

Глава 6

Теоретико-числови преобразования

6.1 Дискретно преобразование на Фурие.

Дефиниция 6.1.1 Нека $X = \{x_n\}$ и $Y = \{y_n\}$ са две редици от комплексни числа. **Взаимна корелация** на редиците X и Y наричаме редицата $\mathcal{R}_{XY} = \{\rho_t\}_{t=0}^\infty$, където

$$\rho_t = \mathcal{R}_{XY}(t) \stackrel{\text{def}}{=} \sum_{n=-\infty}^{\infty} x_n \bar{y}_{n+t}, \quad (6.1)$$

където с \bar{z} означаваме комплексно спрегнатото на $z \in \mathbb{C}$.

Взаимната корелация на X със себе си се нарича **автокорелация** на X и бележим

$$\mathcal{R}_X(t) \stackrel{\text{def}}{=} \mathcal{R}_{XX}(t) = \sum_{n=-\infty}^{\infty} x_n \bar{x}_{n+t} \quad (6.2)$$

Очевидно, че ако X е периодична с период N (т.е. $x_j = x_{j+N}$ за всяко j), то и автокорелационната редица \mathcal{R}_X е периодична с период N .

Нека ξ е N -ти примитивен корен на единицата, т.е.

$$\xi = e^{-\frac{2\pi i}{N}} = \cos\left(\frac{2\pi}{N}\right) + i \sin\left(\frac{2\pi}{N}\right),$$

където $i = \sqrt{-1}$ е имагинерната единица.

Дефиниция 6.1.2 Дискретно преобразование на Фурие (DFT) на редицата $X = \{x_n\}$ с период N наричаме преобразуването $\mathcal{F}(X) = \{X_k\}_{k=0}^{N-1}$, където

$$X_k \stackrel{\text{def}}{=} \sum_{n=0}^{N-1} x_n \xi^{nk}. \quad (6.3)$$

Очевидно редицата $\{X_n\}$ е също с период N и се нарича **спектрална редица** или просто (*фуриеров*) **спектр** на $\{x_n\}$.

Лема 6.1.3 *Обратното преобразование на Фурие се задава с формулата*

$$x_k = \frac{1}{N} \sum_{j=0}^{N-1} X_j \xi^{-jk}, \quad (6.4)$$

а връзката между DFT и автокорелацията с

$$|X_k|^2 = \sum_{t=0}^{N-1} \mathcal{R}_X(t) \xi^{-kt}. \quad (6.5)$$

Доказателство. Замествайки X_j определено от (6.3) в дясната страна на (6.4) получаваме

$$\begin{aligned} \frac{1}{N} \sum_{j=0}^{N-1} X_j \xi^{-jk} &= \frac{1}{N} \sum_{j=0}^{N-1} \left(\sum_{n=0}^{N-1} x_n \xi^{nj} \right) \xi^{-jk} = \frac{1}{N} \sum_{j=0}^{N-1} \sum_{n=0}^{N-1} x_n \xi^{(n-k)j} \\ &= \frac{1}{N} \sum_{n=0}^{N-1} \left(x_n \sum_{j=0}^{N-1} (\xi^{n-k})^j \right) = \frac{1}{N} x_k N = x_k, \end{aligned}$$

тъй като

$$\sum_{j=0}^{N-1} (\xi^{n-k})^j = \begin{cases} 0, & \text{за } n-k \neq 0, \\ N, & \text{за } n-k = 0. \end{cases}$$

За редицата от квадратите от модулите $\{|X_k|^2\}$ е изпълнено:

$$\begin{aligned} |X_k|^2 &= X_k \bar{X}_k = \left(\sum_{n=0}^{N-1} x_n \xi^{nk} \right) \left(\sum_{n=0}^{N-1} \bar{x}_n \bar{\xi}^{nk} \right) = \sum_{t=0}^{N-1} \left(\sum_{n=0}^{N-1} x_n \bar{x}_{n+t} \xi^{nk} \bar{\xi}^{(n+t)k} \right) \\ &= \sum_{t=0}^{N-1} \xi^{-kt} \left(\sum_{n=0}^{N-1} x_n \bar{x}_{n+t} \right) = \sum_{t=0}^{N-1} \mathcal{R}_X(t) \xi^{-kt}, \end{aligned}$$

тъй като $\bar{\xi} = \xi^{-1}$.

