**ממ"ן 15 אלגוריתמיקה**

**שאלה 1**

*א.*

*רעיון האלגוריתם*

בשביל לבדוק אם מספר נתון N הוא ראשוני מספיק לבדוק אם קיים מספר שלם בין 2 ל שמחלק את N כי אם יש מספר שלם שמחלק את N אז גם הוא מספר שלם שמחלק את N (הרי ) ומתקיים *.*

*האלגוריתם*

*בשביל לבדוק בזמן קבוע אם* N *הוא ראשוני נשתמש ב מעבדים ומשתנה בוליאני משותף* prime *שמאותחל ל*TRUE*. כל מעבד יבדוק מספר אחד* בין 2 ל*, אם המספר מחלק את* N *אז זה אומר ש*N *לא ראשוני לכן המעבד יעדכן את* prime *ל*FALSE. *בסוף האלגוריתם יחזיר* prime*.*

*(1)*

*(2) תשתמש בצורה מקבילית ב מעבדים כך שעבור המעבד ה* i*(כאשר* i *בין 1 ל): אם* i+1 *מחלק את*  N *אז* *.*

*(3) החזר*

*זמן ריצה*

*כל מעבד מבצע רק פעולות בזמן קבוע (בדיקת חלוקה של* N *מתבצעת על ידי פעולת החילוק שנתון שהיא מתבצעת בזמן קבוע וגם עדכון משתנה מתבצע בזמן קבוע) ופעולות המעבדים מתרחשות בצורה מקבילית לכן האלגוריתם קץ בזמן קבוע.*

*נכונות*

*אם* N *הוא ראשוני אז הוא לא מתחלק בשום מספר שלם חוץ מעצמו ו1 ובפרט הוא לא מתחלק בשום מספר* בין 2 ל לכן תנאי הif לא יתקיים בכל המעבדים וערך המשתנה prime יישאר TRUE*.*

*אם* N *הוא לא ראשוני אז קיים מספר שלם שמחלק אותו.*

1. *אם אז יהיה מעבד שיבדוק את x, יגלה שהוא מחלק את* N *וישנה את* prime *ל*TRUE.
2. אם אז כמו שהסברנו קודם בהכרח הוא מספר שלם שמחלק את N ומתקיים  *לכן קיים מעבד שיבדוק את x, יגלה שהוא מחלק את* N *וישנה את* prime *ל*TRUE.

*האלגוריתם משתמש בסדר גודל של מעבדים וזהו לא מספר סביר כי מתייחסים לגודל הקלט כמספר הסיביות הדרושות בשביל לייצג את* N *(מדובר על סיביות) ומתקיים וזוהי כמות מעריכית.*

*ב.*

*רעיון האלגוריתם*

*כמו בסעיף א' נשתמש ב מעבדים שייבדקו* אם קיים מספר שלם בין 2 ל שמחלק את N רק שהפעם כל מעבד יכתוב את תשובתו לתא שמיועד לו במערך A, TRUE אם הערך הנבדק מחלק את N וFALSE אם לא*.*

*לאחר שכל הערכים במערך עודכנו נצטרך לבדוק אם יש במערך תא עם הערך* TRUE *(אם קיים כזה זה אומר שיש מספר שלם שונה מ1 ומ*N *שמחלק את* N *ואז* N *אינו ראשוני).* *נבצע את הבדיקה בעזרת שגרה שבה כמות המעבדים היא חצי מגודל המערך וכל מעבד מבצע שער לוגי* OR *ושומר את התוצאה במערך חדש*. *בדרך זו יתקבל מערך חדש* *שגודלו* *חצי מהמערך המקורי כך שבמערך החדש יש ערך* TRUE *אם ורק אם גם במערך המקורי היה ערך* TRUE, *נקרא שוב לשגרה בצורה רקורסיבית על המערך המתקבל עד שנקבל מערך עם תא אחד ונחזיר את ערך התא. (שגרה זו מבוססת על פתרון בעיית הספיקות בשיעור המקוון מספר 8).*

*האלגוריתם*

*שגרה ראשית:*

*(1) צור מערך בוליאני* A  *בגודל*

*(2) בדיקת חלוקה של מעבד* i *(כאשר* i *בין 1 ל): אם* i+1 *מחלק את* N *אז , אחרת*

*(3) החזר* Check(A)

*השגרה שמקבלת מערך A ובודקת אם יש במערך תא עם ערך* TRUE*:*

Check(A)*:*

*(1) הגדר משתנה ששווה לגודל המערך* A

*(2) אם החזר את ערך האיבר היחיד ב*A

*(3) אחרת:*

*(3.1) צור מערך* B *בגודל*

*(3.2) תשתמש בצורה מקבילית ב מעבדים כך שעבור המעבד ה*i*:*

*(3.3) החזר* Check(B)

