פתרונות לתרגיל הראשון

הילוך על המעגל

יהי T המשתנה המקרי של זמן ריצת האלגוריתם. ראשית נשים לב שלכל $i \geq 1$ מתקיים שאם האלגוריתם לא עצר עד סוף הצעד $n(i-1)$, אז הסיכוי שהוא לא יעצור גם עד סוף הצעד ה־ni חסום ע"י $1-2^{-n}$ (אם בכל n הצעדים המונה הוגדל, אז האלגוריתם בטוח יעבור במהלכם דרך מספר המתחלק ב־n). לכן $\Pr[T > ni | T > n(i-1)] \leq 1-2^{-n}$ ובאינדוקציה $\Pr[T > ni] \leq (1-2^{-n})^i$. החסם על התוחלת מתקבל בצורה הבאה:

$$\mathrm{E}[T] = \sum_{i=1}^{\infty} i\Pr[T=i] = \sum_{i=1}^{\infty} \Pr[T \geq i] \leq n\sum_{i=1}^{\infty} \Pr[T > n(i-1)] \leq n\sum_{i=0}^{\infty}(1-2^{-n})^i < \infty$$

כוכבים בגראפים מקריים

ישנן מספר שיטות להוכיח זאת. דרך "אלגנטית" אפשרית היא באמצעות הוכחת הלמה הבאה: בהסתברות $1-o(1)$, הגרף G הוא כזה שלכל קבוצה בת שלושה צמתים $\{v,u,w\}$ קיים צומת נוסף בגרף שהוא שכן של v אבל אינו שכן של u או w.

הוכחת הלמה: עבור קבוצה קבועה של שלושה צמתים, הסיכוי ששאר $n-3$ צמתי הגרף אינם מספקים את המבוקש הוא $(1-\frac{1}{8})^{n-3}$. מכיוון שיש סה"כ $n\binom{n-1}{2}$ קבוצות כאלו (שימו לב שאנו צריכים כאן לספור לחוד את הבחירה של הצומת "v"), הרי שהסיכוי שתהיה קבוצה $\{v,u,w\}$ כל שהיא שעבורה אין צומת שכן ל־v ולא־שכן ל־u,w חסום ע"י $n\binom{n-1}{2}(\frac{7}{8})^{n-3} = o(1)$, כנדרש.

עתה, כשבידינו למה זו, כל שנותר להראות הוא שגרף G המקיים את התכונה הנ"ל מקיים גם את המבוקש לפי תנאי השאלה: בהינתן צומת v, ראשית נבחר צומת u_1 כל שהוא המחובר אליו (קיים כזה לפי שראשית ניקח u,w שרירותיים ואז נמצא צומת המקיים את התכונה למעלה עבור $\{v,u,w\}$). עתה נוכל לבחור (שוב ע"פ התכונה למעלה) צומת u_2 המחובר ל־v ולא ל־u_1. לבסוף נוכל לבחור צומת u_3 המחובר ל־v אך לא ל־u_1, u_2, לקבלת הכוכב המבוקש.

גובה עץ מקרי

לכל $2 \leq k \leq n$ נסמן ב־X_k את משתנה האינדיקטור עבור המאורע שבעת הוספת הצומת ה־k, גובה העץ גדל באחד. עתה נוכיח את החסם $\Pr[X_k = 1] \geq \frac{1}{k-1}$. ממנו נובע שאם נסמן ב־$X$ את גובה העץ הסופי נקבל את חסם התוחלת הדרוש:

$$\mathrm{E}[X] = 1 + \sum_{k=2}^{n} \mathrm{E}[X_k] \geq 1 + \sum_{k=2}^{n} \frac{1}{k-1} = \Omega(\log n)$$

על מנת לחסום מלמטה את $\Pr[X_k = 1]$, נבחר את u להיות אחד העלים הנמוכים ביותר בתת העץ שהתקבל מביצוע האלגוריתם עבור $k-1$ הצמתים הקודמים $\{v_1, \ldots, v_{k-1}\}$. ברור שאם הצומת u נבחר להיות האב של הצומת v_k אז גובה העץ גדל בשלב זה. מכיוון שיש סה"כ $k-1$ צמתים הרי שהסיכוי למאורע זה הוא $\frac{1}{k-1}$, ולכן זהו חסם תחתון עבור $\Pr[X_k = 1]$.

