פתרונות לתרגיל הראשון

אותו דבר והיינו הך

ננתח את ההתפלגות השניה, זו שמבוססת על הפונקציה המקרית $f : \{1, \ldots, n\} \to [0, 1]$. ראשית נשים לב שאם אין $i < j$ עבורם $f(i) = f(j)$, אז ה־σ_f המתקבלת היא באמת פרמוטציה: במקרה כזה לא קשה לראות שאם $f(i_1) < f(i_2)$ אז $\sigma_f(i_1) < \sigma_f(i_2)$, בגלל ש־$\{j : f(j) \leq f(i_1)\}$ מוכלת ממש ב־$\{j : f(j) \leq f(i_2)\}$. כמו כן נשים לב שהסיכוי שיהיו $i < j$ כל שהם עם שוויון בערכי f הוא אפס (ההוכחה היא תרגיל בסיסי בתורת המידה, לכל $i < j$ מתאימים אפשר "לכסות" את קבוצת הערכים האפשריים עם שוויון ע"י מלבנים עם סכום נפחים קטן כרצוננו; עם זאת לא התבקשתם לספק הוכחה כזו).

עתה נטפל במקרים ללא שוויון. נסמן ב־$\mathrm{Im}(f)$ את תמונת הפונקציה f. במקרה שלנו $|\mathrm{Im}(f)| = n$. עבור פרמוטציה τ, נסמן ב־$f \circ \tau$ את הפונקציה המוגדרת לפי $(f \circ \tau)(i) = f(\tau(i))$ (בעצם הרכבת פונקציות רגילה). הדבר לשים לב הוא שמתקיים $\sigma_{f\circ\tau}(i) = \sigma_f(\tau(i))$, או במילים אחרות $\sigma_{f\circ\tau} = (\sigma_f) \circ \tau$. כמו כן לכל τ מתקיים שההתפלגות על $f \circ \tau$ זהה לזו של f (לפי הבחירה הב"ת של כל ערכי f), ולכן לכל σ ו־τ מתקיים $\Pr[\sigma_f = \sigma] = \Pr[\sigma_{f\circ\tau} = \sigma \circ \tau] = \Pr[\sigma_f = \sigma \circ \tau]$, ומכאן שכל הפרמוטציות הן שוות הסתברות, כנדרש.

הערה: מי שטען במקום זאת שלכל קבוצה $A \subset [0, 1]$ מגודל n ולכל פרמוטציה σ ההתפלגות מקיימת $\Pr[\sigma_f = \sigma | \mathrm{Im}(f) = A] = 1/n!$ גם קיבל את הנקודות על השאלה, אפילו אם לא סיפק את ההוכחה לכך (אפשר להוכיח זאת ישירות ע"י אינטגרלים; היה עדיף להיזהר עם טיעוני "סימטריה" כאן אפילו שהיינו די קלים גם בקבלת תשובות כאלה).

קשה לכסות

נגריל באופן יוניפורמי וב"ת תתי קבוצות $B^{(j)} \subseteq \{1, \ldots, n\}$ תחת התנאי ש־$|B^{(j)}|$ הוא אי־זוגי (לכל תת־קבוצה יש 2^{n-1} אפשרויות, וסה"כ יש $2^{(n-1)k}$ אפשרויות לסדרה $B^{(1)}, \ldots, B^{(k)}$, שכל אחת מהן מתקיימת בהסתברות שווה). נסמן את המכפלה הקרטזית $B = \prod_{j=1}^{k} B^{(k)} \subseteq \{1, \ldots, n\}^k$. נשים לב שבפרט $|B| = \prod_{j=1}^{k} |B^{(k)}|$ הוא אי־זוגי תמיד. אם $\bigcup_{i=1}^{m} A_i = \{1, \ldots, n\}^k$, אז $|B \cap \bigcup_{i=1}^{m} A_i| = |B|$ הוא אי־זוגי תמיד. מצד שני תמיד מתקיים $|B \cap \bigcup_{i=1}^{m} A_i| = \sum_{i=1}^{m} |B \cap A_i| = \sum_{i=1}^{m} \prod_{j=1}^{k} |B^{(j)} \cap A_i^{(j)}|$ כי הקבוצות $A_1, \ldots, A_m$ זרות לפי נתוני השאלה.

