**ממן 13 אלגוריתמים**

שאלה 1:

1. אנו מפעילים את האלגוריתם FFT על הפולינום , ראשית, נמיר אותו לתצוגת המקדמים:



*כעת, מכיוון שההפעלה הרקורסיבית של האלגוריתם על הייצוגים בגודל 1 תחזיר את הערך עצמו נקבל, בחזרה מן הקריאה הרקורסיבית:*

כעת, לאחר שיש לנו את ערכי ה"תתי-פולינומים" בשורשי היחידה מסדר 2, נוכל בעזרתם למצוא את ערכי הפולינום בשורשי היחידה מסדר 4, בחזרה מן הקריאה הרקורסיבית:

כלומר, הערכים בנקודות שורשי היחידה מסדר 4 הם *.*

1. *כעת, נפעיל את אלגוריתם , על*  *, בעת ההמרה נשתמש ב בתור .*



*כעת, מכיוון שההפעלה הרקורסיבית של האלגוריתם על הייצוגים בגודל 1 תחזיר את הערך עצמו נקבל, בחזרה מן הקריאה הרקורסיבית:*

כעת, לאחר שיש לנו את ערכי ה"תתי-פולינומים" בשורשי היחידה מסדר 2, נוכל בעזרתם למצוא את ערכי הפולינום בשורשי היחידה מסדר 4, בחזרה מן הקריאה הרקורסיבית:

כלומר, התקבל מהאלגוריתם את ייצוג המקדמים *, כלומר כפולה ב* של ייצוג המקדמים המקורי *, ומכאן ניתן לשחזר את הפולינום .*

*שאלה 2:*

***רעיון האלגוריתם:***

*באלגוריתם של Karatsuba מחלקים כל מספר בעל n ספרות בייצוג הבינארי ל2 בלוקים בעלי ספרות, כל אחת.*

*באלגוריתם שלנו, על מנת להכפיל 2 מספרים נחלק כל מספר בעל n ספרות ל "בלוקים" בעלי K ספרות, ונעשה רדוקציה לכפל פולינומים בשיטת FFT. נסביר את ההגיון:*

*ניתן להסתכל על כל זוג מספרים X,Y בגודל N ספרות כך:*

נבחין כי כל מספר הוא בעצם פולינום בהצבה של .

לכן אם נרצה לבצע , כאמור, רדוקציה לבעיית כפל הפולינומים נסתכל על כל מספר באורך n כעל K מקדמים, הלא הם הסדרה , ולהפעיל עליהם את FFT.

לאחר שנפעיל על 2 המספרים FFT ונקבל את ערכיהם (כמובן, לו היו באמת פולינומים) ב שורשי היחידה, כעת נוכל להכפיל את ערכיהם בנקודות הללו, מהשאלה ניתן להניח כי הערכים החוזרים מן הקריאות הרקורסיביות לא משנות את אורכי המספרים, ולקבל את 2 סדרות מספרים, כל אחת, כפי שציינו, באורך מספרים, כלומר נקבל 2 רשימות , *, מכיוון שנתון כי* הערכים החוזרים מן הקריאות הרקורסיביות לא משנות את אורכי המספרים*, ניתן לכפול כל זוג ב, ולכן, נכפול כל זוג על מנת להגיע לרשימה , על הרשימה הזאת נפעיל את , על מנת להגיע למקדמי פולינום המכפלה המקורית* , נחלק בכמות איברי היחידה, קרי ב- ולאחר שהגענו למקדמי הפולינום שמייצג את המכפלה, נוכל להחזיר לפיהם את תוצאת הכפל:

**מבנה האלגוריתם:**

ראשית, באמצעות הנוסחות

נבודד את הסדרות , לאחר מכן, נבצע השלמת 0-ים עד לקבלת 2 סדרות באורך שהוא חזקה של 2, ממתמטיקה פשוטה נקבל כי אורך הסדרות הוא בדיוק כעת, נבצע את *, ואת , על מנת לקבל את הייצוגים הנוחים יותר להכפלה (-כלומר, ביעילות גבוהה יותר), כעת לאחר שקיבלנו מהפעלת הFFT-ים 2 סדרות בגודל , נכפול בהן איבר-איבר (כאמור, ביעילות של ),נכנה את וקטור התוצאה בשם C לצורך העניין, ונפעיל , על מנת לקבל את תצוגת המקדמים של פולינום המכפלה, את איברי המכפלה נחלק כל אחד ב .*

*כעת לאחר שקיבלנו את תצוגת המקדמים של פולינום המכפלה, ניתן להחזיר את המספר לפי הנוסחה:*

נחזיר את התוצאה וזהו.

**נכונות האלגוריתם:**

נבחין כי אנו מבצעים רדוקציה לבעיית הכפלת הפולינומים**,** כלומר, ניתן להסתמך על כך שFFT עובד כהלכה. נותר רק להראות כי ממיר הקלט וממיר הפלט עובדים כהלכה ומחזירים את התשובה הנכונה:

אם מתייחסים לכל מספר בתצוגת המקדמים שלו, ניתן לראות כי

*וכי ולכן הפירוק שהאלגוריתם מבצע לקלט, בהופכו לn/k מקדמים, נכון עבור כל אחד מ2 המספרים המובאים כקלט.*

*כעת, נניח כי FFT עושה את עבודתו כנדרש, ולכן יש לנו כ- ערכי ה"פולינום" ב שורשי היחידה, לכל אחד מהפולינומים, כעת, האלגוריתם יכפיל אותם לפי הסדר, על מנת לקבל את שורשי היחידה המתאימים עבור פולינום המכפלה (מכיוון שלכל שורש יחידה l, ולכל מספר בעצם, מתקיים: ) ), כעת, האלגוריתם ימצא-ממש כפי שהיינו מבצעים כפל פולינומים- את פולינום המכפלה עצמו, על ידי הפעלת , כאשר C הוא וקטור המייצג את ערכי פולינום המכפלה בשורשי היחידה, כעת לאחר שקיבלנו את פולינום המכפלה, האלגוריתם יחזיר את (גם שקול, בצורה דומה למה שהראנו עבור X, להצבה של בפולינום המכפלה), שבאופן מתמטי שקול בדיוק לכפל הרגיל- המכפלה של כל זוג איברים () מוכפלת בערך המיקום שלהם () מביאה אותנו לכפל.*

*מתמטית, האלגוריתם מבצע את המעברים הבאים:*

ומחזיר את התוצאה.

**סיבוכיות זמן ריצה:**

האלגוריתם מורכב מהמרת הקלט, הפעלתFFT על 2 הפולינומים, הכפלת התוצאה המתקבלת, איבר-איבר, הפעלת והצבת וחישוב (בעצם הצבת ) בפולינום.

המרת הקלט:

בעצם החלוקה לבלוקים היא פעולה על הביטים, ולכן תלויה בכמות הביטים, "נרוץ" על הביטים, וניקח כל K ביטים ונגדירם כבלוק- כלומר המרת הקלט תתבצע ב *.*

*הפעלת FFT על 2 סדרות המקדמים:*

*מכיוון שאנו מוסיפים אפסים עד להגעה לכמות מקדמים שהיא חזקה של 2, אך לא ניתן להישאר עם יותר מפי 2 איברים לכל סדרת מקדמים, כלומר, לכל היותר נפעיל FFT על איברים, וכידוע, סיבוכיות הפעלת FFT על L איברים , אך, כמובן זה בהנחה כי כפל הינו פעולה בסיסית, אם כפל מתבצע בכפי שניתן להניח אצלנו, פתרון נוסחת הנסיגה של FFT הינו*

*הכפלת התוצאות איבר-איבר:*

*הכפלת כל ערך בערך אחר יעשה, לפי הנחת השאלה ב, ולכן מכיוון שישנו סדר גודל של ערכים בכל רשימה, השלב הזה יעשה בסיבוכיות של .*

הפעלת :

בצורה דומה ל להפעלת הFFT, מכיוון שגודל הקלט נשאר זהה, ולכן גם הסיבוכיות זהה.

