# השיטה ההסתברותית

## פרקי העשרה לתלמידים מצטיינים

על בסיס פרקים נבחרים מתוך ספר בעל אותו השם
מאת פרופ׳ נגה אלון ופרופ׳ יואל ספנסר.

תרגם וערך: אוהד פלדהיים

האוניברסיטה העברית

2023

מוקדש למנחי היקר: בְּחֻקֹּתֶיךָ אֶשְׁתַּעֲשָׁע לֹא אֶשְׁכַּח דְּבָרֶךָ.

# מבוא

כל בוגרי הקורס מבוא להסתברות ולסטטיסטיקה, לא יתפלאו לטענה שיש בקומבינטוריקה תועלת רבה בחישוב הסתברויות. למעשה עיקרם של השבועיים הראשונים של הקורס מוקדש לחישוב הסתברותם של מאורעות במרחב הסתברות אחיד לפי הנוסחה: $\mathbb{P}(S) = \frac{|S|}{|\Omega|}$. לפיכך, קל להיווכח שרבה תועלתה של התורה הקומבינטורית להתפתחותה של התורה ההסתברותית, ורעיון זה מופיע כבר במבוא לספרו של אברהם דה-מואבר "תורת הסיכויים" מ-*1718*. עם זאת, הרעיון שתורת ההסתברות יכולה להביא תועלת בחקר הקומבינטוריקה הוא צפוי הרבה פחות ולא בכדי היה עליו לחכות לתגליותיו של פול ארדש מ-1958 על הקשר בין קומבינטוריקה לתורת הגרפים.

אמנם, באותו החישוב ניתן להשתמש לעיתים בחישובים הסתברותיים ככלי עזר בחישוב קומבינטורי כדי לספור את כמות האיברים בקבוצה. כך למשל במהלך הקורס כאשר ספרנו את כמות התמורות שיש להן $k$ נקודות שבת, ניתן היה להציג את החישוב כחישוב הסתברותי או כחישוב קומבינטורי:

סימנו ב-$X$ את מספר נקודות השבת, ב-$B_i$ את המאורע ש-$i$ היא נקודת שבת וכן $B_{i_1,\dots,i_k} = B_{i_1} \cap B_{i_2} \cap \cdots \cap B_{i_k}$.
ראינו כי $\mathbb{P}(B_i) = \frac{1}{n}$ וכי $\mathbb{P}\left(B_{i_1,\cdots,i_k}\right) = \frac{1}{n\cdot(n-1)\cdots(n-k+1)}$ וחישבנו לפי הכלה והפרדה:

$$\mathbb{P}(X=1) = \sum_{k=0}^{n} \sum_{\substack{i_1,i_2,\dots,i_k\subset[n] \\ distinct}} (-1)^k \mathbb{P}\left(B_{i_1,\dots,i_k}\right) = \sum_{k=0}^{n} \binom{n}{k} \frac{(-1)^k}{(n-k)!} = \sum_{k=0}^{n} \frac{(-1)^k}{k!} \approx \frac{1}{e}$$

מתוך כך יכולנו להסיק כי מספר התמורות עם נקודת שבת אחת הוא $n! \cdot \sum_{k=0}^{n} \frac{(-1)^k}{k!}$, עובדה ששימשה אותנו מאוחר יותר בחישוב ההסתברות לכך שתהיינה בדיוק $l$ נקודות שבת בתמורה מקרית.

עם זאת, עיון קפדני בהוכחה יגלה לנו שאילו הכפלנו את כל חישובינו ב-$n!$, היה הנימוק ההסתברותי הופך לנימוק קומבינטורי של ספירה, וההכלה והפרדה ההסתברותית הייתה מתחלפת בהכלה והפרדה קומבינטורית של ספירת מספר האיברים בקבוצה.

כיצד אפוא יכולה תורת ההסתברות לשרת את הקומבינטוריקה **באמת**? ובפרט כיצד היא יכולה להוות עוגן עיקרי בהוכחת קיום?

הרעיון הוא פשוט להפליא:

נניח שעומד לרשותנו מרחב קומבינטורי של אובייקטים מסוימים, למשל גרפים, ואנו מעוניינים לדעת האם קיים אחד מהם שמקיים תכונה $\varphi$. להלן המתכון שמציע ארדש:

1. נגריל באקראי איבר מתוך המרחב לפי ההתפלגות האהובה עלינו.
2. נראה שההסתברות לקיים את תכונה $\varphi$ היא חיובית ונסיק שקיים איבר במרחב שמקיים את התכונה (בלי יכולת לבנות אותו בזמן סביר!).
3. בנוסף, אם ההסתברות לקיום התכונה גבוהה, מצאנו גם אלגוריתם הסתברותית יעיל למציאת האיבר המבוקש.

כשם שהסכמה פשוטה, כך היא גם נדמית כתוכנית מופרכת. מדוע שהוכחה שההסתברות חיובית תהיה קלה יותר מאשר מציאת איבר שמקיים את התכונה?

בסדרת פרקי העשרה זו נראה את קסמה של השיטה הזו בפעולה, נשתכנע בכוחה, וננסה להמחיש מדוע היא פועלת. תוך כדי כך נבין בעקיפין מה כוחה העיקרי של תורת ההסתברות בחישוב כמויות. מטפורה לתוכנית זו היא תוכניתו של אנריקה הספן שהובילה את וסקו דה-גמה מפורטוגל להודו – כאשר דרך היבשה משולה לקומבינטוריקה ודרך הים להסתברות – בתחילה נתקדם לחופיהן של נתיבות מוכרות, ונוכל לתרגם כל מסע הסתברותי בקלות לחישוב קומבינטורי אך ככל שנרחיק להפליג התרגום יעשה כבד ומורכב יותר עד שעליונותה של דרך ההסתברות תראה משכנעת מאד ותגרוף לתוך מחברותינו רווחים תיאורטיים נאים.

# פרק 0 – השיטה הנאיבית

גרף $G=(V,E)$ הוא זוג המורכב מאוסף קודקודים סופי $V$ ומאוסף קשתות $E\subset\{\{v,u\}:\ v,u\in V, v\neq u\}$. דרגתו של קודקוד בגרף המסומנת $d(v)=|\{v,u\}\in E|$. גרף מכוון הוא גרף שבו הקשתות הן זוגות סדורים ולא קבוצות, גרף אינסופי מוגדר באופן דומה עבור $V$ אינסופית, תחת הדרישה שדרגת כל קודקוד תהיה סופית (סופיות מקומית). נסמן $[n]$ עבור המספרים מ-1 עד $n$. וכן $[n]_0$ עבור המספרים מ-0 עד $n-1$.

**דוגמא 1.** $k$-צביעה של גרף $G=(V,E)$ היא פונקציה $f:V\to[k]$ נסמן את כל ה-$k$-צביעות של גרף $G$ ב-$k^G$. תת-גרף הוא קבוצה $E'\subset E$. מחלקת צביעה של צבע $i$ היא התת-גרף הנפרש על ידי $f^{-1}(i)$. נאמר כי $G$ מכיל עותק של גרף $G'$ ונסמן $G'\subset G$ אם יש העתקה חח"ע של קודקודי $G'$ לקודקודי $G$ כך שהתמונה המושרית של כל קשת של $G'$ היא קשת ב-$G$ (זו דרישת הכלה, תוספת קשתות ל-$G$ רק מגדילה את כמות התת-גרפים $G'$. הגרף השלם על $n$ קודקודים (כלומר זה שבו יש קשת בדיוק בין כל שני קודקודים שונים), יסומן ב-$K_n$.

מספר רמזי (*Ramsey*) $R(k,l)$ הוא השלם המינימלי $n$ כך שמתקיים $K_k\subset f^{-1}(1)$ או $K_l\subset f^{-1}(2)$ עבור כל 2-צביעה של הגרף השלם על $n$ קודקודים, כלומר:

$$R(k,l)=min\{n:\ \forall f\in 2^{K_n}, K_k\subset f^{-1}(1)\ or\ K_l\subset f^{-1}(2)\}.$$

רמזי הוכיח ב-1929 שלכל $k$ ו-$l$ מספר רמזי $R(k,l)$ סופי. אנו נבקש להציג חסם תחתון (כמעט הטוב ביותר הידוע) על $R(k,k)$. לשם כך עבור $n$ נתון, עלינו להראות צביעה שעבורה לא קיים עותק של $K_k$ בשתי מחלקות הצבע. זוהי בפירוש בעיית קיום קומבינטורית, הבה נשתמש בשיטה ההסתברותית כדי להראות כי:

**טענה 1.** אם $\binom{n}{k}\cdot 2^{1-\binom{k}{2}}<1$ אז $R(k,k)>n$; בפרט, $R(k,k)>\lfloor 2^{k/2}\rfloor$.

הוכחה. נגריל באקראי ובאופן אחיד צביעה $f\in[2]^{K_n}$. נסמן את אוסף הקבוצות של $k$ קודקודים בגרף ב-$L_k$ ונשים לב כי $|L_k|=\binom{n}{k}$. לכל $S\in L_k$ נסמן מאורע $E_S=\{f(S)\in\{\{1\},\{2\}\}\}$. אנחנו מעוניינים להראות כי

$$\mathbb{P}\left(\bigcup_{S\in L_k}E_s\right)<1$$

ולהסיק כי המאורע המשלים, לפיו קיימת צביעה שבה אין אף עותק מונוכרומטי של $S_k$ בגרף מתרחש בהסתברות חיובית, כלומר קיימת צביעה כזו ולכן $R(k,k)>n$. בוגרי מבוא להסתברות לא יתפלאו אם נפעיל במקרה זה את חסם האיחוד. כיוון שלכל $S$, מתוך האי-תלות של הקשתות השונות בצביעה מתקיים $\mathbb{P}(E_S)=2^{1-\binom{k}{2}}$. לפי חסם האיחוד נקבל אפוא:

$$\mathbb{P}\left(\bigcup_{S\in L_k}E_s\right)\leq\sum_{S\in L_k}\mathbb{P}(E_S)=|L_k|2^{1-\binom{k}{2}}=\binom{n}{k}\cdot 2^{1-\binom{k}{2}}$$

שהנה אמנם קטנה מ-1 לפי הנחת הטענה. לסיום הוכחת הטענה נחשב עבור $n=\lfloor 2^{k/2}\rfloor$ ו-$k\geq 3$:

$$\binom{n}{k}2^{1-\binom{k}{2}}<\frac{n^k}{k!}\cdot\frac{2^{1+\frac{k}{2}}}{2^{k^2/2}}=\frac{2^{1+\frac{k}{2}}}{k!}<1.$$

■

ברמה זו של השיטה היא עדיין קומבינטורית מאד. יכולים היינו לפתוח את ההוכחה ההסתברותית ולהחליף את אי-שוויון בול (חסם האיחוד), בספירת יתר, כאשר אנו סופרים את כמות הצביעות שמשאירות כל קבוצה מונוכרומטית, סוכמים אותן ומסתכנים בספירות חוזרות, ומגלים שלא הגענו לסך כמות הצביעות הכוללת – לכן נותרו צביעות שאינן משאירות שום קבוצה מונוכרומטית.

**דוגמא 2.** נראה עוד דוגמא בסיסית אשר יופייה נובע מהיותה הדוקה. מחלקה של קבוצות נקראת נחתכת אם לכל שתי קבוצות במחלקה חיתוך לא ריק. יהיו $k \le n/2$ מספרים טבעיים ותהי $\mathcal{F}$ מחלקה נחתכת של קבוצות שכל אחת מהן בגודל $k$ והן מורכבות מהמספרים $[n]_0$. קל להיווכח כי קיימת $\mathcal{F}$ כזו, עבורה $|\mathcal{F}| = \binom{n-1}{k-1}$ – זוהי מחלקת הקבוצות שמכילות את המספר 1. משפט ארדש-קו-רדו (*Erdős-Ko-Rado*) קובע כי זו הקבוצה הנחתכת הקטנה ביותר. אנו נבקש להציג עבורו הוכחה בשיטה ההסתברותית. לשם כך נזדקק לטענת העזר הבאה:

**טענת עזר.** לכל $s \in [n]_0$ נגדיר את $A_s$ להיות $k$ האיברים העוקבים החל מ-$s$ מודולו $n$. אזי קבוצה נחתכת יכולה להכיל $k$ קבוצות כאלה לכול היותר.

**הוכחה.** נסתכל על $\boldsymbol{A_{k-1}}$. ישנן בדיוק $2k-2$ קבוצות שנחתכות איתה – $A_0$ עד $A_{2k-2}$. הללו נחלקות לזוגות זרים: $A_i, A_{i+k}$ ולכן כיוון שנוכל לכלול רק את הקבוצה עצמה ועוד אחת מכל זוג נקבל לכל היותר $k$ קבוצות. כעת הטענה נובעת מאינדוקציה. ■

מכך נסיק כי גם לכל תמורה $\sigma_0$ מתקיים כי מחלקה נחתכת יכולה להכיל לכל היותר $k$ קבוצות מ הצורה $\sigma_0(A_i)$.

**משפט 2. ארדש-קו-ראדו (1972).** תהי $\mathcal{F}$ מחלקה נחתכת של קבוצות שכל אחת מהן בגודל $k$ והן מורכבות מהמספרים $[n]_0$. אזי $|\mathcal{F}| \le \binom{n-1}{k-1}$.

