LINEARNI KODI

Definicija: Naj bo Σ končen obseg. Koda $C \subseteq \Sigma^n$ je **linearen**, če je vektorski podprostor Σ^n.

Torej: $c_1, c_2 \in C,\ a, b \in \Sigma \Rightarrow a \cdot c_1 + b \cdot c_2 \in C$

Trditev: Če je C linearen (n, M, d)-kod nad $GF(q)$ dimenzije k, potem je $M = q^k$.

Oznaka: $[n, k, d]$-koda je linearen (n, q^k, d)-koda nad $GF(q)$.

Trditev: Če je C linearen koda, je $d(C) = \min\limits_{\substack{x \neq 0 \\ x \in C}} t(x)$.

Dokaz: $d(x, y) = t(x - y)$

$$\Rightarrow d(C) = \min_{\substack{x,y \in C \\ x \neq y}} d(x,y) = \min_{\substack{x,y \in C \\ x \neq y}} t(x-y) = \min_{\substack{z \in C \\ z \neq 0}} t(z)$$

Definicija: Naj bo C $[n, k, d]$-koda. **Generatorska matrika** G koda C je matrika velikosti $k \times n$. Njene vrstice so bazni elementi koda.

Primer: $C = \{000, 011, 101, 110\}$ dvojiški koda

$n = 3$
$k = 2$
$d = 2$

Linearen:

$011 \oplus 110 = 101$ ✓
$011 \oplus 101 = 101$ ✓
$110 \oplus 101 = 011$ ✓

$x \oplus 000 = x$ ✓
$x \oplus x = 0$ ✓

Generatorska matrika:

$$G = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

Kodiranje:

Naj bo C linearen $[n,k,d]$-kod nad $\Sigma = GF(q)$ in $\{x_1, \dots, x_n\}$ baza C.

Sporočilo: $s = s_1 s_2 \cdots s_k \in \Sigma^k$

$c = s_1 x_1 + s_2 x_2 + \dots + s_k x_k = s \cdot G$

Za lepo generatorsko matriko $G = [I_k \vdots A]$ velja:

$c = s \cdot G = \underbrace{s_1 s_2 \cdots s_k}_{\text{sporočilo}} s_{k+1} \cdots s_n$

Definicija: Če je G v taki obliki, rečemo, da je v standardni obliki.

Definicija: Naj bo C $[n,k,d]$-kod nad $\Sigma = GF(q)$. Potem $C^\perp = \{x \in \Sigma^n ; \langle x, c \rangle = 0 \ \forall c \in C\}$ imenujemo dualni kod kode C.

Posledica: Dualni kod je $C^\perp$ linearni kod.

Oznaka: Generatorsko matriko kode $C^\perp$ pogosto označimo s H in ji pravimo nadzorna matrika kode C.

Trditev: $G \in GF(q)^{k \times n}$, $\operatorname{rang} G = k$
$H \in GF(q)^{(n-k) \times n}$, $\operatorname{rang} H = n-k$

Potem velja:

G generatorska matrika in H nadzorna matrika kode C

$\Leftrightarrow GH^T = 0$

Dokaz: ($\Rightarrow$) $Gx^T = 0 \quad \forall x \in C^\perp$

To velja tudi za bazne vektorje kode $C^\perp$

Ti pa tvorijo H

($\Leftarrow$) Naj bo C kod, generiran z G

$C^\perp$ ničelni podprostor prostora C

$\Rightarrow \dim C^\perp = n-k$

Ker je $G \cdot H^T = 0$, so vrstice H elementi $C^\perp$.

Ker je $\operatorname{rang} H = n-k$, so linearno neodvisne.

Torej so vrstice H baza $C^\perp$.

Primer: $G = [I_k \mid A]$

$H = [-A^T \mid I_{1-k}]$

$G \cdot H^T = -A + A = 0$

DEKODIRANJE S POMOČJO SINDROMOV

Naj bo C $[n,k,d]$-koda, $s = \lfloor \frac{d-1}{2} \rfloor$, H nadzorna matrika, x poslana beseda, y prejeta beseda in $e = y - x$ napaka pri pošiljanju.

$H \cdot y^T$ imenujemo sindrom besede y.

