

פתרון לתרגיל הראשון

האחדה

נתייחס לפונקציות $f : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ ו- $g(i) = nf(i) + i - 1$ כפי שהוגדרו בניסוח של השאלה. בשלב הראשון נראה שאם f היא פונקציה מונוטונית לא-יורדת, אז גם g היא מונוטונית לא-יורדת: אם לכל $1 \leq i < j \leq n$ מתקיים $f(i) \leq f(j)$, אז מתקיים $g(i) = nf(i) + i - 1 \leq nf(j) + j - 1 \leq g(j)$. עתה נראה שהמרחק של g ממונוטוניות אינו עולה על זה של f : אם קיימת פונקציה מונוטונית f' כך שמתקיים $|\{i : f(i) \neq f'(i)\}| \leq k$ (תנאי זהה לזה ש- f היא k/n -קרובה למונוטונית), אז נגדיר את $g' : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ לפי הנוסחה $g'(i) = nf'(i) + i - 1$. לפי ההוכחה מלמעלה g' היא מונוטונית, ולא קשה לוודא שמתקיים $|\{i : g(i) \neq g'(i)\}| \leq k$.

עתה נראה את הכיוון השני, שהמרחק של f ממונוטוניות אינו עולה על זה של g : אם קיימת פונקציה מונוטונית g' כך שמתקיים $|\{i : g(i) \neq g'(i)\}| \leq k$, אז נגדיר את f' לפי הנוסחה $f'(i) = \lfloor g'(i)/n \rfloor$. שימו לב שבפרט לכל i שעבורו $g'(i) = g(i) = nf(i) + i - 1$ מתקיים גם $f'(i) = f(i)$, ולכן $|\{i : f(i) \neq f'(i)\}| \leq k$. כמו כן קל לוודא ש- f' היא מונוטונית לא-יורדת בגלל ש- g' היא מונוטונית לא-יורדת (משתמשים בזה שלכל $x \leq y$ מתקיים $\lfloor \frac{x}{n} \rfloor \leq \lfloor \frac{y}{n} \rfloor$).

זוגיות מושלמת

ראשית ננתח את האלגוריתם הבא:

- לכל $1 \leq i \leq 2n$, נבחר את i להיות ב- Q בהסתברות $2/(\epsilon n)^{1/3}$, באופן ב"ת ב- $i \neq i'$ האחרים.
- נשאל את הערך של f בכל הקבוצה Q . נדחה את f אם מצאנו $i < j < l$ (כולם ב- Q) שעבורם $f(i) = f(j) = f(l)$ ואחרת נקבל את f .

פונקציה f שהיא דו-יחיד-ערכית תתקבל בהסתברות 1 (היא לא תכיל שלישייה כזו). אנחנו נראה עוד מעט שעבור פונקציה ϵ -רחוקה, בהסתברות לפחות $\frac{11}{12}$ אנחנו נמצא שלישייה כזו ונדחה את f . לפי השאלה "לבלוע את החוכמה" מרשימת הקריאה שלכם, נובע מכך שהאלגוריתם הבא (שתמיד יהיו לו $O(n^{2/3}/\epsilon^{1/3})$ שאילתות) ידחה פונקציה ϵ -רחוקה בהסתברות לפחות $\frac{2}{3}$ (אנחנו מפעילים את התוצאה משם עבור $q = \lceil 8n^{2/3}/\epsilon^{1/3} \rceil$, כאשר \mathcal{F} היא משפחת השלישיות הנ"ל).

- נבחר את Q להיות קבוצה בגודל $\lceil 8n^{2/3}/\epsilon^{1/3} \rceil$, באופן יוניפורמי מבין כל תתי-קבוצה של $\{1, \dots, 2n\}$ בגודל הזה.
- נשאל את הערך של f בכל הקבוצה Q . נדחה את f אם מצאנו $i < j < l$ (כולם ב- Q) שעבורם $f(i) = f(j) = f(l)$ ואחרת נקבל את f .

עתה נוכיח את הטענה על הסתברות הדחיה של האלגוריתם הראשון (בחירה של כל i באופן ב"ת). לשם כך נראה את הטענה שאם $f : \{1, \dots, 2n\} \rightarrow \{1, \dots, n\}$ היא ϵ -רחוקה מלהיות דו-יחיד-ערכית, אז קיימת משפחה \mathcal{F}' של לפחות $2\epsilon n/3$ שלשות, שכולן זרות זו לזו, כך שלכל שלשה $\{i, j, l\} \in \mathcal{F}'$ מתקיים $f(i) = f(j) = f(l)$.

לכל $1 \leq k \leq n$, נסמן ב- n_k את מספר האינדקסים $1 \leq i \leq 2n$ שעבורם מתקיים $f(i) = k$. בסימונים של תורת הקבוצות, $n_k = |f^{-1}(\{k\})|$. אפשר לבחור משפחה \mathcal{F}' בגודל $\lfloor \sum_{k=1}^n \lfloor n_k/3 \rfloor \rfloor$, ע"י כך שבכל קבוצה מהצורה " $f^{-1}(\{k\})$ " נבחר מספר מקסימלי של שלשות זרות.

