פתרון עבודת בית 6

שאלה 1:

סעיף א

נגדיר: $B(k_1,k_2) = B[0\dots k_1-1] \circ B'[k_1\dots k_2] \circ B[k_2+1\dots n-1]$

<u>תיאור האלג'</u>

1. אליס מגרילה מספר ראשוני $p < n^4$, מחשבת $a = A \bmod p$ ושולחת לבוב a, p.
2. לכל $0 \le k_1 \le k_2 \le n-1$ בוב בודק האם $B(k_1,k_2) \bmod p = a$
3. אם קיימים k_1, k_2 כך שהשוויון מתקיים (בוב מצא עדות לכך ש-B הינה מודיפיקציה של A) אזי בוב מחזיר "כן", אחרת בוב מחזיר "לא".

<u>הוכחת נכונות</u>

אם B הינה מודיפיקציה של A אזי קיימים $0 \le k_1 \le k_2 \le n-1$ עבורם בוב יימצא כי $B(k_1,k_2) \bmod p = a$ והוא יחזיר "כן" (ללא שום תלות ב-p הראשוני שאליס בחרה).
אם B איננה מודיפיקציה של A אזי האלג' טועה אם קיימים אינדקסים $0 \le k_1 \le k_2 \le n-1$ כך ש- $B(k_1,k_2) \bmod p = a$. כלומר, האלג' טועה אם"ם קיימים k_1, k_2 כך ש-p מחלק את $|A - B(k_1,k_2)|$.
כיוון ש- $A, B(k_1,k_2) < 2^n$ אזי ברור כי $|A - B(k_1,k_2)| < 2^n$ ועל פי משפט שהוכח בכיתה קיימים לכל היותר n ראשוניים המחלקים את ההפרש עבור ה-k_1, k_2 הנתונים.
ישנם n^2 הפרשים ולכן קיימים לכל היותר n^3 ראשוניים המחלקים את אחד ההפרשים.
מכאן וממשפט בנושא צפיפות הראשוניים שנלמד בכיתה,

$$\Pr(\text{The algorithm fails}) \le \frac{|\{p \mid p \text{ divides } |A-B(k_1,k_2)| \text{for same index } 0\le k_1\le k_2\le n-1\}|}{\text{The number of primes smaller then } n^4} =$$

$$= \frac{n^3}{n^4/\log n^4} = \frac{4\log n}{n} < \frac{1}{4}$$

<u>הערה:</u> אי השוויון האחרון מתקיים עבור n גדול מספיק כנדרש.

<u>ניתוח מספר הביטים שנשלחו וזמן הריצה</u>
<u>סיבוכיות תקשורת:</u>
$p < n^4$ ולכן לוקח $4\log n$ ביטים לייצגו. $a < p$ ולכן דרוש לכל היותר מספר דומה של ביטים לייצגו. סה"כ נקבל כי אורך ההודעה שאליס שולחת לבוב הינו לכל היותר $8\log n = O(\log n)$.

<u>סיבוכיות זמן:</u>
אליס: הגרלת p - $O(\log^4 n)$, חישוב $A \bmod p$ - $O(n)$.
בוב: חישוב $B(k_1,k_2) \bmod p$ - $O(n)$, לכל $0 \le k_1 \le k_2 \le n-1$ ולכן סהכ- $O(n^3)$.

סעיף ב

נשים לב ש $p < n^4$ וגם על מנת שהחישוב יתבצע $p < 2^{64}$.
ולכן $n^4 < 2^{64}$ כלומר $n < 2^{16}$.

