SZÉCHENYI ISTVÁN
EGYETEM
GYŐR

KÓDOLÁSELMÉLET

Nagy Szilvia

1. Lineáris blokk-kódok

Shannon hírközlési modellje

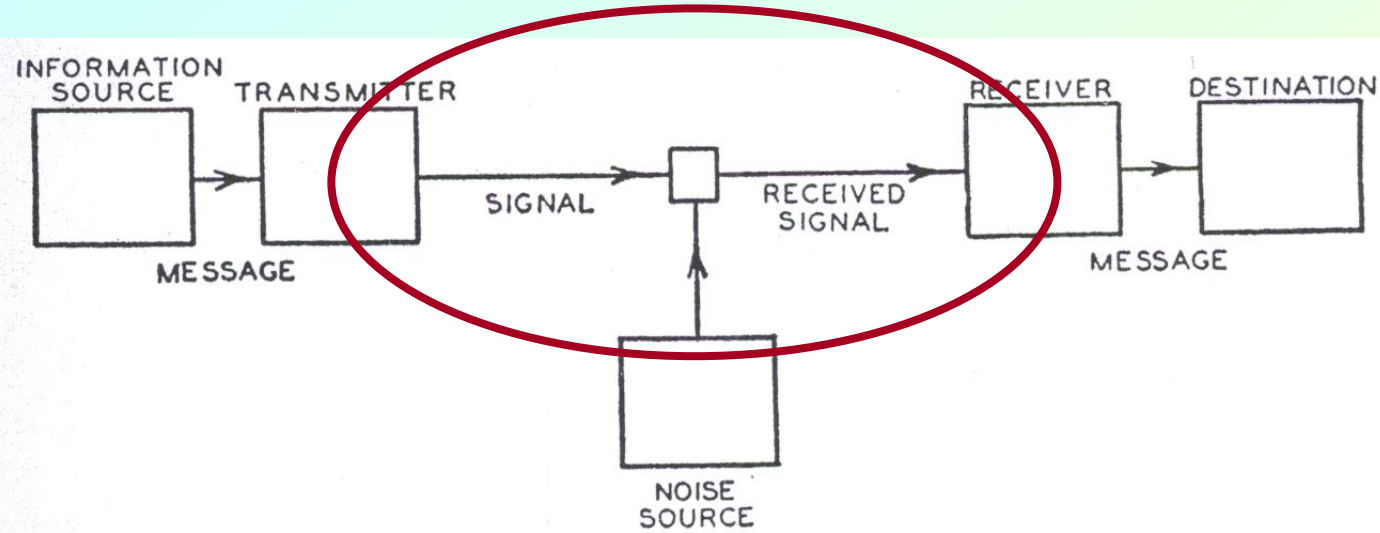

Fig. 1—Schematic diagram of a general communication system.

információforrás
adó

csatorna – zajforrás

vevő
rendeltetési hely

Kódok halmaza, csatornakódolás

A C^n tér azon K részhalmazát, amelyet a kódszavak alkotnak, **kód**nak nevezik.

- Csatornakódolás:

  $F : B^l \mapsto K$

- Dekódolás:
  - döntés:

    $G : C^n \mapsto K$
  - a kódolás inverze:

    $F^{-1} : K \mapsto B^l$

Kódtávolság, javítható hibák száma

Egy *K* kód **kódtávolság**a:

$$d_{\min} = \min_{\mathbf{c}\neq\mathbf{c}';\ \mathbf{c},\mathbf{c}'\in K} d(\mathbf{c},\mathbf{c}')$$

a kódszavak közötti Hamming-távolság minimuma.

Hibajelzés lehetséges, ha a **c** kódszavunkból keletkezett **v** nem egy másik érvényes kódszó: $\mathbf{v}\notin K$. Ha ν a hibák száma, akkor $\nu < d_{\min}$ hibát lehet biztosan jelezni.

Törléses hibák javítása: $\nu < d_{\min}$

Egyszerű hibák javítása: $\nu < (d_{\min}-1)/2$

Lineáris blokk-kódok

Blokk-kódok: a tömörített üzenet *k* hosszúságú blokkjaihoz rendelnek egy-egy *n* hosszúságú kódszót. ($n>k$)

Lineáris blokk-kódok olyan blokk-kódok, melyekre a kódszavak halmaza lineáris tér: *K* altere C^n-nek.

Ha *K* lineáris tér (*k* dimenziós), akkor $\exists \{ \mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{k-1} \}$ bázisrendszere, és minden $\mathbf{c}_i$ kódszó kifejthető e bázisrendszer szerint:

$$\mathbf{c}_i = \sum_{j=0}^{k-1} \alpha_{ij} \mathbf{g}_j$$

Lineáris blokk-kódok

Minden $\mathbf{c}_i$ kódszó kifejthető a bázisrendszer szerint:

$$\mathbf{c}_i = \sum_{j=0}^{k-1} \alpha_{ij}\, \mathbf{g}_j$$

Ha a $\mathbf{g}_j$-k adottak, akkor a $\mathbf{c}_i$-ket jól leírják a kifejtési együtthatóikból álló sorvektorok:

$$\vec{\alpha}_i = \begin{pmatrix} \alpha_{i0} & \alpha_{i1} & \dots & \alpha_{in} \end{pmatrix}$$

A bázisrendszer választása még adott K mellett sem egyértelmű. Más-más bázisrendszerhez más és más együtthatók tartoznak.

Generátormátrix

A $\{ \mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{k-1} \}$ bázisvektorokból az alábbi szabály szerint épített **G** mátrix a kód **generátormátrix**a:

$$\mathbf{G} = \begin{pmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{pmatrix} = \begin{pmatrix} g_{00} & g_{01} & \cdots & g_{0(n-1)} \\ g_{10} & g_{11} & \cdots & g_{1(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ g_{(k-1)0} & g_{(k-1)1} & \cdots & g_{(k-1)(n-1)} \end{pmatrix}$$

Az üzenet $(b_{i0} \quad b_{i1} \quad \ldots \quad b_{i\,k-1})$ együtthatóiból a G mátrix segítségével megkapható a kódszó:

$$\mathbf{c}_i = \mathbf{b}_i \cdot \mathbf{G}$$

Generátormátrix

A *k* darab választott bázisvektor mindegyike *n* hosszúságú, ugyanakkor egy *k*-dimenziós teret írnak le (ehhez k komponens is elég lenne): *n*−*k* szimbólum felesleges, **redundáns**. Ezek a szimbólumok nem tartalmaznak új információt, őket használjuk fel arra, hogy a kódszavak Hamming-távolsága nagy legyen, ők teszik lehetővé a hibajelzést és -javítást.

