SZÉCHENYI ISTVÁN
EGYETEM
GYŐR

KÓDOLÁSELMÉLET

Nagy Szilvia

2. Lineáris blokk-kódok II.

2009.

A $GF(N^M)$ véges számtestekről

Egy {0, 1, 2, …, N^M–1} halmazon lehet úgy összeadást és szorzást definiálni, hogy véges testet alkosson.

Rendeljünk hozzá a halmaz minden elemé-hez egy-egyértelműen a $GF(P(t))$ $GF(N)$ feletti polinom-Galois-test elemei közül egyet, és úgy szorozzuk és adjuk össze a számokat, mint a nekik megfeleltetett polinomokat.

Így tudunk nem prím, hanem prímszám egész hatványa elemszámú véges számtestet létrehozni (1 bájt=8 bit)

A GF (N^M) véges számtestekről

Példa: másodfokú irreducíbilis polinom a $t^2 + t + 1$. A $GF(4) = GF(2^2)$ véges test elemei a 0, 1, 2, 3 számok, bináris alakban 0 0, 0 1, 1 0 és 1 1. Minden számhoz rendeljünk egy legfeljebb 2–1=1-fokú GF(2) feletti polinomot a következőképpen: ha a szám bináris alakja $a\ b$, akkor a hozzá rendelt polinom $a \cdot t + b$.

Az összeadás a következő esetekben triviális:

$$(0t+0)+(0t+0)=0t+0 \qquad (0t+0)+(1t+1)=1t+1$$

$$(0t+0)+(1t+0)=1t+0 \qquad (0t+0)+(0t+1)=0t+1$$

$$(1t+0)+(0t+1)=1t+1$$

A GF (N^M) véges számtestekről

Példa: $GF(4) = GF(2^2)$ véges test, a $t^2 + t + 1$ másodfokú irreducíbilis polinommal.

Összeadás esetén a mod 2 műveleteket is kell használni:

$$(1t+0)+(1t+0)=0t+0 \mod 2$$
$$(1t+0)+(1t+1)=0t+1 \mod 2$$
$$(1t+1)+(1t+1)=0t+0 \mod 2$$
$$(0t+1)+(0t+1)=0t+0 \mod 2$$
$$(0t+1)+(1t+1)=1t+0 \mod 2$$

A polinomos megfontolásokat csak néhány szorzás esetében kell használni:

A GF (N^M) véges számtestekről

$(0t+0)\cdot(0t+0)=0t+0 \quad \Rightarrow \quad 00\cdot 00=00,\ \text{vagy}\ 0\cdot 0=0$

$(0t+0)\cdot(0t+1)=0t+0 \quad \Rightarrow \quad 00\cdot 01=00,\ \text{vagy}\ 0\cdot 1=0$

$(0t+0)\cdot(1t+0)=0t+0 \quad \Rightarrow \quad 00\cdot 10=00,\ \text{vagy}\ 0\cdot 2=0$

$(0t+0)\cdot(1t+1)=0t+0 \quad \Rightarrow \quad 00\cdot 11=00,\ \text{vagy}\ 0\cdot 3=0$

$(1t+0)\cdot(0t+1)=1t \quad \Rightarrow \quad 10\cdot 01=10,\ \text{vagy}\ 2\cdot 1=2$

$(1t+0)\cdot(1t+0)=1t^2\equiv 1t+1 \bmod (t^2+t+1),$

mivel $t^2=t^2+t+1-t-1\equiv$

$\equiv t^2+t+1+t+1 \bmod 2$

$\Rightarrow \quad 10\cdot 10=11,\ \text{vagy}\ 2\cdot 2=3$

$(1t+0)\cdot(1t+1)=1t^2+1t\equiv 0t+1 \bmod (t^2+t+1),$

mivel $t^2+t=t^2+t+1-1\equiv$

$\equiv t^2+t+1+1 \bmod 2$

$\Rightarrow \quad 10\cdot 11=01,\ \text{vagy}\ 2\cdot 3=1$

A GF (N^M) véges számtestekről

Mivel az egység-elem a $0t+1$, az inverz-párok:
01—01
10—11

$(0t+0)\cdot(0t+0)=0t+0 \Rightarrow 00\cdot 00=00$, vagy $0\cdot 0=0$

$(0t+0)\cdot(0t+1)=0t+0 \Rightarrow 00\cdot 01=00$, vagy $0\cdot 1=0$

$(0t+0)\cdot(1t+0)=0t+0 \Rightarrow 00\cdot 10=00$, vagy $0\cdot 2=0$

$(0t+0)\cdot(1t+1)=0t+0 \Rightarrow 00\cdot 11=00$, vagy $0\cdot 3=0$

$(1t+0)\cdot(0t+1)=1t \Rightarrow 10\cdot 01=10$, vagy $2\cdot 1=2$

$(1t+0)\cdot(1t+0)=1t^2\equiv 1t+1 \bmod (t^2+t+1)$,

$\Rightarrow 10\cdot 10=11$, vagy $2\cdot 2=3$

$(1t+0)\cdot(1t+1)=1t^2+1t\equiv 0t+1 \bmod (t^2+t+1)$,

$\Rightarrow 10\cdot 11=01$, vagy $2\cdot 3=1$

$(0t+1)\cdot(0t+1)=0t+1 \Rightarrow 01\cdot 01=01$, vagy $1\cdot 1=1$

$(0t+1)\cdot(1t+1)=1t+1 \Rightarrow 01\cdot 11=11$, vagy $1\cdot 3=3$

$(1t+1)\cdot(1t+1)=1t^2+1\equiv 1t+0 \bmod (t^2+t+1)$,

$\Rightarrow 11\cdot 11=10$, vagy $3\cdot 3=2$

A $GF(N^M)$ véges számtestekről

Példa: $GF(4) = GF(2^2)$ véges test, a $t^2 + t + 1$ másodfokú irreducíbilis polinommal.

Összeadó- és szorzótábla:

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

A GF (N M) véges számtestekről

Példa: $GF(4) = GF(2^2)$ véges test, a $t^2 + t + 1$ másodfokú irreducíbilis polinommal.

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Hatványozás:

ϑ	ϑ^0	ϑ^1	ϑ^2	ϑ^3	ϑ^4	ϑ^5
1	**1**	**1**	**1**	**1**	**1**	**1**
2	**1**	**2**	2·2=**3**	3·2=**1**	1·2=**2**	2·2=**3**
3	**1**	**3**	3·3=**2**	3·2=**1**	1·3=**3**	2·3=**2**

Minden szám 0. hatványa 1, első hatványa önmaga

$\vartheta^{i+1} = \vartheta^i \cdot \vartheta$

Az első 1 eredménytől kezdve a hatványozás ismétlődik, mint GF(N)-ben

A GF (N M) véges számtestekről

A *GF*(2^8) bájtokat kezelni képes véges test *GF*(*P*(*t*)) polinom-Galois-testjének generáló irreducíbilis polinomja

$$P(t) = t^8 + t^4 + t^3 + t^2 + 1$$

Az $p_7\ p_6\ p_5\ p_4\ p_3\ p_2\ p_1\ p_0$ bináris alakú számhoz a következő, *GF*(2) feletti, legfeljebb hetedfokú polinomot rendeljük hozzá:

$$p(t) = p_7 t^7 + p_6 t^6 + p_5 t^5 + p_4 t^4 + p_3 t^3 + p_2 t^2 + p_1 t^1 + p_0$$

Vegyük észre, hogy a fenti hozzárendelés tulajdonképpen egy bináris vektor – bináris polinom hozzárendelés:

$$\underbrace{(p_7 \quad p_6 \quad p_5 \quad p_4 \quad p_3 \quad p_2 \quad p_1 \quad p_0)}_{\text{8 elemű bináris vektor}} \Leftrightarrow \underbrace{p(t)}_{\text{hetedfokú bináris polinom}}$$

BCH-kódok

Bose—Chaudhuri—Hocquenghem-kódnak nevezik azt a ν hibát javító, GF(N) feletti, $n=N^m+1$ kódszóhosszú, $g(t)$ generátorpolinomú ciklikus kódot, melyre $g(t)$ gyökei a GF(N^m) véges számtest ϑ^i, $i=1,2,\ldots,2\nu$ elemei.

A GF(N) a kódhoz tartozó kis test vagy az együtthatók teste, míg GF(N^m) a nagy test, vagy a gyökök teste.

Ha $N=2$, bináris a BCH-kód, ha $m=1$, R—S, ha pedig $\nu=1$ és $N=2$, bináris Hamming.

BCH-kódok

Bose—Chaudhuri—Hocquenghem-kódnak nevezik azt a ν hibát javító, GF(N) feletti, $n=N^m+1$ kódszóhosszú, $g(t)$ generátorpolinomú ciklikus kódot, melyre $g(t)$ gyökei a GF(N^m) véges számtest ϑ^i, $i=1,2,\ldots,2\nu$ elemei.

Belátható, hogy ha valamely $i_0 \geq 0$-ra $d>1$-re

$$g\left(\vartheta^{i_0}\right)=g\left(\vartheta^{i_0+1}\right)=g\left(\vartheta^{i_0+2}\right)=\ldots=g\left(\vartheta^{i_0+d-2}\right)=0,$$

akkor a kód minimális kódtávolsága legalább d.

BCH-kódok

A generátorpolinom:

- minden GF(N) feletti, n kódszóhosszú lineáris ciklikus kód $g(t)$ generátorpolinomja osztója t^n-1-nek
- t^n-1-nek minden nemtriviális osztópolinomja egy-egy GF(N) feletti, n kódszóhosszú, lineáris ciklikus kód generátorpolinomja

Ha $\deg(g(t))=n-k$, akkor a kód (n, k) paraméterű

BCH-kódok

A generátorpolinom:

Legyen GF(N) felett t^n-1 irreducíbilis felbontása:

$$t^n - 1 = f_1(t) \cdot f_2(t) \cdot \ldots \cdot f_s(t),$$

ekkor a lehetséges generátropolinomok száma 2^s-2.
(*s* db elemet vagy beleveszünk a generátorpolinomba, vagy nem: 2^s, az összes elemet tartalmazó és az egyetlen elemet sem tartalmazó szorzat nem kell)

BCH-kódok

A generátorpolinom:

A R—S-kódoknál beláttuk, hogy tetszőleges GF(Q) test felett

$$t^{Q-1}-1=(t-\vartheta_1)\cdot(t-\vartheta_2)\cdot\ldots\cdot(t-\vartheta_{Q-1}),$$

ahol ϑ_i a GF(Q) test nem 0 elemei.

Vegyük az $n=N^m-1$, primitív szóhosszú kódokat GF(N^m)-en (a gyökök testén).

Ekkor minden ϑ_j GF(N^m)-beli elem valamely $f_i(t)$ gyöke is egyben a GF(N)-ben

$$t^n-1=f_1(t)\cdot f_2(t)\cdot\ldots\cdot f_s(t),$$

BCH-kódok

A generátorpolinom:

Mivel $f_i(t)$ irreducíbilis és gyöke ϑ_j, logikus lenne, hogy $f_i(t) = (t - \vartheta_i)$, ha $\vartheta_i \in GF(N)$ lenne. Ehelyett azonban csak annyit tudunk mondani, hogy az $f_i(t)$ a legkisebb fokszámú olyan polinom, amely tartalmazza ϑ_j –t.

Minimálpolinom: egy $\vartheta_j \in GF(N^m)$ testelem GF(N)-beli minimálpolinomja az a legkisebb fokszámú irreducíbilis polinom, amelynek ϑ_j a gyöke.

A BCH-kódhoz GF(N^m) -beli elemek GF(N) feletti minimálpolinomjaira van szükség.

BCH-kódok

A generátorpolinom:

Minimálpolinomok konstruálása:

Ha egy $f(t)$ polinom egy $\vartheta \in GF(N^m)$ szám $GF(N)$-beli minimálpolinomja, akkor $f(t)$ gyökei:

$$\left\{\vartheta, \vartheta^N, \vartheta^{N^2}, \vartheta^{N^3}, \ldots, \vartheta^{N^{\sigma-1}}\right\}$$

ahol σ az a legkisebb szám, melyre $\vartheta^\sigma = \vartheta$.

A fenti halmaz tartalmazza ϑ **konjugált elemeit**.

BCH-kódok

A generátorpolinom:

Minimálpolinomok konstruálása:

Ha egy $f(t)$ polinom egy $\vartheta \in GF(N^m)$ szám $GF(N)$-beli minimálpolinomja, akkor $f(t)$ gyökei:

$$\left\{\vartheta, \vartheta^N, \vartheta^{N^2}, \vartheta^{N^3}, \ldots, \vartheta^{N^{\sigma-1}}\right\}$$

ahol σ az a legkisebb szám, melyre $\vartheta^\sigma = \vartheta$.

Így $GF(N^m)$ felett meg tudjuk adni a minimálpolinomot, azt kifejtjük $GF(N^m)$-ben, és az így kapott nem gyöktényezős alakot visszaírjuk $GF(N)$ –be.

BCH-kódok

Példa: minimálpolinomok konstruálása

GF(4)-ben N=2-re, m=2-re $t^{N^m}-1=t^3-1$

GF(2)-ben a megfelelő felbontás:

$$t^3-1=f_1(t)\cdot f_2(t)=(t-1)(t^2+t+1)$$

GF(4)-ben:

$$t^3-1=(t-1)(t-2)(t-3)=$$

$$=(t-\vartheta_1)(t-\vartheta_2)(t-\vartheta_2{}^2)$$

Mivel ha pl. $\vartheta_2=2$

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Reed—Solomon-kódok $GF(N^M)$ felett

Reed—Solomon kódokat lehet nem csak prím, hanem prímhatvány elemszámú véges test felett is definiálni a $GF(N)$ esettel analóg módon.

A különbségek:

- $GF(N^M)$ összeadó- és szorzótábla
- $GF(N^M)$ hatványok
- a ϑ generáló elemnek $GF(N^M)$-ben kell n-ed-rendűnek lennie.

Matematikai kitérő –

Fourier-transzformálás véges testeken

Legyen a $\mathbf{c}=(c_0, c_1, \ldots, c_{n-1})$ $GF(N^M)$-beli n komponensű vektor

$\mathbf{C}=(C_0, C_1, \ldots, C_{n-1}) \in (GF(N^M))^n$ Fourier-transzformáltjának komponensei a

$$C_j = \sum_{i=0}^{n-1} c_i \cdot \vartheta^{ij}$$

képlet szerint állnak elő, ϑ a véges test n-edrendű eleme.

Szokás a $\mathbf{C}$ Fourier-transzformáltat $F\{\mathbf{c}\}$-ként írni és a $\mathbf{c}$ **spektrum**ának nevezni.

Matematikai kitérő – Fourier-transzformálás véges testeken

Példa: számoljuk ki a **c**=(3 0 1 4) $GF(5)$-beli 4 komponensű vektor Fourier-transzformáltjának komponenseit ϑ=3-mal:

$$C_0 = \sum_{i=0}^{3} c_i \cdot 3^{i\cdot 0} = 3\cdot 1 + 0\cdot 1 + 1\cdot 1 + 4\cdot 1 = 8 \equiv 3 \mod 5$$

$$C_1 = \sum_{i=0}^{3} c_i \cdot 3^{i\cdot 1} = 3\cdot 1 + 0\cdot 3 + 1\cdot 4 + 4\cdot 2 = 15 \equiv 0 \mod 5$$

$$C_2 = \sum_{i=0}^{3} c_i \cdot 3^{i\cdot 2} = 3\cdot 1 + 0\cdot 3^2 + 1\cdot 4^2 + 4\cdot 2^2 =$$

$$= 3\cdot 1 + 0\cdot 4 + 1\cdot 1 + 4\cdot 4 = 20 \equiv 0 \mod 5$$

$$C_3 = \sum_{i=0}^{3} c_i \cdot 3^{i\cdot 3} = 3\cdot 1 + 0\cdot 3^3 + 1\cdot 4^3 + 4\cdot 2^3 =$$

$$= 3\cdot 1 + 0\cdot 2 + 1\cdot 4 + 4\cdot 3 = 19 \equiv 4 \mod 5$$

Matematikai kitérő – Fourier-transzformálás véges testeken

A Fourier-transzformációnak van inverz művelete:

$$c_i = n^{-1} \sum_{i=0}^{n-1} C_j \cdot \vartheta^{-ij}$$

ahol n^{-1} az n-nek a $GF(N^M)$ véges testen belüli inverze.
Bináris esetben, azaz ha $N=2$, $n^{-1}=1$ (ha n páratlan).

Matematikai kitérő – Ciklikus konvolúció

Legyen a $\mathbf{t}=(t_0, t_1, \ldots, t_{n-1})$ és $\mathbf{u}=(u_0, u_1, \ldots, u_{n-1})$ két $GF(N^M)$-beli n komponensű vektor. Az $\mathbf{s}=\mathbf{t} * \mathbf{u}$ **ciklikus konvolúció**ja az az $\mathbf{s}=(s_0, s_1, \ldots, s_{n-1}) \in (GF(N^M))^n$ vektor, melynek komponensei:

$$s_j = n^{-1} \sum_{k=0}^{n-1} t_{(j-k) \bmod n} \cdot u_k \qquad j = 0,1,\ldots,n-1.$$

A ciklikus konvolúcióra érvényes a **konvolúciós tétel**: Ha az $\mathbf{s}$, $\mathbf{t}$, $\mathbf{u}$ vektorok Fourier-transzformáltjai rendre $\mathbf{S}$, $\mathbf{T}$, $\mathbf{U}$, és a vektorok komponensei között fennáll, hogy $s_i = t_i \cdot u_i$,

akkor a spektrum vektorokra igaz, hogy

$$\mathbf{S} = \mathbf{T} * \mathbf{U},$$

Matematikai kitérő – Ciklikus konvolúció

A **konvolúciós tétel** belátása: az **s** vektorok Fourier-transzformáltjának, **S**-nek az *i*-edik komponense

$$S_j = \sum_{i=0}^{n-1} s_i \cdot \vartheta^{ij} = \sum_{i=0}^{n-1} (t_i \cdot u_i)\vartheta^{ij} =$$

behelyettesítve **u**-t, mint **U**-nak az inverz-Fourier-transzformáltját

$$= \sum_{i=0}^{n-1} t_i \cdot \left(n^{-1} \sum_{k=0}^{n-1} U_k \vartheta^{-ik} \right) \vartheta^{ij} = n^{-1} \sum_{k=0}^{n-1} U_k \cdot \underbrace{\left(\sum_{i=0}^{n-1} t_i \cdot \vartheta^{i(j-k)} \right)}_{T_{j-k}} =$$

$$= n^{-1} \sum_{k=0}^{n-1} U_k \cdot T_{j-k \bmod n} =$$

$$= (\mathbf{T} * \mathbf{U})_j .$$

ha $j-k<0$, akkor az n-nel vett osztás utáni maradékát kell venni

Matematikai kitérő – Ciklikus konvolúció

Példa: adjuk meg az **a**=(3 0 1 4) és a **b**=(2 0 2 1) vektorok konvolúcióját GF(5) felett. (n=4, $4^{-1} \equiv 4 \mod 5$.)

$$(\mathbf{a}*\mathbf{b})_0 = 4^{-1}\sum_{k=0}^{3} a_{(0-k) \bmod 4} \cdot b_k =$$

$$= 4(a_0b_0 + a_3b_1 + a_2b_2 + a_1b_3) =$$

$$= 4(3\cdot 2 + 4\cdot 0 + 1\cdot 2 + 0\cdot 1) = 32 \equiv 2 \mod 5$$

$$(\mathbf{a}*\mathbf{b})_1 = 4(a_1b_0 + a_0b_1 + a_3b_2 + a_2b_3) =$$

$$= 4(0\cdot 2 + 3\cdot 0 + 4\cdot 2 + 1\cdot 1) = 33 \equiv 3 \mod 5$$

$$(\mathbf{a}*\mathbf{b})_2 = 4(a_2b_0 + a_1b_1 + a_0b_2 + a_3b_3) =$$

$$= 4(1\cdot 2 + 0\cdot 0 + 3\cdot 2 + 4\cdot 1) = 36 \equiv 1 \mod 5$$

$$(\mathbf{a}*\mathbf{b})_3 = 4(a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3) =$$

$$= 4(4\cdot 2 + 1\cdot 0 + 0\cdot 2 + 3\cdot 1) = 35 \equiv 0 \mod 5$$

Matematikai kitérő – Ciklikus konvolúció

Legyen ϑ a $GF(N^M)$ test n-edrendű eleme.

Egy $\mathbf{c} \in (GF(N^M))^n$ vektor **spektrum-polinomja** a $\mathbf{C}=(C_0, C_1, \ldots, C_{n-1})$ spektrumához rendelt legfeljebb $n-1$-edfokú polinom:

$$C(t) = C_0 + C_1 \cdot t + C_2 \cdot t^2 + \ldots + C_{n-1} \cdot t^{n-1}.$$

Matematikai kitérő – Ciklikus konvolúció

A $\vartheta \in GF(N^M)$ n-edrendű elem i-edik hatványa, ϑ^i akkor és csak akkor lehet gyöke egy $c(t)$ polinomnak, ha a polinomhoz tartozó vektor **C** spektrumában az i-edik elem nulla:

$$C_i = 0.$$

Bizonyítás: ha ϑ^i gyöke $c(t)$-nek, akkor $c(\vartheta^i) = 0$. Kifejtve:

$$0 = c\left(\vartheta^i\right) = c_0 + c_1\vartheta^i + c_2\vartheta^{2i} + \ldots c_{n-1}\vartheta^{(n-1)i} =$$

$$= \sum_{j=0}^{n-1} c_j \vartheta^{ij}$$

ami pont C_i.

Matematikai kitérő – Ciklikus konvolúció

Hasonlóképpen: a $\vartheta \in GF(N^M)$ n-edrendű elem i-edik hatványa, ϑ^i akkor és csak akkor lehet gyöke egy $C(t)$ spektrumpolinomnak, ha az eredeti **c** vektor i-edik komponense nulla:

$$c_i = 0.$$

A bizonyítás az előző állítás belátásához hasonló.

A Reed—Solomon-kódok spektruma

Legyen a Reed—Solomon-kód generátorpolinomja $g(t)$, a kódolandó üzenet polinomja $b(t)$, a hozzárendelt kódszópolinom $c(t)$. A $c(t)$ $n-1$-edfokú, $b(t)$ $k-1$-edfokú, $g(t)$ pedig $n-k-1$-edfokú. Az $n-1$-edfokú polinomok között a $b(t)$-nek és $g(t)$-nek az utolsó együtthatói nullák.

Mindhárom polinom származtatható n komponensű vektorokból is:

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

$$\mathbf{b} = (b_0, b_1, \ldots, b_{k-1}, \underbrace{0, \ldots, 0}_{n-k \text{ db}})$$

$$\mathbf{g} = (g_0, g_1, \ldots, g_{n-k}, \underbrace{0, \ldots, 0}_{k \text{ db}})$$

A Reed—Solomon-kódok spektruma

A Reed—Solomon-kód $c(t)$ kódszópolinomjai a következőképpen állíthatók elő:

$$c(t) = g(t) \cdot b(t)$$

A polinomszorzás definíciója szerint az i-edfokú együttható:

$$c_i = \sum_{j=0}^{n-1} g_{i-j} \cdot b_j$$

ami **g**∗**b** i-edik komponense. Tehát **c** = **g**∗**b**.

A konvolúciós tétel szerint ekkor a vektorok spektruma között a következő összefüggés áll fenn:

$$C_i = G_i \cdot B_i$$

A Reed—Solomon-kódok spektruma

Legyen a Reed—Solomon-kódot generáló és egyben a Fourier- transzformációt definiáló *n*-edrendű $GF(N^M)$-beli elem ϑ. A generátorpolinomnak, s így minden kódszópolinomnak gyöke ϑ 1-től $n-k$-adikig terjedő hatványa.

Így minden kódszóvektor spektrumának az 1-től $n-k$-adikig terjedő indexű komponense nulla:

$$C_i = 0, \qquad i = 1, 2, \ldots, n-k.$$

A Reed—Solomon-kódok spektruma

Minden kódszóvektor spektrumának az 1-től $n-k$-adikig terjedő indexű komponense nulla:

$$C_i = 0, \qquad i = 0, 1, 2, \ldots, n-k-1.$$

Ez a tény lehetővé teszi a kódszavak spektrumukon keresztül történő avagy **transzformációs** definiálását:

a $(b_0, b_1, \ldots, b_{k-1})$ üzenethez rendelt kódszó spektrumának

- az első $n-k$ eleme 0
- az utolsó k eleme $b_0, b_1, \ldots, b_{k-1}$

Transzformációs R—S-kódok

Transzformációs kódolás:

Hibajavítás:

Ha $i_1,\ldots,i_\nu$ helyeken van hiba, a hibavektor $\Delta\mathbf{c}$, a hibapolinom:

$$\Delta c(t) = \Delta c_{i_1} t^{i_1} + \Delta c_{i_2} t^{i_2} + \ldots + \Delta c_{i_\nu} t^{i_\nu}$$

Transzformációs R—S-kódok

Hibajavítás:

Ha $i_1,\ldots,i_\nu$ helyeken van hiba, a hibavektor $\Delta\mathbf{c}$, a hibapolinom:

$$\Delta c(t) = \Delta c_{i_1} t^{i_1} + \Delta c_{i_2} t^{i_2} + \ldots + \Delta c_{i_\nu} t^{i_\nu}$$

A hibahelypolinom:

$$L(t) = 1 + L_1 t^1 + L_2 t^2 + \ldots + L_\nu t^\nu =$$

$$= \prod_{j=1}^{\nu} \left(1 - \vartheta^{i_j} t\right)$$

Transzformációs R—S-kódok

Hibajavítás:

Ha **v** = **c** + Δ**c**, a Fourier-trf: **V**=**C**+Δ**C**.

Mivel **C** első n−k eleme 0, ott Δ**C**-k adottak:

$$\Delta C_\ell = V_\ell, \quad \ell = 1,\ldots n-k$$

A hibahelypolinom gyökei a hibahely-lokátorok ϑ^{i_j} -k, ezeknek a helyén **I**-ben 0-k vannak, ha

I=$\mathbf{F}^{-1}$(**L**)

L az L(t) polinomnak megfeleltethető n hosszúságú vektor

Transzformációs R—S-kódok

Hibajavítás:

Ahol $l_i = 0$, csak ott $\Delta c_i \neq 0$, így

$$\Delta c_i l_i = 0, \quad i = 0,1,\ldots n-1$$

A konvolúciós tétellel

$$\mathbf{L} * \Delta\mathbf{C} = 0$$

amiből az ismert ΔC-kre a

$$\sum_{j=0}^{\nu} L_j \Delta C_{i-j} = 0, \qquad i = \nu, \nu+1, \ldots, 2\nu-1$$

Ezt az egyenletrendszert kell minimális fokszámú $L(t)$-re megoldani.

Transzformációs R—S-kódok

Hibajavítás:

Ismerjük ΔC_i-ket, $i=1,\ldots,n-k$-ra, rekurziós képlettel:

$$\Delta C_j = -\left(L_1 \Delta C_{j-1} + L_2 \Delta C_{j-2} + \ldots + L_v \Delta C_{j-v}\right)$$

(Megoldható léptetőregiszteres visszacsatolt áramkörrel)

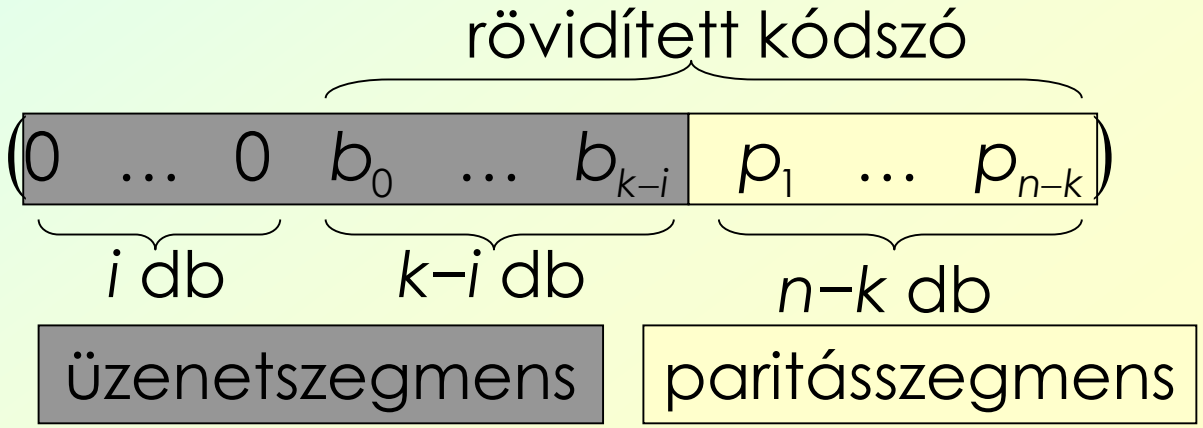
Kódtranszformációk

Rövidítés:

A **c** szisztematikus kódszavak közül csak az *i* db nullával kezdődő üzenetekből keletkezettekkel foglalkozunk, és elhagyjuk belőlük a nullákat, így (*n*−*i*, *k*−*i*) kódokat kapunk.

Kódtávolság legalább akkora, mint az eredeti, (*n*,*k*) kódé volt.

Cél: a feladat paramétereihez való igazítás



Kódtranszformációk

Paritáskarakter:

Egy (n,k) bináris kódból $(n+1,k)$ kódot készít

$$\hat{\mathbf{G}} = \begin{pmatrix} & & 1 \\ & \mathbf{G} & \vdots \\ & & 1 \end{pmatrix}$$

$$\hat{\mathbf{H}}^T = \begin{pmatrix} & & 1 \\ & \mathbf{H}^T & 1 \\ & & \vdots \\ 0 & \dots \quad 0 & 1 \end{pmatrix}$$

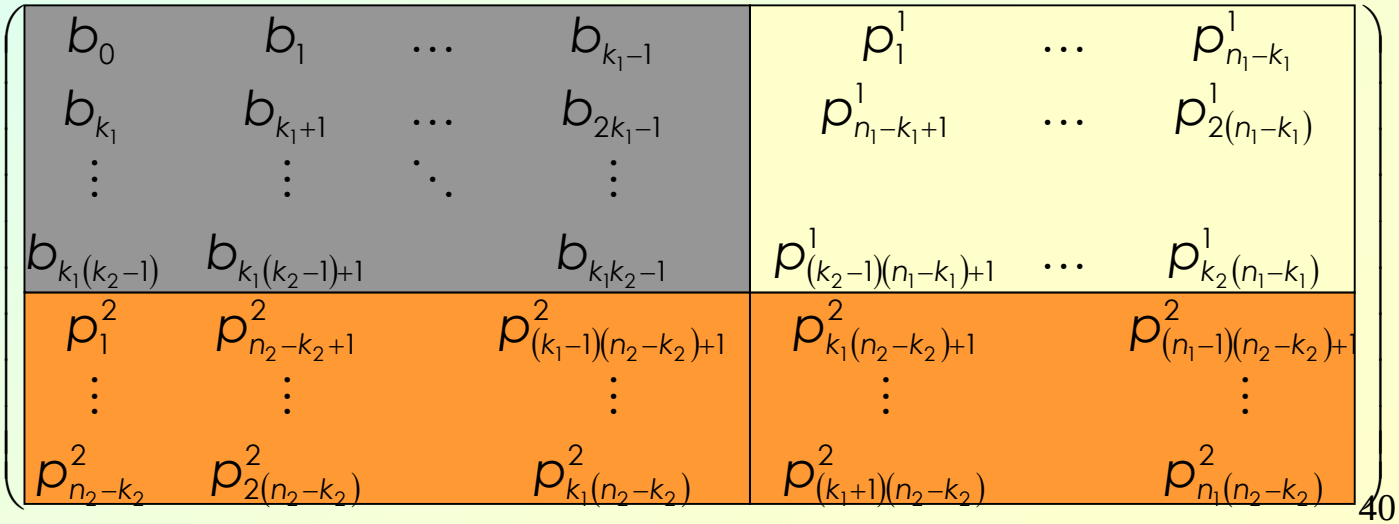
Kódtávolság az eredeti d_{min}, illetve $d_{min}+1$, páros, illetve páratlan d_{min} esetén

Kódtranszformációk

Szorzatkód:

Egy (n_1,k_1) és egy (n_2,k_2) kódból $n_1 \times n_2$ blokkot készít, melynek bal felső része tartalmazza a $k_1 \times k_2$ -s üzenetblokkot szisztematikus esetben.

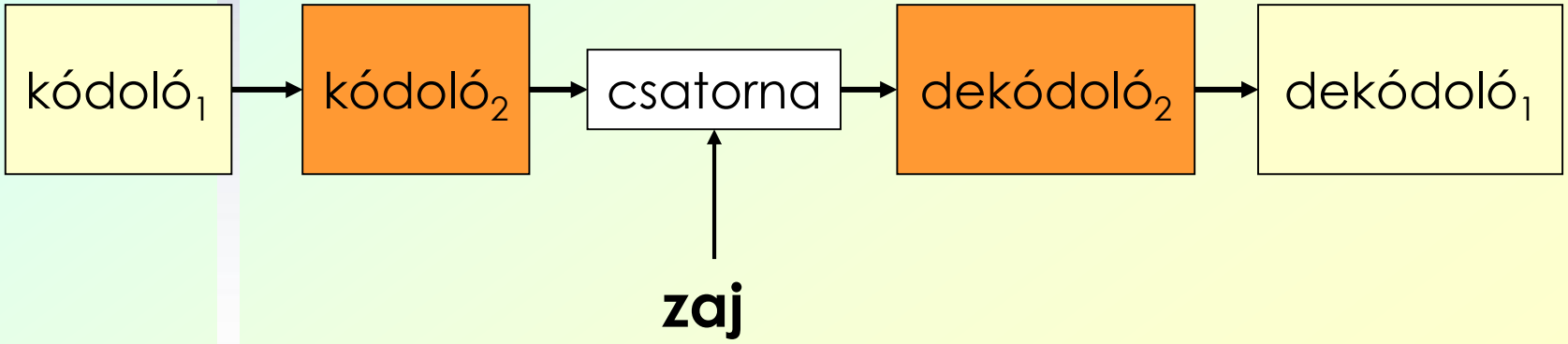
- Az első k_1 oszlop az első kóddal
- A kapott k_2 sor a második kóddal



Kódtranszformációk

Kaszkádkód:

Egy (n_1,k_1) és egy (n_2,n_1) kódoló egymás után fűzése



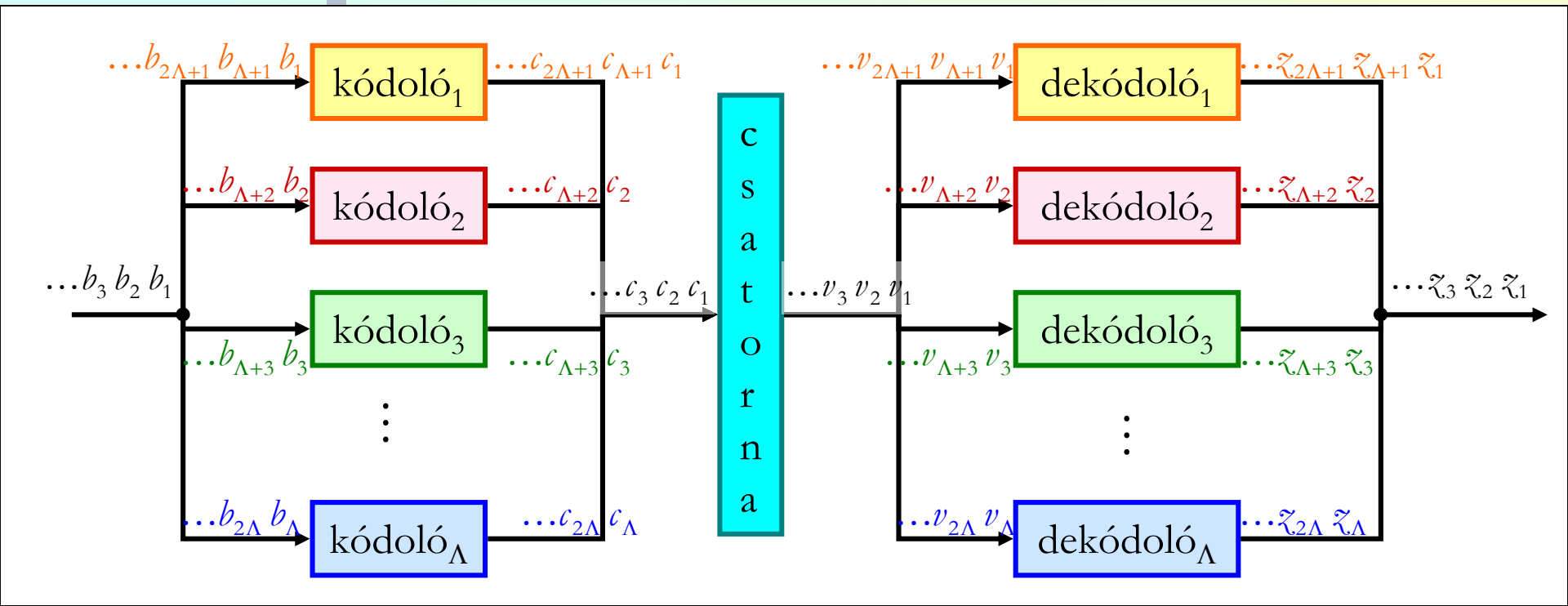
Hibacsomók – kódátfűzések

Egy szimbólumsorozatban több, egymás után előforduló hibából álló sorozat a **hibacsomó**. Egy hosszabb hibacsomó javítása csak rendkívül hosszú kódszavakkal és főleg hosszú paritásszegmenssel lehetséges – hacsak szét nem bontjuk valahogy.

Azokat az eljárásokat, amelyek során a kódolandó, illetve dekódolandó szimbólumsorozatot úgy módosítják, hogy az esetleg előforduló hibacsomók szétoszoljanak több kódszó között, **kódátfűzés**nek vagy interleavingnek hívjuk.

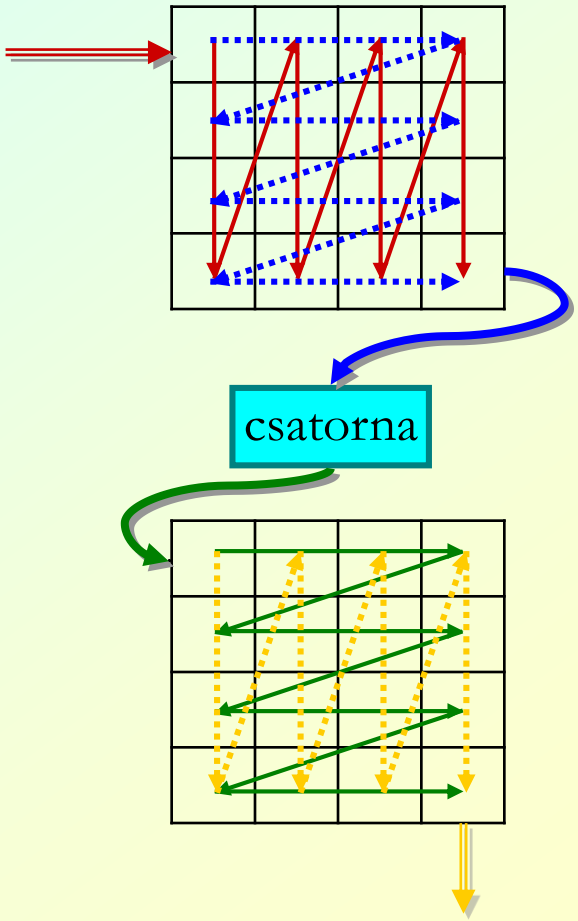
Többutas kódátfűzés

- több kódoló és dekódoló kell
- lassabb (az órajel frekvenciájának Λ-adrészével működő), bonyolultabb kódolási eljárások is alkalmazhatók
- a hibacsomó hossza egy-egy ágon Λ-adrészére csökken



Blokkos kódátfűzés

1. a blokkba oszlopfolytonosan írja be a kódolt üzenetet
2. sorfolytonosan olvassa ki és adja a csatornára
3. vevő sorfolytonosan tölti fel a mátrixát
4. oszlopfolytonosan olvassa ki
5. majd dekódolja.



Blokkos kódátfűzés

Egy $D \times D$-s blokk esetén

- a hibacsomó D-edrészére csökken.
- Nagyobb a memóriaigény de csak egy kódoló és dekódoló szükséges.
- Hosszabb ideig tart, még akkor is, ha két blokkal dolgozik, az egyiket tölti, a másikat olvassa ki.