Asocijacijske sheme

Vedran Krčadinac

6.5.2024.

Hammingova shema i kodovi

Primjer: Hammingova shema

Neka je F skup od q simbola ("slova"). Skup vrhova $X = F^d$ sadrži sve uređene d-torke slova, koje zovemo riječima. Udaljenost riječi $x = (x_1, \ldots, x_d)$ i $y = (y_1, \ldots, y_d)$ definiramo kao broj različitih koordinata: $\partial(x, y) = |\{i \mid x_i \neq y_i\}|$. Funkcija $\partial : X \times X \to \mathbb{R}$ je takozvana Hammingova metrika. Neka su riječi $x, y \in X$ susjedne u grafu G_i ako su na udaljenosti $\partial(x, y) = i$. Tako dobijemo Hammingovu asocijacijsku shemu $H(d, q)$ s d klasa, reda $n = q^d$.

Hammingova shema i kodovi

Primjer: Hammingova shema

Neka je F skup od q simbola ("slova"). Skup vrhova $X = F^n$ sadrži sve uređene n-torke slova, koje zovemo riječima. Udaljenost riječi $x = (x_1, \ldots, x_n)$ i $y = (y_1, \ldots, y_n)$ definiramo kao broj različitih koordinata: $\partial(x, y) = |\{i \mid x_i \neq y_i\}|$. Funkcija $\partial : X \times X \to \mathbb{R}$ je takozvana Hammingova metrika. Neka su riječi $x, y \in X$ susjedne u grafu G_i ako su na udaljenosti $\partial(x, y) = i$. Tako dobijemo Hammingovu asocijacijsku shemu $H(n, q)$ s n klasa, reda $N = q^n$.

Hammingova shema i kodovi

Primjer: Hammingova shema

Neka je F skup od q simbola ("slova"). Skup vrhova $X = F^n$ sadrži sve uređene n-torke slova, koje zovemo riječima. Udaljenost riječi $x = (x_1, \ldots, x_n)$ i $y = (y_1, \ldots, y_n)$ definiramo kao broj različitih koordinata: $\partial(x, y) = |\{i \mid x_i \neq y_i\}|$. Funkcija $\partial : X \times X \to \mathbb{R}$ je takozvana Hammingova metrika. Neka su riječi $x, y \in X$ susjedne u grafu G_i ako su na udaljenosti $\partial(x, y) = i$. Tako dobijemo Hammingovu asocijacijsku shemu $H(n, q)$ s n klasa, reda $N = q^n$.

Definicija.

Za podskup vrhova Hammingove sheme $C \subseteq F^n$ veličine $M = |C|$ kažemo da je kod s parametrima $(n, M, d)_q$ ako je minimalna udaljenost kodnih riječi $d = \min\{\partial(x, y) \mid x, y \in C,\ x \neq y\}$. Elemente od F^n zovemo vektorima, a elemente od C kodnim riječima.

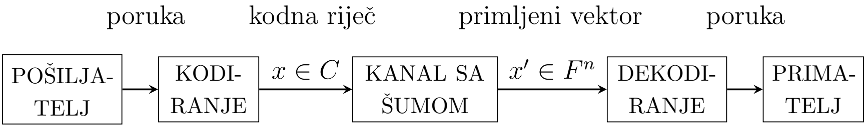
Hammingova shema i kodovi

Primjer: Hammingova shema

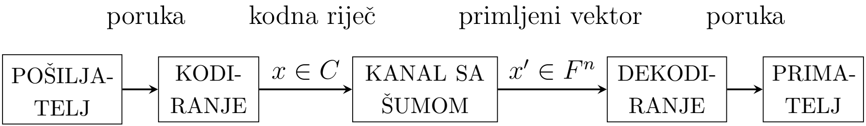
Neka je F skup od q simbola ("slova"). Skup vrhova $X = F^n$ sadrži sve uređene n-torke slova, koje zovemo riječima. Udaljenost riječi $x = (x_1, \ldots, x_n)$ i $y = (y_1, \ldots, y_n)$ definiramo kao broj različitih koordinata: $\partial(x, y) = |\{i \mid x_i \neq y_i\}|$. Funkcija $\partial : X \times X \to \mathbb{R}$ je takozvana Hammingova metrika. Neka su riječi $x, y \in X$ susjedne u grafu G_i ako su na udaljenosti $\partial(x, y) = i$. Tako dobijemo Hammingovu asocijacijsku shemu $H(n, q)$ s n klasa, reda $N = q^n$.

Definicija.

Za potprostor vrhova Hammingove sheme $C \leq \mathbb{F}_q^n$ dimenzije $m = \dim C$ kažemo da je linearni kod s parametrima $[n, m, d]_q$ ako je minimalna udaljenost kodnih riječi $d = \min\{\partial(x, y) \mid x, y \in C,\ x \neq y\}$. Elemente od $\mathbb{F}_q^n$ zovemo vektorima, a elemente od C kodnim riječima.


poruka
kodna riječ
primljeni vektor
poruka
POŠILJA-TELJ
KODI-RANJE
$x \in C$
KANAL SA ŠUMOM
$x' \in F^n$
DEKODI-RANJE
PRIMA-TELJ

Kodiranje s ispravljanjem pogrešaka



Propozicija.

Kod C s parametrima $(n, M, d)_q$ može otkriti bilo kojih $d-1$ ili manje pogrešaka i ispraviti bilo kojih $e = \lfloor \frac{d-1}{2} \rfloor$ ili manje pogrešaka.

