האוניברסיטה הפתוחה

20290

אלגוריתמיקה -
יסודות מדעי המחשב

השלמות לחוברת הקורס

כתב: אייל משיח

פנימי – לא להפצה.

תוכן העניינים

1. תיאור הקורס

הקורס "אלגוריתמיקה - יסודות מדעי המחשב" מבוסס על תרגום לעברית של ספרו של פרופ' דוד הראל:

The Science of Computing:Exploring the Nature and Power of Algorithms, Addison-Wesley, 1989.

בתוספת מדריך למידה.

הספר סוקר נושאים יסודיים ובסיסיים במדעי המחשב. הוא מתרכז במושג התהליך המבוצע על-ידי המחשב, ובמושג האלגוריתם – המתכון המחולל תהליך זה– ואינו עוסק במבנה המחשב ובשימוש הפיסי בו או בשפת תכנות מסוימת. בקורס נידונות שאלות כמו: אילו בעיות ניתנות לפתרון באמצעות מחשב, וכיצד? אילו בעיות אינן ניתנות לפתרון כזה, ומדוע?

2. פרקי הלימוד

פרק 1 - הקדמה וסקירה היסטורית
פרק 2 - אלגוריתמים ונתונים
פרק 3 - שפות תכנות
פרק 4 - שיטות אלגוריתמיות
פרק 5 - נכונותם של אלגוריתמים
פרק 6 - יעילותם של אלגוריתמים
פרק 7 - חוסר יעילות ואי-סבירות
פרק 8 - בעיות שאינן ניתנות לחישוב
פרק 9 - אוניברסליות אלגוריתמית וחסינותה
פרק 10 - מקבילות ובו-זמניות
פרק 11 - אלגוריתמים הסתברותיים
פרק 12 - אלגוריתמיקה ואינטליגנציה

3. כיצד ללמוד?

במצורף לספר הלימוד תקבל מדריך למידה, המהווה את "המדריך הצמוד" שלך לאורך הקורס. מדריך הלמידה מכיל הסברים נוספים, דוגמאות ושאלות פתורות.

רצוי להקדיש ללימוד ותרגול החומר כ-10-15 שעות בשבוע. אם אתה נתקל בקשיים תוך כדי לימוד, נצל את ההנחיה הטלפונית או שאל את שאלתך במפגש עם המנחה.

משנראה לך שהבנת היטב את חומר הלימוד, תוכל לגשת לפתרון המטלה. המטלה כוללת, בדרך-כלל, שאלות קשות ומורכבות יותר מאלו המופיעות בפרקי הלימוד, והן נועדו לבדוק את יכולתך ביישום חומר הלימוד.

הלימוד השיטתי של פרקי הלימוד, יחד עם פתרון המטלות, יקנה לך הכנה מלאה לקראת בחינת הגמר.

שמירה על קצב הלימוד המומלץ והגשת המטלות בזמן, ימנעו ממך קשיים בלתי רצויים במהלך הלימודים, ויסייעו לך בהפקת מלוא התועלת מהקורס.

4. תיאור מפגשי ההנחיה

במסגרת הקורס יתקיימו שמונה מפגשי הנחיה במרכזי הלימוד השונים. מידע על מיקום מרכז הלימוד וכן על התאריכים המדויקים של כל מפגש תמצא ב"לוח מפגשים ומנחים".

ההשתתפות במפגשי ההנחיה אינה חובה אך היא בהחלט רצויה.

במפגשים יידון חומר הלימוד השוטף של הקורס ע"פ הפירוט שלהלן. כמו-כן, יוצגו תרגילים ודוגמאות בנוסף לאלו שבחומר הלימוד.

להלן פירוט הנושאים שיידונו במפגשי ההנחיה:

מפגש 1:	פרקים 1-4	מפגש 5:	פרק 8
מפגש 2:	פרק 5	מפגש 6:	פרק 9
מפגש 3:	פרק 6	מפגש 7:	פרק 10
מפגש 4:	פרק 7	מפגש 8:	פרק 11

שים לב: כדי להפיק את מלוא התועלת מהמפגשים מומלץ ללמוד את החומר **לפני** המפגש.

5. בחינות הגמר

הנך זכאי לגשת לבחינת גמר בקורס רק אם עמדת **בכל** דרישות הקורס **לפני** מועד הבחינה (כלומר הגשת מטלות במשקל מינימלי).
בחינות הגמר יחלו כשבוע ימים לאחר תום הסמסטר. הודעה על המועדים המדויקים תישלח לסטודנטים על-ידי מרכז ההישגים הלימודיים במהלך הסמסטר.
מועדי בחינות הגמר שנקבעו לסמסטרים הבאים מפורטים בידיעון האקדמי.

לתשומת לבך!
הנך זכאי להיבחן בקורס פעמיים: במועדים של הסמסטר הנוכחי או במועדים של הסמסטר הבא בו יילמד הקורס. בכך תמצה את זכותך להיבחן בקורס.
סטודנט שניגש לבחינות גמר בשני מועדים ונכשל בשניהם, יוכל להירשם לקורס זה פעם נוספת ולקבל הנחה בשכר הלימוד. פרטים נוספים מופיעים בידיעון האקדמי.

על מתכונת בחינת הגמר ראה בנספח "בחינות גמר לדוגמה" בחוברת זו.
בחינות הגמר לדוגמה מייצגות בחינות שהתקיימו בסמסטרים קודמים. אנו מצרפים בחינות אלה, כדי שתוכלנה לשמש כלי עזר נוסף ללימוד ולעזור בהכנה למבחן.
אין להסיק מכך שהבחינות בסמסטר הנוכחי תהיינה בהכרח זהות במבנה או באופי השאלות לאחת מן הבחינות לדוגמה.

6. נוהל הגשת מטלות מנחה (ממ״ן)

קיימות שתי חלופות להגשת מטלות:

- **שליחת מטלות באמצעות מערכת המטלות המקוונת**

מערכת שליחת המטלות קלה להפעלה, היא חוסכת את הצורך במילוי טפסים, במשלוח דואר ובשמירת עותק של המטלה, ומאפשרת מעקב אחר המטלה.
הגישה למערכת המטלות המקוונת היא דרך אתר הבית של הקורס בקישור ״מערכת המטלות״.

- **שליחת מטלות באמצעות הדואר או הגשה ישירה למנחה במפגשי ההנחיה**

לכל מטלת מנחה עליכם לצרף טופס נלווה אחד.
הקפידו למלא את כל הפרטים בחלק א של הטופס. הכניסו את הטופס (על כל חלקיו הצבעוניים) יחד עם המטלה למעטפה המיועדת לכך ורשמו בכתב יד ברור את כתובתכם (כולל מיקוד!) במקום המיועד לכך.
רשמו את שם המנחה וכתובתו באופן מדויק. (דוגמה לטופס נלווה לממ״ן ראו בהמשך).
השאירו עותק של המטלה בידכם!

מועדי הגשה ומשלוח מטלות בדואר

בעמוד הראשון של כל מטלה מצוין מועד הגשתה. יש לשלוח את המטלה עד ל״מועד האחרון להגשה״ המצוין עבורה. אסור שחותמת הדואר על המעטפה תישא תאריך מאוחר מ״המועד האחרון״ להגשת הממ״ן.

שימו לב: אין לשלוח מטלות בדואר רשום!
הקפידו לרשום את כתובת המנחה בצורה מדויקת כולל מיקוד.

