7 ÚROVEŇ KÓDER ZDROJA - DEKÓDER PRIJÍMAČA

Základným predpokladom spoľahlivého prenosu je prenos určitej nadbytočnej informácie, na základe ktorej vie posúdiť prijímač informácií (s určitou pravdepodobnosťou), či pri prenose došlo ku skresleniu informácie, poprípade môže sa sám pokúsiť o odstránenie tohoto skreslenia. Prirodzené zdroje informácie takúto nadbytočnosť vytvárajú, avšak signály, ktoré sú nositeľmi informácie sa môžu šíriť rozličnými prostrediami (akustickým, elektrickým, optickým). Úlohou kódera zdroja informácie je odstrániť nadbytočnú informáciu, ktorú generuje zdroj informácie (čím sa zvýši efektívnosť prenosu) a naopak pridať nadbytočnú informáciu tak, aby čo najviac zvýšila spoľahlivosť prenosu daným kanálom.

Vedná disciplína, ktorá sa zaoberá odstraňovaním neúčelnej nadbytočnosti a zavádzaním užitočnej nadbytočnosti do číslicových signálov sa volá teória kódovania. V tomto predmete sa pokúšame modelovať všetky typy signálov v signálovom priestore. Preto aj teóriu číslicových signálov budeme vysvetľovať ináč než klasická teória kódovania. Hoci takýto prístup neposkytuje jednoduché návody na návrh kóderov a dekóderov, veríme, že umožní ľahšie pochopiť podstatu problému.

7.1 ZÁKLADNÉ VLASTNOSTI ČÍSLICOVÝCH SIGNÁLOV

Na úrovni kóder zdroja - dekóder prijímača sa vytvárajú a spracúvajú číslicové signály s konečnou abecedou $F = \{0,1, \ldots, p-1\}$, ktoré sú definované na konečnom časovom intervale $T = \{0,1, \ldots, N-1\}$.
V kapitole 2.2 o operáciách s hodnotami signálov sme požadovali, aby hodnoty signálu s operáciami násobenia a sčítania, t.j. algebraická štruktúra $(F, \oplus, \odot)$ bola poľom. U číslicových signálov s konečnou abecedou konečným poľom, ktoré voláme Galoisovým poľom. Videli sme, že ak operácie súčtu a súčinu sú definované ako súčet a súčin sú modulo p, kde p je prvočíslo, potom štruktúra je poľom a budeme ho označovať

$$GF(p) = (F, \oplus_p, \odot_p)$$

Definícia:

Primitívnym prvkom poľa $GF(p)$ voláme taký prvok α, že prvky poľa okrem nulového sa dajú vyjadriť ako mocnina prvku α. Napríklad v poli GF(5)

platí $2^1 = 2$, $2^2 = 4$, $2^3 = 3$, $2^4 = 1$, takže 2 je primitívnym prvkom poľa GF(5). Dá sa dokázať [9], že v každom Galoisovom poli existuje primitívny prvok.

Od poľa hodnôt číslicového signálu GF(p) sa dá odvodiť množina číslicových signálov, ktoré sú definované na konečnej časovej množine $T = \{0,1, \ldots, \ldots, N-1\}$ napr. v tvare formálnych polynómov

$$F(x) = \left\{ f_0+f_1x + \ldots + f_{N-1}x^{N-1} = \mathbf{f}(x) \ , \quad f_i \in F \ , \quad i = 0, \ldots, N-1 \right\}$$

V kapitole 2.6 sme videli, že množina takýchto číslicových signálov s operáciami súčet a súčin modulo q(x), kde q(x) je ireducibilný polynóm stupňa N, tvorí tiež Galoisovo pole. Budeme ho označovať

$$GF(p^N) = \left(F(x), \underset{q(x)}{\oplus}, \underset{q(x)}{\odot} \right)$$

a budeme hovoriť, že $GF(p^N)$ je jednoduchým rozšírením stupňa N svojho podpoľa GP(p).

