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

$$c_i^p = c_i \underset{N}{\odot} p \quad , \quad i = 0,1, \ldots, N-1 \ .$$

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

$$i, \ i \underset{N}{\odot} p \ , \ldots, \ i \underset{N}{\odot} p^{m_i-1}$$

kde m_i je najmenšie prirodzené číslo, pre ktoré platí

$$i \underset{N}{\odot} p^{m_i} = i$$

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

$$c_0^2 = c_0 \underset{}{\odot} 2 = c_0$$
$$c_1^2 = c_1 \underset{}{\odot} 2 = c_2$$
$$c_2^2 = c_2 \underset{}{\odot} 2 = c_1$$

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

$$A_i = \left\{ i, \ ip, \ \ldots, \ ip^{m_i-1} \right\}$$

$$A_0 = \{0\}$$

$$A_1 = \{1,2,4\} = A_2 = A_4$$

$$A_3 = \{3,6,5\} = A_6 = A_5$$

Na definovanie signálu z uvedeného kódového priestoru potrebujeme poznať tri zložky spektra, napr. c_0, c_1, c_3.

7.4 CYKLICKÉ KÓDY

Ako sme už spomenuli, hlavnou úlohou kódera zdroja je zaviesť nadbytočnosť do prenášanej informácie tak, aby dekóder prijímača dokázal z prijatej informácie určiť, či pri prenose došlo ku chybe, poprípade aby sa pokúsil túto chybu odstrániť. Dosiahneme to tak, že nebudeme používať všetky signály kódového priestoru (nevyužijeme kapacitu kódu), ale použijeme len číslicové signály (slová kódu) s vopred definovanou vlastnosťou. Ak prijatý signál túto vlastnosť nemá, potom pri prenose došlo ku chybe. Keď zavedieme v kódovom signálovom priestore maticu napr. pomocou Hammingovej vzdialenosti (pozri kap. 3.6), potom dekóder prijímača môže opravovať tak, že vyberie číslicový signál s danou vlastnosťou, ktorého vzdialenosť k prijatému signálu je najmenšia. Takýto spôsob voláme dekódovanie podľa minimálnej vzdialenosti.

Najzložitejšou úlohou pri vytvorení kódu je práve výber vhodnej vlastnosti, podľa ktorej určíme, či číslicový signál patrí do kódu alebo nie. V prvom rade budeme požadovať, aby slová kódu tvorili signálový podpriestor základného kódového priestoru. To znamená, že kód musí byť uzavretý vzhľadom na sčítanie signálov a násobenie skalárom.

Jednou z možností je definovanie vlastností slov kódu v spektrálnej oblasti.

Definícia:

Cyklickým (N,k) kódom $\mathcal{K}$ voláme množinu číslicových signálov nad poľom GF(p), ktorých spektrálne zložky so zadanými indexami $i_1, i_2, \ldots, i_{N-k}$ (kontrolnými frekvenciami) sú rovné nule. Jednoducho sa môžeme presvedčiť v spektrálnej oblasti, že ak $\mathbf{f}_1 \in \varphi$, $\mathbf{f}_2 \in \varphi$, potom aj $\mathbf{f}_1 + \mathbf{f}_2 \in \varphi$ a ak $k \in GF(p)$ je skalár a $\mathbf{f} \in \varphi$, potom aj $k.\mathbf{f} \in \varphi$. Slová cyklického kódu môžeme vytvoriť napr. tak, že určíme kontrolné frekvencie, na ktorých bude mať spektrum nulovú hodnotu a na ostatných frekvenciách zvolíme hodnoty spektra tak, aby vyhovovali podmienke existencie signálu nad poľom GF(p):

$$c_i^p = c_i \underset{N}{\odot} p$$

t.j. realizovateľnosť spektra. Z tejto podmienky môžu vyplynúť aj ďalšie nulové zložky spektra.

Príklad:

Vytvorte cyklický kód pre $N = 3$, $p = 2$.

