

התמרת פורייה המהירה FFTתזכורת:

אלגוריתם של Cooley – Tukey שנקרא Radix – 2 לחישוב DFT:

$$DFT = \begin{pmatrix} DFT(\text{זוגיים}) + e^{\frac{2\pi i x}{N}} \cdot DFT(\text{אי-זוגיים}) \\ DFT(\text{זוגיים}) - e^{\frac{2\pi i x}{N}} \cdot DFT(\text{אי-זוגיים}) \end{pmatrix}$$

תרגיל (תשע"ז מועד א'):

חשבו את ה- FFT של הסדרה הבאה 00001111.

פתרון:

$$F \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = F \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} e^{\frac{2\pi i \cdot 0}{8}} \\ e^{\frac{2\pi i \cdot 1}{8}} \\ e^{\frac{2\pi i \cdot 2}{8}} \\ e^{\frac{2\pi i \cdot 3}{8}} \end{pmatrix} \cdot F \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \\ F \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} - \begin{pmatrix} e^{\frac{2\pi i \cdot 4}{8}} \\ e^{\frac{2\pi i \cdot 5}{8}} \\ e^{\frac{2\pi i \cdot 6}{8}} \\ e^{\frac{2\pi i \cdot 7}{8}} \end{pmatrix} \cdot F \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

לכן נצטרך לחשב רק את:

$$F \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = F \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} e^{\frac{2\pi i \cdot 0}{4}} \\ e^{\frac{2\pi i \cdot 1}{4}} \end{pmatrix} \cdot F \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ F \begin{pmatrix} 0 \\ 1 \end{pmatrix} - \begin{pmatrix} e^{\frac{2\pi i \cdot 3}{4}} \\ e^{\frac{2\pi i \cdot 4}{4}} \end{pmatrix} \cdot F \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

ולכן נחשב רק את:

$$F \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} F(0) + F(1) \cdot e^{\frac{-2\pi i \cdot 0}{2}} \\ F(0) - F(1) \cdot e^{\frac{-2\pi i \cdot 1}{2}} \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

נחזור אחורה:

$$F \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix} + \begin{pmatrix} 1 \\ -i \end{pmatrix} \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix} \\ \begin{pmatrix} 1 \\ -1 \end{pmatrix} - \begin{pmatrix} 1 \\ -i \end{pmatrix} \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 2 \\ -1 + i \\ 0 \\ -1 - i \end{pmatrix}$$

נחזור עוד אחורה:

$$F \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ -1+i \\ 0 \\ -1-i \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}i \\ & -i \\ -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}i \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -1+i \\ 0 \\ -1-i \end{pmatrix} = \begin{pmatrix} 4 \\ -1+(1+\sqrt{2})i \\ 0 \\ -1+\sqrt{2}i \\ 0 \\ -1+(1-\sqrt{2})i \\ 0 \\ -1-(1+\sqrt{2})i \end{pmatrix}$$

$$\begin{pmatrix} 2 \\ -1+i \\ 0 \\ -1-i \end{pmatrix} - \begin{pmatrix} 1 & 1 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}i \\ & -i \\ -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}i \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -1+i \\ 0 \\ -1-i \end{pmatrix}$$

וסיימו.

■

הערה::Bit Reverse

אם נבצע היפוך של הביטים של האינדקסים שאנו עובדים איתם נשים לב כי זה יהיה שקול לסדר את האינדקסים כמו באלגוריתם של ה-FFT:

$$\begin{array}{l} 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{array} \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{pmatrix} \Rightarrow \begin{array}{l} 000 \\ 100 \\ 010 \\ 110 \\ 001 \\ 101 \\ 011 \\ 111 \end{array} \begin{pmatrix} 0 \\ 4 \\ 2 \\ 6 \\ 1 \\ 5 \\ 3 \\ 7 \end{pmatrix}$$

אינדקסים ייצוג ביטים אינדקסים ייצוג ביטים

הצפנה

הגדרה: יהיו a, b מספרים שלמים. נאמר כי a מחלק את b אם קיים $k \in \mathbb{Z}$ כך ש $b = ak$.

