Diferencijski skupovi i automorfizmi dizajna

Sanja Vranić

4. lipnja 2009.

Literatura

- **Douglas R. Stinson** ,
  Combinatorial Designs: Construction and Analysis,
  Springer-Verlag, New York, 2004.

Sadržaj

Diferencijski skupovi kvadratnog ostatka

- Neka je $\mathbb{F}_q$ konačno polje gdje je q neparan prim broj. Kvadratni ostatci nad poljem $\mathbb{F}_q$ su elementi skupa
$$QR(q) = \{z^2 : z \in \mathbb{F}_q, z \neq 0\}$$
- Definiramo
$$QNR(q) = \mathbb{F}_q \setminus (QR\{q\} \cup \{0\})$$
elementi skupa $QNR(q)$ se zovu nekvadratni ostatci nad $\mathbb{F}_q$
- $QR(q)$ je multiplikativna podgrupa grupe $\mathbb{F}_q \setminus \{0\}$ indeksa 2
- $QNR(q)$ je suskup grupe $QR(q)$

Diferencijski skupovi kvadratnog ostatka

Vrijedi

- $xy \in QR(q)$ ako $x, y \in QR(q)$
- $xy \in QR(q)$ ako $x, y \in QNR(q)$
- $xy \in QNR(q)$ ako $x \in QR(q), y \in QNR(q)$

Diferencijski skupovi kvadratnog ostatka

- Generator ω grupe $(\mathbb{F}_q\backslash\{0\},\cdot)$ naziva se *primitivnim elementom* polja $\mathbb{F}_q$.
- $\omega \in \mathbb{F}_q$ je primitivni element ako i samo ako vrijedi

$$\{\omega^i : 0 \leq i \leq q-2\} = \mathbb{F}_q\backslash\{0\}$$

- $\left\{\omega^{2i} : 0 \leq i \leq \frac{q-3}{2}\right\}$

Diferencijski skupovi kvadratnog ostatka

- Generator ω grupe $(\mathbb{F}_q \backslash \{0\}, \cdot)$ naziva se *primitivnim elementom* polja $\mathbb{F}_q$.
- $\omega \in \mathbb{F}_q$ je primitivni element ako i samo ako vrijedi

$$\{\omega^i : 0 \leq i \leq q-2\} = \mathbb{F}_q \backslash \{0\}$$

- $\left\{\omega^{2i} : 0 \leq i \leq \frac{q-3}{2}\right\} \subseteq QR(q)$

Diferencijski skupovi kvadratnog ostatka

- Generator ω grupe $(\mathbb{F}_q \setminus \{0\}, \cdot)$ naziva se *primitivnim elementom* polja $\mathbb{F}_q$.
- $\omega \in \mathbb{F}_q$ je primitivni element ako i samo ako vrijedi

$$\{\omega^i : 0 \leq i \leq q-2\} = \mathbb{F}_q \setminus \{0\}$$

- $\left\{\omega^{2i} : 0 \leq i \leq \frac{q-3}{2}\right\} \subseteq QR(q)$

$$\left| \left\{\omega^{2i} : 0 \leq i \leq \frac{q-3}{2}\right\} \right| = \frac{q-1}{2}$$

Diferencijski skupovi kvadratnog ostatka

- Generator ω grupe $(\mathbb{F}_q \backslash \{0\}, \cdot)$ naziva se *primitivnim elementom* polja $\mathbb{F}_q$.
- $\omega \in \mathbb{F}_q$ je primitivni element ako i samo ako vrijedi

$$\{\omega^i : 0 \leq i \leq q-2\} = \mathbb{F}_q \backslash \{0\}$$

- $\left\{\omega^{2i} : 0 \leq i \leq \frac{q-3}{2}\right\} \subseteq QR(q)$

$$\left| \left\{\omega^{2i} : 0 \leq i \leq \frac{q-3}{2}\right\} \right| = \frac{q-1}{2} = |QR(q)|$$

