1 FFT

1.1 התמרת פורייה בדידה והתמרת פורייה מהירה

1.1.1 סיפור רקע

התמרת פורייה מהירה (FFT) הוא אלגוריתם חשוב עם שימושים רבים : דחיסה, עיבוד אותות, למידה, מציאת תבניות טקסטואליות. בהרצאה נראה שימוש אחד שלו (שגם מהווה מוטיבציה) - פעולות יעילות על פולינומים.

1.1.2 ייצוג המקדמים של פולינומים

הגדרה 1: יהי n מספר טבעי. נגדיר V_{n-1} להיות המרחב הווקטורי של כל הפולינומים ממעלה גדולה מ-0 וקטנה מ-$n-1$ עם מקדמים ממשיים.

נאמר כי וקטור המקדמים של הפולינום $a_0 + a_1x + ... + a_{n-1}x^{n-1}$ הוא $\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}$. רישום הפולינום באמצעות המקדמים שלו הוא ייצוג המקדמים של הפולינום. (המרחב הזה הוא ממימד n)

$$V_{n-1} = \left\{ \sum_{k=0}^{n-1} a_k x^k : a_1, ..., a_k \in \right\}$$

הערה 1: ההתאמה $\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} \longleftrightarrow \sum_{k=0}^{n-1} a_k x^k$ מגדירה איזומורפיזם של מרחבים וקטורים בין V_{n-1} ל-$\mathbb{R}^n$.

הערה 2: ייצוג המקדמים של הפולינום מציג את מקדמי הפיתוח של הפולינום לפי בסיס מסוים של V_{n-1} : $\{1, x, ..., x^{n-1}\}$.

1.1.3 פעולות על פולינומים בייצוג המקדמים

חיבור פולינומים

קלט: שני פולינומים $P, Q \in V_{n-1}$ בייצוג מקדמים.

פלט: הפולינום $R = P + Q$ בייצוג מקדמים.

האלגוריתם: יהיו $\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}, \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{bmatrix}$ ייצוג המקדמים של P ו-Q בהתאמה. יהי $\begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix}$ ייצוג המקדמים של R אזי $c =$ $\begin{bmatrix} a_0 + b_0 \\ a_1 + b_1 \\ \vdots \\ a_{n-1} + c_{n-1} \end{bmatrix} = \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix}$. נחשב את c ונחזיר אותו.

זמן ריצה: $O(n)$.

הצבת ערך בפולינום

קלט: פולינום $P \in C_{n-1}$ בייצוג המקדמים ונקודה $x_0 \in \mathbb{R}$.

פלט: $P(x_0)$.

האלגוריתם: נחשב את סדרת החזקות $1, x_0, ..., x_0^{n-1}$ באופן הבא: לכל $0 \geq k$ נחשב $x_0^{k+1} = x_0 \cdot x_0^k$. ניתן לעשות זאת ב-$O(n)$ פעולות כפל. יהי $\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}$ ווקטור המקדמים של P. נחשב את $P(x_0) = \sum_{k=0}^{n-1} a_k x^k$ כמכפלה פנימית של שני ווקטורים ($\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}$ ו- $\begin{bmatrix} 1 \\ x_0 \\ \vdots \\ x_0^{n-1} \end{bmatrix}$.

סה"כ זמן ריצה: $O(n)$.

כפל פולינומים

<u>קלט</u>: שני פולינומים $P, Q \in V_{n-1}$ בייצוג המקדמים.

<u>פלט</u>: הפולינום $R = P \cdot Q \in V_{2n-2}$ בייצוג המקדמים.

<u>הסבר</u>: $\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}$, $\begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{bmatrix}$ ייצוג המקדמים של P ו-Q בהתאמה. יהי $\begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix}$ ווקטור המקדמים של R אזי:

$$R(x) = (a_0 + a_1 x + ... + a_{n-1} x^{n-1}) \cdot (b_0 + b_1 x + ... + b_{n-1} x^{n-1})$$

$$\Downarrow$$

$$\begin{cases} c_0 = a_0 b_0 \\ c_1 = a_0 b_1 + a_1 b_0 \\ \vdots \\ c_{n-1} = a_0 b_{n-1} + a_1 b_{n-2} + ... + a_{n-1} b_0 \\ \vdots \\ c_{2n-2} = a_{n-1} \cdot n_{n-1} \end{cases}$$

c, ווקטור המקדמים של הפולינום R הניתן על פי אוסף הנוסחאות שחישבנו, נקרא הקונבולוציה של הווקטורים $a = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}$, $b = \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{bmatrix}$.