Ocjene za parametre kodova

Propozicija (Singletonova ocjena)

Ako postoji $(n, M, d)_q$ kod C, onda vrijedi

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

Ocjene za parametre kodova

Propozicija (Singletonova ocjena)

Ako postoji $(n, M, d)_q$ kod C, onda vrijedi

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

Verzija za linearne kodove: $m \leq n - d + 1$

Ocjene za parametre kodova

Propozicija (Singletonova ocjena)

Ako postoji $(n, M, d)_q$ kod C, onda vrijedi

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

Verzija za linearne kodove: $m \leq n - d + 1$

Propozicija (Ocjena pakiranja kugli)

Ako postoji $(n, M, d)_q$ kod C i ako je $e = \lfloor \frac{d-1}{2} \rfloor$, onda vrijedi

$$M \leq \frac{q^n}{\sum\limits_{i=0}^{e} \binom{n}{i}(q-1)^i}$$

Linearni kodovi

Težina vektora $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$:

$$w(x) = |\{i \in \{1, \ldots, n\} \mid x_i \neq 0\}|$$

Linearni kodovi

Težina vektora $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$:

$$w(x) = |\{i \in \{1, \ldots, n\} \mid x_i \neq 0\}|$$

Minimalna težina koda C:

$$w(C) = \min\{w(x) \mid x \in C, x \neq 0\}$$

Linearni kodovi

Težina vektora $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$:

$$w(x) = |\{i \in \{1, \ldots, n\} \mid x_i \neq 0\}|$$

Minimalna težina koda C:

$$w(C) = \min\{w(x) \mid x \in C, x \neq 0\}$$

Propozicija.

Za linearne kodove minimalna težina jednaka je minimalnoj udaljenosti koda.

$$d(C) = \{\partial(x, y) \mid x, y \in C,\ x \neq y\}$$

Linearni kodovi

Definicija.

Generirajuća matrica linearnog $[n, m, d]_q$ koda C je $m \times n$ matrica G kojoj reci čine bazu od C. Kažemo da je u standardnom obliku ako je $G = [\, I \;\, A\,]$, gdje je I jedinična $m \times m$ matrica, a A je neka $m \times (n - m)$ matrica nad $\mathbb{F}_q$.

Linearni kodovi

Definicija.

Generirajuća matrica linearnog $[n, m, d]_q$ koda C je $m \times n$ matrica G kojoj reci čine bazu od C. Kažemo da je u standardnom obliku ako je $G = [\, I \;\, A \,]$, gdje je I jedinična $m \times m$ matrica, a A je neka $m \times (n-m)$ matrica nad $\mathbb{F}_q$.

Poruke: vektori iz $\mathbb{F}_q^m$

Linearni kodovi

Definicija.

Generirajuća matrica linearnog $[n, m, d]_q$ koda C je $m \times n$ matrica G kojoj reci čine bazu od C. Kažemo da je u standardnom obliku ako je $G = [\,I\ A\,]$, gdje je I jedinična $m \times m$ matrica, a A je neka $m \times (n-m)$ matrica nad $\mathbb{F}_q$.

Poruke: vektori iz $\mathbb{F}_q^m$

Kodiranje: injektivna funkcija iz $\mathbb{F}_q^m \to \mathbb{F}_q^n$ kojoj je slika C

Linearni kodovi

Definicija.

Generirajuća matrica linearnog $[n, m, d]_q$ koda C je $m \times n$ matrica G kojoj reci čine bazu od C. Kažemo da je u standardnom obliku ako je $G = [\, I \;\, A \,]$, gdje je I jedinična $m \times m$ matrica, a A je neka $m \times (n-m)$ matrica nad $\mathbb{F}_q$.

Poruke: vektori iz $\mathbb{F}_q^m$

Kodiranje: injektivna funkcija iz $\mathbb{F}_q^m \to \mathbb{F}_q^n$ kojoj je slika C

$$u \mapsto u\,G, \quad \forall u \in \mathbb{F}_q^m$$

Linearni kodovi

Definicija.

Generirajuća matrica linearnog $[n, m, d]_q$ koda C je $m \times n$ matrica G kojoj reci čine bazu od C. Kažemo da je u standardnom obliku ako je $G = [\,I\ A\,]$, gdje je I jedinična $m \times m$ matrica, a A je neka $m \times (n-m)$ matrica nad $\mathbb{F}_q$.

Poruke: vektori iz $\mathbb{F}_q^m$

Kodiranje: injektivna funkcija iz $\mathbb{F}_q^m \to \mathbb{F}_q^n$ kojoj je slika C

$$u \mapsto u\,G, \quad \forall u \in \mathbb{F}_q^m$$

Ako je $G = [\,I\ A\,]$ u standardnom obliku i $A = [\alpha_{ij}]$:

$$u\,G = (x_1, \ldots, x_n), \quad x_i = u_i \quad \text{za } i = 1, \ldots, m$$

$$x_{m+j} = \sum_{i=1}^{m} \alpha_{ij} u_i \quad \text{za } j = 1, \ldots, n-m$$

Linearni kodovi

Primjer: binarni $[7,4,3]_2$ kod $(n=7,\ m=4,\ d=3,\ q=2,\ e=1)$

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

Linearni kodovi

Primjer: binarni $[7,4,3]_2$ kod $(n=7,\ m=4,\ d=3,\ q=2,\ e=1)$

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

$0 \to 0000\ 000$	$4 \to 0100\ 101$	$8 \to 1000\ 110$	$\mathrm{C} \to 1100\ 011$
$1 \to 0001\ 111$	$5 \to 0101\ 010$	$9 \to 1001\ 001$	$\mathrm{D} \to 1101\ 100$
$2 \to 0010\ 011$	$6 \to 0110\ 110$	$\mathrm{A} \to 1010\ 101$	$\mathrm{E} \to 1110\ 000$
$3 \to 0011\ 100$	$7 \to 0111\ 001$	$\mathrm{B} \to 1011\ 010$	$\mathrm{F} \to 1111\ 111$

