

מחברים: מרצה דבסון נ שוחט ו מ סמואל נקמת מלמד אביה זקנים

$$T = \begin{bmatrix} t_0 & t_1 & t_2 & \dots & t_{m-1} \\ t_{-1} & t_0 & t_1 & \dots & \vdots \\ t_{-2} & t_{-1} & t_0 & t_1 & \vdots \\ \vdots & \vdots & & \ddots & \\ t_{1-n} & t_{2-m} & \dots & \dots & t_{m-n} \end{bmatrix}$$

- חיבוי של ארביצות טופל ויתן ארביצת טופל
- לא כל הסתכלות

הקונדאציה היא וקטור $h \in \mathbb{R}^n$, $x \in \mathbb{R}^m$ ו- $z = x \otimes h$ היא תוצאה

מ"פאת הוקטור ז לפי:

משפט: שטחית הקונגלוגיה פילמנרית.

שאלות ותשובות בנושא אמנות:

(1) הנח את וקטור x ביצירה $u \cdot x$

$$\dots \quad \boxed{0 \quad 0 \quad 0 \quad \pi_0 \quad \pi_1 \quad \pi_2 \quad \pi_3 \quad \pi_4 \quad \pi_5 \quad \pi_6 \quad \pi_7 \quad \pi_8 \quad \pi_9 \quad 0 \quad 0} \quad \dots$$

$$\boxed{h_3 \quad h_2 \quad h_1 \quad h_0}$$

$$\downarrow$$

$$z_0$$

פונקציה קריפטוגרפית

(2) $\frac{d}{dt} h$ הוא קצב

חשב מכללי: טעמית בין איברי x ואיברי h חוקם (יתרון)

אסמך ב ממשלות חלה - מה ייתן הערך .70

(3) כעת, נסתכל על H וננסה להבין מה זה H ומה זה H^* .

K א פמ נמל , פמל מלמל מלמל מלמל מלמל

זכר ו' / זכר

!@ \$%&' () * + , - . / : ;

הכיתה (מ) חציף: $\underline{z} = \lambda \cdot \underline{h} = H \cdot \underline{x}$

banded \Rightarrow in H. s.c. $h \sim \pi$ h_3, h_2, h_1, h_0 \Rightarrow large ω (i) ω (ii) ω (iii) ω

מרחב וקטורי

המשפט - מרחב וקטורי C המוגדר על ידי n וקטורים c_0, \dots, c_{n-1} הוא מרחב וקטורי אם ורק אם c_0, \dots, c_{n-1} הם בסיס.

$$t_{i,j} = t_{(j-i) \bmod n}$$

$$(j-i) \bmod n = \begin{cases} n+j-i & j-i < 0 \\ j-i & 0 \leq j-i < n \end{cases}$$

$$C = \begin{bmatrix} c_0 & c_{n-1} & \dots & c_2 & c_1 \\ c_1 & c_0 & c_{n-1} & \dots & c_2 \\ \vdots & c_1 & c_0 & \dots & \vdots \\ c_{n-2} & \dots & \dots & \dots & c_{n-1} \\ c_{n-1} & c_{n-2} & \dots & c_1 & c_0 \end{bmatrix}$$

כל n סיבובים הוא טרנספורמציה, אך לא להפוך.
 אפשר לחשוב אותה כמטריצה הנשמרת.

הקונולוציה

המשפט: קונולוציה סיבובית (ציקלית) בין שני וקטורי שוני אורך $h, x \in \mathbb{R}^n$

$$z_k = \sum_{j=0}^{n-1} x_{(k-j) \bmod n} \cdot h_j$$

 $z = \pi \circ h$, מייצג את z לפי h .
 $0 \leq k-j \leq n-1$ הוא המרחב כמו הקונולוציה הליניארית.
 האזור $k-j$ שלט מרחבים:
 הקונולוציה הליניארית נשמרת אפסים.

המקרה הפרט נניח $n=1$ מרחב \mathbb{R} , $x_k = x$, $h_k = h$.
 מרחבים $[0, n]$

משפט: וקטור התוצאה בהקונולוציה ציקלית מרחבי n , צהיי $z_{k+n} = z_k$ לכל k שלם.