Velja: $Hy^T = \underbrace{Hx}_{=0} + He = He$

Trditev: Naj bosta $x_1, x_2 \in \sum^n$ takšni besedi, da sta $t(e_1), t(e_2) \leq s = \lfloor \frac{d-1}{2} \rfloor$ in $e_1 \neq e_2$. Potem je tudi $He_1 \neq He_2$.

Dokaz: Če velja $He_1 = He_2$, je $H(e_1 - e_2) = 0$, zato $e_1 - e_2 \in C$.

$t(e_1 - e_2) \leq 2 \cdot s \leq d - 1$

Kodne besede so na razdalji d.

$\Rightarrow e_1 - e_2 = 0$

$\Rightarrow e_1 = e_2$

Postopek dekodiranja:

Vhod: $y \in \sum^n$ sprejeta beseda

Izhod: $x \in C$, $d(x,y)$ minimalen, ali pa ne obstaja

Izračunamo tabelo parov (He^T, e) za $t(e) \leq s$ (1x za kod).

Za y izračunamo sindrom Hy^T in poiščemo e v tabeli, da velja $He^T = Hy^T$.

Vrnemo $x = y - e$.

Primer: $G = \left[\begin{array}{ccc:cc} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{array}\right]$

$\Rightarrow n = 5, k = 3$

$\Rightarrow d = 3$

$H = \left[\begin{array}{cc:ccc} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{array}\right]$

$(He^T)^T$	e
000	00000
001	10000
010	01000
100	00100
101	00010
110	00001

i) $y = 11111$

$(Hy^T)^T = 100 \Rightarrow e = 00100$

$\Rightarrow x = y - e = 11011$

ii) $y = 111000$

$(Hy^T)^T = 111$ ni v tabeli

$\Rightarrow$ Zahtevamo ponovno pošiljanje

Časovna zahtevnost:

- Direktno iskanje: $q^k \cdot n$
- S pomočjo sindromov:

  Priprava: $1 + n \cdot (q-1) + \binom{n}{2} \cdot (q-1)^2 + \ldots + \binom{n}{s} \cdot (q-1)^s = N$ (tabela)

  Preverjanje koda: $(n-k) \cdot n$ (množenje s H)

Primer: $\sum = \mathbb{Z}_2$

$n = 100$
$k = 79$
$d = 7$

$\Rightarrow s = 3$

$\Rightarrow N \approx 2^{17}$

Velikost tabele: $N \cdot (n + n - k) \approx 16\,MB$

RAČUNANJE RAZMAKNJENOSTI LINEARNEGA KODA

Izrek: Naj bo C linearni kod nad $GF(q)$ z nadzorno matriko H. Potem velja:

$d(C) \geq d \iff$ Vsaka množica $d-1$ stolpcev matrike H je linearno neodvisna

Dokaz: ($\Rightarrow$) Naj bodo $h_{i_1}, \dots, h_{i_j}$ linearno odvisni:

$$\sum_{k=1}^{j} \lambda_{i_k} h_{i_k} = 0 \text{ za neke } \lambda_{i_k}, \text{ ne vse } 0$$

Definirajmo $x \in GF(q)$:

$$x_\ell = \begin{cases} \lambda_{i_k} & ; \ i_k = \ell \\ 0 & ; \ \text{sicer} \end{cases}$$

$$Hx = \sum_{k=1}^{j} \lambda_{i_k} h_{i_k} = 0$$

$\Rightarrow x \in C$

$\Rightarrow t(x) \geq d(C)$

$\Rightarrow j \geq d(C)$

Torej: Če imamo $d(C)-1$ stolpcev, morajo biti lin. neodvisni.

($\Leftarrow$) Naj bo vsakih $d-1$ stolpcev lin. neodvisnih.

Vzemimo $x \in C, x \neq 0$.

$\Rightarrow H \cdot x^T = 0$

$\Rightarrow H \cdot x^T$ je netrivialna lin. kombinacija $t(x)$ stolpcev, ki je enaka 0.