המרחק של f מלהיות דו-יחיד-ערכית הוא בדיוק $\sum_{k=1}^n \min\{0, 2 - n_k\} = \sum_{k=1}^n \min\{0, n_k - 2\}$: השוויון בין שני הסכומים נובע מ- $\sum_{k=1}^n n_k = 2n$ (זהו זהה לגודל התחום של f). כמו כן ברור שלמשל הסכום

השמאלי הוא חסם תחתון על מספר השינויים הדרוש (כי לפונקציה דו־חד־ערכית בפרט לא יכול להיות k שעבורו $n_k < 2$). על מנת להראות שזהו המרחק המדויק, אפשר להפוך את f להיות דו־חד־ערכית באופן הבא: בכל פעם משנים ערך $f(i) = k$ שעבורו $n_k > 2$ להיות שווה ל־ k' שעבורו $n_{k'} < 2$. מכך מתקיים

$$\sum_{k=1}^n \lfloor n_k/3 \rfloor \geq \frac{1}{3} \sum_{k=1}^n \min\{0, n_k - 2\} > 2\epsilon n/3$$

עתה שיש לנו את החסם, נשים לב שעבור שלישייה ספציפית ב־ \mathcal{F}' , הסיכוי של כל האינדקסים שלה להיות ב־ Q (בגלל אי־התלות של בחירת האינדקסים) הוא בדיוק $8/\epsilon n$. הסיכוי שאף שלישייה ב־ \mathcal{F}' לא נכללה בשלמותה הוא אם כן $(1 - 8/\epsilon n)^{|\mathcal{F}'|} < (e^{-8/\epsilon n})^{2\epsilon n/3} < \frac{1}{12}$. כנדרש.

פתרון לתרגיל השני

גבעה רמה

אנחנו נשתמש בהיתר מהשאלה ונניח ש- $f : \{1, \dots, n\} \rightarrow \mathbb{N}$ היא חח"ע. נגדיר את $g : \{1, \dots, n-1\} \rightarrow \mathbb{Z}$ לפי $g(i) = f(i) - f(i+1)$. אם f היא "הרית" (כפי שהתכונה הוגדרה בשאלה), אז קיים $1 \leq i \leq n$ כך שערכי g מעל $\{1, \dots, i-1\}$ הם כולם שליליים (אלא אם כן מתקיים $i=0$), וגם ערכי g מעל $\{i, \dots, n-1\}$ הם כולם חיוביים (אלא אם כן $i=n$). זה מתקיים עבור האינדקס i שמעליו f מקבלת את ערך המקסימום.

גם אם f אינה הרית, מההנחה שהיא חח"ע נובע שאין ערכי "0" ב- g . אם נבצע ב- g חיפוש בינארי עבור הערך הלא-קיים "0", התוצאה תהיה אינדקס i שמקיים גם $g(i-1) < 0$ אם $i > 1$, וגם $g(i) > 0$ אם $i < n$. במקרה ש- f היא הרית, נקבל את האינדקס i שבו g מחליפה סימן, כך ש- f מונוטונית עולה מעל $\{1, \dots, i\}$, ומונוטונית יורדת מעל $\{i, \dots, n\}$ (לא צריך לדאוג למקרה הקיצון ש- f היא כולה מונוטונית עולה, כי אז היא עדיין תהיה "מונוטונית יורדת" מעל $\{n\}$), ובאופן דומה לא צריך לדאוג למקרה הקיצון ש- f היא כולה מונוטונית יורדת).

האלגוריתם שלנו:

- מבצעים חיפוש בינארי עבור הערך "0" בפונקציה $g : \{1, \dots, n-1\} \rightarrow \mathbb{N}$ שהוגדרה למעלה, תוך שימוש ב- $O(\log(n))$ שאילתות ל- g , ולכן $O(\log(n))$ שאילתות ל- f (עבור ביצוע כל שאילתה " $g(j)$ " מבצעים שתי שאילתות ל- f , את " $f(j)$ " ואת " $f(j+1)$ ").
- עבור האינדקס i שהתקבל מהחיפוש ב- g , מבצעים $\epsilon/2$ -בדיקה למונוטוניות של הצמצום של f לקבוצה $\{1, \dots, i\}$ (עם הסתברות לפחות $\frac{2}{3}$). מספר השאילתות הכולל הוא $O(\log(i)/\epsilon) \leq O(\log(n)/\epsilon)$.
- עבור האינדקס i שהתקבל מהחיפוש ב- g , מבצעים $\epsilon/2$ -בדיקה למונוטוניות של הצמצום של f לקבוצה $\{i, \dots, n\}$ (כאן זו בדיקה למונוטוניות לא-עולה - ע"מ לבצע אותה אפשר למשל לבדוק את $-f$ למונוטוניות לא-יורדת). מספר השאילתות הכולל הוא $O(\log(n-i)/\epsilon) \leq O(\log(n)/\epsilon)$.
- מקבלים אם שתי בדיקות המונוטוניות למעלה קיבלו.

מספר השאילתות של האלגוריתם מחושב בתוך התיאור שלו, ולפי הניתוח של הפונקציה g למעלה, אם f היא הרית אז החיפוש הבינארי אכן יתן i שעבורו שני מבחני המונוטוניות יקבלו (בהסתברות 1). לעומת זאת, אם f אינה ϵ -קרובה להיות הרית, אז לכל i שיתקבל, לא יכול להיות ש- f היא גם $\epsilon/2$ -קרובה להיות מונוטונית לא-יורדת מעל $\{1, \dots, i\}$ וגם $\epsilon/2$ -קרובה להיות מונוטונית לא-עולה מעל $\{i, \dots, n\}$. אחרת, היינו יכולים לבצע את התיקון בכל אחד מהמקטעים ולקבל סתירה למרחק של f (אם שני התיקונים דורשים שינוי בערך $f(i)$ עצמו, אז לוקחים את הערך הגבוה מביניהם). מכאן שפונקציות רחוקות ממונוטוניות יידחו בהסתברות לפחות $\frac{2}{3}$.