לכנס מרחביות סיבובית

משפט: כל המרחביות הסיבוביות המוגדרות על ידי n וקטורים c_0, \dots, c_{n-1} הם מרחביות סיבוביות.
 אותם וקטורים c_0, \dots, c_{n-1} , אשר מרחבים הם אותם וקטורים.

משפט: אם A ו- B מרחביות סיבוביות, אזי $A \cdot B = B \cdot A$.

אפשר לחשוב על A ו- B כמרחביות סיבוביות. \checkmark

$$\begin{matrix} x & \xrightarrow{\quad} & x \otimes h & \xrightarrow{\quad} & [x \otimes h] \otimes f \\ h & \xrightarrow{\quad} & f & \xrightarrow{\quad} & f \end{matrix}$$

$$F(xh) = x(Fh) = H(xf) = \dots$$

משפט: נניח A הוא מרחב סיבובי של המרחב A של וקטור v תחת A , $Av = \lambda v$.
 $\rho(A)$ (תחום הערכים) של A הוא λ . $\rho(A)$ הוא λ .
 $Av = \lambda v \Rightarrow \rho(A)v = \lambda v$ לכל v .
 $\rho(A) = \lambda$ לכל v .

$B = -3I + 7\lambda + 3A^5$ ממ"ק $B \in \mathbb{R}$ ממ"ק $A \in \mathbb{R}$ ממ"ק λ
 $\lambda_B = 3 + 7\lambda_A + 3\lambda_A^5$ ממ"ק $A - \lambda$ ממ"ק λ

(באמצעות) C_1 ממ"ק C_1 ממ"ק C_1

$$C_1 v = \begin{bmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & \dots & 0 \end{bmatrix} \begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \\ \vdots \\ v_{n-1} \end{bmatrix} = \alpha \begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \\ \vdots \\ v_{n-1} \end{bmatrix}$$

\rightarrow

$$\begin{aligned} v_1 &= \alpha v_0 \\ v_2 &= \alpha v_1 \\ v_3 &= \alpha v_2 \\ v_4 &= \alpha v_3 \\ &\vdots \\ v_{n-1} &= \alpha v_{n-2} \\ v_0 &= \alpha v_{n-1} \end{aligned}$$

C_1 ממ"ק C_1 ממ"ק C_1

$v_0 = 1$ ממ"ק $v_0 = 1$

$\alpha^n = 1$

n ממ"ק n

$\alpha = \exp\left\{ \frac{j 2\pi \ell}{n} \right\} \quad (j = \sqrt{-1})$

for $\ell = 0, 1, 2, \dots, n-1$ ממ"ק C_1 ממ"ק C_1

$\alpha = \omega_n^{-\ell}$ ממ"ק $\alpha = \omega_n^{-\ell}$

$\omega_n = \exp\left\{ \frac{j 2\pi}{n} \right\}$ ממ"ק $\omega_n = \exp\left\{ \frac{j 2\pi}{n} \right\}$

$C_1^2 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} = C_2$

$C = \sum_{k=0}^{n-1} C_k C_1^k$ ממ"ק $C = \sum_{k=0}^{n-1} C_k C_1^k$

$\lambda_\ell = \sum_{k=0}^{n-1} C_k \alpha_\ell^k = \sum_{k=0}^{n-1} C_k \omega_n^{-k\ell}$ ממ"ק $\lambda_\ell = \sum_{k=0}^{n-1} C_k \omega_n^{-k\ell}$

for $\ell = 0, 1, 2, \dots, n-1$

$$\underline{v}_k = \begin{bmatrix} w_n^{-0k} \\ w_n^{-1k} \\ w_n^{-2k} \\ w_n^{-3k} \\ \vdots \\ w_n^{-(n-1)k} \end{bmatrix}$$