Csatornakódolás során az entrópia csökken.

Paritásmátrix, szindróma

A csatorna kimenetén kapott **v** vektorról el kell dönteni, hogy kódszó-e. Ha a **v** vektor paritásellenőrző $\mathbf{H}^T$ mátrixszal (paritásmátrixszal) vett szorzata **0**, akkor **v** kódszó, ha nem, akkor $\mathbf{v} \notin K$.

A **v** vektor $\mathbf{H}^T$ paritásmátrixszal vett szorzata a vektor **szindróm**aja:

$$\mathbf{s} = \mathbf{v} \cdot \mathbf{H}^T = \begin{cases} \mathbf{0}, & \text{ha } \mathbf{v} \in K \\ \text{nem } \mathbf{0}, & \text{ha } \mathbf{v} \notin K \end{cases}$$

A $\mathbf{c}_i = \mathbf{b}_i \cdot \mathbf{G}$ kódszavakra tehát:

$$\mathbf{0} = \mathbf{s} = \mathbf{c}_i \cdot \mathbf{H}^T = \mathbf{b}_i \mathbf{G} \cdot \mathbf{H}^T \qquad \forall i\text{-re, így} \quad \mathbf{G} \cdot \mathbf{H}^T = \mathbf{0}.$$

Ezt használják fel $\mathbf{H}^T$ előállítására.

Szisztematikus kódok paritásmátrixa

A szisztematikus kódok generátormátrixa egyszerű szerkezetű:

$$\mathbf{G}_{k\times n} = \left[\, \mathbf{I}_{k\times k} \;\middle|\; \mathbf{P}_{k\times(n-k)} \,\right]$$

Paritásmátrixuk szintén egyszerű és a **G** mátrixból könnyen előállítható:

$$\mathbf{H}^T{}_{n\times(n-k)} = \begin{bmatrix} \mathbf{P}'_{k\times(n-k)} \\ \hline \mathbf{I}_{(n-k)\times(n-k)} \end{bmatrix}$$

Belátható, hogy **P=–P'**

Hibavektorok és mellékosztályaik

Legyen a vett **v** vektorunk

$$\mathbf{v} = \mathbf{c} + \Delta\mathbf{c}$$

ahol $\Delta\mathbf{c}$ a **hibavektor**. A **v** szindrómája ekkor

$$\mathbf{s} = \mathbf{v} \cdot \mathbf{H}^T = (\mathbf{c} + \Delta\mathbf{c}) \cdot \mathbf{H}^T = \mathbf{0} + \Delta\mathbf{c} \cdot \mathbf{H}^T$$

ami pont a $\Delta\mathbf{c}$ szindrómája.

A $\Delta\mathbf{c}_i$ hibavektor által a K kódból generált M_i **mellékosztály** azon $\mathbf{v}_k$ vektorok halmaza, amelyek a $\mathbf{c}_k \in K$ kódszavakból jönnek létre. Az M_i mellékosztály összes elemének a szindrómája azonos: megegyezik $\Delta\mathbf{c}_i$ szindrómájával.

Hibavektorok és mellékosztályaik

A $\Delta\mathbf{c}_i$ hibavektorok egy része előáll egy másik $\Delta\mathbf{c}_j$ hibavektorból egy kódszó hozzáadásával:

$$\Delta\mathbf{c}_i = \mathbf{c}_k + \Delta\mathbf{c}_j$$

Ezeknek a szindrómája és egyben a mellékosztálya azonos lesz.

Mivel a mellékosztályok elemei egy hibavektorból a kódszavak hozzáadásával állnak elő, a mellékosztályok tartalmazzák az összes azonos szindrómájú hibamintázatot.

Hibavektorok és mellékosztályaik

A **v** vektorok tehát több $\Delta\mathbf{c}_{ij}$-ből is előállnak, más és más $\mathbf{c}_j$ kódszóból.
(Mindig csak egy mellékosztály $\Delta\mathbf{c}_{ij}$-iből! A szindróma azonos.)
El kell dönteni, melyik kódszóba javítsuk őket. Abba a kódszóba javítjuk **v**-t, amelyiktől a legkisebb a Hamming-távolsága.

Egy $\mathbf{a}=(a_0, a_1, \ldots, a_{n-1})$ **vektor** $w(\mathbf{a})$ **súlya** a nem nulla a_i komponenseinek a száma.

A legkisebb súlyú $\Delta\mathbf{c}_{ij}$ hibamintázat eredményezi az eredeti **c** vektortól a legkisebb Hamming-távolságbeli eltérést.

Hibavektorok és mellékosztályaik

A legkisebb súlyú $\Delta\mathbf{c}_{ij}$ hibamintázat eredményezi az eredeti **c** vektortól a legkisebb Hamming-távolságbeli eltérést.
A **v** vektor szindrómájához tartozó mellékosztályból a legkisebb súlyút, $\Delta\mathbf{c}_{ij0}$t, vesszük hibavektornak, ezzel javítjuk ki **v**-t: $\mathbf{c}_{becsült}=\mathbf{v}-\Delta\mathbf{c}_{ij0}$

A mellékosztályok legkisebb súlyú elemeit a mellékosztályok **vezető elemei**nek nevezik.

Hamming-kódok

A Hamming-kódok olyan perfekt kódok, amelyek egy egyszerű hibát képesek kijavítani.

Bináris Hamming-kódok esetén mind a tömörített üzenet, mind a kódszavak csak 0-kból és 1-esekből állnak: $\mathbf{b} \in \{0,1\}^k$, $\mathbf{c} \in \{0,1\}^n$.

A csatorna által a **v**-ben létrehozott (egyetlen) hiba csak 1 nagyságú lehet, csak a pozíciója kérdéses.

Bináris Hamming-kód

Legyen a paritásmátrix

$$\mathbf{H}^T = \begin{pmatrix} \mathbf{h}_0 \\ \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_{n-1} \end{pmatrix}, \qquad \text{ahol } \mathbf{h}_i = \begin{pmatrix} h_{i0} & h_{i1} & \dots & h_{i\,n-k} \end{pmatrix}$$

Egy hiba esetén $\Delta\mathbf{c}$ egyetlen 1-est (és $n–k–1$ db nullát) tartalmaz, ha az az egyetlen 1-es az i-edik helyen van,

$$\mathbf{s} = \Delta\mathbf{c} \cdot \mathbf{H}^T = \mathbf{h}_i$$

Véges számtestekről

Egy számokból álló $GF(N)=\{0, 1, \ldots, N-1\}$ halmaz véges test, vagy Galois-test, ha értelmezve van a t és $u \in V$ elemei között egy összeadás ($t + u \in GF(N)$) és egy szorzás ($t \cdot u \in GF(N)$) amelyekre:

1.)

a) $t + u = u + t$ (az összeadás kommutatív)

b) ha $s \in GF(N)$, $(s + t) + u = s + (t + u)$ (asszociatív)

c) $\exists\, 0$, melyre $\forall\, t \in GF(N)$: $t + 0 = t$

d) $\forall\, t \in GF(N)$-re $\exists\, -t$, melyre $t + (-t) = 0$

Véges számtestekről

Egy számokból álló $GF(N)=\{0, 1, \ldots, N-1\}$ halmaz véges test, vagy Galois-test, ha értelmezve van a t és $u \in V$ elemei között egy összeadás ($t + u \in GF(N)$) és egy szorzás ($t \cdot u \in GF(N)$) amelyekre:

2.)

a) $t \cdot u = u \cdot t$ (a szorzás kommutatív)

b) ha $s \in GF(N)$, $(s \cdot t) \cdot u = s \cdot (t \cdot u)$ (asszociatív)

c) $\exists$ 1, melyre $\forall\, t \in GF(N)$: $t \cdot 1 = t$

d) $\forall\, t \in GF(N)$-re $\exists\, t^{-1}$, melyre $t \cdot (t^{-1}) = 1$

Véges számtestekről

Egy számokból álló $GF(N)=\{0, 1, \ldots, N-1\}$ halmaz véges test, vagy Galois-test, ha értelmezve van a t és $u \in V$ elemei között egy összeadás ($t + u \in GF(N)$) és egy szorzás ($t \cdot u \in GF(N)$) amelyekre:

3.)

a) ha $s \in GF(N)$, $s \cdot (t + u) = s \cdot t + s \cdot u$
(+ és · disztributív)

b) $\forall\, t \in GF(N)$: $t \cdot 0 = 0$.

Véges számtestekről

Példa: a {0,1} halmaz a következő szorzó és összeadó táblával:

+	**0**	**1**
0	0	1
1	1	0

·	**0**	**1**
0	0	0
1	0	1

Ez a hagyományos összeadás és szorzás azzal a kitétellel, hogy ha az eredmény kivezetne a halmazból, akkor a 2-vel való osztás utáni **maradékát** vesszük.

Más *N* prímszámok maradékosztálya is véges számtestet alkot modulo *N* műveletekkel

Véges számtestekről

Inverz és ellentett elemet az 5-ös esethez hasonlóan:

- $-t = N - t$
- A t^{-1}: $t \cdot GF(N)=\{t \cdot 0 + t \cdot 1 + t \cdot 2 + \ldots + t \cdot (N-1)\}$ számok mindegyike más és más, így közülük az egyik biztosan 1 (az t inverze, amelyikkel összeszorozva az 1-et adja).

Véges számtestekről

Egy $t \in GF(N)$ elem **hatványait** is lehet értelmezni, mint önmagával vett szorzatait: Rekurzív definícióval t n-edik hatványa:

- adott $t^1 = t$
- amíg $i < n$
- $t^{i+1} = t^i \cdot t$.

Véges számtestekről

A $t \in GF(N)$ elem **rend**je

$$\min_{t^\rho = 1} \rho$$

Az 1 rendje 1, a 0-nak nincs rendje.

Az a $t \in GF(N)$ elem, amelyre t első $N-1$ hatványa mind különböző a véges test **primitívelem**e.

Minden $s \in GF(N)$ előáll a primitívelem hatványaként.

Véges számtestekről

Nézzük a *GF*(7) elemeinek szorzótábláját, inverzeit, hatványait, rendjeit és azt, hogy hogy állnak elő a primitívelemből:

	0	1	2	3	4	5	6	inverz
0	0	0	0	0	0	0	0	–
1	0	1	2	3	4	5	6	1
2	0	2	4	6	8≡1	10≡3	12≡5	4
3	0	3	6	9≡2	12≡5	15≡1	18≡4	5
4	0	4	8≡1	12≡5	16≡2	20≡6	24≡3	2
5	0	5	10≡3	15≡1	20≡6	25≡4	30≡2	3
6	0	6	12≡5	18≡4	24≡3	30≡2	36≡1	6

Minden „≡” jel modulo 7 ekvivalenciát jelent.

Véges számtestekről

Nézzük a *GF*(7) elemeinek szorzótábláját, inverzeit, hatványait, rendjeit és azt, hogy hogy állnak elő a primitívelemből:

t	t^2	t^3	t^4	t^5	t^6	rend	$5^?$
1	1	1	1	1	1	1	6
2	4≡4	8≡1	16≡2	32≡4	64≡1	3	4
3	9≡2	27≡6	81≡4	243≡5	729≡1	6	5
4	16≡2	64≡1	256≡4	1024≡2	4096≡1	3	2
5	25≡4	125≡6	625≡2	3125≡3	15625 ≡1	6	1
6	36≡1	216≡6	1296≡1	7776≡6	46656 ≡1	2	3

Minden „≡” jel modulo 7 ekvivalenciát jelent.

Nembináris Hamming-kód

Nembináris Hamming-kódok esetén mind a tömörített üzenet, mind a kódszavak csak 0-n és 1-esen kívül más egész számokat is tartalmaznak: $\mathbf{b} \in \{0, 1, \ldots, N-1\}^k$, $\mathbf{c} \in \{0, 1, \ldots, N-1\}^n$, ahol N prím.

A csatorna által a **v**-ben létrehozott (egyetlen) hiba nem csak 1 nagyságú lehet, így a pozícióján kívül a nagyságát is ki kell találni.

Írjuk fel a paritásmátrixot itt is

$$\mathbf{H}^T = \begin{pmatrix} \mathbf{h}_0 \\ \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_{n-1} \end{pmatrix}, \qquad \text{ahol } \mathbf{h}_i = \begin{pmatrix} h_{i0} & h_{i1} & \ldots & h_{i\,n-k} \end{pmatrix}$$

alakban.

Nembináris Hamming-kód

Egyetlen hiba esetén a $\Delta\mathbf{c}$ hibavektor egyetlen nem nulla elemet (és $n–k–1$ db nullát) tartalmaz. Legyen a hiba nagysága Δc, és legyen az i-edik pozícióban. Ekkor a szindróma:

$$\mathbf{s} = \Delta\mathbf{c} \cdot \mathbf{H}^T = \Delta c \cdot \mathbf{h}_i$$

Ha $\mathbf{H}^T$ sorainak – $\mathbf{h}_i$-knek – első nem nulla eleme 1, akkor a szindróma első nem nulla eleme pont Δc lesz.

A szindrómát a hiba nagyságával elosztva kapott új vektor ($\mathbf{s}/\Delta c$) $\mathbf{H}^T$-beli helye adja meg a hiba pozícióját.

