\right) - \mu_2\left(x\right)\right|$$

אנו יודעים כי יש התכנסות, אבל, אולי נרצה ללכת מספר צעדים מסויים שלא יספיק להגיע להתכנסות - נרצה לדעת במקרה זה לאן נגיע. לצורך כך נשתמש במרחק שהגדרנו מעלה להגדרה נוספת:

$$d\left(t\right) := \max_{\mu}\left(d_{TV}\left(\mu P^t, \pi\right)\right)$$

בהנתן שבאמת אנחנו יודעים שההילוך קשיר ולא מעגלי\דו"צ, ועל כן אנו יודעים כי קיימת $\pi$ שכזו. נסמן:

$$t_{mix}\left(\varepsilon\right) = \min_{t}\left\{t \middle| \, d\left(t\right) \leq \varepsilon\right\}$$

תכונה של זמן ערבוב שלא נוכיח:

$$t_{mix}\left(\frac{1}{2^n}\right) \leq n \cdot t_{mix}\left(\frac{1}{4}\right)$$

**הגדרה 2.146** זמן ערבוב הינו:

$$t_{mix} := t_{mix}\left(\frac{1}{4}\right)$$

### 2.6.7 דגימה של זיווג מושלם

יהי $G$ גרף דו צדדי עם $n$ קודקודים בכל צד. נסמן: $G = (V_1 \cup V_2, E)$. נרצה לדגום זיווג מושלם של $G$ באופן אוניפורמי.

**למה הבעיה הזו קשה, ולמה היא מעניינת (אולי)?** מספר זיווגים מושלמים יכול להיות גם $n!$. אפשר לקוות שהמספר הוא קטן יותר, אבל זה בדר"כ לא קורה - למשל בגרף $4$-רגולרי יש $2^{\frac{n}{2}}$ רכיבי קשירות, וזהו מצב מאוד טיפוסי: מספר רכיבי הקשירות הוא בדר"כ בסדר גודל של $\left(\frac{d}{e}\right)^n$ עבור $d$ גדול, ולכן מספר אקספוננציאלי של זיווגים.
למה הבעיה קשה?

1. $|\Omega|$ גדול.
2. חישוב $|\Omega|$ זה קשה - למעשה היא $\#P$-שלמה.

**הגדרה 2.147** $\#P$ - לספור פתרונות חוקיים לבעיה ב-$NP$.

למה הבעיה מעניינת?

1. אפשר להשתמש בדגימה כדי לבנות אלגוריתם קירוב לבעיית הספירה (כמה זיווגים מושלמים יש) - $FPRAS$ (סכימת קירוב - כלומר בהנתן $\varepsilon$, האלגוריתם יעבוד בקירוב של $\varepsilon + ...$).
2. בהנתן $A_{n\times n}$:

$$det\left(A\right) = \sum_{\sigma \in S_n} sg\left(\sigma\right) \cdot \prod a_i \sigma_i, \;\; Per\left(A\right) = "X"$$

אפשר להתאים את ה-$FPRAS$ מ-$1$ גם ל-$Per\left(A\right)$ של $A$ אי שלילית.

**הקשר בין זיווגים מושלמים לפרמננטה** מספר הזיווגים המושלמים שווה לפרמננטה של "מטריצת השכינויות" כפי שהגדרנו בשיעור (עוד באיור - אמור להיות בסיכום באתר).

**הרעיון:** נבנה הילוך מקרי על המרחב של הזיווגים המושלמים, והמחשב יהיה בתפקיד "ההולך השיכור" $\setminus$ המקרי - לא יחזיק את כל הזיווגים, אלא את הזיווג שהוא כרגע נמצא בו, ויגריל את הזיווג אליו הוא הולך. כלומר, להגדיר הילוך מקרי על קבוצת הז"מ של $G$ = $\Omega$, והמחשב הוא ההולך המקרי.

צריך למצוא הילוך מקרי:

1. קשיר.
2. יש אלגוריתם יעיל להגריל שכן מקרי בגרף של ההילוך.

זו לא בעיה כל כך קלה. למעשה, לא הצליחו לפתור אותה.
**נסיון ראשון**: בכל צעד, בחר שתי צלעות בזיווג באופן מקרי (בצורה אחידה). בהסתברות חצי השאר במקום, בהסתברות חצי אם אפשר לעשות החלפה (כלומר להחליף שני קודקודים בין הצלעות, והצלעות החדשות קיימות בגרף), החלף אותן, אחרת השאר במקום.

בגרף $4$־רגולרי למשל הילוך זה עובד.
אם ניקח את אותו גרף ונחבר את הרכיבים זה לא עובד...

מה בכל זאת אפשר לעשות?

**הגדרה 2.148** זיווג כמעט מושלם הוא זיווג עם $n-1$ צלעות.

נגדיר $\Omega = M_n \cup M_{n-1}$. נדגום בצורה אחידה מ־$\Omega$ החדשה, ואז ההתפלגות המושרה על $M_n$ היא גם אחידה:

$$Pr\left(m \middle| \, m \in M_n\right) = \frac{1}{|M_n|}$$

נניח שאנחנו נמצאים ב־$m$ (שהוא או זיווג מושלם או כמעט מושלם).

1. נבחר קודקוד מקרי $i$ מ־$V_1$ בהתפלגות אוניפורמית.

(א) אם $m$ זיווג מושלם, נעבור לזיווג הכמעט מושלם $m \backslash \{i,j\}$ (יש כזו והיא יחידה, כי $m$ זיווג מושלם)

(ב) אחרת, כלומר אם $m$ זיווג כמעט מושלם, שתי אפשרויות בציור ־ יהי $j$ הקודקוד שלא נמצא בזיווג $m$ בצד השני של הגרף ־ דהיינו $j \in V_2$.

i. אם $i$ גם הוא איננו בזיווג ו־$\{i,j\} \in E$, עבור לזיווג המושלם $m \cup \{i,j\}$.

ii. אם $\{i,j\} \in E$ אבל $i$ נמצא בזיווג $m$, נסמן ב־$\{i,k\}$ את הצלע הקשורה ל־$i$ אשר בזיווג. אזי, עבור לזיווג הכמעט מושלם $(m \backslash \{i,k\}) \cup \{i,j\}$.