הגדרה (משפט החילוק): לכל $n \in \mathbb{Z}, d \neq 0$ קיימים q, r יחידים כך ש $n = q \cdot d + r$ כאשר $0 \leq r < |d|$.

הגדרה: בהינתן שני מספרים שלמים m, n , החלק המשותף המקסימלי (gcd) מוגדר להיות:

$$gcd(m, n) = \max\{d \in \mathbb{N} : d|n \wedge d|m\}$$

סימון: $gcd(m, n) = (m, n)$.

טענה: אם $n = q \cdot m + r$ אזי:

$$(n, m) = (m, r)$$

משפט (אלגוריתם אוקלידס): המתכון למציאת מחלק משותף מינימלי הוא שימוש חוזר בטענה הקודמת.

דוגמה:

נחשב את $gcd(m, n)$.

$$(224, 63) = [224 = 3 \cdot 63 + 35]$$

$$(63, 35) = [63 = 35 + 28]$$

$$(35, 28) = [28 + 7]$$

$$(28, 7) = 7$$

וסיימו.

■

משפט (אפיון ממ"מ): מתקיים לכל שני מספרים שלמים a, b :

$$(a, b) = \min\{au + bv \in \mathbb{N} | u, v \in \mathbb{Z}\}$$

בפרט, קיימים $s, t \in \mathbb{Z}$ כך ש:

$$(a, b) = a \cdot s + b \cdot t$$

דוגמה:

עבור הדוגמה הקודמת:

$$\begin{aligned} \boxed{7} &= 35 - 28 = 35 - (63 - 35) = 224 - 3 \cdot 63 - (63 - 224 + 3 \cdot 63) \\ &= \boxed{2 \cdot 224 - 7 \cdot 63} \end{aligned}$$

הגדרה (חבורה): חבורה G היא מבנה אלגברי בסיסי עם הפעולה בינארית סגורה ומתקיים:

1. אסוציאטיבית.
2. קיום יחידה.
3. קיום הופכי לכל איבר ב G .

 \Leftarrow מהאקסיומות נובע שיש איבר יחידה יחיד ולכל מספר הופכי יחיד.
הגדרה (חבורת אוילר): המספרים שהם ההופכי בחבורה \mathbb{Z}_n :

$$U_n = U(\mathbb{Z}_n)$$

הערה:עבור \mathbb{Z}_p^* (החבורה ללא אפס) כאשר p ראשוני:

$$U_p = \mathbb{Z}_p^*$$

משפט אוילר: פונקציית אוילר $\varphi: \mathbb{N} \rightarrow \mathbb{N}$ מוגדרת להיות $\varphi(n) = |U_n|$.משפט: עבור כל $a \in U_n$ מתקיים: $a^{\varphi(n)} \equiv 1 \pmod{n}$.משפט פרמה הקטן: מקרה פרטי של אוילר עבור p ראשוני:

$$a^{p-1} \equiv 1 \pmod{p}$$

תרגיל:חשב את שתי הספרות האחרונות של 909^{121} .פתרון:

נרצה לעשות מודולו 100.

$$909 \equiv 9^{121} \pmod{100}$$

$$9^{\varphi(100)} = 9^{40} \equiv 1 \pmod{100}$$

ולכן:

$$9^{121} = (9^{40})^3 \cdot 9 \equiv 1^3 \cdot 9 \pmod{100} = 9 \pmod{100}$$

ולכן שתי הספרות האחרונות הן 09.

■

הצפנת RSA:

הצפנה א – סימטרית. ההצפנה היא ציבורית, פענוח פרטי.

דוגמה:

בוב ← אליס.

אליס: בוחרת שני ראשונים (בדרך כלל ניקח גדולים) p, q .

נסמן: $n = p \cdot q$. נחשב את $\varphi(n) = (p-1)(q-1)$. לאחר מכן אליס בוחרת מספר e שזר ל- $\varphi(n)$ (בדרך כלל בוחרת $e = 2^{10} + 1$). נקרא מעריך חזקה.

