# שאלה 1

## סעיף א

אלגוריתם מעל מקדמים של פולינום ו- מתאים (בהתאם למספר המקדמים) מחזיר עבורנו בסיבוכיות את הצבת הפולינום עבור כל שורשי היחידה.

ומכאן שאנחנו עובדים מעל . נחשב את

בתור הסבר, אם נפרק את לשני חלקים בצורה: וגם כאשר מתקיים .

מעקב זימון:

* 1. even 🡨 call :
     1. even 🡨 call :
        1. return
     2. odd 🡨 call :
        1. return
     3. return
  2. odd 🡨 call :
     1. even 🡨 call :
        1. return
     2. odd 🡨 call :
        1. return
     3. return
  3. return

לסיכום קיבלנו:

## סעיף ב

אלגוריתם מעל הצבות של פולינום מעל שורשי היחידה ו- מתאים מחזיר לנו את מקדמי הפולינום.

ולכן לפי השאלה אנחנו עובדים מעל ונחשב .

מעקב זימון:

:

1. call :
   1. even 🡨 call :
      1. even 🡨 call :
         1. return
      2. odd 🡨 call :
         1. return
      3. return
   2. odd 🡨 call :
      1. even 🡨 call :
         1. return
      2. odd 🡨 call :
         1. return
      3. return
   3. return
2. return

סה"כ קיבלנו בחזרה את המקדמים המקוריים של , כלומר הריצה אמורה להיות נכונה.

# שאלה 2

נתונים שני מספרים ו- ואנחנו רוצים לחשב ביעילות. **בשאלה** נתנו מספר הנחות המקלות על האלגוריתם:

* שני המספרים בייצוג בינארי שווי גודל עם סיביות
* שני המספרים חיוביים
* ההכפלות שמתבצעות במהלך הקריאות הרקורסיביות אינן מגדילות את אורכם של המספרים

## הקדמת רעיון מתמטי:

נפרק כל מספר ל- בלוקים כאשר בכל בלוק יש סיביות. אם לא מתחלק ב- אז נוסיף סיביות של אפס משמאל כדי להרחיב למספר שמתחלק ב-. אני אמשיך את ההנחה כאילו כבר מתחלק ב-.

נסמן את המספר המיוצג על ידי סיביות כל בלוק בתור ו- , כלומר נקבל:

לפי הנחה 3 אנחנו מניחים שכל הכפלה של שני בלוקים לא מגדילה את הגודל, ולכן אנחנו מקבלים שכל בלוק (שנסמן ב-) במספר המכפלה הוא קונבולוציה של ושל (בעיקרון דומה לכפל במאונך):

*כלומר אם ניצור פולינום שמקדמיו מתאימים למספר המיוצג על ידי הבלוק נקבל שמקדמי פולינום המכפלה מתאימים למספר הבלוקים ב-.*

*נשים לב שבשאלה אנחנו לא יכולים לבצע המרה מייצוג בסיביות לייצוג מספרי.*

## האלגוריתם:

האלגוריתם מקבל את

1. המר לצורה בינארית את בעלת סיביות ונגדיר
2. נרחיב במידת הצורך עם אפסים משמאל כדי ש- יתחלק ב-
3. נחלק את הקלט בגודל סיביות ל- בלוקים בגודל סיביות ונסמן את הסיביות המתאימות לכל בלוק בשני הווקטורים בהתאמה שהם בגודל .
4. נריץ אלגורית על עם מקדמים. נקבל צורת שנסמן בווקטור .
5. ניצור וקטור מכפלה חדש כך שעבור כל מתקיים
6. נריץ על וקטור ונקבל ווקטור מקדמים שנסמן ב-
7. נסמן את הפעולה בתור פעולת הזזת ב- סיביות שמאלה. נגיע למספר
8. המר את לצורת מספר שלם והחזר

## ניתוח זמן ריצה:

שלב הרחבת גודל המספרים הוא לכל היותר הוספת של סיביות, ולכן הסיבוכיות המרבית היא .