נראה עבור i קבוע שמתקיים ש־$\prod_{j=1}^{k} |B^{(j)} \cap A_i^{(j)}|$ יהיה אי־זוגי בהסתברות 2^{-k}. מכך נובע שאם $m < 2^k$ אז בהתסברות חיובית כל הערכים $|B \cap A_i|$ הם זוגיים, ולכן גם $|B \cap \bigcup_{i=1}^{m} A_i|$ זוגי, אבל כזכור זה אינו יכול לקרות בהסתברות חיובית אם מתקיים $\bigcup_{i=1}^{m} A_i = \{1, \ldots, n\}^k$.

לשם כך נשים לב שכאשר $A_i^{(j)}$ אינו שווה ל־$\{1, \ldots, n\}$ (כפי שאכן נתון בשאלה), אז $|B^{(j)} \cap A_i^{(j)}|$ יהיה אי־זוגי בהסתברות $\frac{1}{2}$ בדיוק (החיתוך יהיה תת קבוצה מקרית יוניפורמית של $A_i^{(j)}$; אנחנו מתעלמים מהמקרה שהקבוצה A_i ריקה כי את אלו אפשר פשוט למחוק מהרשימה). מכיוון שה־$B^{(j)}$ נבחרות באופן ב"ת, זה אומר שהסיכוי ש־$\prod_{j=1}^{k} |B^{(j)} \cap A_i^{(j)}|$ יהיה אי־זוגי לכל ה־j הוא 2^{-k}. על מנת שהמכפלה $\prod_{j=1}^{k} |B^{(j)} \cap A_i^{(j)}|$ תהיה אי־זוגית צריך שכל האיברים יהיו אי־זוגיים, ז"א שהסיכוי לכך הוא גם 2^{-k}.

הולכים במעגלים

ראשית נניח שמתקיים $k < n/10$. אחרת חישוב פשוט מראה שיש לפחות $n/20$ מעגלים מגודל שאינו עולה על 20 (כי סכום אורכי כל המעגלים הוא n), ואז אפשר פשוט להגריל באופן יוניפורמי קבוצה של 40 אינדכסים ולבדוק לכל אחד מהם האם הוא במעגל באורך 20 או פחות (ע"י חישוב הערכים $\sigma(v), \sigma(\sigma(v)), \ldots$, **20** פעמים), וסה"כ יש לנו מספר קבוע של קריאות של ערכי σ (לא הורדנו נקודות למי שהתעלם ממקרה זה בתשובה שלו).

מכיוון שסכום גודלי כל המעגלים בפירוק (כולל "מעגלים מאורך **1**") הוא בדיוק n, אם יש לפחות k מעגלים, אז חישוב פשוט אומר שיש לפחות $k/2$ מעגלים שגודלם אינו עולה על $2n/k$. עבור $0 \leq j \leq \log(2n/k)$, נסמן ב־m_j את מספר המעגלים שגודלם בין 2^j ל־$2^{j+1}-1$. סכום ה־m_j הנ"ל הוא לפחות $k/2$, ומצד שני יש לא יותר מ־$2\log(n/k)$ $\lfloor \log(2n/k) \rfloor + 1$ ערכים אפשריים עבור j. לכן קיים j_* שעבורו $m_{j_*} \geq k/4\log(n/k)$.