<u>האלגוריתם</u>: בהינתן הווקטורים $a, b \in \mathbb{R}^n$ שהם ייצוגי המקדמים של P ו-Q בהתאמה, נחשב את הווקטור $c \in \mathbb{R}^{2n-2}$ שהוא הקונבולוציה של a ו-b ונחזיר את c.

<u>זמן ריצה</u>: $O(n^2)$ (יקר מדי).

1.1.4 ייצוג הערכים של פולינומים

<u>עובדה אלגברית:</u> פולינום ממעלה קטנה או שווה ל-$n-1$ מעל שדה בגודל לפחות n נקבע על ידי הערכים שלו ב-n נקודות שונות.

<u>עובדה שקולה:</u> לפולינום שונה מ-0 ממעלה קטנה או שווה ל-$n-1$ יכולים להיות לכל היותר $n-1$ שורשים שונים בשדה.

<u>הגדרה:</u> תהיינה $x_0, .., x_{n-1}$ n נקודות ממשיות שונות (כרגע שרירותיות). עבור פולינום $P \in V_{n-1}$, <u>ייצוג הערכים</u> של P בנקודות $(x_0, ..., x_{n-1})$

הוא הווקטור $\begin{bmatrix} P(x_0) \\ P(x_1) \\ \vdots \\ P(x_{n-1}) \end{bmatrix}$ (הערכים של הפולינום בנקודות האלה).

הערה 1: ההתאמה בין הפולינום $P \in V_{n-1}$ לווקטור הערכים שלו היא איזומורפיזם של מרחבים ווקטורים בין V_{n-1} ל-$\mathbb{R}^n$ (ובפרט היא על).

הערה 2: ווקטור הערכים של פולינום מציג את מקדמי הפיתוח של הפולינום לפי בסיס אחר של V_{n-1}.

1.1.5 פעולות על פולינומים בייצוג הערכים

חיבור פולינומים

תהיינה $x_0, x_1, ..., x_{n-1}$ נקודות ממשיות שונות.

קלט: שני פולינומים $P, Q \in V_{n-1}$ בייצוג הערכים (בנקודות $x_0, ..., x_{n-1}$).

פלט: הפולינום $R = P + Q$ בייצוג הערכים (בנקודות $x_0, ..., x_{n-1}$).

האלגוריתם: יהיו $\begin{bmatrix} P(x_0) \\ P(x_1) \\ \vdots \\ P(x_{n-1}) \end{bmatrix}, \begin{bmatrix} Q(x_0) \\ Q(x_1) \\ \vdots \\ Q(x_{n-1}) \end{bmatrix}$ ייצוגי הערכים של P ו-Q בהתאמה. ווקטור הערכים של R בנקודות $x_0, ..., x_{n-1}$

הוא $\begin{bmatrix} P(x_0)+Q(x_0) \\ P(x_1)+Q(x_1) \\ \vdots \\ P(x_{n-1})+Q(X_{n-1}) \end{bmatrix} = \begin{bmatrix} R(x_0) \\ R(x_1) \\ \vdots \\ R(x_{n-1}) \end{bmatrix}$.

זמן ריצה: $O(n)$ לחישוב הווקטור.

כפל פולינומים (אלגוריתם לא נכון!)

תהיינה $x_0, x_1, ..., x_{n-1}$ נקודות ממשיות שונות.

קלט: שני פולינומים $P, Q \in V_{n-1}$ בייצוג הערכים (בנקודות $x_0, ..., x_{n-1}$).

פלט: הפולינום $R = P \cdot Q \in V_{2n-2}$ בייצוג הערכים (בנקודות $x_0, ..., x_{n-1}$).