V jednom z predchádzajúcich príkladov sme vypočítali spektrá všetkých trojbitových binárnych signálov. Ak za kontrolnú frekvenciu zvolíme $i = 0$, potom slová cyklického kódu sú

$$\mathbf{f}_0 = (0,0,0) \qquad \mathbf{c}_0 = (0,0,0)$$

$$\mathbf{f}_1 = (0,1,1) \qquad \mathbf{c}_1 = (0,1,1)$$

$$\mathbf{f}_2 = (1,0,1) \qquad \mathbf{c}_2 = (0,x,x+1) = (0, \alpha, \alpha^2)$$

$$\mathbf{f}_3 = (1,1,0) \qquad \mathbf{c}_3 = (0,x+1,x) = (0, \alpha^2, \alpha)$$

Ak za kontrolné frekvencie zvolíme $i_1 = 1$, $i_2 = 2$, potom slová cyklického kódu sú

$$\mathbf{f}_0 = (0,0,0) \qquad \mathbf{c}_0 = (0,0,0)$$

$$\mathbf{f}_1 = (1,1,1) \qquad \mathbf{c}_1 = (1,0,0)$$

Príklad:

Vytvorte cyklický kód so sedembitovými binárnymi slovami.

Pretože $N = 7$, $p = 2$, najmenšie m, pri ktorom je N deliteľom $p-1$ je $m = 3$ a hodnoty spektra budeme vyberať z poľa $GF(2^3)$. Rozdeľme najskôr frekvencie do tried tak, aby číslicové signály so zvolenými spektrami nadobúdali hodnoty z $GF(2)$. Triedy budeme vytvárať podľa vzťahu

$$A_i = \left\{ i, ip, \ldots, ip^{m_i - 1} \right\}$$

kde pre m_i platí

$$ip^{m_i} = i \pmod N$$

V triede A_0 bude len prvok 0, $A_0 = \{0\}$.

$m_1 = 3$, pretože $1.2^3 = 1 \pmod 7$

$$A_1 = \left\{ 1, 1 \underset{7}{\odot} 2, 1 \underset{7}{\odot} 2^2 \right\} = \{1,2,4\}$$

$$A_3 = \left\{ 3, 3 \underset{7}{\odot} 2, 3 \underset{7}{\odot} 2^2 \right\} = \{3,6,5\}$$

Ak zvolíme za kontrolnú frekvenciu $i = 1$, potom kontrolnými frekvenciami musia byť aj $i = 2$, $i = 4$, pretože ležia v jednej triede.

Podmienku realizovateľnosti bitu f_0 nad $GF(2)$, t.j.

$$c_0^2 = c_0 \underset{7}{\odot} 2 \quad , \quad \text{t.j.} \quad c_0^2 = c_0$$

splňujú len hodnoty $C_o = 0$ a $C_o = 1$, t.j. spektrum C na frekvencii $i = 0$ môže nadobúdať hodnoty $C_o \in \{0,1\}$.

Pre zložku spektra C_3 musí platiť

$$C_3^2 = C_6$$

Z tohoto vzťahu vyplýva, že zložka C_3 môže nadobúdať všetky hodnoty z poľa $GF(2^3)$

$$C_3 \in \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$$

kde $\alpha = x$ je primitívny prvok a prvok C_6 je závislý na C_3. Zo vzťahu

$$C_6^2 = C_5$$

vypočítame hodnoty zložky spektra C_5 v závislosti na C_6. Spektrá slov cyklického kódu s kontrolnými frekvenciami $i_o = 1$, $i_1 = 4$ a slová, ktoré dostaneme spätnou Fourierovou transformáciou

$$f_k = \sum_{n=0}^{6} C_n \varepsilon^{nk}, \quad k = 0,1, \ldots, 6$$

pre $\varepsilon = x$ sú v nasledujúcej tabuľke.