פתרונות לתרגיל השני

הפרדה ע"י פונקציה לינארית

אנו נגריל את f באופן מקרי. הווה אומר: כל פונקציה לינארית מ־$(\mathbb{Z}_2)^n$ ל־$\mathbb{Z}_2$ נתונה ע"י וקטור $u \in \mathbb{Z}_2$, כך שלכל $v \in (\mathbb{Z}_2)^n$ מתקיים $f(v) = u \cdot v$ (הכפל הוא כפל וקטורי מעל $\mathbb{Z}_2$). אנו נגריל את u באופן יוניפורמי (כל קורדינטה האופן ב"ת באחרות).

לכל $v \in A$ נסמן ב־X_v את משתנה האינדיקטור עבור המאורע ש־$f(v) = 0$. מתקיים $\mathrm{E}[X_v] = \frac{1}{2}$, וכן לכל $v \neq w$ המ"מ X_v ו־X_w הם בלתי תלויים בזוגות. להוכחת הטענה השניה נניח בלי הגבלת הכלליות שמתקיים $v_n = 0$ ו־$w_n = 1$: ניתן להניח בה"כ שקיימת קורדינטה i שמתאפסת ב־v ולא ב־w (אחרת נחליף את v ו־w), והטיעון הוא זהה אם $i = n$. עתה נחשב (למשל) את $\Pr[X_v = 1 \wedge X_w = 1]$ באמצעות נוסחת ההסתברות השלמה באופן הבא:

$$\begin{aligned}
\Pr[X_v = 1 \wedge X_w = 1] &= \sum_{\substack{\alpha_1,\ldots,\alpha_{n-1} \\ v\cdot(\alpha_1,\ldots,\alpha_{n-1},0)=0}} \Pr[u_1 = \alpha_1, \ldots, u_{n-1} = \alpha_{n-1}]\Pr[w \cdot (\alpha_1, \ldots, \alpha_{n-1}, u_n) = 1] \\
&= \sum_{\substack{\alpha_1,\ldots,\alpha_{n-1} \\ v\cdot(\alpha_1,\ldots,\alpha_{n-1},0)=0}} 2^{1-n} \cdot \frac{1}{2} = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}
\end{aligned}$$

מכך נובע שהמ"מ המתאר את מספר איברי A המאפסים את f, הנתון ע"י $X = \sum_{v\in A} X_v$, מקיים $\mathrm{E}[X] = \frac{k}{2}$ וכן $\mathrm{V}[X] = \frac{k}{4}$. ממשפט צ'בישף נובע עתה שבהסתברות גדולה מ־0 יתקיים (למשל) $|X - \frac{k}{2}| \le \sqrt{k}$, ולכן קיימת פונקציה f המקיימת את המבוקש.

מיון ע"י QuickSort

עבור $b \in A$ נגדיר את ה"קטעים" אשר הוא נמצא בהם במהלך אלגוריתם: בתחילת האלגוריתם הקבוצה A עוד אינה מחולקת ולכן נגדיר $I_{b,0} = A$. לאחר הבחירה המקרית של a (הביטו בתיאור האלגוריתם כפי שמופיע בשאלה) נגדיר את $I_{b,1}$ להיות תת הקבוצה ש־b ישוייך אליה. ז"א, $I_{b,1} = A_0$ אם $a < b$, $I_{b,1} = A_1$ אם $a > b$, ו־$I_{b,1} = \{a\}$ אם $a = b$. אם $I_{b,1}$ אינו בעל איבר יחיד, אז האלגוריתם ימיין בשלב כל שהוא אותו באופן רקורסיבי, ואז נגדיר את $I_{b,2}$ ע"פ תת הקבוצה של $I_{b,1}$ ש־b ישוייך אליה לאחר הבחירה המקרית של $a \in I_{b,1}$, וכו'. לפישוט האנליזה, כאשר $|I_{b,i-1}| = 1$ נגדיר $I_{b,i} = I_{b,i-1}$.

האיבר b משתתף בפעולת השוואה אחת בדיוק בכל פעם שמגדירים את $I_{b,i}$ מ־$I_{b,i-1}$ ואינו משתתף בהשוואות אחרות, ולכן מספר פעולות ההשוואה הכולל שהוא משתתף בהן זהה ל־i המינימלי עבורו $|I_{b,i}| = 1$. לכן אם מראים שבסיכוי $1 - o(1)$ מתקיים $|I_{b,100\log n}| = 1$ לכל $b \in A$, ההוכחה תושלם.