האלגוריתם יעבוד כך: נבחר לכל $0 \leq j \leq \log(2n/k)$ באופן מקרי, יוניפורמי וב"ת $10\log(n/k)n/k2^j$ אינדכסים (עם חזרות, ז"א שמרשים שאותו אינדכס ייבחר יותר מפעם אחת). לכל אינדכס v שנבחר עבור ה־j הנ"ל, נבדוק האם הוא במעגל מגודל קטן מ־2^{j+1} ע"י קריאת $\sigma(v), \sigma(\sigma(v)), \sigma^3(v), \ldots, \sigma^{2^{j+1}}(v)$. סה"כ עבור כל ערך נתון של j אנחנו מבצעים $10 \cdot 2^{j+1}\log(n/k)n/k2^j = O((n/k)\log(n/k))$ קריאות של ערכי σ, וסה"כ לכל ערכי j שאנחנו בודקים אנחנו מבצעים $O((n/k)(\log(n/k))^2)$ קריאות של ערכי σ.

על מנת לסיים צריך להראות שהאלגוריתם מוצא מעגל בהסתברות לפחות $\frac{1}{2}$. אנחנו נראה שזה קורה בסבב הבדיקה של $j = j_*$ (האלגוריתם בודק את כל ערכי j האפשריים כי הוא לא יודע את j_* מראש). במקרה כזה, הסיכוי שלא בחרנו אף אינדכס שנמצא במעגל שגודלו בין 2^{j_*} ל־$2^{j_*+1}-1$ הוא לכל היותר $(1-2^{j_*}m_{j_*}/n)^{10\log(n/k)n/k2^{j_*}} < \frac{1}{2}$. הסבר לביטוי: מספר האינדכסים הכולל במעגלים עם הגדלים הנ"ל הוא לפחות $2^{j_*}m_{j_*}$, ולכן הסיכוי לא למצוא אינדכס כזה חסום ע"י $(1-2^{j_*}m_{j_*}/n)^{10\log(n/k)n/k2^{j_*}}$ כי בחרנו כל אינדכס באופן ב"ת. בהצבת החסם על m_{j_*} תוך שימוש באי השוויון $(1-x) \leq e^{-x}$ מתקבל המבוקש. ברגע שמצאנו לפחות אינדכס אחד כזה, אנחנו אכן נגלה שגודל המעגל המכיל אותו קטן מ־2^{j_*+1}, כי את הבדיקה הזו עשינו באופן דטרמיניסטי לכל אחד מהאינדכסים שנבחרו.

פתרונות לתרגיל השני

משחק בכובעים

נגריל באופן יוניפורמי וב"ת לכל איש את צבע הכובע שלו, שנסמנו ב־$c_i \in \{1,\ldots,k\}$ עבור $1 \le i \le n$. כמו כן נסמן את האסטרטגיה של האיש ה־i (כזכור זו פונקציה שתלויה רק בצבעי הכובעים של האחרים) ב־$f_i : \{1,\ldots,k\}^{n-1} \to \{1,\ldots,k\}$. השלב הבא זה להוכיח שהאיש ה־i ינחש נכון את הצבע של הכובע שלו בהסתברות $\frac{1}{k}$ בלבד, או בסימון מתמטי, $\Pr[c_i = f_i(c_1,\ldots,c_{i-1},c_{i+1},\ldots,c_n)] = \frac{1}{k}$. זה נובע ישירות מאי התלות של בחירת c_i בצבעים האחרים, ולכן גם בפונקציה f_i שלהם. לשם המחשה נכתוב הוכחה כאן, למרות שמספיק היה לציין את אי התלות הנ"ל ללא הוכחה מפורטת.

$$\Pr[c_i = f_i(c_1,\ldots,c_{i-1},c_{i+1},\ldots,c_n)] = \sum_{j=1}^{k} \Pr[c_i = f_i(c_1,\ldots,c_{i-1},c_{i+1},\ldots,c_n) = j]$$

$$= \sum_{j=1}^{k} \sum_{f_i(j_1,\ldots,j_{i-1},j_{i+1},\ldots,j_n)=j} \Pr[c_i = j, c_1 = j_1,\ldots,c_{i-1} = j_{i-1}, c_{i+1} = j_{i=1},\ldots,c_n = j_n]$$

$$= \sum_{j=1}^{k} \sum_{f_i(j_1,\ldots,j_{i-1},j_{i+1},\ldots,j_n)=j} \frac{1}{k} \cdot \Pr[c_1 = j_1,\ldots,c_{i-1} = j_{i-1}, c_{i+1} = j_{i=1},\ldots,c_n = j_n] = \frac{1}{k}$$