$\Rightarrow t(x) \geq d$

$\Rightarrow d(C) \geq d$

Posledica: C linearen

$\Rightarrow d(C) = \max\{d$; vsakih $d-1$ stolpcev v nadzorni matriki linearno neodvisnih$\}$

Primer: $H = \begin{bmatrix} 1&1&1&0&1&0&0&0 \\ 1&1&0&1&0&1&0&0 \\ 1&0&1&1&0&0&1&0 \\ 0&1&1&1&0&0&0&1 \end{bmatrix}$ nad $\mathbb{Z}_2$

- Vsi stolpci neničelni $\Rightarrow d \geq 2$
- Vsi stolpci različni $\Rightarrow d \geq 3$
- Vsota 3 stolpcev ima liho enk $\Rightarrow$ Vsota 3 stolpcev ni 0

  $\Rightarrow d \geq 4$
- $s_1 + s_5 + s_6 + s_7 = 0 \Rightarrow d < 5 \Rightarrow d = 4$

MEJE ZA KODE

Problem: Pri danih n, d iščemo (n, M, d)-kod s čim večjim M.

Definicija: $A_q(n,d) = \max\{M$; obstaja (n, M, d)-kod nad $GF(q)\}$

Trditev: $A_q(n,1) = q^n$

Trditev: $A_2(n,2) = 2^{n-1}$

Dokaz: $C = \{x \in \mathbb{Z}_2^n ;\ t(x) \text{ je soda}\}$

$d = 2$ ✓

$|C| = \frac{2^n}{2} = 2^{n-1}$

$\Rightarrow A_2(n,2) \geq 2^{n-1}$

Naj bo C' optimalen $[n, M, 2]$-kod.

$C'' = \{\overline{x} \ ;\ x \in C\}$

odštejemo zadnjo koordinato

$d \geq 2 \Rightarrow C'' = C'$

$|C''| \leq 2^{n-1}$

$\Rightarrow |C'| \leq 2^{n-1}$

$\Rightarrow C'$ optimalen $\Rightarrow M = 2^{n-1}$

Oznaka: $K(x, r) = \{y \in \Sigma^n ;\ d(x,y) \leq r\}$

Trditev: $|K(x,r)| = \sum_{i=0}^{r} \binom{n}{i} \cdot (q-1)^i$

Izrek (Hammingova ocena):

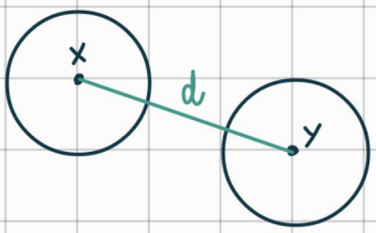
$$A_q(n,d) \leq \frac{q^n}{\sum_{i=0}^{\left[\frac{d-1}{2}\right]} \binom{n}{i}(q-1)^i}$$

Dokaz: Naj bo C poljuben (n, M, d)-kod.

Označimo $s = \left\lfloor \frac{d-1}{2} \right\rfloor$.

Vzemimo poljubna $x, y \in C$, $x \neq y$.

Ker je razmaknjenost d, je $K(x,s) \cap K(y,s) = \emptyset$.



$$\Rightarrow \left| \bigcup_{x \in C} K(x,s) \right| = \sum_{x \in C} |K(x,s)| = \sum_{x \in C} \sum_{i=0}^{s} \binom{n}{i} \cdot (q-1)^i = M \cdot \sum_{i=0}^{s} \binom{n}{i} \cdot (q-1)^i$$

Po drugi strani:

$$\bigcup_{x \in C} K(x,s) \subseteq \sum^n$$

$$\Rightarrow \left| \bigcup_{x \in C} K(x,s) \right| \leq q^n$$

$$\Rightarrow M \leq \frac{q^n}{\sum_{i=0}^{s} \binom{n}{i} (q-1)^i}$$

Definicija: (n, M, d)-kod je popoln, če dosežejo Hammingovo mejo.

Primer: $C = \sum^n$ je popoln kod.

$C = \{00\cdots0, 11\cdots1\}$, n lih, je tudi popolni kod.

To sta trivialna popolna koda.

Izrek: Naj bo C netrivialen popoln (n, M, d)-kod.