ראשית, נבדוק מה הסיכוי ש־$|I_{b,i}|$ קטן משמעותית מ־$|I_{b,i-1}|$. אם $|I_{b,i-1}|$ מתחלק ב־3, אז בסיכוי לפחות $\frac{1}{3}$ כאשר בוחרים באופן מקרי את $a \in I_{b,i-1}$, יבחר איבר השייך לשליש האמצעי של איברי $I_{b,i-1}$. כאשר מאורע זה יקרה, לא קשה לראות שיתקיים $|I_{b,i}| \le \frac{2}{3}|I_{b,i-1}|$. עתה אם $|I_{b,i-1}|$ אינו מתחלק ב־3 אז יהיה עלינו להתחשב בשיקולי חלוקה, אולן עדיין אם $|I_{b,i-1}| > 1$ אז בסיכוי לפחות $\frac{1}{4}$ יתקיים $|I_{b,i}| \le \frac{2}{3}|I_{b,i-1}|$.

מהדיון למעלה נובע שהסיכוי עבור המאורע $|I_{b,100\log n}| > 1$ חסום ע"י הסיכוי שסכומם של $100\log n$ מ"מ ב"ת המקבלים 0 בהסתברות $\frac{3}{4}$ ו־1 בהסתברות $\frac{1}{4}$ הוא קטן מ־$10\log n$, מכיוון שמתקיים $(\frac{2}{3})^{10\log n} < \frac{1}{n}$. אולם לפי החסם על ההתברות לסטיות גדולות לא קשה לראות שההסתברות למאורע הנ"ל עבור מ"מ ב"ת הוא $o(\frac{1}{n})$. לכן מחסימת האיחוד של המאורעות לכל $b \in A$, בסיכוי $1 - o(1)$ מתקיים $|I_{b,100\log n}| = 1$ לכל $b \in A$, כנדרש.

קבוצות ב"ת בהיפרגרפים

נסתכל על הפרוצדורה הבאה: ראשית נגריל קבוצת צמתים U ע"י כך שכל צומת ב־V יבחר באופן ב"ת בהסתברות α (את ערכו של α נבחר אח"כ). עתה נקבל ממנה קבוצת צמתים ב"ת W ע"י כך שמכל משולש של ההיפרגרף המוכל ב־U נחסר את אחד מצמתיו. אם נסמן ב־X את מספר הצמתים ב־U וב־Y את מספר המשולשים המוכלים ב־U, הרי שגודל W הוא לפחות $X - Y$ (יתכן שהוא גדול יותר). נחשב אם כן את תוחלת הפרש זה: $\mathrm{E}[X - Y] = \mathrm{E}[X] - \mathrm{E}[Y] = \alpha n - \alpha^3 m$. עתה נבחר את ה־$\alpha$ שלנו: ע"י גזירה לפי α וחיפוש נקודה המאפסת את הנגזרת נקבל $\alpha = \sqrt{\frac{n}{3m}}$ (כאן חשוב שיתקיים $m \geq \frac{1}{3}n$ כדי שנקבל $\alpha \leq 1$). ע"י הצבה נקבל עבור ערך זה $\mathrm{E}[X - Y] = \frac{2n^{3/2}}{3\sqrt{3m}}$, ומכאן שקיימת בחירה ספציפית של U שעבורה הפרש מספר הצמתים ומספר המשולשים אכן אינו יורד מביטוי זה. הקבוצה W שנקבל מ־U תקיים אם כן את המבוקש.

פתרונות לתרגיל השלישי

הצבה מספקת מינימלית

נסמן את קבוצת המשתנים ב־$x_1,\ldots,x_n$. ע"פ למת הבידוד, אם נגריל באופן מקרי משקל w_i לכל x_i באופן יוניפורמי וב"ת מתוך $\{1,\ldots,3n\}$, אז בהסתברות לפחות $\frac{2}{3}$, מבין ההצבות המספקות עם מספר ערכי 1 מינימלי תהיה הצבה יחידה שבה סכום משקלות המשתנים שקיבלו 1 הוא מינימלי. במידה שזה קורה, אם נגדיר עתה לכל משתנה "משקל כולל" של $v_i = 4n^2 + w_i$, אז תהיה הצבה יחידה (מבין כל ההצבות המספקות באשר הן) עם משקל כולל מינימלי עבור ערכי ה־1, וזו תהיה אחת מההצבות המינימליות המקוריות של ה־3CNF שלנו.

