Asocijacijske sheme

Vedran Krčadinac

20.5.2024.

Dosadašnja predavanja (i majice!)

Asocijacijske sheme

Doktorski studij matematike, 2023./2024.

Predavanja

1. predavanje (06.11.2023.): Uvod i povijest. Video, prezentacija.
2. predavanje (13.11.2023.): Jako regularni i distancijsko regularni grafovi. Video, prezentacija.
3. predavanje (20.11.2023.): Konačne grupe i Schurova konstrukcija. Video 1, video 2, prezentacija.
4. predavanje (04.12.2023.): Koherentne konfiguracije i algebre. Video, prezentacija.
5. predavanje (11.12.2023.): Schurove idempotente. Video, prezentacija.
6. predavanje (18.12.2023.): Primitivne idempotente. Video, prezentacija.
7. predavanje (15.01.2024.): Presječni brojevi i Kreinovi parametri. Video, prezentacija.
8. predavanje (22.01.2024.): Svojstvene vrijednosti. Video, prezentacija.
9. predavanje (29.01.2024.): Kreinov uvjet. Video, prezentacija.
10. predavanje (12.02.2024.): Dopustivi parametri jako regularnih grafova. Video, prezentacija.
11. predavanje (19.02.2024.): Još neki uvjeti za jako regularne grafove. Video, prezentacija.
12. predavanje (26.02.2024.): Euklidska reprezentacija. Video, prezentacija.
13. predavanje (18.03.2024.): Imprimitivnost. Video, prezentacija, majica: Dugi otok trail 2024.
14. predavanje (25.03.2024.): Kvocijentna konfiguracija. Video, prezentacija.
15. predavanje (03.04.2024.): Spojeni sustavi simetričnih dizajna. Video, prezentacija, majica: Hendrix polumaraton 2024.
16. predavanje (22.04.2024.): Kombinatorni dizajni. Video, prezentacija.
17. predavanje (29.04.2024.): Cameron-Delsarteov teorem. Video, prezentacija.
18. predavanje (06.05.2024.): Kodovi za ispravljanje pogrešaka. Video, prezentacija, majica: Promina trail 2023.

Predavanja i seminari do ljetnih praznika

20.5.2024. Helena Marciuš: zadatak 4.32

Assmus-Mattsonov teorem ~~i neki nelinearni kodovi~~

Predavanja i seminari do ljetnih praznika

20.5.2024. Helena Marciuš: zadatak 4.32

Assmus-Mattsonov teorem ~~i neki nelinearni kodovi~~

27.-31.5.2024. Seminar u **utorak, 28.5.2024.**

Valentino Marković – Imprimitivni distancijsko regularni grafovi

Predavanja i seminari do ljetnih praznika

20.5.2024. Helena Marciuš: zadatak 4.32

Assmus-Mattsonov teorem ~~i neki nelinearni kodovi~~

27.-31.5.2024. Seminar u **utorak, 28.5.2024.**

Valentino Marković – Imprimitivni distancijsko regularni grafovi

Predavanje u četvrtak ili petak?

Predavanja i seminari do ljetnih praznika

20.5.2024. Helena Marciuš: zadatak 4.32
Assmus-Mattsonov teorem ~~i neki nelinearni kodovi~~

27.-31.5.2024. Seminar u **utorak, 28.5.2024.**
Valentino Marković – Imprimitivni distancijsko regularni grafovi
Predavanje u četvrtak ili petak?

03.-07.6.2024. Predavanje

Predavanja i seminari do ljetnih praznika

20.5.2024. Helena Marciuš: zadatak 4.32
Assmus-Mattsonov teorem ~~i neki nelinearni kodovi~~

27.-31.5.2024. Seminar u **utorak, 28.5.2024.**
Valentino Marković – Imprimitivni distancijsko regularni grafovi
Predavanje u četvrtak ili petak?

03.-07.6.2024. Predavanje

10.-14.6.2024. Nema predavanja (zbog konferencije u Beogradu)

Predavanja i seminari do ljetnih praznika

20.5.2024. Helena Marciuš: zadatak 4.32
Assmus-Mattsonov teorem ~~i neki nelinearni kodovi~~

27.-31.5.2024. Seminar u **utorak, 28.5.2024.**
Valentino Marković – Imprimitivni distancijsko regularni grafovi
Predavanje u četvrtak ili petak?

03.-07.6.2024. Predavanje

10.-14.6.2024. Nema predavanja (zbog konferencije u Beogradu)

17.-21.6.2024. Predavanje

24.-28.6.2024. Predavanje

01.-05.7.2024. Predavanje

08.-12.7.2024. Nema predavanja (zbog konferencije u Sevilli)

Kodovi za ispravljanje pogrešaka

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.

Kodovi za ispravljanje pogrešaka

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.
Ako je $F = \mathbb{F}_q$ konačno polje, a $C \leq \mathbb{F}_q^n$ potprostor dimenzije $m = \dim C$, kažemo da je C linearni kod i parametre zapisujemo $[n, m, d]_q$.

Kodovi za ispravljanje pogrešaka

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.
Ako je $F = \mathbb{F}_q$ konačno polje, a $C \leq \mathbb{F}_q^n$ potprostor dimenzije $m = \dim C$, kažemo da je C linearni kod i parametre zapisujemo $[n, m, d]_q$.

Propozicija (Singletonova ocjena)

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

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

Kodovi za ispravljanje pogrešaka

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.
Ako je $F = \mathbb{F}_q$ konačno polje, a $C \leq \mathbb{F}_q^n$ potprostor dimenzije $m = \dim C$, kažemo da je C linearni kod i parametre zapisujemo $[n, m, d]_q$.

Propozicija (Singletonova ocjena)

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

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

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

Kodovi za ispravljanje pogrešaka

E. F. Assmus, Jr., H. F. Mattson, Jr., *New* 5-*designs*, J. Combinatorial Theory **6** (1969), 122–151.

Propozicija.

Neka je C linearni kod s parametrima $[n, m, d]_q$. Kod C dostiže Singletonovu ocjenu $m = n - d + 1$ ako i samo ako nosači kodnih riječi minimalne težine čine potpuni d-$(n, d, 1)$ dizajn.

$$\operatorname{supp} x = \{i \in \{1, \ldots, n\} \mid x_i \neq 0\}$$

Kodovi za ispravljanje pogrešaka

E. F. Assmus, Jr., H. F. Mattson, Jr., *New* 5-*designs*, J. Combinatorial Theory **6** (1969), 122–151.

Propozicija.

Neka je C linearni kod s parametrima $[n, m, d]_q$. Kod C dostiže Singletonovu ocjenu $m = n - d + 1$ ako i samo ako nosači kodnih riječi minimalne težine čine potpuni d-$(n, d, 1)$ dizajn.

$$\operatorname{supp} x = \{i \in \{1, \ldots, n\} \mid x_i \neq 0\}$$

Kodovi koji dostižu Singletonovu ocjenu: MDS kodovi

Kodovi koji dostižu ocjenu pakiranja kugli: savršeni 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

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

Kodovi za ispravljanje pogrešaka

Propozicija (Ocjena pakiranja kugli)

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

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

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.

Kodovi i dizajni

Nosači riječi fiksne težine k (ne samo minimalne!) u savršenim kodovima i nekim drugim kodovima također čine dizajne.