Diferencijski skupovi kvadratnog ostatka

Lema 1

Neka je q potencija neparnog prim broja te neka je ω primitivni element polja $\mathbb{F}_q$. Tada je

$$QR(q) = \left\{ \omega^{2i} : 0 \leq i \leq \frac{q-3}{2} \right\}$$

Korolar 1

Neka je q potencija neparnog prim broja. Onda je $-1 \in QR(q)$ ako i samo ako vrijedi $q \equiv 1 \pmod 4$

- $x \in QR(q) \Leftrightarrow -x \in QNR(q)$,
  gdje je q potencija prim broja i $q \equiv 3 \pmod 4$

Diferencijski skupovi kvadratnog ostatka

Teorem 1 - Diferencijski skupovi kvadratnog ostataka

Neka je q potencija prim broja i $q \equiv 3 \pmod 4$. Tada je $QR(q)$ $(q, (q-1)/2, (q-3)/4)$ diferencijski skup u $(\mathbb{F}_q, +)$

Diferencijski skupovi kvadratnog ostatka

$(11, 5, 2)$-diferencijski skup u $(\mathbb{Z}_{11}, +)$

$$1^2 = 1$$
$$2^2 = 4$$
$$3^2 = 9$$
$$4^2 = 5$$
$$5^2 = 3$$
$$QR(11) = \{1, 3, 4, 5, 9\}$$

- Ako je q potencija prim broja te vrijedi $q \equiv 1 \pmod 4$, kvadratni ostatci u $\mathbb{F}_q$ su elementi skupa $\{z^4 : z \in \mathbb{F}_q, z \neq 0\}$
- Ekvivalentno, ako je ω primitivni element u $\mathbb{F}_q$, kvadratni ostatci su elementi skupa $\{\omega^{4i} : 0 \leq i \leq (q-5)/4\}$

Diferencijski skupovi kvadratnog ostatka

Teorem 2

Neka je $p = 4t^2 + 1$ prim broj, gdje je t neparan cijeli broj.
Tada kvadratni ostatci u $\mathbb{F}_p$ čine $(4t^2 + 1, t^2, (t^2 - 1)/4)$-diferencijski skup u $(\mathbb{Z}_p, +)$.

Primjer

$$\{1, 7, 9, 10, 12, 16, 26, 33, 34\}$$

je $(37, 9, 2)$-diferencijski skup u $(\mathbb{Z}_{37}, +)$

Teorem 3

Neka je $p = 4t^2 + 9$ prim broj, gdje je t neparan cijeli broj.
Tada kvadratni ostatci u $\mathbb{F}_p$ zajedno sa 0 čine $(4t^2 + 9, t^2 + 3, (t^2 + 3)/4)$-diferencijski skup u $(\mathbb{Z}_p, +)$

Singerovi diferencijski skupovi

- beskonačna klasa diferencijskih skupova
- omogućuju metodu konstrukcije projektivnih ravnina reda q, gdje je q potencija prim broja

Teorem 4-Singerovi diferencijski skupovi

Neka je q potencija prim broja. Tada postoji $(q^2+q+1, q+1, 1)$-diferencijski skup u $(\mathbb{Z}_{q^2+q+1}, +)$

Singerovi diferencijski skupovi

Teorem 4-Singerovi diferencijski skupovi

Neka je q potencija prim broja. Tada postoji $(q^2+q+1, q+1, 1)$-diferencijski skup u $(\mathbb{Z}_{q^2+q+1}, +)$

Skica dokaza

- konačno polje $V = \mathbb{F}_{q^3}$ je trodimenzionalni vektorski prostor nad $\mathbb{F}_q$
- ω primitivni element u $\mathbb{F}_{q^3}$,
  $f : V \to V, f(z) = \omega z$ (linerano preslikavanje)
- f je automorfiza koji permutira jednodimenzinalne podprostore od $\mathbb{F}_{q^3}$
- f se može prikazati kao jedan ciklus duljine q^2+q+1

Singerovi diferencijski skupovi

Primjer

Konstrukcija Singerovog diferencijskog skupa za projektivne ravnine
Neka je $q = 3$.
Polje $\mathbb{F}_{27}$ se može konstruirati kao kvocijentni prsten $\mathbb{Z}_3/(x^3 + 2x + 1)$ budući je $x^3 + 2x + 1$ ireducibilan nad $\mathbb{Z}_3$.
Pokaže se da je $\omega = x$ primitivni element u tako dobivenom polju $\mathbb{F}_{27}$.