שלב חלוקה שני המספרים ל- מתבצע תוך מעבר לינארי על כל הסיביות והגדרת כל הבלוק ולכן . כך גם הרחבת ווקטור המספרים ל- מקדמים.

הרצת על ווקטור בגודל כאשר בכל קריאה רקורסיבית יש מחיר של עבור הכפלת הסיביות ולכן אי אפשר בצורה ישירה להסתמך על הסיבוכיות הידועה של , יש צורך בחישוב מחדש: עבור קלט נוכחי לזימון של מחלקים ל-2 חלקים בגודל , ומבצעים לכל בלוק בגודל הכפלה שנתון שהיא בסיבוכיות ומספר קבוע של חיבורים וחיסורים במחיר כאשר יש בלוקים ולכן נקבל:

כאשר לפי שיטת האב – מקרה 2 מורחב נקבל

הרצת היא למעשה זימון עם ערכים אחרים ל- (מבחינת סיבוכיות כמובן) ולכן גם כאן המחיר הוא .

בין הרצת להרצת אנחנו מבצעים כפל בין בלוקים כאשר כל בלוק בגודל סיביות ולכן נקבל שהזמן הוא

בזכות שיטת הזזת הסיביות שמאלה, אנחנו מקבלים שהחישוב עבור הוא פשוט הזזה וחיבור, כאשר בזכות הנחה 3 שכל בלוק של הוא גם בגודל נקבל שאין "חיתוך" במקומות של הסיביות בתוצאה ולכן אין גלישת שארית ולכן כל החישוב הוא פשוט מיקום של כל ה- סיביות במספר, כלומר .

המרת מספר לבינארי ומבינארי בחזרה הם בסיבוכיות

סה"כ קיבלנו שסיבוכיות כל האלגוריתם היא:

## הוכחת נכונות:

בהקדמה המתמטית הוכחנו שהערך של כל בלוק בתוצאת המכפלה עבור מתאים לקונבולוציה בין הבלוקים המתאימים במספרים – אבל רק בצורה של מספר רגיל.

בזכות העובדה שלכל מספר רגיל יש ייצוג בודד בינארי (בזכות ההנחה שאין מספרים שליליים אין צורך להיכנס למשלימים וכדומה), אם נגדיר נכון את החישוב של חיבור, חיסור וכפל בין סיביות הבלוק (כדי ש- יוכל לעבוד).

נייצג את הפולינומים שהמקדמים שלהם הם הבלוקים המתאימים של והרחבה ל- מקדמים. לפי הנכונות של אלגוריתם , אנחנו מקבלים בהצלחה את צורת ה- ולפי הצורה שבה הגדרנו נקבל את הצורה מעל נקודות.

שני הפולינומים הם מסדר , ולכן פולינום המכפלה הוא לכל היותר מסדר . כל פולינום מסדר ניתן לייצוג על ידי נקודות שונות בצורה יחידה. לפי הגדרת צורת אנחנו מקבלים לכל  
 מתקיים וגם .  
ולכן עבור פולינום המכפלה מתקיים , ובפרט עבור , ולכן על ידי הכפלה של ערך משני הווקטורים לתוך וקטור חדש נקבל קודקודים של פולינום המכפלה, ו- נקודות אלו מייצגים פולינום בודד שהוא בדיוק פולינום המכפלה. ובזכות נכונות של אנחנו מקבלים את המקדמים של פולינום המכפלה .

# שאלה 3

מסמן את מספר המקדמים בפולינום שנקבל , כאשר המקדמים הם .