Dualni kod

Produkt vektora $x = (x_1, \ldots, x_n)$ i $y = (y_1, \ldots, y_n)$:

$$x \cdot y = \sum_{i=1}^{n} x_i y_i$$

Dualni kod

Produkt vektora $x = (x_1, \ldots, x_n)$ i $y = (y_1, \ldots, y_n)$:

$$x \cdot y = \sum_{i=1}^{n} x_i y_i$$

Vektori su ortogonalni ako je $x \cdot y = 0$.

Dualni kod

Produkt vektora $x = (x_1, \ldots, x_n)$ i $y = (y_1, \ldots, y_n)$:

$$x \cdot y = \sum_{i=1}^{n} x_i y_i$$

Vektori su ortogonalni ako je $x \cdot y = 0$.

Dualni kod:

$$C^{\perp} = \{x \in \mathbb{F}_q^n \mid x \cdot y = 0,\ \forall y \in C\}$$

Dualni kod

Produkt vektora $x = (x_1, \ldots, x_n)$ i $y = (y_1, \ldots, y_n)$:

$$x \cdot y = \sum_{i=1}^{n} x_i y_i$$

Vektori su ortogonalni ako je $x \cdot y = 0$.

Dualni kod:

$$C^\perp = \{x \in \mathbb{F}_q^n \mid x \cdot y = 0,\ \forall y \in C\}$$

Propozicija.

Ako je $\dim C = m$, onda je $C^\perp$ linearni kod dimenzije $n - m$.

Dualni kod

Produkt vektora $x = (x_1, \ldots, x_n)$ i $y = (y_1, \ldots, y_n)$:

$$x \cdot y = \sum_{i=1}^{n} x_i y_i$$

Vektori su ortogonalni ako je $x \cdot y = 0$.

Dualni kod:

$$C^\perp = \{x \in \mathbb{F}_q^n \mid x \cdot y = 0,\ \forall y \in C\}$$

Propozicija.

Ako je $\dim C = m$, onda je $C^\perp$ linearni kod dimenzije $n - m$.

Propozicija.

Za svaki linearni kod $C \leq \mathbb{F}_q^n$ vrijedi $(C^\perp)^\perp = C$.

Dualni kod

Matrica provjere parnosti koda C je generirajuća matrica od $C^{\perp}$

Dualni kod

Matrica provjere parnosti koda C je generirajuća matrica od $C^\perp$

Ako je C kod duljine n i dimenzije m:

$$G \rightsquigarrow m \times n \text{ matrica}$$

$$P \rightsquigarrow (n-m) \times n \text{ matrica}$$

Dualni kod

Matrica provjere parnosti koda C je generirajuća matrica od $C^\perp$

Ako je C kod duljine n i dimenzije m:

$$G \rightsquigarrow m \times n \text{ matrica}$$

$$P \rightsquigarrow (n-m) \times n \text{ matrica}$$

Propozicija.

Neka je P matrica provjere parnosti koda C. Vektor $x \in \mathbb{F}_q^n$ pripada kodu C ako i samo ako je $xP^\tau = 0$.

Dualni kod

Matrica provjere parnosti koda C je generirajuća matrica od $C^\perp$

Ako je C kod duljine n i dimenzije m:

$$G \rightsquigarrow m \times n \text{ matrica}$$

$$P \rightsquigarrow (n-m) \times n \text{ matrica}$$

Propozicija.

Neka je P matrica provjere parnosti koda C. Vektor $x \in \mathbb{F}_q^n$ pripada kodu C ako i samo ako je $xP^\tau = 0$.

Dekodiranje pomoću sindromoma $xP^\tau \ldots$

Dualni kod

Matrica provjere parnosti koda C je generirajuća matrica od $C^\perp$

Ako je C kod duljine n i dimenzije m:

$$G \rightsquigarrow m \times n \text{ matrica}$$

$$P \rightsquigarrow (n-m) \times n \text{ matrica}$$

Propozicija.

Neka je P matrica provjere parnosti koda C. Vektor $x \in \mathbb{F}_q^n$ pripada kodu C ako i samo ako je $xP^\tau = 0$.

Dekodiranje pomoću sindromoma $xP^\tau \dots$

Propozicija.

Neka je $G = [\,I\ A\,]$ generirajuća matrica koda C. Tada je $P = [\,-A^\tau\ I\,]$ matrica provjere parnosti tog koda. Slovo I u matrici G označava jediničnu matricu reda m, a u P jediničnu matricu reda $n-m$.

Dualni kod

Primjer: binarni $[7,4,3]_2$ kod $(n=7,\ m=4,\ d=3,\ q=2,\ e=1)$

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

Dualni kod

Primjer: binarni $[7,4,3]_2$ kod ($n=7,\ m=4,\ d=3,\ q=2,\ e=1$)

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

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

Dualni kod

Propozicija.