לאחר מכן, אליס מוצאת מספר 1 כך ש- $e \cdot d = 1 \pmod{\varphi(n)}$.

את e, n אליס שולחת לבוב (בדרך בטוחה אבל לא מוצפנת). את d היא שומרת לעצמה (d הוא הסוד).

בוב שולח הודעה M בעזרת מספר m כך ש:

$$0 \leq m < n$$

וגם:

$$\gcd(m, n) = 1$$

בוב שולח את ההודעה הבאה:

$$c = m^e \pmod{n}$$

(שולח את c).

כדי לפענח, אליס מעלה את c בחזקת d :

$$c^d = m^{ed} = m^1 \pmod{n}$$

למה ed נתון לנו 1?

$$ed = 1 \pmod{\varphi(n)}$$

$$ed = 1 + k \cdot \varphi(n)$$

$$m^{ed} \pmod{n} = m^{1+k\varphi(n)} \pmod{n} = m \cdot m^{k\varphi(n)} = m \pmod{n}$$

דוגמה:

אליס בוחרת שני מספרים ראשוניים (גדולים) p, q .

$$q = 53, p = 61$$

$$n = p \cdot q = 3233$$

$$\varphi(n) = 60 \cdot 52 = 3120$$

כעת, אליס בוחרת e שזר ל- $\varphi(n)$. נבחר $e = 17$.

אליס צריכה את d :

$$ed = 1 \pmod{\varphi(n)}$$

נחשב את $\gcd(3120, 17)$.

הסבר: קיימים t, s כך ש -

$$(a, b) = a \cdot s + b \cdot t$$

אם a, b זרים, אזי $(a, b) = 1$ ומתקיים:

$$1 = a \cdot s + b \cdot t$$

אם אני נמצא מעל \pmod{a} אזי:

$$1 = b \cdot t$$

אם אני מוצא את t , אני מוצא את ההופכי של e .

אז נחשב את ה- $\gcd(3120, 17)$:

$$(3120, 17) = 183 \cdot 17 + 9$$

↓

$$(17, 9) = 1 \cdot 9 + 8$$

↓

$$(9, 8) = 1$$

נחזור אחורה:

$$\begin{aligned} 1 &= 9 - 8 = 9 - (17 - 9) = 2 \cdot 9 - 17 = 2 \cdot (3120 - 183 \cdot 17) \\ &= 2 \cdot 3120 - 367 \cdot 17 \end{aligned}$$

אם נעשה לזה $\pmod{\varphi(n)}$ אז נקבל ש:

$$1 = -367 \cdot 17$$

נוסיף 3120 ל - 367 ונקבל:

$$d = 2753 \bmod(\varphi(n))$$

אליס שולחת לבוב את $e - n$. בוב שולח הודעה $m = 65$.

$$c = m^e \bmod(n)$$

אזי בוב שולח $65^{17} \bmod(n)$.

חזקה מודולרית:

אנחנו בכל פעם נעלה בחזקת 2 וכך נצמצם.

למשל, עבור x^{41} נחשב לפי:

$$41 = 2^5 + 2^3 + 1$$

$$((((x^2)^2)^2)^2)^2 \cdot ((x^2)^2)^2 \cdot x$$

אצלנו, נחשב את 65^{17} :

$$65^2 = 992 \bmod(3233)$$

$$65^4 = (65^2)^2 = (992)^2 \bmod(3233) = 1232 \bmod(3233)$$

$$65^8 = (65^4)^2 = (1232)^2 \bmod(3233) = 1547 \bmod(3233)$$

$$65^{16} = (65^8)^2 = (1547)^2 \bmod(3233) = 789 \bmod(3233)$$

$$\boxed{65^{17}} = 65^{16} \cdot 65 = \boxed{2790 \bmod(3233)}$$

בוב שולח את:

$$c = 2790 \bmod(3233)$$

ואליס תמצא את ההודעה עם $d = 2753$:

$$2790^{2753} \bmod(3233) = 65^{17 \cdot 2753} \bmod(3233) = 65 \bmod(3233)$$

אלגוריתם Simplexדוגמה:

$$f(x) = 3x_1 + 2x_2 + 4x_3$$

תחת האילוצים:

$$\forall 1 \leq i \leq 3 : x_i \geq 0$$

$$x_1 + x_2 \leq 5$$

$$x_1 - 2x_3 \leq 10$$

רוצים למצוא את המקסימום. אבל בגלל הגורם השלילי של x_3 באילוץ האחרון, הבעיה לא חסומה.