Ciklikus kódok – ciklikus eltolás

Egy $\mathbf{c}=(c_0, c_1, \ldots, c_{n-2}, c_{n-1})$ vektor **ciklikus eltoltján** az

$$S\mathbf{c} = (c_{n-1} \quad c_0 \quad c_1 \quad \ldots \quad c_{n-2})$$

vektort értjük.

Egy K kód **ciklikus**, ha minden $\mathbf{c} \in K$-ra $S\mathbf{c} \in K$:
minden kódszó ciklikus eltoltja is kódszó.

Rendeljünk az egyes kódszavakhoz polinomokat a következő szabály szerint.

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

$$\Updownarrow$$

$$c(t) = c_0 + c_1 t + c_2 t^2 + \ldots + c_{n-1} t^{n-1}$$

Ebben a reprezentációban a ciklikus eltolás t-vel való modulo $(t^n - 1)$ szorzás.

Generátorpolinom

Polinomos reprezentációban egy lineáris ciklikus kód kódszavai között van egy minimális fokszámú, de nem nulladrendű, amelynek a legmagasabb fokú kitaevője 1. Ez a polinom a kód **generátorpolinom**ja, fokszáma $n–k$. A generátorpolinom jele $g(t)$

Egy $c_i(t)$ polinom akkor és csak akkor kódszópolinom, ha a $g(t)$ maradék nélküli osztója $c_i(t)$-nek, így

$$c_i(t) = \alpha_i(t) \cdot g(t)$$

Generátormátrix

A generátormátrix előáll a generátorpolinom együtthatóiból, minden sora a generátorpolinom egy-egy ciklikus eltoltja:

$$\mathbf{G} = \begin{pmatrix} g_0 & g_1 & \dots & g_{n-k-1} & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{n-k-1} & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & g_0 & g_1 & \dots & g_{n-k-1} & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & g_0 & g_1 & \dots & g_{n-k-1} & 1 & 0 \\ 0 & 0 & \dots & 0 & 0 & g_0 & g_1 & \dots & g_{n-k-1} & 1 \end{pmatrix}$$

k db nulla

Paritásellenőrző polinom

A generátorpolinom mindig osztója t^n-1-nek.

A (t^n-1)-nek minden irreducíbilis osztópolinomja egy-egy ciklikus kód generátorpolinomja.

A $g(t)$ generátorpolinomú ciklikus kódok paritásellenőrző polinomja

$$h(t)=\frac{t^n-1}{g(t)}$$

Ezzel a polinommal megszorozva minden érvényes kódszó 0-t ad (moduló t^n-1)

$$c_i(t)h(t)=\alpha_i(t)\cdot g(t)\cdot h(t)=$$

$$=\alpha_i(t)\cdot\left(t^n-1\right)\equiv 0 \mod \left(t^n-1\right)$$

Paritásellenőrző polinom

A nem nulla szindrómájú vektorokat táblázat alapján szokták javítani a legkisebb súlyú, velük azonos szindrómát adó hibapolinomokkal.

A táblázat a következőképpen épül fel:

- Meghatározzák az összes lehetséges hibapolinom szindrómáját
- Csoportosítják az azonos szindrómájú hibamintázatokat (mellékosztályok).
- Kiválasztják közülük a minimális súlyút, ezt a szindrómák szerint táblázatba foglalják.
- Az adott szindróma esetén mindig a szindróma hibamintázatai közül a minimális súlyúval javítanak.

Szisztematikus generálás

Megjegyzés: A ciklikus kódok generálhatók szisztematikusan, azaz minden ciklikus kódhoz létezik egy neki megfelelő szisztematikus kód szisztematikus generátormátrixszal.

A szisztematikus generátormátrix előáll egy ciklikus kód nem szisztematikus generátormátrixából úgy, hogy végrehajtjuk rajta a Gauss-elimináció lépéseit (balról jobbra, hogy egységmátrixot kapjunk a bal oldalra)

Példa:

t^3+t^2+1 polinomból előállt mátrix:

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Szisztematikus generálás

Adott üzenethez természetesen a két kód esetén más és más kódszó fog tartozni, csak a kódszavak halmaza lesz azonos.

A szisztematikusan generált ciklikus kódok azonban könnyen dekódolhatók.

Reed—Solomon-kódok

Legyen $t_0, t_1, t_2, \ldots, t_{n-1}$ a $GF(N)$ véges test n darab különböző eleme, $n<N$.

A Reed—Solomon-kódok a $\mathbf{b}=(b_0, b_1, \ldots, b_{k-1})$ üzenethez azt a $\mathbf{c}=(c_0, c_1, \ldots, c_{n-1})$ kódszót rendelik hozzá, amelynek a c_i komponensei a

$$c_i = b(t_i), \qquad b(t) = b_0 + b_1 t + b_2 t^2 + \ldots + b_{k-1} t^{k-1}$$

formula szerint állnak elő. A t_i generálóelemek kiválasztása határozza meg a kódot.

Generálóelemek

A kód generátormátrixa:

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ t_0 & t_1 & \dots & t_{n-1} \\ t_0^{\,2} & t_1^{\,2} & \dots & t_{n-1}^{\,2} \\ \vdots & \vdots & \ddots & \vdots \\ t_0^{\,k-1} & t_1^{\,k-1} & \dots & t_{n-1}^{\,k-1} \end{pmatrix}$$

Maximális távolság

Egy (n, k) paraméterű Reed—Solomon-kód kódtávolsága $d_{min}=n-k+1$, azaz a kódra a Singleton-korlátban egyenlőség teljesül, tehát a Reed—Solomon-kódok maximális távolságúak (MDS-ek).

Ha $d_{min}=n-k+1$, akkor a kód legfeljebb
$n-k$ hibát tud jelezni,
$n-k$ törléses és
$(n-k)/2$ egyszerű hibát tud javítani.