**הוכחה.** נגריל $i \sim \mathrm{unif}([n]_0)$ ותמורה מקרית $\sigma$ על $[n]_0$. נסתכל על $\sigma(A_i)$. לכל תמורה $\sigma_0$ מתקיים $\mathbb{P}(\sigma_0(A_i) \in \mathcal{F}) \le \frac{k}{n}$ ולכן $\mathbb{P}(\sigma(A_i) \in \mathcal{F}) = \sum_{\sigma_0} \mathbb{P}(\sigma = \sigma_0)\mathbb{P}(\sigma_0(A_i) \in \mathcal{F}) \le \frac{k}{n}\sum_{\sigma_0} \mathbb{P}(\sigma = \sigma_0) = \frac{k}{n}$. אבל $\sigma(A_i)$ היא קבוצה מקרית אחידה (מדוע?), ולכן אם נסמן ב-$S_n$ את אוסף התמורות על $n$ איברים,

$$\frac{|\boldsymbol{\mathcal{F}}|}{|\{\boldsymbol{U} \subset \boldsymbol{S_n} : |\boldsymbol{u}| = \boldsymbol{k}\}|} = \mathbb{P}(\sigma(A_i) \in \boldsymbol{\mathcal{F}}) = \frac{\boldsymbol{k}}{\boldsymbol{n}}$$

והרי: $|\mathcal{F}| \le \binom{n}{k}\frac{k}{n} = \binom{n-1}{k-1}$, כנדרש. ■

גם דוגמא זו ניתנת לכתיבה מחדש בשפה קומבינטורית טהורה, אך המאמץ הדרוש לכך רב יותר (הקורא מוזמן לנסות...). בכל זאת, דוגמאות פשוטות אלה מראות לנו כיצד בידוד של משתנים מקריים ואי-תלות יכולים להעניק השראה לנימוק ספירה. ישנן עוד מגוון דוגמאות נאות לשיטה הבסיסית. נותיר אחת מהן כתרגיל ונמשיך לשיטות מתקדמות יותר שיוסיפו להעמיק ולהצדיק את השימוש בהסתברות להשגת תוצאות קומבינטוריות.

**תרגיל 1.** טורניר הוא גרף מכוון $G = (V, E)$ המקיים $(u,v) \in E \leftrightarrow (v,u) \notin E$. טורניר נקרא עובר (טרנזיטיבי) אם לכל שלושה קודקודים $(u,v),(v,w) \in E \leftrightarrow (u,w) \in E$. קל להיווכח כי טורניר טרנזיטיבי משרה סדר מלא על אברי $V$ ובפרט יש לו "מנצח", קודקוד אשר יוצאות ממנו קשתות לכל יתר הקודקודים. טורניר שאינו עובר מקיים את התכונה שלכל קודקוד נכנסת קשת. הכללה של תכונה זו, מעין אי-עוברות חזקה, היא התכונה הבאה המכונה $S_k$:

$$\forall v_1, \dots, v_k \in V \exists u : (u, v_1), \dots, (u, v_k) \in E.$$

יש להראות שאם $\binom{n}{k}\left(1 - 2^{-k}\right)^{n-k} < 1$ אז קיים טורניר על $n$ קודקודים שמקיים את התכונה $S_k$.

**תרגיל 2**(*). יש להראות שאת קודקודיו של כל גרף בן $n$ קודקודים מדרגה מינימלית $\delta > 10$, ניתן לחלק לשתי קבוצות $A$ ו-$B$, כך שלכל קודקוד באחת מהן יש שכן אחד לפחות בשניה וכן $|A| \le O\left(\frac{n\, lo}{\delta}\right)$.

## פרק 1 – שיטת המומנט הראשון

בלימודי מבוא להסתברות ההכללה הטבעית הראשונה שראינו לאי-שוויון בול היה חסם התוחלת (אי-שוויון מרקוב). צורתו הבסיסית ביותר של החסם הבטיחה לנו שלא יתכן שמשתנה מקרי יהיה כמעט תמיד גדול מתוחלתו. כוחה של התוחלת היה בכך שחישובה היה ליניארי ולכן כדי לחשב את תוחלתו של סכום די היה לחשב את תוחלת כל אחד מאבריו בנפרד ולסכום אותם.

הנה נציג דוגמא לשימוש בליניאריות התוחלת ובצרה מנוונת זו של אי-שוויון מקרוב לצורך השיטה ההסתברותית, ומשם נמשיך לשימושים חזקים יותר של האי-שוויון.

**דוגמא 3.** קבוצה של קודקודים $V' \subset V$ בגרף $G = (V, E)$ נקראת "שולטת" אם כל קודקוד בגרף נמצא במרחק לכל היותר 1 ממנה, כלומר הוא נכלל בה או שכן שלה.

**טענה 3.** בגרף על $n$ קודקודים עם דרגה מינימלית $\delta$ קיימת קבוצה שלטת בה לכל היותר $n\big((1 + log(\delta + 1))\,/(\delta + 1)\big)$ קודקודים.

**הוכחה.** ננסה לבנות באקראי קבוצה שלטת ונראה שאנו עתידים להצליח בהסתברות חיובית. נבחר פרמטר $p$ שיקבע מאוחר יותר, ונגריל לכל קודקוד $v$ באופן בלתי-תלוי משתנה מקרי $X_v \sim Ber(p)$ שישמש כמציין לכך ש-$v$ נכלל במועמדת שלנו לקבוצה השלטת. ההסתברות שקודקוד נתון $u$ נמצא במרחק 1 מקודקוד שנבחר לקבוצה שלנו היא $(1-p)^{d(u)+1}$, כיוון שכל שכניו באופן בלתי-תלוי צריכים שלא להיבחר. תוחלת מספר הקודקודים שאינם מכוסים נתונה אפוא על ידי:

$$\mathbb{E}(|Z_1 \coloneqq \{u: \forall v \in V, d(v,u) \leq 1, X_v = 0\}|) = \sum_{u \in V} (1-p)^{d(u)+1} \leq n(1-p)^{\delta+1}.$$

נהיר שאם תוחלת זו קטנה מ-1, הרי שכיוון שבכל גרף יש מספר שלם של קודקודים לא מכוסים, אז קיימת הסתברות חיובית שמספר הקודקודים הלא מכוסים יהיה 0 – כלומר שכל הקודקודים יכוסו, הבעיה היא שאיננו יודעים כמה קודקודים בחרנו...

תוחלת גודל הקבוצה שבחרנו היא כמובן, לכל $v \in V$,

$$\mathbb{E}(|Z_2 \coloneqq \{u: X_u = 1\}|) = |V|\mathbb{P}(X\_v = 1) = np.$$

נסתכל על הכמות $|Z_1| + |Z_2|$, הקודקודים בשתי הקבוצות הללו מהווים תמיד קבוצה שולטת (כי היא כוללת את הנשלטים על ידי $Z_1$ ביחד עם אלו שלא נשלטים על ידיה. נחשב את תוחלת גודל קבוצה זו ונקבל:

$$\mathbb{E}(|Z_1| + |Z_2|) \leq n\big(p + (1-p)^{\delta+1}\big)$$

זו מערכת שלמה של אי-שוויונים המתאימים להסתברויות בחירה שונות. כל אחד מאי-שוויונים אלה נותן חסם עליון על גודל הקבוצה השולטת המינימלית. נבצע אופטימיזציה על $p$. נקל על עצמנו בהצבה $1 - p < e^{-p}$, נגזור ונשווה ל-0.

$$1 - (\delta + 1)e^{-p(\delta+1)} = 0$$

$$p = \frac{log(\delta + 1)}{\delta + 1}$$

נציב ונקבל כי קיימת בחירה שעבורה

$$|Z_1 + Z_2| \leq n(1 + log(\delta + 1))/(\delta + 1).$$

■

נראה דוגמא הדוקה נוספת מאותו הסוג.