עתה ניתן להגדיר את ה־3CNF החדש: כל משתנה x_i יוחלף ב־v_i משתנים $y_{i,1},\ldots,y_{i,v_i}$ (כאשר v_i מוגרל אקראית בתחום $\{4n^2+1,\ldots,4n^2+3n\}$ כמקודם). לכל פסוקית ב־3CNF המקורי נגדיר פסוקית כאן, שכל משתנה x_i המופיע בה יוחלף ב־$x_{i,1}$. בנוסף, לכל $1 \le i \le n$ נוסיף פסוקיות מעל המשתנים $x_{i,1},\ldots,x_{i,v_i}$ אשר כולן מסתפקות אם ורק אם כל המשתנים הנ"ל זהים זה לזה (לא קשה לראות שניתן לעשות זאת ללא משתנים נוספים). עתה לא קשה לראות שזהו ה־3CNF המבוקש.

מרטינגל חשיפה עבור עץ מקרי

להגדרת המרטינגל נשים לב שניתן לאפיין את תהליך בניית העץ באמצעות פונקציה מקרית $f:\{2,\ldots,n\}\to\{1,\ldots,n-1\}$, כאשר לכל i בוחרים את $f(i)$ מתוך $\{1,\ldots,i-1\}$ באופן יוניפורמי וב"ת בכל הערכים האחרים של f. הנתון $f(i)=j$ מתאר את זה שבשלב ה־i הצומת v_j נבחר להיות האב של v_i. עתה עבור החשיפה פשוט נגדיר את התחומים $\mathcal{D}_i=\{2,\ldots,i\}$. שימו לב שניתן להסתפק ב־$X_2,\ldots,X_n$ מתוך המרטינגל שבנינו (X_2 תמיד יקבל את תוחלת גובה העץ).

עבור סדרת התחומים לא מתקיים תנאי ליפשיץ הקומבינטורי, ולכן נוכיח שהמרטינדל מקיים אותו באופן ישיר. לשם כך, לכל $k_2,\ldots,k_{i-1}$ ולכל $k\neq l$ נגדיר התאמה חד חד ערכית ועל בין הפונקציות f המקיימות $f(j)=k_j$ ל־$j<i$ ו־$f(i)=k$ לבין הפונקציות f' המקיימות $f'(j)=k_j$ ל־$j<i$ ו־$f'(i)=l$, כך שלכל זוג פונקציות שהותאמו זו לזו הפרש גובהי העצים המתאימים הוא לכל היותר אחד. מכאן ינבע (באופן דומה להוכחה מהכיתה עבור תנאי ליפשיץ הקומבינטורי) שהמרטינגל אכן מקיים את תנאי ליפשיץ.

בהינתן f המקיימת את התנאים למעלה, נתאים את f' באופן הבא. לכל $j<i$ נקבע כצפוי $f'(j)=f(j)$, וכן נקבע $f'(i)=l$. לקביעת הערכים האחרים, ראשית נסדר בשני העצים את הצמתים $v_1,\ldots,v_i$ לפי סדר יורד של המרחק שלהם מהשורש, כאשר צמתים מאותו מרחק יסודרו (למשל) לפי האינדקס שלהם. שימו לב עתה שלכל m, גובה הצומת ה־m לפי f וגובה הצומת ה־m לפי f' אינם נבדלים ביותר מ־1.

עתה נסכם את הגדרת f' באופן הבא: לכל $j>i$, אם $f(j)>i$ אז נגדיר $f'(j)=f(j)$. לעומת זאת, אם $f(j)\le i$, אז נמצא m כך שהצומת $v_{f(j)}$ הוא הצומת ה־m בסדר שנקבע למעלה לתת העץ של f, ונגדיר את $f'(j)$ להיות האינדכס של הצומת ה־m בסדר המתאים של f'. ההוכחה הלא קשה שזוהי אכן התאמה חד חד ערכית ועל מושארת לקורא.