את הממ״ן עליכם לשלוח לבדיקה **רק למנחה שלקבוצתו אתם משובצים**. ממ״ן שיישלח למנחה אחר ללא אישור מראש של מרכז ההוראה ציונו לא ייחשב.
הממ״ן ייבדק ויוחזר לכם תוך שלושה שבועות מהתאריך האחרון להגשת הממ״ן. אם הממ״ן לא יוחזר אליכם במועד זה, אנא התקשרו עם המנחה לבירור סיבת העיכוב.

דחייה בהגשת מטלות

במקרים מיוחדים, כגון שירות מילואים, תוכלו לפנות למנחה שלכם לקבלת אישור לדחיית מועד ההגשה. לכל מטלה המוגשת באיחור צרפו מכתב/אישור המנמק את סיבת האיחור.
בסמכותו של המנחה שלכם לאשר לכם איחור של עד שבוע בהגשת ממ״ן (אלא אם קיבל הנחיות אחרות ממרכז ההוראה). במקרה חריג ביותר שנדרש איחור בהגשה של למעלה מזה יש לבקש אישור של מרכז ההוראה בקורס. מטלות שתגענה באיחור וללא אישור תיבדקנה על-ידי המנחה אך לא יינתן להן ציון והן לא תובאנה בחשבון המטלות המוגשות.

ערעור על ציון בממ״ן

אם יש לכם השגות על הציון שקיבלתם בממ״ן תוכלו להגיש ערעור מנומק בכתב למנחה שלכם בצירוף הממ״ן והטופס המלווה (ההעתק הצהוב), תוך שבוע ימים מיום קבלת הממ״ן.
אם המנחה לא יקבל את ערעורכם, הרשות בידכם לערער בפני מרכז ההוראה בקורס בצירוף הממ״ן והטופס המלווה, תוך שבוע מיום קבלת תשובת המנחה על ערעורכם. החלטת מרכז ההוראה היא סופית.

שימו לב!

את התשובות לממ"נים הנכם מתבקשים לכתוב על דפי פוליו (שורות). כתבו על צדו האחד של העמוד והשאירו שוליים רחבים להערות המנחה (לפחות 5 ס"מ).

האוניברסיטה הפתוחה
הקריה ע"ש דורותי דה רוטשילד
רח' רבוצקי 108 ת.ד. 808 רעננה 43104

לשימוש פנימי

611		21
8-10	3-7	1-2

טופס מלווה למטלה לבדיקה מנחה (ממ"ן)

חלק א - ימולא על-ידי התלמיד
מלא נא את כל הפרטים בעט כדורי בכל המלבנים הכהים וכן למטה.
מספר הקורס והמטלה העתק מתוך השאלון.
כן הקפד לרשום את כל תשע הספרות של מספר הזהות (גם אפסים וסיפרת ביקורת)
שלח את כל העתקים בצירוף המטלה אל מנחה קבוצתך.

מטלה	קורס	מספר הזהות
11	10125	123456789
27-28	22-26	11-19

שם התלמיד: ישראל ישראלי
כתובת התלמיד: החשמונאים 19 ת"א
מיקוד: 73332
טלפון: 03-5269710
שם המנחה: [illegible]
מרכז לימוד: ת"א 610
קבי לימוד: 01
נשלח ביום: 1.1.02

חלק ב - ימולא על-ידי המנחה
מלא נא את כל הפרטים (בעט כדורי). שמור את העותק האחרון בידך.
שלח את שאר העותקים בצירוף המטלה למרכז שירות לאוניברסיטה (מש"ל).

התקבל ביום ______ נשלח ביום ______ שם המנחה ______

חלק ג - ציונים
יש לרשום מספרים שלמים
סכום ציוני השאלות צריך להיות שווה ציון המטלה.

31

ציון שאלה 1	34
ציון שאלה 2	37
ציון שאלה 3	39
ציון שאלה 4	41
ציון שאלה 5	43
ציון שאלה 6	45
ציון שאלה 7	47
ציון שאלה 8	49
ציון שאלה 9	51
ציון שאלה 10	53
ציון שאלה 11	55
ציון שאלה 12	57
ציון שאלה 13	59
ציון שאלה 14	61
ציון שאלה 15	63
ציון שאלה 16	65
ציון שאלה 17	67
ציון שאלה 18	69
ציון שאלה 19	71
ציון שאלה 20	73
ציון שאלה 21	75
ציון שאלה 22	77
ציון שאלה 23	79
ציון שאלה 24	81
ציון שאלה 25	83

חלק ד - הערות המנחה לתלמיד (נא כתוב ברור)

מק"ט 9-830-1-9500 יוסף וולף ושות' בע"מ

דוגמה למילוי טופס מלווה לממ"ן

הערות חשובות לתשומת לבך!

- חל איסור מוחלט על הכנה משותפת של מטלות ו/או על העתקת מטלות.

- עליך להשאיר לעצמך העתק של המטלה. אין האוניברסיטה הפתוחה אחראית למטלה שתאבד בשל תקלות בדואר.

בבחינה שש שאלות.
עליכם לענות על **חמש** שאלות מתוכן.

יש לכתוב את הבחינה **בעט**.

ב ה צ ל ח ה !

שאלה 1 (20 נקודות: סעיף א' - 15 נק'; סעיף ב'- 5 נק')

עומק של צומת בעץ הוא אורך המסלול משורש העץ אל הצומת (כלומר, מספר הקשתות במסלול).

א. כתבו אלגוריתם רקורסיבי שמקבל עץ T (לאו דווקא בינרי) ומספר טבעי K, ומחזיר את מספר הצמתים בעץ שעומקם K.

ב. מהי סיבוכיות הזמן של האלגוריתם שכתבתם ? הסבירו את תשובתכם.

שאלה 2 (20 נקודות)

כתבו אלגוריתם יעיל, המקבל רשימת מספרים ומוצא את המספר שמופיע ברשימה הכי הרבה פעמים. נתחו את סיבוכיות הזמן של האלגוריתם והסבירו בקצרה מדוע הוא נכון.

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

נתון גרף בלתי מכוון $G = (V, E)$. לכל קשת e בגרף יש משקל חיובי.

יש למצוא מסלול שעלותו מינימלית, העובר בכל צומת בגרף פעם אחת וחוזר לנקודת המוצא.

פרופ' ידעני הציג בפני הסטודנטים שלו את הבעיה וביקש מהם להציע עבורה אלגוריתם.

אחד הסטודנטים הציע את האלגוריתם הבא:

(1) מיין את הקשתות של G בסדר עולה עפ"י המשקל שלהן;

(2) $E' \leftarrow \varnothing$

(3) כל עוד $|E'| < |V|$ בצע:

(3.1) סמן ב- e את הקשת הבאה ברשימת הקשתות הממוינת של G;

(3.2) בדוק אם מתקיימים התנאים הבאים:

1. בגרף $G' = (V, E' \cup \{e\})$ אין צומת שדרגתו גדולה מ- 2.

2. ב- G' אין מעגל, או שב- G' יש מעגל אך מתקיים $|E' \cup \{e\}| = |V|$.

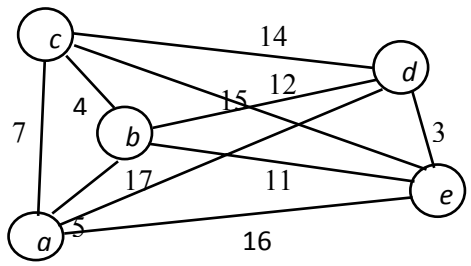
(3.3) אם **שני** התנאים מתקיימים, אז הוסף את e ל- E';

(4) החזר את E'.

א. פרופ' ידעני העיף מבט באלגוריתם, וקבע מייד שאין זה סביר שהוא מוצא את הפתרון האופטימלי לבעיה. איך הגיע הפרופסור למסקנתו ?