Primjer

Možemo prebrojati potencije od ω na sljedeći način

i	ω^i	i	ω^i
0	1	13	2
1	x	14	$2x$
2	x^2	15	$2x^2$
3	x^2+2	16	$2x^2+1$
4	x^2+2x+2	17	$2x^2+x+1$
5	$2x+2$	18	$x+1$
6	$2x^2+2x$	19	x^2+x
7	x^2+1	20	$2x^2+2$
8	x^2+x+2	21	$2x^2+2x+1$
9	$2x^2+2x+2$	22	x^2+x+1
10	x^2+2x+1	23	$2x^2+x+2$
11	$x+2$	24	$2x+1$
12	x^2+2x	25	$2x^2+x$

Singerovi diferencijski skupovi

Primjer

Prebrojavamo jedino vrijednosti y_j takve da je $\omega^{y_j} = j + x$ za $j = 0, 1, 2$. Iz tablice potencija ω^i vidimo da je $y_0 = 1$, $y_1 = 18$ te $y_2 = 11$.

$$D = \{0\} \cup \{y_j \bmod (q^2 + q + 1) : j \in \mathbb{F}_q\}$$

Tada je $D = \{0, 1, 5, 11\}$ $(13, 4, 1)$-diferencijski skup u $\mathbb{Z}_{13}$

Singerovi diferencijski skupovi

Teorem 5-Singerovi diferencijski skupovi

Neka je $q \geq 2$ potencija prim broja te $d \geq 2$ cijeli broj. Tada postoji $\left(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}\right)$-diferencijski skup u $(\mathbb{Z}_{(q^{d+1}-1)/(q-1)}, +)$.

Multiplikatori diferencijskih skupova

- promatramo Abelove grupe!

Definicija 1

Neka je D (v, k, λ)-diferencijski skup u Abelovoj grupi $(G, +)$ reda v. Za cijeli broj m definiramo

$$mD = \{mx : x \in D\},$$

gdje mx označava m puta pribrojen x sam sebi. m se naziva *multiplikatorom* od D ako je $mD = D + g$ za neki $g \in G$. Kažemo da je D fiksiran multiplikatorom m ako je $mD = D$.

Multiplikatori diferencijskih skupova

Primjer

- $D = \{0, 1, 5, 11\}$ je $(13, 4, 1)$-diferencijski skup u $(\mathbb{Z}_{13}, +)$
  $3D = \{0, 2, 3, 7\} = D + 2$ 3 je multiplikator skupa D
- $2D = \{0, 2, 9, 10\}$ je $(13, 4, 1)$-diferencijski skup
  Pretpostavimo da je $2D = D + g$, za neki $g \in \mathbb{Z}_{13}$.
  $$1 = 1 - 0 \text{ u } D$$
  $$1 = 10 - 9 \text{ u } 2D$$
  $(0, 1) + g = (10, 9) \Rightarrow g = 9$
  Međutim, $D + 9 = \{3, 7, 9, 10\} \neq 2D$ pa 2 nije multiplikator skupa D.
- Kvadratni ostatci su multiplikatori diferencijskih skupova iz Teorema 1.

Multiplikatori diferencijskih skupova

Lema 2

Neka je m multiplikator (v, k, λ)-diferencijskog skupa u Abelovoj grupi $(G, +)$ reda v. Tada vrijedi $\mathbf{nzd}(m, v) = 1$

Lema 3

Neka je m multiplikator (v, k, λ)-diferencijskog skupa u Abelovoj grupi $(G, +)$ reda v. Definiramo preslikavanje $\alpha : G \to G$ tako da je $\alpha(x) = mx$. Tada je $\alpha \in Aut(G, Dev(G))$.