2. אחרת, אל תעשה כלום.

על מנת להוכיח ששרשרת מרקוב שהגדרנו מעלה אכן פותרת את הבעיה, עלינו להוכיח:

1. ההילוך קשיר (טיעון קומבינטורי).
2. זמן הערבוב הוא פולינומי ב־$n$ (מאוד מאוד קשה).
3. $M_n$ הוא לא חלק זניח מ־$\Omega$.
4. ההתפלגות הסטציונרית היא אוניפורמית.

### 2.6.8 זמן ערבוב והפער הספקטרלי

תהי $P$ מטריצת מעבר של שרשרת מרקוב סימטרית, לא דו"צ וקשירה. אז ההתפלגות הסטציונרית היא אוניפורמית (ראינו זאת בשיעור).
יהיו $\lambda_1, .., \lambda_n$ הע"ע של $P$, ונניח:

$$1 = |\lambda_1| \geq |\lambda_2| \geq ... \geq |\lambda_n|$$

**הגדרה 2.149** הפער הספקטרלי של $P$ הוא:

$$\triangle := 1 - |\lambda_2|$$

אם הפער הספקטרלי הוא $0$, אז ההילוך לא מתכנס. אחרת, הפער הזה שולט על קצב ההתכנסות של הערבוב.

**משפט 2.150** עבור $P$ כנ"ל:

$$t_{mix} \leq O\left(\frac{\log\left(|\Omega|\right)}{\triangle}\right)$$

ההוכחה - טכנית, מסתכלים על:

$$d_{TV}\left(\mu P^t, \pi\right)$$

והפרטים באתר.

.

# 3 תכנון לינארי

## 3.1 הצגת הבעיה

נתון אוסף של $m$ שיוויונים ואי שיוויונים לינאריים, ורוצים לחפש בין הפתרונות האפשריים פתרון טוב ביותר (כלומר ייתכן והוא לא יחיד) $x \ni \mathbb{R}^n$ כך שנקבל את המקסימום\מינימום $\sum_{i=1}^{n} c_i x_i$, כאשר $\bar{c} \ni \mathbb{R}^n$ וקטור קבוע כלשהוא. כלומר:

$$max\ c^T \cdot x$$

עבור $x \ni \mathbb{R}^n$ כך ש:

$$A \cdot x = b / A \cdot x \geq b$$

כאשר $A$ מטריצה מסדר $m \times n$, $b \ni \mathbb{R}^n$, ו־$n \geq m$[23]. ישנן שתי צורות מקובלות להצגה של תוכניות לינאריות, אותן נראה בתרגול.

מדוע זה מעניין? הרבה בעיות אפשר להעביר לצורה כזו, למשל בעיית הזרימה ברשתות אותה ראינו בקורס "אלגוריתמים".

**דוגמאות**

- נניח כי אנחנו מנהלים רפת, ויש אוסף של סוגי מזון אותו אפשר לתת לפרות. הסוג ה־$i$ מספק $a_{ij}$ מיליגרם ויטמין\קלוריות $j$ לקילו, ומחיר קילו של מוצר $i$ הוא $c_i$. אם מאכילים כל פרה ב־$x_i$ מסוג $i$, המחיר יהיה $\sum_{i=1}^{n} c_i x_i$. כמו כן יש רשימת דרישות ־ כל פרה צריכה לצרוך לפחות כמות מסויימת $b_j$ מכל ויטמין\קלוריות:

$$\sum_{i=1}^{n} a_{ij} x_i \geq b_j,\ j = 1, ..., m$$

בנוסף לזה קיימת הדרישה:

$$x_i \geq 0,\ i = 1, ..., n$$

נרצה למצוא את מינימום העלות, כלומר $x$ שיקיים:

$$min \sum_{i=1}^{n} c_i x_i$$

במקרים הללו $x_i$ הם משתנים רציפים. אולם לא תמיד זה המקרה:

- נתונות נקודות $(x_1, y_1), ..., (x_n, y_n)$ במישור, ומחפשים ישר שנותן אינטרפולציה לינארית טובה ביותר. ברגרסיה לינארית מחפשים $a, b$ כך שבהנתן ישר $y = ax + b$, מחפשים:

$$\min_{a,b} \sum_{i=1}^{n} [y_i - (ax_i + b)]^2$$

[23] זה "המקרה המעניין", אפשר בקלות רבה להגדיר גם אחרת.

הבעיה במרחק הזה היא שברגע שיש נקודה ש"סוטה" מאוד, זה מטה את הקו מאוד - כלומר מספיקה נקודה אחת כדי לקבל ישר מאוד לא טוב. למה כן משתמשים במרחק הזה? כי הוא מאוד פשוט. אפשר גם לתקן לאחר קבלת הערך הטוב ביותר (ותוכנות משוכללות באמת עושות את זה היום).
אפשר, ולפעמים הרבה יותר טוב, לנסות את האופטימיזציה הבאה:

$$\min_{a,b} \sum_{i=1}^{n} |y_i - (ax_i + b)|$$

זה מונע "קצת" את המקרים שתיארנו, ובפועל נותן תוצאות שנראות הרבה יותר טוב. עד כאן הכל טוב ויפה, אבל איך פותרים את זה? זה לא רשום בצורה של תכנון לינארי. הפתרון - להפוך את הבעיה לבעיית תכנון לינארי בצורה די פשוטה - נתבונן בבעיית התכנון הלינארי הבאה:

$$min\ e_1 + ... + e_n$$

תחת האילוצים הבאים:

$$\forall i = 1, ...n : e_i \geq ax_i + b - y_i$$

$$e_i \geq -(ax_i + b - y_i) \Rightarrow e_i \overset{(*)}{\geq} |y_i - (ax_i + b)|$$

כלומר המשתנים שלנו הם $a, b, e_1, ..., e_n$. פתרון אופטימלי מקיים את האי שיוויון $(*)$ בתור שיוויון.

