Teorija števil

Eulerjeva funkcija

Eulerjeva funkcija nam pove koliko je obrnlivih elementov v $\mathbb{Z}_m$. $|\mathbb{Z}_m^*| = \varphi(m)$

Za $n \in \mathbb{N}$ s paraštevilskim razcepom $n = p_1^{\alpha_1} \cdot ... \cdot p_m^{\alpha_m}$ velja:

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot ... \cdot \varphi(p_m^{\alpha_m}) = n \prod_{p_k \in \mathbb{P}} \left(1 - \frac{1}{p_k}\right)$$

Eulerjev izrek: Naj bo G končna grupa. Potem red elementa $a \in G$ deli red grupe G.

$$\gcd(a, m) = 1 \Leftrightarrow a^{\varphi(m)} \equiv_m 1; a \in \mathbb{Z}_m^*$$

$$a, m \in \mathbb{N} \wedge \gcd(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv_m 1$$

$$a^{\varphi(m)} = 1 \text{ v } \mathbb{Z}_m^*$$

Mali Frematov izrek: če je $m \in \mathbb{P}$ ($\varphi(m) = m-1$) in $\gcd(a, m) = 1$, potem: $a^{m-1} \equiv_m 1$

Frematov test praštevilskosti

p praštevilo $\implies a^{p-1} \equiv_p 1$

Če želimo preveriti ali je p praštevilo, zgornjo trditev preizkusimo za nekaj naključnih a-jev.

Miller-Rabinov test

Zapišemo $n - 1 = 2^s d$ z lihim d. Če je n praštevilo, za naključno a velja $a^d \equiv_n 1$ ali $\exists r \in \{0, \ldots, s-1\} : a^{2^r d} \equiv_n -1$. Napaka testa za sestavljeno število je največ 1/4 na ponovitev.

REA (Razširjen Evklidov algoritem)

REA poišče ne le gcd(a,b) ampak tudi $s, t \in \mathbb{Z}$, da velja $a \cdot s + b \cdot t = \gcd(a,b)$.

Postopek

Začetne vrednosti: $r_{-1} = a \quad s_{-1} = 1 \quad t_{-1} = 0$
$r_1 = b \quad s_1 = 0 \quad t_1 = 1$

Iteracija za i = 1,2,... n+1, kjer je n+1 najmanjši indeks, za katerega $r_{n+1} = 0$:

$$k_i = \lfloor \tfrac{r_{i-2}}{r_{i-1}} \rfloor$$
$$r_i = r_{i-2} - k \cdot r_{i-1}$$
$$s_i = s_{i-2} - k \cdot s_{i-1}$$
$$t_i = t_{i-2} - k \cdot t_{i-1}$$

	a	1	0
k_1	b	0	1
k_2	r_1	s_1	t_1
k_3	r_2	s_2	t_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$
k_{n+1}	$r_n \neq 0$	s_n	t_n
	$r_{n+1} = 0$	s_{n+1}	t_{n+1}

$$a \cdot s_i + b \cdot t_i = r_i \quad \text{za } i = -1, 0, 1, \ldots, n+1$$
$$r_n \mid r_i \quad \text{za } i = n, n-1, \ldots, 0, -1$$
$$\gcd(a, b) = r_n$$

Linearne diofantske enačbe

Diofantska enačba $ax + by = c$ ima rešitev $\Leftrightarrow gcd(a,b)|c$.

Če ima eno rešitev $(x_0, y_0) \in \mathbb{Z}^2$ ima neskončno množico rešitev: $\{(x_k, y_k) : k \in \mathbb{Z}\}$

$$x_k = x_0 - k\frac{b}{\gcd(\text{a, b})} \quad y_k = y_0 + k\frac{a}{\gcd(\text{a, b})}$$

