

N	m	N	m	N	m	N	m
3	2	87	28	275	20	819	12
5	4	89	11	279	30	825	20
7	3	91	12	315	12	889	21
9	6	93	10	331	30	993	30
11	10	99	30	337	21	1023	10
13	12	105	12	339	28	1025	20
15	4	113	28	341	10	1057	15
17	8	117	12	357	24	1071	24
19	18	119	24	381	14	1103	29
21	6	123	20	399	18	1105	24
23	11	127	7	435	28	1197	18
25	20	129	14	451	20	1205	24
27	18	133	18	453	30	1247	28
29	28	145	28	455	12	1271	20
31	5	151	15	465	20	1285	16
33	10	153	24	511	9	1353	20
35	12	155	20	513	18	1359	30
39	12	165	20	565	28	1365	12
41	20	171	18	585	12	1387	18
43	14	189	18	595	24	1533	18
45	12	195	12	601	25	1547	24
47	23	205	20	615	20	1661	30
49	21	215	28	635	28	1687	24
51	8	217	15	645	28	1695	28
55	20	219	18	651	30	1705	20
57	18	221	24	657	18	1785	24
63	6	231	30	663	24	1801	25
65	12	233	29	683	22	1905	28
69	22	241	24	693	30	1953	30
73	9	255	8	723	24	1971	18
75	20	257	16	745	24	1989	24
77	30	267	22	771	16	2047	11
85	8	273	12	775	20	2049	22

### 7.3 ROZKLAD ČÍSLICOVÉHO SIGNÁLU

V komplexnom signálovom priestore deterministických diskretných signálov bol dôležitý rozklad do systému diskretných exponenciálnych funkcií

$$\text{def}(n) = \left\{ \text{def}(n,k) = e^{j \frac{2\pi}{N} kn}, k = 0, 1, \dots, N-1 \right\}$$

kde  $n = 0, 1, \dots, N-1$ . Rovnaký význam ako číslo  $e^{j \frac{2\pi}{N}}$  v komplexnom signálovom priestore diskretných signálov hrá v komplexnom signálovom priestore číselných signálov prvok  $\xi \in GF(p^m)$ , pre ktorý  $\xi^N = 1$ .

Signál

$$\text{gef}(n) = \{ \text{gef}(n, k) = \xi^{kn}, k = 0, 1, \dots, N-1 \}$$

pre  $n = 0, 1, \dots, N-1$  budeme nazývať Goloisovou exponenciálnou funkciou.

Podobne ako harmonické signály, diskretné exponenciálne funkcie, Walshove funkcie, aj Goloisove exponenciálne funkcie majú vlastnosť, že okrem jednej,  $\text{gef}(0)$ , ostatné majú nulovú "strednú hodnotu".

Veta:

Pre Goloisove exponenciálne funkcie platí

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

Dôkaz:

Pre  $n = 0$  platí

$$\sum_{k=0}^{N-1} \text{gef}(0, k) = \sum_{k=0}^{N-1} \xi^0 = N$$

Pre  $n \neq 0$  je dôkaz dlhší. Každý nenulový prvok poľa  $GF(p^m)$  je koreňom rovnice

$$x^N - 1 = 0$$

pretože pre každý prvok  $x$  existuje také  $i$ , že  $x = \xi^i$  a  $\xi^{iN} = 1$ . Jedným prvkom poľa je vždy  $\xi^0 = 1$ . Postupným delením  $(x^N - 1) : (x - 1)$  sa môžeme presvedčiť, že podiel je  $x^{N-1} + x^{N-2} + \dots + x + 1$ . Potom rovnicu  $x^N - 1 = 0$  môžeme písať v tvare

$$(x-1)(x^{N-1} + x^{N-2} + \dots + x + 1) = 0$$

Pre  $x \neq 1$  potom musí platiť

$$\sum_{k=0}^{N-1} x^k = 0$$

kde  $x$  je prvok poľa  $GF(p^m)$  rôzny od 1. Keďže pre každý takýto prvok existuje  $n \neq 0$  tak, že  $\xi^n = x$ , musí platiť

$$\sum_{k=0}^{N-1} \varepsilon^{nk} = 0, \quad n \neq 0$$

alebo po prepísaní

$$\sum_{k=0}^{N-1} \text{gef}(n, k) = 0, \quad n \neq 0$$

Veta:

Systém Galoisových exponenciálnych funkcií  $\text{gef}(n)$ ,  $n = 0, 1, \dots, N-1$  tvorí ortogonálnu bázu v komplexnom signálovom priestore číslícových signálov  $\mathbf{f} = (f_0, f_1, \dots, f_{N-1})$ .