יש אלגוריתמים יעילים לתכנון לינארי, אבל הם לא טריוויאלים. נראה אוסף של אלגוריתמים כאלו, ונראה כי ספיציפית לבעיות מסויימות הם אכן פועלים בזמן פולינומיאלי.
אם מחפשים פתרונות אופטימליים בשלמים, הבעיה היא $NP$ קשה - למשל אם נביט בבעיית $3-SAT$: $c_i = x_{i_1} \vee x_{i_2} \vee x_{i_3}$, אפשר להציגה כבעיית תכנון לינארי באופן הבא:

$$\forall c_i : z_{i_1} + z_{i_2} + z_{i_3} \geq 1$$
$$z_i = x_i\ x_i \geq 0\ or\ z_i = 1 - x_i\ x_i \leq 1$$

כאשר $x_i$ משתנה או שלילי. נשים לב כי:

$$x_i \geq 0 \vee x_i \leq 1 \Rightarrow x_i \in \{0, 1\}$$

השאלה אם בכלל קיים פתרון היא בעיה $NP$-שלמה.
אבל, מה שאפשר לעשות הוא לפתור את הבעיה הזו כאשר לא דורשים שלמים, ואז מקבלים פתרון שברי. במקרה זה הרבה פעמים אפשר לקבל פתרון שלם מהפתרון השברי ע"י קירוב רנדומי. פתרונות מסוג זה מספקים פתרונות "מספיק טובים".
עם זאת, מאז שנות השבעים ועד היום יש הרבה מאמרים שלוקחים למשל את בעיית $TSP$ ומנסים לפתור את הבעיה באופן כזה ולקבל את הפתרון האמיתי בשלמים (בניסיון להוכיח כי $P = NP$). הבעיה היא: זה לא עובד - הרדוקציה בשיטה הזו פשוט לא עובדת לבעיה הזו. אנשים ממשיכים לנסות עד היום.
אחד המאמצים הגדולים של תכנון לינארי - בעיית שיבוצים: *scheduling*. במקרה זה כרגע באמת משתמשים בשיטה זו, והיא למשל חוסכת לחברות תעופה בארה"ב הרבה מאוד כסף. גם חברות שמחפשות נפט משתמשות בשיטה זו. 7/1/2014
בסוף השיעור שעבר נתנו אוסף של שאלות שאפשר לשאול. זוהי רק ההתחלה, יכולנו להמשיך כך שעות... יש גם הרבה דוגמאות שלא נראות לינאריות אך ניתן להציגן כך שיהיה ניתן לפתור אותן בעזרת תכנון לינארי. המרצה ממליץ לנו לחפש עוד דוגמאות בספרות.

## 3.2 ייצוגים שונים של בעיה בתכנון לינארי ופתרונותיה

### 3.2.1 הצגות שונות של בעיה בתכנון לינארי

**הצגה כללית**

$$max\ c^T x$$
$$Ax \geq b$$

**הצגה סטנדרטית** כדי לדון בדברים האלה ובאלגוריתמים (לא נראה במסגרת השיעור, אלא בתרגול), נוח להציג את הדברים בצורה סטנדרטית:

$$max\ c^T x$$
$$Ax = b$$
$$x \geq 0$$

כאשר $x \in \mathbb{R}^n$, $b \in \mathbb{R}^m$. אפשר להניח $m \leq n$, ו"לא מעניין" אם השורות תלויות לינארית.

**הצגה כללית $\Leftarrow$ הצגה סטנדרטית** עבור שורה $a^T x \geq b$:

- מוסיפים משתנה חדש $s$.
- מחליפים את השורה ב־$a^T x - s = b$
- מוסיפים א"ש חדש $s \geq 0$.

אם לאחר כל ההחלפות הללו נשאר משתנה $x$ שאיננו מוגבל להיות חיובי:

- מוסיפים משתנים $y, z$.
- דורשים $y, z \geq 0$.
- מוסיפים שיוויון $x = y - z$.

על כן ניתן להניח כי מלכתחילה התוכנית נתונה בהצגה הסטנדרטית.

### 3.2.2 אוסף הפתרונות המותרים

נתבונן בקבוצה:

$$P = \{x \in \mathbb{R}^n \,|x \geq 0,\ Ax = b\}$$

**הגדרה 3.1** הקבוצה נקראת אוסף הפתרונות המותרים $(feasable)$ של מערכת האילוצים.

**הגדרה 3.2** פתרון מותר $x \ni P$ של מערכת סטנדרטית כפי שהגדרנו הוא פתרון מותר בסיסי.

**הגדרה 3.3** פתרון הוא מותר בסיסי - basic feasable, אם יש קבוצה $B \supseteq \{1,...,n\}$ של עמודות במטריצה $A$, $m = |B|$, כך שמתקיים:

1. המטריצה הריבועית $A_B$ לא סינגולרית.
2. התומך של הוקטור $B \supseteq x$, כאשר $supp(x)$, התומך של $x$, הוא אוסף הקואורדינטות השונות מאפס של $x$.

**למה 3.4** יהי $x$ פתרון מותר. אז $x$ פתרון מותר בסיסי של מערכת סטנדרטית $\Leftrightarrow$ העמודות במטריצה $A_K$ בת"ל, כאשר $K = supp(x)$.

**הוכחה:** $\Leftarrow$ תהי $B$ בגודל $m$ כך ש-$A_B$ רגולרית. אזי כל העמודות בת"ל, ולכן גם $A_K$ בת"ל, כי $B \supseteq K$.