סעיף ג

נסמן ב-q את המספר הראשוני שנבחר ע"י האלג'.
תחילה נחשב את ההסתברות שבהרצה כלשהי של האלג' תתרחש שגיאה בעמדה $T_r \bmod q = P \bmod q$, כלומר q מחלק את $|T_r - P|$.
$0 \le r \le m-n$ כלשהי. תנאי הכרחי ומספיק לכך שמקרה זה יתרחש הינו

לכל $0 \le r \le m - n$ מתקיים כי $|T_r - P| \le 2^n$ ולכן (לפי משפט הנלמד בכיתה) קיימים לכל היותר n ראשוניים המחלקים את $|T_r - P|$ ולכן

$$\Pr(\text{the algorithm fails at some execution and index r}) \le \frac{n}{\pi(I)}$$

מאחר ואנו מחזירים את החיתוך של הפתרונות $S_1 \cap \dots \cap S_k$ אזי האלג' טועה בעמדה r כלשהי אם"ם האלג' טועה בכל אחת מ-k ההרצות ולכן

$$\Pr(\text{the algorithm fails at some index r}) \le \left(\frac{n}{\pi(I)}\right)^k$$

מספיק לאלג' להיכשל בעמדה אחת מתוך $m - n$ העמדות על מנת להחזיר תשובה שקרית ולכן לפי משפט "חסם האיחוד" מתורת ההסתברות נקבל כי

$$\Pr(\text{The algorithm fails}) \le m * \left(\frac{n}{\pi(I)}\right)^k$$

שאלה 2:

סעיף א':

העד יהיה הצבה של ערכים 0,1 למשתנים. גודל העד (ההצבה) הוא מספר המשתנים במערכת האי- שוויוניים. אלגוריתם האימות ,בהינתן הצבה למשתנים ,יוודא שההצבה היא הצבה בינארית עבור כל המשתנים ושכל אי שוויון מתקיים .ניתן לעשות זאת במעבר אחד על כל האי שיוונים ולכן זמן הריצה הוא פולינומי בגודל הקלט.

סעיף ב':

נראה רדוקציה $SAT \le_p BI$. בהינתן פסוק Ψ עם n משתנים ו- m פסוקיות נבנה מערכת אי שוויוניים M עם 2n משתנים ו m אי-שוויוניים. יהיו $x_1, \dots, x_n$ המשתנים **הבוליאניים** בפסוק Ψ. נתאים לכל משתנה בוליאני x_i שני משתנים מספריים y_i ו z_i. עבור הפסוקית ה- j מהצורה $l_{j,1} \vee \dots \vee l_{j,t}$ נוסיף ל- M את אי השוויון הבא: אם $l_{j,h}$ הוא משתנה x_k (ללא שלילה) נוסיף לאי-שוויון את המשתנה y_k אחרת אם $l_{j,h}$ מייצג שלילה של משתנה $\overline{x_{kl}}$ נוסיף לאי-השוויון את המשתנה z_k אי השוויון הוא סכום המשתנים הנ"ל ≤ 1.

לדוגמא: עבור הפסוקית $x_1 \vee \overline{x_5} \vee x_{100}$ נבנה את אי השוויון $y_1 + z_5 + y_{100} \ge 1$.

בנוסף, (בשביל לשמור על עקביות ההצבה) נוסיף לכל $1 \le i \le n$ את שני אי-שוויוניים $z_i + y_i \le 1$ $z_i + y_i \ge 1$.

הרדוקציה פולינומית: עבור פסוק עם n משתנים ו- m פסוקיות אנחנו בונים 2n+m אי-שוויוניים.

הוכחת תקפות הרדוקציה:

כיוון ראשון: צריך להוכיח: אם הפסוק Ψ ספיק אז קיימת הצבה בינארית חוקית למערכת האי שיוונים שיצרנו M כך שכל אי-שוויון במערכת יתקיים .מכיוון ש- Ψ ספיק ,קיימת הצבה המספקת את Ψ. נבנה הצבה שתקיים את מערכת האי שיוונים באופן הבא:

- אם $x_i = \text{true}$ אזי $z_i = 0$ ו- $y_i = 1$.
- אם $x_i = \text{false}$ אזי $z_i = 1$ ו- $y_i = 0$.