Dôkaz:

Skalárny súčin Galoisových exponenciálnych funkcií je

$$\begin{aligned} (\text{gef}(n), \text{gef}(m)) &= \sum_{k=0}^{N-1} \overline{\text{gef}(n, k)} \odot \text{gef}(m, k) = \\ &= \sum_{k=0}^{N-1} \varepsilon^{-nk} \odot \varepsilon^{mk} = \sum_{k=0}^{N-1} \varepsilon^{(m-n)k} \end{aligned}$$

Podľa predchádzajúcej vety je pre  $m-n \neq 0$  suma nulová a pre  $m-n = 0$  sa suma rovná  $N \bmod p$ .

$$(\text{gef}(n), \text{gef}(m)) = \begin{cases} 0, & n \neq m \\ N, & n = m \end{cases}$$

Galoisove exponenciálne funkcie sú teda ortogonálne a keďže signálový priestor je  $N$  rozmerný ( $N$ -konečný), vytvárajú v ňom bázu. Výpočet koeficientov rozkladu číslícového signálu do bázy tvorenej Galoisovými exponenciálnymi funkciami

$$c_n^* = \frac{(\mathbf{f}, \mathbf{b}_n)}{(\mathbf{b}_n, \mathbf{b}_n)}, \quad n = 0, 1, \dots, N-1$$

kde  $\mathbf{b}_n = \text{gef}(n)$  budeme volať Fourierovou transformáciou v Galoisovom poli. Po dosadení do skalárneho súčinu dostávame:

Fourierova transformácia číslícového signálu

$$c_n = \frac{1}{N} \sum_{k=0}^{N-1} f_k \varepsilon^{-nk}, \quad n = 0, 1, \dots, N-1$$

a spätná Fourierova transformácia

$$f_k = \sum_{n=0}^{N-1} c_n \varepsilon^{nk}, \quad k = 0, 1, \dots, N-1$$

kde  $\varepsilon$  je primitívny prvok poľa  $GF(p^m)$  taký, že  $\varepsilon^N = 1$ .

Poznámka: Naznačené operácie sú modulo  $q(x)$ , kde  $q(x)$  je ireducibilný polynóm  $N$ -tého stupňa nad poľom  $GF(p)$ . Pod  $1/N$  rozumieme  $N^{-1}$ , t.j. inverzný prvok k  $N$ .

Vektor  $c = (c_0, c_1, \dots, c_{N-1})$  budeme volať spektrom číslicového signálu  $f = (f_0, f_1, \dots, f_{N-1})$  a budeme písať  $c = \mathcal{F}\{f\}$ .

Presvedčíme sa ďalej, že Fourierova transformácia nad Galoisovým poľom má tie isté vlastnosti ako Fourierova transformácia, resp. diskretná Fourierova transformácia.

#### Príklad:

Vypočítajte Fourierov obraz binárneho trojzložkového signálu.

Trojzložkový binárny signál je vektor  $f = (f_0, f_1, f_2)$ , kde  $f_i \in \{0, 1\}$   $i = 0, 1, 2$ . Podľa definície Fourierovho obrazu

$$m = 2 \text{ pretože } 3 \text{ je deliteľom } 2^2 - 1.$$

Zložky spektra budú teda nad poľom  $GF(2^2)$ , t.j. budú mať tvar

$$c_i(x) = c_{i1} + c_{i0}, \quad i = 0, 1, 2, \quad c_{i1}, c_{i0} \in \{0, 1\}$$

Pole  $GF(2^2)$  je štruktúra  $(\mathcal{F}(x), \oplus, \odot)$ , kde  $\mathcal{F}(x)$  je množina polynómov  $c_i(x)$ ,  $i = 0, 1, 2$  prvého stupňa a  $q(x)$  je ireducibilný polynóm druhého stupňa. Jediným takýmto polynómom je  $q(x) = x^2 + x + 1$ .