עבור הטענה על הגבהים נסתכל בעץ המלא עבור f, ולכל צומת שהאינדכס שלו גדול מ־i אולם האינדכס של אביו אינו גדול מ־i נבדוק את תת העץ המתאים. מה שצריך לשים לב הוא שגם עבור f וגם עבור f' המדובר הוא באותם תתי עצים בדיוק (לצמתים הנ"ל בוודאי שאין אף צאצא עם אינדכס שאינו גדול מ־i), ולכן השאלה היא מהו הגובה של האבות שלהם. לפי הבניה, לכל תת עץ כזה גובה האב אינו נבדל ביותר מ־1. זה כמעט מסיים את ההוכחה, פרט לכך שיש עוד את האפשרות שהגובה של אחד או יותר מהעצים נקבע דווקא ע"י עלה שהאינדכס שלו אינו עולה על i. אולם כבר ידוע מקודם שגובהי העצים המתאימים ל־$v_1,\ldots,v_i$ אינם נבדלים ביותר מ־1, ובזאת סיימנו את ההוכחה.

קבוצת צמתים מאולצת

ראשית נסמן את גודל כל V_i ב־k. עתה נגריל באופן יוניפורמי, מקרי וב"ת צומת v_i מכל קבוצה V_i. לכל קשת uv של הגרף G, נסמן ב־E_{uv} את המאורע שקשת זו מוכלת ב־$\{v_1, \ldots, v_n\}$. ברור שאם אף מאורע E_{uv} לא מתקיים אז קבוצת הצמתים הנ"ל אינה מכילה קשתות מ־G כנדרש.

ההסתברות שיתרחש E_{uv} היא k^{-2} אם קיימים $i \neq j$ כך ש־$u \in V_i$ ו־$v \in V_j$, ואחרת היא אפס. נניח אם כן שהמקרה הראשון קורה. נסמן ב־T את קבוצת כל הקשתות של G המכילות לפחות צומת אחד מ־$V_i \cup V_j$. המאורע E_{uv} הוא בלתי תלוי בכל המאורעות פרט לאלו המתייחסים לקשתות מ־T. כמו כן לפי הנתון על דרגת הגרף אנו מקבלים $|T| \leq 2kd$. לכן אם מתקיים $ek^{-2}(2kd+1) < 1$, אז הגרסא הסימטרית של הלמה הלוקלית תתן לנו שבהסתברות חיובית הקבוצה $\{v_1, \ldots, v_n\}$ אכן אינה מכילה קשתות של G. בחירה למשל ב־$c = 10$ וההצבה $k = 10d$ תתן את המבוקש.

פתרונות לתרגיל הרביעי

משפחות נחתכות

ראשית נראה שבלי הגבלת הכלליות, אכן ניתן להניח שכל המשפחות $\mathcal{F}_1, \ldots, \mathcal{F}_k$ הן מונוטוניות לא יורדות: אם המצב אינו כך, אז נוסיף לכל $\mathcal{F}_i$ גם את כל תתי הקבוצות של $\{1, \ldots, n\}$ אשר מכילות קבוצה כל שהיא מ־$\mathcal{F}_i$. עתה לא קשה לראות שנקבל משפחות מונוטוניות לא יורדות, וכן שתכונת הנחתכות של כל אחת מהן נשמרת. מכיוון שמשפחות אלו מכילות את המשפחות המקוריות, מספיק להוכיח את החסם על הקבוצות שאינן שייכות למשפחות החדשות.

את החסם נוכיח באינדוקציה על k. עבור $k = 1$, פשוט נשים לב לכך שעבור אף קבוצה $A \subseteq \{1, \ldots, n\}$ לא יתכן גם $A \in \mathcal{F}_1$ וגם $\{1, \ldots, n\} \setminus A \in \mathcal{F}_1$, ולכן בהכרח $|\mathcal{F}_1| \leq 2^{n-1}$. עבור המעבר מ־$k = i$ ל־$k = i + 1$, משתמשים במשפט קלייטמן עבור החיתוך של הקבוצה $\mathcal{P}(\{1, \ldots, n\}) \setminus \mathcal{F}_{i+1}$ (שגודלה לפחות 2^{n-1} לפי המקרה $k = 1$) עם הקבוצה $\mathcal{P}(\{1, \ldots, n\}) \setminus \bigcup_{j=1}^{i} \mathcal{F}_j$ (שגודלה לפחות 2^{n-i} לפי הנחת האינדוקציה). שימו לב ששתי הקבוצות הנ"ל מונוטוניות לא עולות.

