CIKLIKUS KÓDOK

(Az alábbiak feltételezik a "Hiradástechnika" c. könyv "7. Hibakorlátozó kódolás" fejezetének és a modulo-2 algebra alapjainak ismeretét.)

1. Alapfogalmak

Definíció: egy lineáris kód ciklikus, ha bármely kódszavának bármely ciklikus eltolása kódszót eredményez.

A ciklikus eltolást a balra két lépéssel történõ eltolás példáján szemléltetjük.

Tekintsük a c_i, i= 0,...,n-1 elemek általános, n elembõl álló (n hosszúságú) sorozatát:

$$c=(c_{n-1}, c_{n-2}, c_{n-3},.....c_3, c_2, c_1, c_0).$$

Ennek két lépéssel balra történõ ciklikus eltolása az alábbi.

$$\bar{c}=(c_{n-3}, c_{n-4}, ... c_3, c_2, c_1, c_0, c_{n-1},c_{n-2})$$

Vizsgálatainkat a továbbiakban bináris (elemekbõl (jegyekbõl) álló) kódokra korlátozzuk: $c_i \in (0,1)$. A fenti példa egy 9 elemû bináris sorozatra:

- eredeti: (100111000)
- két lépéssel balra ciklikusan eltolt: (011100010)

A ciklikus kódok használatának motivációi közül megemlítjük az alábbiakat:

- egy n elemi tárolóból álló visszahurkolt shift-regiszter n darab n elemû kódszó tárolására alkalmas
- belátható, hogy a kódolás és a szindróma képzése megfelelõen visszacsatolt shift-regiszterekkel végezhetõ
- a ciklikus kódok matematikailag is jól kezelhetõk.

A ciklikus kód definíciójával kapcsolatban fontos megjegyezni, hogy egy kódszó ciklikus eltolásai általában nem állítják elõ az összes kódszót.

2. A ciklikus eltolás algebrai leírása

A ciklikus eltolás algebrai leírásához rendeljük a

$c=(c_{n-1}, c_{n-2}, ... c_2, c_1, c_0)$ sorozathoz a

$$c(x)= (c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + ,..... + c_2x^2+ c_1x+c_0) \qquad (1)$$

polinomot. Ez az összerendelés a polinomon belüli fokszámon keresztül tükrözi, õrzi a sorozaton belüli pozíciót: az x^j együtthatója (c_j) a sorozat jobbról számított (j+1)-ik eleme. Egy n elemû sorozathoz (n-1)-ed fokú polinom tartozik. Például az 5-öd fokú, bináris együtthatójú polinomok körében a

$c(x)=x^5+x$ polinom a (100010) sorozatot

míg a

$c(x)=x^4+x^3+1$ polinom a (011001) sorozatot írja le. Látjuk, hogy a polinom (lehetséges legmagasabb) fokszámának ismerete fontos, mert nélküle nem ismerhetõk fel a legbaloldalibb pozíció(k)ban lévõ "zérus" elem(ek). Be fogjuk látni, hogy egy c(x) polinommal leírt n elemû sorozat k lépéssel balra történõ ciklikus eltolásával kapott sorozatot leíró polinom az alábbiak szerint határozható meg:

$$\bar{c}(x)=(x^k c(x))\text{-mod-}(x^n+1) \qquad (2)$$

(Olvasd: $x^k c(x)$ modulo (x^n+1)). A modulo-polinom-algebra szabályai szerint a fenti kifejezés az $(x^k c(x))$ polinomnak az (x^n+1) polinommal való negatív kitevõt nem tartalmazó eredményû osztása utáni maradék, miközben a bináris együtthatókra a modulo-2 algebra szabályait kell alkalmazni.

Példa az egy lépéses ciklikus balra tolásra 4 elemû sorozatnál:

legyen $c=(1100)$, ekkor $c(x)=x^3+x^2$; és

$xc(x)=x^1c(x)=x^4+x^3$

Az elvégzendõ polinom osztáshoz célszerû feltüntetni a zérus együtthatójú polinom-tagokat is:

$$(1x^4+1x^3+0x^2+0x^1+0x^0):(x^4+1)=1$$
$$\underline{1x^4 \qquad\qquad\qquad 1x^0}$$
$$0x^4+1x^3+0x^2+0x^1+1x^0$$

(N.B.: az együtthatóknál alkalmazandó mod-2 algebra miatt (0-1) eredménye +1). Az osztás nem negatív kitevõvel tovább nem végezhetõ, a maradék tehát :

$$\bar{c}(x)=1x^3+0x^2+0x^1+1x^0=x^3+1,$$

Az ennek megfelelõ $\bar{c}=(1001)$ sorozat valóban a kiindulási c=(1100) sorozat ciklikusan eggyel balra történõ léptetésébõl származik.

A (2)-vel kapcsolatos szabályt elõször általánosan látjuk be (k=1)-re. Ha

$$c(x)=c_{n-1}x^{n-1}+c_{n-2}x^{n-2}+\ldots\ldots+c_0 \qquad (3)$$

akkor

$$xc(x)= (c_{n-1}x^n + c_{n-2},x^{n-2} + ...+ c_0x). \quad (4)$$

Ha ezt osztjuk $(x^n +1)$-gyel, akkor a polinom-osztás eredménye c_{n-1}, és a maradék:

$$\bar{c}(x)=xc(x) + c_{n-1}(x^n+1).$$

(Közönséges polinom osztásnál a maradék: $xc(x)-c_{n-1}(x^n+1)$, de most az együtthatókat a mod-2 algebra szerint kell kezelni, ezért "-" helyett "+" írható, és ezt a továbbiakban is mindíg igy fogjuk tenni).
Írjuk fel a $\bar{c}(x)$-et részletezve és célszerûen csoportosítva:

$$\bar{c}(x)=(c_{n-1}+ c_{n-1})x^n+ c_{n-2}x^{n-1} +.....+ c_0x + c_{n-1}$$

Ebben a kifejezésben az x^n együtthatója zérus (mod-2!), tehát

$$\bar{c}(x)=c_{n-2}x^{n-1} + ...+ c_0x + c_{n-1} \quad (6)$$

és a hozzátartozó

$$\bar{c}=(c_{n-2},..... c_0, c_{n-1}) \quad (7)$$

sorozat valóban a kiindulási (3) szerinti sorozat ciklikusan egyel balra való eltolása. A (2) szerinti szabályt k=1 esetére általánosan beláttuk. Az eljárást kellõ számban ismételve a szabály tetszõleges k-ra belátható!
A ciklikus eltolást leíró (2) kifejezést sokszor írják az alábbi módon:

$$\bar{c}(x)=\text{rem}\ \frac{x^k \cdot c(x)}{x^n +1} \quad (8)$$

ahol a "rem" a "remainder" (=maradék) szóra utal, és jelentése ugyanaz, mint a (2) egyenlettel kapcsolatban elmondottaké.

3. A ciklikus kódok alaptétele

Tétel: minden ciklikus (n, k) kódot egyértelmûen leír egy (n-k) -ad fokú, az

(x^n+1) -et maradék nélkül osztó g(x) u.n. generátor-polinom. (Megjegyzés: mivel (x^n+1) -et általában egynél több (n-k) -ad fokú polinom osztja maradék nélkül, ezért adott (n,k) számpároshoz is több ciklikus kód rendelhetõ.)

Mivel a kód a kódszavak összessége, e tétel azt jelenti, hogy a generátor-polinom az összes (2^k darab) kódszót meghatározza. Ennek belátásához kihasználjuk, hogy a ciklikus kód a lineáris kódok egy alosztálya. A lineáris kódot egyértelmûen leírja a generátor-mátrixa. Emlékeztetünk arra, hogy a generátor-mátrix sorai egymástól lineárisan független kódszavak, melyek lineáris kombinációi eredményezik a kódot (=a kódszavak összességét).

Lássuk be, hogy egy g(x) polinomból felépíthetõ egy **G** generátor -mátrix.
Tekintsük elõször a nem-szisztematikus esetet. Mivel **G** sorai n elemûek, azokat legfeljebb (n-1)-ed fokú polinomok írják le.
Legyen a legalsó sort leíró polinom $g_k(x)=g(x)$, majd felfelé haladva

$g_{k-1}(x)=xg(x)$, $g_{k-2}(x)=x^2g(x)$ ..... $g_1(x)=x^{k-1}g(x)$. (Vegyük észre, hogy ezzel a választással a generátor-mátrix sorai egymás ciklikus eltolásai). Mivel g(x) pontosan (n-k)-ad fokú, a fenti választással keletkezõ generátor-mátrix az alábbi alakú:

$$\mathbf{G} = \left[\begin{array}{cccc|c} 1 & g_{n-k-1} & \ldots\ldots & g_0 & 0\ldots\ldots 0 \\ & & & & \\ 0 & \ldots\ldots & 1 & & 0\ldots\ldots 0 \\ 0 & \ldots\ldots & 0 & g_{n-k-1} & g_0\ 0\ldots\ldots 0 \\ 0\ldots\ldots 0 & & 1 & g_{n-k-1}\ldots g_1 & g_0 \end{array}\right]$$

k n-k

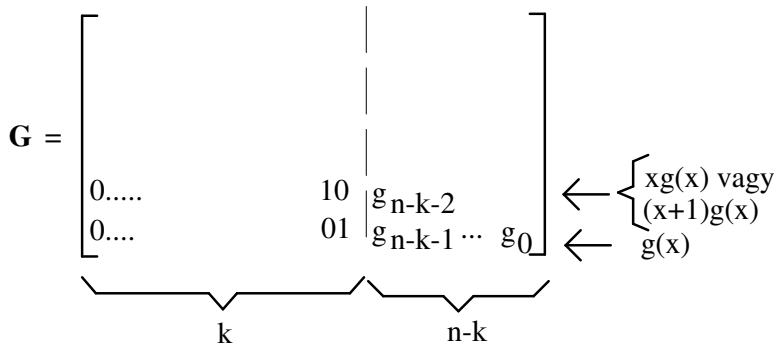
(Itt $g_i \in (0,1)$, a generátor-polinom x^{i+1} tagjának együtthatója.)
Látható, hogy a sorok lineárisan függetlenek, tehát valóban generátor-mátrixról van szó! Olyanról, amelynek (polinom alakban felírt) minden sora osztható g(x)-szel. Következésképpen a generátor-mátrix sorainak minden lineáris kombinációja is osztható g(x)-szel. Másképpen fogalmazva minden kódszó (pontosabban az azt leíró kódpolinom) felírható

$$c(x)=g(x)\ q(x) \qquad (9)$$

alakban. Mivel c(x) legfeljebb (n-1)-ed fokú, g(x) pedig pontosan (n-k)-ad fokú, q(x) legfeljebb (k-1)-ed fokú lehet. Bináris együtthatókkal éppen 2^k darab különbözõ q(x)

létezik, melyek g(x)-szel szorozva éppen 2^k darab különbözõ c(x)-et szolgáltatnak, azaz valóban kiadják az összes kód-polinomot. g(x) tehát meghatározza a kódot.

Térjünk át most a szisztematikus kód esetére, ahol, mint tudjuk, a generátor-mátrix bal oldali partíciója egy k x k méretû egység-mátrix. Legyen a generátor-mátrix alsó (k-adik) sora most is $g_k(x)=g(x)$. A (k-1)-ik sor akkor lehet $g_{k-1}(x)=xg(x)$ ha a g(x) -ben $g_{n-k-2}=0$, mert ekkor kialakul a bal partícióban az egységmátrix. Ha $g_{n-k-2}=1$, akkor az alábbi választás biztosítja az egységmátrix "kifejlõdését": $g_{k-1}(x)=(x+1)g(x)$.
A fentieket szemléltesse az alábbi generátor-mátrix:



A gondolatmenetet folytatva a generátor-mátrix (k-i) -edik sora (i=0,1,...(k-1)), tehát vagy

$$g_{(k-i)}(x)=g_{(k-i+1)}x$$

vagy

$$g_{(k-i)}(x)=g_{(k-i+1)}(x+1)$$

alakú. Kimondhatjuk tehát, hogy

$$g_{(k-i)}(x)=g(x)x^p(1+x)^q,$$

ahol (p+q)=i.

Fontos, hogy a generátor-mátrix sorai, és ezzel ezek kombinációi, tehát az összes kódszó osztható g(x)-szel. Itt is fennáll tehát (9), ennek összes következményével.

Láttuk tehát, hogy mind nem szisztematikus, mind szisztematikus kódnál g(x) a teljes kódot meghatározza.

Hátra van még annak taglalása, hogy a g(x) által meghatározott kód ciklikus-e. Ehhez be kell látni, hogy ha c(x) kódpolinom, akkor

$$\bar{c}(x) = \mathrm{rem}\frac{x \cdot c(x)}{x^n+1}$$

is kódpolinom, azaz osztható g(x)-szel. A korábbiakban már láttuk, hogy

$$\mathrm{rem}\frac{x\cdot c(x)}{x^n+1}=x\cdot c(x)+c_{n-1}x^n+1, \tag{10}$$

továbbá c(x) (és ezzel xc(x) is) osztható g(x)-szel. (10) akkor osztható g(x)-szel, ha (x^n+1) is osztható vele. Ezzel beláttuk, hogy a ciklikussághoz (x^n+1)-nek oszthatónak kell lenni g(x)-szel.

4. Ciklikus kódok kódolása

Legyen adva az u(x) polinommal meghatározott k hosszúságú (max (k-1)-ed fokú polinommal leírt) üzenet, és a g(x) generátor-polinom. Keressük a c(x) kódpolinomot.

A nem szisztematikus esetben (9)-bõl triviális, hogy

$$c(x)=g(x)u(x).$$

Szisztematikus kód esetén a kódszó elsõ k helyén az üzenet, azaz $x^{n-k}u(x)$ áll, és ezt követi a paritás rész:

$$c(x)=x^{n-k}u(x)+p(x) \tag{11}$$

Mivel a kódpolinomnak oszthatónak kell lenni g(x)-szel, fennáll, hogy

$$\mathrm{rem}\frac{x^{n-k}\cdot u(x)+p(x)}{g(x)}=0.$$

Tekintve, hogy p(x) max. (n-k-1)-ed fokú, és g(x) (n-k)-ad fokú, fennáll, hogy

$$p(x)=\mathrm{rem}\frac{x^{n-k}\cdot u(x)}{g(x)} \tag{12}$$

Ezzel egy igen egyszerû szabályt nyertünk a paritás-rész meghatározására. A teljes kódszó pedig:

$$c(x)=x^{n-k}\cdot u(x)+\mathrm{rem}\frac{x^{n-k}\cdot u(x)}{g(x)} \tag{13}$$

5. Szindroma meghatározása ciklikus kódoknál

Szoritkozzunk a szisztematikus ciklikus kódokra. Célszerû a vett n elemû polinomot k -elemû feltételezett üzenet-részre és (n-k) elemû feltételezett paritás részre bontani:

$$v(x) = \tilde{u}(x) + \tilde{p}(x) \tag{14}$$

(A "feltételezett" szó azt jelenti, hogy az elküldött c(x) kódpolinomnak akár az $x^{n-k}u(x)$ üzenet-része, akár a p(x) paritás része, akár mindkettõ meghibásodhatott.) A (14) szerinti felbontásban $\tilde{p}(x)$ fokszáma max. (n-k-1), $\tilde{u}(x)$ pedig max. (n-1) és min. (n-k)-ad fokú tagokat tartalmaz. A lineáris kódoknál megismertek szerint a vételnél képezni kell a megérkezett vett üzenetbõl a "vételi" paritást, $\approx{p}(x)$-et, és ezt kell összehasonlítani a "megérkezett" paritással, azaz $\tilde{p}(x)$-szel. A szindrómát e kettõ összehasonlítása adja:

$$s(x) = \tilde{p}(x) + \approx{p}(x) \tag{15}$$

A vételi paritást ugyanúgy kell képezni, mint a kódolásnál:

$$\approx{p}(x) = \mathrm{rem}\frac{\tilde{u}(x)}{g(x)} \tag{16}$$

(Itt $\tilde{u}(x)$ már az (n-1)-edik hatványnál kezdõdik, hisz a vett sorozat n elemû. Ezért nem kell x^{n-k}-val szorozni, mint azt (11)-nél még kellett.)

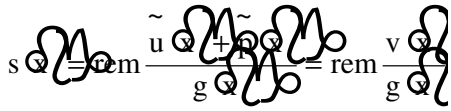
Mivel $\approx{p}(x)$ (n-k-1)-nél nem nagyobb fokszámú, ezért írható, hogy

$$\approx{p}(x) = \mathrm{rem}\frac{\approx{p}(x)}{g(x)}$$

A szindroma (15) alapján:

$$s(x) = \tilde{p}(x) + \approx{p}(x) = \mathrm{rem}\frac{\tilde{u}(x)}{g(x)} + \mathrm{rem}\frac{\tilde{p}(x)}{g(x)}$$

Kihasználva a fokszámok diszjunktitását:



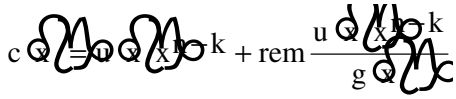
A szindromát tehát egyszerüen a vett n-es sorozathoz tartozó polinom és g(x) osztásának maradéka szolgáltatja.

6. Elméleti összefoglalás

Legyen az (n,k) ciklikus kódot meghatározó generátor-polinom g(x). Tudjuk, hogy g(x) az (x^n+1)-et maradék nélkül osztja.

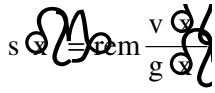
Szisztematikus kódokat tekintünk.

Az u(x) (k-1)-ed fokú üzenet hatására a



kódpolinom küldendõ a csatornára. Az átvitel során c(x) meghibásodhat, és v(x)-é változhat.

A vett v(x) -bõl a szindrómát az



összefüggéssel határozhatjuk meg.

7. Ciklikus kód a gyakorlatban

A ITU (International Telecommunication Union) hibajelzésre az alábbi kódot ajánlja

elsõ 4 bit: szolgálati bit,

következõ 240 vagy 480 vagy 960 bit:

üzenet bit,

következõ 16 bit: az elõzõeket "védõ" bitek, melyeket a

$$g(x)=x^{15}+x^{12}+x^5+1$$

generátor-polinommal képeznek.

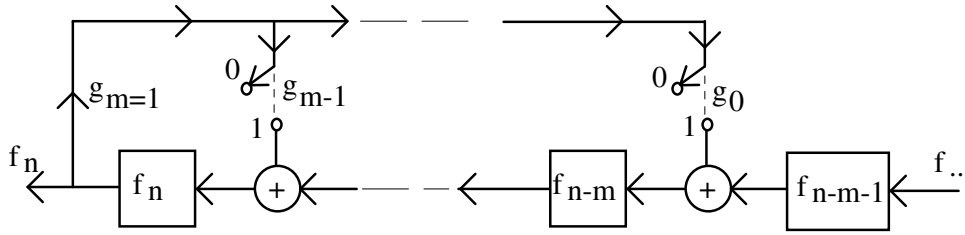
A kódot hibajelzésre (s(x)≠0) használják.

A kód garantáltan jelez minden páratlan számú hibát és minden 16-nál nem hosszabb hibacsomót (és nem garantáltan még sok más hibaalakzatot).

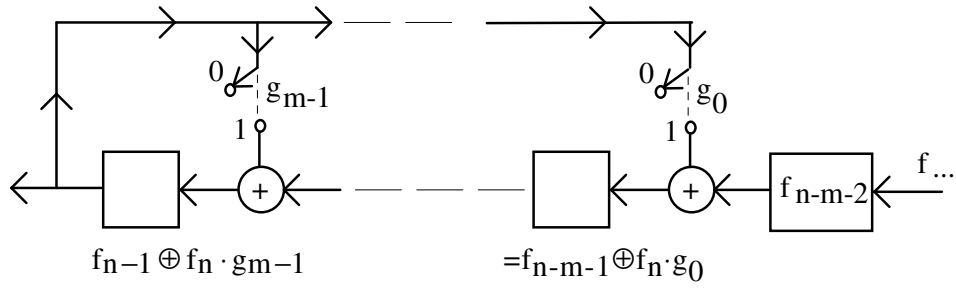
8. A visszacsatolt shift-register

A $g(x)=1\cdot x^m+g_{m-1}\cdot x^{m-1}+.....+g_0x^0$ osztó polinomnak megfelelõen visszacsatolt shift-regiszter (bináris együtthatójú polinomok esetén) polinom-osztást végez, ahol is a léptetési ütem elõtt az aktuális osztandó van a shift-regiszterben, a léptetéskor az osztás eredménye kilép a shift-regiszterbõl és az aktuális "maradék" lesz a shift-regiszter új tartalma
(1. ábra)

Ütem elõtt:



Ütem után



1.ábra