מסר סמוי

נפתור את השאלה בשיטה הראשונה שהוזכרה בהדרכה. נשתמש ב- $k = \lceil 4l/\epsilon \rceil$, כאשר l יסמן את אורך המחזרות המינימלית ב- \mathcal{F} (לחובבי מקרי הקצה: אם $l=0$ אז זה אומר שאין אף קלט שמקיים את התכונה, ואפשר פשוט לדחות בלי לעשות שאילתות). בנוסף לכך נסמן ב- L את אורך המחזרות המקסימלית ב- \mathcal{F} (הוא מוגדר כי הנחנו ש- \mathcal{F} היא סופית).

נסתכל על החלוקה $\{1, \dots, n\} = I_1 \cup \dots \cup I_k$, כאשר $I_j = \{\lfloor \frac{j-1}{k}n \rfloor + 1, \dots, \lfloor \frac{j}{k}n \rfloor\}$. זוהי חלוקה לקטעים זרים שמקיימת $|I_j| \in \{\lfloor n/k \rfloor, \lceil n/k \rceil\}$ (כל חלוקה אחרת עם גדלים דומים גם היתה עובדת). כאן גם נכתוב את ההנחה על גודל n : נניח שהוא גדול מספיק על מנת לקיים $\lfloor n/k \rfloor \geq 2L - 1$.

נבצע את האלגוריתם הבא:

• לכל $1 \leq j \leq k$, נדגום (עם חזרות) $\lceil 4 \log(k)/\epsilon \rceil$ אינדקסים מתוך I_j ונשאל את הערכים שלהם. אם יצא שדגמנו פחות מ- $2L - 1$ אינדקסים שונים, נוסיף באופן שרירותי עוד אינדקסים מ- I_j עד שיהיו לנו $2L - 1$ אינדקסים סה"כ, ונשאל גם אותם. נסמן ב- Q_j את קבוצת השאלות ששאלנו מ- I_j .

• אם בכל השאלות ששאלנו נמצא תת-מחרוזת אסורה, וז"א אם יש מחרוזות $(b_1, \dots, b_t) \in \mathcal{F}$ ואינדקסים $i_1 < \dots < i_t \in Q_1 \cup \dots \cup Q_k$ שעבורם $a_{i_r} = b_r$ לכל $1 \leq r \leq t$, אז נדחה, ואחרת נקבל.

עבור הניתוח, ראשית נשים לב שאנחנו לעולם לא נדחה קלט שאינו מכיל מחרוזת מ- \mathcal{F} . עבור הכיוון השני, ראשית נשים לב שלכל $1 \leq j \leq k$, אם הערך "1" מופיע יותר מ- $\frac{\epsilon}{2}|I_j|$ פעמים בקטע I_j אז בהסתברות לפחות $1 - 1/6k$ נדגום לפחות ערך אחד כזה בתוך Q_j , ואם הערך "0" מופיע יותר מ- $\frac{\epsilon}{2}|I_j|$ פעמים בקטע I_j אז בהסתברות לפחות $1 - 1/6k$ נדגום לפחות ערך אחד כזה בתוך Q_j . סה"כ בהסתברות לפחות $\frac{2}{3}$ לא יהיה אף ערך שמופיע יותר מ- $\frac{\epsilon}{2}|I_j|$ פעמים ב- I_j כל שהוא ולא דגמנו ממנו לפחות פעם אחת.

נראה עתה שבהינתן המאורע למעלה (שקורה בהסתברות לפחות $\frac{2}{3}$), אם לא דחינו את הקלט אז הוא ϵ -קרוב למחרוזת שלא מכילה שום תת-מחרוזת מ- \mathcal{F} . את המחרוזת החדשה נבנה בצורה הבאה: לכל $1 \leq j \leq k$ נבדוק מה הערך שהופיע יותר פעמים כששאלנו את האינדקסים מ- Q_j , ונשנה את כל ערכי המחרוזת ב- I_j להיות זהים לאותו ערך. נסמן את המחרוזת החדשה ב- A' .

ראשית נשים לב שאין יותר מ- l אינדקסים $1 \leq j \leq k$ שעבורם מציאנו ב- Q_j גם ערך של "0" וגם ערך של "1". אחרת, אם יש לנו $j_1 < \dots < j_l$, כך שלכל $1 \leq r \leq l$ קיימים $i_{0,r}, i_{1,r} \in Q_{j_r}$ שמקיימים $a_{i_{0,r}} = 0$ ו- $a_{i_{1,r}} = 1$, אז היינו צריכים לדחות את המחרוזת. זאת מכיוון שקיימת מחרוזת $(b_1, \dots, b_l) \in \mathcal{F}$ (לפי ההגדרה של l), ועבורה מתקיים $a_{i_{b_r,r}} = b_r$ לכל $1 \leq r \leq l$, ולכן נגלה תת-מחרוזת אסורה בשלב האחרון.

