

Unitali i unitarni polariteti simetričnih dizajna

Doris Dumičić
(ddumicic@math.uniri.hr)
Odjel za matematiku, Sveučilište u Rijeci

- **R. Mathon, T. van Trung:** Unitals and Unitary Polarities in Symmetric Designs; *Designs, Codes and Cryptography*, 10 (1997) 237-250.

1 Unital u simetričnom dizajnu

Sadržaj

- 1 Unital u simetričnom dizajnu
- 2 Unitali u dizajnim a točka a hiperravnina, $PG_{d-1}(d, q)$

Sadržaj

- 1 Unital u simetričnom dizajnu
- 2 Unitali u dizajnim a točka i hiperravnina, $PG_{d-1}(d, q)$
- 3 Unitali u Hadamardovim dizajnim a za prim potencije blizance

Sadržaj

- 1 Unital u simetričnom dizajnu
- 2 Unitali u dizajnim a točka i hiperravnina, $PG_{d-1}(d, q)$
- 3 Unitali u Hadamardovim dizajnim a za prim potencije blizance
- 4 Unitali u familiji simetričnih dizajna s parametrima $2 - (4t^2, 2t^2 - t, t^2 - t)$

Sadržaj

- 1 Unital u simetričnom dizajnu
- 2 Unitali u dizajnim a točka i hiperravnina, $PG_{d-1}(d, q)$
- 3 Unitali u Hadamardovim dizajnim a za prim potencije blizance
- 4 Unitali u familiji simetričnih dizajna s parametrima $2 - (4t^2, 2t^2 - t, t^2 - t)$
- 5 Unitali u familiji simetričnih dizajna s parametrima $2 - (q^2(q + 2), q(q^2 + q - 1), q(q^2 - 1))$

Sadržaj

- 1 Unital u simetričnom dizajnu
- 2 Unitali u dizajnim a točka i hiperravnina, $PG_{d-1}(d, q)$
- 3 Unitali u Hadamardovim dizajnim a za prim potencije blizance
- 4 Unitali u familiji simetričnih dizajna s parametrima $2 - (4t^2, 2t^2 - t, t^2 - t)$
- 5 Unitali u familiji simetričnih dizajna s parametrima $2 - (q^2(q + 2), q(q^2 + q - 1), q(q^2 - 1))$
- 6 Unitarni polaritet u simetričnom dizajnu

Uvodni pojmovi

Definicija

Za $n \in \mathbb{N}$, $n \geq 2$, kažemo da je $2 - (n^3 + 1, n + 1, 1)$ dizajn **unital** reda n .

Uvodni pojmovi

Definicija

Za $n \in \mathbb{N}$, $n \geq 2$, kažemo da je $2 - (n^3 + 1, n + 1, 1)$ dizajn **unital** reda n .

Definicija

Unital \mathcal{U} reda n uložen u projektivnu ravninu π reda n^2 je unital čiji su blokovi skupovi kolinearnih točaka od π i svaki pravac te ravnine presjeca \mathcal{U} u $n + 1$ ili jednoj točki.

Polaritet projektivne ravnine

Definicija

Automorfizme projektivnih ravnina nazivamo *kolineacije* projektivne ravnine.

Polaritet projektivne ravnine

Definicija

Automorfizme projektivnih ravnina nazivamo *kolineacije* projektivne ravnine.

Definicija

Neka je $(\mathcal{P}, \mathcal{L}, I)$ projektivna ravnina. *Korelacija* je bijekcija $\rho : \mathcal{P} \cup \mathcal{L} \rightarrow \mathcal{P} \cup \mathcal{L}$ takva da vrijedi $\mathcal{P}^\rho = \mathcal{L}$, $\mathcal{L}^\rho = \mathcal{P}$ i $P \perp m \iff m^\rho \perp P^\rho, \forall P \in \mathcal{P} \text{ i } \forall m \in \mathcal{L}$.

Polaritet ρ je involutorna korelacija, odnosno $\rho^2 = id$.

Polaritet projektivne ravnine

Definicija

Automorfizme projektivnih ravnina nazivamo *kolineacije* projektivne ravnine.

Definicija

Neka je $(\mathcal{P}, \mathcal{L}, I)$ projektivna ravnina. *Korelacija* je bijekcija $\rho : \mathcal{P} \cup \mathcal{L} \rightarrow \mathcal{P} \cup \mathcal{L}$ takva da vrijedi $\mathcal{P}^\rho = \mathcal{L}$, $\mathcal{L}^\rho = \mathcal{P}$ i $P \perp m \iff m^\rho \perp P^\rho, \forall P \in \mathcal{P}$ i $\forall m \in \mathcal{L}$.

Polaritet ρ je involutorna korelacija, odnosno $\rho^2 = id$.

Definicija

Neka je ρ polaritet projektivne ravnine $(\mathcal{P}, \mathcal{L}, I)$. Točke i pravce zovemo *apsolutnim* ako su incidentni sa svojom slikom po ρ . Inače ih zovemo *neapsolutnim* točkama, odnosno pravcima.

Polariteti konačnih projektivnih ravnina

Teorem

Neka je ρ polaritet projektivne ravnine reda $n = s^2$. Tada vrijedi $n + 1 \leq a(\rho) \leq s^3 + 1$, gdje je $a(\rho)$ broj apsolutnih točaka polariteta ρ .

Polariteti konačnih projektivnih ravnina

Teorem

Neka je ρ polaritet projektivne ravnine reda $n = s^2$. Tada vrijedi $n + 1 \leq a(\rho) \leq s^3 + 1$, gdje je $a(\rho)$ broj apsolutnih točaka polariteta ρ .

Definicija

Neka je dana projektivna ravnina reda $n = s^2$. Polaritete čiji je broj apsolutnih točaka maksimalan, odnosno jednak $s^3 + 1$, nazivamo *unitarni polariteti*.

Polariteti konačnih projektivnih ravnina

Teorem

Neka je ρ polaritet projektivne ravnine reda $n = s^2$. Tada vrijedi $n + 1 \leq a(\rho) \leq s^3 + 1$, gdje je $a(\rho)$ broj apsolutnih točaka polariteta ρ .

Definicija

Neka je dana projektivna ravnina reda $n = s^2$. Polaritete čiji je broj apsolutnih točaka maksimalan, odnosno jednak $s^3 + 1$, nazivamo *unitarni polariteti*.

Teorem

Neka je ρ unitarni polaritet projektivne ravnine reda $n = s^2$. Skup apsolutnih točaka i neapsolutnih pravaca od ρ čine unital, tj. $2 - (s^3 + 1, s + 1, 1)$ dizajn.

Polariteti konačnih projektivnih ravnina

Teorem

Neka je ρ polaritet projektivne ravnine reda $n = s^2$. Tada vrijedi $n + 1 \leq a(\rho) \leq s^3 + 1$, gdje je $a(\rho)$ broj apsolutnih točaka polariteta ρ .

