

פתרונות לתרגיל הראשון

קו המשווה

אפשר לפתור את השאלה ע"י חישוב ישיר, אבל כאן נשתמש בתוצאת השאלה "התפלגויות מותנות" מחוברת התרגילים. הרעיון יהיה להגריל ערכים עבור זוג של משתנים מקריים שייצגו את שתי ההתפלגויות, תוך כדי שדואגים לכך שבהתפלגות המשותפת תהיה הסתברות גבוהה למאורע שהם שווים-ערך.

נגדיר מרחב הסתברות τ מעל $\{1, \dots, n\} \times \{1, \dots, n\}$ ומעליו נגדיר שני משתנים מקריים: X שיתפלג כמו μ ו- Y שיתפלג כמו ν , ומאורע מתאים F . נניח בלי הגבלת הכלליות שמתקיים $\Pr_\mu[E] \leq \Pr_\nu[E]$ (אחרת נחליף בין μ ל- ν).

• על מנת להגריל את (i, j) לפי τ : בהסתברות $\Pr_\mu[E]$ נגריל k לפי ההתפלגות של μ המותנה על E (שהיא זהה להתפלגות של ν המותנה על E), ונקבע $i = j = k$. בהסתברות $\Pr_\nu[E] - \Pr_\mu[E]$ (אם זה גדול מ-0) נגריל את i לפי ההתפלגות המותנה של μ על $\neg E$ (זה יהיה מוגדר כי במקרה הזה בפרט $\Pr_\mu[\neg E] > 0$) ובאופן ב"ת את j לפי ההתפלגות המותנה של ν על E . לבסוף, בהסתברות $1 - \Pr_\nu[E]$ (אם היא גדולה מ-0) נגריל את i לפי ההתפלגות המותנה של μ על $\neg E$ ובאופן ב"ת את j לפי ההתפלגות המותנה של ν על $\neg E$ (שתי ההתפלגויות המותנות יהיו מוגדרות במקרה זה).

• המ"מ מוגדרים לפי $X(i, j) = i$ ו- $Y(i, j) = j$.

• המאורע F הוא פשוט זה שמתקיים $i = j$.

נראה עתה שמתקיימים התנאים המבוקשים להפעלת תוצאת השאלה "התפלגויות מותנות".

• לכל $1 \leq i \leq n$ מתקיים

$$\begin{aligned}\Pr_\tau[X = i] &= \Pr_\mu[E]\Pr_\mu[i|E] + (\Pr_\nu[E] - \Pr_\mu[E])\Pr_\mu[i|\neg E] + (1 - \Pr_\nu[E])\Pr_\mu[i|\neg E] \\ &= \Pr_\mu[E]\Pr_\mu[i|E] + \Pr_\mu[\neg E]\Pr_\mu[i|\neg E] = \Pr_\mu[i]\end{aligned}$$

• לכל $1 \leq j \leq n$ מתקיים

$$\begin{aligned}\Pr_\tau[Y = j] &= \Pr_\mu[E]\Pr_\nu[j|E] + (\Pr_\nu[E] - \Pr_\mu[E])\Pr_\nu[j|E] + (1 - \Pr_\nu[E])\Pr_\nu[j|\neg E] \\ &= \Pr_\nu[E]\Pr_\nu[j|E] + \Pr_\nu[\neg E]\Pr_\nu[j|\neg E] = \Pr_\nu[j]\end{aligned}$$

• נובע ישירות מההגדרה שמתקיים $\Pr[X = Y|F] = 1$.

• מתקיים $\Pr_\tau[F] \geq \Pr_\mu[E]$ כי לפי ההגדרה של τ , בהסתברות $\Pr_\mu[E]$ אנחנו במפורש בחרנו ערך k ואז קבענו $i = j = k$. על כן $\Pr_\tau[\neg F] \leq \max\{\Pr_\mu[\neg E], \Pr_\nu[\neg E]\}$.

הערה: נסו לראות מתי מתקבל $d(\mu, \nu) < \max\{\Pr_\mu[\neg E], \Pr_\nu[\neg E]\}$. אפשר למצוא תנאי הכרחי ומספיק.

פגיעות במרחב

אם A אינה פורשת את כל המרחב הלינארי $V = (\mathbb{Z}_2)^n$, אז תתי-מרחב הנפרש $\text{Span}(A)$ הוא ממימד $n-1$ לכל היותר. נסמן ב- \mathcal{B} את משפחת כל המשלימים של תתי-מרחב $U \subset V$ ממימד $n-1$ בדיוק, $\mathcal{B} = \{V \setminus U : \dim(U) = n-1\}$. אם מתקיים $\text{Span}(A) \neq V$ אז קיים $B \in \mathcal{B}$ שעבורו $\text{Span}(A) \cap B = \emptyset$ ולכן גם $A \cap B = \emptyset$ (יכול להיות יותר מ- B אחד כזה, אם $\dim(\text{Span}(A)) \leq n-2$).

