<u>התמרת פורייה וכפל מהיר של פולינומים</u>
נתונים 2 פולינומים מעל שדה F מדרגה חסומה ע"י n.
$$A(x)=a_0+a_1x+a_2x^2+...+a_{n-1}x^{n-1}$$
$$B(x)=b_0+b_1x+b_2x^2+...+b_{n-1}x^{n-1}$$

מעוניינים לחשב את פולינום המכפלה: $C(x)=A(x)\cdot B(x)$
$C(x)=c_0+c_1x+c_2x^2+...+c_{2n-2}x^{2n-2}$.

לדוגמה:
$$A(x)=8+2x+3x^2+x^4$$
$$B(x)=1+x+3x^4$$
$$c_3=a_0\cdot b_3+a_1\cdot b_2+a_2\cdot b_1+a_3\cdot b_0$$
$$c_j=\sum_{k=0}^{j}a_kb_{j-k}$$
זמן חישוב: $\Theta(n^2)$. המטרה היא לשפר ל: $\Theta(n\log n)$.

<u>ייצוגים של פולינומים:</u>
ייצוג ע"י וקטור מקדמים:
$$A(x)=\sum_{j=0}^{n-1}a_jx^j$$
$$a=(a_0,a_1,a_2,...,a_{n-1})$$

אם רוצים לחשב את $A(x_0)$ ניתן להשתמש בכלל *Horner*:
$A(x_0)=a_0+x_0\left(a_1+x_0\left(a_2+...+x_0\left(a_{n-2}+x_0a_{n-1}\right)...\right)\right)$ בזמן ליניארי: $\Theta(n)$.

<u>ייצוג פולינומים ע"י ערכו בנקודות שונות:</u>
משפט יחידות האינטרפולציה הפולינומית: בהינתן קבוצה של ערכים
$(x_0,y_0),(x_1,y_1),(x_2,y_2),...,(x_{n-1},y_{n-1})$ אז קיים פולינום יחיד מדרגה חסומה ע"י n, $A(x)$ כך ש: $A(x_i)=y_i$ לכל $i=0,1,...,n-1$.

ניתן לחשב את פולינום האינטרפולציה ע"י נוסחת לגרנז':
$$A(x)=\sum_{k=0}^{n-1}y_k\frac{\prod_{j\neq k}(x-x_j)}{\prod_{j\neq k}(x_k-x_j)}$$
בסיבוכיות $\Theta(n^2)$.

מסקנה: ניתן לייצג פולינום מדרגה חסומה ע"י n באמצעות ערכיו ב n נקודות שונות וישנם אינסוף ייצוגים כאלה.
היתרון של ייצוג זה: אם נתונים שני פולינומים $A(x),B(x)$, ע"י ערכיהם באותן n נקודות:
$$A(x):(x_0,y_0),(x_1,y_1),...,(x_{n-1},y_{n-1})$$
$$B(x):(x_0,y_{0'}),(x_1,y_{1'}),...,(x_{n-1},y_{n-1'})$$
$$C(x):(x_0,y_0\cdot y_{0'}),...$$

אז ניתן לחשב את ערכיו של $C(x)=A(x)\cdot B(x)$ באותן נקודות, ע"י: $C(x_i)=A(x_i)\cdot B(x_i)$ בזמן ליניארי.

<u>בעיה:</u> C מדרגה חסומה ע"י $2n$.

<u>הפתרון:</u> נייצג את A ואת B ע"י ערכיהם ב $2n$ נקודות.

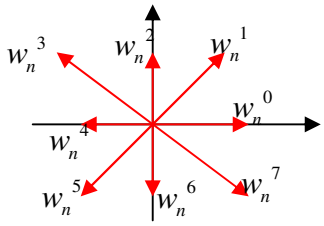
<u>תזכורת:</u>

מספר מרוכב w הוא שורש יחידה מסדר n אם $w^n=1$.