Definicija

Neka je dana projektivna ravnina reda $n = s^2$. Polaritete čiji je broj apsolutnih točaka maksimalan, odnosno jednak $s^3 + 1$, nazivamo *unitarni polariteti*.

Teorem

Neka je ρ unitarni polaritet projektivne ravnine reda $n = s^2$. Skup apsolutnih točaka i neapsolutnih pravaca od ρ čine unital, tj. $2 - (s^3 + 1, s + 1, 1)$ dizajn.

Polaritet klasičnih projektivnih ravnina

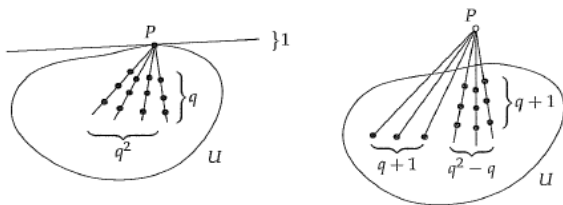
Klasična projektivna ravnina $PG(2, q^2)$, gdje je q prim potencija, ima unitarni polaritet. Unital, tj. $2 - (q^3 + 1, q + 1, 1)$ -dizajn, dobiven od tog unitarnog polariteta nazivamo *klasični ili Hermitski unital*.

Iz kombinatoričkog gledišta imamo:

Karakterizacija unitala uloženih u projektivnu ravninu

Unital \mathcal{U} reda q je uložen u projektivnu ravnini π reda $n = q^2$ ako i samo ako \mathcal{U} je podskup od $q^3 + 1$ točaka sa svojstvom :

Kroz svaku točku $P \in \mathcal{U}$ prolazi točno jedan pravac (tangenta) iz π koji presjeca \mathcal{U} u točki P i postoji q^2 pravaca (sekanti) iz π koji presjecaju \mathcal{U} u $(q + 1)$ -članim podskupovima. (*)



1. Unital u simetričnom dizajnu

Definicija (**)

Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$ simetričan $2 - (v, k, \lambda)$ dizajn. Neka je \mathcal{U} podskup skupa točaka iz \mathcal{D} sa svojstvom:

Svaka točka $P \in \mathcal{U}$ je incidentna s $k - 1$ blokova iz \mathcal{D} koji sijeku \mathcal{U} u α točaka i s točno jednim blokom koji presjeca \mathcal{U} u točki P .

1. Unital u simetričnom dizajnu

Definicija (**)

Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$ simetričan $2 - (v, k, \lambda)$ dizajn. Neka je \mathcal{U} podskup skupa točaka iz \mathcal{D} sa svojstvom:

Svaka točka $P \in \mathcal{U}$ je incidentna s $k - 1$ blokova iz \mathcal{D} koji sijeku \mathcal{U} u α točaka i s točno jednim blokom koji presjeca \mathcal{U} u točki P .

Blokove od \mathcal{D} koji \mathcal{U} sijeku u α - članim podskupovima nazivamo *sekante*, dok blokove koji ga presjecaju u jednoj točki nazivamo *tangente*.

1. Unital u simetričnom dizajnu

Definicija (**)

Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$ simetričan $2 - (v, k, \lambda)$ dizajn. Neka je \mathcal{U} podskup skupa točaka iz \mathcal{D} sa svojstvom:

Svaka točka $P \in \mathcal{U}$ je incidentna s $k - 1$ blokova iz \mathcal{D} koji sijeku \mathcal{U} u α točaka i s točno jednim blokom koji presjeca \mathcal{U} u točki P .

Blokove od \mathcal{D} koji \mathcal{U} sijeku u α - članim podskupovima nazivamo *sekante*, dok blokove koji ga presjecaju u jednoj točki nazivamo *tangente*.

Lema 1.1 [M.J.de Resmini, On sets of type (m, n) in BIBD's with $\lambda \geq 2$]

Neka je \mathcal{U} podskup skupa točaka dizajna \mathcal{D} koji zadovoljava (**). Tada vrijedi:

- (i) $n = k - \lambda$ je kvadrat
- (ii) $\alpha = \sqrt{n} + 1$,
- (iii) $|\mathcal{U}| = 1 + (k - 1)\sqrt{n}/\lambda$, posebno $1 + (k - 1)\sqrt{n}/\lambda \in \mathbb{N}$,
- (iv) Točke od \mathcal{U} i njegove sekante čine $2 - (1 + (k - 1)\sqrt{n}/\lambda, \sqrt{n} + 1, \lambda)$ dizajn.

Definicija

Skup točaka \mathcal{U} iz \mathcal{D} koji ima svojstvo iz definicije (***) nazivamo *unital*.

Također i dizajn dobiven iz \mathcal{U} i pripadnih sekanti nazivamo *unital*.

Definicija

Skup točaka \mathcal{U} iz \mathcal{D} koji ima svojstvo iz definicije (***) nazivamo *unital*.

Također i dizajn dobiven iz \mathcal{U} i pripadnih sekanti nazivamo *unital*.

Lema 1.2

Neka je \mathcal{U} skup od $u = 1 + (k - 1)\sqrt{n}/\lambda$ točaka iz dizajna \mathcal{D} .

Pretpostavimo da svaki blok iz \mathcal{D} presjeca \mathcal{U} u 1 ili $\sqrt{n} + 1$ točaka. Tada je \mathcal{U} unital.

Definicija

Skup točaka \mathcal{U} iz \mathcal{D} koji ima svojstvo iz definicije (***) nazivamo *unital*.

Također i dizajn dobiven iz \mathcal{U} i pripadnih sekanti nazivamo *unital*.

Lema 1.2

Neka je \mathcal{U} skup od $u = 1 + (k - 1)\sqrt{n}/\lambda$ točaka iz dizajna \mathcal{D} .

Pretpostavimo da svaki blok iz \mathcal{D} presjeca \mathcal{U} u 1 ili $\sqrt{n} + 1$ točaka. Tada je \mathcal{U} unital.

Lema 1.3

Neka je \mathcal{U} unital u \mathcal{D} i neka je točka $P \notin \mathcal{U}$. Tada kroz tu točku prolazi $(\sqrt{n} + 1)$ tangenti i $(k - \sqrt{n} - 1)$ sekanti.

Definicija

Skup točaka \mathcal{U} iz \mathcal{D} koji ima svojstvo iz definicije (***) nazivamo *unital*.

Također i dizajn dobiven iz \mathcal{U} i pripadnih sekanti nazivamo *unital*.

Lema 1.2

Neka je \mathcal{U} skup od $u = 1 + (k - 1)\sqrt{n}/\lambda$ točaka iz dizajna \mathcal{D} .

Pretpostavimo da svaki blok iz \mathcal{D} presjeca \mathcal{U} u 1 ili $\sqrt{n} + 1$ točaka. Tada je \mathcal{U} unital.