האלגוריתם: יהיו $\begin{bmatrix} P(x_0) \\ P(x_1) \\ \vdots \\ P(x_{n-1}) \end{bmatrix}, \begin{bmatrix} Q(x_0) \\ Q(x_1) \\ \vdots \\ Q(x_{n-1}) \end{bmatrix}$ ייצוגי הערכים של P ו-Q בהתאמה. ייצוג הערכים של הפולינום R בנקודות האלה הוא הווקטור $\begin{bmatrix} P(x_0) \cdot Q(x_0) \\ P(x_1) \cdot Q(x_1) \\ \vdots \\ P(x_{n-1}) \cdot Q(X_{n-1}) \end{bmatrix} = \begin{bmatrix} R(x_0) \\ R(x_1) \\ \vdots \\ R(x_{n-1}) \end{bmatrix}$ נחשב את הווקטור הזה ונחזיר אותו.

זמן ריצה: $O(n)$.

אבל האלגוריתם הזה לא נכון כי אנחנו אמורים לקבל ווקטור ב-$\mathbb{R}^{2n-2}$!

כפל פולינומים (נכון)

תהיינה $x_0, x_1, ..., x_{2n-2}$ נקודות ממשיות שונות.

קלט: שני פולינומים $P, Q \in V_{n-1}$ בייצוג הערכים (בנקודות $x_0, ..., x_{2n-2}$).

פלט: הפולינום $R = P \cdot Q \in V_{2n-2}$ בייצוג הערכים (בנקודות $x_0, ..., x_{2n-2}$).

האלגוריתם: יהיו $\begin{bmatrix} P(x_0) \\ P(x_1) \\ \vdots \\ P(x_{2n-2}) \end{bmatrix}, \begin{bmatrix} Q(x_0) \\ Q(x_1) \\ \vdots \\ Q(x_{2n-2}) \end{bmatrix}$ ייצוגי הערכים של P ו-Q בהתאמה. ייצוג הערכים של הפולינום R בנקודות האלה הוא הווקטור $\begin{bmatrix} P(x_0) \cdot Q(x_0) \\ P(x_1) \cdot Q(x_1) \\ \vdots \\ P(x_{2n-2}) \cdot Q(X_{2n-2}) \end{bmatrix} = \begin{bmatrix} R(x_0) \\ R(x_1) \\ \vdots \\ R(x_{2n-2}) \end{bmatrix}$ נחשב את הווקטור הזה ונחזיר אותו.

זמן ריצה: $O(n)$.

הצבת ערך בפולינום

<table><tr><td>
תהיינה $x_0, x_1, ..., x_{n-1}$ נקודות ממשיות שונות.
<u>קלט</u>: פולינום $P \in V_{n-1}$ בייצוג הערכים (בנקודות $x_0, ..., x_{n-1}$) ונקודה $x_n \in R$ השונה מ-$x_0, ..., x_{n-1}$.
<u>פלט</u>: $P(x_n)$.
<u>האלגוריתם</u>: משתמשים בפולינומי לגראנז' (העשרה).
<u>זמן ריצה</u>: $O(n^2)$ (איטי מדי).
</td></tr></table>

1.1.6 סיכום

<u>בייצוג המקדמים</u>: חיבור והצבת ערך עולות $O(n)$, כפל $O(n^2)$.

<u>בייצוג הערכים</u>: חיבור וכפל $O(n)$. הצבת ערך: $O(n^2)$.

רעיון: נעבור בין הייצוגים, ונבצע כל פעולה בייצוג שבו היא יעילה.

1.1.7 מעבר בין הייצוגים - הקדמה

<u>הגדרה:</u> תהיינה $x_0, ..., x_{n-1}$, n נקודות ממשיות. <u>מטריצת ונדרמונדה</u> התלויה בנקודות האלה היא המטריצה בגודל $n \times n$:

$$M = \begin{bmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \cdots & x_{n-1}^{n-1} \end{bmatrix}$$

כלומר $M_{i,j} = x_i^j$ לכל $0 \le i, j \le n-1$.

-

<u>עובדה:</u>

$$det(M) = \prod_{i<j}(x_j - x_i)$$

בפרט, אם הנקודות $x_0, ..., x_{n-1}$ שונות זו מזו, אז המטריצה הפיכה.