$\Rightarrow$ אם $P \ni x$ פתרון מותר. הנחנו $Rank(A) = m$, $Ax = b \Leftarrow A_K x_K = b$, $m \geq |k|$. נוסיף ל-$K$ עמודות בת"ל מ-$A$ עד שנגיע ל-$m$ עמודות. ונגיע ל-$m = |B|$, $K \subseteq B$. ■

מכאן, בעזרת משפט נוסף, נוכל להגיע לאלגוריתם, אם כי לא יעיל במיוחד, למציאת פתרון למערכת:

**משפט 3.5** נתבונן במערכת הסטנדרטית כפי שהגדרנו מעלה.

1. אם יש פתרונות מותרים, כלומר $P \neq \phi$, והפונקציה $c^T x$ חסומה על $P$, אזי קיים פתרון אופטימלי.
2. אם קיים פתרון אופטימלי, אזי קיים פתרון מותר בסיסי אופטימלי.

**הוכחה:** נתחיל עם הטענה הראשונה. כדי להוכיח אותה צריך מתמטיקה קצת כללית יותר. כדי להוכיח את זה "ננפנף בידיים":

אם הפתרון האופטימלי סופי, אזי ניתן לחסום את אוסף הפתרונות המותרים, ואז המקסימום מתקבל בתוך הקבוצה.

נמשיך לטענה השניה והמעניינת:

יהי $x_0$ פתרון אופטימלי. אזי $c^T x_0$ הוא המקסימום על $P$ של הפונקציה $c^T x$. יהי $x^*$ פתרון מותר עם מספר קואורדינטות שונות מאפס מינימלי, כלומר $c^T x^*$ הוא מקסימלי, וכן $supp(x^*)$ הוא המינימלי מבין הפתרונות המותרים האופטימליים.

**טענה 3.6** נסמן $B = supp(x^*)$. אזי $A_B$ רגולרית - כלומר עמודות $A_B$ בת"ל לינארית.
**הוכחה:** ההוכחה תלך בצורה הבאה: נניח בשלילה, ונצליח "לתקן" קצת את הוקטור $x^*$ כך שעוד קואורדינטה תתאפס. לחילופין אם לא נצליח לעשות את זה, נראה כי הפתרון אינו חסום.

נניח בשלילה שהעמודות $A_B$ תלויות לינארית, כלומר קיים וקטור $\mathbb{R}^n \ni y$ כך ש-$B \supseteq supp(y)$, $y \neq 0$, וכן $Ay = 0$ (ע"י הרחבת הוקטור שנותן את התלות הלינארית בעזרת אפסים).

מקרה ראשון: נניח $c^T y \geq 0$, ויש קואורדינטה $y_j > 0$.

$$x_t = x^* + ty,\ 0 \leq t \in \mathbb{R}$$
$$\Rightarrow c^T x_t = c^T x^* + tc^T y \geq c^T x^*$$

$x_t \in P$, עבור $t$ קטן, שכן:

$$Ax_t = Ax^* + t\overbrace{Ay}^{0} = Ax^* = b$$

בכל קואורדינטה $y_j$ שלילית, $x_j > 0$, לכן אפשר להגדיל את $t$ כך ש־$x_t \ni P$ עד שקואורדינטה נוספת של $x_t$ תתאפס, וזו סתירה למינימליות של התומך של $x^*$.

מקרה שני: אחרת $c^T y < 0$, לכן ניתן לבחור במקום $y$ את $-y$, ולכן בה"כ אפשר להניח $c^T y \geq 0$. אבל אם אין קואורדינטה $y_j < 0$, כלומר $y \geq 0$, אזי:

$$x_t = x^* + ty \in P$$

לכל $t \geq 0$. מכאן נקבל:

$$c^t x_t = c^T x^* + tc^T y \overset{t\to\infty}{\longrightarrow} \infty$$

לכן לא רק ש־$x^*$ לא אופטימלי, אלא גם אין חסם לפתרון האופטימלי, בסתירה להנחה.

נותר המקרה השלישי בו $c^T y = 0$, וכן $y \geq 0$. אזי ניתן להתבונן ב־$-y$, ואז חוזרים למקרה ראשון. ■

■

על כן אנחנו יודעים כי אנחנו יכולים להסתפק רק במעבר על פתרונות בסיסיים, ומכאן אפשר להגיע לאלגוריתם למציאת פתרון, גם אם הוא לא יעיל במיוחד.

כדי לתאר את אלגוריתם הסימפלקס של דנצינגר, נרצה לדון בקבוצה $P$.

### 3.2.3 כיצד נראית הקבוצה $P$ - על פוליטופים קמורים

**הגדרה 3.7** ב־$\mathbb{R}^n$, על מישור הוא אוסף פתרונות של משוואה לינארית אחת:

$$\sum_{i=1}^{n} a_i x_i = b,\ a = (a_1, ..., a_n) \neq 0$$

על מישור מחלק את $\mathbb{R}^n$ לשני חצאי מרחב:

$$\left\{ x \middle| \sum_{i=1}^{n} a_i x_i \geq b \right\},\ \left\{ x \middle| \sum_{i=1}^{n} a_i x_i \leq b \right\}$$

**הגדרה 3.8** פאון קמור (convex polyhedron) הוא חיתוך סופי של חצאי מרחבים ב־$\mathbb{R}^n$ (כאשר נניח שהקבוצה חסומה - במקרהזה משתמשים במונח *polytope*).

**הגדרה 3.9** המימד של פאון $P \subseteq \mathbb{R}^n$ הוא $d$ אם ניתן לבחור $d+1$ נקודות ב־$P$: $x_0, x_1, ..., x_d$ כך ש: $x_1 - x_0, ..., x_d - x_0$ בת"ל, ואי אפשר למצוא $d$ גדול יותר.

**הגדרה 3.10** $v \in \mathbb{R}^n$ הוא קודקוד של פאון $P \subseteq \mathbb{R}^n$ אם:

1. קיים ווקטור $c \neq 0 \in \mathbb{R}^n$ כך ש:

$$c^T v > c^T x$$

עבור כל $x \neq v \in P$.

2. $v \in P$.