Lema 1.3

Neka je \mathcal{U} unital u \mathcal{D} i neka je točka $P \notin \mathcal{U}$. Tada kroz tu točku prolazi $(\sqrt{n} + 1)$ tangenti i $(k - \sqrt{n} - 1)$ sekanti.

Lema 1.4

Ako simetričan dizajn \mathcal{D} sadrži unital, isto tako će unital sadržavati i njegov dual \mathcal{D}^* .

Rezultati

Primjer 1.1

Biravnina je simetričan $2 - (v, k, 2)$ dizajn, gdje je $k \geq 2$.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

B_1 je $2 - (16, 6, 2)$ biravnina.

Rezultati

Primjer 1.1

Biravnina je simetričan $2 - (v, k, 2)$ dizajn, gdje je $k \geq 2$.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

B_1 je $2 - (16, 6, 2)$ biravnina.

$\mathcal{U} = \{5, 9, 13, 6, 11, 16\}$ je unital u dizajnu B_1 .

$2 - (16, 6, 2)$ biravnine (do na izomorfizam)

Dizajn	B_1	B_2	B_3
#unitala	192	64	0
Red grupe automorfizama	11250	768	384

Primjer 1.2

Hadamardov dizajn je simetričan $2 - (4n - 1, 2n - 1, n - 1)$ dizajn za $n \geq 2$.
 Hadamardovi $2 - (15, 7, 3)$ dizajni (do na izomorfizam)[Nandi, Bhat i Shrikhande]:

Dizajn	C_1	C_2	C_3	C_4	$C_5 \cong PG_2(3, 2)$
#unitala	0	24	0	72	168

Primjer 1.2

Hadamardov dizajn je simetričan $2 - (4n - 1, 2n - 1, n - 1)$ dizajn za $n \geq 2$.
 Hadamardovi $2 - (15, 7, 3)$ dizajni (do na izomorfizam)[Nandi, Bhat i Shrikhande]:

Dizajn	C_1	C_2	C_3	C_4	$C_5 \cong PG_2(3, 2)$
#unitala	0	24	0	72	168

Primjer 1.3

$2 - (56, 11, 2)$ biravnine (do na izomorfizam):

Dizajn	$B_1(11)$	$B_2(11)$	$B_3(11)$	$B_4(11)$	$B_5(11)$
#unitala	13314	2538	462	260	78
Red grupe automorfizama	80640	288	144	64	24

2. Unitali u dizajnama točkaka i hiperravnina, $PG_{d-1}(d, q)$

$PG_{d-1}(d, q)$ je simetričan dizajn točkaka i hiperravnina s parametrima $v = \frac{q^{d+1}-1}{q-1}$, $k = \frac{q^d-1}{q-1}$, $\lambda = \frac{q^{d-1}-1}{q-1}$, gdje je q prim potencija i $d \geq 2$.

2. Unitali u dizajnama točkaka i hiperravnina, $PG_{d-1}(d, q)$

$PG_{d-1}(d, q)$ je simetričan dizajn točkaka i hiperravnina s parametrima $v = \frac{q^{d+1}-1}{q-1}$, $k = \frac{q^d-1}{q-1}$, $\lambda = \frac{q^{d-1}-1}{q-1}$, gdje je q prim potencija i $d \geq 2$.

Teorem 2.1

Ako simetričan dizajn točkaka i hiperravnina, $PG_{d-1}(d, q)$, sadrži unital, tada je $d \in \{2, 3\}$.

2. Unitali u dizajnimu točkama i hiperravnini, $PG_{d-1}(d, q)$

$PG_{d-1}(d, q)$ je simetričan dizajn točkama i hiperravnina s parametrima $v = \frac{q^{d+1}-1}{q-1}$, $k = \frac{q^d-1}{q-1}$, $\lambda = \frac{q^{d-1}-1}{q-1}$, gdje je q prim potencija i $d \geq 2$.

Teorem 2.1

Ako simetričan dizajn točkama i hiperravnina, $PG_{d-1}(d, q)$, sadrži unital, tada je $d \in \{2, 3\}$.

Definicija

Za skup točkama \mathcal{O} projektivne geometrije $P = PG(d, F)$, nad poljem F , kažemo da je *ovoid* ako nikoje tri točke iz \mathcal{O} nisu kolinearne te za svaku točku $T \in \mathcal{O}$ tangencijalni pravci kroz T čine hiperravninu u P .

2. Unitali u dizajnim točkama i hiperravnina, $PG_{d-1}(d, q)$

$PG_{d-1}(d, q)$ je simetričan dizajn točaka i hiperravnina s parametrima $v = \frac{q^{d+1}-1}{q-1}$, $k = \frac{q^d-1}{q-1}$, $\lambda = \frac{q^{d-1}-1}{q-1}$, gdje je q prim potencija i $d \geq 2$.

Teorem 2.1

Ako simetričan dizajn točaka i hiperravnina, $PG_{d-1}(d, q)$, sadrži unital, tada je $d \in \{2, 3\}$.

Definicija

Za skup točaka \mathcal{O} projektivne geometrije $P = PG(d, F)$, nad poljem F , kažemo da je *ovoid* ako nikoje tri točke iz \mathcal{O} nisu kolinearne te za svaku točku $T \in \mathcal{O}$ tangencijalni pravci kroz T čine hiperravninu u P .

Teorem 2.2

Skup točaka \mathcal{U} u $PG_2(3, q)$ je unital akko \mathcal{U} je ovoid u $PG(3, q)$.

3. Hadamardovi dizajni za prim potencije blizance

3. Hadamardovi dizajni za prim potencije blizance

Definicija

Za $x \in GF(p^n)$, $x \neq 0$ kažemo da je *primitivan korijen* tog polja ako je $k = p^n - 1$ najmanji prirodni broj t.d. je $x^k = 1$, p prim broj.

3. Hadamardovi dizajni za prim potencije blizance

Definicija

Za $x \in GF(p^n)$, $x \neq 0$ kažemo da je *primitivan korijen* tog polja ako je $k = p^n - 1$ najmanji prirodni broj t.d. je $x^k = 1$, p prim broj.

Vrijedi:

Svako konačno polje ima primitivan korijen.

Diferencijski skup

Definicija

Neka je G konačna grupa reda v . Neka su $k, \lambda \in \mathbb{N}$ tako da $2 \leq k < v$. k - člani podskup $D \subseteq G$ nazivamo (v, k, λ) - **diferencijski skup** ako multiskup $\{xy^{-1} : x, y \in D, x \neq y\}$ sadrži svaki element osim jedinice točno λ puta.

Diferencijske skupove u Abelovoj (cikličkoj) grupi zovemo Abelovi (ciklički) diferencijski skupovi.