מכאן נובע ש- A' היא ϵ -קרובה למחרוזת המקורית A . מהבחירה של k נובע שלא שינינו יותר מ- $\frac{\epsilon}{2}n$ ערכים סה"כ עבור כל ה- I_j שמציאנו בהם את שני הערכים האפשריים (הבחירה של k עם מקדם 4 היא על מנת להתחשב גם בשגיאות של עיגול למעלה באורך I_j). כמו כן, לפי המאורע שניתחנו קודם, בכל I_j אחר לא שינינו יותר מ- $\frac{\epsilon}{2}|I_j|$ ערכים, ולכן לא שינינו יותר מעוד $\frac{\epsilon}{2}n$ ערכים סה"כ.

לבסוף נראה שאין ב- A' עותק של מחרוזת אסורה מ- \mathcal{F} . נניח בשלילה שקיימת מחרוזת $(b_1, \dots, b_t) \in \mathcal{F}$ שהיא תת-מחרוזת של A' עם אינדקסים $i_1 < \dots < i_t$. כזכור $t \leq L$ לפי הבחירה של L . כמו כן, אנחנו יודעים שלכל Q_j יש קבוצה Q'_j של לפחות L אינדקסים שעבורם הערך של A זהה לערך האחיד של A' מעל I_j (כזכור לקחנו את הערך שמופיע יותר, ודאגנו שמתקיים $|Q_j| \geq 2L - 1$, ולכן בפרט $|Q'_j| \geq L$). על כן ניתן להחליף את האינדקסים i_1, \dots, i_t באינדקסים שכולם מתוך $Q'_1 \cup \dots \cup Q'_k$ ועליהם יש ל- A את אותם ערכים כמו A' , ומכאן שהיינו אמורים לדחות את A בשלב האחרון של האלגוריתם.

כמה מילים על השיטה השניה להוכחה: שיטה זו מבוססת על אינדוקציה על סכום האורכים של המחרוזות ב- \mathcal{F} . בסיס האינדוקציה הוא המקרה שבו המחרוזת הריקה נמצאת ב- \mathcal{F} , ואז אפשר לדחות בלי לקרוא את הקלט כלל, והמקרה שבו \mathcal{F} עצמה ריקה, ואז אפשר לקבל. אחרת, אם יש ב- \mathcal{F} גם מחרוזות שמתחילות ב-"0" וגם כאלו שמתחילות ב-"1", קוראים את הערך a_1 , ומגדירים לפיו את \mathcal{F}' : לכל מחרוזת ב- \mathcal{F} שמתחילה באות זהה ל- a_1 , מסירים את האות הראשונה. כל שנותר הוא לבצע באינדוקציה ϵ -בדיקה של (a_2, \dots, a_n) נגד המשפחה \mathcal{F}' .

המקרה השני הוא כאשר כל המחרוזות ב- \mathcal{F} מתחילות באותו ערך, נניח לדוגמה "1". אז בשלב הראשון דוגמים $O(1/\epsilon)$ אינדקסים שנבחרים יוניפורמית מ- $\{1, \dots, n\}$, ובוחרים מאלו את האינדקס הכי קטן i שעבורו $a_i = 1$ (אם לא מוצאים אינדקס כזה אז מסיקים שאין הרבה ערכי "1" במחרוזת ומקבלים את הקלט). בהסתברות גבוהה זהו אחד מ- $\frac{1}{2}\epsilon n$ האינדקסים הכי קטנים עם ערך של "1" ב- A , ולכן A הוא $\frac{1}{2}\epsilon$ -קרוב למחרוזת A' שבה איפסנו a_1, \dots, a_{i-1} . כל שנותר הוא לבצע $\frac{1}{2}\epsilon$ -בדיקה של המחרוזת (a_i, \dots, a_n) נגד המשפחה \mathcal{F}' , המתקבלת מ- \mathcal{F} ע"י הסרת האות הראשונה מכל אחת מהמחרוזות בה.

השיטה הזו יותר קלה להכללה מהשיטה הקודמת למחרוזות מעל א"ב עם יותר אותיות, למשל למחרוזות מעל $\{0, 1, \dots, c\}$ במקום $\{0, 1\}$.

פתרון לתרגיל השלישי

גלגל ענק

אנחנו נשתמש כאן באופן ישיר בשיטה של יאו נגד אלגוריתמים לא-אדפטיבים. לשם הגדרת ההתפלגויות מעל הקלטים נניח ש- n זוגי. עבור n אי-זוגי נבחר קלט (פרמוטציה) שמעביר את האיבר האחרון לעצמו, ונשתמש בבניה עבור $n - 1$ האיברים האחרים.

- עבור ההתפלגות τ , נבחר באופן יוניפורמי (מבין $n!$ האפשרויות) סדרה של n אינדקסים שונים זה מזה $i_1, \dots, i_n \in \{1, \dots, n\}$, ונגדיר את σ לפי $\sigma(i_k) = i_{k+1}$ עבור $1 \leq k < n$, ו- $\sigma(i_n) = i_1$.
- עבור ν , שוב נבחר באופן יוניפורמי סדרה של n אינדקסים שונים זה מזה $i_1, \dots, i_n \in \{1, \dots, n\}$ והפעם נגדיר את σ לפי $\sigma(i_k) = \sigma(i_{n+1-k})$ לכל $1 \leq k \leq n$.

זה ברור שפרמוטציה שנבחרת לפי ההתפלגות τ היא בהסתברות 1 עגיל מגודל n . באשר להתפלגות ν , בפרמוטציה σ שנבחרת לפיה כל זוג i_k, i_{n+1-k} יהיה עגיל בפני עצמו, ולכן לפחות אחד מהערכים $\sigma(i_k), \sigma(i_{n+1-k})$ צריך להשתנות על מנת לגרום ל- σ להיות עגיל מאורך n . מכאן שפרמוטציה שנבחרת לפי ν תהיה $\frac{1}{2}$ -רחוקה מהתכונה בהסתברות 1.

עתה ננתח את $\tau|_Q$ ו- $\nu|_Q$ עבור קבוצה קבועה של שאילתות $Q \subseteq \{1, \dots, n\}$. עבור $i, j \in Q$ (לא בהכרח שונים זה מזה), נגדיר את המאורע $B_{i,j}$ שמתקיים $\sigma(i) = j$ (שימו לב שעבור $i \neq j$ המאורעות $B_{i,j}$ ו- $B_{j,i}$ הם שונים). הסיכוי שהמאורע הזה מתקיים עבור $i \neq j$ (כאשר לא מתנים אותו על מאורעות אחרים) הוא $\frac{1}{n-1}$ בדיוק, גם עבור τ וגם עבור ν . עבור ν לדוגמה, אם עבור k מסויים אנחנו מתנים על $i_k = i$ (תמיד יהיה k כזה), אז i_{n+1-k} מתפלג יוניפורמית על $\{1, \dots, n\} \setminus \{j\}$, ובהסתברות $\frac{1}{n-1}$ הוא יהיה שווה ל- j . לעומת זאת המאורע $B_{i,i}$ לא מתקיים אף פעם.

לפי חסם איחוד מאורעות, הסיכוי שלפחות אחד מהמאורעות $B_{i,j}$ מתקיים חסום ע"י $2 \binom{|Q|}{2} / (n-1)$, ואם $|Q| < \sqrt{n}/2$, אז בהסתברות גדולה מ- $\frac{3}{4}$ אף אחד מהמאורעות לא קורה. הדבר האחרון לשים לב הוא שכאשר אנחנו מתנים על כך שאף אחד מהמאורעות הנ"ל לא קורה, גם ההתפלגות של $\tau|_Q$ וגם ההתפלגות של $\nu|_Q$ היא יוניפורמית מבין קבוצת כל הפונקציות החד-חד-ערכיות $f: Q \rightarrow \{1, \dots, n\} \setminus Q$.

בבדיקת התשובות לא הורדתי נקודות על הוכחה לא-שלמה של הטענה הנ"ל, אבל נראה לדוגמה איך מוכיחים אותה עבור ν : נראה שהטענה נכונה אפילו כאשר אנחנו מתנים את ההתפלגות בנוסף על זהות הקבוצה $K \subseteq \{1, \dots, n\}$ שעבורה מתקיים $Q = \{i_k : k \in K\}$. המשמעות שאף אחד מהמאורעות $B_{i,j}$ אינו מתקיים היא שלא קיים $k \in K$ שעבורו גם $n+1-k \in K$. אם נסמן $K = \{k_1, \dots, k_{|Q|}\}$, הצמצום של הפרמוטציה המוגרלת σ ל- Q נתון ע"י $\sigma(i_{k_j}) = i_{n+1-k_j}$. כפועל יוצא מהגדרת ההגרלה של i_1, \dots, i_n , כאשר מתנים על ערכי $i_{k_1}, \dots, i_{k_{|Q|}}$ מתקבל שהסידרה $i_{n+1-k_1}, \dots, i_{n+1-k_{|Q|}}$ מתפלגת יוניפורמית מבין כל הסדרות ללא חזרות מתוך $\{1, \dots, n\} \setminus \{i_{k_1}, \dots, i_{k_{|Q|}}\}$, שזה מה שרצינו להוכיח.

מניתוח ההסתברות של המאורעות $B_{i,j}$, ושוויון ההתפלגויות המותנות על אי-קיום המאורעות הנ"ל, עולה שאם $|Q| < \sqrt{n}/2$ אז מתקיים $d(\tau|_Q, \nu|_Q) < \frac{1}{4}$, ויש לנו את הדרוש להסקת החסם התחתון בשיטה של יאו.

קשיים בזוגיות

בפתרון כאן לא נשתמש בשיטה של יאו (יש גם פתרון שמשתמש בהתאמה של השיטה לשגיאה חד-כיוונית). ראשית נשים לב שעבור פונקציה f ועבור פרמוטציה σ מעל $\{1, \dots, 2n\}$, מתקיים שהמרחק של f מדור-חד-ערכיות זהה למרחק של $f \circ \sigma$, הפונקציה המוגדרת ע"י $(f \circ \sigma)(i) = f(\sigma(i))$. לכן אפשר להפעיל את הטכניקה של הסעיף הראשון של השאלה "לא למצוא את הצדק" מתוך התרגילים של 2021 (שהייתם אמורים לקרוא), ולהגיע למסקנה שכל אלגוריתם (אפילו אדפטיבי) עם q שאילתות ניתן להפוך לאלגוריתם

לא־אדפטיבי עם אותו מספר שאילתות, כך שקבוצת השאילתות Q נבחרת באופן יוניפורמי מכל תתי־קבוצה מגודל q של $\{1, \dots, 2n\}$.

מכיוון שהמדובר באלגוריתם עם שגיאה חד־צדדית, האפשרות היחידה לדחות את הקלט היא אם קיימים $i, j, k \in Q$, כולם שונים זה מזה, שעבורם מתקיים $f(i) = f(j) = f(k)$. הסיבה היא שלכל פונקציה $g : Q \rightarrow \{1, \dots, n\}$ שעבורה אין i, j, k כאלו קיימת פונקציה דו־חד־ערכית $f' : \{1, \dots, 2n\} \rightarrow \{1, \dots, n\}$ שעבורה $f'|_Q = g$, ולכן לאלגוריתם הסתברותי שהיה יכול לדחות את הקלט במקרה כזה היה סיכוי גדול מאפס לדחות את f' , בסתירה לדרישה לשגיאה חד־כיוונית.