ובצורה דומה:

**הגדרה 3.11** $F \subseteq P$ הוא פאה ממימד $k$, אם:

1. $F$ פאון ממימד $k$.
2. יש $c \neq 0 \in \mathbb{R}^n$, $b \in \mathbb{R}$ כך ש־$c^T x = b$ לכל $x \in F$, אבל $c^T x < b$ עבור $x \in P \backslash F$.

**הערה 3.12** קודקוד $v$ הוא פאה ממימד 0.

למשל, לקוביה הסטנדרטית ב־$\mathbb{R}^3$ יש 8 קודקודים, 12 פאות ממימד 1, ו־6 פאות ממימד 2.

**טענה 3.13** תהי $P$ קבוצת הפתרונות המותרים של תוכנית סטנדרטית. אזי התנאים הבאים שקולים:

1. $v$ הוא קודקוד של הפאון $P$.
2. $v$ הוא פתרון בסיסי מותר של המערכת.

**הוכחה:** $1 \Leftarrow 2$ $v$ קודקוד של $P$. נתבונן בבעיה הלינארית של מקסום $c^T x$ כאשר $c$ הווקטור המובטח מהגדרת הקודקוד $c^T v > c^T x$ לכל $x \neq v \in P$. כבר הוכחנו שפתרון האופטימלי יכול להתקבל גם בנקודות מותרות בסיסיות, ברור ש־$v$ הוא פתרון מותר בסיסי (כי יש פתרון אופטימלי יחיד).

$2 \Leftarrow 1$ $v$ הוא פתרון בסיסי מותר של המערכת. תהי $B \supseteq K = supp(v)$, כאשר $B$ קבוצה בגודל $m$ של עמודות בת"ל של $A$. נבחר $c \in \mathbb{R}^n$ כך ש:

$$c_j = \begin{cases} 0 & j \in B \\ -1 & j \notin B \end{cases}$$

אזי:

$$0 = c^t v$$

ובנוסף:

$$v_B = A_B^{-1} b$$

נקבע באופן יחיד, ולכן אם $P \ni x$ ו־$x \neq v$, אזי ל־$x$ יש קואורדינטות שונות מאפס מחוץ ל־$B$, $x \leq 0$, ולכן ל־$x$ יש קואורדינטה חיובית ממש מחוץ ל־$B$, ולכן $c^T x < 0$. ■

מה זה אומר? כאשר אנחנו מסתכלים על הפאון של הפתרונות המותרים, אם אנחנו מחפשים פתרון אופטימלי, די "לטייל" על קודקודי הגרף אשר קודקודיו הם קודקודי $P$, ושני קודקודים מחוברים אם יש פאה ממימד $1$ המחברת ביניהם. אנחנו לא טוענים שהמקסימום מתקבל רק בהם, יתכן והוא יתקבל על דופן שלמה, אבל כדי לדעת ערכים מספיק כאמור להסתכל על הקודקודים. זה למעשה מה שאלגוריתם הסימפלקס, עושה - נראה זאת בתרגיל.

מה דצצינגר הציע לעשות? להתחיל ממציאת קודקוד אחד, לעבור רק לקודקודים שכנים, ולבדוק בהם את הערכים, עד שנגיע למקום בו אי אפשר להגדיל יותר את הפונקציה. נראה אותה בצורה מפורשת בתרגיל.

איך מוצאים בכלל את הקודקוד הראשון? זה לא תמיד פשוט (אבל הרבה פעמים וקטור האפס הוא פתרון).

לאחר מכן נוכל לשאול, איך אפשר לבחור לאיזה קודקוד עוברים? אפשר לבחור למשל את הכיוון בו הפונקציה גדלה הכי הרבה. אבל, קל לתת דוגמאות יחסית פשוטות בהן אורך טיול כזה יהיה אקספוננציאלי.

שאלה עקרונית נוספת: בלי כל קשר לשיטה בה בוחרים קודקודים, האם כשעושים את הטיול הזה באמת ניתן להגיע לכל הקודקודים - כלומר, האם המרחק הוא אקספוננציאלי? במקרה שזה אקספוננציאלי, לא משנה באיזו דרך נבחר את הקודקודים, תמיד נקבל אורך אקספוננציאלי. ישנן השערות שונות בנושא הזה, למשל השערת הירש שהופרכה. אנו יודעים היום כי קוטר הגרף שאנו מקבלים הוא $O\left(n^{\log(n)}\right)$ (תוצאה בת 20־15 שנה, והיא הטובה ביותר הידועה עד היום).

**השערת הירש** בכל פאון ממימד $n$ עם $m$ דפנות ממימד $n-1$ יש מסלול באורך $m-n$ בין כל שני קודקודים.

כך למעשה אלגוריתם הסימפלקס הוא למעשה אוסף של אלגוריתמים. בפועל, האלגוריתם הזה רץ מהר בדר"כ, ואנשים ניסו להצדיק זאת במשך הרבה שנים. תוצאה יפה של $Speilman, Teng$ נותנת הסבר בעזרת smooth analysis.

## 3.3 דואליות בתכנון לינארי

אם מסתכלים על בעיית הזרימה המקסימלית ברשת, הבעיה הדואלית המתאימה לה (לוקח הרבה שורות כדי להוכיח זאת, זוהי לא תוצאה מתבקשת) היא גודל החתך המינימלי. הצרה היא שכדי להציג את הבעיות הללו באופן סטנדרטי יש להשקיע עבודה.

נתונה בעיה סטנדרטית:

$$m := max\ c^T x$$
$$s.t. Ax = b$$
$$x \geq 0$$

נשים לב שכל וקטור $\mathbb{R}^m \ni y$ שמקיים:

$$y^T A \geq c$$

גם מקיים:

$$c^T x \leq y^T \overbrace{Ax}^{b} = y^T b$$

כי $x$ חיוביים ולכן אין בעיה לכפול בשני הצדדים. לכן, ניתן להתבונן בתוכנית הבאה:

$$\begin{aligned} M :=& min\ b^T y \\ & s.t. y^T A \geq c^T \end{aligned}$$

אזי $m \leq M$. לאי השיוויון הזה קוראים דואליות חלשה. משפט הדואליות של תכנון לינארי נותן $m = M$.