Diferencijski skup

Definicija

Neka je G konačna grupa reda v . Neka su $k, \lambda \in \mathbb{N}$ tako da $2 \leq k < v$. k -člani podskup $D \subseteq G$ nazivamo (v, k, λ) - **diferencijski skup** ako multiskup $\{xy^{-1} : x, y \in D, x \neq y\}$ sadrži svaki element osim jedinice točno λ puta.

Diferencijske skupove u Abelovoj (cikličkoj) grupi zovemo Abelovi (ciklički) diferencijski skupovi.

Definicija

Neka je D (v, k, λ) -diferencijski skup u grupi $(G, +)$ reda v . $\forall g \in G$ skup $D + g = \{x + g : x \in D\}$ nazivamo *translat* od D . Kolekciju od svih v translata od D , u oznaci $Dev(D)$, zovemo *razvoj* od D .

Diferencijski skup

Definicija

Neka je G konačna grupa reda v . Neka su $k, \lambda \in \mathbb{N}$ tako da $2 \leq k < v$. k -člani podskup $D \subseteq G$ nazivamo (v, k, λ) - **diferencijski skup** ako multiskup $\{xy^{-1} : x, y \in D, x \neq y\}$ sadrži svaki element osim jedinice točno λ puta.

Diferencijske skupove u Abelovoj (cikličkoj) grupi zovemo Abelovi (ciklički) diferencijski skupovi.

Definicija

Neka je D (v, k, λ) -diferencijski skup u grupi $(G, +)$ reda v . $\forall g \in G$ skup $D + g = \{x + g : x \in D\}$ nazivamo *translat* od D . Kolekciju od svih v translata od D , u oznaci $Dev(D)$, zovemo *razvoj* od D .

Teorem 3.1 [Ionin, Shrikhande: *Combinatorics of Symmetric Designs*, 2006.]

k -člani podskup D grupe G reda v je (v, k, λ) -diferencijski skup akko incidencijska struktura $(G, Dev(D), I)$ je simetričan $2 - (v, k, \lambda)$ dizajn.

Konstrukcija diferencijskih skupova, Stanton i Sprott

[Prema članku Stanton, Sprott: A family of difference sets, Canad.J.Math.Vol.10, 1958.]

Neka je dana *Galoisova domena* $GD(v)$, odnosno skup od v elemenata (α, β) takvih da $\alpha \in GF(h)$ i $\beta \in GF(h+2)$, gdje su $h = p^n$ i $h+2 = q^m$ prim potencije, na kojem su definirane operacije "zbrajanja" i "množenja" ovako:

$$(\alpha_1, \beta_1) + (\alpha_2, \beta_2) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2)$$

$$(\alpha_1, \beta_1) \cdot (\alpha_2, \beta_2) = (\alpha_1 \cdot \alpha_2, \beta_1 \cdot \beta_2).$$

Konstrukcija diferencijskih skupova, Stanton i Sprott

[Prema članku Stanton, Sprott: A family of difference sets, Canad.J.Math.Vol.10, 1958.]

Neka je dana *Galoisova domena* $GD(v)$, odnosno skup od v elemenata (α, β) takvih da $\alpha \in GF(h)$ i $\beta \in GF(h+2)$, gdje su $h = p^n$ i $h+2 = q^m$ prim potencije, na kojem su definirane operacije "zbrajanja" i "množenja" ovako:

$$(\alpha_1, \beta_1) + (\alpha_2, \beta_2) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2)$$

$$(\alpha_1, \beta_1) \cdot (\alpha_2, \beta_2) = (\alpha_1 \cdot \alpha_2, \beta_1 \cdot \beta_2).$$

$GD(v)$ je prsten. Posebno, $GD(v)$ je aditivna Abelova grupa.

Konstrukcija diferencijskih skupova, Stanton i Sprott

[Prema članku Stanton, Sprott: A family of difference sets, Canad.J.Math.Vol.10, 1958.]

Neka je dana *Galoisova domena* $GD(v)$, odnosno skup od v elemenata (α, β) takvih da $\alpha \in GF(h)$ i $\beta \in GF(h+2)$, gdje su $h = p^n$ i $h+2 = q^m$ prim potencije, na kojem su definirane operacije "zbrajanja" i "množenja" ovako:

$$(\alpha_1, \beta_1) + (\alpha_2, \beta_2) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2)$$

$$(\alpha_1, \beta_1) \cdot (\alpha_2, \beta_2) = (\alpha_1 \cdot \alpha_2, \beta_1 \cdot \beta_2).$$

$GD(v)$ je prsten. Posebno, $GD(v)$ je aditivna Abelova grupa.

Označimo s ζ , θ primitivan korijen redom polja $GF(h)$ i $GF(h+2)$.

Istaknimo neke elemente u $GD(v)$: $z^i = (\zeta^i, \theta^i)$, $\omega^i = (\zeta^i, 0)$ i $0 = (0, 0)$.

Posebno, $\zeta^i \zeta^j = \zeta^{i+j}$.

Konstrukcija diferencijskih skupova, Stanton i Sprott

[Prema članku Stanton, Sprott: A family of difference sets, Canad.J.Math.Vol.10, 1958.]

Neka je dana *Galoisova domena* $GD(v)$, odnosno skup od v elemenata (α, β) takvih da $\alpha \in GF(h)$ i $\beta \in GF(h+2)$, gdje su $h = p^n$ i $h+2 = q^m$ prim potencije, na kojem su definirane operacije "zbrajanja" i "množenja" ovako:

$$(\alpha_1, \beta_1) + (\alpha_2, \beta_2) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2)$$

$$(\alpha_1, \beta_1) \cdot (\alpha_2, \beta_2) = (\alpha_1 \cdot \alpha_2, \beta_1 \cdot \beta_2).$$

$GD(v)$ je prsten. Posebno, $GD(v)$ je aditivna Abelova grupa.

Označimo s ζ, θ primitivan korijen redom polja $GF(h)$ i $GF(h+2)$.

Istaknimo neke elemente u $GD(v)$: $z^i = (\zeta^i, \theta^i)$, $\omega^i = (\zeta^i, 0)$ i $0 = (0, 0)$.

Posebno, $\zeta^i \zeta^j = \zeta^{i+j}$.

Teorem 3.2

Skup $D = \{z^0, z, z^2, \dots, z^{\frac{1}{2}(h^2-1)-1}, 0, \omega^0, \omega, \dots, \omega^{h-2}\}$ je Abelov diferencijski skup u $GD(v)$ s parametrima $v = h(h+2)$, $k = \frac{1}{2}(v-1)$, $\lambda = \frac{1}{4}(v-3)$.

Definicija

Prim potencije blizanci su dvije neparne prim potencije oblika h i $h + 2$.

Definicija

Prim potencije blizanci su dvije neparne prim potencije oblika h i $h + 2$.