ענה נספור את $|\mathcal{B}|$. כל תתי-מרחב $U \subset V$ ממימד $n-1$ יכול להיות מוגדר לפי וקטור $v \in V$ כך שלכל $u \in U$ מתקיים $u \cdot v = \sum_{i=1}^n u_i v_i = 0$ (זכרו שהסכום הוא מעל \mathbb{Z}_2). למציאת v לוקחים בסיס של U , ומקבלים מערכת הומוגנית ולא מנוונת של $n-1$ משוואות לינאריות ב- n משתנים. הפתרון עבור v הוא יחיד עד כדי כפל בסקלר שונה מ- 0 , רק שב- \mathbb{Z}_2 אין איבר שונה מ- 0 למעט 1 , כך ש- v הוא יחיד. אם נשים לב לכך שההעתקה מ- U ל- v היא הפיכה (בהינתן v אפשר "לשחזר" את $U = \{y \in V : u \cdot v = 0\}$), נקבל שמתקיים $|\mathcal{B}| = |V \setminus \{0\}| = 2^n - 1$ (יש עוד שיטות למציאת $|\mathcal{B}|$). נשים לב גם שמתקיים $|\mathcal{B}| = 2^n - 2^{n-1} = 2^{n-1}$. לכל $B \in \mathcal{B}$ (הגודל של מרחב ממימד k מעל \mathbb{Z}_2 הוא בדיוק 2^k).

עבור קבוצה $B \in \mathcal{B}$ בודדת, הסיכוי ש- A אינה מכילה איבר מ- B (לפי מרחב ההסתברות שלנו) הוא $(1 - 2n/2^n)^{|B|} = (1 - 2n/2^n)^{2^{n-1}} < e^{-n} = o(2^{-n})$. על כן, לפי איחוד מאורעות, ההסתברות שיש קבוצה $B \in \mathcal{B}$ שעבורה מתקיים $A \cap B = \emptyset$ היא $o(1)$, וז"א שבהסתברות $1 - o(1)$ אין קבוצה כזו ואז מתקיים $\text{Span}(A) = V$.

קליקים באקראי

נסמן ב- $V = \{1, \dots, n\}$ את קבוצת הצמתים של הגרף המקרי שלנו. עבור קבוצה $A \subset V$ מגודל $k < n/2$ (אח"כ נטיל הגבלות יותר חזקות על k), נבדוק את ההסתברות שלא קיים צומת $v \in V \setminus A$ שמחובר לכל צמתי A . עבור צומת ספציפי, הסיכוי שיהיה מחובר לכל צמתי A הוא בדיוק α^k . על כן (לפי מאורעות בלתי-תלויים והעובדה שיש לפחות $n/2$ צמתים שאינם ב- A) הסיכוי שלא קיים צומת כזה חסום ע"י $(1 - \alpha^k)^{n/2} < e^{-n\alpha^k/2}$. אם $k < \log(n)/2 \log(1/\alpha)$ אז מתקיים $e^{-n\alpha^k/2} < e^{-\sqrt{n}/2}$.

נבחר אם כן $C = 1/2 \log(1/\alpha)$. מספר הקבוצות מגודל $C \log(n)$ או פחות חסום (באופן גס) ע"י $C \log(n) \cdot n^{C \log(n)} = o(e^{\sqrt{n}/2})$. על כן, לפי איחוד מאורעות, בהסתברות $1 - o(1)$ מתקיים שלכל קבוצה A עם פחות מ- $C \log(n)$ צמתים קיים צומת $v \in V \setminus A$ שמחובר לכל צמתי A .

כאשר המאורע הזה קורה, קיים בגרף קליק כנדרש: על מנת למצוא אותו מתחילים מקבוצה K שמכילה צומת בודד שרירותי, ובכל שלב מוסיפים לה צומת חדש אשר מחובר לכל הצמתים שכבר נמצאים בקבוצה. התהליך יכול להעצר רק כאשר כבר קיימים ב- K לפחות $C \log(n)$ צמתים, ואז זהו הקליק המבוקש.

פתרונות לתרגיל השני

נצחון יצוגי

ראשית נראה (בלי קשר לתנאי על דרגות מינימליות) שלכל k , מספר הצמתים עם דרגת יציאה k או פחות אינו עולה על $2k + 1$. נניח בשלילה שזהו אינו המצב, וניקח את התחרות המושרה על $2k + 2$ הצמתים עם הדרגה הנמוכה ביותר. נסמן את התחרות הזו ב- $T' = (V', E')$ כאשר E' היא הקבוצה $\{uv \in E : u, v \in V'\}$. דרגת היציאה בתוך T' עדיין חסומה ע"י k , אבל מצד שני מתקיים $\sum_{v \in V'} d_{T'}^{\rightarrow}(v) = \binom{2k+2}{2} > k(2k+2)$ (כל זוג uv נספר או כקשת יציאה של u או כקשת יציאה של v), שזו סתירה.

אם עתה נסדר את $V = \{v_1, \dots, v_n\}$ כך שמתקיים $d_T^{\rightarrow}(v_1) \leq \dots \leq d_T^{\rightarrow}(v_n)$, נובע מהדיון למעלה שלכל $1 \leq i \leq n$ מתקיים $d_T^{\rightarrow}(v_i) \geq \lceil \frac{i-1}{2} \rceil$. כמו כן נתון לנו שבפרט עבור $1 \leq i \leq 21$ מתקיים $d_T^{\rightarrow}(v_i) \geq 10$.