עכשיו אפשר לסיים: אם נסמן ב־X_i את משתנה האינדיקטור עבור המאורע שהאיש ה־i ניחש נכון, וב־$X = \sum_{i=1}^{n} X_i$ את המשתנה של מספר האנשים הכולל שניחשו נכון, אז לפי לינאריות התוחלת מתקיים $\mathrm{E}[X] = \frac{n}{k}$. לכן יש בחירת כובעים ספציפית שעבורה $X \le \frac{n}{k}$, ומכיוון שמשתנה זה מקבל ערכים שלמים בלבד אז מתקיים עבור בחירה ספציפית זו $X \le \lfloor \frac{n}{k} \rfloor$.

רב־קרב תרנגולים

נראה מה מתרחש בסוף סיבוב הניקורים הראשון: כל תרנגול ישאר בריא בהסתברות $\frac{1}{4}$, שזו ההסתברות לשני המאורעות הב"ת שגם התרנגול מימינו וגם התרנגול משמאלו לא ניקרו אותו. תרנגול יהפוך להיות בריא ובטוח אם גם לא ניקרו אותו, וגם בצד של התרנגול שהוא עצמו לא ניקר, השכן של השכן בחר כן לנקר את השכן. על כן יש הסתברות של $\frac{1}{8}$ להיות בריא ובטוח, והסתברות של $\frac{1}{8}$ להיות בריא ולא בטוח. מלינאריות התוחלת, תוחלת מספר התרנגולים הבריאים הבטוחים היא $n/8$, וזו גם תוחלת מספר התרנגולים הבריאים הלא־בטוחים.

נשים לב עתה שלאחר סיבוב אחד בכל מקרה לכל תרנגול יהיה שכן מנוקר (השכן שהוא עצמו ניקר). על כן, כל התרנגולים הבריאים הלא־בטוחים יהיו בזוגות זה ליד זה, ללא שכנים בריאים אחרים. מספר הוא בדיוק חצי ממספר התרנגולים המעורבים, ולכן התוחלת שלו היא $n/16$. עתה נרצה לחשב את תוחלת מספר התרנגולים ששורדים בסוף כל הסיבובים מבין הזוגות האלו. לכל זוג בודד מתקיים עתה תהליך זהה לזה של השאלה "דו־קרב תרנגולים", כי בכל סיבוב כל תרנגול יבחר באופן ב"ת האם לנקר את חברו לזוג, או את שכנו השני, המנוקר כבר ממילא. מכיוון שבדף הפתרונות הזה מובא גם הפיתרון של השאלה הנ"ל, נשתמש בו גם כאן, ונציין שעבור כל זוג, הסיכוי שיישאר ממנו תרנגול בריא הוא $2/3$. על כן תוחלת מספר התרנגולים שהיו בריאים לא־בטוחים ונשארו בריאים עד סוף המשחק היא $2/3 \cdot n/16 = n/24$. על כן תוחלת מספר כל התרנגולים הבריאים (ע"י חיבור תוחלות שני המ"מ) היא $n/8 + n/24 = n/6$.

דו־קרב תרנגולים

הפיתרון היותר אלגנטי משתמש בהסתברות מותנית (האופציה השניה היא פשוט לחשב סכום של טור חזקות). המשחק נעצר לאחר סיבוב שיש בו ניקור אחד או יותר, ומכיוון שיש הסתברות קבועה כזו לכל סיבוב, בהסתברות 1 יהיה לבסוף סיבוב כזה. לכל j נרצה לדעת את ההסתברות שנשאר תרנגול בריא בסוף סיבוב זה, כאשר מותנים אותה על המאורע שזהו הסיבוב הראשון (ולכן היחידי) שבוצע בו ניקור. ההסתברויות לאפשרויות בסיבוב ה־j אינן תלויות בסיבובים הקודמים, ז"א שכל אחת מארבעת האפשרויות לפעולות של שני התרנגולים קורית בהסתברות $1/4$. עם זאת, אנחנו מתנים עתה על כך שהיה ניקור, ז"א שיש לנו שלוש אפשרויות שוות הסתברות, שבשתיים מתוכן נשאר תרנגול בריא. על כן קיבלנו סיכוי של $2/3$ שנותר תרנגול כזה, ומכיוון שזה נכון לכל התנייה על j, זוהי גם ההסתברות הלא־מותנה של המאורע.

