אוטומטים ושפות פורמליות - תרגיל בית 1

נא להגיש עד ה 19.12.2019 דרך המודל. ההגשה היא בזוגות. התייעצות מותרת, אך חובה לרשום את הפתרונות לבד (כל אחד כמחצית מהשאלות).

סודיות של מערכות הצפנה, ומושגים מתמטיים שימושיים בהקשר זה

1. בהרצאה טענו שהגדרה 2 והגדרה 3 של בטיחות סטטיסטית של מערכת הצפנה הן שקולות. הוכיחו שהגדרה 2 גוררת את הגדרה 3 (כלומר כל מערכת הצפנה המקיימת את הגדרה 2, מקיימת את הגדרה 3).

2. פונקציות זניחות (תוכלו לפתור רק אחרי ה 19.11)

   א. יהיו $g_1(n), g_2(n) : \mathbb{N} \to \mathbb{R}^+$ פונקציות זניחות. הוכיחו (במדוייק, מההגדרה) כי הפונקציה $f(n) = g_1(n) + g_2(n)$ גם היא זניחה.

   ב. השתמשו בסעיף הקודם, והוכיחו שלכל t פונקציות זניחות $g_1, g_2, \ldots, g_t$,

$f(n) = \sum_{i=1}^{t} g_i(n)$ גם זניחה. ניתן להוכיח זאת באינדוקציה פשוטה על t.

ג. הוכח שסכום של $t(n)$ פונקציות זניחות יכול להיות פונקציה שאינה זניחה (כאן t אינו מספר קבוע, אלא פונקציה של n). הסבירו בקצרה מדוע ההוכחה מהסעיף הקודם אכן אינה עובדת למספר לא קבוע של פונקציות.

ד. הוכח או הפרך : אם g אינה פונקציה זניחה, אזי קיים פולינום $p(n)$ ומספר n_0 כך שלכל $n > n_0$ מתקיים $g(n) \geq 1/p(n)$.

3. נניח ש $G : \{0,1\}^* \to \{0,1\}^*$ הוא גנרטור פסוודו אקראי עם $\ell(n) = n + 10$.

א. תנו חסם תחתון וחסם עליון טוב ככל שתוכלו על המרחק **הסטטיסטי** בין $G(U_n)$ ל $U_{\ell(n)}$ עבור $n = 20$. הסבירו מדוע לא קשה לממש מבחין המקיים את החסם התחתון על יתרון האבחנה שקיבלתם עבור n זה (רמז: יתרון גדול למדי). הסבירו מדוע זה לא סותר את העובדה שיתרון האבחנה של כל מבחין יעיל הוא פונקציה זניחה.

ב. בסעיף זה נתבונן במבחינים יעילים לא יוניפורמיים. אינטואיטיבית, מבחין כזה מקבל בנוסף רמז "קצר" לכל אורך קלט. פורמלית, נאמר ש A הוא מבחין לא יוניפורמי יעיל עם יתרון אבחנה $\epsilon(n)$, אם קיים פולינום $p(n)$ כך בנוסף לקלט שלו x האלגוריתם מקבל "רמז" y באורך $p(|x|)$ כך שקיימת סדרת קלטים אינסופית $y_1, y_2, \ldots$ כך ש $|y_i| = p(i)$ ומתקיים לכל n

$$|Pr_{x \leftarrow U_n}(A(1^n, G(x), y_n) = 1) - Pr_{x \leftarrow U_{\ell(n)}}(A(1^n, x, y_n) = 1)| = \epsilon(n)$$

יהי A מבחין לא יוניפורמי יעיל עבור ה PRG מהסעיף הקודם (בפרט יתרון האבחנה שלו זניח). הראו שקיים מבחין לא יוניפורמי יעיל A'

שעבור כל n גדול מספיק יתרון האבחנה שלו $\epsilon'(n)$ גדול ממש מיתרון האבחנה של A.

אלגוריתמים הסתברותיים

1. בשאלה זו נראה כיצד לשפר יעילות של בדיקת נכונות של מכפלת מטריצות ע"י רנדומיזציה. בבעיה הנתונה, 3 מטריצות נתונות כקלט לבעיה A, B, C. כל אחת מהמטריצות היא בגודל $n \times n$ (עבור אותו n) ומעל שדה סופי. כאן נבחר למשל ב $\mathbb{F}_3$. (כזכור, בשדה זה ישנם רק שלושה איברים 0,1,2 וכפל וחיבור מוגדרים מודולו 3).

   א. הציעו אלגוריתם דטרמיניסטי לבדיקה האם $AB = C$. הראו שסבוכיות זמן הריצה שלו היא $O(n^3)$ פעולות אריתמטיות (כלומר כפלים וחיבורים בשדה $\mathbb{F}_3$).

   ב. בסעיף זה נפתח אלגוריתם הסתברותי לבדיקת הזהות שרץ בזמן $O(n^2)$. האלגוריתם תמיד צודק אם השוויון מתקיים, וטועה בהסתברות $1/1000$ אם השוויון לא מתקיים.

   1. (רמז 1) בהנתן מטריצה A בגודל $n \times n$ מעל $\mathbb{F}_3$ הראו שעבור וקטור r באורך n שנבחר באקראי (מעל $\mathbb{F}_3$ אם $A \neq 0$ אז ההסתברות ש $rA \neq 0$ גדולה מ $1/2$ (כנראה תקבלו חסם מדוייק, רשמו אותו והסבירו מהו).

   2. שימו לב כי $r(AB) = (rA)B$ הסבירו בשתי מילים מדוע זה נכון (ממש בשתי מילים, זה משהו שלמדתם בקורס אלגברה לינארית לגבי מטריצות). אפשר כמובן גם להראות ישירות, אם תרצו.