**דוגמא 4.** נזכר כי 2-צביעה של גרף היא העתקה מקשתותיו ל-$\{1,2\}$ וכי עותק חד צבעי של $K_k$ הוא $k$ קודקודים שנצבעו באותו הצבע.

**טענה 4.** קיימת צביעה של $K_n$ ב-2 צבעים שמכילה לכל היותר $\binom{n}{k}2^{1-\binom{n}{k}}$ עותקים חד-צבעיים של $K_k$.

**הוכחה.** נחשב את תוחלת מספר העותקים החד-צבעיים של $K_k$. בוודאי ישנה צביעה שמספר העותקים בה קטן או שווה מהתוחלת. ההסתברות של כל עותק להיות חד-צבעי היא $2^{1-\binom{n}{k}}$ וכיוון שישנן בדיוק $\binom{n}{k}$ אפשרויות לבחור $k$ קודקודים שמגדירים עותק פוטנציאלי – התוצאה נובעת מיידית מליניאריות התוחלת. ■

**דוגמא 5.** גרף נקרא דו-צדדי אם ניתן לחלק את קודקודיו לשתי מחלקות כך שכל הקשתות בגרף מחברות קודקוד ממחלקה אחת לקודקוד מהמחלקה האחרת. הפעם ננסה לחקור את המבנה של גרפים דו-צדדיים בתוך גרף נתון.

נפתח בתרגיל שמכליל את הדוגמא הקודמת.

**תרגיל 3.** $K_{m,n}$ הגרף הדו-צדדי השלם של $m$ ו-$n$ קודקודים. בגרף זה על $(m+n)$ נמצאות כל הקשתות שמחברות את $n$ הקודקודים הראשונים ל-$m$ האחרונים, ורק הן. יש להראות כי קיימת 2-צביעה של $K_{m,n}$ שבה לכל היותר $\binom{m}{a}\binom{n}{b}2^{1-ab}$ עותקים חד צבעיים של $K_{a,b}$.

עתה, נציג דוגמא נוספת לשיטת המומנט הראשון ונראה כיצד באמצעות כלים חדשים ניתן לשפר את החסם הבסיסי של שיטה זו.

**טענה 5.** לכל גרף על $n$ קודקודים שבו $e$ קשתות, קיים תת-גרף דו-צדדי שבו לפחות $\frac{e}{2}$ קשתות.

**הוכחה.** נגריל לכל קודקוד $v$ בגרף משתנה מקרי בלתי-תלוי $X_v \sim \mathrm{Ber}\left(\frac{1}{2}\right)$. נכנה קשתות מהצורה $\{(u,v): X_u \neq X_v\}$ בשם קשתות חוצות. נשים לב שלכל קשת סיכוי $\frac{1}{2}$ להיות חוצה. מכאן שתוחלת מספר הקשתות החוצות היא $\frac{e}{2}$. לפי שיטתנו נסיק כי קיימת הגרלה של המשתנים המקיים כך שהקשתות החוצות תרכבנה גרף דו-צדדי בן $\frac{e}{2}$ קשתות. ■

נשפר טענה זו באמצעות בחירה זהירה מעט יותר של מרחב ההסתברות.

**טענה 5'.** לכל גרף על $2n$ קודקודים שבו $e$ קשתות, קיים תת-גרף דו-צדדי שבו לפחות $\frac{en}{2n-2}$ קשתות.

**הוכחה.** הפעם נגריל קבוצה בת בדיוק $n$ קודקודים באופן אחיד, ונכנה קשת "חוצה" אם היא מפרידה את הקבוצה הזו משאר הגרף. ההסתברות של קשת להופיע היא ההסתברות לבחור את צדה האחד לקבוצה ולא את השני כלומר

$$\frac{\binom{2n-2}{n-1}}{\binom{2n}{n}} = \frac{n}{2n-2}$$

לפי שיטתנו נסיק כי קיימת הגרלה כזו כך שמניין הקשתות החוצות יהיה $\frac{en}{2n-2}$. ■

נסיים את הפרק בדוגמא עם מרחב הסתברות מורכב עוד יותר.

**טענת עזר.** לכל $P(X_1,\ldots,X_k)$ פולינום הומוגני מדרגה $k$ על $n$ משתנים שמקדמיו $a_{x_{i_1},\ldots,x_{i_k}}$ נמצאים בתחום $[-1,1]$ כאשר מתקיים $a_{x_1,\ldots,x_k}=1$, קיימים $z_1,\ldots,z_k \in [0,1]$ כך ש-$|P(z_1,\ldots,z_k)| > c_k$ כאשר $c_k$ הוא קבוע אוניברסלי חיובי שתלוי רק ב-$k$.

**הוכחה.** קבוצת הפולינומים המתוארת היא תחום קומפקטי של פונקציות רציפות שאף אחת מהן אינה פונקציית האפס ולכן מרחקן המכסימלי מ-0 חיובי. פונקציית המקסימום רציפה במקדמים ופונקציה חיובית רציפה על תחום קומפקטי מקבלת מינימום אבסולוטי.

**טענה 6.** תהי $V=[kn]$, נסמן $V^k=\{U\subset V: |U|=k\}$ קשתות ההיפר-גרף ה-$k$ רגולרי השלם. תהי $h: V^k \to \{\pm 1\}$ פונקציה המתארת צביעה של הקודקודים בשני צבעים. עבור חלוקה מאוזנת של קודקודי הגרף $V = V_1 \dot\cup V_2 \dot\cup \ldots \dot\cup V_k$, כאשר $|V_i|=n$, נאמר כי קבוצה הנה ***k*-חוצה** אם היא מכילה נקודה אחת מכל מחלקה של החלוקה. נניח כי $h$ מקבלת את הערך 1 על כל קבוצה $k$-חוצה. אזי קיימת $S\subset V$ המקיימת

$$h(S) := \sum_{U\subset S, |U|=k} h(U) \geq c_k n^k.$$

במילים אחרות: צביעה של קשתות חוצות של היפר גרף ה-$k$ רגולרי, חייבת בהכרח להיות מוטה מאד על תת-היפר גרף.