קיבלנו מעבר לבעיה עם הרבה פחות משתנים, שכן $y$ בגודל $m$ ולא $n$. בהרבה מאוד מקרים, גם בניתוח של אלגוריתמים וגם באלגוריתמי קירוב, אפשר למשל להסתכל על בעיית ה־$TSP$ גרסת המינימיזציה: אפשר לכתוב אותה כבעיה "ענקית": הרבה אילוצים - $A$ ענק, אפילו אקספננציאלי. בהנתן שיש לנו פתרון, אם נרצה להוכיח כי הוא אופטימלי, אם נוכיח כי הוא אופטימלי בבעיה הדואלית, אזי נקבל שהפתרון הוא גם אופטימלי בבעיה המקורית. כמו כן ניתן להשתמש בבעיה הדואלית על מנת למצוא חסם על הפתרון בבעיה המקורית (וכך לראות שאנחנו מאוד קרובים לפתרון האופטימלי, שכן לפעמים לא ידוע איך להגיע אליו).

**הלמה של פרקש**

**למה 3.14** תהי $A$ מטריצה ממשית מסדר $m \times n$, $b \ni \mathbb{R}^n$ וקטור כלשהוא.
אזי אין פתרון $x \geq 0 \ni \mathbb{R}^n$ למשוואה $Ax = b$ אמ"מ קיים וקטור $y \ni \mathbb{R}^n$ כך ש־$y^T A \geq 0$, וכן $\langle y, b \rangle < 0$.

**הוכחה:** $\Rightarrow$אם $x \geq 0$ פתרון ובכל זאת קיים $y$ כנ"ל, נקבל:

$$\begin{aligned} & Ax = b \\ \Rightarrow & 0 \leq \overbrace{y^T A}^{\geq 0} \overbrace{x}^{\geq 0} = y^T b = \langle y, b \rangle < 0 \end{aligned}$$

וקיבלנו סתירה. ■

## 3.4 תרגולים

31/12/2013

ספר מומלץ על תכנון לינארי - Understanding and Using Linear Programming מאת Jiri Matousek.

### 3.4.1 שתי הצגות לתוכנית לינארית

דוגמא לתוכנית לינארית:

$$\begin{aligned} & min\ x + y + 2z \\ s.t.\ & x \geq 0,\ y \geq 0,\ z \geq 0 \\ & x + y + z = 2 \\ & x + z = 1 \end{aligned}$$

נראה כיצד ניתן להציג אותה:

**ייצוג קאנוני (א"ש)**

מקסם $c^T x$ כך ש:

$$A\vec{x} \leq b$$
$$A_{m\times n},\ b \in \mathbb{R}^n,\ b \in \mathbb{R}^m$$

כאשר בדוגמא שלנו $c^T = (1,1,2)$.
**דוגמא:**

$$max\ \ (-c)^T x$$
$$A\vec{x} \leq b \Rightarrow \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 0 & 1 \\ -1 & 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} \leq \begin{pmatrix} 0 \\ 0 \\ 0 \\ 2 \\ -2 \\ 2 \\ -2 \end{pmatrix}$$

כאשר העברנו את האילוצים לפי סדר הופעתם מעלה.

**תכנון לינארי - ייצוג סטנדרטי (שוויונות)**

מקסם את $c^T x$ כך ש:

$$\vec{x} \geq 0$$
$$A\vec{x} = b$$

איך נביא את התוכנית שלנו לצורה הזו? נוסיף משתנים, למשל:

$$x + y \leq 2 \Rightarrow \begin{cases} x + y + s = 2 \\ s \geq 0 \end{cases}$$

**בדוגמא שלנו**:
מקסם את:

$$(-1,-1,-2) \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

כך ש:

$$x \geq 0$$
$$y \geq 0$$
$$z \geq 0$$

ואז:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} s \\ s \end{bmatrix}$$

טוב, אבל כאן לא באמת שינינו שום דבר... כדי להבין קצת יותר:

**דוגמא נוספת:**

$$\begin{aligned} x + y &\geq 5 \\ x &\leq -1 \end{aligned}$$

ואם ננסה את מה שעשינו קודם נקבל:

$$\begin{aligned} x + s &= 1 \\ s &\geq 0 \\ -x - y + r &= -5 \end{aligned}$$

לא טוב! נגדיר שני משתנים חדשים $x_1, x_2$, $x_1, x_2 \geq 0$, ונחליף את $x$ ב־ $x_1 - x_2$, וכנ"ל לגבי $y$. נקבל:

$$\begin{aligned} -x + x_2 - y_1 + y_2 &= -5 \\ y_1 &\geq 0 \\ y_2 &\geq 0 \end{aligned}$$

טוב, גם כאן החיוביות של $x, y$ נתונה מיידית, אז גם פה לא היינו צריכים את הטריק הזה, אבל חשוב לדעת אותו במידה ונתקל בתוכנית אחרת בה נצטרך לעשות זאת.

**מעבר בין הייצוגים**

- קאנוני $\Leftarrow$ סטנדרטי:
  - לכל א"ש מוסיפים משתנה דמה.
  - כל משתנה "לא מוגבל" $x$ מחליפים ב: $x_1 - x_2$ כאשר $x_1 \geq 0,\ x_2 \geq 0$.
- סטנדרטי $\Leftarrow$ קנוני:
  - מחליפים כל שיוויון בשני אי שיוויונות.
    מקבלים:

$$Ax = b \Rightarrow \begin{bmatrix} A \\ -A \\ -I \end{bmatrix} x \leq \begin{bmatrix} b \\ -b \\ 0 \end{bmatrix}$$

למה צריך את שני היצוגים האלה? תוכנות מחשב "אוהבות לקבל" את הייצוג הקנוני, אבל אלגוריתם הסימפלקס שנלמד בהמשך מקבל את הייצוג הסטנדרטי.