הילוך על הקוביה

ההוכחה נעשית בשיטת הצימוד. ראשית נשים לב שניתן היה להגדיר באופן שקול את ההילוך המקרי $X_0, X_1, \ldots$ ע"י כך שבשלב ה־i קודם נבחר באופן יוניפורמי קורדינטה $1 \leq j \leq n$, ורק אחר כך נחליט בהסתברות $\frac{1}{2}$ אם להפוך את הקורדינטה ה־j. עתה נגדיר הילוך מקרי שני $Y_0, Y_1, \ldots$ על הקוביה $\{0, 1\}^n$ באופן הבא: Y_0 יבחר באופן מקרי ויוניפורמי מהקוביה. בשלב ה־i נבדוק מהי הקורדינטה שנבחרה כשבחרנו את X_{i+1} לפי X_i. אם X_i ו־Y_i זהים על הקורדינטה הנ"ל אז לבחירת Y_{i+1} אנו נהפוך את הקורדינטה אם ורק אם $X_{i+1} \neq X_i$ (ז"א שבסיכוי $\frac{1}{2}$ נהפוך אותה בשני ההילוכים, ובסיכוי $\frac{1}{2}$ לא נהפוך אותה באף אחד מהם). אם X_i ו־Y_i שונים על הקורדינטה הנ"ל אז נהפוך אותה עבור Y_{i+1} אם ורק אם $X_{i+1} = X_i$.

ניתן לראות בשלב זה ש־$Y_0, Y_1, \ldots$ לכשעצמו הוא הילוך מקרי עם אותה מטריצת מעבר כמו $X_0, X_1, \ldots$. מכיוון שהתפלגות של Y_0 היא ההתפלגות הסטציונרית של ההילוך, ההתפלגות (הלא מותנה) של Y_t תהיה זהה לה לכל $0 \leq t$. נראה עתה שהמאורע $X_t = Y_t$ יקרה בהסתברות העולה על $1 - \epsilon$ עבור $t = n \ln(n/\epsilon) = O(n \log n)$ לסיום ההוכחה.

לכל $1 \leq j \leq n$ נגדיר את המאורע A_j כמאורע שהקורדינטה j נבחרה להפיכה אפשרית במעבר מ־X_i ל־X_{i+1} עבור $0 \leq i < t$ כל שהוא. ניתן לראות שאם A_j מתקיים אז X_t ו־Y_t יהיו שווים על הקורדינטה ה־j, ולכן אם $\wedge_{j=1}^{n} A_j$ מתקיים אז בפרט $X_t = Y_t$. אולם $\Pr[\neg A_j] = (1 - \frac{1}{n})^t < \epsilon/n$, ולכן $\Pr[\wedge_{j=1}^{n} A_j] > 1 - \epsilon$ כנדרש.

קבוצות צבעוניות

ראשית ־ הוכחת הקיום: נגריל את הצביעה של כל איבר של $\{1, \ldots, n\}$ באופן מקרי, יוניפורמי וב"ת. יהי E_i המאורע ש־A_i מכילה איברים רק משניים או פחות צבעים. מתקיים $\Pr[E_i] \leq 3(2/3)^{|A_i|}$, ולכן בוודאי מהנתון $\sum_{i=1}^{m} (2/3)^{|A_i|} < 1/6$ נובע שבסיכוי חיובי אף אחד מהמאורעות לא מתקיים, ז"א שהצביעה מקיימת את המבוקש.

למציאת הצביעה משתמשים בשיטת התוחלות המותנות. יהי P_i משתנה האינדיקטור עבור E_i, ויהי $P = \sum_{i=1}^{m} P_i$. המשתנה P מקבל רק ערכים שלמים, וכאשר $P = 0$ עבור צביעה מסויימת הרי שזוהי הצביעה המבוקשת. עתה נבחר את $c : \{1, \ldots, n\} \rightarrow \{1, 2, 3\}$ איבר איבר, כאשר בשלב ה־i נבחר את $c(i)$ כך שהתוחלת המותנה של P על הבחירה של $c(1), \ldots, c(i)$ לא תעלה על התוחלת המותנה של P על הבחירה של $c(1), \ldots, c(i-1)$ בלבד. ניתן לחשב את התוחלות המותנות בזמן פולינומי במדויק באמצעות עקרון ההכלה וההפרדה. מכיוון שהתוחלת הלא־מותנה של P קטנה מ־1 ומשתנה זה מקבל רק ערכים שלמים, הרי שבסוף התהליך הערך שלו יהיה 0, כנדרש.