למה: יהי $\begin{bmatrix} a_0 \\ \vdots \\ a_{n-1} \end{bmatrix}$ ייצוג המקדמים של הפולינום $P(x) = \sum_{k=0}^{n-1} a_k x^k$. תהיינה $x_0, ..., x_{n-1}$ n נקודות ממשיות שונות. אזי:

$$\begin{bmatrix} P(x_0) \\ \vdots \\ P(x_{n-1}) \end{bmatrix} = M \begin{bmatrix} a_0 \\ \vdots \\ a_{n-1} \end{bmatrix}$$

הוכחת הלמה: יהי $0 \le m \le n-1$ נוודא כי $P(x_m) = \left[M \begin{bmatrix} a_0 \\ \vdots \\ a_{n-1} \end{bmatrix} \right]_m$. ואמנם:

$$\left[M \begin{bmatrix} a_0 \\ \vdots \\ a_{n-1} \end{bmatrix} \right]_m = \sum_{k=0}^{n-1} x_m^k a_k = \sum_{k=0}^{n-1} a_k x_m^k = p(x_m)$$

דוגמא:

$n = 3$, $p(x) = 1 + x + x^2$, $\begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$, $x_0 = 1, x_1 = 2, x_2 = 3$. אז:

$$\begin{bmatrix} P(x_0) \\ P(x_1) \\ P(x_2) \end{bmatrix} = \begin{bmatrix} 3 \\ 7 \\ 13 \end{bmatrix}, \quad M = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{bmatrix}$$

$$M \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 7 \\ 13 \end{bmatrix}$$

הערה: נשים לב כי מכיוון ש-M מטריצה הפיכה (עבור $x_0, .., x_{n-1}$ שונות זו מזו) נוכל לעבור מייצוג הערכים לייצוג המקדמים של הפולינום

באמצעות הנוסחא:

$$\begin{bmatrix} a_0 \\ \vdots \\ a_{n-1} \end{bmatrix} = M^{-1} \begin{bmatrix} P(x_0) \\ \vdots \\ P(x_{n-1}) \end{bmatrix}$$

הערה: בפרט זה מוכיח את העובדה האלגברית כי הפולינום היחיד ממעלה קטנה או שווה מ-$n-1$ המתאפס בנקודות $x_0, x_1, ..., x_{n-1}$ הוא פולינום האפס.

1.1.8 מעבר בין הייצוגים - איך בפועל?

כפל של מטריצה $n \times n$ בווקטור באורך n עולה $O(n^2)$ אלא אם כן יש למטריצה מבנה מיוחד. ננסה לבחור את הנקודות $x_0, ..., x_{n-1}$ כך של-M (מטריצת הוונדרמונדה שלנו) יהיה מבנה המאפשר מכפלה יעילה של M בווקטור ממשי באורך n.

הרעיון שפותר את הבעיה: נרצה לבחור את הנקודות $x_0, ..., x_{n-1}$ להיות מספרים מרוכבים בנורמה 1. יותר מזה, נבחר אותם להיות שורשי יחידה (מספר שבחזקה כלשהי שווה ל-1) מסדר n.

תזכורת מספרים מרוכבים :

ייצוג קרטזי :

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}, i^2 = -1\}$$

ייצוג פולארי :

$$a + bi = r \cdot (cos(\theta) + isin(\theta))$$

$$r = \sqrt{a^2 + b^2}, \theta = cos^{-1}(\frac{a}{\sqrt{a^2 + b^2}})$$

$$r_1 cis(\theta_1) \cdot r_2 cis(\theta_2) = r_1 \cdot r_2 \cdot cis(\theta_1 + \theta_2)$$

ייצוג אוילר :

$$z = r(cos(\theta) + isin(\theta) = r \cdot e^{i\theta}$$

$$r_1 e^{i\theta_1} \cdot r_2 e^{i\theta_2} = r_1 \cdot r_2 \cdot e^{i(\theta_1 + \theta_2)}$$

הגדרה: שורשי היחידה המרוכבים מסדר n הם :

$$\{z \in \mathbb{C} : z^n = 1\}$$

החזקות של שורש יחידה מסדר n מ-1 עד n גם הן שורשי יחידה מסדר n וגם הן מחלקות את המעגל לחלקים שווים.