**הערה 3.15** בייצוג הסטנדרטי $A$ היא מסדר $m \times n$. אפשר להניח ששורותיה הן בת"ל, אחרת אחד האילוצים או מיותר או בלתי ספיק. על כן נניח בה"כ כי $m \leq n$ וכי השורות בת"ל.

### 3.4.2 פוליטופים קמורים

קבוצת הפתרונות של תכנון לינארי הוא פוליטופ קמור. מהו? מיד נגדיר.
פוליגון בשני מימדים הוא דבר די מנוון. למזלנו בשלושה מימדים כל התופעות שקורות במימדים גבוהים יותר מתרחשות גם שם, ולכן נוכל לקבל אינטואיציה מפוליגון ב־$\mathbb{R}^3$: קוביה, פירמידה... כעת נשתמש באינטואיציה הזו להגדרות:
ייצוג ראשון:

**הגדרה 3.16** פוליטופ קמור הוא קמור של קבוצה סופית של נקודות.

למשל, הקוביה ה־$n$־מימדית ניתן לייצג כ:

$$C_n = conv\left\{(x_1...,x_n) \middle| x_i \in \{0,1\}\right\}$$

ייצוג שני - "ייצוג חצאי מרחבים":

$$2x - 2y + z \leq 7$$

מחלק את $\mathbb{R}^3$ לשני חצאי מרחבים.

**הגדרה 3.17** פוליטופ קמור הוא:

1. חיתוך של מספר סופי של חצאי מרחבים.
2. חסום.

למשל, נציג את הקוביה בייצוג זה:

$$C_n = \left\{x \in \mathbb{R}^n \middle| \forall i\ x_i \geq 0,\ x_i \leq 1\right\}$$

הייצוג הזה משכן סימפלקס במימד יותר גבוה - למשל נציג את המשולש ב־$\mathbb{R}^3$:

$$S_2 = \left\{x \in \mathbb{R}^3 \middle| x + y + z = 1,\ x \geq 0,\ y \geq 0,\ z \geq 0\right\}$$

עד כה לא אמרנו מהם הקודקודים - אינטואיטיבית הם ה"שפיצים". נגדיר באופן פורמלי:

**הגדרה 3.18** ההגדרות הבאות לקודקוד של פוליטופ $\mathbb{R}^n \supseteq P$ שקולות:

1. נקודה $x \in P$ היא קודקוד אם אי אפשר לרשום את $x$ כממוצע ממושקל של $y, z \in P$, כלומר לא קיים ייצוג:

$$x = \alpha y + (1-\alpha)\, z,\ 0 < \alpha < 1,\ y \neq z$$

2. נקודה $x^* \in P$ היא קודקוד אם קיים וקטור $c$ כך שלפונקציה $c^T x$ (מהפוליטופ ל־$\mathbb{R}$) יש מקסימום **יחיד** ב־$P$ ב־$x^*$.

למה ההגדרה השניה מתאימה למה שאנחנו חושבים עליו בתור קודקוד? נגיד שיש מקסימום יחיד, ונגיד כי $c^T x^* = M$. נתבונן בעל מישור תומך (כלומר הכל הפוליגון נמצא בכיוון אחד של החיתוך שיוצר תת המישור הזה):

$$\left\{ x \in \mathbb{R}^n \middle|\, c^T x = M \right\}$$

למשל אם נביט במשושה בשני מימדים, רק לקודקודים קיים על מישור תומך שעליו החיתוך הוא יחיד.

3. Basic Feasible Solution: תהי $P \subseteq \mathbb{R}^n$ קבוצת הפתרונות החוקיים. נקודה $x \in P$ היא קודקוד אם (בייצוג חצאי מרחבים) לפחות $n$ א"ש בלתי תלויים מתקיימים בשיוויון.

הסבר אינטואיטיבי: נרצה להגיד נקודות על החיתוך של פאות - כלומר אי שיוויון, וצריך להיות שיוויון מספר פעמים מסויים כדי שבאמת זה יהיה קודקוד.
מדוע יש צורך באי תלות? נביט בבעיה $Ax \leq b$, נסמן את השורות של $A$ המסמלות את $n$ האילוצים שמתקיימים ב־$A_B$. אזי $A_B x = b_B$. אם השורות תלויות, אז החיתוך של תת המישורים לא יגדירו לנו נקודה!

אלגוריתם הסימפלקס עובר על כל הקודקודים, ומוצא את הקודקוד הכי טוב. הכי נוח לתאר את זה בעזרת הייצוג השלישי. בשבוע הבא נראה איך הקודקודים האלו נראים בייצוג הסטנדרטי.

### 3.4.3 דוגמא להרצה של אלגוריתם הסימפלקס

7/1/2014

תחילה, תזכורות מהשיעור -
נתונה תוכנית לינארית בצורה הסטנדרטית:

$$\begin{aligned} &max\ c^T x \\ &Ax = b \\ &x \geq 0 \end{aligned}$$

ונסמן את הפוליטופ המוגדר ע"י התוכנית ב־$P$. מניחים כי שורות $A$ בת"ל.
כאשר $A_{m \times n}$, $m$ מספר האילוצים, $n$ מספר המשתנים, ו־$n \geq m$.
כפי שאמרנו בשיעור, מתחילים בקודקוד ראשון, ומסתכלים על הקודקודים השכנים שלו (שכנים במובן של קיימת פאה ממימד 1 המקשרת ביניהם) - אם יש קודקוד שמגדיל את פונקציית המטרה ממשיכים לשכן הבא באותה הצורה, עד שאף שכן לא מגדיל את פונקציית המטרה.

**אלגוריתם 1** אלגוריתם הסימפלקס

1. מצא קודקוד של $P$.
2. עבור לשכן שלו עם ערך יותר גדול.
3. חזור על 2 כל עוד ניתן.