Egyetlen generálóelem

Legyen $\vartheta \in GF(N)$ rendje legalább n. ($\vartheta \neq 0$)
Ekkor ϑ-nak a 0-diktól az $n-1$-edikig terjedő hatványai mind különbözőek lesznek, ezek lehetnek a Reed—Solomon-kódot létrehozó $t_i \in GF(N)$ véges testbeli elemek:

$$t_0 = \vartheta^0 = 1; \quad t_1 = \vartheta^1 = \vartheta; \quad t_2 = \vartheta^2; \quad \ldots \quad t_{n-1} = \vartheta^{n-1}.$$

A generátormátrix ezekkel:

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \vartheta & \vartheta^2 & \ldots & \vartheta^{n-1} \\ 1 & \vartheta^2 & \vartheta^4 & \ldots & \vartheta^{(n-1)2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \vartheta^{k-1} & \vartheta^{2(k-1)} & \ldots & \vartheta^{(n-1)(k-1)} \end{pmatrix}$$

Egyetlen generálóelem

A $\vartheta \in GF(N)$ generáló elemmel definiált Reed—Solomon-kód a $\mathbf{b}=(b_0, b_1, \ldots, b_{k-1})$ üzenethez azt a $\mathbf{c}=(c_0, c_1, \ldots, c_{n-1})$ kódszót rendeli hozzá, amelynek a c_i komponensei:

$$c_i = b\left(\vartheta^i\right) = b_0 + b_1\vartheta^i + b_2\vartheta^{i\cdot 2} + \ldots + b_{k-1}\vartheta^{i(k-1)}$$

avagy

$$c_i = \sum_{j=0}^{k-1} b_j \cdot \left(\vartheta^i\right)^j, \qquad i = 0,1,2,\ldots,n-1.$$

Egyetlen generálóelem

A **c** kódszóhoz, melynek komponensei:

$$c_i = \sum_{j=0}^{k-1} b_j \cdot \left(\vartheta^i\right)^j, \qquad i = 0,1,2,\ldots,n-1.$$

a ciklikus kódoknál megszokott módon polinomokat lehet rendelni:

$$c(t) = c_0 + c_1 t + c_2 t^2 + \ldots + c_{n-1} t^{n-1} = \sum_{i=0}^{n-1} c_i t^i$$

ami c_i kifejezését beírva:

$$c(t) = \sum_{i=0}^{n-1} \sum_{j=0}^{k-1} b_j \vartheta^{ij} \cdot t^i.$$

alakú lesz.

Paritásegyenletek

Helyettesítsünk be a $\vartheta^{\ell} \in GF(N)$ elemeket $\ell = 0, 1, \ldots, n-k$ -ra a Reed—Solomon-kód egyes kódszavaihoz rendelt polinomokba:

$$c\left(\vartheta^{\ell}\right) = \sum_{i=0}^{n-1}\sum_{j=0}^{k-1} b_j \vartheta^{ij} \cdot \left(\vartheta^{\ell}\right)^j = \sum_{j=0}^{k-1} b_j \sum_{i=0}^{n-1} \vartheta^{i(j+\ell)}$$

Mivel $0 < \ell \le n-k$, és $0 \le j \le k-1$, $0 < j+\ell \le n-1$. Mivel ϑ legalább n-edrendű elem $GF(N)$-ben,

$$\vartheta^{j+\ell} \neq 1$$

Így a mértani sor összegképlete szerint:

$$\sum_{i=0}^{n-1} \vartheta^{i(j+\ell)} = \sum_{i=0}^{n-1} \left(\vartheta^{(j+\ell)}\right)^i = \frac{\left(\vartheta^{(j+\ell)}\right)^n - 1}{\vartheta^{(j+\ell)} - 1} = \frac{\left(\vartheta^{n}\right)^{(j+\ell)} - 1}{\vartheta^{(j+\ell)} - 1}$$

Paritásegyenletek

$$c\left(\vartheta^{\ell}\right)=\sum_{i=0}^{n-1}\sum_{j=0}^{k-1}b_j\vartheta^{ij}\cdot\left(\vartheta^{\ell}\right)^{i}=\sum_{j=0}^{k-1}b_j\sum_{i=0}^{n-1}\vartheta^{i(j+\ell)}$$

A mértani sor összegképlete szerint:

$$\sum_{i=0}^{n-1}\vartheta^{i(j+\ell)}=\sum_{i=0}^{n-1}\left(\vartheta^{(j+\ell)}\right)^{i}=\frac{\left(\vartheta^{(j+\ell)}\right)^{n}-1}{\vartheta^{(j+\ell)}-1}=\frac{\left(\vartheta^{n}\right)^{(j+\ell)}-1}{\vartheta^{(j+\ell)}-1}$$

mivel $\vartheta^n = 1$, a számláló 0, így

$c(\vartheta^{\ell}) = 0$, $\ell = 1, \ldots, n-k$ -ra.

Ezek a Reed—Solomon-kód **paritásegyenletei**.

Paritásegyenletek

A $c(\vartheta^{\ell}) = 0$, $\ell = 1, 2, \ldots, n-k$ **paritásegyenletek** alternatív leírása:

$$\sum_{j=0}^{n-1} c_j \left(\vartheta^{\ell}\right)^j = 0, \qquad \ell = 1,2,\ldots, n-k.$$

A $c(\vartheta^{\ell}) = 0$ azt jelenti, hogy minden egyes kódszó polinomjában szerepelnek a

$$\left(t - \vartheta^{\ell}\right), \qquad \ell = 1,2,\ldots, n-k.$$

gyöktényezők, azaz minden egyes kódszó előáll a

$$c_j(t) = \beta_j(t) \cdot \prod_{\ell=0}^{n-k} \left(t - \vartheta^{\ell}\right), \qquad j = 0,1,2,\ldots, k-1.$$

alakban.

Paritásegyenletek

A Reed—Solomon-kódok minden egyes kódszava előáll a

$$c_j(t) = \beta_j(t) \cdot \prod_{\ell=0}^{n-k} \left(t - \vartheta^\ell\right), \qquad j = 0,1,2,\ldots,k-1.$$

alakban.

A Reed—Solomon-kódok tehát tulajdonképpen **ciklikus kódok**, melyeknek a generátorpolinomja

$$g(t) = \prod_{\ell=0}^{n-k} \left(t - \vartheta^\ell\right).$$

Generátorpolinom

A Reed—Solomon-kódunkhoz rendelhető, a $(t^n - 1)$ polinommal meghatározott **ciklikus kód** generátorpolinomja tehát gyöktényezős alakban:

$$g(t) = (t - \vartheta) \cdot (t - \vartheta^2) \cdot \ldots \cdot (t - \vartheta^{n-k})$$

A $(t^n - 1)$ „alap"-polinom gyökei a ϑ^i-ek, i=0, 1, …, n–1, tehát $g(t)$ gyökei $t^n - 1$-nek is gyökei lesznek, így $g(t)$ valóban osztója lesz $t^n - 1$-nek.

A ϑ^i-ek közül az 1-től n–k-ig terjedő hatványokból alkotott gyöktényezők alkotják a generátorpolinomot: a többi adja a paritásellenőrző polinomot.