Multiplikatori diferencijskih skupova

Teorem o multipliaktoru

Neka postoji (v, k, λ)-diferencijski skup D u Abelovoj grupi $(G, +)$ reda v. Neka su još ispunjeni sljedeći uvjeti:

1. p je prim broj
2. $\mathbf{nzd}(p, v) = 1$
3. $k - \lambda \equiv 0 \pmod p$
4. $p > \lambda$

Tada je p multiplikator od D.

Multiplikatori diferencijskih skupova

Teorem 6

Neka je m multiplikator (v, k, λ)-diferencijskog skupa D u Abelovoj grupi $(G, +)$ reda v. Tada postoji translat od D koji je fiksiran sa m.

Teorem 7

Neka je $\mathbf{nzd}(k, v) = 1$ i neka postoji (v, k, λ)-diferencijskog skupa D u Abelovoj grupi $(G, +)$ reda v. Tada postoji translat od D koji je fiksiran sa svakim multiplikatorom m.

Primjer: $(21,5,1)$ diferencijski skup u $(Z_{21},+)$

$p=2$ (Teorem o multiplikatoru)
(Teorem 6) $\Rightarrow$ možemo pretpostaviti da postoji $(21,5,1)$ diferencijski skup u $(Z_{21},+)$ fiksiran multiplikatorom 2
Odredimo orbite grupe $(Z_{21},+)$ dobivene multiplikacijom sa 2.
(Ciklusi u disjunktnoj cikličkoj prezentaciji permutacije grupe $(Z_{21},+)$ definirane sa $x \to 2x$ mod 21)

$$
\begin{array}{r}
(0)\\
(1\quad 2\quad 4\quad 8\quad 16\quad 11)\\
(3\quad 6\quad 12)\\
(5\quad 10\quad 20\quad 19\quad 17\quad 3)\\
(7\quad 14)\\
(9\quad 18\quad 15)
\end{array}
$$

Primjer: $(21,5,1)$ diferencijski skup u $(Z_{21},+)$

$p=2$ (Teorem o multiplikatoru)
(Teorem 6) $\Rightarrow$ možemo pretpostaviti da postoji $(21,5,1)$ diferencijski skup u $(Z_{21},+)$ fiksiran multiplikatorom 2
Odredimo orbite grupe $(Z_{21},+)$ dobivene multiplikacijom sa 2.
(Ciklusi u disjunktnoj cikličkoj prezentaciji permutacije grupe $(Z_{21},+)$ definirane sa $x \rightarrow 2x \bmod 21$)

$$(0)$$
$$(1\quad 2\quad 4\quad 8\quad 16\quad 11)$$
$$(3\quad 6\quad 12)$$
$$(5\quad 10\quad 20\quad 19\quad 17\quad 3)$$
$$(7\quad 14)$$
$$(9\quad 18\quad 15)$$

Diferencijski skupovi su

$$\{3,6,7,12,14\}$$

$$\{7,9,14,15,18\}$$

Familije diferencijskih skupova

Definicija 2

Neka je $(G, +)$ konačna grupa reda v s jediničnim elementom 0. Neka su k i λ pozitivni cijeli brojevi tako da je $2 \leq k \leq v$.
(v, k, λ)-diferencijska familija u $(G, +)$ je familija podskupova od G, $[D_1, \cdots, D_l]$ tako da vrijedi

1. $|D_i| = k$ za $1 \leq i \leq l$
2. unija multiskupova

$$\bigcup_{i=1}^{l} [x - y : x, y \in D_i, x \neq y]$$

sadrži svaki element iz $G \backslash \{0\}$ točno λ puta.

Familije diferencijskih skupova

Primjer

$(13, 3, 1)$ diferencijska familija u $(Z_{13}, +)$

$$\{\{0, 1, 4\}, \{0, 2, 8\}\}$$

- 1,3,4,9,10 i 12
- 2,5,6,7,8 i 11