Kodovi i dizajni

Nosači riječi fiksne težine k (ne samo minimalne!) u savršenim kodovima i nekim drugim kodovima također čine dizajne.

E. F. Assmus, Jr., H. F. Mattson, Jr., *New 5-designs*, J. Combinatorial Theory **6** (1969), 122–151.

Lema.

Neka je $C \leq \mathbb{F}^n$ kod s parametrima $[n, m, d]_q$ i neka je

$$k_{\max} = \begin{cases} n, & \text{ako je } q = 2 \\ \max\left\{k \in \mathbb{N} \mid k - \left\lceil \frac{k}{q-1} \right\rceil < d\right\}, & \text{ako je } q > 2 \end{cases}$$

Ako su $x, y \in C$ kodne riječi s istim nosačem $\operatorname{supp} x = \operatorname{supp} y$ i ako je $w(x) = w(y) \leq k_{\max}$, onda su x i y proporcionalni.

Kodovi i dizajni

Minimalnu težinu u dualnom kodu $C^\perp$ označimo $d^\perp$

Kodovi i dizajni

Minimalnu težinu u dualnom kodu $C^{\perp}$ označimo $d^{\perp}$

$$k^{\perp}_{\max} = \begin{cases} n, & \text{ako je } q = 2 \\ \max\left\{k \in \mathbb{N} \mid k - \left\lceil \frac{k}{q-1} \right\rceil < d^{\perp}\right\}, & \text{ako je } q > 2 \end{cases}$$

Kodovi i dizajni

Minimalnu težinu u dualnom kodu $C^\perp$ označimo $d^\perp$

$$k^\perp_{\max} = \begin{cases} n, & \text{ako je } q = 2 \\ \max\left\{k \in \mathbb{N} \mid k - \left\lceil \frac{k}{q-1} \right\rceil < d^\perp \right\}, & \text{ako je } q > 2 \end{cases}$$

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 $[n, n-m, d^\perp]_q$. Neka su B_i koeficijenti težinskog polinoma dualnog koda: $W_{C^\perp}(X, Y) = \sum_{i=0}^{d} B_i X^{n-i} Y^i$. Neka je $t < d$ takav da je najviše $d - t$ koeficijenata $B_1, \ldots, B_{n-t}$ različito od nule. Tada za svaki k koji zadovoljava $d \leq k \leq k_{\max}$ skup svih nosača vektora težine k u kodu C čini t-dizajn (ako postoje takvi vektori). Nadalje, za svaki k koji zadovoljava $d^\perp \leq k \leq \min\{n - t, k^\perp_{\max}\}$ skup svih nosača vektora težine k u dualnom kodu $C^\perp$ čini t-dizajn (ako postoje takvi vektori).

Kodovi i dizajni

Dokazi Assmus-Mattsonovog teorema:

E. F. Assmus, Jr., H. F. Mattson, Jr., *New* 5*-designs*, J. Combinatorial Theory **6** (1969), 122–151. **Teorem 4.2.**

P. J. Cameron, J. H. van Lint, *Designs, graphs, codes and their links*, Cambridge University Press, Cambridge, 1991. **Teorem 14.11.**

Za $q = 2$:

J. H. van Lint, R. M. Wilson, *A course in combinatorics. Second edition*, Cambridge University Press, 2001. **Teorem 20.4.**

E. Bannai, E. Bannai, T. Ito, R. Tanaka, *Algebraic combinatorics*, De Gruyter, 2021. **Teorem 4.1.**

Kodovi i dizajni

Primjene Assmus-Mattsonovog teorema:

```
gap> H7:=HammingCode(3,2);
a linear [7,4,3]1 Hamming (3,2) code over GF(2)
gap> AddWeights:=l->Filtered(List([1..Size(l)],i->
>   [i-1,l[i]]), x->x[2]>0);
function( l ) ... end
gap> AddWeights(WeightDistribution(H7));
[ [ 0, 1 ], [ 3, 7 ], [ 4, 7 ], [ 7, 1 ] ]
gap> AddWeights(WeightDistribution(DualCode(H7)));
[ [ 0, 1 ], [ 4, 7 ] ]
```

Kodovi i dizajni

Primjene Assmus-Mattsonovog teorema:

```
gap> G11:=TernaryGolayCode();
a cyclic [11,6,5]2 ternary Golay code over GF(3)
gap> AddWeights(WeightDistribution(G11));
[ [ 0, 1 ], [ 5, 132 ], [ 6, 132 ], [ 8, 330 ], [ 9, 110 ],
  [ 11, 24 ] ]
gap> AddWeights(WeightDistribution(DualCode(G11)));
[ [ 0, 1 ], [ 6, 132 ], [ 9, 110 ] ]
```

Kodovi i dizajni

Primjene Assmus-Mattsonovog teorema:

```
gap> G12:=ExtendedTernaryGolayCode();
a linear [12,6,6]3 extended ternary Golay code over GF(3)
gap> AddWeights(WeightDistribution(G12));
[ [ 0, 1 ], [ 6, 264 ], [ 9, 440 ], [ 12, 24 ] ]
gap> AddWeights(WeightDistribution(DualCode(G12)));
[ [ 0, 1 ], [ 6, 264 ], [ 9, 440 ], [ 12, 24 ] ]
gap> G12=DualCode(G12);
true
```

Kodovi i dizajni

Primjene Assmus-Mattsonovog teorema:

```
gap> G23:=BinaryGolayCode();
a cyclic [23,12,7]3 binary Golay code over GF(2)
gap> AddWeights(WeightDistribution(G23));
[ [ 0, 1 ], [ 7, 253 ], [ 8, 506 ], [ 11, 1288 ],
  [ 12, 1288 ], [ 15, 506 ], [ 16, 253 ], [ 23, 1 ] ]
gap> AddWeights(WeightDistribution(DualCode(G23)));
[ [ 0, 1 ], [ 8, 506 ], [ 12, 1288 ], [ 16, 253 ] ]
```

Kodovi i dizajni

Primjene Assmus-Mattsonovog teorema:

```
gap> G24:=ExtendedBinaryGolayCode();
a linear [24,12,8]4 extended binary Golay code over GF(2)
gap> AddWeights(WeightDistribution(G24));
[ [ 0, 1 ], [ 8, 759 ], [ 12, 2576 ], [ 16, 759 ],
  [ 24, 1 ] ]
gap> AddWeights(WeightDistribution(DualCode(G24)));
[ [ 0, 1 ], [ 8, 759 ], [ 12, 2576 ], [ 16, 759 ],
  [ 24, 1 ] ]
gap> G24=DualCode(G24);
true
```

Ciklički kodovi

Za kod $C \leq \mathbb{F}_q^n$ kažemo da je ciklički ako je invarijantan na cikličku rotaciju koordinata, tj. ako vrijedi

$$(a_0, a_1, \ldots, a_{n-1}) \in C \quad \Rightarrow \quad (a_{n-1}, a_0, \ldots, a_{n-2}) \in C$$

Općenitije, cikličkim smatramo sve kodove ekvivalentne takvim kodovima, a to znači da imaju grupu automorfizama izomorfnu sa $\mathbb{Z}_n$.