$\underline{v}_k^H \cdot \underline{v}_l$

$\underline{v}_k^H \cdot \underline{v}_l$

$\underline{v}_k^H \cdot \underline{v}_l$

$\underline{v}_k^H \cdot \underline{v}_l$

$$W = \frac{1}{\sqrt{n}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & w_n^{-1} & w_n^{-2} & w_n^{-3} & w_n^{-4} & \dots & w_n^{-(n-1)} \\ 1 & w_n^{-2} & w_n^{-4} & w_n^{-6} & w_n^{-8} & \dots & w_n^{-2(n-1)} \\ 1 & w_n^{-3} & w_n^{-6} & w_n^{-9} & w_n^{-12} & \dots & w_n^{-3(n-1)} \\ 1 & w_n^{-4} & w_n^{-8} & w_n^{-12} & w_n^{-16} & \dots & w_n^{-4(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w_n^{-(n-1)} & w_n^{-2(n-1)} & w_n^{-3(n-1)} & w_n^{-4(n-1)} & \dots & w_n^{-(n-1)^2} \end{bmatrix}$$

$\underline{v}_k^H \cdot \underline{v}_l$

$$w_n^{-\ell} = \exp\left\{-j2\pi \frac{\ell}{n}\right\} \rightarrow \overline{w_n^{-\ell}} = \exp\left\{+j2\pi \frac{\ell}{n}\right\}$$

הקומפליקס הריבוע של w שזה: $w^{-1} = w^H = \overline{w}$
 אולי סימטריה בין נשאר נשאר
 צמוד לנגזרת

$$W^{-1} = \frac{1}{\sqrt{n}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & w_n^1 & w_n^2 & w_n^3 & w_n^4 & \dots & w_n^{(n-1)} \\ 1 & w_n^2 & w_n^4 & w_n^6 & w_n^8 & \dots & w_n^{2(n-1)} \\ 1 & w_n^3 & w_n^6 & w_n^9 & w_n^{12} & \dots & w_n^{3(n-1)} \\ 1 & w_n^4 & w_n^8 & w_n^{12} & w_n^{16} & \dots & w_n^{4(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w_n^{(n-1)} & w_n^{2(n-1)} & w_n^{3(n-1)} & w_n^{4(n-1)} & \dots & w_n^{(n-1)^2} \end{bmatrix}$$

סמן מתקיים שזה n וזה אולי סימטריה של זה

$$\begin{bmatrix} \lambda_0 \\ \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ \lambda_4 \\ \vdots \\ \lambda_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & w_n^{-1} & w_n^{-2} & w_n^{-3} & w_n^{-4} & \dots & w_n^{-(n-1)} \\ 1 & w_n^{-2} & w_n^{-4} & w_n^{-6} & w_n^{-8} & \dots & w_n^{-2(n-1)} \\ 1 & w_n^{-3} & w_n^{-6} & w_n^{-9} & w_n^{-12} & \dots & w_n^{-3(n-1)} \\ 1 & w_n^{-4} & w_n^{-8} & w_n^{-12} & w_n^{-16} & \dots & w_n^{-4(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w_n^{-(n-1)} & w_n^{-2(n-1)} & w_n^{-3(n-1)} & w_n^{-4(n-1)} & \dots & w_n^{-(n-1)^2} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ \vdots \\ c_{n-1} \end{bmatrix} = \sqrt{n} W \underline{c}$$

התמרת הפורייה:

הפירמה: (מאנל) w נקראת מניצת השורה, והנכסיה היוקטיו c נקראת התמרת השורה
 הפוריית (DFT), המונחה וקטור תוצאה d זה אותו אורך n .

$$\left\{ d_\ell = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} c_k w_n^{-\ell k} \right\}_{\ell=0}^{n-1} \rightarrow d = W \cdot c$$

לזמן, חישו שזה של w סימטריה c (זה כפ. קצת) הוסיף (התמרת השורה הפוריית)
 זה אינני שכתה (הנאשקה!)

משפט: בהינתן שני וקטורים a ו- b באורך n , מתקיים:

$$DFT \{a\} \cdot DFT \{b\} = DFT \{a \otimes b\} \rightarrow a \otimes b = DFT^{-1} \{DFT \{a\} \cdot DFT \{b\}\}$$

לזמן, כתלם לחישוב קונבולוציה סימטריה בין שני וקטורים אלה, ניתן לבצע 2 התמרות DFT, אחת זה w וקטור, להכפיל את התוצאות אינני אינני וזה לבצע התמרת DFT (נשכח).