ב. הסבירו בקצרה את אופן פעולת האלגוריתם.

ג. הריצו את האלגוריתם על הגרף הבא ציירו את המסלול הסגור שהאלגוריתם מוצא:



מהי עלות המסלול ? האם זהו המסלול האופטימלי ? הוכיחו את תשובתכם.

שאלה 4 (20 נקודות)

נדון בגרסה הבאה של בעיית הריצוף:

הקלט לבעיה: קבוצה סופית T של סוגי מרצפות (שונים זה מזה)

השאלה: האם ניתן לרצף את המישור האינסופי בעזרת **מחצית** מסוגי המרצפות (לכל היותר) ?

הוכיחו שגם גרסה זו של בעיית הריצוף היא בלתי כריעה.

שאלה 5 (20 נקודות)

תארו אלגוריתם מקבילי, המקבל מספר טבעי n ומחשב את !n.

סיבוכיות הזמן וסיבוכיות המכפלה של האלגוריתם צריכים להיות קטנים ככל האפשר.

הסבירו את אופן פעולת האלגוריתם ונתחו את סיבוכיות הזמן וסיבוכיות המכפלה.

שאלה 6 (20 נקודות: 2 נק' לכל סעיף)

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

א. כל בעיה שיש לה מסמך אישור קצר עבור קלטי "כן" שייכת ל-NP.

ב. כל בעיה שאין לה מסמך אישור קצר עבור קלטי "כן" שייכת ל-co-NP.

ג. אם בעיה C היא NP-שלמה ויש רדוקציה פולינומיאלית מ-A ל-C, אז גם A היא NP-שלמה.

ד. אם בעיה C היא NP-שלמה ויש רדוקציה פולינומיאלית מ-A ל-C, אז A שייכת ל-NP.

ה. קיים אלגוריתם פולינומיאלי עבור הבעיה של מציאת מסלול קצר ביותר בין שני צמתים בגרף.

ו. אלגוריתם פולינומיאלי לפתרון בעיה כלשהי תמיד ירוץ מהר יותר מאלגוריתם אקספוננציאלי הפותר את הבעיה.

ז. אוטומט סופי דטרמיניסטי יכול לזהות מילים מהצורה 0^n1^n.

ח. אוטומט מחסנית דטרמיניסטי יכול לזהות מילים מהצורה 0^n1^n.

ט. אם מספר N הוא פריק, אז יש סיכוי גדול מ- $\frac{1}{2}$ שמספר אקראי בין 1 ל- $N-1$ יחלק את N.

י. קיים אלגוריתם פולינומיאלי לבעיית התאמת התבניות.

שאלה 1 (20 נקודות: סעיף א' - 15 נק'; סעיף ב' - 5 נק')

מכונת משקאות אוטומטית צריכה להחזיר עודף תוך שימוש במספר מינימלי של מטבעות.

א. כתבו אלגוריתם חמדני לבעיה זו, המשתמש במטבעות של 5 ₪ , 1 ₪ , 1/2 ₪ ו- 10 אגורות.

הקלט לבעיה הוא העודף שהמכונה צריכה להחזיר, והפלט הוא מספר המטבעות מכל סוג שיש להחזיר.

ב. תנו דוגמה לקבוצה של מטבעות ולקלט מתאים, שעבורם הפתרון שימצא האלגוריתם החמדני **לא** יהיה אופטימלי. (המטבעות שבקבוצה יכולים להיות כאלו שלא קיימים במציאות.)

שאלה 2 (20 נקודות: 10 נק' לכל סעיף)

א. כתבו אלגוריתם רקורסיבי, המקבל רשימה L בת N מספרים ומחשב את הממוצע ההנדסי של המספרים. תזכורת: הממוצע ההנדסי של המספרים $a_1, a_2,..., a_N$ הוא $\sqrt[N]{a_1 \cdot a_2 \cdot ... \cdot a_N}$.

ניתן להניח ש-N הוא חזקה שלמה של 2. מותר להשתמש בפעולות של כפל והוצאת שורש ריבועי.

ב. הוכיחו את נכונות האלגוריתם שכתבתם.

שאלה 3 (20 נקודות)

נדון בגרסה הבאה של בעיית הסוכן הנוסע:

הקלט לבעיה: רשימה של N ערים, המרחקים d_{ij} בין כל שתי ערים, עיר מוצא, עיר יעד ועלות K.

השאלה: האם קיים מסלול שמתחיל בעיר המוצא ומסתיים בעיר היעד, מבקר בכל הערים ועלותו הכוללת אינה עולה על K ?

תארו רדוקציה פולינומיאלית מגרסה זו של הבעיה לבעיית הסוכן הנוסע המקורית (כלומר, לגרסה שבה המסלול המבוקש הוא מעגלי).

רמז: הוסיפו לרשימת הערים עיר פיקטיבית.

שאלה 4 (20 נקודות)

נדון בגרסה הבאה לבעיית נחש הדומינו:

הקלט לבעיה: קבוצה סופית T של סוגי מרצפות, שתי נקודות (שונות זו מזו) V ו-W במחצית העליונה של המישור האינסופי ומספר טבעי N.

השאלה: האם ניתן להגיע מ-V ל-W באמצעות נחש דומינו המכיל **יותר** מ-N מרצפות?

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

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

כידוע, כדי שאדם יוכל להשתמש במערכת ההצפנה RSA, עליו לפרסם את המפתח הציבורי שלו (ה"מנעול"), או להפיץ אותו בין המשתמשים האחרים.

נניח שתהליך פרסום המפתחות הציבוריים מתנהל ללא פיקוח, וכל אדם יכול להודיע ברבים, שהמפתח הציבורי של אדם כלשהו x הוא $(Publ_x, Prod_x)$.

א. בועז הוא משתמש במערכת RSA. הסבירו כיצד בועז יכול ליצור חתימה מזויפת של איה.

ב. הראו כיצד בועז יוכל להשתמש בחתימה המזויפת כדי לשלוח הודעות בשם איה.

ג. הציעו דרך לפתור את הבעיה המתוארת בשאלה (כלומר, הציעו מנגנון לפיקוח על תהליך פרסום המפתחות).

שאלה 6 (20 נקודות: 2 נק' לכל סעיף)

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

א. אם לבעיית הכרעה אין מסמך אישור קצר כשהתשובה היא "כן", אז הבעיה אינה שייכת למחלקה NP.

ב. תהי A בעיה השייכת ל-NPC. אם יוכח ש- P≠NP, נוכל להסיק מכך שאין ל-A פתרון פולינומיאלי.

ג. ידוע שקיימת לפחות בעיה אחת ב-NP שאינה שייכת ל-P.

ד. ידוע ש- NP ≠ NPC.

ה. מחלקת הבעיות שניתנות לפתרון בזמן סביר אינה תלויה במודל החישובי שבו משתמשים.

ו. מחלקת הבעיות שניתנות לפתרון בזמן לינארי אינה תלויה במודל החישובי שבו משתמשים.

ז. לא קיימת רדוקציה מבעיית הטוטליות לבעיית העצירה.

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

ט. לכל אלגוריתם מקבילי ניתן לעשות סימולציה באמצעות אלגוריתם סדרתי.

י. קיים אלגוריתם מקבילי לפתרון בעיית המיון של N מספרים, שסיבוכיות המכפלה שלו היא $O(N)$.

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- $86 - (2 \cdot 1) = 84$

$8 - (2 \cdot 4) = 0$

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 <u>או</u>

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-W באמצעות 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. $NP \neq NPC \Rightarrow P \neq NP$

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.