Potem je:

- $n=27,\ d=7,\ q=2$
- $n=11,\ d=5,\ q=3$

} Golayevi kodi

- $n=\frac{q^r-1}{q-1},\ d=3,\ r\geq 2$ poljuben

Primer: $q=2,\ r=3$

$\Rightarrow n=\frac{2^3-1}{1-1}=7$

$$\left[\begin{array}{ccccc|ccc} 1 & 1 & 0 & 1 & & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & & 0 & 0 & 1 \end{array}\right] = H$$

Izrek (Gilbert-Varshamova spodnja meja):

$$A_q(n,d) \geq \frac{q^n}{\sum_{k=0}^{d-1}\binom{n}{k}(q-1)^k}$$

Dokaz: Naj bo C tak optimalen kod, da je $M=A_q(n,d)$.
Naj bo $x\in\sum^n$, da je $d(x,C)\leq d-1$.

$$\bigcup_{c\in C} K(c,d-1)=\sum^n$$

$$q^n \leq \sum_{c\in C}|K(c,d-1)| = M\cdot\sum_{k=0}^{d-1}\binom{n}{k}(q-1)^k$$

$$A_q \geq \frac{q^n}{\sum_{k=0}^{d-1}\binom{n}{k}(q-1)^k}$$

Primer: $n=10$
$q=2$
$d=3$

$$\frac{2^{10}}{\sum_{k=0}^{3}\binom{10}{k}} \leq A_2(10,3) \leq \frac{2^{10}}{\sum_{k=0}^{3}\binom{10}{k}}$$

$$18{,}3 \leq A_2(10,3) \leq 93{,}1$$

Dejansko: $A_2(10,3) = 72$

Trditev (Singletonova meja):

Naj bo C (n, M, d) kod. Potem je $M \leq q^{n-d+1}$.

Dokaz: Zložimo vse kodne besede v matriko:

$$M\begin{bmatrix} & & n & \\ & & & \\ & & & \end{bmatrix}$$

Pobrišemo $d-1$ stolpcev v tej matriki.

Ker je razmik d, sta poljubni vrstici različni.

$\Rightarrow M \leq q^{n-d+1}$

Posledica: Za linearen $[n,k,d]$-kod je $d \leq n-k+1$.

Dokaz: $M = q^k \leq q^{n-d+1}$

$k \leq n-d+1$

$d \leq n-k+1$

Posledica: Linearen $[n,k,d]$-kod lahko popravi največ $\left\lfloor \frac{n-k}{2} \right\rfloor$ napak.

Dokaz: $t = \left\lfloor \frac{d-1}{2} \right\rfloor \leq \left\lfloor \frac{n-k+1-1}{2} \right\rfloor = \left\lfloor \frac{n-k}{2} \right\rfloor$

CIKLIČNI KODI

Definicija: Naj bo $x = x_1 x_2 \cdots x_n \in \sum^n$ beseda.

Označimo $\hat{x} = x_n x_1 x_2 \cdots x_{n-1} \in \sum^n$ ciklični zamik x.

Linearni $[n,k,d]$-kod nad $GF(q)$ je ciklicen, če velja:

$x \in C \Rightarrow \hat{x} \in C$

Besedo $x = x_1 x_2 \cdots x_n$ identificiramo s polinomom $x(t) = x_1 + x_2 t + \ldots + x_n t^{n-1}$ iz $GF(q)[t]/(t^n-1)$.

Besedi $\hat{x}$ ustreza polinom $\hat{x}(t) = x_n + x_1 t + x_2 t^2 + \ldots + x_{n-1} t^{n-1} =$
$= t \cdot x(t) - t^n \cdot x_n + x_n = t \cdot x(t) - x_n \underbrace{(t^n - 1)}_{=0} = t \cdot x(t)$.