נגריל עתה את הצביעה $c : V \rightarrow \{1, 2\}$ באופן מקרי ויוניפורמי, ונראה שבהסתברות חיובית לכל צומת יש קשתות יוצאות לשכנים משני הצבעים. נסמן ב- A_i את המאורע של- v_i אין קשתות לצמתים משני הצבעים, ונקבל $\Pr[A_i] = 2^{1-d_T^{\rightarrow}(v_i)}$. לפי איחוד מאורעות, הסיכוי שמתקיים מאורע כל שהוא מתוך A_1, \dots, A_n חסום ע"י $1 < 2 \cdot 2^{1-k} + \sum_{k=11}^{\lfloor n/2 \rfloor} 2 \cdot 2^{1-k} \leq 21 \cdot 2^{-9} + \sum_{k=11}^{\lfloor n/2 \rfloor} 2 \cdot 2^{1-k} < 1$, ז"א שבסיכוי חיובי אף אחד מהמאורעות הרעים לא מתקיים.

ממוצע מקוצר של פולינום

עבור וקטור של מספרים אי-שליליים שלמים $I = (i_1, \dots, i_n)$ נסמן $|I| = \sum_{j=1}^n i_j$, ונסמן ב- x^I את המכפלה $\prod_{j=1}^n x_j^{i_j}$. אם מסמנים $\mathcal{I}_d = \{I : |I| \leq d\}$, אז כל פולינום בעל n משתנים מדרגה חסומה ע"י d ניתן לכתובה מהצורה $\sum_{I \in \mathcal{I}_d} \alpha_I x^I$, עבור מקדמים מתאימים $\alpha_I \in \mathbb{R}$. לפי לינאריות התוחלת, לכל מרחב הסתברות τ מעל $\{0, \dots, k-1\}^n$ (או מעל \mathbb{R}^n) מתקיים $E_\tau[p(X_1, \dots, X_n)] = \sum_{I \in \mathcal{I}_d} \alpha_I E_\tau[X^I]$.

על מנת להשלים את ההוכחה, נשים לב שעבור ההתפלגות μ וההתפלגות ν המקיימות את תנאי השאלה, לכל $I \in \mathcal{I}_d$ יתקיים $E_\mu[X^I] = E_\nu[X^I]$. $E_\mu[X^I] = \prod_{j=1}^n E_\mu[x_j^{i_j}] = \prod_{j=1}^n (\frac{1}{k} \sum_{l=0}^{k-1} l^{i_j}) = \prod_{j=1}^n E_\nu[x_j^{i_j}] = E_\nu[X^I]$ (כולל אי-התלות של כל קבוצה בת d משתנים או פחות). אם מציבים את השוויון $E_\mu[X^I] = E_\nu[X^I]$ בנוסחת התוחלת של $p(X_1, \dots, X_n)$, מקבלים $E_\mu[p(X_1, \dots, X_n)] = E_\nu[p(X_1, \dots, X_n)]$ כנדרש.

זיווגים מתחמקים

האלגוריתם שנבנה יהיה דומה לאלגוריתם מהחוכרת עבור זיווגים מושלמים, עם ההבדלים הבאים:

- המשקלות w_{ij} עבור $ij \in E$ יוגרלו בדיוק כמו באלגוריתם הזיווג המקורי.
- עבור $ij \notin E$ ועבור $ij \in E \setminus F$, נגדיר את a_{ij} בדיוק כמו באלגוריתם המקורי.
- עבור $ij \in F$, נגדיר $a_{ij} = 2^{w_{ij}+n^3}$ אם $i < j$ ונגדיר $a_{ij} = -2^{w_{ij}+n^3}$ אם $i > j$.
- עבור הפלט, אם $\det A = 0$ האלגוריתם יפלוט "אין זיווג". אחרת, האלגוריתם יחשב את המספר המקסימלי k כך ש- 2^k מחלק את $\det A$, ויפלוט את $\lfloor k/2n^3 \rfloor$.

עבור המשך הניתוח, לכל זיווג מושלם M נסמן ב- $r(M)$ את מספר הקשתות האדומות (מ- F) שהוא מכיל. נסמן ב- r את מספר הקשתות האדומות המינימלי בכל זיווג מושלם כל שהוא, וב- \mathcal{F} את משפחת הזיווגים המושלמים שעבורם $r(M) = r$. נפעיל את למת הבידוד עבור \mathcal{F} (לא משפחת כל הזיווגים המושלמים), ונקבל שבהסתברות לפחות $\frac{1}{2}$ קיים זיווג מושלם יחידי $M_0 \in \mathcal{F}$ שעבורו $w(M_0)$ הוא מינימלי (זה בהנחה שקיימים בכלל זיווגים מושלמים - אחרת תמיד יתקיים $\det A = 0$ בדומה להוכחה המקורית מהשיעור).