**איפיון של קודקוד של תוכנית לינארית בצורה סטנדרטית (שיוויונית):** $x \in P$ הוא פתרון מותר בסיסי, אם קיימת קבוצה $B \subseteq [n]$ כאשר $|B| = m$, ומתקיים:

1. $supp(x) \subseteq B$
2. $A_B$ הפיכה.

נסביר כיצד מבצעים כל שלב באלגוריתם:

**שלב ראשון:**

- נניח בה"כ כי $b \geq 0$ (אחרת נכפיל את השורות ה"שליליות" ב־$(-1)$).
- נגדיר תוכנית לינארית חדשה. האילוצים:

$$Ax \leq b$$
$$x \geq 0$$

**הערה 3.19** $x = \overline{0}$ הוא פתרון חוקי של התוכנית הזו (כי $b$ א"ש).

נמקסם את הפונקציה:

$$\sum_i (Ax - b)_i$$

כאשר כאן מבצעים את שלב 2 של האלגוריתם (בהנתן שאנחנו יודעים לבצע אותו), ומתחילים מקודקוד שאנו יודעים - $\overline{0}$.
הביטוי הזה הוא אי חיובי תמיד, והוא שווה לאפס אמ"מ $Ax = b$. כלומר אם הצלחנו למקסם, הגענו לפתרון של התוכנית המקורית. אחרת לתכנית המקורית אין אף פתרון $(P = \theta)$.

**השלב השני** לאלגוריתם הסימפלקס אובייקט בסיסי שמייצג קודקוד, קבוצה $B$ ואת התוכנית הלינארית.
נסביר שלב זה ע"י דוגמא:

$$\begin{aligned} & max\ x+y \\ s.t. & -x+y \leq 1 \\ & y \leq 2 \\ & x \leq 3 \\ & x,y \geq 0 \end{aligned}$$

נעביר את התוכנית להצגה סטנדרטית:

$$\begin{aligned} & max\ x+y \\ s.t. & -x+y+s_1 = 1 \\ & y+s_2 = 2 \\ & x+s_3 = 3 \\ & x,y,s_1,s_2,s_3 \geq 0 \end{aligned}$$

ובצורה של מטריצות *איור*.
נתחיל מפתרון ההתחלתי:

$$x = y = 0$$

- בכל קודקוד יהיו $m = 3 \geq$ איברים\משתנים חיוביים (גודל הקבוצה $B$) והשאר יהיו 0.

הקודקוד שמתאים לפתרון הזה הוא:

$$(0,0,1,2,3)$$

- כותבים את התוכנית הלינארית מחדש, ומקבלים את התוכנית הבאה שנקראת בשם Simplex tableaux:

$$\begin{aligned} s_1 &= 1+x-y \\ s_2 &= 2-y \\ s_3 &= 3-x \\ z &= x+y \end{aligned}$$

**הערה 3.20** :

1. המשתנים בצד ימין של השיוויונות אינם ב־$B$ (כלומר הערך שלהם שווה ל־0).
2. המשתנים בצד שמאל של השיוויונות הם ב־$B$.

3. $z$ מיוצג ע"י משתנים שאינם בבסיס.

- בוחרים אחד מהמשתנים מ־$z$ ומגדילים אותו, במידה שבה לא נצא מהפוליטופ. בדוגמא שלנו אנחנו נגדיל את $y$, וזה ישנה את הערך של המשתנים שהם ב־$B$. נגדיל אותו עד שאחת המשוואות מכריחה אותנו לעצור. אפשר להגדיל את $y$ עד $1$ ולא יותר, בגלל המשוואה הראשונה. כותבים את ה־simplex tableaux מחדש, כאשר מחליפים את המשוואה שהכריחה אותנו:

$$\begin{aligned}
y &= 1 + x - s_1 \\
s_2 &= 2 - (1 + x - s_1) = 1 - x + s_1 \\
s_3 &= 3 - x \\
z &= x + (1 + x - s_1) = 1 + 2x - s_1
\end{aligned}$$

והפתרון שמייצג הקודקוד החדש הוא:

$$(0, 1, 0, 1, 3)\,,\ B = \{y, s_1, s_2\}$$

- לא נשאר לנו בחירה, כלומר אנחנו חייבים להגדיל את $x$. הפעם המשוואה השניה מאלצת שלא נוכל להגדיל את $x$ מעבר ל־$1$. נקבל:

$$\begin{aligned}
x &= 1 - s_2 + s_1 \\
y &= 1 + (1 - s_2 + s_1) + s_1 = 2 - s_2 \\
s_3 &= 3 - (1 - s_2 + s_1) = 2 + s_2 - s_1 \\
z &= 1 + 2\,(1 - s_2 + s_1) - s_1 = 3 - 2s_2 + s_1
\end{aligned}$$

והפתרון:

$$(1, 2, 0, 0, 2)\,,\ B = \{x, y, s_3\}$$

- נותר להגדיל את $s_1$: המשוואה המאלצת היא השלישית ־ מגדילים אותו ב־$2$. נקבל:

$$\begin{aligned}
s_1 &= 2 + s_2 - s_3 \\
x &= 1 - s_2 + (2 + s_2 - s_3) = 3 - s_3 \\
y &= 2 - s_2 \\
z &= 3 - 2s_2 + (2 + s_2 - s_3) = 5 - s_2 - s_3
\end{aligned}$$

וזו התשובה הסופית, כי המשתנים $s_2, s_3$ מתקבלים במינוס. נקבל:

$$B = \{x, y, s_1\}\ \ x = (3, 2, 2, 0, 0)$$

מה עשינו ולמה זה מתאים לדבר האינטואיטיבי שאמרנו שנעשה?
בשביל האיברים שלא ב־$B$, יש אילוץ שמתקיים בשיוויון $x_i = 0$.
כאשר מכניסים איבר אחר ל־$B$ ומוציאים אחד:

$$B \to B'$$

המעבר הוא על פני קו ־ השתמשנו במשוואה לינארית אחת כל פעם, ועוברים מאחת לאחת.