חישוב :

מכיוון שכפל בחזקה של 2 דורש סה"כ פעולות על ביטים (הזזה קדימה ואחורה של הביטים), ומכיוון שכבר נתונים *לנו המקדמים , אזי הפעולה יכולה להתבצע בזמן לינארי (רק מיקום של מספרים קיימים בביטים ידועים).*

*ולכן, סה"כ, סיבוכיות האלגוריתם היא:*

שאלה 3:

נפתור באופן מקוצר בצורה דומה לפתרון המקוצר של אלגוריתם חיפוש בינארי המופיע באתר.

האלגוריתם:

"נכין" 2 וקטורים , נכפיל אותם לפי אלגוריתםFFT -כלומר נפעיל FFT, נכפיל איבר-איבר, ונפעיל כעת נקבל וקטור באורך *, נחזיר את n+1 האיברים הראשונים, ונחזיר אותם מהסוף להתחלה. כלומר, מכיוון שהנגזרת מסדר n נמצאת במקום 1...והנגזרת מסדר 0 נמצאת במקום הn+1, נהפוך בסדר שלהם ונחזיר.*

*נכונות האלגוריתם:*

*עבור איבר במיקום הK האיבר היה במיקום וככזה, הוא* שווה ל

וזו בדיוק ההגדרה של , כנדרש.

סיבוכיות:

נניח כי אנו שומרים במערך את כל העצרות, עד n, על מנת שכל קריאה לעצרת תהיה בסיבוכיות של 1- דבר זה יתבצע בסיבוכיות *.*

*כעת, "הכנת" הווקטורים תתבצע בסיבוכיות של .*

*הרדוקציה לFFT וההכפלה יתבצעו ב.*

*וגם החזרה בסדר הפוך תתבצע ב*

*ולכן סיבוכיות האלגוריתם הינה*

*שאלה 4:*

*סעיף ד:*

*האלגוריתם הינו בעצם אלגוריתם רקורסיבי, שמפרק כל מטריצה ל4 מטריצות בגודל , כאשר הבסיס שלו-כלומר תנאי העצירה- הינו כפל 2 מטריצות ריבועיות בגודל , האלגוריתם יחשב את התוצאה לפי חישוב 7 מטריצות עזר המובאות בשאלה עצמה, בצורה רקורסיבית:*

*כאמור, לאחר שהאלגוריתם יחשב את המטריצות הללו בצורה רקורסיבית, הוא יחזיר את המטריצה* .

כעת, לאחר הצגת האלגוריתם המובא בצורה בהירה, ניתן לחשב את זמן הריצה:

כידוע, חישוב חיבור וחיסור מטריצות מסדר n נעשה בסיבוכיות של *,*

*לפי האבחנה ביצענו בסעיף ב', חישוב המטריצות מתבצע ב7 פעולות כפל מטריצות- קרי, קריאה לרקורסיה כ7 פעמים על בעיה קטנה פי 2 (כל שורה קטנה פי 2 וכל עמודה קטנה פי 2, אך לפי צורת פעולת האלגוריתם הבעיה עדיין קטנה פי 2 ולא פי 4), (ועוד כמובן חיבור וחיסור מטריצות מהסדר הנ"ל, שגם נעשה ע"י פעולות).*

*לסיכום, אם נבנה נוסחת נסיגה עבור הסיבוכיות, נקבל (עבור קבוע C חסם עליון למספר פעולות החיבור והחיסור על מטריצה):*

נתבונן במשפט האב, מקרה 1:

מכיוון שמתקיים קטנה אסימפטוטית מ, מכיוון שעבור האפסילון מתקיים כי , ולכן, מסקנת משפט האב במקרה הזה מציינת כי פתרון נוסחת הנסיגה הינו  *ולכן האלגוריתם מבצע פעולות אלמנטריות בלבד, כנדרש.*