השלב הבא הוא להשתמש בשאלה "להקיא את החוכמה" מחוברת התרגילים של הקורס "שיטות הסתברותיות ואלגוריתמים", שהופיע ברשימת הקריאה המשלימה מתחילת הקורס, כאשר \mathcal{F} בניסוח השאלה תהיה קבוצת השלשות $i, j, k \in \{1, \dots, 2n\}$ שעבורן $f(i) = f(j) = f(k)$. על כן נסתכל על האפשרות לבחור את הקבוצה Q ע"י כך שכל $i \in \{1, \dots, 2n\}$ יוכנס ל־ Q בהסתברות p , באופן ב"ת באינדקסים האחרים. נראה חסם של $\Omega(1/n^{1/3})$ על p שיכול להבטיח תפיסה של $i, j, k \in Q$ כנדרש בהסתברות לפחות $\frac{1}{2}$, ומכאן נקבל חסם של $\Omega(n^{2/3})$ על q הדרוש לתפיסת שלשה כזו בהסתברות לפחות $\frac{2}{3}$ (כאשר מניחים ש־ n הוא גדול דיו).

עבור החסם התחתון נבדוק עתה את הפונקציה הנתונה ע"י $f(i) = \lceil i/3 \rceil$. עבור n גדול דיו פונקציה זו היא $\frac{1}{4}$ ־רחוקה מדו־חד־ערכיות (צריך לשנות לפחות $\lfloor 2n/3 \rfloor$ מערכי הפונקציה ע"מ להפוך אותה לדו־חד־ערכית). הסיכוי של שלשה בודדת מהצורה $3j - 2, 3j - 1, 3j$ להיות כולה ב־ Q (כאשר כל $i \in \{1, \dots, 2n\}$ מוגרל להיות שם בהסתברות p) הוא p^3 . הסיכוי שנצליח לתפוס שלשה כל שהיא בשלמותה חסום לכן מלמעלה ע"י $2np^3/3$ לפי איחוד מאורעות (אנחנו צריכים חסם מלמעלה, כי זהו חסם על הסיכוי לא להכשל, ואנחנו רוצים להראות שבסיכוי גבוה האלגוריתם כן נכשל). כאשר מתקיים למשל $p \leq 1/2n^{1/3}$ החסם הזה יהיה קטן מ־ $\frac{1}{2}$, מה שנותן לנו חסם תחתון של $\Omega(1/n^{1/3})$ על p שבו האלגוריתם לא נכשל בהסתברות גבוהה.

פתרון לתרגיל הרביעי

מושגים עם פשרות

הבדיקה נעשית באמצעות רדוקציה לבדיקת התפלגויות. עבור הקלט $f: \{1, \dots, 2n\} \rightarrow \{1, \dots, n\}$ נגדיר את ההתפלגות μ_f מעל $\{1, \dots, n\}$, ע"י הנוסחה $\mu_f(k) = |f^{-1}(\{k\})|/2n$. נשים לב שאפשר לקבל דגימה בודדת עבור μ_f ע"י כך שמגרילים $1 \leq i \leq 2n$ באופן יוניפורמי וב"ת בהגרלות קודמות, ולוקחים את $f(i)$ בתור הדגימה שלנו. כזכור, עבור כל ϵ קבוע, ניתן לבצע ϵ -בדיקה עבור היוניפורמיות של $\mu_f(i)$ ב- $O(\sqrt{n})$ דגימות, ולפי הדיון כאן אלו מתרגמות ל- $O(\sqrt{n})$ שאילתות מ- f .

הדבר הבא לשים לב הוא שאם f היא דו-חד-ערכית, אז לכל i מתקיים $\mu_f(i) = 2/2n = 1/n$, ז"א שאז μ_f היא ההתפלגות היוניפורמית. עבור הניתוח של μ_f כאשר f היא ϵ -רחוקה מדו-חד-ערכיות, נזכר בניתוח מהשאלה "זוגיות מושלמת" מהתרגיל הראשון. כזכור מספר השינויים הדרוש להפוך את f לדו-חד-ערכית נתון ע"י $\sum_{k=1}^n \min\{0, n_k - 2\}$ כאשר $n_k = |f^{-1}(\{k\})| = 2n \cdot \mu_f(k)$. לעומת זאת, המרחק של μ_f מיוניפורמיות נתון ע"י $\frac{1}{2} \sum_{k=1}^n |\mu_f(k) - \frac{1}{n}| = \sum_{k: \mu_f(k) > 1/n} (\mu_f(k) - \frac{1}{n}) = \frac{1}{2n} \sum_{k=1}^n \min\{0, n_k - 2\}$ (את השוויון הימני אפשר לראות למשל בשאלה "קרבה בין התפלגויות" בחוברת התרגילים של הקורס שיטות הסתברותיות). קיבלנו שהמרחק של μ_f מיוניפורמיות זהה למרחק של f מדו-חד-ערכיות. על כן, ϵ -בדיקה של μ_f (כהתפלגות) תתן לנו את הבדיקה המבוקשת של f .