בכל פסוקית יש ליטרל $l_{j,h}$ אחד לפחות שהסתפק לכן המשתנה y_k או z_k שמופיע באי - השוויון המתאים יקבל 1 ולכן האי שוויון יתקיים .בנוסף ,לכל $1 \le i \le n$ האי שוויוניים $z_i + y\_i \le 1$ $z_i + y_i \ge 1$ מתקיימים כי $z_i + y_i = 1$.

כיוון שני: צריך להוכיח: אם קיימת הצבה בינארית חוקית למערכת האי שיוונים שיצרנו M כך שכל אי-שוויון במערכת יתקיים, אז קיימת הצבה מספקת לפסוק Ψ. נתבונן על הצבה למערכת

האי שיוונים שיצרנו M כך שכל אי-שוויון במערכת מתקיים ונבנה הצבה המספקת את Ψ באופן הבא: אם $y_i = 1$ אז $x_i = true$; אחרת ($y_i = 0$) $x_i = false$.

כל אי שוויון שמתאים לפסוקית מתקיים כלומר יש משתנה אחד לפחות באי-השוויון שההצבה עבורו היא אחד. אם משתנה זה הוא y_i אזי x_i מופיע בפסוקית ו- $x_i = true$ כלומר הפסוקית מסתפקת .אם המשתנה זה הוא z_i אזי מכיוון ש- $z_i = 1$ נקבל ש- $y_i = 0$ ולכן - $x_i = false$ לפי הרדוקציה $\overline{x_i}$ מופיע בפסוקית ולכן הפסוקית מסתפקת .יש אי שוויון עבור כל פסוקית ולכן כל הפסוקיות מסתפקות ולכן כל הפסוק מסתפק על ידי ההצבה.

<u>סעיף ג'</u>:

בהינתן גרף לא מכוון G ומספר טבעי k נבנה מערכת אי שיוונים M באופן הבא.

- עבור כל קדקוד $v \in V$ נתאים משתנה x_v.
- עבור כל קשת $(u,v) \in E$ נוסיף ל- M את אי השוויון $x_u + x_v \geq 1$.
- בנוסף ,נוסיף ל- M את אי השוויון $\sum_{v \in V} x_v \leq k$.

נחזיר את M.

הבניה היא פולינומית שכן עבור כל צלע אנחנו מוסיפים אי שוויון אחד המורכב מ-2 משתנים ובנוסף מוסיפים אי שוויון המורכב מ |V| משתנים.

הוכחת תקפות הרדוקציה:

<u>כיוון ראשון:</u> צ"ל אם קיים קבוצת כיסוי C בגודל $k \geq$ אז קיימת הצבה חוקית למערכת שבנינו שמקיימת את כל אי- שוויוניים. נסתכל על כיסוי C של הגרף בגודל $k \geq$ ונבנה את ההצבה הבאה :עבור כל $v \in V$ אם $v \in C$ אז $x_v = 1$ אחרת $x_v = 0$. כל צלע $(u,v) \in E$ מכוסה על ידי לפחות קדקוד אחד ולכן $x_u = 1$ או\וגם $x_v = 1$ ולכן אי השוויון $x_u + x_v \geq 1$ מתקיים. בנוסף אי השוויון $\sum_{v \in V} x_v \leq k$ מתקיים כי C בגודל $k \geq$ ולכן יש לכל היותר k משתנים שערכם הוא אחד.