Дефиниция 6.1.4 *Нека $X = \{x_n\}$ и $Y = \{y_n\}$ са две редици. Под **конволюция** на двете редици разбираме редицата*

$$C = X * Y \stackrel{\text{def}}{=} \{x_n y_n\}.$$

Дефиниция 6.1.5 *Нека $X = \{x_n\}$ и $Y = \{y_n\}$ са две редици с период N . Под **произведение** на двете редици разбираме редицата $C = X \circ Y = \{c_n\}$ с общ член*

$$c_n \stackrel{\text{def}}{=} \sum_{j=0}^{N-1} x_j y_{[n-j]}, \quad (6.6)$$

където $[a]$ означава остатък на a по модул N .

С всяка редица $X = \{x_n\}$ с дължина N по естествен начин можем да свържем полином $X(z) = x_0 + x_1z + \dots + x_{N-1}z^{N-1}$, с което получаваме взаимно-еднозначно съответствие между редиците с дължина N и полиномите от степен ненадминаваща $N - 1$.

Упражнение 6.1.1 Покажете, че ако $C = X \circ Y = \{c_n\}$, то

$$C(z) \equiv X(z)Y(z) \pmod{z^N - 1}.$$

Теорема 6.1.6 Ако $X = \{x_n\}$ и $Y = \{y_n\}$ са две редици с период N , то

$$\mathcal{F}(X) * \mathcal{F}(Y) = \mathcal{F}(X \circ Y) \quad (6.7)$$

и

$$\mathcal{F}(X) \circ \mathcal{F}(Y) = \frac{1}{N} \mathcal{F}(X * Y). \quad (6.8)$$

Доказателство.

$$\begin{aligned} X_n Y_n &= \left(\sum_{k=0}^{N-1} x_k \xi^{nk} \right) \left(\sum_{l=0}^{N-1} y_l \xi^{nl} \right) = \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} x_k y_l \xi^{(k+l)n} \\ &= \sum_{s=0}^{N-1} \left(\sum_{j=0}^{N-1} x_j y_{[s-j]} \right) \xi^{sn} = \sum_{s=0}^{N-1} c_s \xi^{sn} = \mathcal{F}(\{x_n\} \circ \{y_n\}) \end{aligned}$$

Тъй като $jk + l[n-k] \equiv ln + (j-l)k \pmod{N}$, то за n -тият член на редицата $\mathcal{F}(X) \circ \mathcal{F}(Y)$ е изпълнено

$$\begin{aligned} \sum_{k=0}^{N-1} X_k Y_{[n-k]} &= \sum_{k=0}^{N-1} \left(\sum_{j=0}^{N-1} x_j \xi^{jk} \right) \left(\sum_{l=0}^{N-1} y_l \xi^{l[n-k]} \right) = \sum_{k=0}^{N-1} \left(\sum_{j=0}^{N-1} \sum_{l=0}^{N-1} x_j y_l \xi^{(j-l)k + ln} \right) \\ &= \sum_{j=0}^{N-1} \sum_{l=0}^{N-1} \left(x_j y_l \xi^{ln} \sum_{k=0}^{N-1} \xi^{(j-l)k} \right) = \sum_{l=0}^{N-1} x_l y_l \xi^{ln} N = N D_n, \end{aligned}$$

където D_n е n -тия член на $\mathcal{F}(\{x_n\} * \{y_n\})$.

Упражнение 6.1.2 Покажете, че

$$\mathcal{F}^{-1}(X) \circ \mathcal{F}^{-1}(Y) = \mathcal{F}^{-1}(X * Y) \quad \text{и} \quad \mathcal{F}^{-1}(X) * \mathcal{F}^{-1}(Y) = N \mathcal{F}^{-1}(X \circ Y). \quad (6.9)$$

Нека p е просто число и g е примитивен корен по модул p . Да разгледаме редицата $A = \{a_n\}$, където

$$a_n = e^{\frac{2\pi i}{p} g^n}, \quad n = 0, 1, 2, \dots \quad (6.10)$$

Очевидно, редицата е периодична с период $N = p - 1$. В сила е:

Твърдение 6.1.7 За редицата $A\{a_n\}$ е в сила

$$\mathcal{R}_A(t) = \begin{cases} -1, & t \not\equiv 0 \pmod{p-1}, \\ p-1, & t \equiv 0 \pmod{p-1}. \end{cases}$$

