### בבחינה שש שאלות.

עליכם לענות על **חמש** שאלות מתוכן.

**יש לכתוב את הבחינה בעט**.

**ב ה צ ל ח ה !**

### שאלה 1 (20 נקודות)

ניתן לבדוק אם מספר שלם מתחלק ב-7 ללא שארית באופן הבא:

מכפילים את ספרת האחדות של המספר ב-2 ומחסירים את התוצאה מהמספר ללא ספרת האחדות.

אם תוצאת החישוב איננה חד-ספרתית, אז חוזרים על התהליך עם הערך המוחלט של התוצאה עד שמקבלים תוצאה חד-ספרתית.

אם תוצאת החישוב היא 0, 7, או 7- אז המספר מתחלק ב-7; אחרת, המספר אינו מתחלק ב-7.

דוגמה: המספר 861 מתחלק ב-7 מכיוון ש- 86 − (2⋅1) = 84

8 − (2⋅4) = 0

כתבו אלגוריתם, המקבל כקלט מספר טבעי x ובודק (באופן המתואר לעיל) אם x מתחלק ב-7 ללא שארית.

### שאלה 2 (20 נקודות)

א. להלן מופיע תיאור סכמטי של אלגוריתם הבודק אם עץ בינרי נתון הוא עץ **חיפוש** בינרי:

(1) לכל צומת בעץ בצע:

    (1.1) השווה את ערך הצומת עם בניו. אם ערך הצומת גדול ממש מערכו של בנו הימני או

ערך הצומת קטן ממש מערכו של בנו השמאלי אז החזר FALSE.

(2) החזר TRUE.

האם אלגוריתם זה נכון ? אם כן, הוכיחו; אם לא, תנו דוגמא נגדית.

ב. להלן תיאור סכמטי של אלגוריתם נוסף לפתרון אותה בעיה:

(1) סרוק את העץ בסריקת ביקור-שני;

(2) בדוק אם רשימת הערכים שהתקבלה היא ממוינת. אם כן – החזר TRUE ועצור.

(3) החזר FALSE.

האם אלגוריתם זה נכון ? אם כן, הוכיחו; אם לא, תנו דוגמא נגדית.

**שאלה 3 (20 נקודות: סעיפים א', ב': 5 נק' לכל אחד; סעיף ג' - 10 נק')**

להלן תיאור לא פורמלי של אלגוריתם שהציע פרופ' כלומסקי לבעיית הסוכן הנוסע:

(1) כל עוד לא בקרת בכל הערים בצע:

(1.1) לך לעיר הכי קרובה אליך שבה טרם בקרת;

(2) חזור לעיר המוצא.

א. מהי השיטה שבה משתמש האלגוריתם ? נמקו את תשובתכם.

ב. מהי סיבוכיות הזמן של האלגוריתם (כפונקציה של מספר הערים) ?

ג. האם האלגוריתם מוצא את הפתרון האופטימלי לבעיה ? הוכיחו או תנו דוגמה נגדית.

**שאלה 4 (20 נקודות)**

נדון בגרסה הבאה לבעיית נחש הדומינו:

**הקלט לבעיה**: קבוצה סופית T של סוגי מרצפות ושלוש נקודות שונות V, W ו- W' במחצית העליונה של המישור האינסופי.

**השאלה**: האם ניתן להגיע מ-V ל- Wבאמצעות נחש דומינו אשר "מתפתל" רק במחצית זו של המישור האינסופי ועובר דרך W' ?

הוכיחו שגם גרסה זו של בעיית נחש הדומינו היא בלתי כריעה.

### שאלה 5 (20 נקודות)

נניח שבמערכת RSA המספר Prod היה מתקבל ע"י העלאה בריבוע של מספר ראשוני גדול (במקום ע"י כפל של שני מספרים ראשוניים).

הוכיחו שבמקרה זה המערכת ניתנת לפיצוח והסבירו במפורט כיצד ניתן לפצח אותה.

**שאלה 6 (20 נקודות: 2 נק' לכל סעיף)**

לכל אחת מהטענות הבאות – סמנו **נכון / לא נכון** (אין צורך לנמק):

א. אם קיימת איזושהי בעיה ב-NP שיש לה פתרון פולינומיאלי, אז P = NP.

ב. NP ≠ NPC ⇒ P ≠ NP

ג. נתון גרף בלתי מכוון G בעל n צמתים. אם דרגת כל צומת ב-G היא לפחות n/2, אז קיים ב-G

מסלול המילטוני.

ד. אם יש רדוקציה פולינומיאלית מבעיה B לבעיה A ובעיה A שייכת ל-NP, אז גם B שייכת ל-NP.

ה. אם כל אחת מהקבוצות X ו-Y בבעיית התאמת המילים מכילה מספר סופי של מילים, אז

הבעיה כריעה.

ו. בעיית העצירה שייכת למחלקה RE.

ז. אוטומט סופי לא-דטרמיניסטי הוא מודל חישובי חזק יותר מאוטומט סופי דטרמיניסטי.

ח. ידוע שמכונת טיורינג לא-דטרמיניסטית שזמן ריצתה פולינומיאלי היא מודל חישובי חזק יותר

ממכונת טיורינג דטרמיניסטית שזמן ריצתה פולינומיאלי.

ט. לא קיים לבעיית מחסום הדרכים אלגוריתם מקבילי, שמשתמש במספר פולינומיאלי של

מעבדים וזמן ריצתו פולינומיאלי.

י. אם עבור בעיה A קיים אלגוריתם סדרתי שזמן ריצתו T, אז בהכרח קיים עבור A אלגוריתם

מקבילי שמשתמש בשני מעבדים וזמן ריצתו T/2.

**ס ו ף**