ישנם בדיוק n שורשי יחידה מרוכבים מסדר n: $e^{i\frac{2\pi k}{n}}$ $k=0,1,2,...,n-1$.

נוסחת אויילר: $e^{i\theta}=\cos\theta+i\sin\theta$

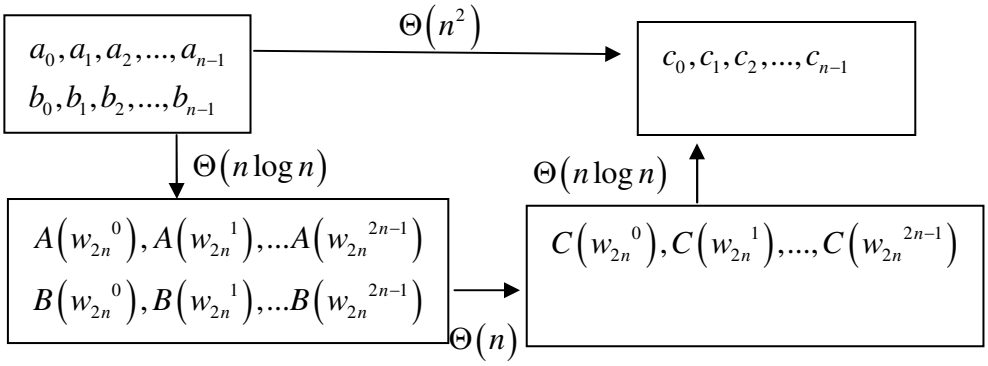
אם נסמן את שורש היחידה הראשי: $e^{i\frac{2\pi}{n}}$ ב w_n אזי שורשי היחידה הם: $w_n^{\,0},w_n^{\,1},w_n^{\,2},...,w_n^{\,n-1}$.



הרעיון הכללי של האלגוריתם:

1. נייצג את 2 הפולינומים ע"י ערכיהם ב $2n$ שורשי היחידה מסדר $2n$. המעבר נקרא התמרת פוריה הבדידה (DFT) וניתן למימוש ע"י אלגוריתם FFT בזמן $\Theta(n\log n)$ (במקום זמן ריבועי ע"י כלל *Honever*).
2. נכפיל את שני הפולינומים בייצוג החדש ונקבל ייצוג ע"י ערכיו ב $2n$ שורשי היחידה מסדר $2n$. $\Theta(n)$.
3. נעבור מייצוג של C ע"י וקטור מקדמיו. המעבר נקרא התמרת פוריה ההפוכה (DFT^{-1}) וממומש ע"י FFT (עם שינויים קלים) בזמן $\Theta(n\log n)$ (במקום בזמן ריבועי ע"י נוסחת לגרנז').

סכימה:



משפט הקונבולוציה:

עבור 2 וקטורים a,b באורך n (כך ש n חזקה של 2) מתקיים:

$$a\otimes b=DFT_{2n}^{-1}\left(DFT_{2n}(a)\cdot DTF_{2n}(b)\right)$$

תכונות של שורשי היחידה המרוכבים:

<u>למת הצמצום:</u> לכל $n \geq 0, k \geq 0, d > 0$ שלמים מתקיים: $w_{dn}^{\ dk} = w_n^k$.

הוכחה: $w_{dn}^{\ dk} = \left(e^{i\frac{2\pi}{dn}} \right)^{dk} = \left(e^{i\frac{2\pi}{n}} \right)^k = w_n^{\ k}$

<u>למת המחצית:</u> יהא $n > 0$ זוגי, אזי הריבועים של n שורשי היחידה מסדר n הם $\frac{n}{2}$ שורשי היחידה מסדר $\frac{n}{2}$.