## הקדמת רעיון מתמטי

יהי קבוצת מקדמים המוגדרת:

יהי קבוצת מקדמים נוספת המוגדרת:

יהי שני פולינומים שהמקדמים שלהם מתאימים לשתי הסדרות הללו ונסמן אותם ו-. אם נחשב את מקדמי פולינום מכפלת שני הפולינומים, בעזרת קונבולוציה על כל מקדם בטווח נקבל:

כלומר קיבלנו שבפולינום המכפלה כל מקדם בפולינום הוא תוצאת הצבה ב- – לזה אפשר להשתמש ב- ו-, וכל מה שנשאר זה לחשב את בזמן טוב – לינארי.

## האלגוריתם:

האלגוריתם מקבל את דרגת הפולינום , מקדמיו וערך עבורו נחשב:

1. נתחיל מ- ו-
2. לכל :
   1. הגדר
   2. עדכן
3. נריץ על ו- כדי לקבל את צורת ה- שלהם מעל נקודות שנסמן ב- בהתאמה. ניצור וקטור חדש כל ש-. נריץ מעל הוקטור החדש ונשמור את התוצאה בווקטור .
4. לכל הצג את הפלט עבור הנגזרת את הערך

## ניתוח זמן ריצה:

שלב 3 למעשה מורכב מ-2 הרצות של והרצה בודדת של מעל ערכים, ולכן הסיבוכיות היא . כמו כן, בשלב 3 יש גם חישוב של כפל עבור כל ה- ערכים, ולכן סיבוכיות החישוב הזאת היא . ההרחבה של ושל ל- היא גם בזמן .

בשלב 4 אנחנו מבצעים פעולה קבועה פעמים ולכן גם זמן . בשלב 2 אנחנו מבצעים פעולות חיבור, כפל וחילוק שהוגדרו להיות בזמן קבוע, וסה"כ מריצים את הלולאה פעמים ולכן גם כאן הזמן הוא .

סה"כ קיבלנו .

## הוכחת נכונות:

לפי מה שתואר בהקדמה המתמטית, מתקיים שהערך של שווה לערך המקדם ה--י של פולינום המכפלה של . לפי הנכונות של אלגוריתם , אנחנו מקבלים בהצלחה את צורת ה- ולפי הצורה שבה הגדרנו נקבל את הצורה מעל נקודות.

שני הפולינומים הם מסדר , ולכן פולינום המכפלה הוא לכל היותר מסדר . כל פולינום מסדר ניתן לייצוג על ידי נקודות שונות בצורה יחידה. לפי הגדרת צורת אנחנו מקבלים לכל מתקיים וגם .  
ולכן עבור פולינום המכפלה מתקיים , ובפרט עבור , ולכן על ידי הכפלה של ערך משני הווקטורים לתוך וקטור חדש נקבל קודקודים של פולינום המכפלה, ו- נקודות אלו מייצגים פולינום בודד שהוא בדיוק פולינום המכפלה. ובזכות נכונות של אנחנו מקבלים את המקדמים של פולינום המכפלה .

# שאלה 4

אם נספור את מספר פעולות החיבור והחיסור באלגוריתם החדש, נקבל פעולות בחלק ו-8 בחלק . עבור מטריצה בגודל זמן לביצוע פעולת חיסור וחיבור היא (מעבר על תא ותא וביצוע ישיר של הפעולה).

אם נספור את מספר פעולות הכפל באלגוריתם החדש, נקבל 7 פעולות בחלק ו-0 בחלק . כאן למעשה הזמן של ביצוע פעולת כפל הוא זמן רקורסיבי על גודל המטריצה החדשה. אבל לפי איך שהגדרנו את התת-מטריצות בכל שלב הרקורסיה, למעשה כל פעם הגודל הוא מחצית מהגודל הנוכחי. ולכן קיבלנו:

כאשר המטריצה בגודל אפשר בצורה ישירה ללא זימון רקורסיבי לחשב את מכפלת המטריצות בעזרת 8 פעולות כפל ו-4 פעולות חיבור, ולכן . ולכן לפי משפט 5.4 (מכיוון ומתקיים ) נקבל: