Asocijacijske sheme

Vedran Krčadinac

3.6.2024.

Reed-Mullerovi kodovi

I. S. Reed, *A class of multiple-error-correcting codes and the decoding scheme*, Trans. IRE, PGIT **4** (1954), 38–49.

D. E. Muller, *Application of Boolean algebra to switching circuit design and to error detection*, Trans. IRE, EC **3** (1954), 6–12.

Reed-Mullerovi kodovi

I. S. Reed, *A class of multiple-error-correcting codes and the decoding scheme*, Trans. IRE, PGIT **4** (1954), 38–49.

D. E. Muller, *Application of Boolean algebra to switching circuit design and to error detection*, Trans. IRE, EC **3** (1954), 6–12.

$\mathrm{RM}(r, m)$ je binarni linearni kod s parametrima:

$$n = 2^m \text{ (duljina)}$$

$$m = \sum_{k=0}^{r} \binom{m}{k} \text{ (dimenzija)}$$

$$d = 2^{m-r} \text{ (minimalna težina)}$$

Reed-Mullerovi kodovi

I. S. Reed, *A class of multiple-error-correcting codes and the decoding scheme*, Trans. IRE, PGIT **4** (1954), 38–49.

D. E. Muller, *Application of Boolean algebra to switching circuit design and to error detection*, Trans. IRE, EC **3** (1954), 6–12.

$\mathrm{RM}(r, m)$ je binarni linearni kod s parametrima:

$$n = 2^m \text{ (duljina)}$$

$$m = \sum_{k=0}^{r} \binom{m}{k} \text{ (dimenzija)}$$

$$d = 2^{m-r} \text{ (minimalna težina)}$$

Parametar r zovemo stupnjem RM koda.

Reed-Mullerovi kodovi

Ambijentni vektorski prostor:

$$V = \{f : \mathbb{F}_2^m \to \mathbb{F}_2\} \text{ nad } \mathbb{F}_2$$

Reed-Mullerovi kodovi

Ambijentni vektorski prostor:

$$V = \{f : \mathbb{F}_2^m \to \mathbb{F}_2\} \text{ nad } \mathbb{F}_2$$

Koordinate kodnih riječi indeksirane su binarnim zapisima brojeva $\{0, \ldots, n-1\}$ umjesto brojevima $\{1, \ldots, n\}$.

Reed-Mullerovi kodovi

Ambijentni vektorski prostor:

$$V = \{f : \mathbb{F}_2^m \to \mathbb{F}_2\} \text{ nad } \mathbb{F}_2$$

Koordinate kodnih riječi indeksirane su binarnim zapisima brojeva $\{0, \ldots, n-1\}$ umjesto brojevima $\{1, \ldots, n\}$.

$\mathrm{RM}(r, m)$ je potprostor svih funkcija $f : \mathbb{F}_2^m \to \mathbb{F}_2$ koje su polinomi stupnja najviše r.

Reed-Mullerovi kodovi

Ambijentni vektorski prostor:

$$V = \{f : \mathbb{F}_2^m \to \mathbb{F}_2\} \text{ nad } \mathbb{F}_2$$

Koordinate kodnih riječi indeksirane su binarnim zapisima brojeva $\{0, \ldots, n-1\}$ umjesto brojevima $\{1, \ldots, n\}$.

$\mathrm{RM}(r, m)$ je potprostor svih funkcija $f : \mathbb{F}_2^m \to \mathbb{F}_2$ koje su polinomi stupnja najviše r.

Varijable: $X_1, \ldots, X_m$

Reed-Mullerovi kodovi

Ambijentni vektorski prostor:

$$V = \{f : \mathbb{F}_2^m \to \mathbb{F}_2\} \text{ nad } \mathbb{F}_2$$

Koordinate kodnih riječi indeksirane su binarnim zapisima brojeva $\{0, \ldots, n-1\}$ umjesto brojevima $\{1, \ldots, n\}$.

RM(r, m) je potprostor svih funkcija $f : \mathbb{F}_2^m \to \mathbb{F}_2$ koje su polinomi stupnja najviše r.

Varijable: $X_1, \ldots, X_m$

Težina $w(f)$ je broj uređenih m-torki $(X_1, \ldots, X_m) \in \mathbb{F}_2^m$ za koje je $f(X_1, \ldots, X_m) \neq 0$, odnosno $f(X_1, \ldots, X_m) = 1$.

Reed-Mullerovi kodovi

Ambijentni vektorski prostor:

$$V = \{f : \mathbb{F}_2^m \to \mathbb{F}_2\} \text{ nad } \mathbb{F}_2$$

Koordinate kodnih riječi indeksirane su binarnim zapisima brojeva $\{0, \ldots, n-1\}$ umjesto brojevima $\{1, \ldots, n\}$.

RM(r, m) je potprostor svih funkcija $f : \mathbb{F}_2^m \to \mathbb{F}_2$ koje su polinomi stupnja najviše r.

Varijable: $X_1, \ldots, X_m$

Težina $w(f)$ je broj uređenih m-torki $(X_1, \ldots, X_m) \in \mathbb{F}_2^m$ za koje je $f(X_1, \ldots, X_m) \neq 0$, odnosno $f(X_1, \ldots, X_m) = 1$.

Teorem.

RM(r, m) je linearni $\left[2^m,\ \sum_{k=0}^{r} \binom{m}{k},\ 2^{m-r}\right]_2$ kod.

Korolar.

Svaka funkcija $f : \mathbb{F}_2^m \to \mathbb{F}_2$ je polinom stupnja najviše m.

Reed-Mullerovi kodovi

Korolar.

Svaka funkcija $f:\mathbb{F}_2^m\to\mathbb{F}_2$ je polinom stupnja najviše m.

Produkt funkcija $f:\mathbb{F}_2^m\to\mathbb{F}_2$ i $g:\mathbb{F}_2^m\to\mathbb{F}_2$ je $f\cdot g=\sum\limits_{X\in\mathbb{F}_2^m} f(X)\,g(X)$

Reed-Mullerovi kodovi

Korolar.

Svaka funkcija $f : \mathbb{F}_2^m \to \mathbb{F}_2$ je polinom stupnja najviše m.

Produkt funkcija $f : \mathbb{F}_2^m \to \mathbb{F}_2$ i $g : \mathbb{F}_2^m \to \mathbb{F}_2$ je $f \cdot g = \sum\limits_{X \in \mathbb{F}_2^m} f(X)\, g(X)$

Teorem.

Dualni kod od RM(r, m) je RM$(m - r - 1, m)$.

Reed-Mullerovi kodovi

Korolar.

Svaka funkcija $f : \mathbb{F}_2^m \to \mathbb{F}_2$ je polinom stupnja najviše m.

Produkt funkcija $f : \mathbb{F}_2^m \to \mathbb{F}_2$ i $g : \mathbb{F}_2^m \to \mathbb{F}_2$ je $f \cdot g = \sum\limits_{X \in \mathbb{F}_2^m} f(X)\, g(X)$

Teorem.

Dualni kod od $\mathrm{RM}(r, m)$ je $\mathrm{RM}(m - r - 1, m)$.

Afina geometrija nad konačnim poljem

U $\mathrm{AG}(m, q)$ točke su vektori iz $\mathbb{F}_q^m$, a ravnine translati potprostora od $\mathbb{F}_q^m$

Reed-Mullerovi kodovi

Korolar.

Svaka funkcija $f:\mathbb{F}_2^m\to\mathbb{F}_2$ je polinom stupnja najviše m.

Produkt funkcija $f:\mathbb{F}_2^m\to\mathbb{F}_2$ i $g:\mathbb{F}_2^m\to\mathbb{F}_2$ je $f\cdot g=\sum\limits_{X\in\mathbb{F}_2^m} f(X)\,g(X)$

Teorem.

Dualni kod od $\mathrm{RM}(r,m)$ je $\mathrm{RM}(m-r-1,m)$.

Afina geometrija nad konačnim poljem

U $\mathrm{AG}(m,q)$ točke su vektori iz $\mathbb{F}_q^m$, a ravnine translati potprostora od $\mathbb{F}_q^m$

$\mathrm{AG}_k(m,q)$ je 2-$(v,\Bbbk,\lambda)$ dizajn za

$$v=q^m,$$

Reed-Mullerovi kodovi

Korolar.

Svaka funkcija $f : \mathbb{F}_2^m \to \mathbb{F}_2$ je polinom stupnja najviše m.

Produkt funkcija $f : \mathbb{F}_2^m \to \mathbb{F}_2$ i $g : \mathbb{F}_2^m \to \mathbb{F}_2$ je $f \cdot g = \sum\limits_{X \in \mathbb{F}_2^m} f(X)\, g(X)$

Teorem.

Dualni kod od $\mathrm{RM}(r, m)$ je $\mathrm{RM}(m - r - 1, m)$.

Afina geometrija nad konačnim poljem

U $\mathrm{AG}(m, q)$ točke su vektori iz $\mathbb{F}_q^m$, a ravnine translati potprostora od $\mathbb{F}_q^m$

$\mathrm{AG}_k(m, q)$ je 2-$(v, \Bbbk, \lambda)$ dizajn za

$$v = q^m, \quad \Bbbk = q^k,$$

Reed-Mullerovi kodovi

Korolar.

Svaka funkcija $f : \mathbb{F}_2^m \to \mathbb{F}_2$ je polinom stupnja najviše m.

Produkt funkcija $f : \mathbb{F}_2^m \to \mathbb{F}_2$ i $g : \mathbb{F}_2^m \to \mathbb{F}_2$ je $f \cdot g = \sum_{X \in \mathbb{F}_2^m} f(X)\, g(X)$

Teorem.

Dualni kod od $\mathrm{RM}(r, m)$ je $\mathrm{RM}(m - r - 1, m)$.

Afina geometrija nad konačnim poljem

U $\mathrm{AG}(m, q)$ točke su vektori iz $\mathbb{F}_q^m$, a ravnine translati potprostora od $\mathbb{F}_q^m$

$\mathrm{AG}_k(m, q)$ je 2-$(v, \Bbbk, \lambda)$ dizajn za

$$v = q^m, \quad \Bbbk = q^k, \quad \lambda = \begin{bmatrix} m-1 \\ k-1 \end{bmatrix}_q ,$$

Reed-Mullerovi kodovi

Korolar.

Svaka funkcija $f : \mathbb{F}_2^m \to \mathbb{F}_2$ je polinom stupnja najviše m.

Produkt funkcija $f : \mathbb{F}_2^m \to \mathbb{F}_2$ i $g : \mathbb{F}_2^m \to \mathbb{F}_2$ je $f \cdot g = \sum_{X \in \mathbb{F}_2^m} f(X)\, g(X)$

Teorem.

Dualni kod od $\mathrm{RM}(r, m)$ je $\mathrm{RM}(m - r - 1, m)$.

Afina geometrija nad konačnim poljem

U $\mathrm{AG}(m, q)$ točke su vektori iz $\mathbb{F}_q^m$, a ravnine translati potprostora od $\mathbb{F}_q^m$

$\mathrm{AG}_k(m, q)$ je 2-$(v, \Bbbk, \lambda)$ dizajn za

$$v = q^m, \quad \Bbbk = q^k, \quad \lambda = \begin{bmatrix} m-1 \\ k-1 \end{bmatrix}_q, \quad b = q^{m-k} \begin{bmatrix} m \\ k \end{bmatrix}_q$$

Reed-Mullerovi kodovi i afina geometrija

$\mathrm{AG}_k(m,2)$ je 3-$(v, \Bbbk, \lambda)$ dizajn za

$$v = 2^m, \quad \Bbbk = 2^k, \quad \lambda = \begin{bmatrix} m-2 \\ k-2 \end{bmatrix}_2, \quad b = 2^{m-k} \begin{bmatrix} m \\ k \end{bmatrix}_2$$

Reed-Mullerovi kodovi i afina geometrija

$\mathrm{AG}_k(m,2)$ je 3-$(v,\Bbbk,\lambda)$ dizajn za

$$v = 2^m, \quad \Bbbk = 2^k, \quad \lambda = \begin{bmatrix} m-2 \\ k-2 \end{bmatrix}_2, \quad b = 2^{m-k} \begin{bmatrix} m \\ k \end{bmatrix}_2$$

Funkciju $f : \mathbb{F}_2^m \to \mathbb{F}_2$ možemo shvatiti kao karakterističnu funkciju podskupa od $\mathrm{AG}(m,2)$.

Reed-Mullerovi kodovi i afina geometrija

$AG_k(m, 2)$ je 3-$(v, \mathcal{k}, \lambda)$ dizajn za

$$v = 2^m, \quad \mathcal{k} = 2^k, \quad \lambda = \begin{bmatrix} m-2 \\ k-2 \end{bmatrix}_2, \quad b = 2^{m-k} \begin{bmatrix} m \\ k \end{bmatrix}_2$$

Funkciju $f : \mathbb{F}_2^m \to \mathbb{F}_2$ možemo shvatiti kao karakterističnu funkciju podskupa od $AG(m, 2)$. Funkcije iz $RM(1, m)$ su oblika

$$f(X_1, \ldots, X_m) = a_0 + a_1 X_1 + \ldots + a_m X_m$$

Reed-Mullerovi kodovi i afina geometrija

$\mathrm{AG}_k(m,2)$ je 3-$(v, \mathscr{k}, \lambda)$ dizajn za

$$v = 2^m, \quad \mathscr{k} = 2^k, \quad \lambda = \begin{bmatrix} m-2 \\ k-2 \end{bmatrix}_2, \quad b = 2^{m-k} \begin{bmatrix} m \\ k \end{bmatrix}_2$$

Funkciju $f : \mathbb{F}_2^m \to \mathbb{F}_2$ možemo shvatiti kao karakterističnu funkciju podskupa od $\mathrm{AG}(m,2)$. Funkcije iz $\mathrm{RM}(1,m)$ su oblika

$$f(X_1, \ldots, X_m) = a_0 + a_1 X_1 + \ldots + a_m X_m$$

Teorem.

Neka je $\Pi \subseteq AG(m,2)$ ravnina dimenzije $m-r$ i $f : \mathbb{F}_2^m \to \mathbb{F}_2$ odgovarajuća karakteristična funkcija:

$$f(X_1, \ldots, X_m) = \begin{cases} 1, & \text{ako je } (X_1, \ldots, X_m) \in \Pi, \\ 0, & \text{inače.} \end{cases}$$

Tada je $f \in \mathrm{RM}(r,m)$.

Reed-Mullerovi kodovi i afina geometrija

Teorem.

Vektori minimalne težine u $\mathrm{RM}(r, m)$ su točno karakteristične funkcije $(m-r)$-ravnina u $\mathrm{AG}(m, 2)$ i razapinju cijeli kod $\mathrm{RM}(r, m)$.

Reed-Mullerovi kodovi i afina geometrija

Teorem.

Vektori minimalne težine u $\mathrm{RM}(r, m)$ su točno karakteristične funkcije $(m - r)$-ravnina u $\mathrm{AG}(m, 2)$ i razapinju cijeli kod $\mathrm{RM}(r, m)$.

F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes. I, II.* North-Holland Publishing Co., 1977.

Reed-Mullerovi kodovi i afina geometrija

Teorem.

Vektori minimalne težine u $\mathrm{RM}(r, m)$ su točno karakteristične funkcije $(m - r)$-ravnina u $\mathrm{AG}(m, 2)$ i razapinju cijeli kod $\mathrm{RM}(r, m)$.

Primjer: $\mathrm{RM}(2, 4)$

Reed-Mullerovi kodovi i afina geometrija

Teorem.

Vektori minimalne težine u $\mathrm{RM}(r, m)$ su točno karakteristične funkcije $(m - r)$-ravnina u $\mathrm{AG}(m, 2)$ i razapinju cijeli kod $\mathrm{RM}(r, m)$.

Primjer: $\mathrm{RM}(2, 4)$

```
gap> C:=ReedMullerCode(2,4);
a linear [16,11,4]2 Reed-Muller (2,4) code over GF(2)
```

Reed-Mullerovi kodovi i afina geometrija

Teorem.

Vektori minimalne težine u $\mathrm{RM}(r, m)$ su točno karakteristične funkcije $(m-r)$-ravnina u $AG(m, 2)$ i razapinju cijeli kod $\mathrm{RM}(r, m)$.

Primjer: $\mathrm{RM}(2, 4)$

```
gap> C:=ReedMullerCode(2,4);
a linear [16,11,4]2 Reed-Muller (2,4) code over GF(2)
gap> AddWeights(WeightDistribution(C));
[ [ 0, 1 ], [ 4, 140 ], [ 6, 448 ], [ 8, 870 ], [ 10, 448 ],
  [ 12, 140 ], [ 16, 1 ] ]
```

Reed-Mullerovi kodovi i afina geometrija

Teorem.

Vektori minimalne težine u $\mathrm{RM}(r, m)$ su točno karakteristične funkcije $(m - r)$-ravnina u $AG(m, 2)$ i razapinju cijeli kod $\mathrm{RM}(r, m)$.

Primjer: $\mathrm{RM}(2, 4)$

```
gap> C:=ReedMullerCode(2,4);
a linear [16,11,4]2 Reed-Muller (2,4) code over GF(2)
gap> AddWeights(WeightDistribution(C));
[ [ 0, 1 ], [ 4, 140 ], [ 6, 448 ], [ 8, 870 ], [ 10, 448 ],
  [ 12, 140 ], [ 16, 1 ] ]
gap> D:=DualCode(C);
a linear [16,5,8]5..6 dual code
gap> AddWeights(WeightDistribution(D));
[ [ 0, 1 ], [ 8, 30 ], [ 16, 1 ] ]
```

Distribucija težina u Reed-Mullerovim kodovima

Distribucija težina u $\mathrm{RM}(1,m)$:

$$W_{\mathrm{RM}(1,m)}(X,Y) = X^{2^m} + (2^{m+1}-2)X^{2^{m-1}}Y^{2^{m-1}} + Y^{2^m}$$

Distribucija težina u Reed-Mullerovim kodovima

Distribucija težina u $\mathrm{RM}(1, m)$:

$$W_{\mathrm{RM}(1,m)}(X, Y) = X^{2^m} + (2^{m+1} - 2)X^{2^{m-1}} Y^{2^{m-1}} + Y^{2^m}$$

Distribucija težina u $\mathrm{RM}(2, m)$?

Distribucija težina u Reed-Mullerovim kodovima

Distribucija težina u RM$(1, m)$:

$$W_{\mathrm{RM}(1,m)}(X, Y) = X^{2^m} + (2^{m+1} - 2)X^{2^{m-1}}Y^{2^{m-1}} + Y^{2^m}$$

Distribucija težina u RM$(2, m)$? Funkcije su oblika

$$f(X) = a_0 + a_1X_1 + \ldots + a_mX_m + \sum_{1 \le i < j \le m} q_{ij}X_iX_j$$

Distribucija težina u Reed-Mullerovim kodovima

Distribucija težina u RM$(1, m)$:

$$W_{\mathrm{RM}(1,m)}(X, Y) = X^{2^m} + (2^{m+1} - 2)X^{2^{m-1}}Y^{2^{m-1}} + Y^{2^m}$$

Distribucija težina u RM$(2, m)$? Funkcije su oblika

$$f(X) = a_0 + a_1X_1 + \ldots + a_mX_m + \sum_{1\leq i<j\leq m} q_{ij}X_iX_j$$

RM$(1, m) \leq$ RM$(2, m)$, susjedne klase određene su koeficijentima $q_{ij} \in \mathbb{F}_2$.

Distribucija težina u Reed-Mullerovim kodovima

Distribucija težina u RM$(1, m)$:

$$W_{\mathrm{RM}(1,m)}(X, Y) = X^{2^m} + (2^{m+1} - 2)X^{2^{m-1}} Y^{2^{m-1}} + Y^{2^m}$$

Distribucija težina u RM$(2, m)$? Funkcije su oblika

$$f(X) = a_0 + a_1 X_1 + \ldots + a_m X_m + \sum_{1 \le i < j \le m} q_{ij} X_i X_j$$

RM$(1, m) \le$ RM$(2, m)$, susjedne klase određene su koeficijentima $q_{ij} \in \mathbb{F}_2$. Zapišimo ih u simetričnu $m \times m$ matricu $B = [q_{ij}]$ s nulama na dijagonali i $q_{ji} = q_{ij}$ ispod dijagonale. To su tzv. simplektičke matrice.

Distribucija težina u Reed-Mullerovim kodovima

Distribucija težina u $\mathrm{RM}(1,m)$:

$$W_{\mathrm{RM}(1,m)}(X,Y) = X^{2^m} + (2^{m+1}-2)X^{2^{m-1}}Y^{2^{m-1}} + Y^{2^m}$$

Distribucija težina u $\mathrm{RM}(2,m)$? Funkcije su oblika

$$f(X) = a_0 + a_1X_1 + \ldots + a_mX_m + \sum_{1\le i<j\le m} q_{ij}X_iX_j$$

$\mathrm{RM}(1,m) \le \mathrm{RM}(2,m)$, susjedne klase određene su koeficijentima $q_{ij} \in \mathbb{F}_2$. Zapišimo ih u simetričnu $m \times m$ matricu $B = [q_{ij}]$ s nulama na dijagonali i $q_{ji} = q_{ij}$ ispod dijagonale. To su tzv. simplektičke matrice.

$$\mathbb{Q}(B) = \{f(X) = a_0 + a_1X_1 + \ldots + a_mX_m + \sum_{1\le i<j\le m} q_{ij}X_iX_j \mid a_0,\ldots,a_m \in \mathbb{F}_2\}$$

Distribucija težina u Reed-Mullerovim kodovima

Koliko ima simplektičkih matrica reda m?

Distribucija težina u Reed-Mullerovim kodovima

Koliko ima simplektičkih matrica reda m? $\quad 2^{\binom{m}{2}}$

Distribucija težina u Reed-Mullerovim kodovima

Koliko ima simplektičkih matrica reda m? $\quad 2^{\binom{m}{2}}$

$N(m,r)$ = broj simplektičkih matrica reda m i ranga r

Distribucija težina u Reed-Mullerovim kodovima

Koliko ima simplektičkih matrica reda m? $\quad 2^{\binom{m}{2}}$

$N(m,r) =$ broj simplektičkih matrica reda m i ranga r

Lema.

Vrijedi rekurzija

$$N(m+1,r) = 2^r N(m,r) + (2^m - 2^{r-2}) N(m,r-2)$$

Distribucija težina u Reed-Mullerovim kodovima

Koliko ima simplektičkih matrica reda m? $\quad 2^{\binom{m}{2}}$

$N(m,r)$ = broj simplektičkih matrica reda m i ranga r

Lema.

Vrijedi rekurzija

$$N(m+1,r) = 2^r N(m,r) + (2^m - 2^{r-2}) N(m,r-2)$$

Teorem.

Broj simplektičkih matrica neparnog ranga je $N(m,2k+1)=0$, a parnog ranga je

$$N(m,2k) = \frac{(2^m-1)(2^{m-1}-1)\cdots(2^{m-2k+2})(2^{m-2k+1})}{(2^{2k}-1)(2^{2k-2}-1)\cdots(2^2-1)} \cdot 2^{k(k-1)}$$

Distribucija težina u Reed-Mullerovim kodovima

Korolar.

Ako postoji regularna simplektička matrica, onda je njezin red m paran broj.

Distribucija težina u Reed-Mullerovim kodovima

Korolar.

Ako postoji regularna simplektička matrica, onda je njezin red m paran broj.

Teorem.

Ako je B simplektička matrica reda m i ranga $2k$, distribucija težina u susjednoj klasi $\mathbb{Q}(B)$ dana je u tablici:

Težina	$2^{m-1} - 2^{m-k-1}$	2^{m-1}	$2^{m-1} + 2^{m-k+1}$
Br. vektora	2^{2k}	$2^{m+1} - 2^{2k+1}$	2^{2k}

Distribucija težina u Reed-Mullerovim kodovima

Korolar.

Ako postoji regularna simplektička matrica, onda je njezin red m paran broj.

Teorem.

Ako je B simplektička matrica reda m i ranga $2k$, distribucija težina u susjednoj klasi $\mathbb{Q}(B)$ dana je u tablici:

Težina	$2^{m-1} - 2^{m-k-1}$	2^{m-1}	$2^{m-1} + 2^{m-k+1}$
Br. vektora	2^{2k}	$2^{m+1} - 2^{2k+1}$	2^{2k}

Za $k = 0$ je $\mathbb{Q}(0) = \mathrm{RM}(1, m)$ i tablica se podudara s

$$W_{\mathrm{RM}(1,m)}(X, Y) = X^{2^m} + (2^{m+1} - 2)X^{2^{m-1}}Y^{2^{m-1}} + Y^{2^m}$$

Distribucija težina u Reed-Mullerovim kodovima

Korolar.

Ako postoji regularna simplektička matrica, onda je njezin red m paran broj.

Teorem.

Ako je B simplektička matrica reda m i ranga $2k$, distribucija težina u susjednoj klasi $\mathbb{Q}(B)$ dana je u tablici:

Težina	$2^{m-1} - 2^{m-k-1}$	2^{m-1}	$2^{m-1} + 2^{m-k+1}$
Br. vektora	2^{2k}	$2^{m+1} - 2^{2k+1}$	2^{2k}

Za $k > 0$ minimalna težina od $\mathbb{Q}(B)$ raste s k i najveća je za $2k = m$. U tom slučaju ne pojavljuje se "srednja" težina, nego samo težine $2^{m-1} - \varepsilon\, 2^{m/2-1}$ za $\varepsilon = \pm 1$. Kažemo da su funkcije tipa ε i ima ih 2^m.

Distribucija težina u Reed-Mullerovim kodovima

Time je potpuno određena distribucija težina u $\mathrm{RM}(2, m)$!

Distribucija težina u Reed-Mullerovim kodovima

Time je potpuno određena distribucija težina u $\text{RM}(2, m)$!

Distribucija težina u $\text{RM}(m-3, m) = \text{RM}(2, m)^\perp$ i $\text{RM}(m-2, m) = \text{RM}(1, m)^\perp$ slijedi iz MacWilliamsinog identiteta:

Teorem (MacWilliamsin identitet)

Za binarni linearni kod C vrijedi

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

Distribucija težina u Reed-Mullerovim kodovima

Time je potpuno određena distribucija težina u $\mathrm{RM}(2, m)$!

Distribucija težina u $\mathrm{RM}(m-3, m) = \mathrm{RM}(2, m)^{\perp}$ i $\mathrm{RM}(m-2, m) = \mathrm{RM}(1, m)^{\perp}$ slijedi iz MacWilliamsinog identiteta:

Teorem (MacWilliamsin identitet)

Za binarni linearni kod C vrijedi

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

Zadatak.

Napišite eksplicitno distribucije težina u $\mathrm{RM}(m-1, m)$ i $\mathrm{RM}(m, m)$.

Distribucija težina u Reed-Mullerovim kodovima

Time je potpuno određena distribucija težina u $\mathrm{RM}(2,m)$!

Distribucija težina u $\mathrm{RM}(m-3,m) = \mathrm{RM}(2,m)^\perp$ i $\mathrm{RM}(m-2,m) = \mathrm{RM}(1,m)^\perp$ slijedi iz MacWilliamsinog identiteta:

Teorem (MacWilliamsin identitet)

Za binarni linearni kod C vrijedi

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

Zadatak.

Napišite eksplicitno distribucije težina u $\mathrm{RM}(m-1,m)$ i $\mathrm{RM}(m,m)$.

Distribucija težina u $\mathrm{RM}(r,m)$ za $2 < r < m-3$?

Distribucija težina u Reed-Mullerovim kodovima

Time je potpuno određena distribucija težina u $\mathrm{RM}(2, m)$!

Distribucija težina u $\mathrm{RM}(m-3, m) = \mathrm{RM}(2, m)^{\perp}$ i $\mathrm{RM}(m-2, m) = \mathrm{RM}(1, m)^{\perp}$ slijedi iz MacWilliamsinog identiteta:

Teorem (MacWilliamsin identitet)

Za binarni linearni kod C vrijedi

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

Zadatak.

Napišite eksplicitno distribucije težina u $\mathrm{RM}(m-1, m)$ i $\mathrm{RM}(m, m)$.

Distribucija težina u $\mathrm{RM}(r, m)$ za $2 < r < m-3$?

F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes. I, II.* North-Holland Publishing Co., 1977.

Neki nelinearni kodovi

Zadatak.

Pokažite da je $\mathrm{RM}(r, m)$ prošireni ciklički kod.

Neki nelinearni kodovi

Zadatak.

Pokažite da je $\mathrm{RM}(r, m)$ prošireni ciklički kod.

Punktirani kod $\mathrm{RM}^*(r, m)$ dobivamo uklanjanjem koordinate koja odgovara nulvektoru u $\mathbb{F}_2^m$.

Neki nelinearni kodovi

Zadatak.

Pokažite da je $\mathrm{RM}(r, m)$ prošireni ciklički kod.

Punktirani kod $\mathrm{RM}^*(r, m)$ dobivamo uklanjanjem koordinate koja odgovara nulvektoru u $\mathbb{F}_2^m$. Na primjer, $\mathrm{RM}^*(2, 4)$ je ciklički $[15, 11, 3]_2$ kod i ekvivalentan je Hammingovom kodu $\mathrm{Ham}(4, 2)$.

Neki nelinearni kodovi

Zadatak.

Pokažite da je $\mathrm{RM}(r,m)$ prošireni ciklički kod.

Punktirani kod $\mathrm{RM}^*(r,m)$ dobivamo uklanjanjem koordinate koja odgovara nulvektoru u $\mathbb{F}_2^m$. Na primjer, $\mathrm{RM}^*(2,4)$ je ciklički $[15,11,3]_2$ kod i ekvivalentan je Hammingovom kodu $\mathrm{Ham}(4,2)$.

```
gap> C:=BCHCode(15,5,GF(2));
a cyclic [15,7,5]3..5 BCH code, delta=5, b=1 over GF(2)
gap> AddWeights(WeightDistribution(C));
[ [ 0, 1 ], [ 5, 18 ], [ 6, 30 ], [ 7, 15 ], [ 8, 15 ],
  [ 9, 30 ], [ 10, 18 ], [ 15, 1 ] ]
```

Neki nelinearni kodovi

Zadatak.

Pokažite da je $\mathrm{RM}(r,m)$ prošireni ciklički kod.

Punktirani kod $\mathrm{RM}^*(r,m)$ dobivamo uklanjanjem koordinate koja odgovara nulvektoru u $\mathbb{F}_2^m$. Na primjer, $\mathrm{RM}^*(2,4)$ je ciklički $[15,11,3]_2$ kod i ekvivalentan je Hammingovom kodu $\mathrm{Ham}(4,2)$.

```
gap> C:=BCHCode(15,5,GF(2));
a cyclic [15,7,5]3..5 BCH code, delta=5, b=1 over GF(2)
gap> AddWeights(WeightDistribution(C));
[ [ 0, 1 ], [ 5, 18 ], [ 6, 30 ], [ 7, 15 ], [ 8, 15 ],
  [ 9, 30 ], [ 10, 18 ], [ 15, 1 ] ]
```

Početkom 1960-ih bilo je poznato da ne postoji **linearni** kod s $n=15$ i $d=5$ dimenzije veće od 7, tj. s više od $M=2^7=128$ kodnih riječi.

Neki nelinearni kodovi

Zadatak.

Pokažite da je $\mathrm{RM}(r, m)$ prošireni ciklički kod.

Punktirani kod $\mathrm{RM}^*(r, m)$ dobivamo uklanjanjem koordinate koja odgovara nulvektoru u $\mathbb{F}_2^m$. Na primjer, $\mathrm{RM}^*(2, 4)$ je ciklički $[15, 11, 3]_2$ kod i ekvivalentan je Hammingovom kodu $\mathrm{Ham}(4, 2)$.

```
gap> C:=BCHCode(15,5,GF(2));
a cyclic [15,7,5]3..5 BCH code, delta=5, b=1 over GF(2)
gap> AddWeights(WeightDistribution(C));
[ [ 0, 1 ], [ 5, 18 ], [ 6, 30 ], [ 7, 15 ], [ 8, 15 ],
  [ 9, 30 ], [ 10, 18 ], [ 15, 1 ] ]
```

Početkom 1960-ih bilo je poznato da ne postoji **linearni** kod s $n = 15$ i $d = 5$ dimenzije veće od 7, tj. s više od $M = 2^7 = 128$ kodnih riječi.

Koliko kodnih riječi može imati **nelinearni** kod s $n = 15$ i $d = 5$?

Neki nelinearni kodovi

Propozicija (Ocjena pakiranja kugli)

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

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

Neki nelinearni kodovi

Propozicija (Ocjena pakiranja kugli)

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

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

$$n = 15,\ d = 5 \quad \Rightarrow \quad M \leq \frac{2^{15}}{121} \approx 270.81,\ \text{tj. } M \leq 270$$

Neki nelinearni kodovi

Propozicija (Ocjena pakiranja kugli)

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

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

$$n = 15,\ d = 5 \quad \Rightarrow \quad M \leq \frac{2^{15}}{121} \approx 270.81,\ \text{tj. } M \leq 270$$

S. M. Johnson, *A new upper bound for error-correcting codes*, IRE Trans. IT **8** (1962), 203–207.

Neki nelinearni kodovi

Propozicija (Ocjena pakiranja kugli)

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

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

$$n = 15,\ d = 5 \quad \Rightarrow \quad M \le \frac{2^{15}}{121} \approx 270.81,\ \text{tj.}\ M \le 270$$

S. M. Johnson, *A new upper bound for error-correcting codes*, IRE Trans. IT **8** (1962), 203–207.

$A(n, d, t)$ = najveća moguća veličina binarnog koda duljine n i minimalne udaljenosti barem d sa svim kodnim riječima težine t

Neki nelinearni kodovi

Lema.

$$A(n, 2k-1, t) = A(n, 2k, t) \leq \left\lfloor \frac{n}{t} \left\lfloor \frac{n-1}{t-1} \left\lfloor \cdots \left\lfloor \frac{n-t+k}{k} \right\rfloor \cdots \right\rfloor \right\rfloor \right\rfloor$$

Neki nelinearni kodovi

Lema.

$$A(n, 2k-1, t) = A(n, 2k, t) \le \left\lfloor \frac{n}{t} \left\lfloor \frac{n-1}{t-1} \left\lfloor \cdots \left\lfloor \frac{n-t+k}{k} \right\rfloor \cdots \right\rfloor \right\rfloor \right\rfloor$$

Teorem (Johnsonova ocjena)

Ako postoji binarni (n, M, d) kod minimalne udaljenosti $d = 2e + 1$, onda vrijedi

$$M \le \frac{2^n}{\displaystyle\sum_{i=0}^{e} \binom{n}{i} + \frac{\binom{n}{e+1} - \binom{d}{e} A(n, d, d)}{\left\lfloor \frac{n}{e+1} \right\rfloor}}.$$

Neki nelinearni kodovi

Lema.

$$A(n, 2k-1, t) = A(n, 2k, t) \leq \left\lfloor \frac{n}{t} \left\lfloor \frac{n-1}{t-1} \left\lfloor \cdots \left\lfloor \frac{n-t+k}{k} \right\rfloor \cdots \right\rfloor \right\rfloor \right\rfloor$$

Teorem (Johnsonova ocjena)

Ako postoji binarni (n, M, d) kod minimalne udaljenosti $d = 2e + 1$, onda vrijedi

$$M \leq \frac{2^n}{\sum_{i=0}^{e} \binom{n}{i} + \frac{\binom{n}{e+1} - \binom{d}{e} A(n,d,d)}{\left\lfloor \frac{n}{e+1} \right\rfloor}}.$$

$$n = 15,\ d = 5 \quad \Rightarrow \quad A(15, 5, 5) \leq \left\lfloor \frac{15}{5} \left\lfloor \frac{14}{4} \left\lfloor \frac{13}{3} \right\rfloor \right\rfloor \right\rfloor = 42$$

Nordstrom-Robinsonov kod

$$n = 15,\ d = 5 \quad \Rightarrow \quad M \leq \frac{2^{15}}{121 + \frac{455 - 10 \cdot 42}{5}} = 256 = 2^8$$

Nordstrom-Robinsonov kod

$$n = 15,\ d = 5 \quad \Rightarrow \quad M \leq \frac{2^{15}}{121 + \frac{455 - 10 \cdot 42}{5}} = 256 = 2^8$$

Najveći linearni $[15, m, 5]_2$ kod ima $M = 2^7 = 128$ kodnih riječi.

Nordstrom-Robinsonov kod

$$n = 15,\ d = 5 \quad \Rightarrow \quad M \le \frac{2^{15}}{121 + \frac{455 - 10\cdot 42}{5}} = 256 = 2^8$$

Najveći linearni $[15, m, 5]_2$ kod ima $M = 2^7 = 128$ kodnih riječi.

Postoji li veći nelinearni $(15, M, 5)_2$ kod?

Nordstrom-Robinsonov kod

$$n = 15,\ d = 5 \quad \Rightarrow \quad M \le \frac{2^{15}}{121 + \frac{455-10\cdot 42}{5}} = 256 = 2^8$$

Najveći linearni $[15, m, 5]_2$ kod ima $M = 2^7 = 128$ kodnih riječi.

Postoji li veći nelinearni $(15, M, 5)_2$ **kod?**

A. W. Nordstrom, J. P. Robinson, *An optimum nonlinear code*, Information and Control **11** (1967), 613–616.

$$(15, 256, 5)_2$$

Nordstrom-Robinsonov kod

$$n = 15,\ d = 5 \quad \Rightarrow \quad M \le \frac{2^{15}}{121 + \frac{455 - 10\cdot 42}{5}} = 256 = 2^8$$

Najveći linearni $[15, m, 5]_2$ kod ima $M = 2^7 = 128$ kodnih riječi.

Postoji li veći nelinearni $(15, M, 5)_2$ **kod?**

A. W. Nordstrom, J. P. Robinson, *An optimum nonlinear code*, Information and Control **11** (1967), 613–616.

$$(15, 256, 5)_2$$

Prošireni kod ima parametre $(16, 256, 6)_2$, zovemo ga Nordstrom-Robinsonovim kodom i označavamo $\mathcal{N}_{16}$.

Nordstrom-Robinsonov kod

$$n = 15,\ d = 5 \quad \Rightarrow \quad M \le \frac{2^{15}}{121 + \frac{455 - 10\cdot 42}{5}} = 256 = 2^8$$

Najveći linearni $[15, m, 5]_2$ kod ima $M = 2^7 = 128$ kodnih riječi.

Postoji li veći nelinearni $(15, M, 5)_2$ kod?

A. W. Nordstrom, J. P. Robinson, *An optimum nonlinear code*, Information and Control **11** (1967), 613–616.

$$(15, 256, 5)_2$$

Prošireni kod ima parametre $(16, 256, 6)_2$, zovemo ga Nordstrom-Robinsonovim kodom i označavamo $\mathcal{N}_{16}$.

```
gap> N16:=NordstromRobinsonCode();
a (16,256,6)4 Nordstrom-Robinson code over GF(2)
gap> AddWeights(WeightDistribution(N16));
[ [ 0, 1 ], [ 6, 112 ], [ 8, 30 ], [ 10, 112 ], [ 16, 1 ] ]
```

Povijest teorije kodiranja

E. R. Berlekamp (ur.), *Key papers in the development of coding theory*, IEEE Press, New York, 1974.

Povijest teorije kodiranja

E. R. Berlekamp (ur.), *Key papers in the development of coding theory*, IEEE Press, New York, 1974.

table of contents would be omitted. While I will not attempt to compile such an honor roll, I will reveal my nominations for certain work in coding theory which deserves this modest recognition as we commemorate our 25th anniversary.

Best papers: Bose–Chaudhuri and Hocquenghem (close second: Reed–Solomon).

Most influential book: Peterson, 1961.

Most influential conference: MIT, 1954 [51].

Best single published page: Golay, 1949.

Best talk to nonspecialists: Robinson (see the introduction to Section II of this volume).

Most entertaining conference paper: E. C. Posner, Madison, May 1968 [38].

Best open problem: Resolve the asymptotic discrepancy between the Elias bound and the Gilbert bound.

Povijest teorije kodiranja

E. R. Berlekamp (ur.), *Key papers in the development of coding theory*, IEEE Press, New York, 1974.

and Zierler met with mixed success. It was shown that no *linear* code of distance 5 has more codewords of length 15 than the double-error-correcting binary BCH code; which has 2^7. The best upper bound that could be obtained on the number of codewords of a nonlinear code of distance 5 and length 15 was Johnson's [34] 2^8. Since this was the simplest example in which the difference between the bounds and the known constructions differed by a full power of two, Robinson chose it as an example of a problem which he posed to high school students in an introductory talk on coding theory. One of them, named Nordstrom, accepted the challenge, and by trial and error, constructed a nonlinear code with 2^8 codewords of length 15 and distance 5, the now-classic Nordstrom–Robinson code [35]. This code was also independently dis-

E. R. Berlekamp (ur.), *Key papers in the development of coding theory*, IEEE Press, New York, 1974.

covered by Zietsiev and Zinoviev [36]. Several previously known nonlinear codes, including the Nadler code [37], were found to be shortened versions of the NR code. Goethals [38] showed how the Nordstrom-Robinson code can be more readily derived as a subcode of the Golay code, and Berlekamp [39] used this observation to explain the surprisingly large symmetry group of the Nordstrom-Robinson code. (It is isomorphic to A_7, the alternating group on 7 letters. The symmetry groups of this code and virtually all good codes of lengths less than 25 are closely related to M_{24} in one way or another.)

Preparatini i Kerdockovi kodovi

F. P. Preparata, *A class of optimum nonlinear double-error-correcting codes*, Information and Control **13** (1968), 378–400.

$$(2^m, 2^{2^m-2m}, 6) \quad \ldots \quad \mathscr{P}(m),\ m \geq 4 \text{ paran}$$

Preparatini i Kerdockovi kodovi

F. P. Preparata, *A class of optimum nonlinear double-error-correcting codes*, Information and Control **13** (1968), 378–400.

$$(2^m, 2^{2^m-2m}, 6) \quad \dots \quad \mathscr{P}(m),\ m \geq 4 \text{ paran}$$

A. M. Kerdock, *A class of low-rate nonlinear binary codes*, Information and Control **20** (1972), 182–187 (ispravka u **21** (1972), 395).

$$(2^m, 2^{2m}, 2^{m-1} - 2^{(m-2)/2}) \quad \dots \quad \mathscr{K}(m),\ m \geq 4 \text{ paran}$$

Preparatini i Kerdockovi kodovi

F. P. Preparata, *A class of optimum nonlinear double-error-correcting codes*, Information and Control **13** (1968), 378–400.

$$(2^m, 2^{2^m-2m}, 6) \quad \ldots \quad \mathscr{P}(m),\ m \geq 4 \text{ paran}$$

A. M. Kerdock, *A class of low-rate nonlinear binary codes*, Information and Control **20** (1972), 182–187 (ispravka u **21** (1972), 395).

$$(2^m, 2^{2m}, 2^{m-1} - 2^{(m-2)/2}) \quad \ldots \quad \mathscr{K}(m),\ m \geq 4 \text{ paran}$$

i	0	$2^{m-1} - 2^{m/2-1}$	2^{m-1}	$2^{m-1} + 2^{m/2-1}$	2^m
A_i	1	$2^m(2^{m-1} - 1)$	$2^{m+1} - 2$	$2^m(2^{m-1} - 1)$	1

Preparatini i Kerdockovi kodovi

F. P. Preparata, *A class of optimum nonlinear double-error-correcting codes*, Information and Control **13** (1968), 378–400.

$$(2^m, 2^{2^m-2m}, 6) \quad \ldots \quad \mathscr{P}(m),\ m \geq 4 \text{ paran}$$

A. M. Kerdock, *A class of low-rate nonlinear binary codes*, Information and Control **20** (1972), 182–187 (ispravka u **21** (1972), 395).

$$(2^m, 2^{2m}, 2^{m-1} - 2^{(m-2)/2}) \quad \ldots \quad \mathscr{K}(m),\ m \geq 4 \text{ paran}$$

i	0	$2^{m-1} - 2^{m/2-1}$	2^{m-1}	$2^{m-1} + 2^{m/2-1}$	2^m
A_i	1	$2^m(2^{m-1} - 1)$	$2^{m+1} - 2$	$2^m(2^{m-1} - 1)$	1

Kodovi $\mathscr{K}(m)$ i $\mathscr{P}(m)$ su distancijsko invarijantni, tj. distribucija udaljenosti od bilo koje fiksne kodne riječi je ista.

Preparatini i Kerdockovi kodovi

Neka su težinski polinomi Kerdockovog i Preparatinog koda

$$W_{\mathscr{K}(m)}(X,Y) = \sum_i A_i X^{2^m - i} Y^i \quad \text{i} \quad W_{\mathscr{P}(m)}(X,Y) = \sum_i B_i X^{2^m - i} Y^i$$

Preparatini i Kerdockovi kodovi

Neka su težinski polinomi Kerdockovog i Preparatinog koda

$$W_{\mathscr{K}(m)}(X,Y) = \sum_i A_i X^{2^m - i} Y^i \quad \text{i} \quad W_{\mathscr{P}(m)}(X,Y) = \sum_i B_i X^{2^m - i} Y^i$$

Vrijedi

$$W_{\mathscr{P}(m)}(X,Y) = 2^{-2m}\, W_{\mathscr{K}(m)}(X+Y, X-Y)$$

Preparatini i Kerdockovi kodovi

Neka su težinski polinomi Kerdockovog i Preparatinog koda

$$W_{\mathcal{K}(m)}(X,Y) = \sum_i A_i X^{2^m - i} Y^i \quad \text{i} \quad W_{\mathcal{P}(m)}(X,Y) = \sum_i B_i X^{2^m - i} Y^i$$

Vrijedi

$$W_{\mathcal{P}(m)}(X,Y) = 2^{-2m}\, W_{\mathcal{K}(m)}(X+Y, X-Y)$$

P. J. Cameron, J. H. van Lint, *Designs, graphs, codes and their links*, Cambridge University Press, Cambridge, 1991.

> *From Lemma 12.9 we find the distance enumerator of $\mathcal{K}(m)$. (...) If we substitute the distance enumerator in MacWilliams' relation we actually find a polynomial with integer coefficients B_i (for $A^\perp$). This is in fact the distance enumerator of an extended Preparata code.* ***There is no explanation for this strange fact!***

Preparatini i Kerdockovi kodovi

A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, *The* $\mathbb{Z}_4$*-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.

Preparatini i Kerdockovi kodovi

A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.

Propozicija.

Nosači vektora fiksne težine u $\mathscr{P}(m)$ i $\mathscr{K}(m)$ čine 3-dizajne.

Preparatini i Kerdockovi kodovi

A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.

Propozicija.

Nosači vektora fiksne težine u $\mathscr{P}(m)$ i $\mathscr{K}(m)$ čine 3-dizajne.

i	0	$2^{m-1}-2^{m/2-1}$	2^{m-1}	$2^{m-1}+2^{m/2-1}$	2^m
A_i	1	$2^m(2^{m-1}-1)$	$2^{m+1}-2$	$2^m(2^{m-1}-1)$	1

Preparatini i Kerdockovi kodovi

A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.

Propozicija.

Nosači vektora fiksne težine u $\mathscr{P}(m)$ i $\mathscr{K}(m)$ čine 3-dizajne.

i	0	$2^{m-1}-2^{m/2-1}$	2^{m-1}	$2^{m-1}+2^{m/2-1}$	2^m
A_i	1	$2^m(2^{m-1}-1)$	$2^{m+1}-2$	$2^m(2^{m-1}-1)$	1

$\mathscr{k} = 2^{m-1}+2^{m/2-1}$

Preparatini i Kerdockovi kodovi

A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.

Propozicija.

Nosači vektora fiksne težine u $\mathscr{P}(m)$ i $\mathscr{K}(m)$ čine 3-dizajne.

i	0	$2^{m-1}-2^{m/2-1}$	2^{m-1}	$2^{m-1}+2^{m/2-1}$	2^m
A_i	1	$2^m(2^{m-1}-1)$	$2^{m+1}-2$	$2^m(2^{m-1}-1)$	1

$\mathscr{k} = 2^{m-1}+2^{m/2-1} \rightsquigarrow$ 3-$(2^m, \mathscr{k}, \Lambda)$ dizajn s $b = A_{\mathscr{k}} = 2^m(2^{m-1}-1)$

Preparatini i Kerdockovi kodovi

A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.

Propozicija.

Nosači vektora fiksne težine u $\mathscr{P}(m)$ i $\mathscr{K}(m)$ čine 3-dizajne.

i	0	$2^{m-1}-2^{m/2-1}$	2^{m-1}	$2^{m-1}+2^{m/2-1}$	2^m
A_i	1	$2^m(2^{m-1}-1)$	$2^{m+1}-2$	$2^m(2^{m-1}-1)$	1

$\Bbbk = 2^{m-1}+2^{m/2-1} \rightsquigarrow$ 3-$(2^m, \Bbbk, \Lambda)$ dizajn s $b = A_{\Bbbk} = 2^m(2^{m-1}-1)$

$$\Lambda = 2^{m/2-4}\left(2^{m/2}+2\right)\left(2^m+2^{m/2}-4\right)$$

Preparatini i Kerdockovi kodovi

A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.

Propozicija.

Nosači vektora fiksne težine u $\mathscr{P}(m)$ i $\mathscr{K}(m)$ čine 3-dizajne.

i	0	$2^{m-1}-2^{m/2-1}$	2^{m-1}	$2^{m-1}+2^{m/2-1}$	2^m
A_i	1	$2^m(2^{m-1}-1)$	$2^{m+1}-2$	$2^m(2^{m-1}-1)$	1

$\Bbbk = 2^{m-1}+2^{m/2-1} \rightsquigarrow$ 3-$(2^m,\Bbbk,\Lambda)$ dizajn s $b = A_{\Bbbk} = 2^m(2^{m-1}-1)$

$$\operatorname{supp}(x+y) = \operatorname{supp} x \,\Delta\, \operatorname{supp} y = (\operatorname{supp} x \cup \operatorname{supp} y) \setminus (\operatorname{supp} x \cap \operatorname{supp} y)$$

Preparatini i Kerdockovi kodovi

A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.

Propozicija.

Nosači vektora fiksne težine u $\mathscr{P}(m)$ i $\mathscr{K}(m)$ čine 3-dizajne.

i	0	$2^{m-1}-2^{m/2-1}$	2^{m-1}	$2^{m-1}+2^{m/2-1}$	2^m
A_i	1	$2^m(2^{m-1}-1)$	$2^{m+1}-2$	$2^m(2^{m-1}-1)$	1

$\Bbbk = 2^{m-1}+2^{m/2-1} \rightsquigarrow$ 3-$(2^m,\Bbbk,\Lambda)$ dizajn s $b = A_{\Bbbk} = 2^m(2^{m-1}-1)$

$$|\operatorname{supp} x \cap \operatorname{supp} y| = \Bbbk - \frac{1}{2}w(x+y)$$

Preparatini i Kerdockovi kodovi

A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.

Propozicija.

Nosači vektora fiksne težine u $\mathscr{P}(m)$ i $\mathscr{K}(m)$ čine 3-dizajne.

i	0	$2^{m-1}-2^{m/2-1}$	2^{m-1}	$2^{m-1}+2^{m/2-1}$	2^m
A_i	1	$2^m(2^{m-1}-1)$	$2^{m+1}-2$	$2^m(2^{m-1}-1)$	1

$\Bbbk = 2^{m-1}+2^{m/2-1} \rightsquigarrow$ 3-$(2^m, \Bbbk, \Lambda)$ dizajn s $b = A_{\Bbbk} = 2^m(2^{m-1}-1)$

$$|\operatorname{supp} x \cap \operatorname{supp} y| = \Bbbk - \frac{1}{2}w(x+y)$$

$x = 2^{m-2}+2^{m/2-2}, \quad y = 2^{m-2}+2\cdot 2^{m/2-2}, \quad z = 2^{m-2}+3\cdot 2^{m/2-2}$

Preparatini i Kerdockovi kodovi

Teorem (Cameron, Delsarte)

Neka je $\mathscr{D}$ kombinatorni t-$(v, \mathscr{k}, \lambda)$ dizajn stupnja d s presječnim brojevima $x_1 > \ldots > x_d \geq 0$. Stavimo $x_0 = \mathscr{k}$ i za blokove $X, Y \in \mathscr{D}$ definiramo da su i-asocirani ako je $|X \cap Y| = x_i$. Ako je $\boldsymbol{t \geq 2d - 2}$, onda na taj način dobivamo asocijacijsku shemu s d klasa, podshemu Johnsonove sheme $J(v, \mathscr{k})$.

Preparatini i Kerdockovi kodovi

Teorem (Cameron, Delsarte)

Neka je $\mathscr{D}$ kombinatorni t-$(v, \Bbbk, \lambda)$ dizajn stupnja d s presječnim brojevima $x_1 > \ldots > x_d \geq 0$. Stavimo $x_0 = \Bbbk$ i za blokove $X, Y \in \mathscr{D}$ definiramo da su i-asocirani ako je $|X \cap Y| = x_i$. Ako je $\boldsymbol{t \geq 2d - 2}$, onda na taj način dobivamo asocijacijsku shemu s d klasa, podshemu Johnsonove sheme $J(v, \Bbbk)$.

Teorem (Nodina nejednakost)

Ako postoji $SSSD(v, \Bbbk, \lambda; r)$, onda je

$$(r-1)\left[(\Bbbk-2)\lambda\binom{\Bbbk}{3} - (v-2)\left[(v-\Bbbk)\binom{\nu}{3} + \Bbbk\binom{\mu}{3}\right]\right] \leq$$

$$\leq (v-2)\left[(v-1)\binom{\lambda}{3} + \binom{\Bbbk}{3} - \left[(v-k)\binom{\nu}{3} + \Bbbk\binom{\mu}{3}\right]\right]$$

Jednakost se dostiže ako i samo ako $(X_1, X_2 \cup \cdots \cup X_r)$ čini 3-dizajn.

Shematski 3-dizajni stupnja 3

3-$(2^m,\, 2^{m-1} + 2^{m/2-1},\, \Lambda)$ dizajn s $b = 2^m(2^{m-1} - 1)$ blokova

$$\Lambda = 2^{m/2-4}\left(2^{m/2} + 2\right)\left(2^m + 2^{m/2} - 4\right)$$

$x = 2^{m-2} + 2^{m/2-2}, \quad y = 2^{m-2} + 2 \cdot 2^{m/2-2}, \quad z = 2^{m-2} + 3 \cdot 2^{m/2-2}$

Shematski 3-dizajni stupnja 3

3-(2^m, $2^{m-1}+2^{m/2-1}$, Λ) dizajn s $b=2^m(2^{m-1}-1)$ blokova

$$\Lambda = 2^{m/2-4}\left(2^{m/2}+2\right)\left(2^m+2^{m/2}-4\right)$$

$x=2^{m-2}+2^{m/2-2}$, $\;y=2^{m-2}+2\cdot 2^{m/2-2}$, $\;z=2^{m-2}+3\cdot 2^{m/2-2}$

Relacija "presjek je veličine y" je relacija ekvivalencije na skupu blokova. Klase ekvivalencije su simetrični $(v,\Bbbk,\lambda)$ dizajni za $\lambda=y$, vlakna blokovne sheme.

Shematski 3-dizajni stupnja 3

3-$(2^m, 2^{m-1} + 2^{m/2-1}, \Lambda)$ dizajn s $b = 2^m(2^{m-1} - 1)$ blokova

$$\Lambda = 2^{m/2-4}\left(2^{m/2} + 2\right)\left(2^m + 2^{m/2} - 4\right)$$

$$x = 2^{m-2} + 2^{m/2-2}, \quad y = 2^{m-2} + 2 \cdot 2^{m/2-2}, \quad z = 2^{m-2} + 3 \cdot 2^{m/2-2}$$

Relacija "presjek je veličine y" je relacija ekvivalencije na skupu blokova. Klase ekvivalencije su simetrični $(v, \Bbbk, \lambda)$ dizajni za $\lambda = y$, vlakna blokovne sheme.

Ako dodamo još jedno vlakno kojeg čine točke 3-dizajna, dobivamo SSSD sa $r = b/v + 1 = 2^{m-1}$ vlakna. To je najveći mogući broj vlakna i dostiže Nodinu nejednakost

$$r \leq \frac{(v-2)\sqrt{\Bbbk - \lambda}}{2\Bbbk - v} + 1$$

Shematski 3-dizajni stupnja 3

3-$(2^m, 2^{m-1}+2^{m/2-1}, \Lambda)$ dizajn s $b = 2^m(2^{m-1}-1)$ blokova

$$\Lambda = 2^{m/2-4}\left(2^{m/2}+2\right)\left(2^m+2^{m/2}-4\right)$$

$$x = 2^{m-2}+2^{m/2-2}, \quad y = 2^{m-2}+2\cdot 2^{m/2-2}, \quad z = 2^{m-2}+3\cdot 2^{m/2-2}$$

Relacija "presjek je veličine y" je relacija ekvivalencije na skupu blokova. Klase ekvivalencije su simetrični $(v, \Bbbk, \lambda)$ dizajni za $\lambda = y$, vlakna blokovne sheme.

Ako dodamo još jedno vlakno kojeg čine točke 3-dizajna, dobivamo SSSD sa $r = b/v + 1 = 2^{m-1}$ vlakna. To je najveći mogući broj vlakna i dostiže Nodinu nejednakost

$$r \leq \frac{(v-2)\sqrt{\Bbbk-\lambda}}{2\Bbbk - v} + 1$$

Parametri $\mu = z$ i $\nu = x$ SSSD-a su druga dva presječna broja.

Shematski 3-dizajni stupnja 3

Definicija.

Sustav spojenih simetričnih dizajna $SSSD(v, \Bbbk, \lambda; r)$ (eng. linked system of symmetric designs, $LSSD$) je graf sa skupom vrhova $X = X_1 \cup \cdots \cup X_r$ (disjunktna unija). Skupove X_i zovemo vlaknima i svaki ima v vrhova, pa je ukupan broj vrhova $n = r\,v$. Bridovi zadovoljavaju:

1. svaki brid ima krajeve u različitim vlaknima
2. za sve $i, j \in \{1, \ldots, r\}$, $i \neq j$, inducirani podgraf na $X_i \cup X_j$ je incidencijski graf nekog $(v, \Bbbk, \lambda)$ dizajna
3. postoje konstante μ i ν takve da za različite $i, j, k \in \{1, \ldots, r\}$ i za svaki izbor vrhova $x \in X_i$, $y \in X_j$, broj zajedničkih susjeda od x i y u vlaknu X_k je μ ako su x i y susjedni, a ν ako nisu susjedni

Konstrukcija Kerdockovih kodova

```
gap> C:=ReedMullerCode(2,4);
a linear [16,11,4]2 Reed-Muller (2,4) code over GF(2)
gap> AddWeights(WeightDistribution(C));
[ [ 0, 1 ], [ 4, 140 ], [ 6, 448 ], [ 8, 870 ], [ 10, 448 ],
  [ 12, 140 ], [ 16, 1 ] ]
```

Konstrukcija Kerdockovih kodova

```
gap> C:=ReedMullerCode(2,4);
a linear [16,11,4]2 Reed-Muller (2,4) code over GF(2)
gap> AddWeights(WeightDistribution(C));
[ [ 0, 1 ], [ 4, 140 ], [ 6, 448 ], [ 8, 870 ], [ 10, 448 ],
  [ 12, 140 ], [ 16, 1 ] ]
```

- 3-$(16, 4, 1)$ s $b = 140$

Konstrukcija Kerdockovih kodova

```
gap> C:=ReedMullerCode(2,4);
a linear [16,11,4]2 Reed-Muller (2,4) code over GF(2)
gap> AddWeights(WeightDistribution(C));
[ [ 0, 1 ], [ 4, 140 ], [ 6, 448 ], [ 8, 870 ], [ 10, 448 ],
  [ 12, 140 ], [ 16, 1 ] ]
```

- 3-$(16, 4, 1)$ s $b = 140 \rightsquigarrow AG_2(4, 2)$

Konstrukcija Kerdockovih kodova

```
gap> C:=ReedMullerCode(2,4);
a linear [16,11,4]2 Reed-Muller (2,4) code over GF(2)
gap> AddWeights(WeightDistribution(C));
[ [ 0, 1 ], [ 4, 140 ], [ 6, 448 ], [ 8, 870 ], [ 10, 448 ],
  [ 12, 140 ], [ 16, 1 ] ]
```

- 3-$(16, 4, 1)$ s $b = 140 \rightsquigarrow AG_2(4, 2)$
- 3-$(16, 8, 87)$ s $b = 870$

Konstrukcija Kerdockovih kodova

```
gap> C:=ReedMullerCode(2,4);
a linear [16,11,4]2 Reed-Muller (2,4) code over GF(2)
gap> AddWeights(WeightDistribution(C));
[ [ 0, 1 ], [ 4, 140 ], [ 6, 448 ], [ 8, 870 ], [ 10, 448 ],
  [ 12, 140 ], [ 16, 1 ] ]
```

- 3-$(16,4,1)$ s $b = 140 \rightsquigarrow AG_2(4,2)$
- 3-$(16,8,87)$ s $b = 870$
  Ima poddizajn 3-$(16,8,3)$ s $b = 30 \rightsquigarrow AG_3(4,2)$

Konstrukcija Kerdockovih kodova

```
gap> C:=ReedMullerCode(2,4);
a linear [16,11,4]2 Reed-Muller (2,4) code over GF(2)
gap> AddWeights(WeightDistribution(C));
[ [ 0, 1 ], [ 4, 140 ], [ 6, 448 ], [ 8, 870 ], [ 10, 448 ],
  [ 12, 140 ], [ 16, 1 ] ]
```

- 3-$(16, 4, 1)$ s $b = 140 \rightsquigarrow AG_2(4, 2)$
- 3-$(16, 8, 87)$ s $b = 870$
  Ima poddizajn 3-$(16, 8, 3)$ s $b = 30 \rightsquigarrow AG_3(4, 2)$
- 3-$(16, 10, 96)$ s $b = 448$

Konstrukcija Kerdockovih kodova

```
gap> C:=ReedMullerCode(2,4);
a linear [16,11,4]2 Reed-Muller (2,4) code over GF(2)
gap> AddWeights(WeightDistribution(C));
[ [ 0, 1 ], [ 4, 140 ], [ 6, 448 ], [ 8, 870 ], [ 10, 448 ],
  [ 12, 140 ], [ 16, 1 ] ]
```

- 3-$(16,4,1)$ s $b = 140 \rightsquigarrow AG_2(4,2)$
- 3-$(16,8,87)$ s $b = 870$
  Ima poddizajn 3-$(16,8,3)$ s $b = 30 \rightsquigarrow AG_3(4,2)$
- 3-$(16,10,96)$ s $b = 448$
  Ima poddizajn 3-$(16,10,24)$ s $b = 112$ i $x = 5$, $y = 6$, $z = 7$

Konstrukcija Kerdockovih kodova

```
gap> C:=ReedMullerCode(2,4);
a linear [16,11,4]2 Reed-Muller (2,4) code over GF(2)
gap> AddWeights(WeightDistribution(C));
[ [ 0, 1 ], [ 4, 140 ], [ 6, 448 ], [ 8, 870 ], [ 10, 448 ],
  [ 12, 140 ], [ 16, 1 ] ]
```

- 3-$(16,4,1)$ s $b = 140 \rightsquigarrow AG_2(4,2)$
- 3-$(16,8,87)$ s $b = 870$
  Ima poddizajn 3-$(16,8,3)$ s $b = 30 \rightsquigarrow AG_3(4,2)$
- 3-$(16,10,96)$ s $b = 448$
  Ima poddizajn 3-$(16,10,24)$ s $b = 112$ i $x = 5$, $y = 6$, $z = 7$
  Blokovna shema je $SSSD(16,10,6;7)$ s $\mu = 7$, $\nu = 5$

Konstrukcija Kerdockovih kodova

```
gap> C:=ReedMullerCode(2,4);
a linear [16,11,4]2 Reed-Muller (2,4) code over GF(2)
gap> AddWeights(WeightDistribution(C));
[ [ 0, 1 ], [ 4, 140 ], [ 6, 448 ], [ 8, 870 ], [ 10, 448 ],
  [ 12, 140 ], [ 16, 1 ] ]
```

- 3-$(16,4,1)$ s $b = 140 \rightsquigarrow AG_2(4,2)$
- 3-$(16,8,87)$ s $b = 870$
  Ima poddizajn 3-$(16,8,3)$ s $b = 30 \rightsquigarrow AG_3(4,2)$
- 3-$(16,10,96)$ s $b = 448$
  Ima poddizajn 3-$(16,10,24)$ s $b = 112$ i $x = 5$, $y = 6$, $z = 7$
  Blokovna shema je $SSSD(16,10,6;7)$ s $\mu = 7$, $\nu = 5$
- 3-$(16,6,16)$ s $b = 448$
  Ima poddizajn 3-$(16,6,4)$ s $b = 112$ i $x = 1$, $y = 2$, $z = 4$
  Blokovna shema je $SSSD(16,6,2;7)$ s $\mu = 1$, $\nu = 3$

```
gap> C:=ReedMullerCode(2,4);
a linear [16,11,4]2 Reed-Muller (2,4) code over GF(2)
gap> AddWeights(WeightDistribution(C));
[ [ 0, 1 ], [ 4, 140 ], [ 6, 448 ], [ 8, 870 ], [ 10, 448 ],
  [ 12, 140 ], [ 16, 1 ] ]
gap> N16:=NordstromRobinsonCode();
a (16,256,6)4 Nordstrom-Robinson code over GF(2)
gap> AddWeights(WeightDistribution(N16));
[ [ 0, 1 ], [ 6, 112 ], [ 8, 30 ], [ 10, 112 ], [ 16, 1 ] ]
```

Konstrukcija Kerdockovih kodova

```
gap> C:=ReedMullerCode(2,4);
a linear [16,11,4]2 Reed-Muller (2,4) code over GF(2)
gap> AddWeights(WeightDistribution(C));
[ [ 0, 1 ], [ 4, 140 ], [ 6, 448 ], [ 8, 870 ], [ 10, 448 ],
  [ 12, 140 ], [ 16, 1 ] ]
gap> N16:=NordstromRobinsonCode();
a (16,256,6)4 Nordstrom-Robinson code over GF(2)
gap> AddWeights(WeightDistribution(N16));
[ [ 0, 1 ], [ 6, 112 ], [ 8, 30 ], [ 10, 112 ], [ 16, 1 ] ]
```

$$\mathrm{RM}(1,m) \subset \mathscr{K}(m) \subset \mathrm{RM}(2,m)$$

Konstrukcija Kerdockovih kodova

```
gap> C:=ReedMullerCode(2,4);
a linear [16,11,4]2 Reed-Muller (2,4) code over GF(2)
gap> AddWeights(WeightDistribution(C));
[ [ 0, 1 ], [ 4, 140 ], [ 6, 448 ], [ 8, 870 ], [ 10, 448 ],
  [ 12, 140 ], [ 16, 1 ] ]
```

```
gap> N16:=NordstromRobinsonCode();
a (16,256,6)4 Nordstrom-Robinson code over GF(2)
gap> AddWeights(WeightDistribution(N16));
[ [ 0, 1 ], [ 6, 112 ], [ 8, 30 ], [ 10, 112 ], [ 16, 1 ] ]
```

$$\mathrm{RM}(1,m) \subset \mathscr{K}(m) \subset \mathrm{RM}(2,m)$$

$\mathscr{K}(m)$ je sastavljen od susjednih klasa $\mathbb{Q}(B_i)$ za neke $B_1, B_2, B_2, \ldots$

Konstrukcija Kerdockovih kodova

```
gap> C:=ReedMullerCode(2,4);
a linear [16,11,4]2 Reed-Muller (2,4) code over GF(2)
gap> AddWeights(WeightDistribution(C));
[ [ 0, 1 ], [ 4, 140 ], [ 6, 448 ], [ 8, 870 ], [ 10, 448 ],
  [ 12, 140 ], [ 16, 1 ] ]
```

```
gap> N16:=NordstromRobinsonCode();
a (16,256,6)4 Nordstrom-Robinson code over GF(2)
gap> AddWeights(WeightDistribution(N16));
[ [ 0, 1 ], [ 6, 112 ], [ 8, 30 ], [ 10, 112 ], [ 16, 1 ] ]
```

$$\mathrm{RM}(1,m) \subset \mathscr{K}(m) \subset \mathrm{RM}(2,m)$$

$\mathscr{K}(m)$ je sastavljen od susjednih klasa $\mathbb{Q}(B_i)$ za neke $B_1, B_2, B_2, \ldots$

Da dobijemo što veću minimalnu udaljenost, razlike $B_i - B_j$ trebaju biti regularne simplektičke matrice. Zato m mora biti paran broj.

Konstrukcija Kerdockovih kodova

```
gap> C:=ReedMullerCode(2,4);
a linear [16,11,4]2 Reed-Muller (2,4) code over GF(2)
gap> AddWeights(WeightDistribution(C));
[ [ 0, 1 ], [ 4, 140 ], [ 6, 448 ], [ 8, 870 ], [ 10, 448 ],
  [ 12, 140 ], [ 16, 1 ] ]
```

```
gap> N16:=NordstromRobinsonCode();
a (16,256,6)4 Nordstrom-Robinson code over GF(2)
gap> AddWeights(WeightDistribution(N16));
[ [ 0, 1 ], [ 6, 112 ], [ 8, 30 ], [ 10, 112 ], [ 16, 1 ] ]
```

$$\mathrm{RM}(1,m) \subset \mathcal{K}(m) \subset \mathrm{RM}(2,m)$$

$\mathcal{K}(m)$ je sastavljen od susjednih klasa $\mathbb{Q}(B_i)$ za neke $B_1, B_2, B_2, \ldots$

Da dobijemo što veću minimalnu udaljenost, razlike $B_i - B_j$ trebaju biti regularne simplektičke matrice. Zato m mora biti paran broj.

Koliko najviše takvih matrica možemo naći?

Konstrukcija Kerdockovih kodova

```
gap> C:=ReedMullerCode(2,4);
a linear [16,11,4]2 Reed-Muller (2,4) code over GF(2)
gap> AddWeights(WeightDistribution(C));
[ [ 0, 1 ], [ 4, 140 ], [ 6, 448 ], [ 8, 870 ], [ 10, 448 ],
  [ 12, 140 ], [ 16, 1 ] ]

gap> N16:=NordstromRobinsonCode();
a (16,256,6)4 Nordstrom-Robinson code over GF(2)
gap> AddWeights(WeightDistribution(N16));
[ [ 0, 1 ], [ 6, 112 ], [ 8, 30 ], [ 10, 112 ], [ 16, 1 ] ]
```

$$\mathrm{RM}(1,m) \subset \mathcal{K}(m) \subset \mathrm{RM}(2,m)$$

$\mathcal{K}(m)$ je sastavljen od susjednih klasa $\mathbb{Q}(B_i)$ za neke $B_1, B_2, B_2, \ldots$

Da dobijemo što veću minimalnu udaljenost, razlike $B_i - B_j$ trebaju biti regularne simplektičke matrice. Zato m mora biti paran broj.

Koliko najviše takvih matrica možemo naći? 2^{m-1}

Konstrukcija Kerdockovih kodova

Definicija.

Za skup $\{B_1, \ldots, B_r\}$ simplektičkih matrica reda m kažemo da je Kerdockov skup ako je razlika bilo koje dvije matrice $B_i - B_j$ regularna i ako je veličine $r = 2^{m-1}$.

Konstrukcija Kerdockovih kodova

Definicija.

Za skup $\{B_1, \ldots, B_r\}$ simplektičkih matrica reda m kažemo da je Kerdockov skup ako je razlika bilo koje dvije matrice $B_i - B_j$ regularna i ako je veličine $r = 2^{m-1}$.

Teorem.

Ako je $\{B_1, \ldots, B_{2^{m-1}}\}$ Kerdockov skup simplektičkih matrica reda m, onda je $\mathscr{K}(m) = \bigcup_{i=1}^{2^{m-1}} \mathbb{Q}(B_i)$ distancijsko invarijantni binarni kod s distribucijom udaljenosti od fiksne kodne riječi danom u tablici:

Težina	0	$2^{m-1} - 2^{m/2-1}$	2^{m-1}	$2^{m-1} + 2^{m/2-1}$	2^m
Br. vektora	1	$2^m(2^{m-1} - 1)$	$2^{m+1} - 2$	$2^m(2^{m-1} - 1)$	1

Konstrukcija Kerdockovih kodova

Definicija.

Za skup $\{B_1, \ldots, B_r\}$ simplektičkih matrica reda m kažemo da je Kerdockov skup ako je razlika bilo koje dvije matrice $B_i - B_j$ regularna i ako je veličine $r = 2^{m-1}$.

Teorem.

Ako je B simplektička matrica reda m i ranga $2k$, distribucija težina u susjednoj klasi $\mathbb{Q}(B)$ dana je u tablici:

Težina	$2^{m-1} - 2^{m-k-1}$	2^{m-1}	$2^{m-1} + 2^{m-k+1}$
Br. vektora	2^{2k}	$2^{m+1} - 2^{2k+1}$	2^{2k}

Konstrukcija Kerdockovih kodova

Definicija.

Za skup $\{B_1, \ldots, B_r\}$ simplektičkih matrica reda m kažemo da je Kerdockov skup ako je razlika bilo koje dvije matrice $B_i - B_j$ regularna i ako je veličine $r = 2^{m-1}$.

Teorem.

Neka je $\{B_1, \ldots, B_r\}$ skup simplektičkih matrica parnog reda m takav da su razlike $B_i - B_j$ regularne matrice. Kao vlakna uzmimo klase $X_i = \mathbb{Q}_0(B_i)$ i definiramo da su kvadratne forme $f \in X_i$, $g \in X_j$ iz različitih vlakna susjedne ako je $f - g$ tipa $+1$. Tako dobijemo sustav spojenih simetričnih dizajna $SSSD(2^m, 2^{m-1} + 2^{m/2-1}, 2^{m-2} + 2^{m/2-1}; r)$.

Konstrukcija Kerdockovih kodova

Definicija.

Za skup $\{B_1, \ldots, B_r\}$ simplektičkih matrica reda m kažemo da je Kerdockov skup ako je razlika bilo koje dvije matrice $B_i - B_j$ regularna i ako je veličine $r = 2^{m-1}$.

Teorem.

Neka je $\{B_1, \ldots, B_r\}$ skup simplektičkih matrica parnog reda m takav da su razlike $B_i - B_j$ regularne matrice. Kao vlakna uzmimo klase $X_i = \mathbb{Q}_0(B_i)$ i definiramo da su kvadratne forme $f \in X_i$, $g \in X_j$ iz različitih vlakna susjedne ako je $f - g$ tipa $+1$. Tako dobijemo sustav spojenih simetričnih dizajna $SSSD(2^m, 2^{m-1} + 2^{m/2-1}, 2^{m-2} + 2^{m/2-1}; r)$.

W. M. Kantor, *Symplectic groups, symmetric designs, and line ovals*, J. Algebra **33** (1975), 43–58.

Kvadratne i bilinearne forme

Definicija.

Kvadratna forma je funkcija $f : V \to \mathbb{F}$ koja ima svojstva

1. $f(\alpha x) = \alpha^2 f(x)$ za sve $\alpha \in \mathbb{F}$ i $x \in V$,
2. funkcija $B : V \times V \to \mathbb{F}$ definirana s $B(x, y) = f(x + y) - f(x) - f(y)$ je bilinearna.

Kvadratne i bilinearne forme

Definicija.

Kvadratna forma je funkcija $f : V \to \mathbb{F}$ koja ima svojstva

1. $f(\alpha x) = \alpha^2 f(x)$ za sve $\alpha \in \mathbb{F}$ i $x \in V$,
2. funkcija $B : V \times V \to \mathbb{F}$ definirana s $B(x, y) = f(x + y) - f(x) - f(y)$ je bilinearna.

Bilin. forma iz 2. svojstva je simetrična: $B(x, y) = B(y, x)$, $\forall x, y \in V$.

Kvadratne i bilinearne forme

Definicija.

Kvadratna forma je funkcija $f : V \to \mathbb{F}$ koja ima svojstva

1. $f(\alpha x) = \alpha^2 f(x)$ za sve $\alpha \in \mathbb{F}$ i $x \in V$,
2. funkcija $B : V \times V \to \mathbb{F}$ definirana s $B(x, y) = f(x + y) - f(x) - f(y)$ je bilinearna.

Bilin. forma iz 2. svojstva je simetrična: $B(x, y) = B(y, x)$, $\forall x, y \in V$.

U slučaju $\mathbb{F} = \mathbb{F}_2$ je alternirajuća, tj. zadovoljava $B(x, x) = 0$, $\forall x \in V$.

Kvadratne i bilinearne forme

Definicija.

Kvadratna forma je funkcija $f : V \to \mathbb{F}$ koja ima svojstva

1. $f(\alpha x) = \alpha^2 f(x)$ za sve $\alpha \in \mathbb{F}$ i $x \in V$,
2. funkcija $B : V \times V \to \mathbb{F}$ definirana s $B(x, y) = f(x + y) - f(x) - f(y)$ je bilinearna.

Bilin. forma iz 2. svojstva je simetrična: $B(x, y) = B(y, x)$, $\forall x, y \in V$.

U slučaju $\mathbb{F} = \mathbb{F}_2$ je alternirajuća, tj. zadovoljava $B(x, x) = 0$, $\forall x \in V$.

Kažemo da se kvadratna forma f polarizira u bilinearnu formu $B = B_f$.

Kvadratne i bilinearne forme

Definicija.

Kvadratna forma je funkcija $f : V \to \mathbb{F}$ koja ima svojstva

1. $f(\alpha x) = \alpha^2 f(x)$ za sve $\alpha \in \mathbb{F}$ i $x \in V$,
2. funkcija $B : V \times V \to \mathbb{F}$ definirana s $B(x, y) = f(x + y) - f(x) - f(y)$ je bilinearna.

Bilin. forma iz 2. svojstva je simetrična: $B(x, y) = B(y, x)$, $\forall x, y \in V$.

U slučaju $\mathbb{F} = \mathbb{F}_2$ je alternirajuća, tj. zadovoljava $B(x, x) = 0$, $\forall x \in V$.

Kažemo da se kvadratna forma f polarizira u bilinearnu formu $B = B_f$.

Za polja $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ i $\mathbb{F}_q$ za neparne q preslikavanje $f \mapsto B_f$ je bijekcija:

$$f(x) = \frac{1}{2} B(x, x)$$

Kvadratne forme su homogeni polinomi drugog stupnja.

Kvadratne i bilinearne forme

Za polje $\mathbb{F}_2$ preslikavanje $f \mapsto B_f$ nije bijekcija! Prvo stvojstvo iz definicije kvadratne forme ekvivalentno je s $f(0) = 0$.