מעשה נתמקד במקרה שבו יש זיווגים מושלמים בגרף, ובתוכם יש זיווג מושלם M_0 יחיד עם משקל מינמלי, מבין כל הזיווגים המושלמים שלהם מספר קשתות אדומות מינימלי. להשלמת ההוכחה (בדומה להוכחה המקורית עבור זיווגים מושלמים), צריך להראות שבמקרה זה הדטרמיננטה $\det A = \sum_{\sigma \in S_n} (-1)^{\text{sgn}(\sigma)} \prod_{i=1}^n a_{i\sigma(i)}$ אינה מתאפסת ואף אינה מתחלקת ב- $2^{2(r+1)n^3}$, וכמו כן צריך להראות שבכל מקרה (גם כאשר לא קיים M_0 יחיד כמתואר) הדטרמיננטה תתחלק ב- 2^{2rn^3} . הניתוח של איברי הסכום נעשה באופן הבא:

עבור פרמוטציות שמכילות עגילים מגודל אי-זוגי, יהיה קיזוז הדדי בדיוק כמו בהוכחה המקורית. עבור פרמוטציה σ שניתנת לפירוק לזיווגים מושלמים M_1 ו- M_2 (כזכור כל פרמוטציה ללא עגילים אי-זוגיים ניתנת לפירוק מסוג זה), יתקיים $|\prod_i a_{i\sigma(i)}| = 2^{w(M_1)+w(M_2)+(r(M_1)+r(M_2))n^3}$. בפרט אם σ_0 היא הפרמוטציה המתארת מעבר הלוך ושוב על קשתות M_0 , אז מתקיים $|\prod_i a_{i\sigma_0(i)}| = 2^{2w(M_0)+2rn^3}$.

אם מתקיים $M_1 \notin \mathcal{F}$ או $M_2 \notin \mathcal{F}$, אז מכיוון שלכל זיווג M מתקיים $n^3/2 \leq w(M) \leq n^3/2$, יתקיים $w(M_1) + w(M_2) + (r(M_1) + r(M_2))n^3 \geq w(M_1) + w(M_2) + (2r + 1)n^3 > 2w(M_0) + 2rn^3$ ולכן $|\prod_i a_{i\sigma(i)}|$ יתחלק ב- $2^{2w(M_0)+2rn^3+1}$. אם מתקיים $M_1, M_2 \in \mathcal{F}$ אבל לא שניהם זהים ל- M_0 , אז בדומה להוכחה בחוברת גם כאן נקבל ש- $|\prod_i a_{i\sigma(i)}|$ יתחלק ב- $2^{2w(M_0)+2rn^3+1}$. בזאת כיסינו את כל המקרים עבור כל הפרמוטציות השונות מ- σ_0 , ולכן בסכום של $\det A$ יהיה איבר יחיד שאינו מתחלק ב- $2^{2w(M_0)+2rn^3+1}$, ז"א שהדטרמיננטה (הסכום הכולל) בפרט אינה מתאפסת ואינה מתחלקת ב- $2^{2w(M_0)+2rn^3+1}$. מכיוון שמתקיים $n/2 \leq w(M_0) \leq n^3/2$, נובע מכך שהדטרמיננטה אינה מתחלקת ב- $2^{2(r+1)n^3}$.

מצד שני, כל האיברים בסכום שמגדיר את הדטרמיננטה, גם במקרה שלא קיים M_0 יחיד כמתואר (כאשר יכולים להיות זיווגים אחרים עם r קשתות אדומות שמשגיגים את מינימום המשקל), תמיד יתחלקו ב- $2^{2w(M_0)+2rn^3}$, ובפרט יתחלקו ב- 2^{2rn^3} . מאלו נובע שהערך k שהאלגוריתם מחשב (במקרה שלא פולט "אין זיווג") יקיים $2rn^3 \leq k < 2(r+1)n^3$ כאשר M_0 הוא יחיד, ובכל מקרה יתקיים $2rn^3 \leq k$. מכך נובע ש- $\lfloor k/2n^3 \rfloor$ יהיה זהה ל- r כאשר M_0 יחיד (דבר הקורה בהסתברות $\frac{1}{2}$ לפחות), ובכל מקרה לא יהיה קטן מ- r .

פתרונות לתרגיל השלישי

כולם שונים

נגריל את $d \in \mathbb{Z}_p \setminus \{0\}$ באופן מקרי ויוניפורמי, ולכל זוג איברים $a \neq b$ בשדה \mathbb{Z}_p נגדיר את המאורע B_{ab} כמאורע שמתקיים $f(da) = f(db)$. על מנת לקבל את תוצאת השאלה, נראה שלכל $a \neq b$ מתקיים $\Pr[B_{ab}] < 1/\binom{m}{2}$, ואז ניתן לסיים באמצעות איחוד מאורעות: בסיכוי חיובי לא יתקיים אף מאורע מהצורה B_{ab} עבור $a, b \in A$.