הגדרה: שורש יחידה פרימיטיבי מסדר n הוא המספר $\omega_n = cos(\frac{2\pi}{n}) + isin(\frac{2\pi}{n})$.

למה:

שורשי היחידה מסדר n הם $1, \omega_n, \omega_n^2, ..., \omega_n^{n-1}$.

הוכחה : מתקיים :

$$\omega_n^n = cis(\frac{2\pi}{n})^n = cis(n \cdot \frac{2\pi}{n}) = cis(2\pi) = 1$$

ולכן לכל $0 \le k \le n-1$

$$(\omega_n^k)^n = (\omega_n^n)^k = 1^k = 1$$

אז קיבלנו n שורשי יחידה שונים מסדר n, ובגלל העובדה האלגברית שראינו אלו כל שורשי היחידה מסדר n.

הערה: עבור בחירת שורשי היחידה בתור נקודות הייצוג של הפולינום $x_k = \omega_n^k$, עבור $1 \le k \le n-1$, המטריצה M (וונדרמונדה) נראית באופן הבא (לכל $0 \le k, j \le n-1$):

$$M_{k,j} = x_k^j = \omega_n^{k \cdot j}$$

דוגמאות:

1. $n = 2$, $\omega_2 = -1$ $M_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

2. $n = 4$, $\omega_4 = i$. השורשים מסדר 4: $1, i, -1, -i$. $M_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$

הגדרה: (התמרת פורייה בדידה) יהי n מספר טבעי, יהי ω_n שורש יחידה פרימיטיבי מסדר n. עבור וקטור $\begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix} \in \mathbb{C}^n$ יהי p הפולינום $p(z) = \sum_{k=0}^{n-1} a_k z^k$ נגדיר התמרת פורייה בדידה של $\begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix}$ להיות הווקטור $\begin{pmatrix} p(\omega_n^0) \\ \vdots \\ p(\omega_n^{n-1}) \end{pmatrix}$.

סימון: נסמן התמרת פורייה של וקטור $a \in \mathbb{C}^n$ ע"י $DFT_n(a)$

הערה 1: התמרת פורייה בדידה של וקטור $a \in \mathbb{C}^n$ הוא ייצוג הערכים בשורשי היחידה של הפולינום ש-a הוא ייצוג המקדמים שלו.

הערה 2: מתקיים $DFT_n(a) = M_n \cdot a$ כאשר המטריצה M_n היא המטריצה המקיימת $(M_n)_{k,j} = \omega_n^{k \cdot j}$.

הגדרה: יהי $p \in \mathbb{C}^n$ נגדיר $DFT_n^{-1}(p) = M_n^{-1} \cdot p$. נשים לב כי:

$$\begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix} = DFT_n^{-1} \begin{pmatrix} p_0 \\ \vdots \\ p_{n-1} \end{pmatrix}$$

הוא ייצוג המקדמים של הפולינום $p(z)=\sum_{k=0}^{n-1}a_kz^k$ המקיים:

$$\begin{pmatrix} p(\omega_n^0) \\ \vdots \\ p(\omega_n^{n-1}) \end{pmatrix} = \begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix}$$

משפט ה-FFT:

יהי n חזקה של 2. אזי:

1. לכל $a\in\mathbb{C}^n$ ניתן לחשב את $DFT_n(a)$ בזמן $O(nlog(n))$ (קבוע: $3nlogn+O(n)$).
2. לכל $p\in\mathbb{C}^n$ ניתן לחשב את $DFT_n^{-1}(p)$ בזמן $O(nlog(n))$.

לפני הוכחת המשפט נסתכל על 3 למות:

למה (תרגיל):

מתקיים לכל $0\le k,j\le n-1$:

$$((M_n)^{-1})_{k,j}=\frac{1}{n}(\omega_n^{-kj})$$

למה 1:

יהי n מספר זוגי. אזי:

1. $\omega_n^2=\omega_{\frac{n}{2}}$ ובאופן כללי, לכל $0\le k\le\frac{n}{2}-1$ מתקיים $(\omega_n^k)^2=\omega_{\frac{n}{2}}^k$ וגם $(\omega_n^{\frac{n}{2}+k})^2=\omega_{\frac{n}{2}}^k$
2. $\omega_n^{\frac{n}{2}}=-1$.