אם נחליף את האילוצים ל:

$$\forall 1 \leq i \leq 3 : x_i \geq 0$$

$$x_1 + x_2 \leq -10$$

$$x_1 + 2x_3 \leq 10$$

נקבל שלבעיה אין פתרון.

נפתור את הבעיה הבאה:

$$f(x) = 3x_1 + 2x_2 + 4x_3$$

$$\forall 1 \leq i \leq 3 : x_i \geq 0$$

$$x_1 + x_2 \leq 5$$

$$x_1 - 2x_3 \leq 10$$

בשביל להימנע מאי שוויונים, נוסיף משקלים w_1, w_2 :

$$\begin{cases} w_1 = 5 - x_1 - x_2 \\ w_2 = 8 - x_1 - 2x_3 \end{cases}$$

ונקבל:

$$\begin{cases} x_1 + x_2 + w_1 = 5 \\ x_1 + 2x_3 + w_2 = 8 \end{cases}$$

נתחיל מ- $w_1, w_2 \neq 0$ ו- $x = 0$. ננסה להגדיל את x_3 (לו יש את המקדם הגדול ביותר).

נראה את x_3 באמצעות האחרים:

$$x_3 = \frac{8 - w_2 - x_1}{2}$$

לקן:

$$f(x) = 3x_1 + 2x_2 + 4 \left[\frac{8 - w_2 - x_1}{2} \right] = x_1 + x_2 + 0 \cdot x_3 + 0 \cdot w_1 - 2w_2 + 14$$

והאילוצים שלנו הם:

$$x_1 + 2x_2 + 0 \cdot x_3 + w_1 + 0 \cdot w_2 = 5$$

$$\frac{1}{2}x_1 - 0 \cdot x_2 + x_3 + \frac{w_2}{2} = 4$$

נסתכל כעת על $x_2 = 5 - x_1 - w_1$

$$f(x) = -x_1 + 2[5 - x_1 - w_1] - 2w_2 + 16 = -x_1 + 0 \cdot x_2 - 2w_1 - 2w_2 + 26$$

וכעת, לא נרצה להגדיל את x_1 כיה הוא עם סימן שלילי. לכן נעצור והגענו לזה שהמקסימום שלנו הוא 26. הנקודה שלנו היא (0,5,4).

דוגמה:

פונקציית מטרה:

$$\max z = 3x_1 + 5x_2$$

האילוצים הם:

$$x_1 \leq 4$$

$$2x_2 \leq 12$$

$$3x_1 + 2x_2 \leq 18$$

$$\forall j : x_j \geq 0$$

הבעיה היא:

$$\max z = 3x_1 + 5x_2$$

$$z - 3x_1 - 5x_2 = 0$$

האילוצים הם:

$$x_1 + x_3 = 4$$

$$x_2 + x_4 = 6$$

$$3x_1 + 2x_2 + x_5 = 18$$

$$\forall j : x_j \geq 0$$

ניצור טבלה:

משתני בסיס נוכחיים	z	x_1	x_2	x_3	x_4	x_5	אגף ימין
z	1	-3	-5	0	0	0	0
x_3	0	1	0	1	0	0	4
x_4	0	0	1	0	1	0	6
x_5	0	3	2	0	0	1	18

(משתני הבסיס הם אלו שבעמודה שלהם יש רק אחד במקום יחיד והשאר אפסים).

אם נסתכל על היחס בכל שורה (חוץ מהראשונה) נקבל שהיחס הכי קטן (בשורה השלישית) הוא $\frac{6}{1} = 6$. לוקחים יחס שהוא הערך באגף ימין חלקי הערך בעמודה שבחרנו. נשים לב שבמקום שבו יש לנו יחס של מספר חלקי 0, אז אין לנו הגבלה.