Neka je C linearni kod s matricom provjere parnosti P. Minimalna težina od C jednaka je minimalnom broju linearno zavisnih stupaca od P. Točnije, vrijedi $w(C) = d$ ako i samo ako u P postoji d linearno zavisnih stupaca, a bilo kojih $d - 1$ ili manje stupaca su linearno nezavisni.

Dualni kod

Propozicija.

Neka je C linearni kod s matricom provjere parnosti P. Minimalna težina od C jednaka je minimalnom broju linearno zavisnih stupaca od P. Točnije, vrijedi $w(C) = d$ ako i samo ako u P postoji d linearno zavisnih stupaca, a bilo kojih $d - 1$ ili manje stupaca su linearno nezavisni.

Težinski polinom:

$$W_C(X, Y) = \sum_{x \in C} X^{n-w(x)} Y^{w(x)} = \sum_{i=0}^{n} A_i X^{n-i} Y^i$$

$$A_i = |\{x \in C \mid w(x) = i\}|$$

Dualni kod

Propozicija.

Neka je C linearni kod s matricom provjere parnosti P. Minimalna težina od C jednaka je minimalnom broju linearno zavisnih stupaca od P. Točnije, vrijedi $w(C) = d$ ako i samo ako u P postoji d linearno zavisnih stupaca, a bilo kojih $d-1$ ili manje stupaca su linearno nezavisni.

Težinski polinom:

$$W_C(X,Y) = \sum_{x\in C} X^{n-w(x)} Y^{w(x)} = \sum_{i=0}^{n} A_i X^{n-i} Y^i$$

$$A_i = |\{x \in C \mid w(x) = i\}|$$

Teorem (MacWilliamsin identitet)

Za linearni kod C nad $\mathbb{F}_q$ vrijedi

$$W_{C^\perp}(X,Y) = \frac{1}{|C|} W_C(X+(q-1)Y, X-Y)$$

Dualni kod

```
gap> LoadPackage("GUAVA");;
gap> G:=[[1, 0, 0, 0, 1, 1, 0],
         [0, 1, 0, 0, 1, 0, 1],
         [0, 0, 1, 0, 0, 1, 1],
         [0, 0, 0, 1, 1, 1, 1]];;
gap> C:=GeneratorMatCode(G,GF(2));
a linear [7,4,1..3]1 code defined by gen. matrix over GF(2)
gap> CodeWeightEnumerator(C);
x_1^7+7*x_1^4+7*x_1^3+1
gap> D:=DualCode(C);
a linear [7,3,4]2..3 dual code
gap> CodeWeightEnumerator(D);
7*x_1^4+1
```

Dualni kod

```
gap> LoadPackage("GUAVA");;
gap> G:=[[1, 0, 0, 0, 1, 1, 0],
         [0, 1, 0, 0, 1, 0, 1],
         [0, 0, 1, 0, 0, 1, 1],
         [0, 0, 0, 1, 1, 1, 1]];;
gap> C:=GeneratorMatCode(G,GF(2));
a linear [7,4,1..3]1 code defined by gen. matrix over GF(2)
gap> CodeWeightEnumerator(C);
x_1^7+7*x_1^4+7*x_1^3+1
gap> D:=DualCode(C);
a linear [7,3,4]2..3 dual code
gap> CodeWeightEnumerator(D);
7*x_1^4+1
```

$$W_C(X,Y) = X^7 + 7X^4Y^3 + 7X^3Y^4 + Y^7, \quad W_D(X,Y) = X^7 + 7X^3Y^4$$

Hammingovi kodovi

$\mathbb{F}_q = \{\alpha_0, \alpha_1, \ldots, \alpha_{q-1}\}$, $\alpha_0 = 0$, $\alpha_1 = 1$

Hammingovi kodovi

$\mathbb{F}_q = \{\alpha_0, \alpha_1, \ldots, \alpha_{q-1}\}$, $\alpha_0 = 0$, $\alpha_1 = 1$

$$P = \begin{bmatrix} 0 & 0 & 0 & 0 & \cdots & 0 & \cdots\cdots & 1 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & \cdots\cdots & 0 & 0 & 0 & \cdots & \alpha_{q-1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & 1 & 1 & \cdots & 1 & \cdots\cdots & 0 & 0 & 0 & \cdots & \alpha_{q-1} \\ 1 & 0 & 1 & \alpha_2 & \cdots & \alpha_{q-1} & \cdots\cdots & 0 & 1 & \alpha_2 & \cdots & \alpha_{q-1} \end{bmatrix}$$

Hammingovi kodovi

$\mathbb{F}_q = \{\alpha_0, \alpha_1, \ldots, \alpha_{q-1}\}$, $\alpha_0 = 0$, $\alpha_1 = 1$

$$P = \begin{bmatrix} 0 & 0 & 0 & 0 & \cdots & 0 & \cdots\cdots & 1 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & \cdots\cdots & 0 & 0 & 0 & \cdots & \alpha_{q-1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & 1 & 1 & \cdots & 1 & \cdots\cdots & 0 & 0 & 0 & \cdots & \alpha_{q-1} \\ 1 & 0 & 1 & \alpha_2 & \cdots & \alpha_{q-1} & \cdots\cdots & 0 & 1 & \alpha_2 & \cdots & \alpha_{q-1} \end{bmatrix}$$

Primjer (Hammingovi kodovi)

Linearni kod definiran matricom provjere parnosti P zovemo q-arnim Hammingovim kodom s parametrom r i označavamo $\mathrm{Ham}(r, q)$. To je $[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3]_q$ kod koji dostiže ocjenu pakiranja kugli.