<u>כיוון שני:</u> צ"ל אם קיימת הצבה חוקית למערכת שבנינו שמקיימת את כל אי- שוויוניים אז קיים כיסוי C בגודל $k \geq$ בגרף G. ניקח הצבה חוקית למערכת אי- שוויוניים ונבנה כיסוי C של הגרף על סמך ההצבה: לכל $v \in V$ אם $x_v = 1$ אז נוסיף את v ל- C.
לכל u, v כך ש- $(u,v) \in E$, אי השוויון $x_u + x_v \geq 1$ מתקיים ,כלומר, $x_u = 1$ או\וגם $x_v = 1$. לפי הבנייה של $v \in C$,C או\וגם $v \in C$, לכן הצלע $(u,v) \in E$ מכוסה על ידי לפחות קדקוד אחד .בנוסף ,אי השוויון $\sum_{v \in V} x_v \leq k$ מתקיים אז הכנסנו היותר k קודקודיים לכיסוי.

שאלה 3:

סעיף א':

הוכחה:

נניח בשלילה כי $P = NP$ ונגיע לסתירה עם $NP \neq co-NP$:

1. $NP \subseteq co-NP$: מטענה 4 - $P \subseteq co-NP$ ומההנחה בשלילה $P = NP$ ולכן $NP \subseteq co-NP$.
2. $NP \supseteq co-NP$: תהי L כך ש- $L \in co-NP$, לכן $\overline{L} \in NP$, מההנחה כי $P = NP$ נקבל $\overline{L} \in P$. מטענה 3 $L \in P$ ולכן $L \in NP$. כלומר $NP \supseteq co-NP$.

מ- 1 ו- 2 קבלנו $NP = co-NP$ סתירה!

כלומר $NP \neq P$.

הוכחת טענה 3:

$L \in P$ כלומר קיים אלגוריתם פולינומיאלי המקבל את השפה L. נריץ את האלגוריתם ונחזיר תשובה הפוכה עבור כל קלט (כלומר במקום כן שייך לשפה נחזיר לא שייך ולהיפך), וקיבלנו אלגוריתם פולינומיאלי המקבל את $\overline{L}$ כלומר $\overline{L} \in P$.

הוכחת טענה 4:

תהי L כך ש- $L \in P$ לכן מטענה 3 - $\overline{L} \in P$, מטענה 1- $\overline{L} \in NP$ ולכן $L \in co-NP$.
כלומר $P \subseteq co-NP$.

סעיף ב':

הוכחה:

לפי ההגדרות:

$$\overline{L_1} \leq_p \overline{L_2} \Leftrightarrow (x \in \overline{L_1} \leftrightarrow f(x) \in \overline{L_2}) \Leftrightarrow (x \notin L_1 \leftrightarrow f(x) \notin L_2) \Leftrightarrow (x \in L_1 \leftrightarrow f(x) \in L_2) \Leftrightarrow L_1 \leq_p L_2$$

סעיף ג':

הוכחה:

נניח בשלילה כי קיימת שפה L כך ש- $L \in NPC$ וגם $\overline{L} \in NPC$, ונגיע לסתירה עם $NP \neq co-NP$:

1. $NP \supseteq co-NP$: $L \in NPC$ כלומר לכל 'L כך ש- $L' \in NP$ מתקיים $L' \leq_p L$. לכן לפי סעיף ב' לכל $L' \in co-NP$, $\overline{L'} \leq_p \overline{L}$. מההנחה בשלילה ש $\overline{L} \in NPC$ מתקיים $L \leq_p \overline{L}$, וקיבלנו $L \leq_p \overline{L} \leq_p \overline{L'}$.

כלומר $L \leq_p \overline{L'}: \forall \overline{L'} \in co-NP$. מהנתון $L \in NP$ ומטענה 2 סעיף א' נקבל- $\forall \overline{L'} \in co-NP: \overline{L'} \in NP$ כלומר $NP \supseteq co-NP$.

2. $NP \subseteq co-NP$: $L \in NP$ לכן $\overline{L} \in co-NP$, הראנו כי $NP \supseteq co-NP$ ולכן $\overline{L} \in NP$, מהגדרת $co-NP$ נקבל $\overline{\overline{L}} \in co-NP$ ומכיוון ש $\overline{\overline{L}} = L$ אזי $L \in co-NP$.
כלומר $NP \subseteq co-NP$.