הוכחת למה 1:

1. מתקיים:

$$\omega_n^2=(cis(\frac{2\pi}{n}))^2=cis(\frac{2\pi}{\frac{n}{2}})=\omega_{\frac{n}{2}}$$

יהי $0\le k\le\frac{n}{2}-1$ אזי:

$$(\omega_n^k)^2=(\omega_n^2)^k=\omega_{\frac{n}{2}}^k$$
$$(\omega_n^{\frac{n}{2}+k})^2=\omega_n^n\cdot(\omega_n^k)^2=\omega_{\frac{n}{2}}^k$$

למה 2:

יהי n מספר זוגי. יהי $\begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix} \in \mathbb{C}^n$. יהי p הפולינום $p(z)=\sum_{k=0}^{n-1} a_k z^k$ אזי לכל $z\in\mathbb{C}$ מתקיים:

$$p(z) = p_0(z^2) + zp_1(z^2)$$

כאשר:

$$\begin{aligned} p_0(y) &= \sum_{l=0}^{\frac{n}{2}-1} a_{2l} y^l \\ p_1(y) &= \sum_{m=0}^{\frac{n}{2}-1} a_{2m+1} y^m \end{aligned}$$

הוכחת למה 2:

$$\begin{aligned} p_0(z^2) + zp_1(z^2) &= \sum_{l=0}^{\frac{n}{2}-1} a_{2l}(z^2)^l + z\sum_{m=0}^{\frac{n}{2}-1} a_{2m+1}(z^2)^m = \\ &= \sum_{l=0}^{\frac{n}{2}-1} a_{2l} z^{2l} + \sum_{m=0}^{\frac{n}{2}-1} a_{2m+1} z^{2m+1} \\ &= \sum_{k=0}^{n-1} a_k z^k \\ &= p(z) \end{aligned}$$

הוכחת משפט ה-FFT

יהי $\begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix} \in \mathbb{C}^n$. יהי p הפולינום $p(z)=\sum_{k=0}^{n-1} a_k z^k$. יהיו

$$\begin{aligned} p_0(y) &= \sum_{l=0}^{\frac{n}{2}-1} a_{2l} y^l \\ p_1(y) &= \sum_{m=0}^{\frac{n}{2}-1} a_{2m+1} y^m \end{aligned}$$

אזי:

$$
\begin{aligned}
DFT_n \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} &= \begin{pmatrix} p(\omega_n^0) \\ p(\omega_n^1) \\ \vdots \\ p(\omega_n^{n-1}) \end{pmatrix} \\
&\overset{\star}{=} \begin{pmatrix} p_0((\omega_n^0)^2) + \omega_n^0 \cdot p_1((\omega_n^0)^2) \\ p_0((\omega_n^1)^2) + \omega_n^1 \cdot p_1((\omega_n^1)^2) \\ \vdots \\ p_0((\omega_n^{n-1})^2) + \omega_n^{n-1} + \cdot p_1((\omega_n^{n-1})^2) \end{pmatrix} \\
&= \begin{pmatrix} p_0((\omega_n^0)^2) \\ p_0((\omega_n^1)^2) \\ \vdots \\ p_0((\omega_n^{n-1})^2) \end{pmatrix} + \begin{pmatrix} \omega_n^0 \\ \omega_n^1 \\ \vdots \\ \omega_n^{n-1} \end{pmatrix} \cdot \begin{pmatrix} p_1((\omega_n^0)^2) \\ p_1((\omega_n^1)^2) \\ \vdots \\ p_1((\omega_n^{n-1})^2) \end{pmatrix} \\
&\overset{◷}{=} \left(\begin{array}{c} p_0(\omega_{\frac{n}{2}}^0) \\ p_0(\omega_{\frac{n}{2}}^1) \\ \vdots \\ p_0(\omega_{\frac{n}{2}}^{n-1}) \\ \hline p_0(\omega_{\frac{n}{2}}^0) \\ p_0(\omega_{\frac{n}{2}}^1) \\ \vdots \\ p_0(\omega_{\frac{n}{2}}^{n-1}) \end{array}\right) + \begin{pmatrix} \omega_n^0 \\ \omega_n^1 \\ \vdots \\ \omega_n^{n-1} \end{pmatrix} \left(\begin{array}{c} p_1(\omega_{\frac{n}{2}}^0) \\ p_1(\omega_{\frac{n}{2}}^1) \\ \vdots \\ p_1(\omega_{\frac{n}{2}}^{n-1}) \\ \hline p_1(\omega_{\frac{n}{2}}^0) \\ p_1(\omega_{\frac{n}{2}}^1) \\ \vdots \\ p_1(\omega_{\frac{n}{2}}^{n-1}) \end{array}\right)
\end{aligned}
$$