**הוכחה:** נגריל לכל קודקוד $u$ במחלקה ה-$i$ משתנה מקרי ב"ת $X_u \sim \mathrm{Ber}(p_i)$, כאשר ערכים אלו יקבעו בהמשך. נתעניין ב-

$$h(\{u: X_u = 1\}) = \sum_{U\subset V, |U|=k} h(U) \prod_{u\in U} X_u.$$

ניקח תוחלת, נקבץ לפי סוגי איברים ונקבל

$$\mathbb{E}(h(\{u: X_u = 1\})) = \sum_{a_1+\cdots+a_k=k} \prod_{i=1}^{k} p_i^{a_k} \sum_{\substack{U\subset V, |U|=k \\ |U\cap V_i|=a_i}} h(U),$$

כאשר הטיפוס $a_1, \dots, a_k = 1$ תורם לסכום בדיוק $n^k$ לפי הנחתנו, ואילו תרומתו של כל טיפוס קטנה בערכה המוחלט מ-$n^k$, כיוון שהגורם המולטינומי $\binom{n}{a_1}\cdots\binom{n}{a_k}$ שלו קטן מ-$n^k$. נסיק אפוא כי $\mathbb{E}(h(\{u: X_u = 1\}))/n^k$ ניתנת לכתיבה כפולינום הומגני המקיים את דרישות טענת העזר, ולכן קיימים $p_1, \dots, p_k$ המקיימים

$$|\mathbb{E}(h(\{u: X_u = 1\}))| \ge c_k n^k,$$

ולפי שיטתנו קיימת בחירה של המשתנים שנותנת את המסקנה המבוקשת.■

למשפט מסקנה מעניינת: ארדש הוכיח ב-1965 שכל 2-צביעה של $k$-יות מתוך קבוצה של $n$ איברים מכילה לפחות $m$-$k$-יות זרות כך שכל הקשתות החוצות ביניהן צבועות באותו צבע עבור $m = C(\log n)^{\frac{1}{k-1}}$. מהמשפט שהראינו נוכל אפוא להסיק שקיימת קבוצה בגודל $C(\log n)^{\frac{1}{k-1}}$ כך שלפחות $\frac{1}{2}+\epsilon_k$ מה-$k$-יות שמרכיבות אותה חד-צבעיות, תוצאה מעניינת כיוון שאילו רצינו קבוצה שכולה חד צבעית – היינו יכולים למצא כזו רק מגודל $\underbrace{\log \dots \log}_{k-2 \text{ times}} n$.

**תרגיל 4**. יהי $H$ גרף ונניח כי קיים גרף בן $n$ קודקודים ו-$t$ קשתות שאין בו עותקים של $H$. לכל $t > \frac{n^2 \log n}{k}$ יש להראות כי לא קיימת צביעה של הגרף השלם $K_t$ ב-$k$ צבעים שאין בה עותק חד-צבעי של $H$.

**תרגיל 5** (*). יהי $X$ אוסף אורתונורמלי של וקטורים ב-$R^n$ (כל שניים אורתוגונלים, וכל אחד בעל נורמה 1). נניח שההיטל של כל וקטור באוסף על $k$ הקורדינטות הראשונות הינו מנורמה לפחות $\epsilon$. הראו כי $|X| \le k/\epsilon^2$ וכי חסם זה הדוק כאשר $\epsilon^2 = \frac{k}{2^r} < 1$.

# פרק 2 – שיטת התיקון המקומי

עד כה עסקנו במודלים שבהם תכונה מבוקשת מתרחשת באקראי בתוחלת ולעיתים קרובות גם בהסתברות גבוהה. בפרק זה נראה כמה דוגמאות שבהן שיטה זו נכשלת, אך הכישלון אינו חרוץ כל כך, ובאמצעות תיקון אקראי\קומבינטורי נוסף ניתן להוכיח את קיומו של האובייקט המבוקש.

נפתח בשיפור לחסם התחתון למספר רמזי.

**טענה 7.** לכל שלם $n$ מתקיים $R(k,k) > n - \binom{n}{k}2^{1-\binom{k}{2}}$.

**הוכחה.** תהי $f: K_k \to \{1,2\}$ צביעה מקרית ואחידה של קשתות $K_k$. לכל $S$ $k$-יה של קודקודים נגדיר משתנה מקרי באמצעות $X_S = \mathbb{1}\{|f^{-1}(S)| = 1\}$. כהרגלנו נרשום $X = \sum_S X_S$ ונחשב

$$\mathbb{E}\left(\sum_S X_S\right) = \sum_S \mathbb{E}(X_S) = \binom{n}{k}2^{1-\binom{k}{2}}$$

נסיק כי קיימת צביעה עם מספר זה של $k$-יות חד-צבעיות לכל היותר. כעת נסיר קודקוד אחד מכל $k$-יה כזו ובגרף שיוותר לא תהיינה $k$-יות מונוכרומטיות. סה"כ נותרנו עם $n - \binom{n}{k}2^{1-\binom{k}{2}}$ קודקודים, כנדרש.■

כעת נבצע אופטימיזציה על $n$, נרצה שיתקיים

$$n = 2\binom{n}{k}2^{1-\binom{k}{2}} < 2\left(\frac{ne}{k}\right)^k 2^{1-\binom{k}{2}}$$

כלומר:

$$\frac{k^k 2^{1-\binom{k}{2}}}{e^k} < n^{k-1}$$

ניקח שורש $k-1$ ונקבל שכדאי לבחור $n > \frac{k^{1-o(1)}2^{\frac{1}{k-1}-\frac{k}{2}}}{e}$.

נבחר אפוא $n = e^{-1}k2^{k/2}\big(1+o(1)\big)$ ונקבל:

$$\mathrm{R}(k,k) > \frac{1}{e}\big(1+o(1)\big)k2^{k/2}$$

שימוש זהיר יותר בחסם מטענה 1 היה נותן לעומת זאת

$$R(k,k) > \frac{1}{e\sqrt{2}}\big(1+o(1)\big)k2^{k/2}.$$

נראה דוגמא מסובכת יותר העוסקת בצביעת קבוצות.

**דוגמא 6.** נגדיר $m(n)$ להיות הכמות המינימלית של קבוצות בגודל $n$ כך שבהכרח בכל צביעה בשני צבעים של אברי הקבוצות – אחת הקבוצות תהיה חד-צבעית. אנחנו נראה את החסם העליון הטוב ביותר הידוע עבור $m(n)$.

המשפט הוא הרחבה של שיטות של ארדש (1963) ושיפורים של בק (1978).

**טענה 8.** [*Radhakrishnan-Srivasan, 2000*] אם קיים $\mathrm{p} \in [0,1]$ המקיים $k(1-p)^n + k^2p < 1$, אז מתקיים $m(n) > 2^{n-1}k$.

**מסקנה.** $m(n) > C2^n\left(\frac{n}{\log n}\right)$

**הוכחת המסקנה.** נשתמש בכך ש-$1 - p < e^{-p}$. נגזור את $\mathrm{k}e^{-np} + k^2 p$ לפי $p$ ונשווה ל-0 כדי ונקבל:

$$k^2 - nke^{-np} = 0$$

כלומר $p = \frac{\log(n/k)}{n}$. נציב ונקבל שהתנאי מתקיים אם

$$ke^{-np} + k^2 p = \frac{k^2}{n}(1 + \log(n/k)) \; < 1$$

נשתמש בכך שעבור $k = c\sqrt{\frac{n}{\log n}}$ מתקיים

$$\frac{k^2}{n}\left(1 + \log\left(\frac{n}{k}\right)\right) = \frac{c}{\log n}\left(1 + \log\left(c\sqrt{\frac{\log n}{n}}\right)\right) < 1$$

לכל $c < \sqrt{2}$. ■

כעת נשתמש בשיטת התיקון המקומי ובליניאריות התוחלת כדי להוכיח את הטענה עצמה.