и

$$|A_k|^2 = \begin{cases} 1, & k \equiv 0 \pmod{p-1}, \\ p, & k \not\equiv 0 \pmod{p-1}. \end{cases}$$

Доказателство.

$$\mathcal{R}_A(t) = \sum_{n=0}^{p-2} a_n \bar{a}_{n+t} = \sum_{n=0}^{p-2} e^{\frac{2\pi i g^n}{p} - \frac{2\pi i g^{n+t}}{p}} = \sum_{n=0}^{p-2} e^{\frac{2\pi i g^n(1-g^t)}{p}}.$$

Но тъй като $1 - g^t \not\equiv 0 \pmod{p}$ при $t \not\equiv 0 \pmod{p-1}$, то $k = g^n(1 - g^t)$ описва пълна система от ненулеви остатъци по модул p . Следователно

$$\mathcal{R}_A(t) = \sum_{k=1}^{p-1} e^{\frac{2\pi i k}{p}} = \sum_{k=1}^{p-1} \xi^k = -1.$$

При $t \equiv 0 \pmod{p-1}$, $1 - g^t \equiv 0 \pmod{p}$, което влече

$$\mathcal{R}_A(0) = \mathcal{R}_A(p-1) = \mathcal{R}_A(2p-2) = \dots = p-1.$$

Да разгледаме преобразование на Фурие $\mathcal{F}(A) = \{A_k\}$ на A . Съгласно дефиницията

$$A_k = \sum_{n=0}^{p-2} a_n \xi^{nk}.$$

Равенство(6.5) и пресметнатата по-горе корелация ни дават

$$|A_0|^2 = \sum_{t=0}^{p-2} \mathcal{R}_X(t) = (p-1) + (p-2)(-1) = 1.$$

$$|A_k|^2 = (p-1) + \sum_{t=1}^{p-2} (-1) \xi^{-kt} = p-1 - (-1) = p.$$

Твърдение 6.1.8 Редицата $B = \{b_n\}$, дефинирана с

$$b_n \stackrel{\text{def}}{=} \begin{cases} \left(\frac{n}{p}\right), & n \not\equiv 0 \pmod{p}, \\ 0, & n \equiv 0 \pmod{p}. \end{cases} \quad (6.11)$$

е периодична с период p и

$$(1) \quad B_0 = 0, \quad B_k = b_k B_1;$$

$$(2) |B_k|^2 = |B_1|^2 = \text{const}, \quad \text{за всяко } k = 1, 2, \dots, p-1.$$

Доказателство.

Периодичността е очевидна. За фуриеровия ѝ спектър получаваме

$$B_0 = \sum_{j=0}^{p-1} b_j = 0,$$

тъй като $b_j = 1$ за $(p-1)/2$ стойности на j и за още толкова е $b_j = -1$. От мултипликативността на символа на Лъжандр следва, че

$$b_n = b_n b_k^2 = b_{nk} b_k,$$

откъдето получаваме

$$B_k = \sum_{n=0}^{p-1} b_n \xi^{kn} = \sum_{n=0}^{p-1} b_k b_{nk} \xi^{kn} = b_k \sum_{l=0}^{p-1} b_l \xi^l = b_k B_1.$$

Следователно

$$|B_k|^2 = b_k^2 |B_1|^2 = |B_1|^2 = \text{const}, \quad \text{за всяко } k = 1, 2, \dots, p-1.$$

6.2 Допълнителни задачи към Глава 6.

Задача 6.1 Нека $r_n^{(k)} = e^{\frac{2\pi i k n^2}{p}}$, където p е просто число, $k = 1, 2, \dots, p-1$. Докажете, че всяка от редиците $\{r_n^{(k)}\}_{n=0}^{\infty}$ е периодична с период p и са в сила

$$\mathcal{R}(t) = \begin{cases} 0, & t \not\equiv 0 \pmod{p}, \\ p, & t \equiv 0 \pmod{p}. \end{cases}$$

$$|R_n^{(k)}|^2 = p, \quad n = 0, 1, \dots, p-1,$$

където $\{R_n^{(k)}\} = \mathcal{F}(\{r_n^{(k)}\})$.

Задача 6.2 При условието на предишната задача, покажете, че при $k \neq l$

$$\mathcal{R}_{kl}(t) = \sum_{n=0}^{p-1} r_n^{(k)} \bar{r}_{n+t}^{(l)} = 0$$

за всяко t .