צרות עם אופציות

ההוכחה תהיה בשיטה של יאו. ראשית, נשים לב לכך שמספיק לבצע את השיטה נגד אלגוריתמים לא אדפטיביים, ז"א שצריך לנתח את הצמצומים של ההתפלגויות מעל קלטים ν ו- τ שאנחנו נבנה רק עבור צמצום לקבוצת שאילתות קבועה Q . הסיבה לכך היא שאפשר להפוך אלגוריתם אדפטיבי ללא-אדפטיבי ע"י פרמוטציה מקרית ויוניפורמית של תחום הפונקציה, כפי שכבר עשיתם בשאלה "קשיים בזוגיות", וקראתם בשאלה "לא למצוא את הצדק" משנת 2021 (בכל מקרה הפעם לא הייתם צריכים להוכיח את זה). כמו כן נניח ש- n הוא מספר זוגי. אם n הוא אי-זוגי, אז אפשר למשל פשוט להגביל את עצמנו לפונקציות שעבורן $f(2n-1) = f(2n) = n$, ולהמשיך לעבוד עם המקרה של $n-1$.

אנחנו נגדיר את ההתפלגויות שלנו באופן הבא:

- גם עבור τ וגם עבור ν , נבחר באופן מקרי ויוניפורמי מבין כל האפשרויות סדרה של רביעיות זרות $C_1, \dots, C_{n/2}$ שביחד מכסות את כל $\{1, \dots, 2n\}$.
- עבור τ , בכל רביעיה C_k , נבחר באופן מקרי ויוניפורמי זוג $P_k \subset C_k$ (מבין 6 האפשרויות). כמו כן נבחר באופן ב"ת בבחירת P_k שני ערכים $i_k \neq j_k$ מתוך $\{4k-3, 4k-2, 4k-1, 4k\}$, באופן יוניפורמי מתוך 12 האפשרויות. נקבע את f להיות שווה ל- i_k על איברי P_k , ולהיות שווה ל- j_k על איברי $C_k \setminus P_k$. נבצע את ההגרלות הנ"ל באופן ב"ת לכל אחת מהרביעיות.
- עבור ν , לכל רביעיה C_k , בהסתברות $\frac{1}{3}$ נקבע את f על כל איברי C_k להיות שווה לערך בודד שנבחר יוניפורמית מתוך $\{4k-3, 4k-2, 4k-1, 4k\}$, ובהסתברות $\frac{2}{3}$ נקבע את $f|_{C_k}$ להיות פונקציה חח"ע ועל $\{4k-3, 4k-2, 4k-1, 4k\}$ שבחרים יוניפורמית מבין 24 האפשרויות. גם ההגרלות כאן נעשות באופן ב"ת לכל אחת מהרביעיות.

ראשית נשים לב ש- τ היא אכן התפלגות על פונקציות דו-חד-ערכיות בלבד. לעומת זאת, כל פונקציה שנבחרת לפי ν היא ממרחק $\frac{1}{2}$ מלהיות דו-חד-ערכית: כל רביעיה שנקבע עבורה ערך יחיד יחיד מצריכה שינוי של לפחות שניים מארבעת האיברים שלה על מנת שלא יהיו יותר משני איברים עם אותו ערך. לעומת זאת, רביעיה שנקבעו עבורה ארבעה ערכים מבטיחה שיש ארבעה ערכים שמופיעים רק פעם אחת בפונקציה (הערכים שלה לא יכולים להופיע ברביעיות אחרות). אם היו בסה"כ l רביעיות מהסוג השני, אז צריך לשנות

לפחות $2l$ מתוך $4l$ הערכים המתאימים של f על־מנת שלא יהיו ערכים כאלה (בכל שינוי בודד אפשר לכל היותר להפוך ערך אחד ללא־קיים, וערך שני לזוה שמופיע פעמיים). זה מתוסף ל־ $n - 2l$ הערכים שצריך לשנות עבור $n/2 - l$ הרביעיות מהסוג הראשון, לקבלת n שינויים סה"כ.

עתה נניח ש־ $Q \subset \{1, \dots, 2n\}$ היא קבוצה מגודל שאינו עולה על $n^{2/3}$, וננתח את הסיכוי שקיים C_k כל שהוא שעבורו $|Q \cap C_k| > 2$. נשתמש באיחוד מאורעות. עבור שלישייה של איברים T שנבחרת יוניפורמית, הסיכוי שתהיה מוכלת ב־ Q הוא $\frac{1}{8n} < \frac{\binom{|Q|}{3}}{\binom{2n}{3}}$. אפשר להסתכל על כל רביעיה כעל בחירה של ארבע שלישיות, שנבחרות לא באופן ב"ת זו בזו, אבל כל אחת מהן כן נבחרת באופן יוניפורמי כאשר לא מתנים אותה על האחרות. על כן לפי איחוד מאורעות, לכל רביעיה C_k ההסתברות עבור $|Q \cap C_k| > 2$ חסומה ע"י $\frac{1}{2n}$, וההסתברות שקיימת רביעיה כל שהיא שעבורה $|Q \cap C_k| > 2$ חסומה ע"י $\frac{1}{4}$.