Paritásellenőrzés

A **paritásellenőrző polinom** tehát :

$$h(t) = \frac{t^n - 1}{g(t)} =$$

$$= \left(t - \vartheta^{n-k+1}\right) \cdot \left(t - \vartheta^{n-k+2}\right) \cdot \ldots \cdot \left(t - \vartheta^{n-1}\right) \cdot \left(t - \vartheta^{n}\right)$$

A $\vartheta \in GF(N)$ generálóelemmel definiált Reed—Solomon-kód **paritásellenőrző mátrixa**

$$\mathbf{H}^T = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \vartheta & \vartheta^2 & \cdots & \vartheta^{n-k} \\ \vartheta^2 & \vartheta^4 & \cdots & \vartheta^{(n-k)\cdot 2} \\ \vdots & \vdots & \ddots & \vdots \\ \vartheta^{n-1} & \vartheta^{2(n-1)} & \cdots & \vartheta^{(n-k)\cdot(n-1)} \end{pmatrix}$$

belátható, hogy $\mathbf{G}\cdot\mathbf{H}^T=0$, így az állítás ellenőrizhető.

A hibák javítása

A paritásellenőrző mátrix:

$$\mathbf{H}^T = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \vartheta & \vartheta^2 & \cdots & \vartheta^{n-k} \\ \vartheta^2 & \vartheta^4 & \cdots & \vartheta^{(n-k)\cdot 2} \\ \vdots & \vdots & \ddots & \vdots \\ \vartheta^{n-1} & \vartheta^{2(n-1)} & \cdots & \vartheta^{(n-k)\cdot(n-1)} \end{pmatrix}$$

Ebből a szindróma: $\mathbf{s} = \Delta\mathbf{c} \cdot \mathbf{H}^T$

Elemenként kifejtve: $s_j = \sum_{i=0}^{n-1} \Delta c_i \vartheta^{ij}$

Ismerve a szindróma $n-k$ elemét, ennek az egyenletrendszernek kell a legkisebb súlyú $\Delta\mathbf{c}$ megoldását megkeresni

Törléses hibák javítása

Törléses hibák esetén ismerjük azt, hogy $\Delta\mathbf{c}$ mely komponensei biztosan 0-k és melyek nem azok.

A 0 elemek a $\mathbf{H}^T$ bármely oszlopával összeszorozva 0 járulékot adnak, így a velük azonos sorszámú sorokat törölhetjük $\mathbf{H}^T$-ből.

Összesen legfeljebb $n-k$ nem nulla elem van $\Delta\mathbf{c}$-ben, így legfeljebb $n-k$ sora marad a csonkolt $\mathbf{H}^T$-nek. Eleve csak $n-k$ oszlopa volt, így négyzetes mátrix marad.

Legyen a csonkolt paritásellenőrző mátrix $\tilde{\mathbf{H}}^T$

Húzzuk ki $\Delta\mathbf{c}$-ből is a 0 elemeket, az így kapott vektor: $\Delta\tilde{\mathbf{c}}$

Törléses hibák javítása

A kapott

$$\Delta\tilde{\mathbf{c}} \cdot \tilde{\mathbf{H}}^T = \mathbf{s}$$

avagy

$$\begin{aligned}
\tilde{H}_{00} \cdot \Delta\tilde{c}_0 + \ldots + \tilde{H}_{n-k-1\,0} \cdot \Delta\tilde{c}_{n-k-1} &= s_0 \\
\tilde{H}_{01} \cdot \Delta\tilde{c}_0 + \ldots + \tilde{H}_{n-k-1\,1} \cdot \Delta\tilde{c}_{n-k-1} &= s_1 \\
&\vdots \\
\tilde{H}_{0\,n-k-1} \Delta\tilde{c}_0 + \ldots + \tilde{H}_{n-k-1\;n-k-1} \Delta\tilde{c}_{n-k-1} &= s_{n-k-1}
\end{aligned}$$

$n-k$ változós egyenletrendszer megoldható.

Egyszerű hibák javítása

A Reed—Solomon-kódok $\nu<(n-k)/2$ egyszerű hibát tudnak javítani.

Tegyük fel, hogy az ℓ-edik helyen van hiba. Ekkor minden

$$s_j = \sum_{i=0}^{n-1} \Delta c_i \vartheta^{ij}$$

egyenletben szerepel egy-egy nem 0 tag:

$$\Delta c_\ell \left(\vartheta^\ell\right)^j$$

ϑ^ℓ-ből egyértelműen megadható a hiba helye, csak meg kell keresni, hogy hányadik hatványa ϑ-nak.

A ϑ^ℓ mennyiség a **hibahely-lokátor**

Egyszerű hibák javítása

Legyen

$$L(t)=\prod_{i=1}^{\nu}\left(1-\vartheta^{\ell_i}\cdot t\right)=1+L_1t+\ldots+L_\nu t^\nu$$

a **hibahely-polinom**, melynek gyökei a hibahely-lokátorok inverzei.

Ha meg tudjuk határozni $L(t)$-t, akkor

- a gyökeit ki tudjuk számolni
- meg tudjuk adni a gyökök inverzét, azaz a hibahely-lokátorokat
- meg tudjuk keresni, hogy azok ϑ hányadik hatványai, azaz meg tudjuk adni, hol vannak hibák

Ha a hibák helyét ismerjük, akkor törléses hibákat kell javítani, azt meg láttuk hogyan kell.

Egyszerű hibák javítása

L-re igaz, hogy

$$L\left(\vartheta^{-\ell}\right)=0$$

Szorozzuk mindkét oldalt $\Delta c_\ell \cdot \left(\vartheta^{\ell}\right)^{\nu+j}$ -nel

$$\Delta c_\ell \cdot \left(\vartheta^{\ell}\right)^{\nu+j} L\left(\vartheta^{-\ell_i}\right)=0$$

Összegezzünk $\ell=1,2,\ldots,\nu$ –re

$$\sum_{\ell=1}^{\nu} \Delta c_\ell \cdot \left(\vartheta^{\ell}\right)^{\nu+j} L\left(\vartheta^{-\ell}\right)=0$$

Helyettesítsük be $L(t)=1+L_1 t+\ldots+L_\nu t^\nu$ polinom egyelőre ismeretlen együtthatóit:

$$\sum_{\ell=1}^{\nu} \Delta c_\ell \cdot \left(\vartheta^{\ell}\right)^{\nu+j}\left(1+L_1\cdot\vartheta^{-\ell}+\ldots+L_\nu\cdot\left(\vartheta^{-\ell}\right)^{\nu}\right)=0$$

Egyszerű hibák javítása

$$\sum_{\ell=1}^{\nu} \Delta c_\ell \cdot \left(\vartheta^\ell\right)^{\nu+j} \left(1 + L_1 \cdot \vartheta^{-\ell} + \ldots + L_\nu \cdot \left(\vartheta^{-\ell}\right)^{\nu}\right) = 0$$