Ciklički kodovi

Za kod $C \leq \mathbb{F}_q^n$ kažemo da je ciklički ako je invarijantan na cikličku rotaciju koordinata, tj. ako vrijedi

$$(a_0, a_1, \ldots, a_{n-1}) \in C \quad \Rightarrow \quad (a_{n-1}, a_0, \ldots, a_{n-2}) \in C$$

Općenitije, cikličkim smatramo sve kodove ekvivalentne takvim kodovima, a to znači da imaju grupu automorfizama izomorfnu sa $\mathbb{Z}_n$.

Zadatak.

Pokažite da su Hammingovi kodovi $\mathrm{Ham}(r, q)$ ciklički, a Reed-Solomonovi kodovi su proširenja cikličkih kodova.

Ciklički kodovi

Za kod $C \leq \mathbb{F}_q^n$ kažemo da je ciklički ako je invarijantan na cikličku rotaciju koordinata, tj. ako vrijedi

$$(a_0, a_1, \ldots, a_{n-1}) \in C \;\Rightarrow\; (a_{n-1}, a_0, \ldots, a_{n-2}) \in C$$

Općenitije, cikličkim smatramo sve kodove ekvivalentne takvim kodovima, a to znači da imaju grupu automorfizama izomorfnu sa $\mathbb{Z}_n$.

Zadatak.

Pokažite da su Hammingovi kodovi $\mathrm{Ham}(r, q)$ ciklički, a Reed-Solomonovi kodovi su proširenja cikličkih kodova.

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

Ciklički kodovi

Za kod $C \leq \mathbb{F}_q^n$ kažemo da je ciklički ako je invarijantan na cikličku rotaciju koordinata, tj. ako vrijedi

$$(a_0, a_1, \ldots, a_{n-1}) \in C \;\Rightarrow\; (a_{n-1}, a_0, \ldots, a_{n-2}) \in C$$

Općenitije, cikličkim smatramo sve kodove ekvivalentne takvim kodovima, a to znači da imaju grupu automorfizama izomorfnu sa $\mathbb{Z}_n$.

Zadatak.

Pokažite da su Hammingovi kodovi $\mathrm{Ham}(r, q)$ ciklički, a Reed-Solomonovi kodovi su proširenja cikličkih kodova.

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

Ciklički kodovi

Za kod $C \leq \mathbb{F}_q^n$ kažemo da je ciklički ako je invarijantan na cikličku rotaciju koordinata, tj. ako vrijedi

$$(a_0, a_1, \ldots, a_{n-1}) \in C \;\Rightarrow\; (a_{n-1}, a_0, \ldots, a_{n-2}) \in C$$

Općenitije, cikličkim smatramo sve kodove ekvivalentne takvim kodovima, a to znači da imaju grupu automorfizama izomorfnu sa $\mathbb{Z}_n$.

Zadatak.

Pokažite da su Hammingovi kodovi $\mathrm{Ham}(r, q)$ ciklički, a Reed-Solomonovi kodovi su proširenja cikličkih kodova.

$$P' = \begin{bmatrix} 1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{q-1} \\ 1 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_{q-1}^2 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_2^{r-1} & \alpha_3^{r-1} & \cdots & \alpha_{q-1}^{r-1} \end{bmatrix} \qquad \alpha_i = \xi^{i-1}$$

Ciklički kodovi

Za kod $C \leq \mathbb{F}_q^n$ kažemo da je ciklički ako je invarijantan na cikličku rotaciju koordinata, tj. ako vrijedi

$$(a_0, a_1, \ldots, a_{n-1}) \in C \;\Rightarrow\; (a_{n-1}, a_0, \ldots, a_{n-2}) \in C$$

Općenitije, cikličkim smatramo sve kodove ekvivalentne takvim kodovima, a to znači da imaju grupu automorfizama izomorfnu sa $\mathbb{Z}_n$.

Zadatak.

Pokažite da su Hammingovi kodovi $\mathrm{Ham}(r, q)$ ciklički, a Reed-Solomonovi kodovi su proširenja cikličkih kodova.

$$P' = \begin{bmatrix} 1 & \xi & \xi^2 & \ldots & \xi^{q-2} \\ 1 & \xi^2 & \xi^4 & \ldots & \xi^{2(q-2)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \xi^{r-1} & \xi^{2(r-1)} & \ldots & \xi^{(r-1)(q-2)} \end{bmatrix}$$

Ciklički kodovi

Za kod $C \leq \mathbb{F}_q^n$ kažemo da je ciklički ako je invarijantan na cikličku rotaciju koordinata, tj. ako vrijedi

$$(a_0, a_1, \ldots, a_{n-1}) \in C \quad \Rightarrow \quad (a_{n-1}, a_0, \ldots, a_{n-2}) \in C$$

Općenitije, cikličkim smatramo sve kodove ekvivalentne takvim kodovima, a to znači da imaju grupu automorfizama izomorfnu sa $\mathbb{Z}_n$.

Zadatak.

Pokažite da su Hammingovi kodovi $\mathrm{Ham}(r, q)$ ciklički, a Reed-Solomonovi kodovi su proširenja cikličkih kodova.

$$\mathbb{F}_q^r \quad \equiv \quad \mathbb{F}_{q^r}$$

Ciklički kodovi

Za kod $C \leq \mathbb{F}_q^n$ kažemo da je ciklički ako je invarijantan na cikličku rotaciju koordinata, tj. ako vrijedi

$$(a_0, a_1, \ldots, a_{n-1}) \in C \quad \Rightarrow \quad (a_{n-1}, a_0, \ldots, a_{n-2}) \in C$$

Općenitije, cikličkim smatramo sve kodove ekvivalentne takvim kodovima, a to znači da imaju grupu automorfizama izomorfnu sa $\mathbb{Z}_n$.

Zadatak.

Pokažite da su Hammingovi kodovi $\mathrm{Ham}(r, q)$ ciklički, a Reed-Solomonovi kodovi su proširenja cikličkih kodova.

$$\mathbb{F}_q^r \quad \equiv \quad \mathbb{F}_{q^r}$$

Množenje s primitivnim elementom polja $\mathbb{F}_{q^r} \rightsquigarrow$ Singerov ciklus projektivnog prostora $PG(r-1, q)$

Ciklički kodovi

$$\mathbb{F}_q^n \quad \equiv \quad \mathbb{F}_q[X]/(X^n - 1)$$

Ciklički kodovi

$$\mathbb{F}_q^n \equiv \mathbb{F}_q[X]/(X^n - 1)$$

$$(a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1 X + \ldots + a_{n-1} X^{n-1} + (X^n - 1)$$

Ciklički kodovi

$$\mathbb{F}_q^n \equiv \mathbb{F}_q[X]/(X^n - 1)$$

$$(a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1 X + \ldots + a_{n-1} X^{n-1} + (X^n - 1)$$

Kod C je ciklički akko je invarijantan na množenje s varijablom X:

$$a_0 X + a_1 X^2 + \ldots + a_{n-1} X^n \equiv a_{n-1} + a_0 X + \ldots + a_{n-2} X^{n-1} \mod (X^n - 1)$$

Ciklički kodovi

$$\mathbb{F}_q^n \equiv \mathbb{F}_q[X]/(X^n-1)$$

$$(a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1X + \ldots + a_{n-1}X^{n-1} + (X^n-1)$$

Kod C je ciklički akko je invarijantan na množenje s varijablom X:

$$a_0X + a_1X^2 + \ldots + a_{n-1}X^n \equiv a_{n-1} + a_0X + \ldots + a_{n-2}X^{n-1} \mod (X^n-1)$$

Dakle, C nije samo potprostor, nego je **ideal** prstena $\mathbb{F}_q[X]/(X^n-1)$

Ciklički kodovi

$$\mathbb{F}_q^n \equiv \mathbb{F}_q[X]/(X^n-1)$$

$$(a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1X + \ldots + a_{n-1}X^{n-1} + (X^n-1)$$

Kod C je ciklički akko je invarijantan na množenje s varijablom X:

$$a_0X + a_1X^2 + \ldots + a_{n-1}X^n \equiv a_{n-1} + a_0X + \ldots + a_{n-2}X^{n-1} \mod (X^n-1)$$

Dakle, C nije samo potprostor, nego je **ideal** prstena $\mathbb{F}_q[X]/(X^n-1)$

$\mathbb{F}_q[X]/(X^n-1)$ je prsten glavnih ideala, pa postoji jedinstveni normirani polinom $g(X)$ koji dijeli X^n-1 takav da je $C = (g(X)) \rightsquigarrow$ generirajući polinom ili generator cikličkog koda C

Ciklički kodovi

$$\mathbb{F}_q^n \equiv \mathbb{F}_q[X]/(X^n-1)$$

$$(a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1X + \ldots + a_{n-1}X^{n-1} + (X^n-1)$$

Kod C je ciklički akko je invarijantan na množenje s varijablom X:

$$a_0X + a_1X^2 + \ldots + a_{n-1}X^n \equiv a_{n-1} + a_0X + \ldots + a_{n-2}X^{n-1} \mod (X^n-1)$$

Dakle, C nije samo potprostor, nego je **ideal** prstena $\mathbb{F}_q[X]/(X^n-1)$

$\mathbb{F}_q[X]/(X^n-1)$ je prsten glavnih ideala, pa postoji jedinstveni normirani polinom $g(X)$ koji dijeli X^n-1 takav da je $C = (g(X)) \rightsquigarrow$ generirajući polinom ili generator cikličkog koda C

Ako je $\dim C = m$, onda je $\{g(X), Xg(X), \ldots, X^{m-1}g(X)\}$ baza od C, a stupanj od $g(X)$ je $n-m$.

Ciklički kodovi

$$g(X) = g_0 + g_1 X + \ldots + g_{n-m-1} X^{n-m-1} + X^{n-m}$$

Ciklički kodovi

$$g(X) = g_0 + g_1 X + \ldots + g_{n-m-1} X^{n-m-1} + X^{n-m}$$

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-m-1} & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-m-1} & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & & \ddots & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & g_0 & g_1 & \cdots & g_{n-m-1} & 1 \end{bmatrix}$$

Ciklički kodovi

$$g(X) = g_0 + g_1 X + \ldots + g_{n-m-1} X^{n-m-1} + X^{n-m}$$

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-m-1} & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-m-1} & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & & \ddots & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & g_0 & g_1 & \cdots & g_{n-m-1} & 1 \end{bmatrix}$$

$$g(X)h(X) = X^n - 1, \quad h(X) = h_0 + h_1 X + \ldots + h_{m-1} X^{m-1} + X^m$$

Ciklički kodovi

$$g(X) = g_0 + g_1 X + \ldots + g_{n-m-1} X^{n-m-1} + X^{n-m}$$

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-m-1} & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-m-1} & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & & \ddots & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & g_0 & g_1 & \cdots & g_{n-m-1} & 1 \end{bmatrix}$$

$$g(X)h(X) = X^n - 1, \quad h(X) = h_0 + h_1 X + \ldots + h_{m-1} X^{m-1} + X^m$$

$h(X)$ je polinom provjere parnosti (check polynomial) cikličkog koda C:

$$p(X) + (X^n - 1) \in C \iff p(X)h(X) \equiv 0 \mod (X^n - 1)$$

Ciklički kodovi

$$g(X) = g_0 + g_1 X + \ldots + g_{n-m-1} X^{n-m-1} + X^{n-m}$$

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-m-1} & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-m-1} & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & & \ddots & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & g_0 & g_1 & \cdots & g_{n-m-1} & 1 \end{bmatrix}$$

$$H = \begin{bmatrix} 1 & h_{m-1} & \cdots & h_1 & h_0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & h_{m-1} & \cdots & h_1 & h_0 & 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & & \ddots & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & h_{m-1} & \cdots & h_1 & h_0 \end{bmatrix}$$

Kodovi kvadratnih ostataka

Cikličke kodove zadajemo s polinomom $g(X)$ ili $h(X)$:

$$g(X)h(X) = X^n - 1 = (X-1)(X^{n-1} + \ldots + X + 1)$$

Kodovi kvadratnih ostataka

Cikličke kodove zadajemo s polinomom $g(X)$ ili $h(X)$:

$$g(X)h(X) = X^n - 1 = (X-1)(X^{n-1} + \ldots + X + 1)$$

Pretpostavimo da je duljina koda n neparan prost broj, a veličina alfabeta q kvadratni ostatak modulo n. To znači da q pripada skupu

$$R_0 = \{i^2 \mid i \in \mathbb{F}_n, i \neq 0\}$$

Kodovi kvadratnih ostataka

Cikličke kodove zadajemo s polinomom $g(X)$ ili $h(X)$:

$$g(X)h(X) = X^n - 1 = (X-1)(X^{n-1} + \ldots + X + 1)$$

Pretpostavimo da je duljina koda n neparan prost broj, a veličina alfabeta q kvadratni ostatak modulo n. To znači da q pripada skupu

$$R_0 = \{i^2 \mid i \in \mathbb{F}_n, i \neq 0\} \qquad R_1 = \mathbb{F}_n^* \setminus R_0$$

Kodovi kvadratnih ostataka

Cikličke kodove zadajemo s polinomom $g(X)$ ili $h(X)$:

$$g(X)h(X) = X^n - 1 = (X-1)(X^{n-1} + \ldots + X + 1)$$

Pretpostavimo da je duljina koda n neparan prost broj, a veličina alfabeta q kvadratni ostatak modulo n. To znači da q pripada skupu

$$R_0 = \{i^2 \mid i \in \mathbb{F}_n, i \neq 0\} \qquad R_1 = \mathbb{F}_n^* \setminus R_0$$

Zadatak.

Dokažite da je broj $i \in \{1, \ldots, n-1\} = \mathbb{F}_n^*$ kvadratni ostatak modulo n ako i samo ako vrijedi $i^{(n-1)/2} \equiv 1 \pmod{n}$. Za $i = 2$, pokažite da je uvjet ekvivalentan s $n \equiv \pm 1 \pmod{8}$.

Kodovi kvadratnih ostataka

Cikličke kodove zadajemo s polinomom $g(X)$ ili $h(X)$:

$$g(X)h(X) = X^n - 1 = (X-1)(X^{n-1} + \ldots + X + 1)$$

Pretpostavimo da je duljina koda n neparan prost broj, a veličina alfabeta q kvadratni ostatak modulo n. To znači da q pripada skupu

$$R_0 = \{i^2 \mid i \in \mathbb{F}_n, i \neq 0\} \qquad R_1 = \mathbb{F}_n^* \setminus R_0$$

Zadatak.

Dokažite da je broj $i \in \{1, \ldots, n-1\} = \mathbb{F}_n^*$ kvadratni ostatak modulo n ako i samo ako vrijedi $i^{(n-1)/2} \equiv 1 \pmod{n}$. Za $i = 2$, pokažite da je uvjet ekvivalentan s $n \equiv \pm 1 \pmod{8}$.

Neka je α primitivni n-ti korijen jedinice u nekom proširenju $\mathbb{F}_{q^k}$ osnovnog polja $\mathbb{F}_q$: $\alpha^n = 1$, $\alpha^i \neq 1$ za $i = 1, \ldots, n-1$.

Kodovi kvadratnih ostataka

U prstenu polinoma $\mathbb{F}_{q^k}[X]$ istaknimo sljedeća dva polinoma:

$$g_0(X) = \prod_{i \in R_0} (X - \alpha^i), \qquad g_1(X) = \prod_{i \in R_1} (X - \alpha^i)$$

Kodovi kvadratnih ostataka

U prstenu polinoma $\mathbb{F}_{q^k}[X]$ istaknimo sljedeća dva polinoma:

$$g_0(X) = \prod_{i \in R_0} (X - \alpha^i), \qquad g_1(X) = \prod_{i \in R_1} (X - \alpha^i)$$

Zadatak.

Dokažite da je $X^n - 1 = (X-1)g_0(X)g_1(X)$. Nadalje, dokažite da koeficijenti polinoma $g_0(X)$ i $g_1(X)$ pripadaju osnovnom polju $\mathbb{F}_q$.

Kodovi kvadratnih ostataka

U prstenu polinoma $\mathbb{F}_{q^k}[X]$ istaknimo sljedeća dva polinoma:

$$g_0(X) = \prod_{i \in R_0} (X - \alpha^i), \qquad g_1(X) = \prod_{i \in R_1} (X - \alpha^i)$$

Zadatak.

Dokažite da je $X^n - 1 = (X-1)g_0(X)g_1(X)$. Nadalje, dokažite da koeficijenti polinoma $g_0(X)$ i $g_1(X)$ pripadaju osnovnom polju $\mathbb{F}_q$.

J. H. van Lint, *Introduction to coding theory. Third edition*, Springer-Verlag, Berlin, 1999. **Teorem 1.1.22.**

Kodovi kvadratnih ostataka

U prstenu polinoma $\mathbb{F}_{q^k}[X]$ istaknimo sljedeća dva polinoma:

$$g_0(X) = \prod_{i \in R_0} (X - \alpha^i), \qquad g_1(X) = \prod_{i \in R_1} (X - \alpha^i)$$

Zadatak.

Dokažite da je $X^n - 1 = (X-1)g_0(X)g_1(X)$. Nadalje, dokažite da koeficijenti polinoma $g_0(X)$ i $g_1(X)$ pripadaju osnovnom polju $\mathbb{F}_q$.

J. H. van Lint, *Introduction to coding theory. Third edition*, Springer-Verlag, Berlin, 1999. **Teorem 1.1.22.**

Kod kvadratnih ostataka $QR(n, q)$ je ciklički kod nad poljem $\mathbb{F}_q$ s generirajućim polinomom $g_0(X)$. Dimenzija mu je $m = (n+1)/2$, a polinom provjere parnosti je $(X-1)g_1(X)$.

Kodovi kvadratnih ostataka

U prstenu polinoma $\mathbb{F}_{q^k}[X]$ istaknimo sljedeća dva polinoma:

$$g_0(X) = \prod_{i \in R_0} (X - \alpha^i), \qquad g_1(X) = \prod_{i \in R_1} (X - \alpha^i)$$

Zadatak.

Dokažite da je $X^n - 1 = (X-1)g_0(X)g_1(X)$. Nadalje, dokažite da koeficijenti polinoma $g_0(X)$ i $g_1(X)$ pripadaju osnovnom polju $\mathbb{F}_q$.

J. H. van Lint, *Introduction to coding theory. Third edition*, Springer-Verlag, Berlin, 1999. **Teorem 1.1.22.**

Kod kvadratnih ostataka $QR(n, q)$ je ciklički kod nad poljem $\mathbb{F}_q$ s generirajućim polinomom $g_0(X)$. Dimenzija mu je $m = (n+1)/2$, a polinom provjere parnosti je $(X-1)g_1(X)$.

Minimalna težina?

Kodovi kvadratnih ostataka

Teorem.

Neka je d minimalna težina koda $QR(n, q)$. Tada vrijedi $d^2 \geq n$, a u slučaju $n \equiv 3 \pmod 4$ vrijedi bolja ocjena $d^2 - d + 1 \geq n$.

F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland Publishing Co., 1977. **Teorem 16.2.1.**

Mali primjeri QR kodova

$QR(7,2) \rightsquigarrow [7,4,d]_2$

Mali primjeri QR kodova

$QR(7,2) \rightsquigarrow [7,4,d]_2$

Teorem $\Rightarrow d \geq 3$

Ocjena pakiranja kugli $\Rightarrow d \leq 3$

Mali primjeri QR kodova

$QR(7,2) \rightsquigarrow [7,4,d]_2$

Teorem $\Rightarrow d \geq 3$

Ocjena pakiranja kugli $\Rightarrow d \leq 3$

Dakle, $QR(7,2)$ je savršeni $[7,4,3]_2$ kod ekvivalentan s $\mathrm{Ham}(3,2)$

Kodovi kvadratnih ostataka

Mali primjeri QR kodova

$QR(7,2) \rightsquigarrow [7,4,d]_2$

Teorem $\Rightarrow d \geq 3$

Ocjena pakiranja kugli $\Rightarrow d \leq 3$

Dakle, $QR(7,2)$ je savršeni $[7,4,3]_2$ kod ekvivalentan s $\mathrm{Ham}(3,2)$

```
gap> C:=QRCode(7,GF(2));
a cyclic [7,4,3]1 quadratic residue code over GF(2)
gap> IsEquivalent(C,H7);
true
```

Mali primjeri QR kodova

$QR(11,3) \rightsquigarrow [11,6,d]_3$

Mali primjeri QR kodova

$QR(11,3) \rightsquigarrow [11,6,d]_3$

Teorem $\Rightarrow d \geq 4$

Ocjena pakiranja kugli $\Rightarrow d \leq 5$

Kodovi kvadratnih ostataka

Mali primjeri QR kodova

$QR(11,3) \rightsquigarrow [11,6,d]_3$

Teorem $\Rightarrow d \geq 4$

Ocjena pakiranja kugli $\Rightarrow d \leq 5$

```
gap> C:=QRCode(11,GF(3));
a cyclic [11,6,4..5]2 quadratic residue code over GF(3)
gap> MinimumWeight(C);
5
gap> IsEquivalent(C,G11);
true
```

Mali primjeri QR kodova

$QR(23, 2) \rightsquigarrow [23, 12, d]_2$

Mali primjeri QR kodova

$QR(23, 2) \rightsquigarrow [23, 12, d]_2$

Teorem $\Rightarrow d \geq 6$

Ocjena pakiranja kugli $\Rightarrow d \leq 7$

Kodovi kvadratnih ostataka

Mali primjeri QR kodova

$QR(23, 2) \rightsquigarrow [23, 12, d]_2$

Teorem $\Rightarrow d \geq 6$

Ocjena pakiranja kugli $\Rightarrow d \leq 7$

```
gap> C:=QRCode(23,GF(2));
a cyclic [23,12,7]3 quadratic residue code over GF(2)
gap> MinimumWeight(C);
7
gap> IsEquivalent(C,G23);
true
```

Kodovi kvadratnih ostataka i shematski 4-dizajni

Br.	v	k	λ	x	y	z	$\exists$
1	11	5	1	1	2	3	✓
2	23	8	4	0	2	4	✓
3	23	11	48	3	5	7	✓
4	24	8	5	0	2	4	✓
5	47	11	8	1	3	5	✓
6	71	35	264	14	17	20	?
7	199	99	2328	44	49	54	?
8	391	195	9264	90	97	104	?
9	647	323	25680	152	161	170	?
10	659	329	390874	153	164	175	?
11	967	483	57720	230	241	252	?