Hammingovi kodovi

$\mathbb{F}_q = \{\alpha_0, \alpha_1, \ldots, \alpha_{q-1}\}$, $\alpha_0 = 0$, $\alpha_1 = 1$

$$P = \begin{bmatrix} 0 & 0 & 0 & 0 & \cdots & 0 & \cdots\cdots & 1 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & \cdots\cdots & 0 & 0 & 0 & \cdots & \alpha_{q-1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & 1 & 1 & \cdots & 1 & \cdots\cdots & 0 & 0 & 0 & \cdots & \alpha_{q-1} \\ 1 & 0 & 1 & \alpha_2 & \cdots & \alpha_{q-1} & \cdots\cdots & 0 & 1 & \alpha_2 & \cdots & \alpha_{q-1} \end{bmatrix}$$

Primjer (Hammingovi kodovi)

Linearni kod definiran matricom provjere parnosti P zovemo q-arnim Hammingovim kodom s parametrom r i označavamo Ham(r, q). To je $[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3]_q$ kod koji dostiže ocjenu pakiranja kugli.

R. W. Hamming, *Error detecting and error correcting codes*, Bell System Tech. J. **29** (1950), 147–160. ($q = 2$)

Hammingovi kodovi: $\mathrm{Ham}(3,2)$

Primjer: binarni $[7,4,3]_2$ kod $(n=7,\ m=4,\ d=3,\ q=2,\ e=1)$

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

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

Reed-Solomonovi kodovi

$\mathbb{F}_q = \{\alpha_0, \alpha_1, \ldots, \alpha_{q-1}\}$, $\alpha_0 = 0$, $\alpha_1 = 1$

$$P = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{q-1} \\ 0 & 1 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_{q-1}^2 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & \alpha_2^{r-1} & \alpha_3^{r-1} & \cdots & \alpha_{q-1}^{r-1} \end{bmatrix}$$

Reed-Solomonovi kodovi

$\mathbb{F}_q = \{\alpha_0, \alpha_1, \ldots, \alpha_{q-1}\}$, $\alpha_0 = 0$, $\alpha_1 = 1$

$$P = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{q-1} \\ 0 & 1 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_{q-1}^2 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & \alpha_2^{r-1} & \alpha_3^{r-1} & \cdots & \alpha_{q-1}^{r-1} \end{bmatrix}$$

Primjer (Reed-Solomonovi kodovi)

Linearni kod definiran matricom provjere parnosti P nad poljem $\mathbb{F}_q$ ima parametre $[q, q-r, r+1]_q$ i dostiže Singletonovu ocjenu.

Reed-Solomonovi kodovi

$\mathbb{F}_q = \{\alpha_0, \alpha_1, \ldots, \alpha_{q-1}\}$, $\alpha_0 = 0$, $\alpha_1 = 1$

$$P = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{q-1} \\ 0 & 1 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_{q-1}^2 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & \alpha_2^{r-1} & \alpha_3^{r-1} & \cdots & \alpha_{q-1}^{r-1} \end{bmatrix}$$

Primjer (Reed-Solomonovi kodovi)

Linearni kod definiran matricom provjere parnosti P nad poljem $\mathbb{F}_q$ ima parametre $[q, q-r, r+1]_q$ i dostiže Singletonovu ocjenu.

I. S. Reed, G. Solomon, *Polynomial codes over certain finite fields*, J. Soc. Indust. Appl. Math. **8** (1960), 300–304. ($q = 2^k$)

Reed-Solomonovi kodovi

$\mathbb{F}_q = \{\alpha_0, \alpha_1, \ldots, \alpha_{q-1}\}$, $\alpha_0 = 0$, $\alpha_1 = 1$

$$P = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{q-1} \\ 0 & 1 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_{q-1}^2 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & \alpha_2^{r-1} & \alpha_3^{r-1} & \cdots & \alpha_{q-1}^{r-1} \end{bmatrix}$$

Primjer (Reed-Solomonovi kodovi)

Linearni kod definiran matricom provjere parnosti P nad poljem $\mathbb{F}_q$ ima parametre $[q, q-r, r+1]_q$ i dostiže Singletonovu ocjenu.

Primjene: zapisivanje podataka na CD-ove, DVD-ove i Blu-ray diskove, QR kodovi, satelitske komunikacije, sustavi za pohranu podataka kao što je RAID 6...