Príklad:

Pole $GF(2^3)$, ktoré dostaneme jednoduchým rozšírením tretieho stupňa GF(2) je poľom $(F(x), \underset{q(x)}{\oplus}, \underset{q(x)}{\odot})$, kde

$$F(x) = \left\{ \mathbf{f}(x) = f_2x^2 + f_1x + f_0 \ ; \ f_0, f_1, f_2 \in \{0,1\} \right\}$$

a q(x) je ireducibilným polynómom tretieho stupňa, t.j.

$$q(x) = x^3 + x + 1$$

Primitívnym prvkom poľa $GF(2^3)$ je $\alpha(x) = x$, pretože

$$\alpha^0 = 1$$
$$\alpha^1 = x$$
$$\alpha^2 = x^2$$
$$\alpha^3 = x + 1$$
$$\alpha^4 = x^2 + x$$
$$\alpha^5 = x^2 + x + 1$$
$$\alpha^6 = x^2 + 1$$
$$(\alpha^7 = 1 = \alpha^0)$$

Taký ireducibilný polynóm $q(x)$, pre ktorý je primitívnym prvkom polynóm $\alpha(x) = x$ voláme primitívny polynóm. V uvedenom príklade je teda polynóm $q(x) = x^3 + x + 1$ primitívnym.

V nasledujúcej tabuľke sú uvedené primitívne polynómy pre $q = 2$ [3].

Primitívne polynómy pre $q = 2$ Tab. 2

Stupeň	Primitívny polynóm
2	$x^2 + x + 1$
3	$x^3 + x + 1$
4	$x^4 + x + 1$
5	$x^5 + x^2 + 1$
6	$x^6 + x + 1$
7	$x^7 + x^3 + 1$
8	$x^8 + x^4 + x^3 + x^2 + 1$
9	$x^9 + x^4 + 1$
10	$x^{10} + x^3 + 1$
11	$x^{11} + x^2 + 1$
12	$x^{12} + x^6 + x^4 + x + 1$
13	$x^{13} + x^4 + x^3 + x + 1$
14	$x^{14} + x^{10} + x^6 + x + 1$
15	$x^{15} + x + 1$
16	$x^{16} + x^{12} + x^3 + x + 1$
17	$x^{17} + x^3 + 1$
18	$x^{18} + x^7 + 1$
19	$x^{19} + x^5 + x^2 + 1$
20	$x^{20} + x^3 + 1$
21	$x^{21} + x^2 + 1$
22	$x^{22} + x + 1$
23	$x^{23} + x^5 + 1$
24	$x^{24} + x^7 + x^2 + x + 1$
25	$x^{25} + x^3 + 1$
26	$x^{26} + x^6 + x^2 + x + 1$
27	$x^{27} + x^5 + x^2 + x + 1$
28	$x^{28} + x^3 + 1$

Pomocou vyjadrenia prvkov poľa ako mocniny primitívneho prvku vieme rýchlo určiť súčin dvoch prvkov, napr.

$$(x^2+x) \underset{q(x)}{\odot} (x^2+x+1) = \alpha^4 \underset{q(x)}{\odot} \alpha^5 = \alpha^{4 \overset{7}{\oplus} 5} = \alpha^2 = x^2$$

Veta:

Každý prvok Galoisovho poľa $GF(p^n)$ je koreňom rovnice

$$x^{p^n} - x = 0$$

Dôkaz:

Nech α je jedným z primitívnych prvkov poľa $GF(p^n)$ a β ľubovoľný nenulový prvok tohoto poľa. β je možné vyjadriť ako mocninu α, t.j. $\beta = \alpha^i$. Potom

$$\beta^{p^n-1} = \alpha^{i \odot (p^n-1)}$$

Pretože v exponente prvku α je súčin modulo p^n-1, bude $i \odot (p^n-1) = 0$ a teda

$$\alpha^{i \odot (p^{n-1})} = \alpha^0 = 1$$

teda

$$\beta^{p^n-1} = 1$$

Prvok β je potom koreňom rovnice $x^{p^n-1} - 1 = 0$ a teda aj rovnice

$$x^{p^n} - x = 0$$

Pre nás bude významná nasledujúca veta.

Veta:

Galoisovo pole $GF(p^N)$ je N-rozmerným signálovým priestorom nad poľom $GF(p)$.