Spektrum cyklického kódu — Tab. 4

Spektrum							Slovo kódu						
C_o	C_1	C_2	C_3	C_4	C_5	C_6	f_o	f_1	f_2	f_3	f_4	f_5	f_6
0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	ε^o	0	ε^o	ε^o	1	1	1	0	1	0	0
0	0	0	ε^1	0	ε^4	ε^2	0	0	1	1	1	0	1
0	0	0	ε^2	0	ε^1	ε^4	0	1	0	0	1	1	1
0	0	0	ε^3	0	ε^5	ε^6	1	1	0	1	0	0	1
0	0	0	ε^4	0	ε^2	ε^1	0	1	1	1	0	1	0
0	0	0	ε^5	0	ε^6	ε^3	1	0	0	1	1	1	0
0	0	0	ε^6	0	ε^3	ε^5	1	0	1	0	0	1	1
1	0	0	0	0	0	0	1	1	1	1	1	1	1
1	0	0	ε^o	0	ε^o	ε^o	0	0	0	1	0	1	1
1	0	0	ε^1	0	ε^4	ε^2	1	1	0	0	0	1	0
1	0	0	ε^2	0	ε^1	ε^4	1	0	1	1	0	0	0
1	0	0	ε^3	0	ε^2	ε^6	0	0	1	0	1	1	0
1	0	0	ε^4	0	ε^2	ε^1	1	0	0	0	1	0	1
1	0	0	ε^5	0	ε^6	ε^3	0	1	1	0	0	0	1
1	0	0	ε^6	0	ε^3	ε^5	0	1	0	1	1	0	0

Veta:

Nech je v komplexnom kódovom priestore φ zadané realizovateľné spektrum $\mathbf{G} = (G_0, G_1, \ldots, G_{N-1})$, v ktorom aspoň jedna jeho zložka sa rovná nule (nazveme ho generujúcim filtrom cyklického kódu). Ak $\mathbf{H} \in \varphi$ je realizovateľné spektrum, potom

$$\mathbf{f} = \mathcal{F}^{-1}\left\{\mathbf{H} \odot \mathbf{G}\right\}$$

je slovo cyklického kódu.

V tejto vete $\mathcal{F}^{-1}\{\cdot\}$ je spätná Fourierova transformácia a

$$\mathbf{F} = \mathbf{H} \odot \mathbf{G}$$

znamená, že $F_i = H_i \odot G_i$, $i = 0,1, \ldots, N-1$

Dôkaz:

Ukážte, že ak $\mathbf{H}$ je realizovateľné spektrum, potom aj $\mathbf{F} = \mathbf{H} \odot \mathbf{G}$ je realizovateľné spektrum.

Veta:

Nech $\mathbf{G}$ je generujúcim filtrom cyklického kódu $\mathcal{K}$. Každé slovo kódu je deliteľné slovom

$$\mathbf{g} = \mathcal{F}^{-1}\left\{\mathbf{G}\right\}$$

bezo zvyšku. Slovo $\mathbf{g} = g(x)$ voláme generujúcim polynómom.

Dôkaz:

Z predchádzajúcej vety vyplýva vzhľadom na konečnosť kódového priestoru, že ku každému slovu $\mathbf{f} \in \mathcal{K}$ existuje aspoň jedno kódové slovo $\mathbf{H} \in \varphi$, tak, že

$$\mathbf{f} = \mathcal{F}^{-1}\left\{\mathbf{H} \odot \mathbf{G}\right\}$$

podľa vety o Fourierovom obraze konvolúcie kódových slov

$$f_i = \sum_{k=0}^{N-1} h_k \underset{p}{\odot} g_i \ominus_{N} k$$

alebo podľa definície súčinu signálov

$$f(x) = h(x) \underset{x^N-1}{\odot} g(x)$$

Detekovať, či v cyklickom kóde došlo pri prenose ku chybe, môžeme v časovej oblasti tak, že sa presvedčíme, či prijaté slovo je bezo zvyšku deliteľné polynómom $g(x)$.

Definícia:

Nech v kódovom signálovom priestore Ψ je definovaný cyklický kód $\mathcal{K}$. Rozdiel medzi prijatým signálom $\mathbf{f} \in \Psi$ a vyslaným slovom kódu $\mathbf{f} \in \mathcal{K}$ voláme chybovým slovom

$$\mathbf{e} = \mathbf{f}' \ominus \mathbf{f}$$

Veta:

Cyklický kód odhalí tie chybové slová, ktorých hodnoty spektra na kontrolných frekvenciách je nenulová.