Savršeni kodovi

Kodovi koji dostižu Singletonovu ocjenu: MDS kodovi

Savršeni kodovi

Kodovi koji dostižu Singletonovu ocjenu: MDS kodovi

Kodovi koji dostižu ocjenu pakiranja kugli: savršeni kodovi

Savršeni kodovi

Kodovi koji dostižu Singletonovu ocjenu: MDS kodovi

Kodovi koji dostižu ocjenu pakiranja kugli: savršeni kodovi

$$M \cdot \sum_{i=0}^{e} \binom{n}{i} (q-1)^i = q^n$$

Savršeni kodovi

Kodovi koji dostižu Singletonovu ocjenu: MDS kodovi

Kodovi koji dostižu ocjenu pakiranja kugli: savršeni kodovi

$$M \cdot \sum_{i=0}^{e} \binom{n}{i} (q-1)^i = q^n$$

Trivijalni primjeri:

$C = \{00\cdots 0\}$, $e = n$

$C = F^n$, $e = 0$

$C = \{00\cdots 0, 11\cdots 1\}$, $d = n$ neparan i $q = 2$

Savršeni kodovi

Kodovi koji dostižu Singletonovu ocjenu: MDS kodovi

Kodovi koji dostižu ocjenu pakiranja kugli: savršeni kodovi

$$M \cdot \sum_{i=0}^{e} \binom{n}{i} (q-1)^i = q^n$$

Trivijalni primjeri:

$C = \{00\cdots 0\}$, $e = n$

$C = F^n$, $e = 0$

$C = \{00\cdots 0,\, 11\cdots 1\}$, $d = n$ neparan i $q = 2$

Netrivijalni primjeri:

$\mathrm{Ham}(r, q)$, $d = 3$

Savršeni kodovi

Kodovi koji dostižu Singletonovu ocjenu: MDS kodovi

Kodovi koji dostižu ocjenu pakiranja kugli: savršeni kodovi

$$M \cdot \sum_{i=0}^{e} \binom{n}{i} (q-1)^i = q^n$$

Trivijalni primjeri:

$C = \{00\cdots 0\}$, $e = n$

$C = F^n$, $e = 0$

$C = \{00\cdots 0,\, 11\cdots 1\}$, $d = n$ neparan i $q = 2$

Netrivijalni primjeri:

$\mathrm{Ham}(r, q)$, $d = 3$

M. J. E. Golay, *Notes on digital coding*, Proc. I.R.E. **37** (1949), 657.

$G_{23} \rightsquigarrow [23, 12, 7]_2$ $\quad G_{11} \rightsquigarrow [11, 6, 5]_3$

Savršeni kodovi

E. F. Assmus, Jr., H. F. Mattson, Jr., *On tactical configurations and error-correcting codes*, J. Combinatorial Theory **2** (1967), 243–257.

Teorem.

Neka je C linearni $[n, m, d]_q$ kod s neparnom minimalnom težinom $d = 2e + 1$. Kod C je savršen ako i samo ako nosači kodnih riječi minimalne težine čine $(e+1)$-$(n, d, (q-1)^e)$ dizajn.

Savršeni kodovi

E. F. Assmus, Jr., H. F. Mattson, Jr., *On tactical configurations and error-correcting codes*, J. Combinatorial Theory **2** (1967), 243–257.

Teorem.

Neka je C linearni $[n, m, d]_q$ kod s neparnom minimalnom težinom $d = 2e + 1$. Kod C je savršen ako i samo ako nosači kodnih riječi minimalne težine čine $(e + 1)$-$(n, d, (q - 1)^e)$ dizajn.

$\mathrm{Ham}(r, q) \leadsto 2\text{-}(\frac{q^r-1}{q-1}, 3, q - 1)$

Savršeni kodovi

E. F. Assmus, Jr., H. F. Mattson, Jr., *On tactical configurations and error-correcting codes*, J. Combinatorial Theory **2** (1967), 243–257.

Teorem.

Neka je C linearni $[n, m, d]_q$ kod s neparnom minimalnom težinom $d = 2e + 1$. Kod C je savršen ako i samo ako nosači kodnih riječi minimalne težine čine $(e+1)$-$(n, d, (q-1)^e)$ dizajn.

$\mathrm{Ham}(r, q) \rightsquigarrow 2\text{-}(\frac{q^r-1}{q-1}, 3, q-1)$

$q = 2$: Steinerov sustav trojki $2\text{-}(2^r - 1, 3, 1)$

Savršeni kodovi

E. F. Assmus, Jr., H. F. Mattson, Jr., *On tactical configurations and error-correcting codes*, J. Combinatorial Theory **2** (1967), 243–257.

Teorem.

Neka je C linearni $[n,m,d]_q$ kod s neparnom minimalnom težinom $d=2e+1$. Kod C je savršen ako i samo ako nosači kodnih riječi minimalne težine čine $(e+1)$-$(n,d,(q-1)^e)$ dizajn.

$\mathrm{Ham}(r,q) \rightsquigarrow 2\text{-}(\frac{q^r-1}{q-1},3,q-1)$

$q=2$: Steinerov sustav trojki $2\text{-}(2^r-1,3,1)$

G_{23}, $[23,12,7]_2 \rightsquigarrow 4\text{-}(23,7,1)$

Savršeni kodovi

E. F. Assmus, Jr., H. F. Mattson, Jr., *On tactical configurations and error-correcting codes*, J. Combinatorial Theory **2** (1967), 243–257.

Teorem.

Neka je C linearni $[n, m, d]_q$ kod s neparnom minimalnom težinom $d = 2e + 1$. Kod C je savršen ako i samo ako nosači kodnih riječi minimalne težine čine $(e + 1)$-$(n, d, (q - 1)^e)$ dizajn.