$QR(11,3) \equiv G_{11}$

$QR(23,2) \equiv G_{23}$

$QR(23,2) \equiv G_{23}$

$\widehat{QR}(23,2) \equiv G_{24}$

Kodovi kvadratnih ostataka i shematski 4-dizajni

Br.	v	k	λ	x	y	z	$\exists$
1	11	5	1	1	2	3	✓
2	23	8	4	0	2	4	✓
3	23	11	48	3	5	7	✓
4	24	8	5	0	2	4	✓
5	47	11	8	1	3	5	✓
6	71	35	264	14	17	20	?
7	199	99	2328	44	49	54	?
8	391	195	9264	90	97	104	?
9	647	323	25680	152	161	170	?
10	659	329	390874	153	164	175	?
11	967	483	57720	230	241	252	?

$QR(11,3) \equiv G_{11}$

$QR(23,2) \equiv G_{23}$

$QR(23,2) \equiv G_{23}$

$\widehat{QR}(23,2) \equiv G_{24}$

$QR(47,2)$?

Malo veći primjer QR koda

```
gap> C:=QRCode(47,GF(2));
```

Malo veći primjer QR koda

```
gap> C:=QRCode(47,GF(2));
Error, GUAVA cannot compute in a finite field of size larger
 than 2^16 at /opt/gap-4.11.1/pkg/guava-3.19/lib/util.gi:171
 called from PrimitiveUnityRoot( q, n ) at
 /opt/gap-4.11.1/pkg/guava-3.19/lib/codegen.gi:1973 called
 from QRCode( n, Size( F ) ) at
 /opt/gap-4.11.1/pkg/guava-3.19/lib/codegen.gi:2013 called
 from <function "QRCode modulus, field">( <arguments> )
 called from read-eval loop at *stdin*:2
you can 'quit;' to quit to outer loop, or
you can 'return;' to continue
brk>
```

Malo veći primjer QR koda

W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.

Malo veći primjer QR koda

W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.

```
> C:=QRCode(GF(2),47);
> WeightDistribution(C);
[ <0, 1>, <11, 4324>, <12, 12972>, <15, 178365>, <16,
356730>, <19, 1664740>, <20, 2330636>, <23, 3840840>,
<24, 3840840>, <27, 2330636>, <28, 1664740>, <31,
356730>, <32, 178365>, <35, 12972>, <36, 4324>, <47, 1> ]
> WeightDistribution(Dual(C));
[ <0, 1>, <12, 12972>, <16, 356730>, <20, 2330636>, <24,
3840840>, <28, 1664740>, <32, 178365>, <36, 4324> ]
> IsPerfect(C);
false
```

Kodovi kvadratnih ostataka i shematski 4-dizajni

Br.	v	k	λ	x	y	z	$\exists$
1	11	5	1	1	2	3	✓
2	23	8	4	0	2	4	✓
3	23	11	48	3	5	7	✓
4	24	8	5	0	2	4	✓
5	47	11	8	1	3	5	✓
6	71	35	264	14	17	20	?
7	199	99	2328	44	49	54	?
8	391	195	9264	90	97	104	?
9	647	323	25680	152	161	170	?
10	659	329	390874	153	164	175	?
11	967	483	57720	230	241	252	?

$QR(11,3) \equiv G_{11}$

$QR(23,2) \equiv G_{23}$

$QR(23,2) \equiv G_{23}$

$\widehat{QR}(23,2) \equiv G_{24}$

$QR(47,2)$

Kodovi kvadratnih ostataka i shematski 4-dizajni

Br.	v	k	λ	x	y	z	$\exists$	
1	11	5	1	1	2	3	✓	$QR(11,3) \equiv G_{11}$
2	23	8	4	0	2	4	✓	$QR(23,2) \equiv G_{23}$
3	23	11	48	3	5	7	✓	$QR(23,2) \equiv G_{23}$
4	24	8	5	0	2	4	✓	$\widehat{QR}(23,2) \equiv G_{24}$
5	47	11	8	1	3	5	✓	$QR(47,2)$
6	71	35	264	14	17	20	?	$QR(71,2)$?
7	199	99	2328	44	49	54	?	
8	391	195	9264	90	97	104	?	
9	647	323	25680	152	161	170	?	
10	659	329	390874	153	164	175	?	
11	967	483	57720	230	241	252	?	

Još veći primjer QR koda

```
> C:=QRCode(GF(2),71);
> WeightDistribution(C);
[ <0, 1>, <11, 497>, <12, 2485>, <15, 47570>, <16, 166495>,
<19, 5084310>, <20, 13219206>, <23, 154102305>, <24,
308204610>, <27, 1710651635>, <28, 2688166855>, <31,
7377935180>, <32, 9222418975>, <35, 12879738244>, <36,
12879738244>, <39, 9222418975>, <40, 7377935180>, <43,
2688166855>, <44, 1710651635>, <47, 308204610>, <48,
154102305>, <51, 13219206>, <52, 5084310>, <55, 166495>,
<56, 47570>, <59, 2485>, <60, 497>, <71, 1> ]
> WeightDistribution(Dual(C));
[ <0, 1>, <12, 2485>, <16, 166495>, <20, 13219206>, <24,
308204610>, <28, 2688166855>, <32, 9222418975>, <36,
12879738244>, <40, 7377935180>, <44, 1710651635>,
<48, 154102305>, <52, 5084310>, <56, 47570>, <60, 497> ]
```

Kodovi kvadratnih ostataka i shematski 4-dizajni

Br.	v	k	λ	x	y	z	$\exists$
1	11	5	1	1	2	3	✓
2	23	8	4	0	2	4	✓
3	23	11	48	3	5	7	✓
4	24	8	5	0	2	4	✓
5	47	11	8	1	3	5	✓
6	71	35	264	14	17	20	?
7	199	99	2328	44	49	54	?
8	391	195	9264	90	97	104	?
9	647	323	25680	152	161	170	?
10	659	329	390874	153	164	175	?
11	967	483	57720	230	241	252	?