*זמן ריצה*

*בשגרה* Check *בכל צעד מחלקים את גודל המערך ב2 עד שגודל המערך הוא 1 וחוץ מהקריאה הרקורסיבית כל הפעולות רצות בזמן קבוע לכן זמן הריצה הוא .*

*בשגרה הראשית שורות 1 ו2 רצות בזמן קבוע ובשורה 3 משתמשים ב* Check*על מערך בגודל לכן זמן הריצה שלה הוא וזהו זמן פולינומי בגודל הקלט (מספר הסיביות של* N*) כנדרש.*

*נכונות*

*תחילה נראה נכונות לשגרה* Check *באינדוקציה על גודל המערך הבוליאני* A.

*אם גודל המערך הוא 1*

*אם ערך התא היחיד הוא* FALSE *אז בוודאות אין תא אחר שערכו* TRUE *לכן האלגוריתם יחזיר* FALSE *(וזהו ערך התא) ואם ערך התא הוא* TRUE *אז קיים תא שערכו* TRUE *לכן האלגוריתם יחזיר* TRUE *(וזהו ערך התא).*

*אם האלגוריתם עובד על כל מערך שגודלו קטן מ*N *אז עבור מערך בגדול* N

*כל מעבד בודק שני תנאים שונים ואין חריגה מגודל המערך (עבור* i=1 2i-1=1 *ועבוק* i= *אז* 2i=N*) כך שכל התאים נבדקים.*

*אם לא קיים במערך תא שערכו* TRUE *זה אומר שכל ערכי המערך הם* FALSE *ולכן כל המעבדים יכתבו ל*B FALSE *(הרי* FALSEORFALSE = FALSE*)* *מה שאומר שגם ב*B *לא קיים תא שערכו* TRUE *וערכו של* B הוא *ולפי הנחת האינדוקציה הקריאה הרקורסיבית תחזיר* FALSE*.*

*אם קיים במערך תא שערכו* TRUE *אז המעבד שיבדוק אותו בוודאות יכתוב* TRUE *ב*B *(הרי ביצוע OR על שני ערכים שידוע שאחד מהם (לפחות) הוא* TRUE *בוודאות יחזיר* TRUE*)* *מה שאומר שגם ב*B *קיים תא שערכו* TRUE *ולפי הנחת האינדוקציה הקריאה הרקורסיבית תחזיר* TRUE.

**שאלה 2**

*א.*

*הפתרון לא נכון כי יכול להיות מצב שבו שני המעבדים מבצעים את הקטע הקריטי במקביל.*

המשתנים *ו* *מאותחלים בערך 'לא' וערכם יכול להשתנות ל 'כן' רק בשורה 3.*

*יכול להיות מצב ש* *ביצע את הבדיקה בשורה 2 וראה ש* הוא 'לא' אבל לפני *ש* הספיקלעדכןאת ל 'כן' בשורה 3 *ביצע את הבדיקה בשורה 2 וראה ש* הוא 'לא' והתקדם גם לשורה 3 ואז זה אפשרי ששני המעבדים יגיעו לשורה 4 ויבצעו את הקטע הקריטי במקביל.

*כלומר יכול לקרות ששני המעבדים עוברים בתשובה חיוביות את הבדיקה בשורה 2 ממש באותו זמן וזה יכול להוביל למצב ששני המעבדים מבצעים את הקטע הקריטי במקביל ולכן הפתרון לא נכון*

*ב.*

*הפתרון לא יהיה נכון לאחר ההחלפה כי יכול להיות קיפאון, למשל אם מבצע את שורה 2 ומעדכן את ל- 'כן' ומיד לאחר מכן מבצע את שורה 2 ומעדכן את ל- 'כן' אז הגענו למצב ששני המעבדים בשורה 3 והערכים של ושל הם 'כן' מה שאומר ששני המעבדים לא יכולים להתקדם (כי הם מחכים שה*X *המקביל ישתנה) וקיבלנו מצב של קיפאון.*

**שאלה 3**

*א. ,*RP *היא מחלקת סיבוכיות שמכילה את כל בעיות ההכרעה שקיים אלגוריתם אקראי שפותר אותן בזמן פולינומי כך שההסתברות לטעות עבור קלטים שעבורם התשובה היא* TRUE *קטנה מחצי ועבור קלטים שעבורם התשובה היא* FALSE *האלגוריתם תמיד יחזיר* FALSE*.*

*דוגמא לבעיה השייכת ל*RP

*נתון מערך* A *בגודל* N *של מספרים שלמים, בדוק האם יש במערך איבר אי זוגי.*

*אפשר לכתוב אלגוריתם שבודק אקראית*  *תאים* *שונים* *במערך*, *אם אחד מהם אי זוגי האלגוריתם יחזיר* TRUE *ואם כולם זוגיים יחזיר* FALSE.