Grupe

Naj bo $(G, \cdot)$ grupa. **Red elementa** $\#a$ je najmanjše naravno število $n \in \mathbb{N}$, da velja $a^n = e$. **Red grupe** je število elementov G, oznaka $|G|$. Grupa je **ciklična**, če vsebuje a reda $|G|$:

$$G = \left\{a, a^2, a^3, \ldots, a^{|G|} = e\right\}$$

Množica $\mathbb{Z}_m = \{0, 1, ..., m-1\}$ Vpeljemo seštevanje $+_m$ po modulu m in množenje $\cdot_m$ po modulu m. Dobimo grupo $(\mathbb{Z}_m, +_m)$ in monoid $(\mathbb{Z}_m, \cdot_m)$. Red elementa $x \in \mathbb{Z}_m$ je $\frac{m}{\gcd(m,x)}$. $\mathbb{Z}_m^* = \mathbb{Z}_m \setminus \{0\}$. $|\mathbb{Z}_m^*| = \varphi(m)$. Element $x \in \mathbb{Z}_m$ je obrnljiv, če se da rešiti *diofantsko enačbo* za neznanki y (inverz od x) in k: $xy + km = 1$

Grupa $\mathbb{Z}_p^*$

$$(\mathbb{Z}_p^*, \cdot) \cong (\mathbb{Z}_{p-1}, +)$$

$$\text{red}_{\mathbb{Z}_p^*}(\alpha^i) = \text{red}_{\mathbb{Z}_{p-1}}(i) = \frac{p-1}{\gcd(i, p-1)}$$

x je generator grupe $\mathbb{Z}_p^* \iff \#x = p - 1$

x je generator grupe $\mathbb{Z}_p^* \iff x^{\frac{p-1}{p_i}} \neq 1 \mod p$, za vsak i, jer je $p - 1 = p_1^{k_1} \ldots p_l^{k_l}$.

Končni obsegi

$(K, +, \cdot)$ je obseg, če je

- $(K, +)$ abelova grupa
- $(K^*, \cdot)$ grupa ($K^* = K \setminus \{0\}$)
- velja distributivnost

Obseg je **komutativen**, če je $(K^*, \cdot)$ komutativna.

Praštevilski obsegi

Če je p praštevilo, je $(\mathbb{Z}_p, +_p, \cdot_p)$ končen obseg.

Galoisovi obsegi

$$\text{GF}(p) \cong \mathbb{Z}_p \qquad p \in \mathbb{P}$$

$$\text{GF}(p^n) \cong \mathbb{Z}_p[x]/(u)$$

- $u \in \mathbb{Z}_p[x]$ je nerazcepen polinom stopnje n
- elementi $\text{GF}(p^n)$ so ostanki polinomov iz $\mathbb{Z}_p$ pri deljenju z polinomom u
- seštevanje je enako kot seštevanje v $\mathbb{Z}_p[x]$
- produkt izračunamo v $\mathbb{Z}_p[x]$ nato pa vzamemo ostanek pri deljenju z u

Množica neničelnih/obrnljivih elementov $(GF(p^n)^*, \cdot) \cong (\mathbb{Z}_{p^n-1}, \cdot)$ je vedno izomorfna neki ciklični grupi. Generatorjem te grupe rečemo **primitivni elementi** Galoisovega obsega.

Kitajski izrek o ostankih

Naj bodo $n_1, \ldots, n_k$ paroma tuja.

$$x \equiv a_1 \mod n_1 \ldots x \equiv a_k \mod n_k$$

Vse rešitve zgornjega sistema so kongurentne po modulu $N = n_1 \cdot n_2 \cdot \cdots \cdot n_k$.

$$N_i = \frac{N}{n_i} \qquad M_i = \text{ inverz } N_i \text{ po modulu } n_i$$
$$x = \sum_{i=1}^{k} a_i M_i N_i \mod N$$

Če so si vsi n_i med sabo tuji, potem preslikava definira izomorfizem kolobarja

$$x \bmod N \mapsto (x \bmod n_1, x \bmod n_2, \ldots, x \bmod n_k)$$

$$(\mathbb{Z}/N\mathbb{Z}, +, \cdot) \cong (\mathbb{Z}/n_1\mathbb{Z}, +, \cdot) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z}, +, \cdot),$$

kjer je $N = n_1 \cdot n_2 \cdot \cdots \cdot n_k$.

RSA

$n = pq$ kjer sta p in q različni veliki praštevili.
$m = \varphi(n) = (p-1)(q-1)$
Potem je kriptosistem podan z:

$$\mathcal{B} = \mathcal{C} = \mathbb{Z}_n \qquad E_{(n,e)}(x) \equiv x^e \mod n$$
$$\mathcal{K} = \{n\} \times \mathbb{Z}_m^* \qquad E_{(n,d)}(y) \equiv y^d \mod n$$

e mora biti tuj m. Kodirnemu ključu (n, e) pripada dekodirni ključ (n, d), kjer je $d = e^{-1} \in \mathbb{Z}_m^*$

Modularno potenciranje - algoritem kvadriranja in množenja

$a^m \bmod n$ za velike vrednosti. Potem za dvojiško predstavitev $m = (b_{k-1} \ldots b_0)_2$:

```
p = 1
za i = 0,..., k-1:
    ce je b_i = 1: p = p * a mod n
    a = a^2 mod n
vrni p
```

Problem diskretnega logaritma

Naj bo G multiplikativna grupa. Za dana $\alpha, \beta \in G$, kjer je $red\alpha = n$, je treba poiskati takšen $x \in \{0, \ldots, n-1\}$, da je $\alpha^x = \beta$ Številu x rečemo diskretni logaritem elementa β z osnovo α.

Shanksov algoritem (veliki korak - mali korak)

```
vhod: G grupa, α, β ∈ G, n = red(α)
izhod: x = log_α β
m = ⌈√n⌉
za j = 0, ..., m - 1:
    (j, α^(m-j)) → L_1
uredi L_1 po drugi komponenti
za i = 0, ..., m - 1:
    (i, βα^(-i)) → L_2
uredi L_2 po drugi komponenti
poisci (j, y) ∈ L_1 in (i, y) ∈ L_2
x = (mj + i)
vrni x
```

Diffie-Hellmanova izmenjava ključev

- Alenka in Bojan se dogovorita za veliko praštevilo p in $\alpha \in \mathbb{Z}_p^*$, ki ima velik red n.
- Alenka si izbere naključno število $a \in [n]$, izračuna $A = \alpha^a \mod p$ in pošlje A Bojanu.
- Bojan si izbere naključno število $b \in [n]$, izračuna $B = \alpha^b \mod p$ in pošlje B Alenki.
- Alenka in bojan vsak zase izračunata skupni tajni ključ $K = \alpha^{ab} = A^b = B^a$

Varnost temelji na težavnosti diskretnega logaritma.

ElGamalov kriptosistem

- Alenka in Bojan izmenjata tajni ključ k z Diffie-Hellmanovo shemo
- Alenka želi poslati sporočilo x. Izračuna kriptogram $y = k \cdot x \mod p$ in ga pošlje Bojanu.
- Bojan izračuna $x = k^{-1} \cdot y \mod p$

Formalna definicija:

$$\mathcal{B} = \mathcal{C} = \mathbb{Z}_p^* \qquad E_{(a,B)}(x) \equiv B^a \cdot x \mod p$$
$$\mathcal{K} = \mathbb{Z}_p^* \times \mathbb{Z}_p^* \qquad D_{(b,A)}(y) \equiv A^{p-b-1} \cdot y \mod p$$

Naj bo $B = \alpha^b \mod p$ in $A = \alpha^a \mod p$. Potem kodirnemu ključu (a, B) ustreza dekodirni ključ (b, A). Bojan izbere skrivni ključ b in izračuna $B \equiv \alpha^b \pmod p$. Objavi svoj javni ključ (p, α, B).

Učenje z napakami (LWE)

Naj bo $A \in \mathbb{Z}_p^{m \times n}$, $x \in \mathbb{Z}_p^n$, $e \in \mathbb{Z}_p^m$ (majhen šum):

$$y \equiv Ax + e \pmod p.$$

Če bi bil $e = 0$, bi dobili navaden linearni sistem; pri LWE je zaradi šuma iskanje x težko.