**הוכחת טענה 8.** התנאי בטענה מאפיין את שיטת התיקון ומזכיר את הבניה שראינו לקבוצה שולטת בטענה 3. נבצע בניה בשני שלבים, הראשון ינסה להשיג צביעה לא מונוכרומטית של מרבית הקשתות והשני ינסה לתקן את אלו שצביעתן נכשלה. אנו מעוניינים שסיכויי כישלון בתהליך דו-שלבי כזה יהיו קטנים מ-1, ולשם כך נבקש שהסיכויים לכישלון בכל שלב יהיו קטנים מחצי. סיכויים אלה מגולמים בשני הגורמים שבהנחת הטענה.

יהי $\mathcal{F}$ אוסף קבוצות של איברים ב-$V$ שכל אחת מהן מגודל $n$ ומספרן $2^{n-1}k$ עבור $k$ המקיים את תנאי השאלה ביחס ל-$p$ מסוים. נגריל צביעה $f_0 \colon V \to [2]$ מקרית של $V$ באופן אחיד ומשתנים מקריים בלתי תלויים $Y_v \sim \mathrm{Ber}(p)$ לכל $v \in V$.

**שלב 1.** $X_v$ מהווה הצעה לצביעה של הקודקודים בצבעים 0 ו-1. נסמן ב-$D_0$ את הקבוצה המקרית:

$$D_0 := \{v \in V : \exists S \in \mathcal{F}, v \in S, |f_0(S)| = 1\}$$

אלו הם הקודקודים שמשתתפים בקשת חד-צבעית לפי הצביעה המושרית על ידי $f_0$.

**שלב 2.** נעבור על קודקודי V בסדר מקרי, לצורך כך נסמנם $v_1, \dots, v_\ell$ ולסדר כולו נקרא $\sigma$. בשלב נגדיר

$$f_i(v) = \begin{cases} f_{i-1}(v) & v \notin D_i \text{ or } v \neq v_i, \\ f_{i-1}(v) & Y_{v_i} = 0, \\ 2 - f_0(v) & \text{otherwise.} \end{cases}$$

כעת נעדכן את הקבוצה המשתתפת בקבוצה חד-צבעית

$$D_i := \{v \in V : \exists S \in \mathcal{F}, v \in S, |f_{i-1}(S)| = 1\}.$$

נשים לב שקודקוד אינו עשוי להחליף צבע יותר מפעם אחת ויחידה.

**ניתוח.** נאמר שהצביעה נכשלה אם קיימת קבוצה $S \in \mathcal{F}$ כך ש-$|f_\ell(S)| = 1$. את המאורע הזה נפרק לארבעה מקרים:

$$E_{0,b}(S) = \{f_\ell(S) = f_0(S) = \{b\}\} \qquad E_{1,b}(S) = \{f_0(S) \neq f_\ell(S) = \{b\}\}$$

ונסמן $E_{a,b} = \cup_S E_{a,b}(S)$.

נחשב בקלות את הסיכוי שקבוצה תתחיל חד-צבעית ולא תתוקן:

$$\mathbb{P}\left(E_{0,b}(S)\right) = 2^{-n}(1-p)^n.$$

ניתוח הגורם השני מעניין ומורכב בהרבה. נאמר כי קבוצה $S$ מאשימה קבוצה $U$ בצבע $b$ ונסמן $\mathrm{E}_{\mathrm{U}\to b}(\mathrm{S})$ אם:

1. $|S \cap U| = 1$, ונסמן $S \cap U = v_i$. [חפיפה של קודקוד יחיד]
2. $f_\ell(S) = \{b\}, f_0(U) = \{2-b\}$. [$U$ התחילה בצבע הפוך לזה שסיימה בו $S$]
3. $f_i(S \setminus U) = \{b\}$, $f_{i+1}(S) = \{b\}$. [$v_i$ הוא שסיים את הפיכת $S$ לחד צבעית]
4. $f_i(U) = \{2-b\}$. [הוא עשה זאת בגלל $U$]

כל קבוצה ששייכת ל-$E_{1,b}(S)$ הייתה צריכה להחליף קודקוד כלשהו אחרון. קודקוד זה חייב להיות חלק מקבוצה חד-צבעית בצבע ההפוך, ולכן לא יכול להיות שהוא בחפיפה לקבוצה שלנו של יותר מקודקוד יחיד. הקבוצה דנן חייבת הייתה עדיין להיות בצבע ההפוך (אחרת לא היינו הופכים את הקודקוד). מסקנה – כל קבוצה ב-$E_{1,b}(S)$ חייבת להאשים קבוצה כלשהי.

נניח כי $S \cap U = v_i$ הוא הקודקוד ה-$\alpha$ בקשת $S$ וה-$\beta$ בקשת $U$ ונחשב

$$\mathbb{P}(\mathrm{E}_{\mathrm{U}\to b}(\mathrm{S}) \mid \sigma) \leq \underbrace{p}_{\text{התחלף } v_i} \quad \underbrace{2^{-n}}_{\substack{\text{הקשת האשמה} \\ \text{התחילה בצבע נתון}}} \quad \underbrace{(1-p)^{\beta}}_{\substack{\text{כל קודמיו ב-U} \\ \text{לא התחלפו}}} \underbrace{2^{-n+1+i}}_{\substack{\text{כל עוקביו ב-S} \\ \text{התחילו בצבע b}}} \underbrace{\left(\frac{1+p}{2}\right)^{i}}_{\substack{\text{כל קודמיו התחילו} \\ \text{הפוכים או התחלפו}}}$$

נשכתב וניקח תוחלת כדי לקבל

$$\mathbb{P}(\mathrm{E}_{\mathrm{U}\to b}(\mathrm{S})\ ) \leq 2^{1-2n} p \mathbb{E}\left[(1+p)^i (1-p)^j\right]$$

**טענת עזר.** בסידור מקרי מתקיים $\mathbb{E}\left[(1+p)^i (1-p)^j\right] \leq 1$.

נדחה את הוכחת טענת העזר לסוף ההוכחה כיוון שהיא יפה מכדי לעבור עליה בחטף.

על סמך טענה זו קיבלנו כי

$$\mathbb{P}(\mathrm{E}_{\mathrm{U}\to b}(\mathrm{S})\ ) \leq 2^{1-2n} p$$

נשתמש בכך ונחשב

$$\mathbb{P}\left(E_{0,b}\right) = (2^{n-1}k) 2^{-n} (1-p)^n = \frac{k(1-p)^n}{2}.$$

$$\mathbb{P}\left(E_{1,b}(S)\right) = \sum_{U,S} \mathbb{P}(\mathrm{E}_{\mathrm{U}\to b}(\mathrm{S})\ ) \leq (2^{n-1}k)^2 2^{1-2n} p \leq \frac{pk^2}{2}$$

קיבלתנו כי

$$\mathbb{P}\left(E_{1,1}(S)\right) + \mathbb{P}\left(E_{1,2}(S)\right) + \mathbb{P}\left(E_{0,1}(S)\right) + \mathbb{P}\left(E_{0,2}(S)\right) \leq k(1-p)^n + k^2 p < 1,$$

ולכן חייבת להיות סיכוי שלא ניכשל וכל הקשתות לא תהיינה חד-צבעיות.■

להשלמת ההוכחה נוכיח את טענת העזר.