סוף

שאלה 1 (20 נקודות: 10 נק׳ לכל סעיף)

נתון עץ כלשהו T (לאו דווקא בינרי). יש למצוא כיסוי ע״י צמתים של קשתות העץ שגודלו מינימלי. כלומר, יש למצוא תת קבוצה של הצמתים, כך שאם (a,b) היא קשת בעץ אז התת-קבוצה מכילה את a או את b (או את שניהם).

א. תארו אלגוריתם חמדני המוצא את הפתרון האופטימלי לבעיה.

ב. הסבירו מדוע האלגוריתם שתיארתם מוצא תמיד את הפתרון האופטימלי לבעיה.

הערה: אין צורך בהוכחה פורמלית.

שאלה 2 (20 נקודות: 10 נק׳ לכל סעיף)

בשנת 2002 התגלה אלגוריתם פולינומיאלי לבדיקת ראשוניות. אלגוריתם זה נקרא AKS על-פי ראשי התיבות של שלושת החוקרים שגילו אותו.

פרופ׳ כלומסקי התרגש מאד מגילוי האלגוריתם וטען שכעת אפשר לקבוע אחת ולתמיד אם השערת גולדבך נכונה. (עפ״י השערת גולדבך ניתן להציג כל מספר זוגי (גדול מ-2) כסכום של שני מספרים ראשוניים. למשל: $100 = 59 + 41$, $38 = 31 + 7$, $24 = 19 + 5$, $4 = 2 + 2$)

להלן האלגוריתם שהציע פרופסור כלומסקי לבדיקת השערת גולדבך:

(1) $flag \leftarrow True$, $N \leftarrow 4$

(2) $N \leftarrow N + 2$

(3) כל עוד $flag = True$ בצע:

(3.1) $i \leftarrow 3$

(3.2) כל עוד $i \leq N/2$ בצע:

(3.2.1) אם i ראשוני וגם $N - i$ ראשוני אז חזור לשורה (2);

(3.2.2) אחרת $i \leftarrow i + 2$

(3.3) $flag \leftarrow False$

(4) החזר את flag ועצור.

הערה: בדיקת הראשוניות בשורה (3.2.1) מתבצעת באמצעות אלגוריתם AKS.

א. האם פרופ׳ כלומסקי יצליח לדעתכם לקבוע אם השערת גולדבך נכונה?

ב. האם השערת גולדבך מהווה בעיה אלגוריתמית?

נמקו את תשובותיכם.

שאלה 3 (20 נקודות: 10 נק' לכל סעיף)

גרף **שלם** הוא גרף שבו יש קשת בין כל שני צמתים.

גרף **גלגל** הוא גרף שבו יש צומת מרכזי המחובר לכל שאר הצמתים, וכל הצמתים האלו מחוברים

ביניהם במעגל (כלומר, לכל צומת בגרף, פרט לצומת המרכזי, יש שלושה שכנים: הצומת המרכזי ושני שכניו במעגל). קבעו עבור כל אחד משני סוגי הגרפים שהוגדרו לעיל אם יש בגרף:

א. מסלול אוילריאני

ב. מסלול המילטוני

נמקו את קביעותיכם. (הערה: אם התשובה אינה חד-משמעית, הפרידו לכמה מקרים לפי הצורך.)

שאלה 4 (20 נקודות)

נדון בגרסה הבאה של בעיית העצירה:

הקלט לבעיה: תכנית Q וקלט y לתכנית.

השאלה: האם Q עוצרת על y לאחר **יותר** מ- 10,000 צעדים?

הוכיחו שגם גרסה זו של בעיית העצירה איננה כריעה.

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

נדון בבעיית החיפוש הבאה:

הקלט לבעיה הוא רשימת איברים באורך N. ייתכן שיש ברשימה כפילויות; כלומר, איבר כלשהו יכול להופיע ברשימה יותר מפעם אחת. בהינתן איבר x, יש לבדוק אם x נמצא ברשימה.

אם x נמצא ברשימה, יש להחזיר את האינדקס **הגבוה ביותר** של איבר ברשימה השווה ל-x.

אם x לא נמצא ברשימה, יש להחזיר "לא".

א. תארו אלגוריתם מקבילי, המשתמש ב- $\sqrt{N}$ מעבדים ופותר את הבעיה בזמן $O(\sqrt{N})$.

ב. תארו אלגוריתם מקבילי, המשתמש ב- $O(N)$ מעבדים ופותר את הבעיה בזמן $O(\log N)$.

ג. תארו אלגוריתם מקבילי, המשתמש ב- $N/\log N$ מעבדים ופותר את הבעיה בזמן $O(\log N)$.

שאלה 6 (20 נקודות: 2 נק' לכל סעיף)

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

א. ניתן למצוא עץ פורש מינימלי של גרף נתון G בזמן פולינומי.

ב. תהי A בעיה השייכת ל-NP. אם יוכח ש- $P \neq NP$, נוכל להסיק מכך שאין ל-A פתרון פולינומי.

ג. קיימת רדוקציה פולינומיאלית מכל בעיה ב-NP לכל בעיה אחרת ב-NP.

ד. קיימת רדוקציה פולינומיאלית בין כל שתי בעיות ב-NPC.

ה. כל הבעיות ב-NPC הן כריעות.

ו. ידוע שלכל הבעיות ב-NPC יש חסם תחתון אקספוננציאלי.

ז. אם בעיה A שייכת למחלקה P, אז גם הבעיה המשלימה ל-A שייכת ל-P.

ח. עפ"י התזה של צ'רץ' וטיורינג כל המודלים החישוביים שקולים זה לזה.

ט. תהי A בעיה השייכת ל-P. אם יוכח ש- $P \neq RP$, נוכל להסיק מכך ש- $A \notin RP$.

י. אם בעיה A שייכת ל-P, אז בהכרח קיים אלגוריתם לאס-וגאס הפותר את A.

סוף

שאלה 1 (20 נקודות)

נתון עץ בינארי בעל n צמתים. בכל צומת x בעץ קיימים השדות data, left ו-right.

משקל של מסלול בעץ הוא סכום הערכים הנמצאים בשדה data של הצמתים לאורך מסלול.

כתבו אלגוריתם לחישוב משקלו של המסלול הכבד ביותר בעץ מהשורש לעלה כלשהו.

שאלה 2 (20 נקודות: סעיף א' - 15 נק; סעיף ב' - 5 נק')

להלן נתון אלגוריתם המקבל מספר שלם אי-שלילי n ומחשב את ערכו של 2^n:

(1) $pw \leftarrow 1$;

(2) $c \leftarrow 0$;

(3) כל עוד $c < n$ בצע:

(3.1) $pw \leftarrow pw \times 2$;

(3.2) $c \leftarrow c + 1$;

(4) החזר את pw.

א. הוכיחו את נכונותו המלאה של האלגוריתם.

ב. מהו זמן הריצה של האלגוריתם ? האם זמן הריצה הוא פולינומיאלי בגודל הקלט ?

הערה: הניחו שפעולת הכפל בשורה (3.1) מתבצעת בזמן קבוע.

שאלה 3 (20 נקודות: סעיף א' - 5 נק; סעיף ב' - 15 נק')

נתבונן בשתי הגרסאות של בעיית הצביעה של גרף.

גרסת ההכרעה:

הקלט לבעיה: גרף לא מכוון $G = (V, E)$ ומספר חיובי שלם k

השאלה: האם ניתן לצבוע את הגרף ב-k צבעים לכל היותר ?