Sporočilo $\mu \in \mathbb{Z}_q$ kodiramo z razdelitvijo $\mathbb{Z}_p$ na q odsekov:

$$m(\mu) = \left\lfloor \frac{p}{q} \right\rfloor \mu \in \mathbb{Z}_p,$$

privzeto $q = 2$ (bita 0/1).

Tajni ključ: x. Javni ključ: (A, y), kjer je $y = Ax + e$.

Šifriranje ($s \in \{0,1\}^m$):

$$c_1 = A^T s, \qquad c_2 = y^T s + m(\mu), \qquad c = (c_1, c_2).$$

Dešifriranje: $w = c_2 - x^T c_1 = e^T s + m(\mu)$. Odločimo μ po najbližjem odseku v $\mathbb{Z}_p$. Korektnost velja, če

$$|e^T s| < \frac{1}{2} \left\lfloor \frac{p}{q} \right\rfloor.$$

Veriženje kodnih blokov (CBC)

Izberemo inicializacijski vektor IV dolžine n. Napaka na bloku c_j vpliva le na b_j in b_{j+1}

Kodiranje

```
c_0 = IV
za j = 1, ..., m:
    c_j = E_e(b_j ⊕ c_{j-1})
c = c_1 ... c_m
```

Dekodiranje

```
c_0 = IV
za j = 1, ..., m:
    b_j = D_e(c_j) ⊕ c_{j-1}
b = b_1 ... b_m
```

Napadi na kriptosisteme

- **Napad z izbranim besedilom (CPA)**: napadalec ima dostop do oracle-a za kodiranje in lahko pridobi pare (b, c) za izbrana besedila b.
- **Napad z izbranim kriptogramom (CCA)**: napadalec lahko zahteva dešifriranje izbranih kriptogramov

Zgoščevalne funkcije

Zgoščevalna funkcija besedilu poljubne dolžine kratek izvleček. Želene lastnosti:

- **Naključnost**: Če se dve sporočili razlikujeta na enem samem mestu morata povzetka izgledati kot neodvisno izbrani naključni števili.
- **Odpornost praslik (enosmernost)**: za poljuben izvleček z je računsko nemogoče poiskati sporočilo x, ja je $h(x) = z$.
- **Odpornost drugih praslik**: za dano sporočilo x je nemogoče najti drugo sporočilo x', ki ima enak izvleček.
- **Odpornost na trke**: računsko je nemogoče poiskati dve različni sporočili x in x' z enakim povzetkom.

Trk je par različnih sporočil z enakim povzetkom.
Kompresijska funkcija: $f : \{0,1\}^{r+n} \to \{0,1\}^n$
Zgoščevalna funkcija: $h : \{0,1\}^* \to \{0,1\}^n$
Če je kompresijska funkcija odporna na trke, je tudi zgoščevalna funkcija odporna na trke.

Digitalni podpisi

Podpisovanje z algoritmom RSA

Naj bosta p, q praštevili in $n = pq$. Naj bo (n, d) zasebni in (n, e) javni ključ. Potem za $K = (n, e, d)$ definiramo:

$$\text{sig}_K(x) = x^d \mod n$$
$$\text{ver}_K(x, y) = (\text{true} \iff x = y^e \mod n)$$

ElGamalov sistem za digitalno podpisovanje

Generiranje ključa

Naj bo p takšno praštevilo, ja je v $\mathbb{Z}$ težko izračunati diskretni logaritem in $\alpha \in \mathbb{Z}_p^*$ primitivni element.

Potem je $\mathcal{B} = \mathbb{Z}_p^*$, $\mathcal{A} = \mathbb{Z}_p^* \times \mathbb{Z}_{p-1}$ in $\mathcal{K} = \{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \mod p\}$.

Število a je zasebno. Števila p, α in β pa so javna.