מ- 1 ו- 2 קבלנו $NP = co-NP$ סתירה!

לא קיימת שפה L כך ש- $L \in NPC$ וגם $\overline{L} \in NPC$.

שאלה 4:

סעיף א':

הפסוק $(x_1 = 0 \vee x_1 = 1) \wedge (x_1 = 1 \vee x_1 = 2) \wedge (x_1 = 0 \vee x_1 = 2)$
הוא פסוק 2-CNF מוכלל, שעבורו אין השמה מספקת. הרדוקציה מעבירה אותו לפסוק
$(x_{1,0} \vee x_{1,2}) \wedge (x_{11} \vee x_{1,2}) \wedge (x_{1,0} \vee x_{1,1})$ שעבורו קיימת השמה מספקת.

סעיף ב':

$$g(x_1, x_2, x_3) = (\overline{x_1} \vee \overline{x_2}) \wedge (\overline{x_1} \vee \overline{x_3}) \wedge (\overline{x_2} \vee \overline{x_3})$$

סעיף ג':

שימו לב שהבעיה ברדוקציה היא שבהצבה מספקת של $f(\varphi)$ ייתכן שלדוגמא $A(x_{i,0}) = A(x_{i,1}) = A(x_{i,2}) = T$ והצבה זו לא מתאימה להצבה לפסוק המקורי. לכן נדאג שלכל היותר אחד מבין $x_{i,0}, x_{i,1}, x_{i,2}$ יקבל את הערך T. נוסיף לפסוק ψ פסוקית $g(x_{i,1}, x_{i,2}, x_{i,3})$ עבור כל x_i שמופיע ב φ. נסמן $\varphi' = f(\varphi)$.
נוכיח כי $\varphi \in$ E-2-SAT אם"ם $\varphi' \in$ 2-SAT.

נניח $\varphi \in$ E-2-SAT ונוכיח כי $\varphi' \in$ 2-SAT. קימת השמה A המספקת את הפסוקיות ב φ. נגדיר השמה A' המתאימה ל A, כלומר אם $A(x_i) = a$ אז $A'(x_{i,a}) = T$ ו $A'(x_{i,b}) = F$ עבור b שונה מ a. מכך ש A מספקת את φ נובע כי לכל פסוקית $(x_i = a \vee x_j = b)$ מתקיים כי A שולחת את x_i ל a או את x_j ל b. מכאן שב הפסוקית Ψ $(x_{i,a} \vee x_{j,b})$ מסופקת ע"י A'. כמו כן כל פסוקית שהוספנו ל Ψ מתקיימות כיוון שלכל x_i שמופיע ב φ רק אחד מבין $x_{i,0}, x_{i,1}, x_{i,2}$ יקבל את הערך T. כיוון ש φ' הוא Ψ בתוספת הפסוקיות החדשות כל פסוקית בו מסתפקת. לכן $\varphi' \in$ 2-SAT.

נניח $\varphi' \in$ 2-SAT ונוכיח $\varphi \in$ E-2-SAT. קיימת השמה מספקת A' ל φ'. נסמן ב A את ההשמה המתאימה ל A, כלומר אם $A'(x_{i,a}) = T$ אז $A(x_i) = a$ ואם $A'(x_{i,0}) = A'(x_{i,1}) = A'(x_{i,2}) = F$ אז $A(x_i) = 1$ (הבחירה ב - 1 היא שרירותית). כיוון שההשמה מספקת גם את הפסוקיות שהוספנו ל Ψ השמה מוגדרת היטב (כלומר לא יכול להיות ש $A(x_i) = a$ וגם $A(x_i) = b$ עבור a, b שונים). A' מספקת את φ' ובפרט את Ψ. לכן לכל פסוקית ב Ψ, $(x_{i,a} \vee x_{j,b})$ מתקיים ש $A(x_{i,a}) = T$ או $A(x_{j,b}) = T$. מכאן שב φ הפסוקית $(x_i = a \vee x_j = b)$ מסתפקת ע"י A. כיוון שלכל פסוקית ב φ יש פסוקית מתאימה ב Ψ כל הפסוקיות ב φ מסתפקות ע"י A לכן $\varphi \in$ E-2-SAT.