$QR(11,3) \equiv G_{11}$

$QR(23,2) \equiv G_{23}$

$QR(23,2) \equiv G_{23}$

$\widehat{QR}(23,2) \equiv G_{24}$

$QR(47,2)$

~~$QR(71,2)$~~

Kodovi kvadratnih ostataka i shematski 4-dizajni

Br.	v	k	λ	x	y	z	$\exists$	
1	11	5	1	1	2	3	✓	$QR(11,3) \equiv G_{11}$
2	23	8	4	0	2	4	✓	$QR(23,2) \equiv G_{23}$
3	23	11	48	3	5	7	✓	$QR(23,2) \equiv G_{23}$
4	24	8	5	0	2	4	✓	$\widehat{QR}(23,2) \equiv G_{24}$
5	47	11	8	1	3	5	✓	$QR(47,2)$
6	71	35	264	14	17	20	?	$QR(71,3)$?
7	199	99	2328	44	49	54	?	
8	391	195	9264	90	97	104	?	
9	647	323	25680	152	161	170	?	
10	659	329	390874	153	164	175	?	
11	967	483	57720	230	241	252	?	

Još veći primjer QR koda

```
> C:=QRCode(GF(3),71);
> MinimumWeight(C);
17
> MinimumWeight(Dual(C));
18
```

Još veći primjer QR koda

```
> C:=QRCode(GF(3),71);
> MinimumWeight(C);
17
> MinimumWeight(Dual(C));
18
> WeightDistribution(Dual(C));
```

Kodovi kvadratnih ostataka i shematski 4-dizajni

Još veći primjer QR koda

```
> C:=QRCode(GF(3),71);
> MinimumWeight(C);
17
> MinimumWeight(Dual(C));
18
> WeightDistribution(Dual(C));
```

Razlog za sporost:

$\dim QR(71, q) = 36$

$M = |QR(71, q)| = q^{36}$

$q = 2 \Rightarrow M = 2^{36} \approx 6.9 \cdot 10^{10}$

$q = 3 \Rightarrow M = 3^{36} \approx 1.5 \cdot 10^{17}$

Kodovi kvadratnih ostataka i shematski 4-dizajni

Još veći primjer QR koda

```
> C:=QRCode(GF(3),71);
> MinimumWeight(C);
17
> MinimumWeight(Dual(C));
18
> E:=ExtendCode(C);
> IsSelfDual(E);
true
```

Razlog za sporost:

$\dim QR(71, q) = 36$

$M = |QR(71, q)| = q^{36}$

$q = 2 \Rightarrow M = 2^{36} \approx 6.9 \cdot 10^{10}$

$q = 3 \Rightarrow M = 3^{36} \approx 1.5 \cdot 10^{17}$

Kodovi kvadratnih ostataka i shematski 4-dizajni

Još veći primjer QR koda

```
> C:=QRCode(GF(3),71);
> MinimumWeight(C);
17
> MinimumWeight(Dual(C));
18
> E:=ExtendCode(C);
> IsSelfDual(E);
true
```

Razlog za sporost:

$\dim QR(71, q) = 36$

$M = |QR(71, q)| = q^{36}$

$q = 2 \Rightarrow M = 2^{36} \approx 6.9 \cdot 10^{10}$

$q = 3 \Rightarrow M = 3^{36} \approx 1.5 \cdot 10^{17}$

Teorem.

Ako je $n \equiv 3 \pmod 4$, prošireni kod $\widehat{QR}(n, q)$ je samodualan.

Kodovi kvadratnih ostataka i shematski 4-dizajni

Još veći primjer QR koda

```
> C:=QRCode(GF(3),71);
> MinimumWeight(C);
17
> MinimumWeight(Dual(C));
18
> E:=ExtendCode(C);
> IsSelfDual(E);
true
```

Razlog za sporost:

$$\dim QR(71, q) = 36$$

$$M = |QR(71, q)| = q^{36}$$

$$q = 2 \Rightarrow M = 2^{36} \approx 6.9 \cdot 10^{10}$$

$$q = 3 \Rightarrow M = 3^{36} \approx 1.5 \cdot 10^{17}$$

Teorem.

Ako je $n \equiv 3 \pmod 4$, prošireni kod $\widehat{QR}(n, q)$ je samodualan.

```
> PartialWeightDistribution(E,20);
[ <0, 1>, <18, 357840> ]
```

Teorem (MacWilliamsin identitet)

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

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

Kodovi kvadratnih ostataka i shematski 4-dizajni

Teorem (MacWilliamsin identitet)

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

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

$$W_E(X, Y) = 3^{-36}\, W_E(X + 2Y, X - Y)$$

Teorem (MacWilliamsin identitet)

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

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

$$W_E(X,Y) = X^{72} + 357840X^{54}Y^{18} + 29772288X^{51}Y^{21} + 2688809760X^{48}Y^{24} +$$
$$125992569472X^{45}Y^{27} + 3526708233024X^{42}Y^{30} + 59355639700560X^{39}Y^{33} +$$
$$607803719012256X^{36}Y^{36} + 3798836081510400X^{33}Y^{39} +$$
$$14443540225111008X^{30}Y^{42} + 33060319439473536X^{27}Y^{45} +$$
$$44727780092682960X^{24}Y^{48} + 34777050459847488X^{21}Y^{51} +$$
$$14918073393482560X^{18}Y^{54} + 3328268946790464X^{15}Y^{57} +$$
$$3540301402135 68X^{12}Y^{60} + 156905983 10400X^{9}Y^{63} +$$
$$230439513024X^{6}Y^{66} + 701366400X^{3}Y^{69} + 242112Y^{72}$$

Kodovi kvadratnih ostataka i shematski 4-dizajni

Teorem (MacWilliamsin identitet)

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

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

```
> WeightDistribution(E);
[ <0, 1>, <18, 357840>, <21, 29772288>, <24, 2688809760>,
<27, 125992569472>, <30, 3526708233024>, <33, 59355639700560>,
<36, 607803719012256>, <39, 3798836081510400>, <42,
14443540225111008>, <45, 33060319439473536>, <48,
44727780092682960>, <51, 3477705045984748 8>, <54,
14918073393482560>, <57, 3328268946790464>, <60,
354030140213568>, <63, 15690598310400>, <66, 230439513024>,
<69, 701366400>, <72, 242112> ]
```

Kodovi kvadratnih ostataka i shematski 4-dizajni

Teorem (MacWilliamsin identitet)

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

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

```
> WeightDistribution(E);
[ <0, 1>, <18, 357840>, <21, 29772288>, <24, 2688809760>,
<27, 125992569472>, <30, 3526708233024>, <33, 59355639700560>,
<36, 607803719012256>, <39, 3798836081510400>, <42,
14443540225111008>, <45, 33060319439473536>, <48,
44727780092682960>, <51, 34777050459847488>, <54,
14918073393482560>, <57, 3328268946790464>, <60,
354030140213568>, <63, 15690598310400>, <66, 230439513024>,
<69, 701366400>, <72, 242112> ]
```

$B_{18}, \ldots, B_{69} \rightsquigarrow$ 18 nenul težina

Teorem (MacWilliamsin identitet)

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

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

$$W_{C^\perp}(X,Y) = X^{71} + 268380X^{53}Y^{18} + 21088704X^{50}Y^{21} + 1792539840X^{47}Y^{24} +$$
$$78745355920X^{44}Y^{27} + 2057246469264X^{41}Y^{30} + 32150971504470X^{38}Y^{33} +$$
$$303901859506128X^{35}Y^{36} + 1741133204025600X^{32}Y^{39} +$$
$$6018141760462920X^{29}Y^{42} + 12397619789802576X^{26}Y^{45} +$$
$$14909260030894320X^{23}Y^{48} + 10143306384122184X^{20}Y^{51} +$$
$$3729518348370640X^{17}Y^{54} + 6933893639146 80X^{14}Y^{57} +$$
$$590050233689 28X^{11}Y^{60} + 1961324788800X^{8}Y^{63} + 19203292752X^{5}Y^{66} +$$
$$29223600X^{2}Y^{69}$$