פתרונות לתרגיל האחרון

דו־קרב תרנגולים עייפים

הפיתרון כאן דומה לפיתרון עבור השאלה "דו־קרב תרנגולים" מהתרגיל הקודם, רק שצריך ניתוח דו־שלבי. ראשית ננתח את ההסתברויות המותנות עבור הסיבוב הראשון שבו לפחות אחד התרנגולים עושה משהו (מנקר או הולך לישון). ההסתברות ששני התרנגולים הולכים לישון בו־זמנית הוא $1/9$, אבל אם מתנים אותה על ההסתברות שלפחות אחד התרנגולים עושה משהו (מאורע בהסתברות $8/9$) אז מקבלים הסתברות מותנה של $1/8$. כמו כן, בהסתברות מותנה של $1/4$, בסיבוב הראשון שבו נעשית פעולה, אחד התרנגולים ילך לישון והתרנגול השני לא יעשה כלום. שאר המאורעות האפשריים עבור הסיבוב הראשון שבו נעשית פעולה מסתיימים בלפחות תרנגול אחד מנוקר, ולכן אלו לא יתרמו להסתברות שאנחנו מחשבים.

אם בסיבוב הראשון שבו נעשתה פעולה נשארנו עם תרנגול אחד עירני ותרנגול אחד ישן, אז ננתח את הסיבוב הבא שבו נעשית פעולה. כאן ההסתברות המותנה שהתרנגול העירני הלך לישון היא $1/2$ (והאפשרות השניה היא שהתרנגול העירני ניקר את התרנגול הישן). סה"כ ההסתברות שבסוף כל התהליך נשארנו עם שני תרנגולים בריאים ישנים היא $1/8 + 1/4 \cdot 1/2 = 1/4$.

תלויים באופן טוב

אפשרות אחת היא לפתוח את ההוכחה של אי השוויון על חסימת סטיות גדולות, יחד עם טיעון של "תלות בכל ערך אפשרי" בדומה להוכחה של אי־שוויון אזומה. להרחבת האופקים נראה כאן טיעון מבוסס צימוד.

נבנה כאן סדרה שניה של משתנים $Y_1, \ldots, Y_m$, תלויים ב־$X_1, \ldots, X_m$, שתקיים את הדברים הבאים: לכל i מתקיים $X_i \leq Y_i$ (בהסתברות 1), וכן $Y_1, \ldots, Y_m$ בלתי תלויים לחלוטין זה בזה. על כן מתקיים $\sum_{i=1}^m X_i \leq \sum_{i=1}^m Y_i$ תמיד, ואת ההסתברות עבור $\sum_{i=1}^m Y_i > a$ חוסמים ע"י חסימת סטיות גדולות רגילה.