עתה נראה שכאשר מתנים על המאורע שלא קיים C_k שעבורו $|Q \cap C_k| > 2$, ההתפלגויות $\nu|_Q$ ו־ $\tau|_Q$ זהות, דבר הגורר את החסם על ההתפלגויות הלא־מותנות של $d(\tau|_Q, \nu|_Q) < \frac{1}{4}$, שממנו מקבלים את החסם התחתון המבוקש על ϵ בדיקה לכל $\frac{1}{2} < \epsilon$. אנחנו נראה את השוויון בין שתי ההתפלגויות על כל התניה אפשרית על זהות הקבוצות $Q \cap C_1, \dots, Q \cap C_{n/2}$, ובלבד שכולן בנות שני איברים לכל היותר.

בהינתן הקבוצות $Q \cap C_1, \dots, Q \cap C_{n/2}$, נזכור שהגרלת ערכי f בוצעה באופן ב"ת לכל C_k בנפרד, ולכן מספיק להוכיח שלכל k יש זהות בין ההתפלגויות $\nu|_{Q \cap C_k}$ ו־ $\tau|_{Q \cap C_k}$ כאשר מתנים אותן על זהות $Q \cap C_k$. במקרה ש־ $Q \cap C_k = \emptyset$ אין מה להוכיח. במקרה שגודל החיתוך הוא 1, נסמן $Q \cap C_k = \{v_k\}$, ונשים לב ש־ $f(v_k)$ מתפלג באופן יוניפורמי מתוך $\{4k-3, 4k-2, 4k-1, 4k\}$. על־מנת להראות את זה צריך לעבור על כל המקרים. עבור $\nu|_{Q \cap C_k}$, גם אם בחרנו את f להיות בעלת ערך יחיד שנבחר מהקבוצה הנ"ל, וגם אם בחרנו את $f|_{C_k}$ להיות התאמה מקרית ל־ $\{4k-3, 4k-2, 4k-1, 4k\}$, התפלגות הערך v_k תהיה יוניפורמית מבין ארבעת האפשרויות. עבור $\tau|_{Q \cap C_k}$, נשים לב כי גם ההתפלגות הלא־מותנה של i_k (שיתקבל אם $v_k \in P_k$) וגם ההתפלגות הלא־מותנה של j_k (שיתקבל אם $v_k \in C_k \setminus P_k$) הן יוניפורמיות.

עתה נעבור למקרה האחרון, גודל חיתוך של 2, ונסמן $Q \cap C_k = \{v_k, w_k\}$. ראשית ננתח את $\tau|_{Q \cap C_k}$ בהסתברות $\frac{1}{3}$ יתקיים או $\{v_k, w_k\} \subset P_k$ או $\{v_k, w_k\} \subset Q_k \setminus P_k$, ואז $f(v_k)$ ו־ $f(w_k)$ יהיו שניהם שווים לערך אחד שנבחר יוניפורמית מ־ $\{4k-3, 4k-2, 4k-1, 4k\}$. בהסתברות $\frac{2}{3}$ יתקיים המקרה השני, $|\{v_k, w_k\} \cap P_k| = 1$, ואז $f(v_k), f(w_k)$ יהיו שני ערכים שונים מ־ $\{4k-3, 4k-2, 4k-1, 4k\}$. שנבחרים יוניפורמית מבין 12 האפשרויות. כשנעבור לניתוח של $\nu|_{Q \cap C_k}$, נראה בדיוק את אותה ההתפלגות. בהסתברות $\frac{1}{3}$ ערכי $f(v_k), f(w_k)$ יהיו שווים לערך בודד שנבחר יוניפורמית (כאשר בחרנו לתת את אותו הערך לכל C_k), ובהסתברות $\frac{2}{3}$ אלו יהיו שווים לשני ערכים שונים שנבחרו יוניפורמית מהאפשרויות (כאשר בחרנו ש־ f תקבל את כל ארבעת הערכים השונים עבור C_k).

מותר להציץ

מכיוון שאנחנו בודקים יוניפורמיות, אפשר לדחות את הקלט מיידית ברגע שאנחנו מקבלים דגימה A_i שעבורה $\mu(A_i) \neq \frac{1}{n}$ (כזכור לפי תנאי השאלה אנחנו מקבלי גם את ערכי μ עבור הדגימות שלנו). אנחנו נשתמש באלגוריתם הבא: עבור q שנבחר בהמשך, ניקח את הדגימות A_1, \dots, A_q ונבדוק את $\mu(A_1), \dots, \mu(A_q)$. אנחנו נדחה אם קיים i שעבורו $\mu(A_i) \neq \frac{1}{n}$, ואחרת נקבל.

זה ברור שההתפלגות היוניפורמית תתקבל בהסתברות 1. עבור ניתוח התפלגות רחוקה מיוניפורמית, כאשר מסמנים את ההתפלגות היוניפורמית ב־ π , נרשום עבור המרחק בין ההתפלגויות:

$$d(\mu, \pi) = \frac{1}{2} \sum_{i=1}^n |\mu(i) - \frac{1}{n}| = \sum_{i:\mu(i) > 1/n} (\mu(i) - \frac{1}{n}) \leq \sum_{i:\mu(i) > 1/n} \mu(i) = \Pr_\mu[\mu(i) > \frac{1}{n}] \leq \Pr_\mu[\mu(i) \neq \frac{1}{n}]$$

יוצא בפרט שלכל i , הסיכוי לדחות התפלגות שהיא ϵ ־רחוקה מיוניפורמית בגלל $\mu(A_i)$ הוא לפחות ϵ . לכן בחירה (למשל) של $q = \lceil \frac{2}{\epsilon} \rceil$ תתן לנו הסתברות כוללת גדולה מ־ $\frac{2}{3}$ לדחות התפלגות כזו.