Kodovi kvadratnih ostataka i shematski 4-dizajni

Teorem (MacWilliamsin identitet)

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

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

```
> WeightDistribution(Dual(C));
[ <0, 1>, <18, 268380>, <21, 21088704>, <24, 1792539840>,
<27, 78745355920>, <30, 2057246469264>, <33, 32150971504470>,
<36, 303901859506128>, <39, 1741133204025600>, <42,
6018141760462920>, <45, 12397619789802576>, <48,
14909260030894320>, <51, 10143306384122184>, <54,
3729518348370640>, <57, 693389363914680>, <60,
59005023368928>, <63, 1961324788800>, <66, 19203292752>,
<69, 29223600> ]
```

Kodovi kvadratnih ostataka i shematski 4-dizajni

Teorem (MacWilliamsin identitet)

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

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

```
> WeightDistribution(Dual(C));
[ <0, 1>, <18, 268380>, <21, 21088704>, <24, 1792539840>,
<27, 78745355920>, <30, 2057246469264>, <33, 32150971504470>,
<36, 303901859506128>, <39, 1741133204025600>, <42,
6018141760462920>, <45, 12397619789802576>, <48,
14909260030894320>, <51, 10143306384122184>, <54,
3729518348370640>, <57, 693389363914680>, <60,
59005023368928>, <63, 1961324788800>, <66, 19203292752>,
<69, 29223600> ]
```

$B_{18}, \ldots, B_{69} \rightsquigarrow$ 18 nenul težina

Kodovi kvadratnih ostataka i shematski 4-dizajni

Teorem (MacWilliamsin identitet)

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

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

$W_C(X,Y) = X^{71} + 89460X^{54}Y^{17} + 268380X^{53}Y^{18} + 8683584X^{51}Y^{20} + 21088704X^{50}Y^{21} +$
$896269920X^{48}Y^{23} + 1792539840X^{47}Y^{24} + 47247213552X^{45}Y^{26} + 78745355920X^{44}Y^{27} +$
$1469461763760X^{42}Y^{29} + 2057246469264X^{41}Y^{30} + 27204668196090X^{39}Y^{32} +$
$32150971504470X^{38}Y^{33} + 303901859506128X^{36}Y^{35} + 303901859506128X^{35}Y^{36} +$
$1741133204025600X^{32}Y^{39} + 2057702877484800X^{33}Y^{38} + 8425398464648088X^{30}Y^{41} +$
$6018141760462920X^{29}Y^{42} + 20662699649670960X^{27}Y^{44} + 12397619789802576X^{26}Y^{45} +$
$29818520061788640X^{24}Y^{47} + 14909260030894320X^{23}Y^{48} + 2463374407572530 4X^{21}Y^{50} +$
$1014330638412218 4X^{20}Y^{51} + 1118855504511192 0X^{18}Y^{53} + 372951834837064 0X^{17}Y^{54} +$
$263487958287578 4X^{15}Y^{56} + 69338936391468 0X^{14}Y^{57} + 29502511684464 0X^{12}Y^{59} +$
$5900502336892 8X^{11}Y^{60} + 1372927352160 0X^{9}Y^{62} + 196132478880 0X^{8}Y^{63} +$
$2112362202 72X^{6}Y^{65} + 1920329275 2X^{5}Y^{66} + 67214280 0X^{3}Y^{68} + 2922360 0X^{2}Y^{69} + 242112Y^{71}$

Kodovi kvadratnih ostataka i shematski 4-dizajni

Br.	v	k	λ	x	y	z	$\exists$
1	11	5	1	1	2	3	✓
2	23	8	4	0	2	4	✓
3	23	11	48	3	5	7	✓
4	24	8	5	0	2	4	✓
5	47	11	8	1	3	5	✓
6	71	35	264	14	17	20	?
7	199	99	2328	44	49	54	?
8	391	195	9264	90	97	104	?
9	647	323	25680	152	161	170	?
10	659	329	390874	153	164	175	?
11	967	483	57720	230	241	252	?

$QR(11,3) \equiv G_{11}$

$QR(23,2) \equiv G_{23}$

$QR(23,2) \equiv G_{23}$

$\widehat{QR}(23,2) \equiv G_{24}$

$QR(47,2)$

~~$QR(71,3)$~~

Kodovi kvadratnih ostataka i shematski 4-dizajni

Još jedan problem:

Lema.

Neka je $C \leq \mathbb{F}^n$ kod s parametrima $[n, m, d]_q$ i neka je

$$\Bbbk_{\max} = \begin{cases} n, & \text{ako je } q = 2 \\ \max\left\{ \Bbbk \in \mathbb{N} \mid \Bbbk - \left\lceil \dfrac{\Bbbk}{q-1} \right\rceil < d \right\}, & \text{ako je } q > 2 \end{cases}$$

Ako su $x, y \in C$ kodne riječi s istim nosačem $\operatorname{supp} x = \operatorname{supp} y$ i ako je $w(x) = w(y) \leq \Bbbk_{\max}$, onda su x i y proporcionalni.

Kodovi kvadratnih ostataka i shematski 4-dizajni

Još jedan problem:

Lema.

Neka je $C \leq \mathbb{F}^n$ kod s parametrima $[n, m, d]_q$ i neka je

$$\Bbbk_{\max} = \begin{cases} n, & \text{ako je } q = 2 \\ \max\left\{ \Bbbk \in \mathbb{N} \mid \Bbbk - \left\lceil \dfrac{\Bbbk}{q-1} \right\rceil < d \right\}, & \text{ako je } q > 2 \end{cases}$$

Ako su $x, y \in C$ kodne riječi s istim nosačem $\operatorname{supp} x = \operatorname{supp} y$ i ako je $w(x) = w(y) \leq \Bbbk_{\max}$, onda su x i y proporcionalni.

Za $QR(71, 3)$ dobivamo $\Bbbk_{\max} = 33$, a 4-$(71, 35, 264)$ dizajn ima $\Bbbk = 35$

Kodovi kvadratnih ostataka i shematski 4-dizajni

Još jedan problem:

Lema.

Neka je $C \leq \mathbb{F}^n$ kod s parametrima $[n, m, d]_q$ i neka je

$$\Bbbk_{\max} = \begin{cases} n, & \text{ako je } q = 2 \\ \max\left\{ \Bbbk \in \mathbb{N} \mid \Bbbk - \left\lceil \dfrac{\Bbbk}{q-1} \right\rceil < d \right\}, & \text{ako je } q > 2 \end{cases}$$

Ako su $x, y \in C$ kodne riječi s istim nosačem $\operatorname{supp} x = \operatorname{supp} y$ i ako je $w(x) = w(y) \leq \Bbbk_{\max}$, onda su x i y proporcionalni.

Za $QR(71, 3)$ dobivamo $\Bbbk_{\max} = 33$, a 4-$(71, 35, 264)$ dizajn ima $\Bbbk = 35$

V. Krčadinac, R. Vlahović Kruc, *Schematic 4-designs*, Discrete Math. **346** (2023), no. 7, članak 113385, 7 str.