$\mathrm{Ham}(r, q) \rightsquigarrow 2\text{-}(\frac{q^r-1}{q-1}, 3, q - 1)$

$q = 2$: Steinerov sustav trojki $2\text{-}(2^r - 1, 3, 1)$

G_{23}, $[23, 12, 7]_2 \rightsquigarrow 4\text{-}(23, 7, 1)$

G_{11}, $[11, 6, 5]_3 \rightsquigarrow 3\text{-}(11, 5, 4)$

Savršeni kodovi

E. F. Assmus, Jr., H. F. Mattson, Jr., *On tactical configurations and error-correcting codes*, J. Combinatorial Theory **2** (1967), 243–257.

Teorem.

Neka je C linearni $[n, m, d]_q$ kod s neparnom minimalnom težinom $d = 2e + 1$. Kod C je savršen ako i samo ako nosači kodnih riječi minimalne težine čine $(e+1)$-$(n, d, (q-1)^e)$ dizajn.

$\mathrm{Ham}(r, q) \rightsquigarrow 2\text{-}(\frac{q^r-1}{q-1}, 3, q-1)$

$q = 2$: Steinerov sustav trojki $2\text{-}(2^r - 1, 3, 1)$

G_{23}, $[23, 12, 7]_2 \rightsquigarrow 4\text{-}(23, 7, 1)$

G_{11}, $[11, 6, 5]_3 \rightsquigarrow 3\text{-}(11, 5, 4) \rightsquigarrow 4\text{-}(11, 5, 1)$

Savršeni kodovi

```
gap> M24:=MathieuGroup(24);
gap> diz3:=KramerMesnerSearch(5,24,8,1,M24)[1];;
gap> diz7:=DerivedBlockDesign(diz3,1);;
gap> AllTDesignLambdas(diz7);
[ 253, 77, 21, 5, 1 ]
gap> IntersectionNumbers(diz7);
[ 1, 3 ]
```

Savršeni kodovi

```
gap> M24:=MathieuGroup(24);
gap> diz3:=KramerMesnerSearch(5,24,8,1,M24)[1];;
gap> diz7:=DerivedBlockDesign(diz3,1);;
gap> AllTDesignLambdas(diz7);
[ 253, 77, 21, 5, 1 ]
gap> IntersectionNumbers(diz7);
[ 1, 3 ]

gap> mat7:=BlocksToIncidenceMat(diz7.blocks);;
gap> DimensionsMat(mat7);
[ 23, 253 ]
```

Savršeni kodovi

```
gap> M24:=MathieuGroup(24);
gap> diz3:=KramerMesnerSearch(5,24,8,1,M24)[1];;
gap> diz7:=DerivedBlockDesign(diz3,1);;
gap> AllTDesignLambdas(diz7);
[ 253, 77, 21, 5, 1 ]
gap> IntersectionNumbers(diz7);
[ 1, 3 ]

gap> mat7:=BlocksToIncidenceMat(diz7.blocks);;
gap> DimensionsMat(mat7);
[ 23, 253 ]

gap> mat7t:=TransposedMat(mat7);;
gap> DimensionsMat(mat7t);
[ 253, 23 ]
```

Savršeni kodovi

```
gap> G23:=GeneratorMatCode(mat7t,GF(2));
a linear [23,12,1..7]3 code defined by generator matrix
  over GF(2)
gap> IsPerfectCode(G23);
true
```

Savršeni kodovi

```
gap> G23:=GeneratorMatCode(mat7t,GF(2));
a linear [23,12,1..7]3 code defined by generator matrix
  over GF(2)
gap> IsPerfectCode(G23);
true

gap> wd:=WeightDistribution(G23);
[ 1, 0, 0, 0, 0, 0, 0, 253, 506, 0, 0, 1288, 1288, 0, 0, 506,
  253, 0, 0, 0, 0, 0, 0, 1 ]
gap> AddWeights:=l->List([1..Size(l)],i->[i-1,l[i]]);
function( l ) ... end
gap> AddWeights(wd);
[ [ 0, 1 ], [ 1, 0 ], [ 2, 0 ], [ 3, 0 ], [ 4, 0 ], [ 5, 0 ],
  [ 6, 0 ], [ 7, 253 ], [ 8, 506 ], [ 9, 0 ], [ 10, 0 ],
  [ 11, 1288 ], [ 12, 1288 ], [ 13, 0 ], [ 14, 0 ],
  [ 15, 506 ], [ 16, 253 ], [ 17, 0 ], [ 18, 0 ], [ 19, 0 ],
  [ 20, 0 ], [ 21, 0 ], [ 22, 0 ], [ 23, 1 ] ]
```

Savršeni kodovi

```
gap> supp23:=List(Elements(G23),Support);;
gap> diz8:=BlockDesign(23,Filtered(supp23,x->Size(x)=8));;
gap> AllTDesignLambdas(diz8);
[ 506, 176, 56, 16, 4 ]
gap> IntersectionNumbers(diz8);
[ 0, 2, 4 ]
gap> diz9:=BlockDesign(23,Filtered(supp23,x->Size(x)=11));;
gap> AllTDesignLambdas(diz9);
[ 1288, 616, 280, 120, 48 ]
gap> IntersectionNumbers(diz9);
[ 3, 5, 7 ]
```