$\star$ נובע מלמה 2, ◷ נובע מלמה 1.

נשים לב כי ייצוג המקדמים של הפולינום $p_0(y)$ הוא הווקטור $\begin{pmatrix} a_0 \\ a_2 \\ \vdots \\ a_{n-2} \end{pmatrix} \in \mathbb{C}^{\frac{n}{2}}$ ולכן על פי הגדרת התמרת פורייה מסדר $\frac{n}{2}$ מתקיים:

$$
\begin{pmatrix} p_0(\omega_{\frac{n}{2}}^0) \\ p_0(\omega_{\frac{n}{2}}^1) \\ \vdots \\ p_0(\omega_{\frac{n}{2}}^{n-1}) \end{pmatrix} = DFT_{\frac{n}{2}} \begin{pmatrix} a_0 \\ a_2 \\ \vdots \\ a_{n-2} \end{pmatrix}
$$

כנ"ל לגבי p_1 ולכן קיבלנו

$$DFT_n\begin{pmatrix}a_0\\a_1\\\vdots\\a_{n-1}\end{pmatrix}=\left(\frac{DFT_{\frac{n}{2}}\begin{pmatrix}a_0\\a_2\\\vdots\\a_{n-2}\end{pmatrix}}{DFT_{\frac{n}{2}}\begin{pmatrix}a_0\\a_2\\\vdots\\a_{n-2}\end{pmatrix}}\right)+\begin{pmatrix}\omega_n^0\\\omega_n^1\\\vdots\\\omega_n^{n-1}\end{pmatrix}\left(\frac{DFT_{\frac{n}{2}}\begin{pmatrix}a_1\\3\\\vdots\\a_{n-1}\end{pmatrix}}{DFT_{\frac{n}{2}}\begin{pmatrix}a_1\\a_3\\\vdots\\a_{n-1}\end{pmatrix}}\right)$$

1.1.9 האלגוריתם

הזהות הרקורסיבית מאפשרת לבנות את האלגוריתם הבא לחישוב התמרת פורייה מסדר n:

אלגוריתם 1 חישוב התמרת פורייה מסדר n כאשר n חזקה של 2

---

1. בהינתן $\mathbb{C}^n \ni a = \begin{pmatrix}a_0\\\vdots\\a_{n-1}\end{pmatrix}$ נחשב באופן רקורסיבי את $DFT_{\frac{n}{2}}\begin{pmatrix}a_0\\a_2\\\vdots\\a_{n-2}\end{pmatrix}$, $DFT_{\frac{n}{2}}\begin{pmatrix}a_1\\3\\\vdots\\a_{n-1}\end{pmatrix}$, ובעזרת הזהות הרקורסיבית נחשב את $DFT_n(a)$ על ידי $3n$ פעולות נוספות. (n כפלים, n חיבורים, n שכפולים).
2. ניקח בתור בסיס הרקורסיה את המקרה $n=2$, שבו $DFT_2 = \underbrace{\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}}_{M_2}\begin{pmatrix}a_o\\a_1\end{pmatrix}$

<u>זמן הריצה:</u> נסמן את זמן הריצה לחישוב DFT_n ב-$T(n)$. קיבלנו כי:

$$T(n) \le 2T(\frac{n}{2}) + 3n$$

ולכן (לפי משפט האב או חישוב ישיר) $T(n) \le 3nlog_2(n) + O(n)$.