לאחר שערכי $X_1, \ldots, X_m$ הוגרלו, נגריל את ערכי ה־Y_i באינדוקציה: בהינתן $Y_1, \ldots, Y_{i-1}$, אם $X_i = 1$ אז נקבע $Y_i = 1$ בהסתברות 1. אם $X_i = -1$, אז נחשב את $\alpha_i = \Pr[X_i = 1 | X_1, \ldots, X_{i-1}]$ לפי הערכים שכבר הגרלנו ל־$X_1, \ldots, X_{i-1}$. עתה נבחר $Y_i = 1$ בהסתברות $(\frac{1}{2} - \alpha_i)/(1 - \alpha_i)$ (לפי נתוני השאלה תמיד $\alpha_i \leq \frac{1}{2}$), ונבחר $Y_i = -1$ בהסתברות $\frac{1}{2}/(1 - \alpha_i)$. מההגדרה ברור מיידית שתמיד יתקיים $X_i \leq Y_i$. חישוב מיידי יראה גם שלכל סדרת ערכים של $X_1, \ldots, X_{i-1}$ ושל $Y_1, \ldots, Y_{i-1}$, מתקיים $\Pr[Y_i = 1 | Y_1, \ldots, Y_{i-1}] = \frac{1}{2}$. לכן $\Pr[Y_i = 1 | Y_1, \ldots, Y_{i-1}, X_1, \ldots, X_{i-1}] = \frac{1}{2}$, ומכאן אפשר להראות באינדוקציה ש־$Y_1, \ldots, Y_m$ בלתי־תלויים (כל סדרת ערכים אפשרית תתקבל בהסתברות 2^{-m} בדיוק).

מספרים מכוסים

נניח ש־$C : \{1, \ldots, n\} \to \{1, \ldots, n\}$ תסמן את סדרת n המספרים שבחרנו, ונסמן ב־$f(C)$ את הפונקציה שאומרת כמה מספרים נבחרו לפחות k פעמים. ראשית נחסום את התוחלת שלה: לכל מספר $1 \leq i \leq n$, הסיכוי ש־i נבחר לפחות k פעמים הוא לפחות הסיכוי ש־i נבחר בדיוק k פעמים, שהוא $\binom{n}{k} n^{-k} (1 - \frac{1}{n})^{n-k}$, שכל מה שמעניין אותנו זה שעבור $n > k$ הביטוי חסום מלמטה ע"י קבוע מתאים β_k (עבור k קבוע הביטוי הזה שואף ל־$1/ek!$). אפשר לראות את $f(C)$ כסכום של n משתני האינדיקטור עבור כל $1 \leq i \leq n$, ולכן מלינאריות התוחלת $\mathrm{E}_C[f(C)] \geq \beta_k n$.

עתה נבנה מרטינגל חשיפה של $f(C)$ כאשר חושפים את C איבר־איבר, ז"א $\mathcal{D}_i = \{1, \ldots, i\}$. לא קשה לראות שהפונקציה הזו היא ליפשיץ ביחס לחשיפה, ז"א ששינוי של C במקום אחד משנה את כמות המספרים שמופיעים לפחות k פעמים בלא יותר מאחד (השינוי יכול רק להוסיף או להוציא מספר בודד מהרשימה הזו). מכאן שגם המרטינגל $X_0, \ldots, X_m$ מקיים $|X_i - X_{i-1}| \leq 1$, ולכן לפי אי שוויון אזומה מתקיים $\Pr[f(C) = 0] \leq \Pr[f(C) \leq \mathrm{E}[f(C)] - \beta_k n] \leq e^{-\beta_k^2 n/2}$.

פרמוטציות מעורבבות

נבנה מרטינגל חשיפה איבר־איבר של הפרמוטציה σ, עבור הפונקציה $M(\sigma)$. נשים לב שמספיק להסתכל על $X_0, \ldots, X_{n-1}$, כי אחרי שחשפנו את ערכי הפרמוטציה σ על $\{1, \ldots, n-1\}$ אנחנו כבר ממילא יודעים גם את $\sigma(n)$. הכוונה היא להשתמש באי־שוויון אזומה על מנת לחסום את ההסתברות למרחק גדול בין X_{n-1} (שמתפלג כמו $M(\sigma)$) לבין $X_0 = \mathrm{E}_\sigma[M(\sigma)]$. ראשית נחשב את התוחלת: עבור $i < j$, נגדיר את Y_{ij} להיות משתנה האינדיקטור עבור $\sigma(i) > \sigma(j)$. נשים לב ש־$M(\sigma)$ הוא סכום כל משתני האינדיקטור, וכן ש־$\Pr[Y_{ij}] = \frac{1}{2}$. לכן מלינאריות התוחלת $\mathrm{E}[M(\sigma)] = \frac{1}{2}\binom{n}{2}$.