Trditev: C je ciklicen kod dolzine n nad $GF(q)$

$\Leftrightarrow C$ ustreza idealu v $GF(q)[t]/(t^n-1)$

Dokaz: ($\Rightarrow$) C ciklicen

$\Rightarrow$ Zaprt za množenje s t

$\Rightarrow$ Zaprt za množenje s t^i (i)

C linearen

$\Rightarrow C$ vektorski podprostor

$\Rightarrow$ C zaprt za seštevanje in množenje s skalarjem (ii)

(i)+(ii) $\Rightarrow$ C zaprt za množenje s polinomom $\sum a_i t^i$

($\Leftarrow$) C ideal

$\Rightarrow$ C zaprt za seštevanje in množenje s skalarjem

$\Rightarrow$ C vektorski podprostor

$\Rightarrow$ C linearen kod (i)

C ideal

$\Rightarrow$ C zaprt za množenje s t

$\Rightarrow$ C zaprt za ciklične zamike (ii)

(i)+(ii) $\Rightarrow$ C ciklični kod

Trditev: Naj bo C ciklični kod in $g(t)$ neničeln polinom minimalne stopnje v C. Potem velja:

1) $C = \langle g(t) \rangle = \{ g(t) \cdot a(t) \mod t^n - 1 \; ; \; a(t) \in \mathbb{F}(q)[t] \}$

2) $g(t) \mid t^n - 1$

3) $\dim(C) = k = n - \deg(g)$

$B = \{ g(t), t \cdot g(t), \ldots, t^{k-1} \cdot g(t) \}$ baza C

Dokaz: 1) $p(t) \in C$

$p(t) = f(t) \cdot g(t) + r(t)$, $\deg(r) < \deg(g)$

v $GF(q)[t]/(t^n - 1)$

$p(t),\ f(t) \cdot g(t) \in C$

C ideal $\Rightarrow r(t) \in C$

$\Rightarrow r(t) = 0$ v $GF(q)[t]$

$p(t) = f(t) \cdot g(t)$

$\deg(p) = \deg(f) + \deg(g)$

2) $t^n - 1 = f(t) \cdot g(t) + r(t)$, $\deg(r) < \deg(g)$

$0 = f(t) \cdot g(t) + r(t)$

$0,\ f(t) \cdot g(t) \in C$

$\Rightarrow r(t) \in C$

$\Rightarrow r(t) = 0$

3) B linearno neodvisna:

$$g(t) = g_0 + g_1 t + g_2 t^2 + \dots + g_\sigma t^\sigma$$

$$\begin{bmatrix} g_0 & g_1 & g_2 & \cdots & \cdots & \cdots & g_\sigma & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & \cdots & \cdots & g_{\sigma-1} & g_\sigma & 0 & \cdots & 0 \\ & & & & & & & & & & \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & \cdots & \cdots & \cdots & \cdots & g_\sigma \end{bmatrix}$$

$\leftarrow g(t)$

$\leftarrow t \cdot g(t)$

Vrstice očitno linearno neodvisne

B tvori ogrodje C:

$p(t) \in C$

po (1): $p(t) = f(t) \cdot g(t)$, $\deg(p) < n$

$\Rightarrow \deg(f) < n - \deg(g)$

$\Rightarrow f(t) = f_0 + f_1 t + \dots + f_{k-1} t^{k-1}$

$p(t) = f_0 \cdot g(t) + f_1 \cdot t \cdot g(t) + \dots + f_{k-1} \cdot t^{k-1} \cdot g(t)$

Posledica: Ciklični kodi dolžine n nad $GF(q)$ ustrezajo deliteljem polinoma $t^n - 1 \in GF(q)[t]$.

Definicija: Če je $C = \langle g(t) \rangle$, imenujemo $g(t)$ generatorski polinom kode C.

Primer: $q = 2$
$n = 3$

$C = \{000, 110, 011, 101\}$ je ciklični $[3,2,2]$-kod

$C = \{0, 1+t, t+t^2, 1+t^2\}$

$g(t) = 1+t$

$k = n - \deg(g) = 3 - 1 = 2$

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

$\Rightarrow C = \langle g(t) \rangle$

$$G = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{matrix} \leftarrow g(t) \\ \leftarrow t \cdot g(t) \end{matrix}$$

Primer: Poišči ciklični $[7,3,d]$-kod nad $GF(2)$.