*אם אין איבר אי זוגי אז בוודאות לא ימצא כזה בין התאים שנבדקים והאלגוריתם יחזיר* FALSE*. אם קיים איבר אי זוגי אז ההסתברות שהאלגוריתם "ימצא" אותו (ויחזיק* TRUE*) ב התאים שנבדקים היא לכן ההסתברות שלו לטעות (ולהחזיר* FLASE*) היא (פחות מחצי).*

*בנוסף זמן הריצה הוא פולינומי (מעבר על*  *תאים סך הכל ).*

*ב.*

*בהינתן בעיה* X *ב*RP, *ידוע שקיים אלגוריתם אקראי S שפותר אותה בזמן פולינומי כך שההסתברות שלו לטעות קטנה מחצי עבור קלטים שעבורם התשובה היא* TRUE *ואפס עבור קלטים שעבורם התשובה היא* FALSE*.*

*ניצור אלגוריתם חדש* S' *שמריץ את* S *פעמיים בצורה הבאה:*

*(1) הרץ את S*

*(2) אם S החזיר* TRUE *החזר* TRUE

*(3) אחרת (S החזיר* FALSE*) הרץ שוב את S*

*(4) אם הפעם S החזיר* TRUE *החזר* TRUE *אחרת החזר* FALSE

*אם התשובה לבעיה היא* FALSE *אז לפי הגדרת RP S תמיד יחזיר* FALSE *לכן S' גם יחזיר* FALSE *אחרי ההרצה השנייה של S (הסתברות של 1 וכמובן ש- ).*

*אם התשובה לבעיה היא* TRUE *אז ההסתברות שS יחזיר* FALSE *היא לכל היותר לכן ההסתברות שS יחזיר* FALSE *פעמיים היא לכל היותר* לכן הסיכוי שS' יטעה קטן מ (הרי )*.*

*לפי הגדרת RP S רץ בזמן פולינומי לכן גם אלגוריתם זה המריץ את S פעמיים רץ בזמן פולינומי.*

**שאלה 4**

**א.**

**בשיטתו של כלומסקי** Prod **מחושב על ידי העלאת מספר ראשוני בריבוע כך שאם** Prod=P\*Q **אז** P=Q.

**לפי המפתח הציבורי אנחנו יודעים ש-** Prod=961 **לכן אפשר למצוא את המספר הראשוני על ידי חישוב שורש** Prod**,** **בדרך זו נקבל שהמספר הראשוני הוא**  ***כלומר ומכאן נקבל***

***.***

***בשלב זה ידועים לנו*** R ***ו*** Publ ***(לפי המפתח הציבורי*** Publ=53***) ומכאן נקבל ש-***Priv ***זר ל900 וש-*****כלומר**  **(כאשר** k **מספר שלם אי שלילי) ונקבל כאשר ידוע ש**Priv **מספר שלם חיובי*, נשים לב שאם נציב ל***k=1  ***נקבל*** Priv=17 ***לכן*** .

***המספר 53 הוא ראשוני ו900 לא מתחלק בו לכן הם זרים מה שאומר שבוודאות*** k-1 ***מתחלק ב53 ללא שארית וקיבלנו ש*** ***כאשר*** d  ***מספר שלם אי שלילי.***

***לפי כמה מקורות מהימנים באינטרנט ב***RSA ***קיימת ההגבלה*** Priv<R ***ולפי הגבלה זו נקבל*** Priv=17 ***(כי אם אז ואז*** d=0***).***

***ב.***

***לדעתי הצעתו של כלומסקי היא לא טובה.***

***אם במקום להכפיל שני מספרים ראשוניים אחד בשני מכפלים מספר ראשוני אחד בעצמו אפשר בקלות למצוא את המספר הראשוני הזה לפי המפתח הציבורי (על ידי חישוב השורש הריבועי של*** Prod***).***

***לפי עמוד 318 בספר אפשר לחשב באמצעות*** P, Q ***ו-*** Publ ***(שנתון במפתח הציבורי) את*** Priv ***לכן בשיטתו של כלומסקי אפשר לקבל מהמפתח הציבורי את המפתח הפרטי ואז כולם (לפחות כל מי שיש לו מפצח ציבורי) יוכלו לפענח בקלות הודעות שמוצפנות בשיטת ה***RSA ***של כלומסקי.***