Dôkaz:

Po Fourierovej transformácii vzťahu $\mathbf{e} = \mathbf{f}' \ominus \mathbf{f}$ dostávame $\mathbf{E} = \mathbf{F}' \ominus \mathbf{F}$, kde $\mathbf{E}, \mathbf{F}, \mathbf{F}'$ sú spektrá postupne $\mathbf{e}, \mathbf{f}, \mathbf{f}'$. Pre zložky spektra platí

$$e_i = f_i' \ominus f_i , \quad i = 0,1, \ldots, N-1$$

Pretože slovo cyklického kódu má na kontrolnej frekvencii nulovú hodnotu, spektrum chyby bude mať nenulovú hodnotu práve na tých kontrolných frekvenciách, na ktorých nadobúda nenulové hodnoty spektrum prijatého signálu.

Príklad:

V trojbitovom binárnom cyklickom kóde s kontrolnou frekvenciou $f = 0$ môžu existovať chybové slová, ktorých spektrum s prihliadnutím na podmienku realizovateľnosti nadobúda hodnoty

$$\mathbf{E}_1 = (1, \alpha^2, \alpha)$$
$$\mathbf{E}_2 = (1, \alpha, \alpha^2)$$
$$\mathbf{E}_3 = (1,1,1)$$
$$\mathbf{E}_4 = (1,0,0)$$

čomu odpovedajú chybové slová

$$\mathbf{e}_1 = (0,0,1)$$
$$\mathbf{e}_2 = (0,1,0)$$
$$\mathbf{e}_3 = (1,0,0)$$
$$\mathbf{e}_4 = (1,1,1)$$

Tento cyklický kód dokáže zistiť chybu na jednom mieste a súčasne na všetkých miestach slova kódu (resp. na nepárnom počte miest).

Ak chybové slovo $\mathbf{e}$ vyjadríme v jednotkovej báze

$$\mathbf{e} = \sum_{i=0}^{N-1} e_i \, \boldsymbol{\delta}_i$$

kde $\delta_i = (\delta_{ik} , \; k = 0,1, \ldots, N-1)$

a

$$\delta_{ik} = \begin{cases} 1 , & i = k \\ 0 , & i \neq k \end{cases}$$

potom jeho spektrum je

$$\mathcal{F}\{\mathbf{e}\} = \sum_{i=0}^{N-1} e_i \; \mathcal{F}\{\delta_i\}$$

$$E(n) = \frac{1}{N} \sum_{i=0}^{N-1} e_i \; \varepsilon^{-ni} , \quad n = 0,1, \ldots, N-1$$

Ak pre vyslané slovo $\mathbf{f}$ platí $F(n) = 0$, t.j. n je kontrolná frekvencia, potom pre prijaté slovo $\mathbf{f}'$ platí

$$F'(n) = E(n)$$

Chybový vektor $\mathbf{e}$ potom dostaneme riešením sústavy rovníc

$$F'(n) = \frac{1}{N} \sum_{i=0}^{N-1} e_i \; \varepsilon^{-ni} , \quad \forall n: F(n) = 0$$

Pretože sústava má viac neznámych než rovníc, existuje viac chybových vektorov, ktoré sústave vyhovujú. Spomedzi nich vyberieme jeden podľa ďalších údajov o pravdepodobnosti výskytu jednotlivých chybových slov. Pokiaľ takéto údaje nemáme, zvyčajne predpokladáme, že väčšiu pravdepodobnosť výskytu má chybový vektor s menšou veľkosťou.

Z lineárnej algebry je Vám známe, že pokiaľ sústava s n-neznámymi

$$\mathbf{A}\,\mathbf{x} = \mathbf{b}$$

má nekonečne mnoho riešení, potom riešenia môžeme zapísať v tvare

$$\mathbf{x} = \mathbf{x}_0 + \sum_{i=1}^{s} \alpha_i \, \mathbf{u}_i$$

kde $s = n-h(A)$, $\mathbf{x}_0$ je ľubovoľné riešenie a $\mathbf{u}_i$ je riešením homogénnej sústavy

$$\mathbf{A}\,\mathbf{u}_i = \mathbf{0} , \quad i = 1,2, \ldots, s$$

V prípade sústavy chybových slov cyklického kódu to znamená, že každé chybové slovo môžeme napísať

$$\mathbf{e} = \mathbf{e}_o + \mathbf{f}$$

kde $\mathbf{e}_o$ je nejaké chybové slovo a $\mathbf{f}$ je slovo cyklického kódu.