סעיף ד':

נשים לב כי הרדוקציה שתוארה בסעיף ג' היא פולינומיאלית מ E-2-SAT ל 2-SAT. בהינתן פסוק φ נתרגם בזמן פולינומיאלי בגודל φ ונקבל את Ψ. נוסיף לכל משתנה את הפסוקיות מסוג g (כל משתנה תורם 3 פסוקיות ולכן גם כאן הזמן הוא לינארי). כיוון ש 2-SAT. היא ב P, פתרון הבעיה המתורגמת לוקח זמן פולינומיאלי (וגם אורך הקלט פולינומיאלי) ומנכונות הרדוקציה התשובה לבעיה המתורגמת שווה לתשובה לבעיה המקורית .כל הצעדים בוצעו בזמן פולינומיאלי.

שאלה 5:

סעיף א':

Base(G,k) היא ב NP: אלגוריתם אימות יקבל את (G,k) ו-y, קבוצת קדקודים מ G (אינדקסים) ויבדוק ש – y אכן בסיס בגודל k ל- G. לכל קדקוד ב- y סמן את כל השכנים שלו ואת הקדקוד עצמו .אם בסוף התהליך כל הקדקודים מסומנים החזר "כן" ואחרת "לא".
האלגוריתם הוא פולינומיאלי כי עברנו על כל צלע פעם אחת לכל היותר ועל הקדקודים פעמיים לכל היותר .כמו כן נבדוק כי y מכילה k קדקודים .מההגדרה של Base אם $(G, K) \in Base$ אז קיימת קבוצת בסיס שעבורה נחזיר "כן" ואחרת כל תת קבוצה של G אינה קבוצת בסיס.

Base(G,k) היא NP-hard: נראה רדוקציה מ Set-Cover ל Base. בהינתן $(S_1, S_2, \dots, S_l, k)$ (למי שהרשה לכיסוי לכלול את אם $k > l$ נבנה גרף G עם קדקוד אחד והרדוקציה תחזיר (G,0)

אותה קב 'כמה פעמים זה לא נחוץ). אחרת נבנה גרף G שעבורו $V = \{S_1, \dots, S_l\} \cup U$ כלומר קדקוד לכל קבוצה ולכל איבר ב U. צלעות הגרף הן $E = E_1 \cup E_2$ כאשר
$E_1 = \{(S_i, u) | u \in S_i\}$ (כלומר ב E_1 יש צלע מכל קדקוד המייצג קבוצה לכל קדקוד המייצג איבר בקבוצה) ו- $E_2 = \{(S_i, S_j) | 1 \leq i, j \leq l\}$ (כלומר יש צלע בין כל שני קדקודים המייצגים קבוצות).

חישוב הרדוקציה לוקח זמן פולינומיאלי ,כיוון שעברנו פעם אחת על כל קבוצה ובדקנו על כל איבר אם ראינו אותו בעבר (כלומר זמן שהוא ריבועי ב $|U|$).

נראה כי $(S_1, S_2, \dots, S_l, k) \in Set - Cover$ אם"ם $(G, k) \in$ Base.

נניח $(S_1, S_2, \dots, S_l, k) \in Set - Cover$. אז קיים כיסוי ל U ע"י k קבוצות $S_{i_1}, \dots, S_{i_k}$ בגרף G, קבוצת הקדקודים המתאימים לקבוצות $S_{i_1}, \dots, S_{i_k}$ זו בסיס בגודל k ל- G. כל קדקוד S_i מכסה את קבוצת הקדקודים המתאימים לאיברים מ- U שהקבוצה S_i מכסה. לכן כל U מכוסה. מצד שני S_i מכסה את כל קדקודי הקבוצות (כי קדקודי הקבוצות מחוברים בקליקה). מכאן ש $(G, K) \in$ Base.