Szétszorozva ϑ hatványait:

$$\sum_{\ell=1}^{\nu} \Delta c_\ell \left(1 \cdot \left(\vartheta^\ell\right)^{\nu+j} + L_1 \cdot \left(\vartheta^\ell\right)^{\nu+j-1} + \ldots + L_\nu \cdot \left(\vartheta^\ell\right)^{j}\right) = 0$$

$$\sum_{\ell=1}^{\nu} \Delta c_\ell \left(\vartheta^\ell\right)^{\nu+j} \quad L_1 \cdot \sum_{\ell=1}^{\nu} \Delta c_\ell \left(\vartheta^\ell\right)^{\nu+j-1} \qquad L_\nu \cdot \sum_{\ell=1}^{\nu} \Delta c_\ell \left(\vartheta^\ell\right)^{j}$$

$$= s_{\nu+j} \qquad = L_1 \cdot s_{\nu+j-1} \qquad = L_\nu \cdot s_j$$

A szindróma a következő volt:

$$s_j = \sum_{i=1}^{\nu} \Delta c_i \vartheta^{ij}$$

Egyszerű hibák javítása

Így kaptunk egy egyenletrendszert $L(t)$ együtthatóira, amelyben csak a szindróma szerepel:

$$1 \cdot s_{\nu+j} + L_1 \cdot s_{\nu+j-1} + \ldots + L_\nu \cdot s_j = 0$$

ahol j lehet $0,1,\ldots,\nu$.

A szindróma legmagasabb indexszel a $j+\nu$-vel fordul elő az egyenletrendszerben, ami legfeljebb 2ν lehet, ami nem haladja meg **s** komponenseinek a számát. (Hiszen legfeljebb (n−k)/2 egyszerű hiba javítható, a szindróma meg n−k komponensű.)

Az egyenletrendszer tehát mindig felírható.

Egyszerű hibák javítása

Legyen $\vartheta = 6$, a $GF(11)$ véges test tizedrendű eleme A $GF(11)$ elemeinek az első 10 hatványa:

ϑ	ϑ^2	ϑ^3	ϑ^4	ϑ^5	ϑ^6	ϑ^7	ϑ^8	ϑ^9	ϑ^{10}
2	4	8	5	10	9	7	3	6	1
3	9	5	4	1	3	9	5	4	1
4	5	9	3	1	4	5	9	3	1
5	3	4	9	1	5	3	4	9	1
6	3	7	9	10	5	8	4	2	1
7	5	2	3	10	4	6	9	8	1
8	9	6	4	10	3	2	5	7	1
9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1

Egyszerű hibák javítása

Legyen $\vartheta = 6$, a $GF(11)$ véges test feletti (10,6) paraméterű Reed—Solomon-kód generáló eleme. A generátormátrix:

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 6 & 3 & 7 & 9 & 10 & 5 & 8 & 4 & 2 \\ 1 & 3 & 9 & 5 & 4 & 1 & 3 & 9 & 5 & 4 \\ 1 & 7 & 5 & 2 & 3 & 10 & 4 & 6 & 9 & 8 \\ 1 & 9 & 4 & 3 & 5 & 1 & 9 & 4 & 3 & 5 \\ 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 \end{pmatrix}$$

A (0 2 6 7 1 1) üzenet által létrehozott kódszó:

$$\mathbf{c} = (6 \quad 10 \quad 1 \quad 5 \quad 3 \quad 8 \quad 0 \quad 5 \quad 6 \quad 0)$$

Egyszerű hibák javítása

Legyen $\vartheta = 6$, a $GF(11)$ véges test feletti (10,6) paraméterű Reed—Solomon-kód generáló eleme.

A paritásellenőrző mátrix:

$$\mathbf{H}^T = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 6 & 3 & 7 & 9 \\ 3 & 9 & 5 & 4 \\ 7 & 5 & 2 & 3 \\ 9 & 4 & 3 & 5 \\ 10 & 1 & 10 & 1 \\ 5 & 3 & 4 & 9 \\ 8 & 9 & 6 & 4 \\ 4 & 5 & 9 & 3 \\ 2 & 4 & 8 & 5 \end{pmatrix}$$

A (6 10 7 5 0 8 0 5 6 0) vett vektorból kapott szindróma:

(233 108 230 141)≡
≡(2 9 10 9).

Egyszerű hibák javítása

Dekódoljuk a $\vartheta = 6$ generáló elemű, $GF(11)$ feletti (10,6) Reed—Solomon-kód kódszavából torzult (6 10 7 5 0 8 0 5 6 0) vektort. A szindróma: (**2 9 10 9**).

$$1 \cdot s_{\nu+j} + L_1 \cdot s_{\nu+j-1} + \ldots + L_\nu \cdot s_j = 0$$

alkalmazása j=0 és 1-re:

$$s_2 + L_1 \cdot s_1 + L_2 \cdot s_0 = 0$$

$$s_3 + L_1 \cdot s_2 + L_2 \cdot s_1 = 0$$

azaz

$$10 + L_1 \cdot 9 + L_2 \cdot 2 = 0$$

$$9 + L_1 \cdot 10 + L_2 \cdot 9 = 0 \Rightarrow 9 + L_1 \cdot 10 =$$

$$= L_2 \cdot (-9) \equiv L_2 \cdot 2 \mod 11$$

Egyszerű hibák javítása

Dekódoljuk a $\vartheta = 6$ generáló elemű, $GF(11)$ feletti (10,6) Reed—Solomon-kód kódszavából torzult (6 10 7 5 0 8 0 5 6 0) vektort.

$$\Rightarrow 9 \cdot 6 + L_1 \cdot 10 \cdot 6 = L_2$$

$$L_2 = 10 + 5L_1$$

$$\begin{aligned} 10 + L_1 \cdot 9 + L_2 \cdot 2 &= 0 \\ 9 + L_1 \cdot 10 + L_2 \cdot 9 &= 0 \end{aligned} \Rightarrow 10 + L_1 \cdot 9 + (10 + 5L_1) \cdot 2 = 0$$

$$8 + L_1 \cdot 8 = 0$$

$$L_1 = -1 \equiv 10 \mod 11$$

$$L_2 = 10 + 5 \cdot 10 \equiv 5 \mod 11$$

Egyszerű hibák javítása

Dekódoljuk a $\vartheta = 6$ generáló elemű, $GF(11)$ feletti (10,6) Reed—Solomon-kód kódszavából torzult (6 10 7 5 0 8 0 5 6 0) vektort.