עבור החסם, נסתכל על $|\hat{da} - \hat{db}|$. מכיוון ש- f מוגדר ע"י השארית בחלוקה ל- n , מתקיים $f(da) = f(db)$ אם ורק אם $|\hat{da} - \hat{db}|$ מתחלק ב- n . יש שתי אפשרויות. אם $\hat{da} > \hat{db}$, אז מכיוון שמתקיים $0 < \hat{da} - \hat{db} < p$, מתקיים $|\hat{da} - \hat{db}| = \widehat{da - db} = d(a - b)$. על כן (לפי הקריטריון של חלוקה ל- n) יתקיים במקרה הזה $f(da) = f(db)$ אם ורק אם $f(d(a - b)) = 0$. באופן דומה, אם $\hat{da} < \hat{db}$, אז יתקיים במקרה הזה $f(da) = f(db)$ אם ורק אם $f(d(b - a)) = 0$.

משני אלו נובע שמתקיים $\Pr[B_{ab}] \leq \Pr[f(d(a - b)) = 0] + \Pr[f(d(b - a)) = 0]$ עבור $c \in \mathbb{Z}_p \setminus \{0\}$. קבוע, הערך dc מתפלג יוניפורמית מעל $\mathbb{Z}_p \setminus \{0\}$ (מכיוון שהמדובר בשדה - כאן השתמשנו בנתון ש- p הוא ראשוני). על כן מתקיים $\Pr[f(dc) = 0] \leq 1/n < 1/2 \binom{m}{2}$ יש $\frac{p-1}{n} \leq \frac{p-1}{n} < 1/2 \binom{m}{2}$ (מכיוון שבין איברי $\mathbb{Z}_p \setminus \{0\}$ יש $\frac{p-1}{n}$ כנדרש. איברים שמאפסים את f). בהצבת שתי האפשרויות $c = a - b$ ו- $c = b - a$ נקבל $\Pr[B_{ab}] < 1/\binom{m}{2}$ כנדרש.

פרישה נרחבת

אם מוכיחים עבור $x, y \in \mathbb{Z}_p$ ש- $x \cdot A + y$ חותך כל קטע מהצורה $I_{r,l}$ עבור $l \geq cp/\sqrt{k}$, אז הדבר יהיה נכון גם עבור $x \cdot A$, מכיוון שמתקיים $(x \cdot A) \cap I_{r,l} = \emptyset$ אם ורק אם $(x \cdot A + y) \cap I_{r+l,y} = \emptyset$. עתה נגדיר את $x, y \in \mathbb{Z}_p$ באופן יוניפורמי וב"ת, ונראה שבהסתברות חיובית $x \cdot A + y$ תקיים את התכונה המבוקשת (בהגרלה אנחנו מרשים ל- x לקבל ערך 0 בשביל הניתוח ההסתברותי, בכל מקרה זה לא יהיה הערך שיקיים בסוף את תוצאת השאלה). את הערך של c נבחר בהמשך. כמו כן נניח ש- p גבוה מספיק (יספיק למשל להניח $p \geq 100$), כי אפשר יהיה (עם הגדלה אפשרית בערך של c) לוודא שתוצאת השאלה תהיה טריביאלית עבור p קטנים מדי.

עתה נסמן $m = \lfloor cp/2\sqrt{k} \rfloor$, ולכל $0 \leq i < \lfloor p/m \rfloor < 4\sqrt{k}/c$ נגדיר את $J_i = I_{i,m,m}$. אם $x \cdot A + y$ חותך את כל הקטעים $J_0, \dots, J_{\lfloor p/m \rfloor - 1}$ אז הוא יחתוך כל קטע $I_{r,l}$ לכל $0 \leq r < p$ ולכל $l \geq cp/\sqrt{k}$, פשוט כי מתקיים אז $J_{\lfloor r/m \rfloor} \subset I_{r,l}$.

נבחן עתה את ההסתברות ש- $x \cdot A + y$ אינו חותך את J_i עבור i קבוע כל שהוא. לכל $a \in A$ נגדיר את X_a להיות משתנה האינדיקטור עבור המאורע " $x \cdot a + y \in J_i$ ", וכן נגדיר את $X = \sum_{a \in A} X_a$. המאורע ש- $x \cdot A + y$ אינו חותך את J_i הוא בדיוק המאורע " $X = 0$ ". חישוב ישיר שמשמש בלינאריות התוחלת נותן לנו $E[X] = |A| \cdot m/p > \frac{1}{4}c\sqrt{k}$.

עבור חישוב המומנט השני, נראה שלכל $a \neq b$ מתקיים ש- X_a ו- X_b הם בלתי-תלויים. עבור $u, v \in \mathbb{Z}_p$ כל שהם (שווים או שונים), יש פתרון יחיד עבור x ו- y למערכת המשוואות $x \cdot a + y = u \wedge x \cdot b + y = v$, כי המדובר במערכת לא-מנוונת. על כן ההסתברות עבור המאורע " $x \cdot a + y \in J_i \wedge x \cdot b + y \in J_i$ " היא בדיוק m^2/p^2 , ו"א שהמאורעות (ולכן המשתנים המתאימים להם) הם ב"ת.