נקבע זיווג $P = (u_1, s_1), \dots, (u_{k-1}, s_{k-1})$ בין אברי $U$ לאביר $S$, להוציא את האיבר היחיד $S \cap U$ $v \in U \cap S$. נסמן $X_i$ משתנה מקרי שסופר כמה מבין $\{u_i, s_i\}$ קודמים ל-$v$. ונראה כי

$$\mathbb{E}\left[(1+p)^i (1-p)^j \mid X_1 = x_1 \dots X_{k-1} = x_{k-1}\right] \leq 1$$

לצורך כך נשים לב שאם $\mathrm{X}_i = 0$ הוא אינו תורם ולכן תרומתו למכפלה היא 1, אם $\mathrm{X}_i = 2$ הוא תורם $(1+p)(1-p)$ ותרומתו קטנה מ-1. אחרת בסיכוי חצי הוא תורם $(1+p)$ ובסיכוי חצי $(1-p)$, ושניהם באופן בלתי תלוי בכל יתר האיברים (כי מדובר בחילוף בדיוק בין שני איברים ולכן יש התאמה חד-חד-ערכית ועל בין כל תמורה שבה יופיע איבר $U$

ראשון לזו שבה יופיע האיבר מ-$S$), ולכן תרומתו הממוצעת היא 1. כיוון שכל הגורמים חסומים מלמעלה ב-1, קיבלנו את המבוקש. ■

**תרגיל 6.** להוכיח כי $\mathrm{R}(4,K) > C\left(\frac{k}{\log k}\right)^2$.

**תרגיל 7.** להוכיח כי כל אוסף של לפחות $n/3$ תת-קבוצות בגודל 3 של $[n]$ מכיל קבוצה בלתי-תלויה (קבוצת קודקודים שאף שניים מהם אינם שכנים) בגודל $\frac{2n^{\frac{3}{2}}}{3\sqrt{3}\sqrt{m}}$.

# פרק 3 - שיטת המומנט השני

עוד במבוא להסתברות ראינו את כוחה של השונות בהוכחת ריכוז סביב התוחלת, בנימוק דומה נוכל להשתמש כדי להראות אסימפטוטיקה של בעיות ספירה דטרמיניסטיות.

נפתח בדוגמא מתורת הגרפים, שהנן מקריות במהותן; כלומר עוסקות בתכונות של גרף מקרי.

נזכיר כי $G(n,p)$ הוא גרף מקרי על $n$ קודקודים שבו כל קשת מופיעה באופן בלתי-תלוי בהסתברות $p$. תכונה נקראת מונוטונית אם קיומה בתת-גרף מבטיח את קיומה בגרף כולו. נאמר כי $r(n)$ היא פונקציית סף של תכונה אם עבור כל $p = o\big(r(n)\big)$ ההסתברות לקיום התכונה דועכת ל-0 ואילו עבור $p = \omega\big(r(n)\big)$ היא נוסקת ל-1. תופעה זו התגלתה בהשראת תופעות דומות בפיסיקה של החומר (למשל שינוי מצבי צבירה) והיא בעלת חשיבות יישומית ותיאורטית רבה.

נסתכל בתור התחלה על תכונה פשוטה. נסמן $w(g) = \max\{m: K_m \subset G(n,p)\}$.

**טענה 9.** $w(G) \geq 4$ היא תכונה בעלת פונקציית סף $n^{-2/3}$.

**הוכחה.** נסמן $G_4 = \{S \subset V, |S| = 4\}$ ונגדיר $X_S = \mathbb{1}(\forall u \neq v \in S: (u,v) \in E)$. כעת $\mathbb{P}(X_S = 1) = p^6$. נסמן $X = \sum_{S \in G_4} X_S$. תוחלתו של $X$ הנה:

$$\mathbb{E}(X) = \binom{\mathrm{n}}{4} p^6 \approx \frac{n^4 p^6}{24}$$

עבור $p = o\big(n^{-2/3}\big)$ תוחלת זו קורסת ל-0, ולפי שיטת המומנט הראשון ההסתברות לקיום התכונה אף היא דועכת.

עבור $p = \omega\big(n^{-2/3}\big)$ התוחלת עולה ל-$\infty$, אך לא די בכך כדי להוכיח שבהסתברות גבוהה $X \geq 1$, לשם כך נחשב את שונותו של $X$ לפי נוסחת השונות השלמה.

$$\begin{aligned}\mathrm{var}(X) = \mathbb{E}((X - \mathbb{E}(X))^2) &= \sum_{S,U \in G_4} \mathbb{E}\big((X_S - \mathbb{E}(X_s))(X_U - \mathbb{E}(X_U))\big) \\ &= \sum_{S \in G_4} \mathbb{P}(X_S = 1) \sum_{U \sim S} \mathbb{E}(X_U | X_S = 1)\end{aligned}$$

כאשר $U \sim S$ אם יש להן קשת משותפת.

משיקולי סימטריה $\sum_{U \sim S} \mathbb{E}(X_U | X_S = 1)$ אינו תלוי ב-$S$. ולכן

$$\mathrm{var}(X) = \sum_{U \sim \{1,2,3,4\}} \mathbb{E}(X_U | X_S = 1) \sum_{S \in G_4} \mathbb{P}(X_S = 1) = \sum_{U \sim \{1,2,3,4\}} \mathbb{E}(X_U | X_S = 1)\, \mathbb{E}(\mathrm{X})$$

שני גרפים של 4 קודקודים החולקים קשת יכולים לחלוק 2 או 3 או 4 קודקודים.

במקרה הראשון מדובר ב-$\Theta(n^2)$ גרפים בשני ב-$\Theta(n)$ ובאחרון בגרף יחיד. בכל מקרה אלו סדרי גודל נמוכים יותר מאשר $n^3$ ולכן $\mathrm{var}(X) = o\big(\mathbb{E}(\mathrm{X})\big)$. המסקנה מאי-שוויון צ'בישב היא כי

$$\mathbb{P}\big(X - \mathbb{E}(X) > \epsilon \mathbb{E}(X)\big) \leq \frac{\mathrm{var}(X)}{\epsilon^2 \mathbb{E}(X)^2} = \frac{o(1)}{\epsilon^2}$$

ומכך נובעת הטענה.■

שיטה זו ניתנת להפעלה בכל מקרה בו אנו מעוניינים להראות שכמות אובייקטים במרחב מקרי מרוכזת סביב תוחלתה. ולמעשה גם עבור תת-גרפים מושרים ולא רק עבור תת-גרפים מוכלים (כלומר גם כאשר היעדר קשתות צריך להתאים לגרף שנבחר ולא רק קיומן).