Kvadratne i bilinearne forme

Za polje $\mathbb{F}_2$ preslikavanje $f \mapsto B_f$ nije bijekcija! Prvo stvojstvo iz definicije kvadratne forme ekvivalentno je s $f(0) = 0$.

$$\mathrm{RM}_0(1, m) = \{f : \mathbb{F}_2^m \to \mathbb{F}_2 \mid f(X) = a_1 X_1 + \ldots + a_m X_m\}$$

$$\mathrm{RM}_0(2, m) = \{f : \mathbb{F}_2^m \to \mathbb{F}_2 \mid f(X) = a_1 X_1 + \ldots + a_m X_m + \sum_{1 \leq i < j \leq m} q_{ij} X_i X_j\}$$

Kvadratne i bilinearne forme

Za polje $\mathbb{F}_2$ preslikavanje $f \mapsto B_f$ nije bijekcija! Prvo stvojstvo iz definicije kvadratne forme ekvivalentno je s $f(0) = 0$.

$$\mathrm{RM}_0(1,m) = \{f : \mathbb{F}_2^m \to \mathbb{F}_2 \mid f(X) = a_1X_1 + \ldots + a_mX_m\}$$

$$\mathrm{RM}_0(2,m) = \{f : \mathbb{F}_2^m \to \mathbb{F}_2 \mid f(X) = a_1X_1 + \ldots + a_mX_m + \sum_{1\le i<j\le m} q_{ij}X_iX_j\}$$

$$\mathbb{Q}_0(B) = \{f(X) = a_1X_1 + \ldots + a_mX_m + \sum_{1\le i<j\le m} q_{ij}X_iX_j \mid a_1,\ldots,a_m \in \mathbb{F}_2\}$$

Kvadratne i bilinearne forme

Za polje $\mathbb{F}_2$ preslikavanje $f \mapsto B_f$ nije bijekcija! Prvo stvojstvo iz definicije kvadratne forme ekvivalentno je s $f(0) = 0$.

$$\mathrm{RM}_0(1, m) = \{f : \mathbb{F}_2^m \to \mathbb{F}_2 \mid f(X) = a_1 X_1 + \ldots + a_m X_m\}$$

$$\mathrm{RM}_0(2, m) = \{f : \mathbb{F}_2^m \to \mathbb{F}_2 \mid f(X) = a_1 X_1 + \ldots + a_m X_m + \sum_{1 \le i < j \le m} q_{ij} X_i X_j\}$$

$$\mathbb{Q}_0(B) = \{f(X) = a_1 X_1 + \ldots + a_m X_m + \sum_{1 \le i < j \le m} q_{ij} X_i X_j \mid a_1, \ldots, a_m \in \mathbb{F}_2\}$$

Teorem.

Neka je $\{B_1, \ldots, B_r\}$ skup simplektičkih matrica parnog reda m takav da su razlike $B_i - B_j$ regularne matrice. Kao vlakna uzmimo klase $X_i = \mathbb{Q}_0(B_i)$ i definiramo da su kvadratne forme $f \in X_i$, $g \in X_j$ iz različitih vlakna susjedne ako je $f - g$ tipa $+1$. Tako dobijemo sustav spojenih simetričnih dizajna $SSSD(2^m, 2^{m-1} + 2^{m/2-1}, 2^{m-2} + 2^{m/2-1}; r)$.

Kvadratne i bilinearne forme

Za polje $\mathbb{F}_2$ preslikavanje $f \mapsto B_f$ nije bijekcija! Prvo stvojstvo iz definicije kvadratne forme ekvivalentno je s $f(0) = 0$.

$$\mathrm{RM}_0(1,m) = \{f : \mathbb{F}_2^m \to \mathbb{F}_2 \mid f(X) = a_1 X_1 + \ldots + a_m X_m\}$$

$$\mathrm{RM}_0(2,m) = \{f : \mathbb{F}_2^m \to \mathbb{F}_2 \mid f(X) = a_1 X_1 + \ldots + a_m X_m + \sum_{1 \le i < j \le m} q_{ij} X_i X_j\}$$

$$\mathbb{Q}_0(B) = \{f(X) = a_1 X_1 + \ldots + a_m X_m + \sum_{1 \le i < j \le m} q_{ij} X_i X_j \mid a_1, \ldots, a_m \in \mathbb{F}_2\}$$

Bilinearnu formu reprezentiramo matricom $B \in M_m(\mathbb{F})$, $B(x,y) = x^\tau B y$

Kvadratne i bilinearne forme

Za polje $\mathbb{F}_2$ preslikavanje $f \mapsto B_f$ nije bijekcija! Prvo stvojstvo iz definicije kvadratne forme ekvivalentno je s $f(0) = 0$.

$$\mathrm{RM}_0(1, m) = \{f : \mathbb{F}_2^m \to \mathbb{F}_2 \mid f(X) = a_1 X_1 + \ldots + a_m X_m\}$$

$$\mathrm{RM}_0(2, m) = \{f : \mathbb{F}_2^m \to \mathbb{F}_2 \mid f(X) = a_1 X_1 + \ldots + a_m X_m + \sum_{1 \le i < j \le m} q_{ij} X_i X_j\}$$

$$\mathbb{Q}_0(B) = \{f(X) = a_1 X_1 + \ldots + a_m X_m + \sum_{1 \le i < j \le m} q_{ij} X_i X_j \mid a_1, \ldots, a_m \in \mathbb{F}_2\}$$

Bilinearnu formu reprezentiramo matricom $B \in M_m(\mathbb{F})$, $B(x, y) = x^\tau B y$

Bilinearna forma je nedegenerirana ako iz $B(x, y) = 0$, $\forall y \in V$ slijedi $x = 0$. To je evivalentno s regularnosti odgovarajuće matrice B.

Kvadratne i bilinearne forme

Za polje $\mathbb{F}_2$ preslikavanje $f \mapsto B_f$ nije bijekcija! Prvo stvojstvo iz definicije kvadratne forme ekvivalentno je s $f(0) = 0$.

$$\mathrm{RM}_0(1, m) = \{f : \mathbb{F}_2^m \to \mathbb{F}_2 \mid f(X) = a_1 X_1 + \ldots + a_m X_m\}$$

$$\mathrm{RM}_0(2, m) = \{f : \mathbb{F}_2^m \to \mathbb{F}_2 \mid f(X) = a_1 X_1 + \ldots + a_m X_m + \sum_{1 \le i < j \le m} q_{ij} X_i X_j\}$$

$$\mathbb{Q}_0(B) = \{f(X) = a_1 X_1 + \ldots + a_m X_m + \sum_{1 \le i < j \le m} q_{ij} X_i X_j \mid a_1, \ldots, a_m \in \mathbb{F}_2\}$$

Bilinearnu formu reprezentiramo matricom $B \in M_m(\mathbb{F})$, $B(x, y) = x^\tau B y$

Bilinearna forma je nedegenerirana ako iz $B(x, y) = 0$, $\forall y \in V$ slijedi $x = 0$. To je evivalentno s regularnosti odgovarajuće matrice B.

Bilinearna forma nad $\mathbb{F}_2$ je alternirajuća ako i samo ako je odgovarajuća matrica simplektička.

Konstrukcija Kerdockovih skupova

P. J. Cameron, J. H. van Lint, *Designs, graphs, codes and their links*, Cambridge University Press, Cambridge, 1991.

Konstrukcija Kerdockovih skupova

P. J. Cameron, J. H. van Lint, *Designs, graphs, codes and their links*, Cambridge University Press, Cambridge, 1991.

Constructions of Kerdock sets.

We sketch a construction of Kerdock sets due to Dillon (1974), Dye (1977), and Kantor (1983). We shall describe the easiest construction of a Kerdock set, working out the case of four by four matrices in detail.

Konstrukcija Kerdockovih skupova

P. J. Cameron, J. H. van Lint, *Designs, graphs, codes and their links*, Cambridge University Press, Cambridge, 1991.

Consider a vector $\mathbf{x}$ not on $\hat{Q}$. Then we have a natural map from $\mathbf{x}^\perp$ to the symplectic $(4n-2)$-dimensional space $W := \mathbf{x}^\perp/\mathbf{x}$. Note that $\mathbf{x}^\perp$ meets $\hat{Q}$ in (several) subspaces of dimension $2n-1$ (see Fig. 12.1).

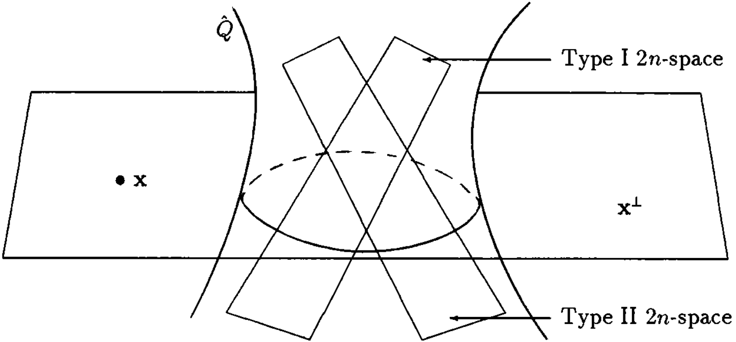

Fig. 12.1. A quadric

Konstrukcija Kerdockovih skupova

W. M. Kantor, *Codes, quadratic forms and finite geometries*, u: *Different aspects of coding theory* (Proc. Sympos. Appl. Math., San Francisco, 1995), American Mathematical Society, 1995., str. 153–177.

Konstrukcija Kerdockovih skupova

W. M. Kantor, *Codes, quadratic forms and finite geometries*, u: *Different aspects of coding theory* (Proc. Sympos. Appl. Math., San Francisco, 1995), American Mathematical Society, 1995., str. 153–177.

P. J. Cameron, J. J. Seidel, *Quadratic forms over* $GF(2)$, Nederl. Akad. Wetensch. Proc. Ser. A **76** Indag. Math. **35** (1973), 1–8.

Konstrukcija Kerdockovih skupova

W. M. Kantor, *Codes, quadratic forms and finite geometries*, u: *Different aspects of coding theory* (Proc. Sympos. Appl. Math., San Francisco, 1995), American Mathematical Society, 1995., str. 153–177.

P. J. Cameron, J. J. Seidel, *Quadratic forms over $GF(2)$*, Nederl. Akad. Wetensch. Proc. Ser. A **76** Indag. Math. **35** (1973), 1–8.

$$\mathrm{Tr} : \mathbb{F}_{2^k} \to \mathbb{F}_2, \quad \mathrm{Tr}(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{k-1}}$$

Konstrukcija Kerdockovih skupova

W. M. Kantor, *Codes, quadratic forms and finite geometries*, u: *Different aspects of coding theory* (Proc. Sympos. Appl. Math., San Francisco, 1995), American Mathematical Society, 1995., str. 153–177.

P. J. Cameron, J. J. Seidel, *Quadratic forms over GF*(2), Nederl. Akad. Wetensch. Proc. Ser. A **76** Indag. Math. **35** (1973), 1–8.

$$\mathrm{Tr} : \mathbb{F}_{2^k} \to \mathbb{F}_2, \quad \mathrm{Tr}(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{k-1}}$$

$V = \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ nad poljem $\mathbb{F}_{2^k}$ (identificiramo ga s $\mathbb{F}_2^m$ za $m = 2k$)

Konstrukcija Kerdockovih skupova

W. M. Kantor, *Codes, quadratic forms and finite geometries*, u: *Different aspects of coding theory* (Proc. Sympos. Appl. Math., San Francisco, 1995), American Mathematical Society, 1995., str. 153–177.

P. J. Cameron, J. J. Seidel, *Quadratic forms over GF*(2), Nederl. Akad. Wetensch. Proc. Ser. A **76** Indag. Math. **35** (1973), 1–8.

$$\mathrm{Tr} : \mathbb{F}_{2^k} \to \mathbb{F}_2, \quad \mathrm{Tr}(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{k-1}}$$

$V = \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ nad poljem $\mathbb{F}_{2^k}$ (identificiramo ga s $\mathbb{F}_2^m$ za $m = 2k$)

Prvo uzmemo nedegeneriranu alternirajuću formu na V:

$$b((x_1, x_2), (y_1, y_2)) = x_1 y_2 + x_2 y_1$$

Konstrukcija Kerdockovih skupova

W. M. Kantor, *Codes, quadratic forms and finite geometries*, u: *Different aspects of coding theory* (Proc. Sympos. Appl. Math., San Francisco, 1995), American Mathematical Society, 1995., str. 153–177.

P. J. Cameron, J. J. Seidel, *Quadratic forms over GF(2)*, Nederl. Akad. Wetensch. Proc. Ser. A **76** Indag. Math. **35** (1973), 1–8.

$$\mathrm{Tr} : \mathbb{F}_{2^k} \to \mathbb{F}_2, \quad \mathrm{Tr}(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{k-1}}$$

$V = \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ nad poljem $\mathbb{F}_{2^k}$ (identificiramo ga s $\mathbb{F}_2^m$ za $m = 2k$)

Prvo uzmemo nedegeneriranu alternirajuću formu na V:

$$b((x_1, x_2), (y_1, y_2)) = x_1 y_2 + x_2 y_1$$

Zatim za $\alpha \in \mathbb{F}_{2^k}$ definiramo

$$B_\alpha : V \times V \to \mathbb{F}_2, \quad B_\alpha(x, y) = \mathrm{Tr}(\alpha\, b(x, y))$$

Konstrukcija Kerdockovih skupova

Propozicija.

Skup $\{B_\alpha \mid \alpha \in \mathbb{F}_{2^k}\}$ sadrži alternirajuće bilinearne forme na $\mathbb{F}_2^m$ takve da je $B_\alpha - B_\beta$ nedegenerirana za $\alpha \neq \beta$. Veličina tog skupa je $r = 2^k = 2^{m/2}$.