מזאת נובע שמתקיים $V[X] = \sum_{a \in A} V[X_a] < |A| \cdot m/p < \frac{1}{2}c\sqrt{k}$. משני אלו, לפי אי-שוויון צ'בישף, $\Pr[X = 0] \leq V[X]/(E[X])^2 < 8/c\sqrt{k}$. בחירה של $c = 6$ תוודא שמתקיים $(4\sqrt{k}/c) \cdot (8/c\sqrt{k}) < 1$ ובמקרה כזה לפי איחוד מאורעות יש סיכוי חיובי לכך שכל הקטעים $J_0, \dots, J_{\lfloor p/m \rfloor - 1}$ יחתכו ע"י $x \cdot A + y$. על כן בפרט יש בחירה ספציפית של x ו- y שתתן לנו את המבוקש.

קירוב להסתברות

אנחנו נשתמש בתוצאת סעיף ב של השאלה "קרבה בין התפלגויות" מחוברת התרגילים הפתורים. אנחנו נראה, עבור בחירה מתאימה של C , שבהסתברות $1 - o(1)$ לכל מאורע E יתקיים $|\Pr_\mu[E] - \Pr_\nu[E]| \leq \epsilon$, ומכאן נובע ש- $d(\mu, \nu) \leq \epsilon$ מכיוון שתמיד קיים מאורע E שעבורו ההפרש $|\Pr_\mu[E] - \Pr_\nu[E]|$ שווה בדיוק ל- $d(\mu, \nu)$.

נניח שאנחנו לוקחים את הדגימות i_1, \dots, i_q לפי המתואר בשאלה, ונחסום עבור מאורע E ספציפי את ההסתברות (ביחס לתהליך לקיחת הדגימות) שמתקיים $|\Pr_\mu[E] - \Pr_\nu[E]| \leq \epsilon$. כזכור, מאורע במרחב הסתברות מתואר ע"י תת-קבוצה של קבוצת הבסיס שלו, ובמקרה שלנו E הוא תת-קבוצה של $\{1, \dots, n\}$. לפי ההגדרה של ν , מתקיים $\Pr_\nu[E] = |\{1 \leq j \leq q : i_j \in E\}|/q$.

עבור התהליך של לקיחת הדגימות נגדיר מ"מ X_1, \dots, X_q כאשר X_j הוא האינדיקטור של המאורע " $i_j \in E$ ", ונגדיר את $X = \sum_{j=1}^q X_j$. בפרט מתקיים $\Pr_\nu[E] = X/q$. הדבר הבא לשים לב הוא ש- X_1, \dots, X_q הם ב"ת לחלוטין זה בזה, וכל X_j מקבל 1 בהסתברות $\Pr_\mu[E]$ בדיוק, כך שמתקיים $\Pr_\mu[E] = E[X]/q$.

עבור $q = Cn$, יתקיים $|\Pr_\mu[E] - \Pr_\nu[E]| > \epsilon$ אם ורק אם $X > E[X] + \epsilon Cn$ או $X < E[X] - \epsilon Cn$. לפי החסם על סטיות גדולות מההרצאה, ההסתברות לאיחוד שני המאורעות האלו חסומה ע"י $2 \exp(-2\epsilon^2 Cn)$. אם למשל נבחר $C = \lceil 1/\epsilon^2 \rceil$ אז הסתברות זו תהיה $o(2^{-n})$.

לבסוף, נשים לב שיש בדיוק 2^n אפשרויות עבור המאורע E (היינו יכולים לצמצם ל- 2^{n-1} אפשרויות אם היינו שמים לב לכך שאי השוויון מתקיים עבור E אם ורק אם הוא מתקיים עבור $\neg E$). על כן, לפי איחוד מאורעות, בהסתברות $1 - o(1)$ לא יהיה מאורע E שעבורו $|\Pr_\mu[E] - \Pr_\nu[E]| > \epsilon$, כפי שרצינו להוכיח.

פתרונות לתרגיל הרביעי

סוגריים מקולקלים

נסתכל על המחזרות המקרית כעל פונקציה $f : \{1, \dots, 2n\} \rightarrow \{0, 1\}$ (המספרים 0,1 מייצגים "פתח סוגריים" ו"סגור סוגריים"). נגדיר מרטינגל חשיפה איבר-איבר עבור f , לפי $\mathcal{D}_i = \{1, \dots, i\}$, עבור הפונקציה של מספר התיקונים שצריך לעשות על מנת לקבל ביטוי-סוגריים חוקי. נסמן את מרטינגל החשיפה ב- X_0, \dots, X_{2n} , כאשר כזכור X_0 הוא קבוע ששווה לתוחלת מספר התיקונים שצריך, ו- X_{2n} הוא מספר התיקונים שצריך לעשות במחזרות המוגרלת. הפונקציה הזו מקיימת את תנאי ליפשיץ (עם קבוע ליפשיץ 1), ולכן מאי-שוויון אזומה מתקיים $\Pr[X_{2n} > X_0 + \sqrt{n \log n}] < e^{-(\log n)/4} = o(1)$. מספיק אם כן לחסום את X_0 , עבור n גדול דיו, ע"י ערך מהצורה $\Omega(\sqrt{n \log n})$.