**שאלה 5**

***א.***

***נניח בשלילה שאפשר לצבוע את הקשתות של***  ***ב4 צבעים, דרגתו של כל קודקוד היא 4 מה שאומר שמכל קודקוד יוצאת קשת בכל צבע (אחרת יש 2 קשתות באותו צבע שיוצאות מאותו קודקוד והצביעה לא חוקית) לכן כל צבע הוא שידוך מושלם (קבוצה של קשתות כך שכל קודקוד בגרף הוא קצה של קשת אחת בדיוק מהקבוצה) וקיבלנו סתירה כי לא יכול להיות שידוך מושלם בגרף עם מספר אי זוגי של קודקודים (כל קשת מחברת בין שני קודקודים ויש מספר שלם של קשתות לכן חייב להיות מספר זוגי של קודקודים).***

***ב.***

***נניח שלבועז יש את השגרות הבאות:***

1. ***שגרה*** gtn(graph to number) ***שממירה גרף לערך מספרי בצורה חד חד ערכית ועל***
2. ***שגרת הצפנה*** Encr ***ושגרת פענוח מתאימה*** Decr
3. ***שגרה*** valid ***שמקבלת גרף וצביעה שלו ובודקת האם זו צביעה חוקית בארבעה צבעים*** ***(מחזירה 1 אם כן ו0 אם לא).*** ***בהכרח קיימת שגרה פולינומית כזאת כי ידוע שבעיית צביעת הקשתות שייכת ל***NP***.***
4. ***שגרה*** possible\_coloring ***שמקבלת גרף*** G ***וצביעה*** C ***ומחזירה*** Encr(gtn(G)+valid(G,C))

***הפרוטוקול הולך ככה:***

1. ***בועז שולח לאיה תוכנה שמבצעת את*** possible\_coloring ***כך שאיה יכולה להריץ את התוכנה אבל לא לקרוא את המימוש שלה***
2. ***איה מריצה את התוכנה ושלחת את הפלט לבועז***
3. ***בועז מקבל מאיה את הפלט שנסמנו ב***X ***ובודק את הערך של*** Decr(X)-gtn(G) ***אם הערך הוא 1 אז איה מצאה צביעה חוקית ואם הערך הוא 0 אז איה לא מצאה צביעה חוקית (הרי*** Decr(X)-gtn(G)= Decr(Encr(gtn(G)+valid(G,C)))-gtn(G)= gtn(G)+valid(G,C) -gtn(G)= valid(G,C)***). אם הערך הוא לא 0 ולא 1 זה סימן שאיה לא השתמשה ב*** possible\_coloring***על הגרף*** G  ***ושהיא כנראה ניסתה "לשקר" לבועז.***

***איה לא יכולה להשתמש בשגרות*** gtn,Encr ***ו-*** Decr, ***בשביל שבועז יאמין לתשובה של איה היא חייבת לשלוח לו הודעה שמוצפנת עם*** Encr ***(אחרת שבועז יפעיל את*** Decr ***הוא יקבל ערך לא הגיוני) והדרך היחידה שלה לעשות את זה היא באמצעות*** possible\_coloring***.***

***אם איה תפעיל את*** possible\_coloring ***על גרף*** G***' שונה מהגרף הנתון*** G ***וצביעה*** C ***אז בועז יגלה את זה כי הוא יחסיר מהערך המפוענח את*** gtn(G) ***ואז יקבל תשובה שהיא כמעט בוודאות לא 1. האפשרות היחידה שבכל זאת יתקבל 1 היא ש*** gtn(G')= gtn(G)+1***ו***valid(G',C) =0 ***ואז בועז יקבל*** gtn(G')+valid(G',C) - gtn(G)= gtn(G)+1+0 - gtn(G) = 1 ***אבל בגלל ש***gtn ***היא חד חד ערכית ועל יש רק גרף*** G' ***אחד*** ***שמקיים*** gtn(G')= gtn(G)+1 ***מתוך אינסוף גרפים אפשריים לכן הסיכוי שאיה תבחר בגרף כזה הוא אפסי.***

**שאלה 6 (בונוס)**

***אני חושב שההגדרה הזו לא מספיק טובה, יש הרבה דברים שאנו עושים היום בעזרת המחשבים שבעבר אנשים לא היו מאמינים שמחשבים יכולים לעשות. לדוגמא לפני 50 שנים אנשים לא היו מאמינם שאפשר באמצעות מחשב לנווט ממקום למקום והיום לכל אחד יש תוכנת ניווט (למשל*** waze***) בטלפון למרות שתוכנות אלה לא משתמשות בבינה מלאכותית (מערכות ניווט כאלה כנראה מייצגות את הדרכים כגרף ממושקל ומריצות את האלגוריתם של דייקסטרה).***

***המחשבות של אנשים על מחשבים נובעות ממה שהם מכירים אבל הטכנולוגיה מתפתחת ועם הזמן יש עוד ועוד חידושים שלא בהכרח קשורים לבינה מלאכותית וגורמים למחשבים לעשות דברים שאנשים לא האמינו שמחשבים יכולים לעשות.***