A hibahelypolinom:

$$L(t) = L_2 \cdot t^2 + L_1 \cdot t + 1 = 5t^2 + 10t + 1$$

Gyökei: 4 és 5:

$$L(4) = 5 \cdot 4^2 + 10 \cdot 4 + 1 = 121 \equiv 0 \mod 11$$

$$L(5) = 5 \cdot 5^2 + 10 \cdot 5 + 1 = 176 \equiv 0 \mod 11$$

Inverzeik: $4^{-1} \equiv 3 \mod 11$, és $5^{-1} \equiv 9 \mod 11$

Egyszerű hibák javítása

ϑ	ϑ^2	ϑ^3	ϑ^4	ϑ^5	ϑ^6	ϑ^7	ϑ^8	ϑ^9	ϑ^{10}
2	4	8	5	10	9	7	3	6	1
3	9	5	4	1	3	9	5	4	1
4	5	9	3	1	4	5	9	3	1
5	3	4	9	1	5	3	4	9	1
6	3	7	9	10	5	8	4	2	1
7	5	2	3	10	4	6	9	8	1
8	9	6	4	10	3	2	5	7	1
9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1

A hibák tehát a 2. és 4. helyen vannak.

$4^{-1} \equiv 3 \bmod 11$, és $5^{-1} \equiv 9 \bmod 11$

Egyszerű hibák javítása

A hibák tehát a 2. és 4. helyen vannak.

A csonkolt paritás-ellenőrző mátrix:

$$\mathbf{H}^T = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 6 & 3 & 7 & 9 \\ 3 & 9 & 5 & 4 \\ 7 & 5 & 2 & 3 \\ 9 & 4 & 3 & 5 \\ 10 & 1 & 10 & 1 \\ 5 & 3 & 4 & 9 \\ 8 & 9 & 6 & 4 \\ 4 & 5 & 9 & 3 \\ 2 & 4 & 8 & 5 \end{pmatrix}$$

Egyszerű hibák javítása

A hibák tehát a 2. és 4. helyen vannak.

A csonkolt paritás-ellenőrző mátrix:

$$\tilde{\mathbf{H}}^T = \begin{pmatrix} 3 & 9 & 5 & 4 \\ 9 & 4 & 3 & 5 \end{pmatrix}$$

A csonkolt hibavektor: $\Delta\tilde{\mathbf{c}} = (\Delta c_2 \quad \Delta c_4)$

A szindróma (2 9 10 9) volt,

$$\begin{aligned} \tilde{H}_{00} \cdot \Delta\tilde{c}_0 + \ldots + \tilde{H}_{n-k-1\,0} \cdot \Delta\tilde{c}_{n-k-1} &= s_0 \\ \tilde{H}_{01} \cdot \Delta\tilde{c}_0 + \ldots + \tilde{H}_{n-k-1\,1} \cdot \Delta\tilde{c}_{n-k-1} &= s_1 \\ &\vdots \\ \tilde{H}_{0\,n-k-1} \Delta\tilde{c}_0 + \ldots + \tilde{H}_{n-k-1\;n-k-1} \Delta\tilde{c}_{n-k-1} &= s_{n-k-1} \end{aligned}$$

Egyszerű hibák javítása

A hibák tehát a 2. és 4. helyen vannak.

A csonkolt paritás-ellenőrző mátrix:

$$\tilde{\mathbf{H}}^T = \begin{pmatrix} 3 & 9 & 5 & 4 \\ 9 & 4 & 3 & 5 \end{pmatrix}$$

A csonkolt hibavektor: $\Delta\tilde{\mathbf{c}} = (\Delta c_2 \quad \Delta c_4)$

A szindróma (2 9 10 9) volt,

$$\begin{aligned} \tilde{H}_{00} \cdot \Delta c_2 + \tilde{H}_{10} \cdot \Delta c_4 &= s_0 \\ \tilde{H}_{01} \cdot \Delta c_2 + \tilde{H}_{11} \cdot \Delta c_4 &= s_1 \\ \tilde{H}_{02} \cdot \Delta c_2 + \tilde{H}_{12} \cdot \Delta c_4 &= s_2 \\ \tilde{H}_{03} \cdot \Delta c_2 + \tilde{H}_{13} \cdot \Delta c_4 &= s_3 \end{aligned}$$

Egyszerű hibák javítása

Behelyettesítés után:

$$\begin{aligned} 3\cdot\Delta c_2 + 9\cdot\Delta c_4 &= 2 \\ 9\cdot\Delta c_2 + 4\cdot\Delta c_4 &= 9 \\ 5\cdot\Delta c_2 + 3\cdot\Delta c_4 &= 10 \\ 4\cdot\Delta c_2 + 5\cdot\Delta c_4 &= 9 \end{aligned} \quad \left| \begin{aligned} \cdot 3^{-1} &\equiv \cdot 4 \\ \cdot 9^{-1} &\equiv \cdot 5 \\ \cdot 5^{-1} &\equiv \cdot 9 \\ \cdot 4^{-1} &\equiv \cdot 3 \end{aligned} \right.$$

$$\begin{aligned} \Delta c_2 + 3\cdot\Delta c_4 &= 8 \\ \Delta c_2 + 9\cdot\Delta c_4 &= 1 \\ \Delta c_2 + 5\cdot\Delta c_4 &= 2 \\ \Delta c_2 + 4\cdot\Delta c_4 &= 5 \end{aligned}$$

Egyszerű hibák javítása

Átrendezve:

$$\Delta c_2 = 8 - 3 \cdot \Delta c_4 \equiv 8 + 8 \cdot \Delta c_4$$

$$\Delta c_2 = 1 - 9 \cdot \Delta c_4 \equiv 1 + 2 \cdot \Delta c_4$$

$$\Delta c_2 = 2 - 5 \cdot \Delta c_4 \equiv 2 + 6 \cdot \Delta c_4$$

$$\Delta c_2 = 5 - 4 \cdot \Delta c_4 \equiv 5 + 7 \cdot \Delta c_4$$

$$8 + 8 \cdot \Delta c_4 = 1 + 2 \cdot \Delta c_4$$

$$6 \cdot \Delta c_4 = 1 - 8 \equiv 1 + 3$$

$$\Delta c_4 = 4/6 \equiv 4 \cdot 2 = 8$$

$$\Delta c_2 = 1 + 2 \cdot 8 \equiv 6$$

A többi egyenletbe behelyettesítve az eredmény ellenőrizhető.

Egyszerű hibák javítása

Dekódoljuk a $\vartheta = 6$ generáló elemű, $GF(11)$ feletti (10,6) Reed—Solomon-kód kódszavából torzult (6 10 **7** 5 **0** 8 0 5 6 0) vektort.

A hibavektor komponensei:

$$\Delta c_2 = 6$$

$$\Delta c_4 = 8$$

A javított kódszó:

(6 10 **1** 5 **3** 8 0 5 6 0)