Stoga, možemo pisati da je skup $D = \{z^0, z, z^2, \dots, z^{\frac{h^2-3}{2}}, 0, \omega^0, \omega, \dots, \omega^{h-2}\}$
 $\left(4 \left(\frac{h+1}{2}\right)^2 - 1, 2 \left(\frac{h+1}{2}\right)^2 - 1, \left(\frac{h+1}{2}\right)^2 - 1\right)$ -diferencijski skup u grupi
 $GD(h(h+2))$.

Definicija

Prim potencije blizanci su dvije neparne prim potencije oblika h i $h + 2$.

Stoga, možemo pisati da je skup $D = \{z^0, z, z^2, \dots, z^{\frac{h^2-3}{2}}, 0, \omega^0, \omega, \dots, \omega^{h-2}\}$
 $\left(4\left(\frac{h+1}{2}\right)^2 - 1, 2\left(\frac{h+1}{2}\right)^2 - 1, \left(\frac{h+1}{2}\right)^2 - 1\right)$ -diferencijski skup u grupi
 $GD(h(h+2))$.

Stavimo li $t = \frac{h+1}{2}$, tada incidencijska struktura dobivena od D je
 Hadamardov $2 - (4t^2 - 1, 2t^2 - 1, t^2 - 1)$ dizajn kojega nazivamo
Hadamardov dizajn za prim potencije blizance ($h = 2t - 1$ i $h + 2 = 2t + 1$).

Definicija

Prim potencije blizanci su dvije neparne prim potencije oblika h i $h + 2$.

Stoga, možemo pisati da je skup $D = \{z^0, z, z^2, \dots, z^{\frac{h^2-3}{2}}, 0, \omega^0, \omega, \dots, \omega^{h-2}\}$
 $(4(\frac{h+1}{2})^2 - 1, 2(\frac{h+1}{2})^2 - 1, (\frac{h+1}{2})^2 - 1)$ -diferencijski skup u grupi
 $GD(h(h+2))$.

Stavimo li $t = \frac{h+1}{2}$, tada incidencijska struktura dobivena od D je Hadamardov $2 - (4t^2 - 1, 2t^2 - 1, t^2 - 1)$ dizajn kojega nazivamo *Hadamardov dizajn za prim potencije blizance* ($h = 2t - 1$ i $h + 2 = 2t + 1$).

Teorem 3.3

Hadamardov dizajn za prim potencije blizance sadrži unital.

Primjeri

Primjer 3.1

Uzmemo li $h = 7$, tada će Hadamardov dizajn za prim potencije blizance $2 - (63, 31, 15)$ sadržavati unitale. Parametri su mu isti kao i za $PG_4(5, 2)$ koji ne sadrži unitale. U ovom primjeru $(63, 31, 15)$ - diferencijski skup konstruiran iz grupe $Z_7 \times Z_3 \times Z_3$, koji nije izomorfan s cikličkim diferencijskim skupom.

Primjeri

Primjer 3.1

Uzmemo li $h = 7$, tada će Hadamardov dizajn za prim potencije blizance $2 - (63, 31, 15)$ sadržavati unitale. Parametri su mu isti kao i za $PG_4(5, 2)$ koji ne sadrži unitale. U ovom primjeru $(63, 31, 15)$ - diferencijski skup konstruiran iz grupe $Z_7 \times Z_3 \times Z_3$, koji nije izomorfan s cikličkim diferencijskim skupom.

Primjer 3.2

[*M.Hall: A survey of difference sets, Proc.Amer.Math.Soc, Vol.7 (1956.)*]

Hall je pokazao da postoji još jedan $2 - (63, 31, 15)$ dizajn, koji nije izomorfan s $PG_4(5, 2)$, dobiven iz cikličkog diferencijskog skupa:

$H = (0, 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 16, 17, 18, 20, 23, 24, 27, 29, 32, 33, 34, 36, 40, 43, 45, 46, 48, 53, 54, 58) \pmod{63}$.

Lako se pokaže da je $\mathcal{U} = \{0, 7, 14, 21, 28, 35, 42, 49, 56\}$ unital u danom dizajnu.

4. Familija simetričnih dizajna s parametrima

$$2 - (4t^2, 2t^2 - t, t^2 - t)$$

[Shrikhande: *On a two-parameter family of balanced incomplete block designs*, *Sankhya A*, Vol.24(1962.)]

Shrikhande je konstruirao familiju simetričnih Menonovih

$2 - (4t^2, 2t^2 - t, t^2 - t)$ dizajna za $2t - 1$ i $2t + 1$ prim potencije blizance.

4. Familija simetričnih dizajna s parametrima

$$2 - (4t^2, 2t^2 - t, t^2 - t)$$

[Shrikhande: *On a two-parameter family of balanced incomplete block designs*, *Sankhya A*, Vol.24(1962.)]

Shrikhande je konstruirao familiju simetričnih Menonovih

$2 - (4t^2, 2t^2 - t, t^2 - t)$ dizajna za $2t - 1$ i $2t + 1$ prim potencije blizance.

Teorem 4.1

Ako su $h = 2t - 1$ i $h + 2$ prim potencije blizanci, tada postoji simetričan $2 - (4t^2, 2t^2 - t, t^2 - t)$ dizajn koji sadrži unitale.

$$2 - (q^2(q+2), q(q^2+q-1), q(q^2-1))$$

5. Familija simetričnih dizajna s parametrima

$$2 - (q^2(q+2), q(q^2+q-1), q(q^2-1))$$

5. Familija simetričnih dizajna s parametrima

$$2 - (q^2(q+2), q(q^2+q-1), q(q^2-1))$$

Definicija

Baerov poddizajn \mathcal{D}^* simetričnog $2 - (v, k, \lambda)$ dizajna \mathcal{D} je $2 - (v^*, k^*, \lambda)$ simetričan poddizajn od \mathcal{D} za koji vrijedi $k^* = 1 + \sqrt{k - \lambda}$.

5. Familija simetričnih dizajna s parametrima

$$2 - (q^2(q+2), q(q^2+q-1), q(q^2-1))$$

Definicija

Baerov poddizajn \mathcal{D}^* simetričnog $2 - (v, k, \lambda)$ dizajna \mathcal{D} je $2 - (v^*, k^*, \lambda)$ simetričan poddizajn od \mathcal{D} za koji vrijedi $k^* = 1 + \sqrt{k - \lambda}$.

Teorem 5.1 [Ionin, Shrikhande: *Combinatorics of Symmetric Designs*, 2006.]

$2 - (v_1, k_1, \lambda)$ poddizajn $\mathcal{D}_1 = (\mathcal{P}_1, \mathcal{B}_1, I)$ simetričnog $2 - (v, k, \lambda)$ dizajna $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$, $v_1 < v$, je Baerov poddizajn od \mathcal{D} ako i samo ako $\forall B \in \mathcal{B} \setminus \mathcal{B}_1$ sadrži točno jednu točku iz \mathcal{D}_1 .