Dôkaz:

Vezmime ľubovoľný prvok $\mathbf{f}_1 \in \{F(x) - 0\}$ a zostrojme signálový priestor $GF_1(p^N) = \{a_1 \mathbf{f}_1, a_1 = 0,1, \ldots, p-1\}$. Ak $GF(p^N) - GF_1(p^N)$ nie je prázdny, potom vyberieme ľubovoľný prvok $\mathbf{f}_2 \in GF(p^N) - GF_1(p^N)$ a zostrojíme signálový priestor

$$GF_2(p^N) = \{a_1 \mathbf{f}_1 + a_2 \mathbf{f}_2, \quad a_1, a_2 = 0,1, \ldots, p-1\}$$

Ak budeme v tejto procedúre pokračovať ďalej, potom v dôsledku konečnosti poľa $GF(p^N)$ dostaneme pri nejakej hodnote m signálový priestor $GF_m(p^N)$ tak, že množina signálov $F_m(x) = \{a_1 f_1 + \ldots + a_m f_m, a_i = 0,1, \ldots, p-1, i = 1,\ldots,$

..., m} bude zhodná s množinou prvkov $GF(p^N)$. Podľa spôsobu výberu musia byť prvky $\mathbf{f}_1, \ldots, \mathbf{f}_m$ lineárne nezávislé, takže sú bázou m rozmerného signálového priestoru. Pretože počet signálov v ňom sa rovná počtu prvkov poľa $GF(p^N)$, bude $m = N$.

7.2 KOMPLEXNÝ KÓDOVÝ SIGNÁLOVÝ PRIESTOR

Pri spracovaní reálnych signálov sme sa presvedčili o pravdivosti Hadamardovho výroku, že "najkratšia cesta medzi prvkami v reálnej oblasti prechádza často cez komplexnú oblasť". Silným nástrojom pre spracovanie diskrétnych signálov je diskrétna Fourierova transformácia, ktorú sme tiež interpretovali ako výpočet koeficientov rozkladu diskrétneho signálu s konečným časom $T \in \{0,1, \ldots, N-1\}$ do systému bázických signálov

$$\mathbf{b}_k = \mathrm{def}(k) = \left(1, \ldots, e^{j\frac{2\pi}{N}ik}, \ldots, e^{j\frac{2\pi}{N}(N-1)k}\right)$$

Táto báza vytvára N-rozmerný komplexný signálový priestor, v ktorom zložky $c_i = \mathrm{Re}\, c_i + j\, \mathrm{Im}\, c_i$; $i = 0, \ldots, N-1$ vektora

$$\mathbf{c} = (c_0, c_1, \ldots, c_{N-1})$$

sú komplexné čísla. Môžeme ich vyjadriť tiež v tvare

$$c_i = c_i\, e^{j\alpha_i}$$

kde

$$\alpha_i \in \left\{ \frac{2\pi}{N} k\,, \quad k = 0,1, \ldots, N-1 \right\}$$

Základnú úlohu v komplexnom signálovom priestore diskrétnych signálov má teda prvok

$$\xi = e^{j\frac{2\pi}{N}}$$

pre ktorý $(\xi)^N = 1$. Na prvku s touto vlastnosťou založíme aj komplexný kódový signálový priestor. Komplexný kódový signálový priestor budeme definovať nad takým poľom $GF(p^m)$, v ktorom existuje prvok ξ tak, že

$$\xi^N = 1$$

Rovnica bude splnená, ak N bude deliteľom čísla p^m-1. Z uvedeného vyplýva nasledujúca definícia:

Definícia:

Nech N je prirodzené číslo, p-prvočíslo a $\mathcal{F}(x) = \{a_0+a_1x + \ldots + a_{N-1}x^{N-1}$; $a_i \in \{0,1, \ldots, p-1\}$, $i = 0,1, \ldots, N-1\}$ je množina číslicových signálov nad poľom $GF(p)$. Ďalej nech m je najmenšie číslo, pre ktoré je N deliteľom čísla $p^m - 1$. Potom signálový priestor φ nad poľom $GF(p^m)$ voláme komplexným kódovým signálovým priestorom.