Podpisovanje

Podpisnik s ključem $K = (p, \alpha, a, \beta)$ izbere naključno skrito število $k \in \mathbb{Z}_{p-1}^*$ in določi:

$$r \equiv \alpha^k \mod p, \quad s \equiv (x - ar)k^{-1} \mod p$$

Preverjanje podpisa

$$\text{ver}_K(x, r, s) = (\text{true} \iff \beta^r r^s \equiv_p \alpha^x)$$

Digital Signature Standard (DSA)

Generiranje ključa

- Izberi 160-bitno praštevilo q
- Izberi 1024-bitno praštevilo p, da $q|(p-1)$
- Izberi element $h \in \mathbb{Z}_p^*$ in izračunaj $\alpha = h^{(p-1)/q} \mod p$; ponavljaj dokler $\alpha \neq 1$. (α je generator natanko določen ciklične grupe red q v $\mathbb{Z}_p^*$)
- Izberi naključno naravno število $a < q$
- Izračunaj $\beta = \alpha^a \mod p$
- Javni ključ osebe A je (p, q, α, β), zasebni pa a.

Opomba: red α, β, r je enak q.

Podpisovanje

- Izberi naključno naravno število $k < q$.
- Izračunaj $r = \left(\alpha^k \mod p\right) \mod q$
- Izračunaj $k^{-1} \mod q$.
- Izračunaj $s = k^{-1}(h(x) + ar) \mod q$, kjer je $h(x)$ SHA-1 povzetek sporočila x
- Če je $r = 0$ ali $s = 0$, začni ponovno.
- Podpis sporočila je (r, s).

Preverjanje podpisa

- Priskrbi si overjeno kopijo javnega ključa (p, q, α, β) podpisnika
- Izračunaj $w = s^{-1} \mod q$ in $h(x)$
- Izračunaj $e_1 = h(x)w \mod q$ in $e_2 = rw \mod q$
- Izračunaj $v = (\alpha^{e_1}\beta^{e_2} \mod p) \mod q$
- Sprejmi podpis, če je $v = r$

Kodi

Naj bo Σ končna abeceda. Definirajmo $\Sigma^* = \cup_{n=0}^{\infty}\Sigma^n$. **Kod** $\mathcal{C}$ nad abecedo Σ je končna podmnožica Σ^* ($\mathcal{C} \subset \Sigma^*$)

- **Kodiranje** je preslikava $f : \mathcal{S} \to \mathcal{C}$
- Po prenosu po komunikacijskem kanalu prejmemo besedo y.
- Če $y \notin \mathcal{C}$, ji po nekem pravilu priredimo besedo $x\prime \in \mathcal{C}$. Pravimo, da besedo **dekodiramo**.

Bločni kodi

Kod $\mathcal{C}$ nad abecedo Σ je **bločni kod dolžine** n, če imajo vse kodne besede dolžino n ($\mathcal{C} \subseteq \Sigma^n$).

Hammingova razdalja med besedama x in y je definirana kot $d(x, y) = |\{i; x_i \neq y_i\}|$.

Teža besede x ($t(x)$) je definirana kot število neničelnih mest v besedi.

Razmaknjenost koda:

$$d = d(\mathcal{C}) = \min\{d(x, y); x, y \in \mathcal{C}, x \neq y\}$$

Kod $\mathcal{C}$ označimo z (n, M, d)-kod, kjer je

n	...	bločna dolžina
M	...	št. kodnih besed
d	...	razmaknjenost

Pravila za dekodiranje

- **Pravilo najmanjše napake**
  Prejeto besedo y dekodiramo v tisti $x \in \mathcal{C}$, ki maksimizira $P[x \text{ oddana}|y \text{ sprejeta}]$

$$P[x|y] = \frac{P[y|x] \cdot P[x]}{P[y]} = \frac{P[y|x] \cdot P[x]}{\sum_{c \in \mathcal{C}} P[y|c] \cdot P[c]}$$

- **Pravilo največje verjetnosti**
  Prejeto besedo y dekodiramo v tisti $x \in \mathcal{C}$, ki maksimizira $P[y \text{ sprejeta}|x \text{ oddana}]$ *Če so vse kodne besede enako verjetne, sta PNN in PNV enaki.*
- **Pravilo najbližjega soseda**
  Prejeto besedo $y \in \Sigma^n$ dekodiramo v tisto besedo $x \in \mathcal{C}$, pri kateri je $d(x, y)$ najmanjša. *Če je $p < 1/2$, dajeta PNV in PNS enak rezultat.*

Verjetnostne formule

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \quad P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$
$$P(A) = \sum_{i=1}^{n} P(A|B_i)P(B_i)$$

Napaka

$y = x + e$, kjer je $e \in \Sigma^n$ **napaka**.