$t^7 - 1 = (1+t)(1+t+t^3)(1+t^2+t^3)$

$\deg(g) = 7-3 = 4$

Dve možnosti:

$g_1(t) = (1+t)(1+t+t^3) = 1+t^2+t^3+t^4$
$g_2(t) = (1+t)(1+t^2+t^3) = 1+t+t^2+t^4$

$$G_1 = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$G_2 = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Kodiranje s polinomi:

$x(t) = s(t) \cdot g(t)$

REED-SOLOMONOVI KODI

Trditev: $\alpha_1, \dots, \alpha_p \in GF(p)$, $\alpha_i \neq 0$, $\alpha_i \neq \alpha_j$

$$\Rightarrow g(t) = (t-\alpha_1)(t-\alpha_2)\cdots(t-\alpha_p) \mid (t^{q-1}-1)$$

Dokaz: $\alpha_i^{q-1} = \alpha_i^{|GF(q)\setminus\{0\}|} = 1$

$$\alpha_i^{q-1} - 1 = 0$$

$\Rightarrow \alpha_i$ ničla $t^{q-1} - 1$

Posledica: $g(t)$ generira ciklični kod dolžine $n = q-1$ nad $GF(q)$.

Definicija: Naj bo $n = q-1$, $\delta \in \{2, \dots, n\}$, β primitivni element $GF(q)$.
Reed-Solomonov kod $RS(n,k)$ je ciklični kod dolžine n in dimenzije $k = n - \delta + 1$ nad $GF(q)$, generiran z $g(t) = (t-\beta)(t-\beta^2)(t-\beta^3)\cdots(t-\beta^{\delta-1})$.

Definicija: Vandermondova matrika za $\alpha_i \in F$, $i = 1, \dots, p$, F obseg, je definirana kot:

$$A = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \alpha_1^3 & \cdots & \alpha_1^{p-1} \\ 1 & \alpha_2 & \alpha_2^2 & \alpha_2^3 & \cdots & \alpha_2^{p-1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_p & \alpha_p^2 & \alpha_p^3 & \cdots & \alpha_p^{p-1} \end{bmatrix}$$

Trditev: $\det A = \prod_{1 \le i < j \le p} (\alpha_i - \alpha_j)$

Dokaz: Vemo iz Algebre 1.

Izrek: Naj bo C Reed-Solomonov kod dolžine $n = q-1$ in dimenzije k. Potem je $d(C) = n - k + 1$.

Dokaz: $\sigma = n-k+1$

$g(t) = (t-\beta)(t-\beta^2)\cdots(t-\beta^{n-1})$

Zapišemo: $g(t) = g_0 + g_1 t + g_2 t^2 + \dots + g_{\sigma-1} t^{\sigma-1}$

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{\sigma-1} & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & \vdots & g_{\sigma-1} & \cdots & 0 \\ \vdots & & & & \vdots & & & \\ 0 & & & 0 & g_0 & g_1 & \cdots & g_{\sigma-1} \end{bmatrix}$$

$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ 1 & \beta^2 & \beta^4 & \cdots & (\beta^2)^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \beta^{\sigma-1} & (\beta^{\sigma-1})^2 & \cdots & (\beta^{\sigma-1})^{n-1} \end{bmatrix}$$

Trdimo: H je nadzorna matrika.

$G \cdot H^T = 0$?

$$G \cdot H^T = \begin{bmatrix} \underbrace{g_0 + g_1\beta + g_2\beta^2 + \dots + g_{\sigma-1}\beta^{\sigma-1}}_{=g(\beta)=0} & \underbrace{g_0 + g_1\beta^2 + \dots + g_{\sigma-1}(\beta^2)^{\sigma-1}}_{=g(\beta^2)=0} & \cdots \\ \underbrace{g_0 + g_1\beta^2 + \dots + g_{\sigma-1}\beta^{\sigma}}_{=\beta\cdot g(\beta)=0} & \underbrace{\dots}_{=\beta^2 g(\beta^2)=0} & \cdots \\ \vdots & \vdots & \end{bmatrix}$$