1.1.10 שימוש במשפט ה-FFT - אלגוריתם מהיר לכפל פולינומים בייצוג המקדמים.

בעיית כפל פולינומים מהיר בייצוג המקדמים

<u>קלט</u>: שני פולינומים $P,Q \in V_{n-1}$ בייצוג המקדמים.

<u>פלט</u>: הפולינום $R = P \cdot Q \in V_{2n-2}$ בייצוג המקדמים.

אלגוריתם 2 כפל פולינומים מהיר בייצוג המקדמים

יהיו $\begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix}, \begin{pmatrix} b_0 \\ \vdots \\ b_{n-1} \end{pmatrix} \in \mathbb{C}^n$ ייצוגי המקדמים של P ו-Q בהתאמה. יהי $\begin{pmatrix} c_0 \\ \vdots \\ c_{2n-2} \end{pmatrix} \in \mathbb{C}^{2n-1}$ ייצוג המקדמים של R. תהי m חזקת 2 הקטנה ביותר הגדולה או שווה ל-$2n-1$.

1. נחשב את $\begin{pmatrix} p_0 \\ \vdots \\ p_{m-1} \end{pmatrix} = DFT_m \begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, $\begin{pmatrix} q_0 \\ \vdots \\ q_{m-1} \end{pmatrix} = DFT_m \begin{pmatrix} b_0 \\ \vdots \\ b_{n-1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$.
2. נחשב $\begin{pmatrix} \tilde{c}_0 \\ \vdots \\ \tilde{c}_{m-1} \end{pmatrix} = DFT_m^{-1} \begin{pmatrix} p_0 \cdot q_0 \\ \vdots \\ p_{n-1} \cdot q_{m-1} \end{pmatrix}$.
3. נחזיר את $\begin{pmatrix} \tilde{c}_0 \\ \vdots \\ \tilde{c}_{2n-2} \end{pmatrix}$.

<u>טענה:</u>

1. $\begin{pmatrix} c_0 \\ \vdots \\ c_{2n-2} \end{pmatrix} = \begin{pmatrix} \tilde{c}_0 \\ \vdots \\ \tilde{c}_{2n-2} \end{pmatrix}$. (נכונות).
2. זמן הריצה של האלגוריתם הוא $O(nlog(n))$.

<u>הוכחה:</u>

1. יהי ω_m שורש היחידה הפרימיטיבי מסדר m. לפי הגדרת DFT_m, מתקיים $\begin{pmatrix} P(\omega_m^0) \\ \vdots \\ P(\omega_m^{m-1}) \end{pmatrix} = \begin{pmatrix} p_0 \\ \vdots \\ p_{m-1} \end{pmatrix}, = \begin{pmatrix} q_0 \\ \vdots \\ q_{m-1} \end{pmatrix}$

$\begin{pmatrix} Q(\omega_m^0) \\ \vdots \\ Q(\omega_m^{m-1}) \end{pmatrix}$ ולכן $\begin{pmatrix} R(\omega_m^0) \\ \vdots \\ R(\omega_m^{m-1}) \end{pmatrix} = \begin{pmatrix} p_0 q_0 \\ \vdots \\ p_{m-1} q_{m-1} \end{pmatrix}$. לפי טענה אלגברית שראינו, R הוא הפולינום היחיד ממעלה קטנה או שווה ל-$n-1$ המקבל את הערכים האלה בשורשי היחידה מסדר m, ולכן על פי הגדרת DFT_m^{-1} :

$$\begin{pmatrix} \tilde{c}_0 \\ \vdots \\ \tilde{c}_{m-1} \end{pmatrix} = \begin{pmatrix} c_0 \\ \vdots \\ c_{2n-2} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

ולכן השוויון מתקיים.

2. על פי משפט ה-FFT זמן הריצה של האלגוריתם הוא $O(mlogm)$. על פי הגדרת m, מתקיים $m \leq 4n-2$, (אחרת $\frac{m}{2}$ הייתה חזקת 2 קטנה יותר שגדולה או שווה ל-$2n-1$). ולכן $m = O(n)$ וזמן הריצה של האלגוריתם הוא $O(nlog(n))$.