גרסת האופטימיזציה:

הקלט לבעיה: גרף לא מכוון $G = (V, E)$

השאלה: מהו מספר הצבעים המינימלי הדרוש לצביעת הגרף ?

א. הוכיחו שגרסת האופטימיזציה של הבעיה איננה קלה יותר מגרסת ההכרעה. כלומר, הראו שאם אפשר לפתור את גרסת האופטימיזציה בזמן פולינומיאלי, אז אפשר לפתור גם את גרסת ההכרעה בזמן פולינומיאלי.

ב. הוכיחו שגרסת ההכרעה של הבעיה איננה קלה יותר מגרסת האופטימיזציה. כלומר, הראו שאם אפשר לפתור את גרסת ההכרעה בזמן פולינומיאלי, אז אפשר לפתור גם את גרסת האופטימיזציה בזמן פולינומיאלי.

שאלה 4 (20 נקודות: 10 נק׳ לכל סעיף)

מכונת טיורינג **מוגבלת-סרט** היא מכונת טיורינג, שבה הראש הקורא-כותב אינו יכול לנוע מעבר לחלק של הסרט האינסופי המכיל את הקלט.

תהא M מכונת טיורינג מוגבלת-סרט בעלת Q מצבים וא״ב בגודל m.

נסמן ב-n את אורכה של מחרוזת הקלט ל-M.

א. **קונפיגורציה** של מכונת טיורינג היא אפיון מלא של מצב המכונה ברגע מסוים: המצב שבו המכונה נמצאת, מיקום הראש הקורא-כותב ותוכן הסרט.

הוכיחו שמספר הקונפיגורציות האפשריות של המכונה M הוא $Q \cdot n \cdot m^n$.

ב. נתבונן בבעיה הבאה:

הקלט לבעיה: מכונת טיורינג מוגבלת-סרט M ומילת קלט w

השאלה: האם M עוצרת על w ?

הוכיחו שהבעיה כריעה.

שאלה 5 (20 נקודות: 10 נק׳ לכל סעיף)

א. כתבו אלגוריתם מקבילי, הבודק בזמן **קבוע** אם מספר נתון N הוא ראשוני.

הניחו שפעולת חילוק בין שני מספרים מתבצעת בזמן קבוע.

בכמה מעבדים האלגוריתם משתמש ? האם זהו מספר סביר ?

ב. נניח כעת שאין בין המעבדים שיתוף בכתיבה; כלומר, לא קיים משתנה ששני מעבדים או יותר יכולים לשנות את ערכו.

בצעו את השינוי הנדרש באלגוריתם מסעיף א׳ וחשבו את זמן ריצתו של האלגוריתם.

האם זמן הריצה הוא פולינומיאלי בגודל הקלט ?

שאלה 6 (20 נקודות: 5 נק׳ לכל סעיף)

הוכיחו או הפריכו את הטענות הבאות:

א. ידוע שאם בעיה A שייכת ל-NP אך איננה NP-שלמה, אז A שייכת ל-P.

ב. אם בעיה A שייכת ל-P, אז גם הבעיה המשלימה ל-A שייכת ל-P.

ג. אם קיימת רדוקציה פולינומיאלית מכל בעיה ב-NP לבעיה נתונה A, אז A שייכת ל-NP.

ד. נסמן ב-RE את מחלקת הבעיות שיש להן אישורי ״כן״.

אם בעיה A שייכת ל- co-RE ∩ RE, אז A כריעה.

סוף

שאלה 1 (20 נקודות: סעיף א' - 5 נק'; סעיף ב' - 10 נק'; סעיף ג' - 5 נק'; סעיף ד' - בונוס)

גרף $G = (V, E)$ נקרא **דו-צדדי** אם ניתן לחלק את צמתיו לשתי קבוצות זרות V_1 ו- V_2, כך שכל קשת בגרף מחברת בין צומת ב-V_1 לצומת ב-V_2.

נתון גרף דו-צדדי G בעל n צמתים. ברצוננו לצבוע את צומתי הגרף בצביעה חוקית; כלומר, כל שני צמתים שיש ביניהם קשת צריכים להיות צבועים בצבעים שונים.

א. כמה צבעים דרושים לצביעת הגרף G ? הוכיחו את תשובתכם.

ב. נניח כעת שלכל צבע יש עלות. הצבעים ממוספרים ("צבע מספר 1", "צבע מספר 2" וכו')

וצביעת צומת בצבע מספר i עולה i יחידות. ברצוננו לצבוע את הגרף G, כך שעלות הצביעה

הכוללת תהיה מינימלית. החלוקה של צומתי הגרף G לשתי קבוצות זרות היא נתונה.

תארו אלגוריתם חמדני, הצובע את G בעלות של $3n/2$ לכל היותר.

באיזה מקרה עלות הצביעה תהיה בדיוק $3n/2$?

ג. הסבירו מדוע יחס הקירוב שמשיג האלגוריתם שתיארתם הוא 3/2.

ד. תנו דוגמה לגרף דו-צדדי, שעבורו האלגוריתם שתיארתם לא ימצא את הפתרון האופטימלי.

שאלה 2 (20 נקודות: 10 נק' לכל סעיף)

א. כתבו אלגוריתם **יעיל**, המקבל מספר שלם וחיובי x ובודק אם x הוא תוצאה של הפעלת פונקציית העצרת על איזשהו מספר. כלומר, השאלה היא אם קיים מספר k כך ש- $x = k!$.

הסבירו בקצרה את אופן הפעולה של האלגוריתם.

ב. הוכיחו את נכונותו המלאה של האלגוריתם שכתבתם.

שאלה 3 (20 נקודות)

נניח שנתונה שגרת "קופסה שחורה", הפותרת את גרסת הכן/לא של בעיית הסוכן הנוסע. כלומר, בהינתן גרף עם משקלות G ומספר K, השגרה קובעת אם קיים ב-G מעגל המילטוני שעלותו אינה עולה על K. הראו כיצד אפשר להשתמש בשגרה כדי למצוא ביעילות את משקלו של המסלול האופטימלי עבור הסוכן הנוסע. הניחו שהמשקלות על הקשתות והמספר K הם שלמים וחיוביים.

שאלה 4 (20 נקודות: 10 נק' לכל סעיף)

להלן נתונות שתי גרסאות של בעיית נחש הדומינו במחצית העליונה של המישור האינסופי.

עבור כל אחת מהגרסאות – קבעו אם הבעיה כריעה או לא. אם הבעיה כריעה, קבעו לאיזו מחלקת סיבוכיות היא שייכת. הוכיחו את תשובותיכם.

א. הקלט לבעיה: קבוצת מרצפות T, שתי נקודות V ו-W במחצית העליונה של המישור האינסופי ומספר טבעי N.

השאלה: האם קיים נחש דומינו של מרצפות מ-T המחבר בין V ל-W ואורכו לכל היותר N ?

ב. הקלט לבעיה: קבוצת מרצפות T, שתי נקודות V ו-W במחצית העליונה של המישור האינסופי ומרצפת ספציפית $t \in T$.

השאלה: האם קיים נחש דומינו של מרצפות מ-T המחבר בין V ל-W והמתחיל במרצפת t ?

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

נתון גרף לא מכוון $G = (V, E)$ ושני צמתים s ו-t ב-G.

ברצוננו לדעת, אם קיים בגרף G מסלול מ-s ל-t.

להלן נתון אלגוריתם אקראי לפתרון הבעיה:

(1) $v \leftarrow s$;

(2) כל עוד $v \neq t$ בצע:

(2.1) בחר באופן אקראי את אחד השכנים של v והצב אותו ב-v;

(3) הדפס "כן" ועצור.

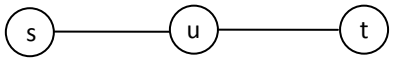
א. האם האלגוריתם נכון ? האם האלגוריתם נכון חלקית ? נמקו את תשובותיכם.

ב. נסמן ב-n את מספר הצמתים בגרף G. אפשר להוכיח שאם קיים ב-G מסלול מ-s ל-t,

אז בהסתברות שגדולה מ- ½ האלגוריתם ימצא אותו בפחות מ- $2n^3$ צעדים.

הציעו דרך להפוך את האלגוריתם הנתון לאלגוריתם מונטה-קרלו.

ג. נתבונן בגרף הבא:



מהי ההסתברות שהאלגוריתם יגיע לצומת t לאחר שני צעדים ?

מהי ההסתברות שהאלגוריתם יגיע לצומת t לאחר ארבעה צעדים לכל היותר ?

הוכיחו את תשובותיכם.

(בונוס: מהי ההסתברות שהאלגוריתם יגיע לצומת t לאחר 2k צעדים לכל היותר ?)

שאלה 6 (20 נקודות: 5 נק' לכל סעיף)

הוכיחו או הפריכו את הטענות הבאות:

א. ידוע שאם בעיה A שייכת גם ל-NP וגם ל-co-NP, אז A שייכת ל-P.

ב. אם בעיה A היא כריעה, אז גם הבעיה המשלימה ל-A היא כריעה.

ג. אם $P \neq NP$, אז לכל הבעיות ב-NP יש חסם תחתון אקספוננציאלי.

ד. אפשר לבצע סימולציה של כל אלגוריתם מקבילי באמצעות אלגוריתם סדרתי.

סוף

שאלה 1 (20 נקודות: סעיף א' - 5 נק'; סעיף ב' - 15 נק')

א. נדון בגרסה של בעיית תרמיל הגב בשלמים שבה כל הפריטים הם בעלי אותו משקל.

כתבו אלגוריתם יעיל הפותר את הגרסה הזו של הבעיה ונתחו את זמן ריצתו.

ב. נדון כעת בגרסה של הבעיה שבה לכל פריט יכול להיות אחד משני משקלים אפשריים – a או b.

כתבו אלגוריתם יעיל הפותר את הגרסה הזו של הבעיה ונתחו את זמן ריצתו.

(רמז: מה יהיה הרכב הפריטים אם התרמיל חייב להכיל בדיוק k פריטים במשקל a?)

שאלה 2 (20 נקודות: סעיף א' - 15 נק'; סעיף ב' - 5 נק')

א. כתבו אלגוריתם, המקבל מספר טבעי x ומחשב את סכום כל הגורמים **הראשוניים** של x.
למשל, $48 = 2^4 \cdot 3$ ולכן סכום כל הגורמים הראשוניים של 48 הוא $2 + 3 = 5$.
מותר להשתמש באלגוריתם AKS לבדיקת ראשוניות (האלגוריתם הפולינומיאלי לבעיה שהתגלה בשנת 2002).
תארו בקצרה את דרך פעולתו של האלגוריתם שכתבתם והסבירו מדוע הוא נכון.

ב. נתחו את זמן הריצה של האלגוריתם.
האם זמן הריצה הוא פולינומיאלי בגודל הקלט? הסבירו את תשובתכם.

שאלה 3 (20 נקודות)

נניח שקיים אורקל הפותר בזמן פולינומיאלי את בעיית העצירה.

הראו כיצד אפשר להשתמש באורקל כדי לפתור בזמן פולינומיאלי את בעיית שיבוץ הקופים.

שאלה 4 (20 נקודות)

נדון בגרסה הבאה של בעיית נחש הדומינו במחצית המישור האינסופי:

הקלט לבעיה: קבוצה סופית T של סוגי מרצפות (שונים זה מזה), שתי נקודות V ו-W במחצית העליונה של המישור האינסופי ומספר טבעי k ($k \leq |T|$).

השאלה: האם ניתן להגיע מ-V ל-W באמצעות "נחש דומינו" המשתמש לכל היותר ב-k סוגי מרצפות מתוך סוגי המרצפות שב-T?

הוכיחו שגרסה זו של הבעיה היא גם-כן בלתי כריעה.

שאלה 5 (20 נקודות: סעיף א' - 15 נק'; סעיף ב' - 5 נק')

נתונה רשת של N מחשבים. כל אחד מהמחשבים יכול לשדר ולקלוט הודעות. בכל מחזור זמן,

כל אחד מהמחשבים יכול לשדר הודעה רק לאחד משכניו. לעיתים יש צורך להעביר הודעה מאחד המחשבים לכל שאר המחשבים ברשת והמטרה היא לעשות זאת במספר מינימלי של מחזורים.

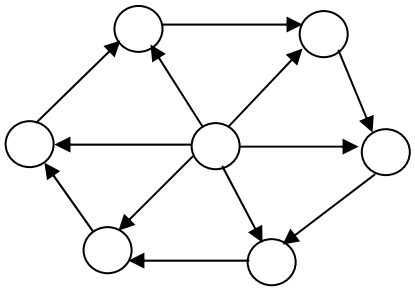
ניתן לתאר את רשת המחשבים באמצעות גרף מכוון, כך שכל מחשב מיוצג ע"י צומת בגרף; קיימת

קשת בגרף מצומת x לצומת y אם ורק אם אפשר לשדר הודעה מהמחשב המיוצג על-ידי x למחשב המיוצג על-ידי y.

גרף גלגל הוא גרף שבו יש צומת מרכזי אחד המחובר לכל שאר הצמתים ושאר הצמתים מסודרים במעגל (כלומר, לכל אחד משאר הצמתים יש עוד שני שכנים בנוסף לצומת המרכזי).

נניח שהקשתות מכוונות מהצומת המרכזי לשאר הצמתים וקשתות המעגל הן בכיוון השעון.

דוגמה לגרף גלגל:



א. הראו שאם הגרף המתאר את רשת המחשבים הוא גרף גלגל, אז אפשר להעביר הודעה

מהמחשב המרכזי לכל שאר המחשבים ברשת תוך $2\sqrt{N}-1$ מחזורים.

ב. הסבירו באופן כללי כיצד אפשר לשפר את הפתרון של סעיף א', כך שמספר המחזורים הכולל

יהיה קטן יותר מ- $2\sqrt{N}-1$.

שאלה 6 (20 נקודות: 5 נק' לכל סעיף)

עבור כל אחת מהטענות הבאות – כתבו מהו הסטטוס הנוכחי של הטענה

(נכונה / לא נכונה / לא ידוע עדיין אם היא נכונה). נמקו בקצרה את תשובותיכם:

א. אם קיימת בעיה ב-NP שאיננה פתירה בזמן פולינומיאלי, אז כל הבעיות השלמות ב-NP אינן פתירות בזמן פולינומיאלי.

ב. אם לבעיה A קיים מסמך אישור קצר, אז גם לבעיה המשלימה של A קיים מסמך אישור קצר.

ג. אם בעיה A ניתנת לפתרון בזמן פולינומיאלי באמצעות מכונת טיורינג אי-דטרמיניסטית,

אז קיימת מכונת טיורינג דטרמיניסטית שפותרת את A בזמן אקספוננציאלי.

ד. לא קיים אוטומט סופי דטרמיניסטי, המסוגל להחליט אם מילת קלט נתונה מעל האי"ב {a, b}

מכילה בדיוק 100 פעמים את התו a ו-100 פעמים את התו b.

סוף

שאלה 1 (20 נקודות: 5 נק' לכל סעיף)

נתון הקלט הבא לבעיית תרמיל הגב בשלמים (משקלו של הפריט ה-i הוא w_i וערכו v_i):

i	w_i	v_i
1	5 ק"ג	50 ₪
2	10 ק"ג	90 ₪
3	15 ק"ג	120 ₪

המשקל המקסימלי שאפשר להכניס לתרמיל: 25 ק"ג

א. מהו הפתרון האופטימלי לבעיה? נמקו את תשובתכם בקצרה.

ב. מה יהיה הפתרון שימצא האלגוריתם החמדני (אלגוריתם הבוחר את הפריטים על-פי הערך ליחידת משקל)?

ג. האם יש הבדל בין הפתרון האופטימלי לפתרון שמוצא האלגוריתם החמדני?
אם כן, הסבירו מדוע האלגוריתם החמדני לא הצליח למצוא את הפתרון האופטימלי.

ד. נניח כעת שהקלט לעיל הוא קלט לגרסת **השברים** של הבעיה.
מהו הפתרון האופטימלי לבעיה במקרה זה?

שאלה 2 (20 נקודות: 10 נק' לכל סעיף)

נתון וקטור A באורך n המכיל את המשכורות של עובדי מחלקת המים בעיריית ת"א.

א. כתבו אלגוריתם יעיל ככל האפשר המוצא את ההפרש המקסימלי בין שתי משכורות ברשימה.

ב. כתבו אלגוריתם יעיל המוצא את ההפרש המינימלי בין שתי משכורות ברשימה.

בכל אחד מהסעיפים – נתחו את זמן הריצה של האלגוריתם והסבירו בקצרה מדוע הוא נכון.

בסעיף א' יש להתייחס למספר ההשוואות המדויק שמבצע האלגוריתם.

שאלה 3 (20 נקודות: סעיף א' - 5 נק'; סעיף ב' - 15 נק')

נתבונן בבעיה הבאה:

הקלט לבעיה: גרף לא מכוון G ומספר שלם k.

השאלה: האם קיים ב-G מסלול פשוט שאורכו גדול מ-k ?

(מסלול פשוט הוא מסלול שאינו מכיל מעגלים. אורך המסלול הוא מספר הקשתות במסלול.)

א. הוכיחו שאם P = NP אז קיים אלגוריתם פולינומיאלי עבור הבעיה.

ב. הוכיחו שאם P ≠ NP אז לא קיים אלגוריתם פולינומיאלי עבור הבעיה.

שאלה 4 (20 נקודות: 10 נק' לכל סעיף)

א. נתונה גרסה של מכונת טיורינג שבה הראש הקורא-כותב יכול גם להישאר במקום.

כלומר, מעבר של המכונה נראה כך: $(q,\sigma) \to (q', \sigma', \text{L/R/S})$.

הוכיחו שגרסה זו של המכונה שקולה למכונת טיורינג רגילה.

ב. בנו אוטומט סופי דטרמיניסטי שמקבל את כל המלים מעל $\sum = \{0,1\}$, שהן ייצוג בינרי של מספרים המתחלקים ב-4 אך לא מתחלקים ב-8.

הערה: במספרים יכולים להיות אפסים מובילים.

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

ידוע שבתחום $1..N$ קיימים בערך $N / \log N$ מספרים ראשוניים.

להלן נתון אלגוריתם אקראי לבחירת מספר ראשוני בתחום $1..N$. האלגוריתם משתמש באלגוריתם AKS – האלגוריתם הדטרמיניסטי לבדיקת ראשוניות שהתגלה בשנת 2002.

(1) הגרל מספר אקראי x בתחום 2..N;

(2) אם AKS(x) = true, אז החזר את x ועצור.

(3) אחרת, חזור לשורה (1);

א. מה הסיכוי שהאלגוריתם יצליח למצוא מספר ראשוני כבר בניסיון הראשון ?

ב. מה הסיכוי שגם לאחר עשרה ניסיונות האלגוריתם לא ימצא מספר ראשוני ?

ג. הוכיחו שהסיכוי שהאלגוריתם לא יצליח למצוא מספר ראשוני ב- $\log N$ הניסיונות הראשונים קטן מ- 2/5 (עבור N מספיק גדול).

ד. איה מעוניינת להתחיל להשתמש במערכת RSA. לשם כך היא צריכה ליצור מפתח פרטי וציבורי. היא הפעילה את האלגוריתם המתואר לעיל כדי לבחור שני מספרים ראשוניים. המספרים שהתקבלו הם 11 ו- 29. המספר Priv שאיה בחרה הוא 187. מה יהיה המפתח הציבורי של איה ?

שאלה 6 (20 נקודות: 5 נק' לכל סעיף)

עבור כל אחת מהטענות הבאות – כתבו מהו הסטטוס הנוכחי של הטענה

(נכונה / לא נכונה / לא ידוע עדיין אם היא נכונה). נמקו בקצרה את תשובותיכם:

א. אם קיימת בעיה ב-NP שאיננה פתירה בזמן פולינומיאלי, אז כל הבעיות השלמות ב-NP אינן פתירות בזמן פולינומיאלי.

ב. אם לבעיה A קיים מסמך אישור קצר, אז גם לבעיה המשלימה של A קיים מסמך אישור קצר.

ג. באמצעות אורקל לבעיית העצירה אפשר לפתור את בעיית האימות.

ד. אפשר לפתור את בעיית הקליקה בזמן פולינומיאלי באמצעות מספר פולינומיאלי של מעבדים.

סוף

שאלה 1 (20 נקודות)

כתבו אלגוריתם, הקורא מהקלט מחרוזת תווים ובודק אם היא פלינדרום.

מותר לאלגוריתם להשתמש בשתי מחסניות. אורכה של מחרוזת הקלט אינו ידוע מראש.

שאלה 2 (20 נקודות: 10 נק' לכל סעיף)

נתון מערך A באורך n. ברצוננו למצוא את האיבר המינימלי ואת האיבר המקסימלי במערך.

א. להלן אלגוריתם לפתרון הבעיה:

(1) min ← A[1];

(2) max ← A[1];

(3) עבור i המקבל את הערכים 2 עד n, בצע:

(3.1) אם A[i] < min, אז min ← A[i];

(3.2) אחרת, אם A[i] > max, אז max ← A[i];

(4) החזר את min ו- max.

אפיינו את המקרה הטוב והמקרה הגרוע, וחשבו את מספר ההשוואות המדויק שהאלגוריתם מבצע בכל אחד מהמקרים.

ב. להלן אלגוריתם נוסף לפתרון הבעיה:

(1) אם A[1] > A[2] אז החלף ביניהם;

(2) min ← A[1];

(3) max ← A[2];

(4) עבור i המקבל את הערכים 2 עד n/2, בצע:

(4.1) אם A[2i] < A[2i–1] אז החלף ביניהם;

(4.2) אם A[2i–1] < min, אז min ← A[2i–1];

(4.3) אם A[2i] > max, אז max ← A[2i];

(5) החזר את min ו- max.

חשבו את מספר ההשוואות המדויק שהאלגוריתם מבצע.

הערה: הניחו ש-n זוגי.

איזה משני האלגוריתמים טוב יותר ?

שאלה 3 (20 נקודות: סעיף א' - 5 נק'; סעיף ב' - 15 נק')

גרף מישורי הוא גרף שניתן לצייר אותו על דף נייר מבלי שיהיו קשתות שיחתכו זו את זו.

ידוע שמספר הקשתות בגרף מישורי בעל n צמתים הוא לכל היותר $3n-6$.

א. מהו הגודל המקסימלי האפשרי של קליקה בגרף מישורי ? הוכיחו את תשובתכם.