על מנת לחסות את $|X_i - X_{i-1}|$, נשים לב שאם σ' מתקבלת מ־σ ע"י החלפת הערכים $\sigma(i), \sigma(j)$ עבור $i < j$, אז ההפרש $|M(\sigma) - M(\sigma')|$ חסום ע"י $2(j-i) - 1$. זאת מכיוון שהזוגות המושפעים בחילוף הם i, j וכן i, k ו־k, j לכל $i < k < j$. אם משתמשים בלמה מהתרגול, ובעובדה שהערך הנ"ל חסום ע"י $2n$, מקבלים $|X_i - X_{i-1}| < 2n$ לכל $0 < i < n$, ואז ניתן להפעיל את אי־שוויון אזומה לקבלת המבוקש.

אם רוצים לקבל את החסם היותר חזק, אז משתמשים בלמה הבאה שההוכחה שלה זהה לחלוטין להוכחה הלמה מהתרגול: אם הפונקציה הנחשפת, $M(\sigma)$ במקרה שלנו, מקיימת לכל $i < j$ ולכל σ ו־σ' המתקבלת ממנה ע"י החלפת הערכים $\sigma(i), \sigma(j)$ את החסם $|M(\sigma) - M(\sigma')| \leq c_i$, אז המרטינגל מקיים $|X_i - X_{i-1}| \leq c_i$ לכל i. במקרה שלנו זה מתקיים עבור $c_i = 2(n-i) - 1$.

לא חוזרים לאחור

השיטה הכי טובה היא לנתח התפלגויות של $X_{i-1}X_i$ כזוגות מסודרים של צמתים. נראה באינדוקציה על i שההתפלגות הזו (כשאינה מותנה על משתנים אחרים) היא יוניפורמית מעל $2|E|$ הכיוונים האפשריים של הקשתות של G (לכל קשת יש שני סידורים של הצמתים שלה). מזה נובע בפרט שההתפלגות הלא־מותנה של X_i היא זו המתוארת בשאלה.

הבסיס הוא הזוג X_0X_1, וזה נובע מההגדרה: לכל u, v שהם שני צמתי קצה של קשת של G, מתקיים $\Pr[X_0 = u, X_1 = v] = \frac{d(v)}{2|E|} \cdot \frac{1}{d(v)} = \frac{1}{2|E|}$.

עבור המעבר, נניח שההנחה מתקיימת עבור $X_{i-1}X_i$, ונראה שהיא מתקיימת עבור X_iX_{i+1}. נניח ש־u, v הם שני צמתי קצה של קשת מ־G. אלו יכולים להיות הערכים של X_i, X_{i+1} אך ורק אם מתקיים $X_i = u$ אולם לא מתקיים $X_{i-1} = v$ (בגלל תנאי החוסר חזרה לאחור). ישנם $d-1$ שכנים של u ששונים מ־v. לכל שכן w כזה, לפי הנחת האינדוקציה $\Pr[X_{i-1} = w, X_i = v] = \frac{1}{2|E|}$, ואלו מאורעות זרים. כמו כן, לכל w כזה מתקיים $\Pr[X_{i+1} = v | X_{i-1} = w, X_i = u] = \frac{1}{d-1}$, לפי הגדרת ההילוך חסר החזרות. מכאן ניתן לסיים ע"י חוק בייז, ואיחוד המאורעות הזרים ש־X_{i-1}, X_i, X_{i+1} שווים בהתאמה ל־w, u, v (עבור כל w מתאים).

גן השבילים המתפצלים

נגדיר את $X_0, \ldots, X_k$ להיות הילוך מקרי ללא חזרות לאחור, בדיוק כמו בשאלה הקודמת. מהשאלה הזו נובע שאז ההתפלגות הלא מותנה על X_k נתונה ע"י $\Pr[X_k = v] = \frac{d(v)}{2|E|}$. עתה נבדוק מהי האנטרופיה המותנית $\mathrm{H}[X_1, \ldots, X_k | X_0]$.