**תרגיל 8.** להראות שלכל גרף $H=(V,E)$ שצפיפות הקשתות שלו ביחס לקודקודים $\frac{|V|}{|E|}$ גדולה או שווה לזו של כל תת-גרף שלו. יש להראות כי $H\subset G(n,p)$ היא תכונה בעלת פונקציית סף $n^{-|V|/|E|}$.

נסיים את הפרק בדוגמא לשימוש קומבינטורי באמת של שיטת המומנט השני.

**דוגמא 7.** נזכיר כי טורניר הנו גרף מכוון שבו נבחר בדיוק אחד הכיוונים של כל קשת. מסלול המילטון בטורניר $G=(V,E)$ בן $n$ קודקודים הוא מסלול שמתחיל מקודקוד מסוים ומסיים בו, שכל קשתותיו נמצאות בגרף. כלומר $\sigma\in S_n$ כך שמתקיים $\left(\sigma(\mathrm{i}),\sigma(\mathrm{i}+1)\right)\in \mathrm{E}$ לכל $i\in[n-1]$.

נסמן ב-$P(n)$ את מספר מסלולי המילטון המירבי בגרף בן $n$ קודקודים. אנו מעוניינים להעריך מהו מספר זה.

טיבור סזלה הראה ב-1943 את החסם הבא שנובע משיטת המומנט הראשון.

**טענה 10.** $P(n)\geq n!\,/2^{n-1}$.

לצורך הטענה נזדקק לכמה טענות עזר שהוכחתן תובא בסוף.

**טענת עזר א' – משפט ברגמן.** הפרמננטה של מטריצה [אחותה של הדטרמיננטה בלי סימן התמורה], הלא היא

$$\mathrm{per}(R_{n\times n})=\sum_{\sigma\in S_n}\prod_{i\in[n]}R_{i,\sigma_i}$$

עבור מטריצה של אפסים ואחדות, מקיימת:

$$\mathrm{per}(R_{n\times n})\leq\prod_{1\leq i\leq n}(r_i!)^{1/r_i}$$

כאשר $r_i=\sum_{j\in[n]}r_{i,j}$.

**טענת עזר ב' –** $\prod_{1\leq i\leq n}(r_i!)^{1/r_i}$ תחת האילוץ $\sum_{i\in n}r_i=s$ כאשר $r_i$ שלמים חיוביים, מירבית כאשר $r_i\in\left\{\left\lfloor\frac{s}{n}\right\rfloor,\left\lceil\frac{s}{n}\right\rceil\right\}$.

**הוכחת טענה 10.** נחשב את ההסתברות בטורניר מקרי שמסלול מסוים יהיה מסלול המילטון. זו כמובן $2^{-n+1}$ מכיוון שכל קשת עשויה להיות בכיוון המסלול בהסתברות חצי. ישנם $n!$ מסלולים כאלה ולכן חסם הטענה הוא בעצם תוחלת מספר המסלולים.

סזלה גם הוכיח כי מתקיים:

$$\frac{1}{2}\leq\lim_{n\to\infty}\sqrt[n]{\frac{P(n)}{n!}}\leq\frac{1}{2^{3/4}},$$

ושיער שהגבול קיים ושווה לחצי.

עובדה זו ואף טענה חזקה יותר הוכחה על ידי נגה אלון ב-1990 ואנחנו נסיים את הפרק בה.

**טענה 11.** קיים $c$ כך שמתקיים לכל $n$:

$$P(n)\leq cn^{3/2}\frac{n!}{2^{n-1}},$$

**הוכחה.** נסמן עבור טורניר G ב-$P(G)$ את מספר מסלולי המילטון בטורניר וב-$C(G)$ את מספר מעגלי המילטון, כלומר שמקיימים בנוסף $\left(\sigma(n),\sigma(1)\right)\in E$. בנוסף נסמן ב-$F(G)$ את מספר התת-גרפים הפורשים שבהם דרגתו הנכנסת ודרגתו היוצאת של כל קודקוד היא 1 (כלומר אוסף מעגלים מכוונים). כמובן שמתקיים $P(G)\leq C(G)\leq F(G)$.

נרשום $A_G$ עבור מטריצת השכנויות של G כאשר הכניסה $A_G(i,j)$ מציינת את קיום הקשת $(i,j)\in E$. נסמן את מספר ה-1-ים בשורה ה-$i$ ב-$r_i$ ונקבל

$$\sum_{i=1}^{n} r_i = \binom{n}{2}$$

נקבל כי $F(G) = \mathrm{Per}(A_G)$ כלומר הפרמננטה של $A_G$. אם בגרף יש קודקוד שדרגת היציאה שלו היא 0, כמובן שמספר מעגלי המילטון הוא 0. אחרת, לפי טענת עזר א' (משפט ברגמן) בשילוב עם טענת עזר ב' מתקיים כי $F(G)$ חסומה על ידי $\prod_{1\le i\le n}(r_i!)^{1/r_i}$ כאשר $r_i \in \left\{\left\lfloor \frac{s}{n} \right\rfloor, \left\lceil \frac{s}{n} \right\rceil\right\}$, עבור $s = \binom{n}{2}$ כל שנותר הוא לחסום את גודלה של הפונקציה הזו. על ידי שימוש בנוסחת סטרלינג לפיה

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n (1 + o(1))$$

נקבל

$$\begin{aligned}\prod_{1\le i\le n}(r_i!)^{1/r_i} &\le \big(1+o(1)\big)\cdot\prod_{1\le i\le n}\left(\sqrt{2\pi}\frac{s}{n}\left(\frac{s}{ne}\right)^{\frac{s}{n}}\right)^{\frac{n}{s}} = \big(1+o(1)\big)\sqrt{2\pi}\left(\frac{s}{ne}\right)^n\left(\sqrt{2\pi}\frac{s}{n}\right)^{\frac{n^2}{s}} \\ &= \big(1+o(1)\big)\left(\frac{n-1}{2e}\right)^n\left(\sqrt{2\pi}\frac{n-1}{2}\right)^{\frac{2n}{n-1}} = \big(1+o(1)\big)\frac{(n-1)^n}{2^n e^n}\frac{(n-1)^2}{4}2\pi \\ &= \big(1+o(1)\big)\frac{\sqrt{\pi}}{e\sqrt{2}}n^{\frac{3}{2}}\frac{(n-1)!}{2^n}\end{aligned}$$

כעת נשים לב כי אם נבחן טורניר G באורך $n$ ונוסיף לו קודקוד חדש ליצירת \`G ההסתברות שמסלול המילטון בטורניר המקורי יהפוך למעגל בטורניר החדש היא רבע. לכן

$$\frac{1}{4}P_G \le C_{G'}$$

וראינו כי

$$C_{G'} \le \big(1+o(1)\big)\frac{\sqrt{\pi}}{e\sqrt{2}}(n+1)^{\frac{3}{2}}\frac{n!}{2^{n+1}}$$

ולכן

$$P_G \le O\left(n^{\frac{3}{2}}\frac{n!}{2^{n-1}}\right)$$

כנדרש. ■

נסיים בהוכחת טענות העזר.

**הוכחת טענת עזר א'.**

**הוכחת טענת עזר ב'.**