- Kod **odkrije** s napak, če $x + e \notin \mathcal{C}$ za vse $x \in \mathcal{C}$ in vse e, za katere je $1 \leq t(e) \leq s$
- Kod **popravi** s napak, če $d(x + e, x) < d(x + e, x')$ za vse $x, x' \in \mathcal{C}$ in vse $e \in \Sigma^n$, za katere je $t(e) \leq s$.

Bločni kod z dolžino n in razmaknjenostjo d **odkrije** $d - 1$ napak in **popravi** $\lfloor \frac{d-1}{2} \rfloor$ napak.

Linearni kodi

Kod $\mathcal{C} \subseteq \Sigma^n$ je **linearen**, če je vek. podprostor:

$$\forall c_1, c_2 \in \mathcal{C},\ \alpha, \beta \in \Sigma \implies \alpha c_1 + \beta c_2 \in \mathcal{C}$$

Dimenzija koda (k) je dimenzija vektorskega podporstora. $[n, k, d]$-kod nad $\Sigma = GF(q)$ je linearen (n, q^k, d)-kod.

$$d = \min_{x \in \mathcal{C}, x \neq 0} t(x) \quad M = q^k$$

Generatorska matrika G koda $\mathcal{C}$ je matrika velikosti $k \times n$. Njene vrstice so kodne besede, ki sestavljajo bazo kode (vektorskega podporstora).

Nadzorna matrika

$\mathcal{C}^\perp = \{x \in \Sigma^n; cx^T = 0\ \forall c \in \mathcal{C}\}$ je **dualni kod** koda $\mathcal{C}$. Generatorsko matriko koda $\mathcal{C}^\perp$ imenujemo **nadzorna matrika** koda $\mathcal{C}$

$$G \in \Sigma^{k \times n}, H \in \Sigma^{(n-k) \times n}$$
$$\text{rang}(G) = k, \text{rang}(H) = n - k$$

potem velja: G je generatorska in H nadzorna matrika nekega linearnega koda $\iff GH^T = 0$.

Sindrom

Sporočilo z napako $y = x + e$. Hy^T imenujemo **sindrom** besede y. Velja $Hy^T = He^T$

Kodiranje $c = sG$

Dekodiranje

- Izračunaj sindrom $\sigma = Hy^T$.
- Poišči napako e po sindromu ($He^T = \sigma$); če ni v tabeli, zahtevaj ponoven prenos.
- Vrni $x = y - e$.

Razmaknjenost

Naj bo $\mathcal{C}$ linearen kod nad abecedo $GF(q)$ z ndzorno matriko H. Potem velja:

$d(\mathcal{C}) \geq d \iff$ vsaka množica $d-1$ stolpcev matrike H je linearno neodvisna nad $GF(q)$

$d(\mathcal{C}) = \max\{d; \text{vsakih } d-1 \text{ stolpcev } H \text{ je lin. neodvisnih}\}$

Ekvivalentnost

Koda $\mathcal{C}_1 \sim \mathcal{C}_2$ sta **ekvivalentna**, če lahko iz enega dobimo drugega z zaporedjem transformacij **kodne matrike**

- permutacije stolpcev
- permutacije simbolov v izbranem stolpcu
- permutacije vrstic

Za vsak $[n, k, d]$-kod obstaja ekvivalenten kod z generatorsko matriko v standardni obliki

$$G = [I_k|A] \qquad H = [-A^T|I_{n-k}]$$

Hammingov kod reda r

nad $\Sigma = GF(q)$ je $[n, k, d]$-kod dolžine $n = \frac{q^r-1}{q-1}$ in dimenzije $k = n - r$, podan z nadzorno matriko $H \in \Sigma^{r \times n}$, v kateri sta vsaka dva stolpca linearno neodvisna. *Hammingovi kodi so popolni.*