Definícia:

Kódom BCH (Bose-Chaudhuri-Hochquenghem) voláme cyklický kód, ktorého kontrolné frekvencie sú susedné.

Veta (hranica BCH):

Nech N delí $q^m - 1$. Jediným slovom z $GF(q^N)$ váhy nie väčšej než $d - 1$ a ktorý má $d - 1$ susedných nulových hodnôt spektra je nulový vektor.

Dôkaz:

Nech najmenšou frekvenciou $n \in \{0,1, \ldots, N-1\}$ ktorá je kontrolná je $n = j$. Potom platí

$$C_n = 0 \qquad n = j, j+1, \ldots, j+d-2$$

a použitím spätnej Fourierovej transformácie

$$\sum_{i=0}^{N-1} f_i \, \varepsilon^{-in} = 0 , \qquad n = k, \ldots, j+d-2$$

resp.

$$\sum_{i=0}^{N-1} f_i \, \boldsymbol{\varepsilon}_i = 0$$

kde $\boldsymbol{\varepsilon}_i^T = (\varepsilon^{-ij}, \varepsilon^{-i(j+1)}, \ldots, \varepsilon^{-i(j+d-2)})$

Ak označíme

$$\boldsymbol{\varepsilon}_i = \varepsilon^{-ij} \, \boldsymbol{\varepsilon}_i^*$$

kde

$$\boldsymbol{\varepsilon}_i^* = (\varepsilon^{o}, \varepsilon^{i}, \ldots, \varepsilon^{i(d-2)}) \qquad i = 0,1, \ldots, N-1$$

potom $\boldsymbol{\varepsilon}_i^*$ je i-tou Galoisovou exponenciálnou funkciou v $(d-1)$-rozmernom komplexnom kódovom priestore.

Preto v rovnici

$$\sum_{i=0}^{N-1} f_i \, \boldsymbol{\varepsilon}_i = 0$$

je $d-1$ lineárne nezávislých vektorov $\boldsymbol{\varepsilon}_k \in \{ \boldsymbol{\varepsilon}_i, i = 0,1, \ldots, N-1 \}$. Jej triviálnym riešením je $f_i = 0$, $i = 0,1, \ldots, N-1$.

Vetu môžeme teraz dokázať sporom. Predpokladajme, že nenulový vektor $\mathbf{f} = (f_0, f_1, \ldots, f_{N-1})$ má r nenulových hodnôt $r \leq d-1$ $f_{i_1}, f_{i_2}, \ldots, f_{i_r}$. Potom môžeme písať

$$\sum_{j=1}^{r} f_{ij} \mathcal{E}_{ij} = 0$$

to znamená, že vektory $\{\mathcal{E}_{ij}, j = 1,2, \ldots, r\}$ sú lineárne závislé. To je v rozpore so zistením, že ľubovoľná podmnožina nanajvýš $d-1$ susedných vektorov z množiny $\{\mathcal{E}_i, i = 0,1, \ldots, N-1\}$ je lineárne nezávislá.

Dôsledok:

Najmenšia vzdialenosť medzi dvomi slovami BCH kódu s $d-1$ susednými kontrolnými frekvenciami je d.

Dôkaz:

Pretože slová kódu tvoria signálový priestor, rozdiel dvoch slov je opäť slovo kódu. Keďže neexistuje nenulové slovo kódu s veľkosťou menšou než d, neexistujú ani dve slová kódu, ktorých vzdialenosť by bola menšia než d.

To znamená, že takýto kód umožňuje každému slovu

$$\mathbf{f}' = \mathbf{f} + \mathbf{e}$$

kde Hammingova veľkosť chybového vektora je

$$\| \mathbf{e} \| < \frac{d}{2}$$

jednoznačne priradiť slovo $\mathbf{f}$. Hovoríme, že kód opravuje chyby, do veľkosti $d/2$.

Chybové vektory v tomto prípade (porovnajte s hľadaním chybového vektora všeobecným cyklickým kódom) dostaneme riešením sústavy

$$F'(j+k) = \frac{1}{N} \sum_{i=0}^{N-1} e_i \, \mathcal{E}^{-(j+k)i}, \quad k = 0,1, \ldots, d-2$$

kde j je najnižšia kontrolná frekvencia.