נניח $(G, K) \in$ Base. אז קיימת קבוצת בסיס בגודל k ל- G. נבנה כיסוי ל U בגודל k. אם קבוצת הבסיס מכילה רק קדקודים שמתאימים לקבוצות $S_{i_1}, \dots, S_{i_k}$ אז הקבוצות האלה הן כיסוי ל U וסיימנו (כיוון שהבסיס הוא שכן של כל קדקודי הגרף וקדקוד-קבוצה שכן של קדקוד-איבר אם"ם האיבר שייך לקבוצה). אחרת ניתן להחליף קדקוד-איבר u ששייך לבסיס בקדקוד- קבוצה שלא שייך לבסיס בצורה הבאה :אם קיים קדקוד-קבוצה S_i שמחובר ל u ואינו שייך לבסיס החלף את u ב S_i, אחרת החלף את u בקדקוד-קבוצה שלא שייך לבסיס .קיבלנו כי כל u כזה מכוסה ע"י קבוצה אחת לפחות. לכל u שהקדקוד שלו לא היה בבסיס קיים קדקוד-קבוצה בבסיס. לכן U מכוסה ע"י קבוצת הקבוצות שהגדרנו שגדלה k.
לכן $(S_1, S_2, \dots, S_l, k) \in Set - Cover$.

<u>סעיף ב'</u>:

עבור אינדקס (i, j) של תא ריק במטריצה $M_{n^2*n^2}$ ומספר טבעי $v \in \{1, \dots, n\}$ נסמן $up(M_{n^2*n^2}, i, j, v)$ מטריצה חדשה באותו הגודל כך שבכל תא ששונה מ (i, j) ערכי המטריצה זהיים ובתא (i, j) הוצב הערך v.

בהינתן מופע של $M_{n^2*n^2}$ של $FindSudoku(M_{n^2*n^2})$:

1. עבור כל אינדקס (i, j) של תא ריק במטריצה $M_{n^2*n^2}$:
  1.1. עבור כל מספר טבעי $v \in \{1, \dots, n\}$:
    1.1.1 אם $Sudoku(up(M_{n^2*n^2}, i, j, v)) = true$ אז
      1.1.1.1 $M_{n^2*n^2} \leftarrow up(M_{n^2*n^2}, i, j, v)$
      1.1.1.2 חזור ל **1.**
  1.2. החזר אין פתרון!
2. החזר את $M_{n^2*n^2}$

נשים לב ש $Sudoku(up(M_{n^2*n^2}, i, j, v))$ בודק האם יש פתרון לבעיה שבו בתא (i, j) בעל ערך v. כלומר אם לכל ערך אפשרי $v \in \{1, \dots, n\}$ השאילתה מחזירה false זה אומר שאין אף פתרון לבעיה ולכן נגיע ל **1.2** ונחזיר שאין פתרון. ברגע שמצאנו ערך שמחזיר true נעדכן את המטריצה ונמשיך למצוא באותו האופן ערכים לשאר התאים הריקים במטריצה.

מה זמן ריצה של האלגוריתם?
ישנם לכל היותר $n^2 * n^2$ תאים ריקים, לכל תא אנחנו בודקים במקרה הגרוע n ערכים.
כלומר סך הכל נבצע לכל היותר n^5 קריאות ל קופסה השחורה שפותרת את בעיית ההכרעה.

כמו כן נתון שעבור בעיית זו קיים אלגוריתם פולינומיאלי כלומר זמן הריצה שלו הוא $O(n^k)$ עבור k טבעי כלשהו. לכן סה"כ זמן הריצה הכולל הוא $O(n^{k+5})$.