עתה ניזכר במספר קטלן $C_n = \frac{1}{n+1} \binom{2n}{n}$, אשר מתאר את מספר ביטויי הסוגריים החוקיים בעלי $2n$ אותיות. מתקיים $C_n = (1 - o(1)) 4^n / n^{3/2} \sqrt{\pi}$ (ניתן להוכיח את זה באמצעות קירוב סטירלינג), ולכן $\Pr[X_{2n} = 0] = \Omega(n^{-3/2})$. על כן עבור n גדול דיו חייב להתקיים $X_0 \leq 3\sqrt{n \log n}$, מכיוון שלפי אי-שוויון אזומה מתקיים בפרט $\Pr[X_{2n} < X_0 - 3\sqrt{n \log n}] < e^{-9(\log n)/4} = o(n^{-3/2})$. על כן ניתן לבחור $c = 4$ על מנת לקבל את טענת השאלה המבוקשת.

מיון לא ראוי

האלגוריתם הזה הוא בעצם הילוך מקרי על הגרף $G = (V, E)$ הבא: V הוא אוסף כל $n!$ הפרמוטציות האפשריות, ושתי פרמוטציות $\sigma, \tau \in V$ יהיו קשת בגרף אם ורק אם הן נבדלות בדיוק בחילוף בודד של שני ערכים. לשם קבלת אינטואיציה, שימו לב גם שהגרף הזה הוא בעל התכונה הבאה: לכל $\sigma \neq \tau$, יש אוטומורפיזם של הגרף שבפרט מחליף בין σ ו- τ . תקציר ההוכחה: ראשית מראים שהפונקציה $f(\nu) = \nu^{-1}$ היא אוטומורפיזם של הגרף, מכיוון שאם β מתקבלת מ- α ע"י החלפת α_i ו- α_j , אז β^{-1} מתקבלת מ- α^{-1} ע"י החלפת α_i^{-1} ו- α_j^{-1} . כמו כן לא קשה לראות שעבור פרמוטציה λ , הפונקציה $g_\lambda(\nu) = \lambda\nu$ היא גם אוטומורפיזם (הכפל אומר "בצע את λ אחרי ν "). על כן הפונקציה $h(\nu) = g_\sigma(f(g_{\tau^{-1}}(\nu))) = \sigma\nu^{-1}\tau$ היא אוטומורפיזם (כהרכבה של אוטומורפיזמים), וזו מחליפה בין σ ל- τ .

התכונה הזו של קיום האוטומורפיזמים (שנקראת "טרנזיטיביות בצמתים") מבטיחה שמתקיים $h_{\sigma\tau} = h_{\tau\sigma}$ ובפרט $h_{\sigma\tau} = \frac{1}{2}k_{\sigma\tau}$ (פתרון השאלה עובד גם ללא האבחנה הזו, אבל היא מסייעת להבנה).

סעיף ראשון: משתמשים בקשר לרשתות חשמליות, $k_{\sigma\tau} = 2mR_{\sigma\tau}$, כאשר m הוא מספר הקשתות בגרף ו- $R_{\sigma\tau}$ היא "ההתנגדות השקולה" בין שני הצמתים כשרואים את הגרף כרשת חשמלית. לכל הצמתים בגרף יש דרגה $\binom{n}{2}$ בדיוק, ולכן $m = \frac{1}{2} \binom{n}{2} n!$. בקשר להתנגדות, היא תמיד תהיה חסומה ע"י אורך המסלול הקצר ביותר על הגרף בין σ ו- τ , ואורך זה חסום ע"י $n-1$ (מוכיחים זאת באינדוקציה על מספר האינדקסים שעבורם $\sigma_i \neq \tau_i$ - בכל שלב מבצעים חילוף ב- σ בין הערך i לבין j שעבורו $\sigma_j = \tau_j \neq \tau_j$). סה"כ קיבלנו $k_{\sigma\tau} \leq (n-1) \binom{n}{2} n! = (n+O(1))n!$.

סעיף שני: הסיבה שמספיק להסתכל על σ שנבדל ממצב ממיון בחילוף בודד היא שכל הילוך מקרי על הגרף צריך ממילא לעבור (לפחות פעם אחת) דרך מצב כזה לפני שיגיע למצב הממוין. הסיבה שזמן ההגעה הממוצע זהה לכל σ כזה היא שעבור כל σ שמתקבל ע"י החלפת (a, b) ו- τ שמתקבל ע"י החלפת (c, d) יש איזומורפיזם של הגרף שגם שומר על המיקום של $(1, \dots, n)$ וגם מעביר את σ ל- τ . האיזומורפיזם מתבצע ע"י כתיבת כל פרמוטציה כאוסף עגילים זרים, ואז החלפת התפקידים של a ו- c ושל b ו- d (אם מתקיים $|\{a, b\} \cap \{c, d\}| = 1$, אז דואגים לכתוב את שני החילופים כך שמתקיים $a \neq c$ ו- $b = d$). עד כאן הטיעונים שלא נתבקשתם להסביר בתשובתכם (אבל עדיין כדאי לדעת אותם).