Meje za kode

$$A_q(n, d) = \max\{M; \exists(n, M, d) \text{ kod nad } GF(q)\}$$
$$A_q(n, 1) = q^n \quad A_2(n, 2) = 2^{n-1}$$
$$|K(x, r)| = \sum_{k=0}^{r} \binom{n}{k}(q-1)^k$$

Hamingova zgornja meja

$$A_q(n, d) \leq \frac{q^n}{\sum_{k=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{k}(q-1)^k}$$

Če kod dosega Hammingovo mejo, je **popoln**.

Gilbert-Varshamova spodnja meja

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

Singletonova meja

Naj bo $\mathcal{C}$ (n, M, d)-kod nad $GF(q)$. Potem je $M \leq q^{n-d+1}$. Za linearni $[n, k, d]$-kod je $d \leq n - k + 1$. Linearni $[n, k, d]$-kod lahko popravi največ $\lfloor \frac{n-k}{2} \rfloor$ napak.

Ciklični kodi

Besedo $\hat{x} = x_n x_1 \cdots x_{n-1}$ imenujemo **ciklični pomik** besede x. Linearen kod je **cikličen**, če velja $x \in \mathcal{C} \Rightarrow \hat{x} \in \mathcal{C}$

Besedo $x = x_1 \cdots x_n$ identificiramo s polinomom

$$x(t) = x_1 + x_2 t + \cdots + x_n t^{n-1} \in GF(q)[t]/(t^n - 1)$$

Besedi $\hat{x}$ ustreza polinom $t \cdot x(t) (\mod t^n - 1)$.

Naj bo $\mathcal{C}$ cikličen kod in $g(t)$ neničeln polinom najmanjše stopnje v $\mathcal{C}$. Potem velja:

- $\mathcal{C} = \langle g(t) \rangle = \{g(t) \cdot a(t) \mod t^n - 1; a(t) \in GF(q)[t]\}$ (ideal, ki ga generira $g(t)$)
- $g(t) \mid (t^n - 1)$
- $\dim(\mathcal{C}) = k = n - \deg(g)$
- $B = \{g(t), tg(t), \cdots, t^{k-1}g(t)\}$ je baza $\mathcal{C}$.

Ciklični kodi dolžine n nad $GF(q)$ ustrezajo deliteljem polinoma $t^n - 1 \in GF(q)[t]$. Če $\mathcal{C} = \langle g(t) \rangle$, imenujemo g **generatorski polinom** koda $\mathcal{C}$.

$$G = \begin{bmatrix} g(t) \\ tg(t) \\ \vdots \\ t^{k-1}g(t) \end{bmatrix}$$

je generatorska matrika za $\mathcal{C}$.

Naj bo $c(t)$ polinom besede. Najmanjši ciklični kod, ki vsebuje $c(t)$, je ideal, ki ga generira

$$g(t) = \gcd(c(t),\ t^n - 1),$$

tj. $\langle g(t) \rangle$; dimenzija je $k = n - \deg g$.

$$t^{n-k+i} = q_i(t)g(t) + r_i(t)$$

Potem velja:

$$t^{n-k+i} - r_i(t) = q_i(t)g(t) \in \mathcal{C}$$

$$G' = \begin{bmatrix} -r_0(t) & 1 & 0 & \cdots & 0 \\ -r_1(t) & 0 & 1 & \cdots & 0 \\ \vdots & & & & \\ -r_{k-1}(t) & 0 & 0 & \cdots & 1 \end{bmatrix}$$

je potem generatorska matrika za $\mathcal{C}$.

Kodiranje

$t^{n-k}s(t) = q(t)g(t) + r(t) \implies x(t) = t^{n-k} \cdot s(t) - r(t) \in \mathcal{C}$

Sporočilo $s(x)$ pomnožimo z generatorskim polinomom $g(x)$

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