Savršeni kodovi

```
gap> supp23:=List(Elements(G23),Support);;
gap> diz8:=BlockDesign(23,Filtered(supp23,x->Size(x)=8));;
gap> AllTDesignLambdas(diz8);
[ 506, 176, 56, 16, 4 ]
gap> IntersectionNumbers(diz8);
[ 0, 2, 4 ]
gap> diz9:=BlockDesign(23,Filtered(supp23,x->Size(x)=11));;
gap> AllTDesignLambdas(diz9);
[ 1288, 616, 280, 120, 48 ]
gap> IntersectionNumbers(diz9);
[ 3, 5, 7 ]
```

```
gap> G11:=TernaryGolayCode();
a cyclic [11,6,5]2 ternary Golay code over GF(3)
gap> wd:=WeightDistribution(G11);
[ 1, 0, 0, 0, 0, 132, 132, 0, 330, 110, 0, 24 ]
```

Savršeni kodovi

```
gap> AddWeights(wd);
[ [ 0, 1 ], [ 1, 0 ], [ 2, 0 ], [ 3, 0 ], [ 4, 0 ],
  [ 5, 132 ], [ 6, 132 ], [ 7, 0 ], [ 8, 330 ], [ 9, 110 ],
  [ 10, 0 ], [ 11, 24 ] ]
gap> supp11:=List(Elements(G11),Support);;
gap> BlockDesign(11,AsSet(Filtered(supp11,x->Size(x)=5)));;
gap> AllTDesignLambdas(last);
[ 66, 30, 12, 4, 1 ]
```

Savršeni kodovi

```
gap> AddWeights(wd);
[ [ 0, 1 ], [ 1, 0 ], [ 2, 0 ], [ 3, 0 ], [ 4, 0 ],
  [ 5, 132 ], [ 6, 132 ], [ 7, 0 ], [ 8, 330 ], [ 9, 110 ],
  [ 10, 0 ], [ 11, 24 ] ]
gap> supp11:=List(Elements(G11),Support);;
gap> BlockDesign(11,AsSet(Filtered(supp11,x->Size(x)=5)));;
gap> AllTDesignLambdas(last);
[ 66, 30, 12, 4, 1 ]
```

Prošireni kod:

$$\bar{C} = \{(x_1, \ldots, x_n, x_{n+1}) \in \mathbb{F}_q^{n+1} \mid (x_1, \ldots, x_n) \in C,\ x_{n+1} = -\sum_{i=1}^{n} x_i\}$$

Savršeni kodovi

```
gap> AddWeights(wd);
[ [ 0, 1 ], [ 1, 0 ], [ 2, 0 ], [ 3, 0 ], [ 4, 0 ],
  [ 5, 132 ], [ 6, 132 ], [ 7, 0 ], [ 8, 330 ], [ 9, 110 ],
  [ 10, 0 ], [ 11, 24 ] ]
gap> supp11:=List(Elements(G11),Support);;
gap> BlockDesign(11,AsSet(Filtered(supp11,x->Size(x)=5)));;
gap> AllTDesignLambdas(last);
[ 66, 30, 12, 4, 1 ]
```

Prošireni kod:

$$\bar{C} = \{(x_1, \ldots, x_n, x_{n+1}) \in \mathbb{F}_q^{n+1} \mid (x_1, \ldots, x_n) \in C,\ x_{n+1} = -\sum_{i=1}^{n} x_i\}$$

$G_{12} = \bar{G}_{11} \rightsquigarrow [12, 6, 6]_3, \qquad G_{24} = \bar{G}_{23} \rightsquigarrow [24, 12, 8]_2$

Savršeni kodovi

```
gap> G12:=ExtendedTernaryGolayCode();
a linear [12,6,6]3 extended ternary Golay code over GF(3)
gap> WeightDistribution(G12);
[ 1, 0, 0, 0, 0, 0, 264, 0, 0, 440, 0, 0, 24 ]
gap> G24:=ExtendedBinaryGolayCode();
a linear [24,12,8]4 extended binary Golay code over GF(2)
gap> WeightDistribution(G24);
[ 1, 0, 0, 0, 0, 0, 0, 0, 759, 0, 0, 0, 2576, 0, 0, 0, 759,
  0, 0, 0, 0, 0, 0, 0, 1 ]
gap> IsPerfectCode(G12);
false
gap> IsPerfectCode(G24);
false
```

Assmus-Mattsonov teorem

Teorem (Assmus-Mattson)

Neka je $C \leq \mathbb{F}^n$ kod s parametrima $[n, m, d]_q$ i neka dualni kod $C^\perp$ ima parametre $[n, n-m, e]_q$. Neka su B_i koeficijenti težinskog polinoma dualnog koda: $W_{C^\perp}(X, Y) = \sum_{i=0}^{d} B_i X^{n-i} Y^i$. Za $q = 2$ stavimo $v_0 = w_0 = n$, a inače neka je

$$v_0 = \max\left\{v \in \mathbb{N} \mid v - \left\lfloor \frac{v+q-2}{q-1} \right\rfloor < d\right\},$$

$$w_0 = \max\left\{w \in \mathbb{N} \mid w - \left\lfloor \frac{w+q-2}{q-1} \right\rfloor < e\right\}.$$

Neka je $t < d$ takav da je najviše $d - t$ koeficijenata $B_0, \ldots, B_{n-t}$ različito od nule. Tada za svaki $\Bbbk$, $d \leq \Bbbk \leq v_0$ skup svih nosača vektora težine $\Bbbk$ u C čini t-dizajn (ako postoje takvi vektori). Nadalje, za svaki $\Bbbk$, $e \leq \Bbbk \leq w_0$ skup svih nosača vektora težine $\Bbbk$ u $C^\perp$ čini t-dizajn (ako postoje takvi vektori).