עתה נזכיר את הטענה הבאה מחוברת הקורס (היא הובאה ללא הוכחה שם, אבל יש לה הוכחה בשאלה "בלי הרבה נפנוף ידיים" שבחוברת התרגילים הפתורים): תוחלת מספר הצעדים בהילוך מקרי מצומת v כל שהוא

עד הפעם הראשונה שהוא חוזר ל- v היא $1/\alpha$, כאשר α היא ההסתברות ל- v תחת ההתפלגות הסטציונרית. במקרה שלנו כל דרגות הצמתים בגרף שוות, לכן ההתפלגות הסטציונרית היא ההתפלגות היוניפורמית מעל קבוצת הצמתים, ולכן תוחלת מספר הצעדים בהילוך מקרי שיוצא מ- $(1, \dots, n)$ עד הפעם הבאה שהוא מגיע ל- $(1, \dots, n)$ היא בדיוק $|V| = n!$.

לסיום נשים לב שהילוך מקרי שיוצא מ- $(1, \dots, n)$ תמיד עובר בצעד הראשון שלו בפרמוטציה שנבדלת מ- $(1, \dots, n)$ בחילוף בודד. על כן תוחלת מספר הצעדים מפרמוטציה כזו עד שמגיעים ל- $(1, \dots, n)$ (מכיוון שהיא זהה לכל הפרמוטציות מסוג זה) היא $(n - O(1))! - 1 = n!$.

הוכחה קלה אלטרנטיבית לסעיף השני: חלקכם מצאתם שיטה פשוטה יחסית לחסום את ההתנגדות השקולה בגרף ההילוך המקרי. נסתכל על החתך $\{(1, \dots, n)\}, V \setminus \{(1, \dots, n)\}$ בגרף, ונשים לב שיש בו $\binom{n}{2}$ קשתות. זה נותן חסם תחתון של $1/\binom{n}{2}$ על ההתנגדות השקולה בין $(1, \dots, n)$ לבין הפרמוטציה שיוצאים ממנה, ולכן מוביל לחסם תחתון של $(n - O(1))!$ על זמן הביקור. לסיום משתמשים בתכונת הטרנזיטיביות שהצגנו בתחילת הפתרון של השאלה, לקבלת חסם תחתון גם על זמן הפגיעה.

צלילה לתוך עץ

לכל עץ T נסמן ב- n_T את מספר הצמתים של T , וב- α_T את התוחלת $E[Z_d]$ כאשר מבצעים את התהליך המתואר בשאלה על העץ T . נוכיח את אי-השוויון $\alpha_T \leq \log(n_T)/\log(d)$ באינדוקציה על גובה העץ. הבסיס הוא המקרה שבו העץ מורכב מעלה בודד שהוא גם השורש, ובמקרה זה אכן מתקיים $E[Z_d] = 0$.

עבור ההמשך, נסמן ב- X את המ"מ שמקבל את זהות העלה שמגיעים אליו בסוף התהליך (כעיקרון מרחב ההסתברות תלוי ב- T , אבל נשמיט את האינדקס כשזה ברור מהקשר). נסמן $\beta_T = H[X]$, ונשים לב שמתקיים (לפי החסם העליון על אנטרופיה) $\beta_T \leq \log(n_T)$. אנחנו נראה בעצם שמתקיים $\beta_T \geq \alpha_T \cdot \log(d)$ על מנת להשלים את ההוכחה (אפשר לוודא שגם זה מתקיים במקרה הבסיס).

נניח שלשורש העץ T יש k בנים, ונסמנם ב- u_1, \dots, u_k את תתי-העץ המתאימים להם נסמן ב- T_1, \dots, T_k . נסמן ב- Y את המ"מ שמקבל את זהות הבן של השורש שעוברים אליו. לפי כלל השרשרת, והעובדה ש- Y הוא פונקציה של X , מתקיים $\beta_T = H[X] = H[X, Y] = H[Y] + H[X|Y]$. לפי הצבת הסתברות המאורעות " $Y = i$ " והנחת האינדוקציה מתקיים $\beta_T = H[Y] + \frac{1}{k} \sum_{i=1}^k \beta_{T_i} \geq H[Y] + \frac{1}{k} \sum_{i=1}^k \alpha_{T_i} \cdot \log(d)$. מכאן מפצלים לשני מקרים.

אם $k < d$ אז מתקיים לפי נוסחת התוחלת השלמה $\alpha_T = \frac{1}{k} \sum_{i=1}^k \alpha_{T_i}$. בהצבה בנוסחה עבור β_T מתקיים $\beta_T = H[Y] + \frac{1}{k} \sum_{i=1}^k \beta_{T_i} \geq \frac{1}{k} \sum_{i=1}^k \alpha_{T_i} \cdot \log(d) = \alpha_T \cdot \log(d)$ כנדרש.

אם $k \geq d$ אז מתקיים $\alpha_T = 1 + \frac{1}{k} \sum_{i=1}^k \alpha_{T_i}$. כמו כן $H[Y] = \log(k) \geq \log(d)$. בהצבה מתקיים $\beta_T = H[Y] + \frac{1}{k} \sum_{i=1}^k \beta_{T_i} \geq \log(d) + \frac{1}{k} \sum_{i=1}^k \alpha_{T_i} \cdot \log(d) = \alpha_T \cdot \log(d)$ כנדרש.