Poznámka:

Ak platí $N = p^m - 1$, potom $\mathcal{E}$ je zároveň primitívnym prvkom. Ak k prvku $c \in GF(p^m)$ definujeme komplexne združený prvok ako inverzný, t.j.

$$\bar{c} = c^{-1}$$

(pripomíname, že inverzný prvok je taký, že $c \odot c^{-1} = 1$), potom skalárny súčin dvoch signálov

$$\mathbf{f} = (f_0, \ldots, f_{N-1})$$

$$\mathbf{f}' = (f_0', \ldots, f_{N-1}')$$

z komplexného kódového signálového priestoru φ definovaný

$$(\mathbf{f}, \mathbf{f}') = \sum_{i=0}^{N-1} \overline{f_i} \underset{q(x)}{\odot} f_i'$$

kde $q(x)$ je ireducibilný polynóm stupňa m, vyhovuje definícii skalárneho súčinu v komplexnom signálovom priestore (pozri kap. 3.4).

Príklad:

Nech $N=7$ a $p=2$. Najmenším m, pre ktoré je N deliteľom 2^m-1 je $m=3$, pretože $7 = 2^3-1$. Signály v tomto komplexnom signálovom priestore budú teda nadobúdať hodnoty z abecedy

$$F = \left\{ a_0+a_1x+a_2x^2 \ , \ a_0,a_1,a_2 \in \{0,1\} \right\}$$

Aby sme mohli hodnoty sčítať a násobiť, musíme zvoliť niektorý ireducubilný polynóm tretieho stupňa

$$q_1(x) = x^3 + x^2 + 1$$

$$q_2(x) = x^3 + x + 1$$

Zvoľme $q(x) = q_2(x)$, ktorý je primitívny. Štruktúra $(F, \underset{q(x)}{\oplus}, \underset{q(x)}{\odot})$ je Galoisovým poľom $GF(2^3)$. Nad týmto poľom zostrojíme komplexný kódový signálový priestor číslicových signálov

$$\mathbf{f} = (f_0, f_1, \ldots, f_6) ,$$

kde $f_i \in F$, $i = 0, \ldots, 6$.

Určíme skalárny súčin komplexných číslicových signálov

$$\mathbf{f} = (0, x, x^2, x+1, x+1, x^2+1, x)$$

$$\mathbf{f}' = (x^2+1, x+1, x, x+1, x^2, x^2, x)$$

Signály $\mathbf{f}$, $\mathbf{f}'$ môžeme vyjadriť tiež v tvare

$$\mathbf{f} = (0, \alpha, \alpha^2, \alpha^3, \alpha^3, \alpha^6, \alpha)$$

$$\mathbf{f}' = (\alpha^6, \alpha^3, \alpha, \alpha^3, \alpha^2, \alpha)$$

kde α je primitívny prvok poľa $GF(2^3)$, $\alpha = x$.

Komplexne združeným signálom k $\mathbf{f}$ je

$$\tilde{\mathbf{f}} = (0, \alpha^{-1}, \alpha^{-2}, \alpha^{-3}, \alpha^{-3}, \alpha^{-6}, \alpha^{-1})$$

t.j.

$$\tilde{\mathbf{f}} = (0, \alpha^6, \alpha^5, \alpha^4, \alpha^4, \alpha, \alpha^6)$$

Podľa definície skalárneho súčinu pre komplexné číslicové signály bude

$$(\mathbf{f}, \mathbf{f}') = \sum_{i=0}^{6} \overline{f_i} \underset{q(x)}{\odot} f_i' =$$

$$= 0 \odot \alpha^6 \oplus \alpha^6 \odot \alpha^3 \oplus \alpha \odot \alpha^5 \oplus \alpha^3 \odot \alpha^4 \oplus$$

$$\oplus \alpha^2 \odot \alpha^4 \oplus \alpha^2 \odot \alpha \oplus \alpha^6 \odot \alpha =$$

$$= 0 \oplus \alpha^2 \oplus \alpha^6 \oplus \alpha^0 \oplus \alpha^6 \oplus \alpha^3 \oplus \alpha^0 =$$

$$= \alpha^2 \oplus \alpha^3 = x^2 + x + 1$$

V uvedenom príklade pre $N = 7$, $p = 2$ sme našli $m = 3$. Avšak nie pre každé N , p musí m existovať. V nasledujúcej tabuľke sú uvedené prakticky použiteľné hodnoty N a im odpovedajúce m pre binárne číslicové signály ($p = 2$).

Dĺžky kódov so spektrom Tab. 3

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 diskrétnych signálov bol dôležitý rozklad do systému diskrétnych exponenciálnych funkcií

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