נרצה לבצע עדכון של שורות ולאפס את הערכים בעמודה של x_2 (שאותו בחרנו) חוץ מהשורה עם היחס הכי מינימלי.

לכן נבצע:

$$5R_3 + R_1 \rightarrow R_1$$

$$-2R_3 + R_4 \rightarrow R_5$$

קיבלנו טבלה חדשה:

משתני בסיס נוכחיים	z	x_1	x_2	x_3	x_4	x_5	אגף ימין
z	1	-3	0	0	5	0	30
x_3	0	1	0	1	0	0	4
x_2	0	0	1	0	1	0	6
x_5	0	3	0	0	-2	1	6

נמשיך באותו אופן:

היחס המינימלי כעת הוא בשורה הרביעית שהוא $\frac{6}{3} = 2$. לכן נרצה לאפס את הערכים

בעמודה ולכן נבצע:

$$R_4 + R_1 \rightarrow R_1$$

$$-\frac{1}{3}R_4 + R_2 \rightarrow R_2$$

$$\frac{1}{3}R_4 \rightarrow \frac{1}{3}R_4$$

נקבל טבלה חדשה:

משתני בסיס נוכחיים	z	x_1	x_2	x_3	x_4	x_5	אגף ימין
z	1	0	0	0	-3	1	36
x_3	0	0	0	1	$\frac{2}{3}$	$-\frac{1}{3}$	2
x_2	0	0	1	0	1	0	6
x_1	0	1	0	0	$-\frac{2}{3}$	$\frac{1}{3}$	2

קיבלנו שהמקסימום מתקבל עבור $z = 36$ וזה קורה בנקודה ש - (2,6).

הערה:

הסימפלקס צריך להתחיל מפתרון אפשרי. נשים לב שאנו מניחים כי הנקודה (0,0) יכולה להיות פתרון למשוואה שלנו. אם זה לא המצב, אז נעבור למצב הדואלי.

תמונה...

מה שפתרנו עכשיו זאת הבעיה הפרמלית.

דוגמה:

$$\max(2x_1 + 3x_2 + 4x_3)$$

$$\forall j : x_j \geq 0$$

$$x_1 + 2x_2 + x_3 \leq 8$$

$$x_1 + 2x_3 \leq 10$$

נעבור לבעיה הדואלית:

$$\max(-8y_1 - 12y_2)$$

$$-y_1 - y_2 \leq -2$$

$$-2y_1 \leq -3$$

$$-y_1 - 2y_2 \leq -4$$

הערה:**בבעיה הפרמלית (1):**

$$\max(c^t x)$$

$$S.T : a_j^t x \leq b_j$$

בבעיה הדואלית (2):

$$c \rightarrow -b$$

$$b \rightarrow -c$$

$$a^t \rightarrow -a$$

משפט הדואליות החלש: עבור בעיה פרמלית:

$$\max z = cx$$

ככה ש:

$$Ax \leq b$$

$$x \geq 0$$

והבעיה הדואלית לה:

$$\min w = yb$$

ככה ש:

$$yA \geq c$$

$$y \geq 0$$

אם x פתרון אפשרי ל- (1) ו- y פתרון אפשרי ל- (2), אזי:

$$cx \leq yb$$

כלומר, כל פתרון אפשרי של בעיית מקסימום מהווה חסם תחתון לבעיית מינימום.

משפט הדואליות החזק: אם x פתרון ל- (1) ו- y פתרון ל- (2) כך שמתקיים $cx = yb$, אזי x אופטימלי ל- (1) ואופטימלי ל- (2).

הערה:

משוואה מקורית	משוואה דואלית
אילוץ 1 פעיל	$y_1 \neq 0$
אילוץ 2 לא פעיל	$y_2 = 0$
$x_1 = 0$	$w_1 = 0$
$x_2 \neq 0$	$w_2 \neq 0$
$x_3 = 0$	$w_3 = 0$