$= 0$

$$\det \begin{bmatrix} \beta^{j_1} & \beta^{j_2} & \cdots & \beta^{j_{n-k}} \\ (\beta^{j_1})^2 & (\beta^{j_2})^2 & \cdots & (\beta^{j_{n-k}})^2 \\ (\beta^{j_1})^3 & (\beta^{j_2})^3 & \cdots & (\beta^{j_{n-k}})^3 \\ \vdots & \vdots & & \vdots \\ (\beta^{j_1})^{n-1} & (\beta^{j_2})^{n-k} & \cdots & (\beta^{j_{n-k}})^{n-k} \end{bmatrix}$$

$$= \beta^{j_1+j_2+\dots+j_{n-k}} \cdot \det \begin{bmatrix} 1 & 1 & \dots \\ \beta^{j_1} & \beta^{j_2} & \dots \\ \vdots & \vdots & \\ (\beta^{j_1})^{n-k-1} & (\beta^{j_2})^{n-k-1} & \dots \end{bmatrix}$$

$$= \beta^{j_1+j_2+\dots+j_{n-k}} \cdot \prod_{\substack{i,\ell \in \{1,\dots,n-k\} \\ i>\ell}} (\beta^{j_i} - \beta^{j_\ell}) \neq 0$$

$$\Rightarrow d(C) = n-k+1$$

DEKODIRANJE REED-SOLOMONOVIH KODOV

$$g(t) = (t-\alpha)(t-\alpha^2)\cdots(t-\alpha^{d-1})$$

Kodna beseda: $c(t) = h(t) \cdot g(t)$

Prejeta beseda: $r(t) = c(t) + e(t)$

$$S_i := r(\alpha^i) = e(\alpha^i), \quad i \leq d-1$$

$$e(t) = \sum_{j=0}^{\ell-1} \lambda_j t^{a_j}, \quad \ell \leq \frac{d-1}{2}$$

$$S_i = e(\alpha^i) = \sum_{j=0}^{\ell-1} \lambda_j (\alpha^{a_j})^i$$

$$X_j = \alpha^{a_j}$$

$$S_1 = \lambda_0 X_0 + \lambda_1 X_1 + \dots + \lambda_{\ell-1} X_{\ell-1}$$
$$S_2 = \lambda_0 X_0^2 + \lambda_1 X_1^2 + \dots + \lambda_{\ell-1} X_{\ell-1}^2$$
$$S_{d-1} = \lambda_0 X_0^{d-1} + \lambda_1 X_1^{d-1} + \dots + \lambda_{\ell-1} X_{\ell-1}^{d-1}$$

$$\sigma(t) := \prod_{i=0}^{\ell-1} (1 - X_i t) = 1 + \sigma_1 t + \sigma_2 t^2 + \dots + \sigma_\ell t^\ell$$

$\lambda_j X_j^{\ell+u} \cdot \sigma(X_j^{-1}) = 0$ za vse $j = 0, \dots, \ell-1$, $u = 1, \dots, \ell$

$$\Rightarrow 0 = \sum_{j=0}^{\ell-1} \lambda_j X_j^{\ell+u} \left(1 + \sum_{i=1}^{\ell} \sigma_i X_j^{-i}\right)$$

$$= S_{u+\ell} + \sum_{i=1}^{\ell} \sigma_i \sum_{j=0}^{\ell-1} \lambda_j X_j^{\ell+u-i}$$

$$= S_{u+\ell} + \sum_{i=1}^{\ell} \sigma_i \cdot S_{\ell+u-i}$$

Dobimo nov sistem enačb:

$$\begin{bmatrix} S_1 & S_2 & \cdots & S_\ell \\ S_2 & S_3 & \cdots & S_{\ell+1} \\ \vdots & \vdots & & \vdots \\ S_\ell & S_{\ell+1} & \cdots & S_{2\ell} \end{bmatrix} \begin{bmatrix} \sigma_\ell \\ \sigma_{\ell-1} \\ \vdots \\ \sigma_1 \end{bmatrix} = - \begin{bmatrix} S_{\ell+1} \\ S_{\ell+2} \\ \vdots \\ S_{2\ell} \end{bmatrix}$$

S_i poznamo

rešimo sistem

$\Rightarrow$ Dobimo σ_i

$\Rightarrow$ Dobimo polinom $\sigma(t)$

$\Rightarrow$ Ničle $\sigma(t)$ določijo X_i-je

$\Rightarrow$ X_i-ji določijo lokacije napak

$\Rightarrow$ Z rešitvijo linearnega sistema dobimo še λ_i (napake)