הוכחה: $\left(w_n^{\ k} \right)^2 = \left(w_n^{\ 2k} \right) = \left(w_{2\frac{n}{2}}^{\ \ 2k} \right) = w_{\frac{n}{2}}^{\ k}$

$$\left(w_n^{\ k+\frac{n}{2}} \right)^2 = w_n^{\ 2k+n} = w_n^{\ 2k} \cdot \underbrace{w_n^{\ n}}_{=1} = w_n^{\ 2k}$$

מסקנה: כל שורש יחידה מסדר $\frac{n}{2}$: $w_{\frac{n}{2}}^{\ k}$ מתקבל מהעלאה בריבוע של 2 שורשי יחידה מסדר n: $w_n^{\ k}, w_n^{\ k+\frac{n}{2}}$.

<u>למת הסכום:</u> לכל $k > 0, n \geq 1$ כך ש k לא מתחלק ב n מתקיים: $\sum_{j=0}^{n-1} \left(w_n^{\ k} \right)^j = 0$

הוכחה: $\sum_{j=0}^{n-1} \left(w_n^{\ k} \right)^j = \frac{\left(w_n^{\ k} \right)^n - 1}{w_n^{\ k} - 1}$ (ע"פ נוסחת טור הנדסי)

$w_n^{\ i} \cdot w_n^{\ j} = w_n^{\ i+j} = w_n^{\ (i+j) \bmod n}$ שורשי היחידה מסדר n הם חבורה ביחס לכפל

$w_n^{\ n} = 1$

(דומה לחבורה: $(\mathbb{Z}_n, +\bmod n)$)

$$\frac{\left(w_n^{\ k} \right)^n - 1}{w_n^{\ k} - 1} = \frac{\left(w_n^{\ n} \right)^k - 1}{w_n^{\ k} - 1} = \frac{1^k - 1}{w_n^{\ k} - 1} = 0$$ (המכנה לא מתאפס כי k לא מתחלק ב n).

אנו מעוניינים לחשב את $A(x)$ ב n שורשי היחידה מסדר n:

$$k = 0,1,2,...n-1 \qquad y_k = A\left(w_n^{\ k} \right) = \sum_{j=0}^{n-1} a_j \cdot \left(w_n^{\ k} \right)^j$$

$y = (y_0, y_1, ..., y_{n-1})$ נקרא התמרת פוריה הבדידה (Discrete Fourie Transform) ומסומנת: $y = DFT(a)$, $a = (a_0, a_1, ...a_{n-1})$.

<u>FFT (Fast Fourie Transform)</u>

נחלק את $A(x)$ לחזקות זוגיות ואי זוגיות:

$$A(x) = a_0 + a_2 x^2 + a_4 x^4 + ... + a_{n-2} x^{n-2}$$
$$+ a_1 x + a_3 x^3 + a_5 x^5 + ... a_{n-1} x^{n-1}$$

נגדיר שני פולינומים מדרגה חסומה ע"י $\frac{n}{2}$:

$$A^{[0]}(x) = a_0 + a_2 x + a_4 x^2 + a_6 x^3 + ... + a_{n-2} x^{n/2-1}$$
$$A^{[1]}(x) = a_1 + a_3 x + a_5 x^2 + a_7 x^3 + ... + a_{n-1} x^{n/2-1}$$

נקבל: $A(x) = A^{[0]}(x^2) + x \cdot A^{[1]}(x^2)$. (נסמן מסקנה זו ב *).

אם חישבנו (רקורסיבית) את ערכי הפולינומים:

$A^{[0]}(x), A^{[1]}(x)$ בריבועי שורשי היחידה מסדר n: $(w_n^{\,0})^2, (w_n^{\,1})^2, ..., (w_n^{\,n-1})^2$ שהם בעצם $\frac{n}{2}$ שורשי היחידה מסדר $\frac{n}{2}$ וקיבלנו

$$y^{[0]} = \left(A^{[0]}(w_{n/2}^{\,0}), A^{[0]}(w_{n/2}^{\,1}), ..., A^{[0]}(w_{n/2}^{\,n/2-1}) \right)$$
$$y^{[1]} = \left(A^{[1]}(w_{n/2}^{\,0}), A^{[1]}(w_{n/2}^{\,1}), ..., A^{[1]}(w_{n/2}^{\,n/2-1}) \right)$$