   3. השתמשו ב 1,2 בתור רמזים לפיתוח האלגוריתם (ההסתברותי) שלכם. הציעו אלגוריתם לבדיקת השוויון, והוכיחו שהוא רץ בזמן $O(n^2)$. השוו לאלגוריתם הדטרמיניסטי

בנוסף (n) כל הסיכוי לאלגוריתם הסתברותי
הנאיבי לבצוע ההשוואה.

2. בשאלה זו ננתח אלגוריתם הסתברותי יעיל לבדיקת ראשוניות. האלגוריתם פותח ע"י Miller ו Rabin ב 1980, והוא האלגוריתם הראשון שעובד נכון (פרט לטעות קטנה) לכל קלט. אלגוריתם זה הוא הכללה של הרעיון שאם n ראשוני אז $a^{n-1} = 1$ מודולו n לכל a (משפט פרמה הקטן). לשמחתינו, אם n פריק, הבדיקה עובדת לא רע, אך לא לכל קלט.

א. בשאלה זו נפתח את אלגוריתם MR (לא להיבהל, רב העבודה הקשה תעשה כאן בשבילכם :). המשפט הבא הוא נכון (ללא הוכחה, אתם מוזמנים לחפש את ההוכחה באינטרנט ולהבין אותה. זה בהחלט אפשרי עם רקע מסויים בתורת המספרים).

משפט: יהי $n > 2$ מספר אי זוגי. נסמן $n - 1 = 2^s \cdot d$ כאשר d מספר אי זוגי. אזי, אם n ראשוני, מתקיים לכל a בקבוצה $A = \{a|0 < a < n, gcd(a, n) = 1\}$

$a^d = 1 \bmod n$ or $a^{2^r d} = -1 \bmod n$ for some $0 \leq r < s$ $(*)$.

יתרה מזאת, אם n אינו ראשוני, אז לפחות $3/4$ מהאיברים בקבוצה A אינם מקיימים את התנאי (*) לעיל (זה החלק היותר מעניין בהוכחת המשפט). בנה אלגוריתם הסתברותי יעיל (פולינומי באורך הקלט) לבדיקת ראשוניות על סמך המשפט, הטועה בהסתברות $O(1/n)$.

ב. מה סבוכיות זמן הריצה של האלגוריתם מהסעיף הקודם (כאן נמדוד זמן ריצה במספר פעולות כפל וחיבור מודולו n)? השוו לסבוכיות האלגוריתם הדטרמיניסטי הנאיבי המחפש מחלקים עד השרש.

ג. (בונוס 3 נקודות לציון הסופי) אלגוריתם MR שראינו משפר על פני האלגוריתם לבדיקת

ראשוניות המתבסס על משפט פרמה הקטן. בגרסתו המוכרת יותר, המשפט טוען $a^{n-1} \equiv 1(\ mod\ n)$ לכל n ראשוני ומספר $a < n$ הזר ל n. המשפט משמש לבדיקת ראשוניות, כיוון שבדרך כלל מקרים השוויון אינו מתקיים ל n שאינו ראשוני עבור "רבים" מה a הזרים ל n. עובדה זו גוררת קיום אלגוריתם הסתברותי פשוט לבדיקת ראשוניות שעובד לרוב הקלטים. אולם, כיוון שקיימים n-ים פריקים, הנקראים מספרי Carmichael, המקיימים את התנאי לכל a, מה שגורם לאלגוריתם לעיל לא לעבוד נכון על קלטים אלה. כאן נתבונן בהכללה של משפט פרמה, ונבין טוב יותר מה קורה במספרי Carmichael. באופן כללי, מתקיים $a^{\phi(n)-1} = 1(mod\ n)$

לכל מספר $n \geq 2$. הוכחת המשפט המוכלל היא כדלקמן: לכל מספר ב $\mathbb{Z}_n$,החבורה החיבורית מודולו n. כזכור, חבורה אבלית היא

קבוצה עם פעולה אסוציאטיבית וקומוטטיבית $*$, שבה קיים איבר אדיש e המקיים $a * e = a$ לכל איבר, וכן קיים הופכי b לכל איבר a, המקיים $a * b = e$). במקרה שלנו $*$ היא פעולת החיבור מודולו n. בחבורה סופית, הסדר של איבר מוגדר בתור המספר המינימלי x כך ש $a^x = e$ (כאן a^x מסמל סדרה $a * a \ldots * a$) באורך x. ממשפט Lagrange, לכל חבורה סופית בגודל m, הסדר של כל איבר בחבורה מחלק את m. כעת, הטענה נובעת מהסתכלות על החבורה הכפלית $\mathbb{Z}_n^*$. גודלה של חבורה זו הוא $\phi(n)$ ולכן הסדר של כל איבר בה מחלק את גודל החבורה. כעת, לשאלה..

מספר Charmichael בקטן ביותר הוא **561**. הוכיחו שזהו אכן מספר Charmichael. הדרכה: חשבו מהם הסדרים האפשריים של איברים ב $\mathbb{Z}_n^*$, והראו שכל אחד מהם מחלק את $\phi(n)$. לשם כך, תוכלו לקרא את העמוד

לכן, המכלל לקבל את הטענה.

על מבנה החבורה $\mathbb{Z}_n$ ממנו נובע ש $\mathbb{Z}_n$
איזומורפית לחבורה מהצורה
$\mathrm{A}_1 \times A_2 \times \ldots \times A_w$ שכל אחת מהן ציקלית.
השתמשו במבנה המסויים הנובע מהמשפט עבור
$\mathbb{Z}_{561}$.