5. Familija simetričnih dizajna s parametrima

$$2 - (q^2(q+2), q(q^2+q-1), q(q^2-1))$$

Definicija

Baerov poddizajn \mathcal{D}^* simetričnog $2 - (v, k, \lambda)$ dizajna \mathcal{D} je $2 - (v^*, k^*, \lambda)$ simetričan poddizajn od \mathcal{D} za koji vrijedi $k^* = 1 + \sqrt{k - \lambda}$.

Teorem 5.1 [Ionin, Shrikhande: *Combinatorics of Symmetric Designs*, 2006.]

$2 - (v_1, k_1, \lambda)$ poddizajn $\mathcal{D}_1 = (\mathcal{P}_1, \mathcal{B}_1, I)$ simetričnog $2 - (v, k, \lambda)$ dizajna $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$, $v_1 < v$, je Baerov poddizajn od \mathcal{D} ako i samo ako $\forall B \in \mathcal{B} \setminus \mathcal{B}_1$ sadrži točno jednu točku iz \mathcal{D}_1 .

Svaki blok u \mathcal{D} presjeca Baerov poddizajn \mathcal{D}^* u 1 ili k^* točaka.
Kroz svaku točku iz \mathcal{D}^* prolazi k^* sekanti i $k - k^*$ tangenti.

5. Familija simetričnih dizajna s parametrima

$$2 - (q^2(q+2), q(q^2+q-1), q(q^2-1))$$

Definicija

Baerov poddizajn \mathcal{D}^* simetričnog $2 - (v, k, \lambda)$ dizajna \mathcal{D} je $2 - (v^*, k^*, \lambda)$ simetričan poddizajn od \mathcal{D} za koji vrijedi $k^* = 1 + \sqrt{k - \lambda}$.

Teorem 5.1 [Ionin, Shrikhande: *Combinatorics of Symmetric Designs*, 2006.]

$2 - (v_1, k_1, \lambda)$ poddizajn $\mathcal{D}_1 = (\mathcal{P}_1, \mathcal{B}_1, I)$ simetričnog $2 - (v, k, \lambda)$ dizajna $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$, $v_1 < v$, je Baerov poddizajn od \mathcal{D} ako i samo ako $\forall B \in \mathcal{B} \setminus \mathcal{B}_1$ sadrži točno jednu točku iz \mathcal{D}_1 .

Svaki blok u \mathcal{D} presjeca Baerov poddizajn \mathcal{D}^* u 1 ili k^* točaka.
Kroz svaku točku iz \mathcal{D}^* prolazi k^* sekanti i $k - k^*$ tangenti.

Neka Baerov poddizajn \mathcal{D}^* ima parametre $2 - (t+2, t+1, t)$, odnosno neka je trivijalni dizajn. Tada je \mathcal{D} $2 - (t^2(t+2), t(t+1), t)$ dizajn.

Komplementaran dizajn simetričnog $2 - (v, k, \lambda)$ dizajna \mathcal{D} je simetričan dizajn $\bar{\mathcal{D}}$ koji se dobije iz \mathcal{D} "zamjenom incidencije".

Teorem 5.2

Ako je \mathcal{D} je simetričan $2 - (v, k, \lambda)$ dizajn, tada $\bar{\mathcal{D}}$ ima parametre $2 - (v, v - k, v - 2k + \lambda)$.

Teorem 5.2

Ako je \mathcal{D} je simetričan $2 - (v, k, \lambda)$ dizajn, tada $\bar{\mathcal{D}}$ ima parametre $2 - (v, v - k, v - 2k + \lambda)$.

U našem slučaju $\bar{\mathcal{D}}$ je simetričan $2 - (t^2(t+2), t(t^2+t-1), t(t^2-1))$ dizajn.

Teorem 5.2

Ako je \mathcal{D} je simetričan $2 - (v, k, \lambda)$ dizajn, tada $\bar{\mathcal{D}}$ ima parametre $2 - (v, v - k, v - 2k + \lambda)$.

U našem slučaju $\bar{\mathcal{D}}$ je simetričan $2 - (t^2(t+2), t(t^2+t-1), t(t^2-1))$ dizajn.

Svaki blok iz $\bar{\mathcal{D}}$ presjeca \mathcal{D}^* u 1 ili $(t+1)$ točaka. \mathcal{D}^* ima $(t+2)$ točke. Točke iz \mathcal{D}^* čine unital u $\bar{\mathcal{D}}$.

Teorem 5.2

Ako je \mathcal{D} je simetričan $2 - (v, k, \lambda)$ dizajn, tada $\bar{\mathcal{D}}$ ima parametre $2 - (v, v - k, v - 2k + \lambda)$.

U našem slučaju $\bar{\mathcal{D}}$ je simetričan $2 - (t^2(t+2), t(t^2+t-1), t(t^2-1))$ dizajn.

Svaki blok iz $\bar{\mathcal{D}}$ presjeca \mathcal{D}^* u 1 ili $(t+1)$ točaka. \mathcal{D}^* ima $(t+2)$ točke. Točke iz \mathcal{D}^* čine unital u $\bar{\mathcal{D}}$.

Teorem 5.3

Ako je q prim potencija, tada postoji familija simetričnih dizajna s parametrima $2 - (q^2(q+2), q(q^2+q-1), q(q^2-1))$ koji sadrže unitale.

6. Unitarni polaritet simetričnog dizajna

6. Unitarni polaritet simetričnog dizajna

Definicija

Polaritet simetričnog dizajna čije apsolutne točke čine unital nazivamo unitarni polaritet.

6. Unitarni polaritet simetričnog dizajna

Definicija

Polaritet simetričnog dizajna čije apsolutne točke čine unital nazivamo unitarni polaritet.

Lema 6.1 [*Hughes, Piper: Design Theory, 1985.*]

Neka je D simetričan $2 - (v, k, \lambda)$ dizajn s polaritetom σ . Tada je $a(\sigma)$, broj apsolutnih točaka od σ jednak:

$$a(\sigma) = k + s\sqrt{n} - (v - 1 - s)\sqrt{n}$$

gdje je $n = k - \lambda$ i s je cijeli broj za koji vrijedi $\frac{1}{2}(v - 1 - \frac{k}{\sqrt{n}}) \leq s \leq v - 1$.

6. Unitarni polaritet simetričnog dizajna

Definicija

Polaritet simetričnog dizajna čije apsolutne točke čine unital nazivamo unitarni polaritet.

Lema 6.1 [Hughes, Piper: Design Theory, 1985.]

Neka je D simetričan $2 - (v, k, \lambda)$ dizajn s polaritetom σ . Tada je $a(\sigma)$, broj apsolutnih točaka od σ jednak:

$$a(\sigma) = k + s\sqrt{n} - (v - 1 - s)\sqrt{n}$$

gdje je $n = k - \lambda$ i s je cijeli broj za koji vrijedi $\frac{1}{2}(v - 1 - \frac{k}{\sqrt{n}}) \leq s \leq v - 1$.