עבור $k = 0,..,n-1$:

$$A(w_n^{\,k}) \overset{*}{=} A^{[0]}((w_n^{\,k})^2) + w_n^{\,k} \cdot A^{[1]}((w_n^{\,k})^2) = A^{[0]}(w_{n/2}^{\,k}) + w_n^{\,k} A^{[1]}(w_{n/2}^{\,k})$$

$$A(w_n^{\,k+n/2}) \overset{*}{=} A^{[0]}((w_n^{\,k+n/2})^2) + w_n^{\,k+n/2} \cdot A^{[1]}((w_n^{\,k+n/2})^2) = A^{[0]}(w_{n/2}^{\,k}) + w_n^{\,k+n/2} \cdot A^{[1]}(w_{n/2}^{\,k})$$
$$= A^{[0]}(w_{n/2}^{\,k}) - w_n^{\,k} \cdot A^{[1]}(w_{n/2}^{\,k})$$

$$\left(w_n^{\,n/2} = w_{n/2\cdot 2}^{\,n/2\cdot 1} = w_2 = -1 \right)$$

מסקנה: כדי לפתור את הבעיה מספיק לפתור 2 תת בעיות שגודלן מחצית מהבעיה המקורית (טכניקת הפרד ומשול).

(האלגוריתם הרקורסיבי לביצוע FFT נמצא באתר הקורס)

סיבוכיות: $\begin{cases} T(n) = 2T(n/2) + \Theta(n) \\ T(1) = O(1) \end{cases} \Rightarrow T(n) = \Theta(n \log n)$

$$\underbrace{\begin{pmatrix} 1 & 1 & 1 & ... & 1 \\ 1 & w_n & w_n^{\,2} & ... & w_n^{\,n-1} \\ 1 & w_n^{\,2} & (w_n^{\,2})^2 & ... & (w_n^{\,2})^{n-1} \\ \vdots & & & & \\ 1 & w_n^{\,n-1} & (w_n^{\,n-1})^2 & ... & (w_n^{\,n-1})^{n-1} \end{pmatrix}}_{V_n} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_{n-1} \end{pmatrix} : y = DTF(a)$$

ניתן לחשב את a ע"י $a = V_n^{-1} \cdot y$

טענה: $(V_n^{-1})_{j,k} = \frac{w_n^{\,-jk}}{n}$

הוכחה: נראה ש: $(V_n^{-1}) \cdot V_n = I$

$$\left(V_n^{-1}\cdot V_n\right)_{j'.j}=\sum_{k=0}^{n-1}\frac{w_n^{-jk}}{n}\cdot w_n^{kj'}=\frac{1}{n}\sum_{k=0}^{n-1}w_n^{k(j'-j)}$$

אם $j'=j$ אז התוצאה היא כמובן 1.

אחרת, אם $j'-j$ לא מתחלק ב n אז לפי למת הסכום, התוצאה היא 0.

כלומר: $a-V_n^{-1}\cdot y$

$$a_k=\sum_{j=0}^{n-1}\left(V_n^{-1}\right)_{kj}\cdot y_j=\frac{1}{n}\sum_{j=0}^{n-1}y_j\cdot w_n^{-jk}$$

$$y_k=\sum_{j=0}^{n-1}a_j\cdot\left(w_n^{\,k}\right)^j$$

זה כמו להעריך את הפולינום שמקדמיו $\frac{y_j}{n}$ ב n שורשי היחידה מסדר n:

$$\left(w_n^{-1}\right)^0,\left(w_n^{-1}\right)^1,...,\left(w_n^{-1}\right)^{n-1}$$

כלומר, השינויים שיש לבצע ב FFT הם:

1. לחלק את התוצאה ב n.
2. להחליף תפקידים בן a ו y.
3. להחליף w_n ב w_n^{-1}.