מצד אחד, בגלל שאין מעגלים מגודל קטן מ־$2k+1$, אם אנחנו יודעים את X_0 ואת X_k, אז אנחנו בהכרח יודעים גם את $X_1, \ldots, X_2$ (עבור X_0, X_k לגיטימים יהיה מסלול יחיד מאורך k ביניהם). על כן מתקיים $\mathrm{H}[X_1, \ldots, X_k | X_0] = \mathrm{H}[X_k | X_0] \leq \mathrm{H}[X_k] \leq \log(n)$.

מצד שני, נשתמש בכלל השרשרת לקבלת $\mathrm{H}[X_1, \ldots, X_k | X_0] = \sum_{i=1}^{k} \mathrm{H}[X_i | X_0, \ldots, X_{i-1}]$. כמו כן, מכיוון שאופן ההגרלה של X_i תלוי אך ורק בערך של X_{i-1}, מתקיים $\mathrm{H}[X_i | X_0, \ldots, X_{i-1}] = \mathrm{H}[X_i | X_{i-1}]$. הוכחה מהירה של הטענה הזו (בבדיקה לא ירדו נקודות על שימוש ללא הוכחה):

$$\begin{aligned}\mathrm{H}[X_i|X_0,\ldots,X_{i-1}] &= \sum_{\alpha_0,\ldots,\alpha_{i-1}} \mathrm{H}[X_i|X_0=\alpha_0,\ldots,X_{i-1}=\alpha_{i-1}]\Pr[X_0=\alpha_0,\ldots,X_{i-1}=\alpha_{i-1}] \\ &= \sum_{\alpha_0,\ldots,\alpha_{i-1}} \mathrm{H}[X_i|X_{i-1}=\alpha_{i-1}]\Pr[X_0=\alpha_0,\ldots,X_{i-1}=\alpha_{i-1}] \\ &= \sum_{\alpha_{i-1}} \mathrm{H}[X_i|X_{i-1}=\alpha_{i-1}]\Pr[X_{i-1}=\alpha_{i-1}] = \mathrm{H}[X_i|X_{i-1}]\end{aligned}$$

עתה נחסום את המחוברים לפי ההגדרה של אנטרופיה מותנית כממוצע של אנטרופיות מותנות על ערכים ספציפים.

מחובר ראשון: $\mathrm{H}[X_1|X_0] = \sum_{v\in V}\log(d(v))\cdot\frac{d(v)}{2|E|} = \frac{n}{2|E|}\cdot\frac{1}{n}\sum_{v\in V}d(v)\log(d(v))$ **ובהפעלת אי־שוויון ינסן** Jensen **על הפונקציה** $f(z)=z\log(z)$ **מקבלים** $\mathrm{H}[X_1|X_0]\geq\frac{n}{2|E|}d\log(d)=\log(d)$, **כאשר כזכור** $d=\frac{1}{n}\sum_{v\in V}d(v)$, **"תוחלת הדרגה" מעל בחירה יוניפורמית של צומת.**

עבור המחובר $\mathrm{H}[X_i|X_{i-1}]$ **כאשר** $1<i\leq k$, **מפתחים באופן דומה, כשהפעם אי שוויון ינסן מופעל על הפונקציה** $f(z)=z\log(z-1)$ **(שימו לב שעבור** $z\geq 2$ **הנגזרת השניה של הפונקציה היא** $\frac{1}{z-1}-\frac{1}{(z-1)^2}\geq 0$**):**
$\mathrm{H}[X_i|X_{i-1}] = \sum_{v\in V}\log(d(v)-1)\cdot\frac{d(v)}{2|E|}\geq\frac{n}{2|E|}d\log(d-1)=\log(d-1)$.

סה"כ קיבלנו כאן $\mathrm{H}[X_1,\ldots,X_k|X_0]\geq\log(d)+k\log(d-1)$. **יחד עם אי השוויון הראשון (זה שחוסם מלמעלה) נקבל** $\log(d)+k\log(d-1)\leq\log(n)$, **והעלאת חזקה בשני האגפים תתן לנו את המבוקש.**