Primitívnym prvkom v  $GF(2^2)$  je  $x$  pretože

$$\begin{aligned} x^0 &= 1 \\ x^1 &= x \\ x^2 &= x + 1 \\ (x^3 &= 1) \end{aligned}$$

pričom operácia násobenia je mod  $q(x)$ , napr.  $x^2 = x \odot_{q(x)} x$ .

Podľa definície bude Fourierov obraz signálu  $f = (1, 1, 1)$  mať zložky

$$c_0 = 1 \cdot x^{0 \cdot 0} \oplus 1 \cdot x^{1 \cdot 0} \oplus 1 \cdot x^{2 \cdot 0} = 1$$

$$c_1 = 1 \cdot x^{0 \cdot 1} \oplus 1 \cdot x^{1 \cdot 1} \oplus 1 \cdot x^{2 \cdot 1} = 1 + x + (x+1) = 0$$

$$c_2 = 1 \cdot x^{0 \cdot 2} \oplus 1 \cdot x^{1 \cdot 2} \oplus 1 \cdot x^{2 \cdot 2} = 1 + (x+1) + x = 0$$



Teda signál  $f = (1, 1, 1)$  má spektrum  $c = (1, 0, 0)$ .

Podobne vypočítame spektrum aj ostatných signálov:

signál	spektrum
$f_0 = (0, 0, 0)$	$c_0 = (0, 0, 0)$
$f_1 = (0, 0, 1)$	$c_1 = (1, x+1, x)$
$f_2 = (0, 1, 0)$	$c_2 = (1, x, x+1)$
$f_3 = (0, 1, 1)$	$c_3 = (0, 1, 1)$
$f_4 = (1, 0, 0)$	$c_4 = (1, 1, 1)$
$f_5 = (1, 0, 1)$	$c_5 = (0, x, x+1)$
$f_6 = (1, 1, 0)$	$c_6 = (0, x+1, x)$
$f_7 = (1, 1, 1)$	$c_7 = (1, 0, 0)$

Ako zložky spektra vyjadríme pomocou primitívneho prvku  $\xi = x$ , môžeme tiež písať

$$\begin{aligned} c_0 &= (0, 0, 0) & c_4 &= (1, 1, 1) \\ c_1 &= (1, \xi^2, \xi) & c_5 &= (0, \xi, \xi^2) \\ c_2 &= (1, \xi, \xi^2) & c_6 &= (0, \xi^2, \xi) \\ c_3 &= (0, 1, 1) & c_7 &= (1, 0, 0) \end{aligned}$$

Veta:

Nech  $f = (f_0, \dots, f_{N-1})$  a  $f' = (f'_0, \dots, f'_{N-1})$  sú číslkové signály v komplexnom kódovom signálovom priestore so spektrami  $F = \mathcal{F}(f) = (F_0, \dots, F_{N-1})$  a  $F' = \mathcal{F}(f') = (F'_0, \dots, F'_{N-1})$ . Ak pre signál  $g = (g_0, \dots, g_{N-1})$  so spektrom  $G = \mathcal{F}(g) = (G_0, \dots, G_{N-1})$  platí

$$g_i = f_i \odot_p f'_i, \quad i = 0, 1, \dots, N-1$$

potom

$$G_i = \sum_{k=0}^{N-1} F'_k \odot_{q(x)} F_i \ominus_N k$$

Dôkaz:

Vypočítame spektrum signálu  $g$

$$\begin{aligned} G_i &= \frac{1}{N} \sum_{j=0}^{N-1} g_j \odot \xi^{-ij} = \frac{1}{N} \sum_{j=0}^{N-1} f_j \odot f'_j \xi^{-ij} = \\ &= \frac{1}{N} \sum_{j=0}^{N-1} f_j \odot \xi^{-ij} \sum_{k=0}^{N-1} F'_k \odot \xi^{jk} = \end{aligned}$$

$$= \sum_{k=0}^{N-1} \left\{ F'_k \odot \frac{1}{N} \odot \sum_{j=0}^{N-1} f_j \odot \xi^{-j(i-k)} \right\} = \sum_{k=0}^{N-1} F'_k \odot F_i \ominus k$$

Uvedená veta tvrdí, že súčin signálov odpovedá kruhová konvolúcia spektier (argumenty sa sítavajú modulo  $N$ ). Rovnakým spôsobom sa presvedčte, že platí aj analogické tvrdenie: Kruhovej konvolúcii číslícových signálov

$$g_i = \sum_{k=0}^{N-1} f'_k \odot_p f_i \ominus_N k$$

odpovedá súčin spektier

$$G_i = F_i \odot_{q(x)} F'_i$$

Poznamenajme, že kruhovú konvolúciu signálov  $f, f'$  môžeme tiež zapísať pomocou polynómov

$$g(x) = f(x) \odot_{h(x)} f'(x)$$

kde  $h(x) = x^N - 1$ .