ב. ידוע שהבעיה של מציאת הקליקה המקסימלית בגרף כלשהו היא NP-שלמה.

האם הדבר נכון גם כשמדובר בגרף מישורי ? אם כן – הוכיחו זאת; אחרת – תארו אלגוריתם פולינומיאלי המוצא את הקליקה המקסימלית בגרף מישורי.

שאלה 4 (20 נקודות)

נתבונן בגרסה הבאה של בעיית התאמת המילים:

הקלט לבעיה: שתי סדרות מילים X ו-Y.

השאלה: האם קיימת סדרת אינדקסים באורך זוגי, כך שאם נשרשר את המילים המתאימות מ-X ומ-Y תתקבל אותה מילה ?

הוכיחו שגרסה זו של הבעיה היא גם כן בלתי כריעה.

שאלה 5 (20 נקודות)

איה הגישה מועמדות לתפקיד נהגת קטר ברכבת ישראל והוזמנה לראיון אצל בועז.

כדי להתקבל לתפקיד, עליה לשכנע את בועז שהיא איננה עיוורת צבעים (כלומר, שהיא מבחינה בין הצבעים אדום וירוק).

תכננו פרוטוקול הוכחה פשוט, שיאפשר לבועז להשתכנע בהסתברות גדולה מ- 0.99 שאיה איננה עיוורת צבעים.

שאלה 6 (20 נקודות: סעיף א' - 5 נק'; סעיף ב' - 15 נק')

א. נתונה הבעיה הבאה:

הקלט לבעיה: מספר שלם n ושני מספרים a, b (a < b).

השאלה: האם יש גורם של n הנמצא בין a ו-b?

(כלומר, האם קיים m, כך ש- $a \leq m \leq b$ ו- $n \bmod m = 0$?)

הוכיחו שהבעיה שייכת ל-NP.

ב. הוכיחו שאם P = NP, אז מערכת ההצפנה RSA ניתנת לפיצוח.

רמז: היעזרו בסעיף א'.

סוף

שאלה 1 (20 נקודות: 10 נק׳ לכל סעיף)

א. נתונה קבוצה S של קורסים. לכל קורס יש שני מאפיינים: שעת ההתחלה שלו ושעת הסיום.

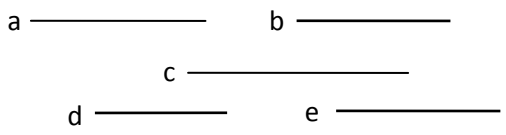
ברצוננו לשבץ את כל הקורסים שב-S למספר מינימלי של אולמות. (שני קורסים המתקיימים באותן שעות, או ששעותיהם חופפות חלקית לא יכולים להתקיים באותו אולם.)

הסבירו כיצד אפשר לייצג את הבעיה באמצעות גרף, כך שמספר האולמות המינימלי יהיה שווה למספר הצבעים הדרוש לצביעת הגרף.

ב. להלן נתונה קבוצה S של חמישה קורסים, a, b, c, d, e.

ציירו את הגרף המתאים לאוסף הקורסים וצבעו אותו במספר מינימלי של צבעים.

חלקו את חמשת הקורסים לאולמות, בהתאם לצביעה של הגרף.



שאלה 2 (20 נקודות)

מספר יפה הוא מספר טבעי, המורכב מרצף של אחדים ואחריו רצף של אפסים.

נתונה מחרוזת המייצגת מספר יפה. המחרוזת מאוחסנת במערך A באורך n.

כתבו אלגוריתם המוצא **בצורה יעילה** את מספר האחדים במספר.

הסבירו מדוע האלגוריתם נכון ונתחו את סיבוכיות זמן הריצה שלו.

שאלה 3 (20 נקודות: סעיף א׳ - 5 נק׳; סעיף ב׳ - 15 נק׳)

א. הוכיחו שהפסוק $(A\wedge B)\rightarrow(A\vee B)$ הוא טאוטולוגיה.

ב. נתבונן בבעיה הבאה:

הקלט לבעיה: פסוק ϕ בתחשיב הפסוקים.

השאלה: האם ϕ הוא טאוטולוגיה?

הוכיחו שהבעיה שייכת ל-co-NP.

האם לדעתכם הבעיה שייכת גם ל-NP? נמקו את תשובתכם.

שאלה 4 (20 נקודות)

נתונה גרסה של מכונת טיורינג, שבה אפשר לקרוא את התו שעל גבי הסרט ולנוע ימינה / שמאלה **או** לכתוב תו חדש על גבי הסרט (אך אי אפשר לבצע את שתי הפעולות באותו צעד).

כלומר, מעבר של המכונה יכול להיות משני סוגים:

- פעולת קריאה: $(q,\sigma) \to (q_1, L/R)$
- פעולת כתיבה: $(q,\sigma) \to (q_1, \sigma_1)$

הוכיחו שגרסה זו של המכונה שקולה למכונת טיורינג רגילה.

שימו לב שצריך להוכיח את שני הכיוונים של השקילות.

שאלה 5 (20 נקודות: סעיף א' - 15 נק'; סעיף ב' - 5 נק')

להלן נתון אלגוריתם מקבילי, המקבל כקלט שני מספרים טבעיים m ו- n ומשתמש ב- mמעבדים:

(1) לכל $1 \le i \le m$ בצע **במקביל** $y_i \leftarrow 0$;

(2) $y_0 \leftarrow 1$;

(3) בצע את הפעולות הבאות n פעמים:

(3.1) לכל $1 \le i \le m$ בצע **במקביל** $y_i \leftarrow y_i + y_{i-1}$;

(4) החזר את y_m.

א. הדגימו את פעולת האלגוריתם עבור m = 4 ו- n = 6. מה מבצע האלגוריתם?

ב. נתחו את סיבוכיות הזמן המקבילית של האלגוריתם ואת סיבוכיות המכפלה שלו.

שאלה 6 (20 נקודות: סעיפים א', ב' - 10 נק' לכל אחד; סעיף ג' - בונוס)

בתשובה לשאלה 2 בפרק 11 במדריך הלמידה מופיע אלגוריתם נאיבי לבדיקת ראשוניות, המנסה למצוא מחלק של מספר נתון N על-ידי בדיקה שיטתית של המספרים שבין 2 ל- $\sqrt{N}$.

פרופ' כלומסקי טוען שאלגוריתם זה מבצע הרבה בדיקות מיותרות. הוא מציע את השיפור הבא: נשתמש במערך בוליאני בגודל $\sqrt{N}$ ונאתחל את איבריו ל-true. ננסה תחילה לחלק את N ב-2. אם N מתחלק ב-2 אז סיימנו; אחרת, נעבור על איברי המערך ונשנה ל-false את הערכים בכל התאים הזוגיים. לאחר מכן ננסה לחלק את N ב-3. אם N מתחלק ב-3 אז סיימנו; אחרת, נשנה

ל-false את הערכים בכל התאים שהם כפולה של 3. נמשיך באותו אופן עד שנגיע ל- $\sqrt{N}$. בכל שלב ננסה לחלק את N באינדקס של התא הבא במערך שערכו true.

א. הסבירו מדוע האלגוריתם של פרופ' כלומסקי הוא נכון.

ב. נתחו את סיבוכיות זמן הריצה של האלגוריתם. הניחו שפעולת חילוק מתבצעת בזמן קבוע.

האם הושג שיפור לעומת האלגוריתם הנאיבי ?

ג. האם תשובתכם תשתנה אם נניח שפעולת חילוק מתבצעת בזמן $O(\log N)$?

סוף