Konstrukcija Kerdockovih skupova

Propozicija.

Skup $\{B_\alpha \mid \alpha \in \mathbb{F}_{2^k}\}$ sadrži alternirajuće bilinearne forme na $\mathbb{F}_2^m$ takve da je $B_\alpha - B_\beta$ nedegenerirana za $\alpha \neq \beta$. Veličina tog skupa je $r = 2^k = 2^{m/2}$.

```
CameronSeidelSet:=function(m)
local k,Tr,b,B1,B2;
  k:=m/2;
  Tr:=x->Sum([1..k],i->x^(2^i));
  b:=function(x,y) return x[1]*y[2]+x[2]*y[1]; end;
  B1:=List([0..k-1],i->Z(2^k)^i);
  B2:=Concatenation(Cartesian(B1,[0*Z(2)]),
    Cartesian([0*Z(2)],B1));
  return List(Elements(GF(2^k)),
    a->List(B2,x->List(B2,y->Tr(a*b(x,y)))));
end;
```

Konstrukcija Kerdockovih skupova

Propozicija.

Skup $\{B_\alpha \mid \alpha \in \mathbb{F}_{2^k}\}$ sadrži alternirajuće bilinearne forme na $\mathbb{F}_2^m$ takve da je $B_\alpha - B_\beta$ nedegenerirana za $\alpha \neq \beta$. Veličina tog skupa je $r = 2^k = 2^{m/2}$.

```
gap> CameronSeidelSet(4);
```

Konstrukcija Kerdockovih skupova

Propozicija.

Skup $\{B_\alpha \mid \alpha \in \mathbb{F}_{2^k}\}$ sadrži alternirajuće bilinearne forme na $\mathbb{F}_2^m$ takve da je $B_\alpha - B_\beta$ nedegenerirana za $\alpha \neq \beta$. Veličina tog skupa je $r = 2^k = 2^{m/2}$.

```
gap> CameronSeidelSet(4);

[ [ [ 0*Z(2), 0*Z(2), 0*Z(2), 0*Z(2) ],
      [ 0*Z(2), 0*Z(2), 0*Z(2), 0*Z(2) ],
      [ 0*Z(2), 0*Z(2), 0*Z(2), 0*Z(2) ],
      [ 0*Z(2), 0*Z(2), 0*Z(2), 0*Z(2) ] ],

  [ [ 0*Z(2), 0*Z(2), 0*Z(2), Z(2)^0 ],
      [ 0*Z(2), 0*Z(2), Z(2)^0, Z(2)^0 ],
      [ 0*Z(2), Z(2)^0, 0*Z(2), 0*Z(2) ],
      [ Z(2)^0, Z(2)^0, 0*Z(2), 0*Z(2) ] ],
```

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

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

Konstrukcija Kerdockovih skupova

Propozicija.

Skup $\{B_\alpha \mid \alpha \in \mathbb{F}_{2^k}\}$ sadrži alternirajuće bilinearne forme na $\mathbb{F}_2^m$ takve da je $B_\alpha - B_\beta$ nedegenerirana za $\alpha \neq \beta$. Veličina tog skupa je $r = 2^k = 2^{m/2}$.

```
[ [ 0*Z(2), 0*Z(2), Z(2)^0, Z(2)^0 ],
    [ 0*Z(2), 0*Z(2), Z(2)^0, 0*Z(2) ],
    [ Z(2)^0, Z(2)^0, 0*Z(2), 0*Z(2) ],
    [ Z(2)^0, 0*Z(2), 0*Z(2), 0*Z(2) ] ],
```

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

```
[ [ 0*Z(2), 0*Z(2), Z(2)^0, 0*Z(2) ],
    [ 0*Z(2), 0*Z(2), 0*Z(2), Z(2)^0 ],
    [ Z(2)^0, 0*Z(2), 0*Z(2), 0*Z(2) ],
    [ 0*Z(2), Z(2)^0, 0*Z(2), 0*Z(2) ] ] ]
```

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

Konstrukcija Kerdockovih skupova

W. M. Kantor, *Codes, quadratic forms and finite geometries*, u: *Different aspects of coding theory* (Proc. Sympos. Appl. Math., San Francisco, 1995), American Mathematical Society, 1995., str. 153–177.

Na vektorskom prostoru $\mathbb{F}_{2^k}$ nad $\mathbb{F}_2$ imamo "skalarni produkt", tj. nedegeneriranu simetričnu bilinearnu formu $\langle x, y\rangle = \mathrm{Tr}(xy)$.

Konstrukcija Kerdockovih skupova

W. M. Kantor, *Codes, quadratic forms and finite geometries*, u: *Different aspects of coding theory* (Proc. Sympos. Appl. Math., San Francisco, 1995), American Mathematical Society, 1995., str. 153–177.

Na vektorskom prostoru $\mathbb{F}_{2^k}$ nad $\mathbb{F}_2$ imamo "skalarni produkt", tj. nedegeneriranu simetričnu bilinearnu formu $\langle x, y\rangle = \mathrm{Tr}(xy)$.

Identificiramo ga s vektorskim prostorom $\mathbb{F}_2^k$ s pomoću ortonormirane baze $\mathscr{B}_1$ obzirom na taj skalarni produkt.

Konstrukcija Kerdockovih skupova

W. M. Kantor, *Codes, quadratic forms and finite geometries*, u: *Different aspects of coding theory* (Proc. Sympos. Appl. Math., San Francisco, 1995), American Mathematical Society, 1995., str. 153–177.

Na vektorskom prostoru $\mathbb{F}_{2^k}$ nad $\mathbb{F}_2$ imamo "skalarni produkt", tj. nedegeneriranu simetričnu bilinearnu formu $\langle x, y\rangle = \operatorname{Tr}(xy)$.

Identificiramo ga s vektorskim prostorom $\mathbb{F}_2^k$ s pomoću ortonormirane baze $\mathscr{B}_1$ obzirom na taj skalarni produkt.

Uzmemo $k = m - 1$ i dodamo još jednu koordinatu:

$$V = \mathbb{F}_{2^k} \times \mathbb{F}_2 \quad \text{(direktni produkt vektorskih prostora)}$$

$$\langle (x_1, x_2), (y_1, y_2)\rangle = \operatorname{Tr}(x_1 y_1) + x_2 y_2$$

$$\mathscr{B}_2 = \{(x_1, 0) \mid x_1 \in \mathscr{B}_1\} \cup \{(0, 1)\}$$

Konstrukcija Kerdockovih skupova

Simplektičke matrice dobivamo kao matrice u bazi $\mathscr{B}_2$ linearnih operatora

$$M_\alpha : V \to V, \quad M_\alpha\,(x_1, x_2) = \Big(\alpha^2 x_1 + \alpha\,\mathrm{Tr}(\alpha x_1) + \alpha x_2,\ \mathrm{Tr}(\alpha x_1)\Big)$$

za $\alpha \in \mathbb{F}_{q^k}$. Broj tih matrica je $r = 2^k = 2^{m-1}$.

Konstrukcija Kerdockovih skupova

Simplektičke matrice dobivamo kao matrice u bazi $\mathscr{B}_2$ linearnih operatora

$$M_\alpha : V \to V, \quad M_\alpha(x_1, x_2) = \left(\alpha^2 x_1 + \alpha\,\mathrm{Tr}(\alpha x_1) + \alpha x_2,\ \mathrm{Tr}(\alpha x_1)\right)$$

za $\alpha \in \mathbb{F}_{q^k}$. Broj tih matrica je $r = 2^k = 2^{m-1}$.

Propozicija.

Matrice linearnih operatora $\{M_\alpha \mid \alpha \in \mathbb{F}_{2^k}\}$ u ortonormiranoj bazi $\mathscr{B}_2$ su simplektičke i razlike su im regularne, tj. tvore Kerdockov skup.

Konstrukcija Kerdockovih skupova

Simplektičke matrice dobivamo kao matrice u bazi $\mathscr{B}_2$ linearnih operatora

$$M_\alpha : V \to V, \quad M_\alpha(x_1, x_2) = \left(\alpha^2 x_1 + \alpha\,\mathrm{Tr}(\alpha x_1) + \alpha x_2,\ \mathrm{Tr}(\alpha x_1)\right)$$

za $\alpha \in \mathbb{F}_{q^k}$. Broj tih matrica je $r = 2^k = 2^{m-1}$.

Propozicija.

Matrice linearnih operatora $\{M_\alpha \mid \alpha \in \mathbb{F}_{2^k}\}$ u ortonormiranoj bazi $\mathscr{B}_2$ su simplektičke i razlike su im regularne, tj. tvore Kerdockov skup.

```
KerdockSet:=function(m)
local e,B1,B2,p,vec,Tr;
  e:=Elements(GF(2^(m-1)));
  B1:=OrthogonalNormalBasis(m-1);
  B2:=Concatenation(List(B1,x->[x,0*Z(2)]),[[0*Z(2),Z(2)^0]]);
  p:=Cartesian(List([1..m],x->[0,1]));
  vec:=List(p,x->x*B2);
  Tr:=x->Sum([1..m-1],i->x^(2^i));
  return Z(2)^0*List(e,a->List(B2,x->p[Position(vec,
    [a^2*x[1]+a*Tr(a*x[1])+a*x[2],Tr(a*x[1])])]));
end;
```

Konstrukcija Kerdockovih skupova

```
OrthogonalNormalBasis:=function(k)
local e,Tr,Gram,i,B;
  e:=Elements(GF(2^k));
  Tr:=x->Sum([1..k],i->x^(2^i));
  Gram:=v->List(v,x->List(v,y->IversonBracket(Tr(x*y)=Z(2)^0)));
  i:=0;
  repeat
    i:=i+1;
    B:=List([0..k-1],j->e[i]^(2^j));
  until Gram(B)=IdentityMat(k) or i=Size(e);
  if Gram(B)=IdentityMat(k) then
    return B;
  else
    return fail;
  fi;
end;
```

Konstrukcija Kerdockovih skupova

```
gap> KerdockSet(4);
```

Konstrukcija Kerdockovih skupova

```
gap> KerdockSet(4);

[ [ [ 0*Z(2), 0*Z(2), 0*Z(2), 0*Z(2) ],
      [ 0*Z(2), 0*Z(2), 0*Z(2), 0*Z(2) ],
      [ 0*Z(2), 0*Z(2), 0*Z(2), 0*Z(2) ],
      [ 0*Z(2), 0*Z(2), 0*Z(2), 0*Z(2) ] ],

  [ [ 0*Z(2), Z(2)^0, Z(2)^0, Z(2)^0 ],
      [ Z(2)^0, 0*Z(2), Z(2)^0, Z(2)^0 ],
      [ Z(2)^0, Z(2)^0, 0*Z(2), Z(2)^0 ],
      [ Z(2)^0, Z(2)^0, Z(2)^0, 0*Z(2) ] ],

  [ [ 0*Z(2), 0*Z(2), Z(2)^0, 0*Z(2) ],
      [ 0*Z(2), 0*Z(2), 0*Z(2), Z(2)^0 ],
      [ Z(2)^0, 0*Z(2), 0*Z(2), Z(2)^0 ],
      [ 0*Z(2), Z(2)^0, Z(2)^0, 0*Z(2) ] ],
```

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

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

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

Konstrukcija Kerdockovih skupova

```
[ [ 0*Z(2), Z(2)^0, 0*Z(2), Z(2)^0 ],
    [ Z(2)^0, 0*Z(2), 0*Z(2), 0*Z(2) ],
    [ 0*Z(2), 0*Z(2), 0*Z(2), Z(2)^0 ],
    [ Z(2)^0, 0*Z(2), Z(2)^0, 0*Z(2) ] ],
```

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

```
[ [ 0*Z(2), 0*Z(2), Z(2)^0, Z(2)^0 ],
    [ 0*Z(2), 0*Z(2), Z(2)^0, 0*Z(2) ],
    [ Z(2)^0, Z(2)^0, 0*Z(2), 0*Z(2) ],
    [ Z(2)^0, 0*Z(2), 0*Z(2), 0*Z(2) ] ],
```

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

```
[ [ 0*Z(2), 0*Z(2), 0*Z(2), Z(2)^0 ],
    [ 0*Z(2), 0*Z(2), Z(2)^0, Z(2)^0 ],
    [ 0*Z(2), Z(2)^0, 0*Z(2), 0*Z(2) ],
    [ Z(2)^0, Z(2)^0, 0*Z(2), 0*Z(2) ] ],
```

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

Konstrukcija Kerdockovih skupova

```
[ [ 0*Z(2), Z(2)^0, 0*Z(2), 0*Z(2) ],
    [ Z(2)^0, 0*Z(2), Z(2)^0, 0*Z(2) ],
    [ 0*Z(2), Z(2)^0, 0*Z(2), Z(2)^0 ],
    [ 0*Z(2), 0*Z(2), Z(2)^0, 0*Z(2) ] ],
```

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

```
[ [ 0*Z(2), Z(2)^0, Z(2)^0, 0*Z(2) ],
    [ Z(2)^0, 0*Z(2), 0*Z(2), Z(2)^0 ],
    [ Z(2)^0, 0*Z(2), 0*Z(2), 0*Z(2) ],
    [ 0*Z(2), Z(2)^0, 0*Z(2), 0*Z(2) ] ] ]
```

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