Lema 6.2

Ako simetričan $2 - (v, k, \lambda)$ dizajn dopušta unitarni polaritet, tada $s = \frac{k-1}{2\lambda}(k + 1 - \frac{\lambda}{\sqrt{n}})$ je cijeli broj.

Napomena [*Mathon, Spence: On $2 - (45, 12, 3)$ designs, J. Combin. Des., Vol.4(1996.)*]

Pronađeno je puno polariteta u $2 - (45, 12, 3)$ dizajnu s 12 apsolutnih točaka koji nisu unitarni.

Napomena [*Mathon, Spence: On $2 - (45, 12, 3)$ designs, J. Combin. Des., Vol.4(1996.)*]

Pronađeno je puno polariteta u $2 - (45, 12, 3)$ dizajnu s 12 apsolutnih točaka koji nisu unitarni.

Propozicija 6.3

Neka je q prim potencija. Ako simetričan $2 - \left(\frac{q^4-1}{q-1}, \frac{q^3-1}{q-1}, \frac{q^2-1}{q-1}\right)$ dizajn ima unitarni polaritet, tada je q neparan. Posebno, $PG_2(3, 2^n)$ nema unitale dobivene iz polariteta, $n \in \mathbb{N}$.

Dobiveni rezultat za simetričan 2 – (45, 12, 3) dizajn

Dobiveni rezultat za simetričan $2 - (45, 12, 3)$ dizajn

Do na izomorfizam postoji točno jedan simetričan $2 - (45, 12, 3)$ dizajn s punom grupom automorfizama reda 11, konstruirao [*Mathon, Computational methods in design theory, Surveys in Combinatorics 1991.*]. Taj dizajn označimo s $D(11)$.

Dobiveni rezultat za simetričan $2 - (45, 12, 3)$ dizajn

Do na izomorfizam postoji točno jedan simetričan $2 - (45, 12, 3)$ dizajn s punom grupom automorfizama reda 11, konstruirao [*Mathon, Computational methods in design theory, Surveys in Combinatorics 1991.*].

Taj dizajn označimo s $D(11)$.

Teorem 6.4

Jedinstveni simetričan $2 - (45, 12, 3)$ dizajn s punom grupom automorfizama reda 11 ima 3 unitala. Točno jedan od njih je dobiven iz unitarnog polariteta.

Dobiveni rezultat za simetričan $2 - (45, 12, 3)$ dizajn

Do na izomorfizam postoji točno jedan simetričan $2 - (45, 12, 3)$ dizajn s punom grupom automorfizama reda 11, konstruirao [*Mathon, Computational methods in design theory, Surveys in Combinatorics 1991.*].

Taj dizajn označimo s $D(11)$.

Teorem 6.4

Jedinstveni simetričan $2 - (45, 12, 3)$ dizajn s punom grupom automorfizama reda 11 ima 3 unitala. Točno jedan od njih je dobiven iz unitarnog polariteta.

DOKAZ

Neka je automorfizam ρ reda 11 koji djeluje na točke dizajna $D(11)$ kao što slijedi: $\rho = (0, \dots, 10)(11, \dots, 21)(22, \dots, 32)(33, \dots, 43)(44)$

$D(11)$ - jedinstveni 2 – (45, 12, 3) dizajn s punom grupom automorfizama reda 11.

0	9	10	1	2	19	31	24	26	30	35	38	40
1	10	0	2	3	20	32	25	27	31	36	39	41
2	0	1	3	4	21	22	26	28	32	37	40	42
3	1	2	4	5	11	23	27	29	22	38	41	43
4	2	3	5	6	12	24	28	30	23	39	42	33
5	3	4	6	7	13	25	29	31	24	40	43	34
6	4	5	7	8	14	26	30	32	25	41	33	35
7	5	6	8	9	15	27	31	22	26	42	34	36
8	6	7	9	10	16	28	32	23	27	43	35	37
9	7	8	10	0	17	29	22	24	28	33	36	38
10	8	9	0	1	18	30	23	25	29	34	37	39
11	3	14	15	18	19	25	26	28	23	36	38	43
12	4	15	16	19	20	26	27	29	24	37	39	33
13	5	16	17	20	21	27	28	30	25	38	40	34
14	6	17	18	21	11	28	29	31	26	39	41	35
15	7	18	19	11	12	29	30	32	27	40	42	36
16	8	19	20	12	13	30	31	22	28	41	43	37
17	9	20	21	13	14	31	32	23	29	42	33	38
18	10	21	11	14	15	32	22	24	30	43	34	39
19	0	11	12	15	16	22	23	25	31	33	35	40
20	1	12	13	16	17	23	24	26	32	34	36	41
21	2	13	14	17	18	24	25	27	22	35	37	42

22	2	3	7	9	16	18	19	21	22	41	33	34
23	3	4	8	10	17	19	20	11	23	42	34	35
24	4	5	9	0	18	20	21	12	24	43	35	36
25	5	6	10	1	19	21	11	13	25	33	36	37
26	6	7	0	2	20	11	12	14	26	34	37	38
27	7	8	1	3	21	12	13	15	27	35	38	39
28	8	9	2	4	11	13	14	16	28	36	39	40
29	9	10	3	5	12	14	15	17	29	37	40	41
30	10	0	4	6	13	15	16	18	30	38	41	42
31	0	1	5	7	14	16	17	19	31	39	42	43
32	1	2	6	8	15	17	18	20	32	40	43	33
33	4	6	9	17	19	12	32	22	25	38	39	44
34	5	7	10	18	20	13	22	23	26	39	40	44
35	6	8	0	19	21	14	23	24	27	40	41	44
36	7	9	1	20	11	15	24	25	28	41	42	44
37	8	10	2	21	12	16	25	26	29	42	43	44
38	9	0	3	11	13	17	26	27	30	43	33	44
39	10	1	4	12	14	18	27	28	31	33	34	44
40	0	2	5	13	15	19	28	29	32	34	35	44
41	1	3	6	14	16	20	29	30	22	35	36	44
42	2	4	7	15	17	21	30	31	23	36	37	44
43	3	5	8	16	18	11	31	32	24	37	38	44
44	33	34	35	36	37	38	39	40	41	42	43	44