Platí tiež rovnosť Parsevalovho typu. Ak totiž v konvolúcii počítanej pri dôkaze predchádzajúcej vety

$$G_i = \frac{1}{N} \sum_{j=0}^{N-1} f_j \odot f'_j \odot \xi^{-i} \odot j = \sum_{j=0}^{N-1} F'_j \odot F_i \ominus j$$

položíme  $i = 0$ , dostávame

$$\frac{1}{N} \sum_{j=0}^{N-1} f_j \odot f'_j = \sum_{j=0}^{N-1} F'_j \odot F_{-j}$$

Platí veta o posunutí spektra, resp. signálu.

Veta:

Ak  $F = \mathcal{F}\{f\}$ , kde  $F = (F_0, \dots, F_{N-1})$  a  $f = (f_0, \dots, f_{N-1})$ , potom

$$\mathcal{F}\{(f_{N-1}, f_0, f_1, \dots, f_i, \dots, f_{N-2})\} = (F_0 \omega^0, \dots, F_i \omega^i, \dots, F_{N-1} \omega^{N-1})$$

$$\mathcal{F}\{(\omega^0 f_0, \dots, \omega^i f_i, \dots, \omega^{N-1} f_{N-1})\} = (F_1, F_2, \dots, F_i, \dots, F_{N-1}, F_0)$$

O správnosti sa presvedčte dosadením do definičných vzťahov.

Tak ako pri Fourierovej transformácii platilo, že amplitúdové spektrum reálneho signálu je párna funkcia a fázové spektrum je nepárna funkcia, existuje ohraničenie aj u spektier číslicových signálov.

Veta:

Nech  $c$  je spektrom signálu  $f$  v kódovom signálovom priestore nad poľom  $GF(p^m)$ . Hodnoty signálu  $f_i$ ,  $i = 0, 1, \dots, N-1$  sú z poľa  $GF(p)$  práve vtedy, keď platí

$$c_i^p = c_i \odot_N p, \quad i = 0, 1, \dots, N-1.$$

Dôkaz je možné nájsť v [3]. Budeme hovoriť, že spektrum  $c$  je realizovateľné, ak koeficienty  $c_i$ ,  $i = 0, 1, \dots, N-1$  spĺňajú podmienku uvedenej vety. Podľa tejto vety môžeme rozdeliť koeficienty  $c_i$ ,  $i = 0, 1, \dots, N-1$  do tried tak, že v jednej triede sú koeficienty viazané vyššie uvedeným vzťahom, t.j. v jednej triede sú koeficienty s indexami

$$i, i \odot_N p, \dots, i \odot_N p^{m_i-1}$$

kde  $m_i$  je najmenšie prirodzené číslo, pre ktoré platí

$$i \odot_N p^{m_i} = i$$

Pretože pole je konečné, takéto  $m_i$  existuje.

Príklad:

V predchádzajúcom príklade sme vypočítali spektrá číslicových signálov pre  $N = 3$ ,  $p = 2$ . Podľa uvedenej vety platí

$$c_0^2 = c_0 \odot_2 2 = c_0$$

$$c_1^2 = c_1 \odot_2 2 = c_2$$

$$c_2^2 = c_2 \odot_2 2 = c_1$$

Presvedčte sa o správnosti týchto vzťahov dosadením zložiek spektier z predchádzajúceho príkladu. Na určenie spektra uvedených signálov je teda potrebná zložka  $c_0$  a jedna zo zložiek  $c_1, c_2$ .

Príklad:

Nech je daný binárny kódový signálový priestor sedembitových signálov, t.j.  $p = 2$ ,  $N = 7$ . Určte, ktoré zložky spektra tieto signály definujú, pričom ich je čo najmenej.

Indexy závislých koeficientov vytvoria triedy

$$A_i = \{ i, ip, \dots, ip^{m_i-1} \}$$