22	2	3	7	9	16	18	19	21	22	41	33	34
23	3	4	8	10	17	19	20	11	23	42	34	35
24	4	5	9	0	18	20	21	12	24	43	35	36
25	5	6	10	1	19	21	11	13	25	33	36	37
26	6	7	0	2	20	11	12	14	26	34	37	38
27	7	8	1	3	21	12	13	15	27	35	38	39
28	8	9	2	4	11	13	14	16	28	36	39	40
29	9	10	3	5	12	14	15	17	29	37	40	41
30	10	0	4	6	13	15	16	18	30	38	41	42
31	0	1	5	7	14	16	17	19	31	39	42	43
32	1	2	6	8	15	17	18	20	32	40	43	33
33	4	6	9	17	19	12	32	22	25	38	39	44
34	5	7	10	18	20	13	22	23	26	39	40	44
35	6	8	0	19	21	14	23	24	27	40	41	44
36	7	9	1	20	11	15	24	25	28	41	42	44
37	8	10	2	21	12	16	25	26	29	42	43	44
38	9	0	3	11	13	17	26	27	30	43	33	44
39	10	1	4	12	14	18	27	28	31	33	34	44
40	0	2	5	13	15	19	28	29	32	34	35	44
41	1	3	6	14	16	20	29	30	22	35	36	44
42	2	4	7	15	17	21	30	31	23	36	37	44
43	3	5	8	16	18	11	31	32	24	37	38	44
44	33	34	35	36	37	38	39	40	41	42	43	44

Jedinstveni unitarni polaritet π definiran je $\pi : i \mapsto \mathbf{i}$. Njegove apsolutne točke 22, 23, ..., 32, 44 i neapsolutni blokovi čine $2 - (12, 4, 3)$ unital.

Druga dva unitala koja nisu dobivena iz unitarnog polariteta su $\{0, \dots, 10, 44\}$ i $\{11, \dots, 22, 44\}$.

Familije simetričnih dizajna čiji parametri ispunjavaju nužan aritmetički uvjet u lemi 6.2 za egzistenciju unitarnih polariteta:

1. Projektivne ravnine kvadratnog reda

$$v = n^4 + n^2 + 1, k = n^2 + 1, \lambda = 1.$$

2. Dizajni s parametrima kao $PG_2(3, q)$

$$v = q^3 + q^2 + q + 1, k = q^2 + q + 1, \lambda = q + 1, n = q^2, q \text{ je neparna prim potencija.}$$

3. Diferencijski skupovi [*Menon: On difference sets whose parameters satisfy a certain relation, Proc.Amer.Math.Soc., 1962.*]

$$v = 4t^2, k = 2t^2 - t, \lambda = t^2 - t, n = t^2. \quad (\text{Ali, } s = 2t^2 - t + \frac{1}{t} + 1)$$

4. Wallisovi dizajni

$$v = q^{m+1}(q^m + \dots + q + 2), k = q^m(q^m + \dots + q + 1), \lambda = q^m(q^{m-1} + \dots + q + 1), n = q^{2m}, q \text{ je prim potencija, } m \text{ je pozitivan cijeli broj. (Ali za } q = 3 \text{ i } m = 2, \text{ tada}$$

$$s = \frac{551}{3}, \text{ jer } s = \frac{[q^m(q^{m+1}-1)-q+1][q^{m-1}(q^{m+1}-1)+1-q^{m-1}]}{2q^{m-1}(q^m-1)(q-1)}.)$$

5. [*Spence: A family of difference sets in non-cyclic groups, J.Comb.Theory A, 1977.*]

$$v = \frac{3^m(3^m-1)}{2}, k = \frac{3^{m-1}(3^m+1)}{2}, \lambda = \frac{3^{m-1}(3^{m-1}+1)}{2},$$

$$n = 3^{2(m-1)}, \text{ a } \frac{3^m+1}{2} \text{ je neparan broj.}$$

$$(\text{Ali, } s = \frac{1}{4}3^{-m}(3^m - 2)(9^m + 3), \text{ što za } m = 2 \text{ daje } s = \frac{49}{3})$$

n	v	k	λ	Unital	Unitarni polaritet
4	21	5	1	da	da, $PG(2, 4)$
4	16	6	2	da, primjer 1.1	ne
4	15	7	3	da, primjer 1.2	ne, lema 6.2
9	56	11	2	da, primjer 1.3	ne, lema 6.2
9	45	12	3	da	da, teorem 6.4
9	40	13	4	da	da, $PG_2(3, 3)$
9	36	15	6	da	?
9	35	17	8	da, teorem 3.3	ne, lema 6.2
16	273	17	1	da	da, $PG(2, 16)$
16	154	18	2	?	ne, lema 6.2
16	115	19	3	?	ne, lema 6.2
16	96	20	4	?	?
16	85	21	5	da	ne, lema 6.2
16	78	22	6	?	ne, lema 6.2
16	70	24	8	ne, lema 1.1	
16	66	26	10	da	ne, lema 6.2
16	64	28	12	da, teorem 4.1	?
16	63	31	15	da, teorem 3.3	ne, lema 6.2
25	651	26	1	da	da, $PG(2, 25)$
25	352	27	2	?	ne, lema 6.2
25	253	28	3	?	ne, lema 6.2
25	204	29	4	?	ne, lema 6.2
25	175	30	5	?	?
25	156	31	6	da	da, $PG_2(3, 5)$
25	133	33	8	?	ne, lema 6.2
25	120	35	10	?	?
25	112	37	12	?	ne, lema 6.2
25	105	40	15	?	?
25	100	45	20	da, teorem 4.1	?
25	99	49	24	da, teorem 3.3	ne, lema 6.2

Tablica 1, R. Mathon i T.van Trung

n	v	k	λ	Unital	Unitarni polaritet
4	21	5	1	da	da, $PG(2, 4)$
4	16	6	2	da, primjer 1.1	ne, lema 6.2
4	15	7	3	da, primjer 1.2	ne, lema 6.2
9	56	11	2	da, primjer 1.3	ne, lema 6.2
9	45	12	3	da	da, teorem 6.4
9	40	13	4	da	da, $PG_2(3, 3)$
9	36	15	6	da	ne, lema 6.2
9	35	17	8	da, teorem 3.3	ne, lema 6.2
16	273	17	1	da	da, $PG(2, 16)$
16	154	18	2	?	ne, lema 6.2
16	115	19	3	?	ne, lema 6.2
16	96	20	4	?	ne, lema 6.2
16	85	21	5	da	ne, lema 6.2
16	78	22	6	?	ne, lema 6.2
16	70	24	8	ne, lema 1.1	
16	66	26	10	da	ne, lema 6.2
16	64	28	12	da, teorem 4.1	ne, lema 6.2
16	63	31	15	da, teorem 3.3	ne, lema 6.2
25	651	26	1	da	da, $PG(2, 25)$
25	352	27	2	?	ne, lema 6.2
25	253	28	3	?	ne, lema 6.2
25	204	29	4	?	ne, lema 6.2
25	175	30	5	?	?
25	156	31	6	da	da, $PG_2(3, 5)$
25	133	33	8	?	ne, lema 6.2
25	120	35	10	?	ne, lema 6.2
25	112	37	12	?	ne, lema 6.2
25	105	40	15	?	ne, lema 6.2
25	100	45	20	da, teorem 4.1	ne, lema 6.2
25	99	49	24	da, teorem 3.3	ne, lema 6.2

Tablica 2: Promjena tablice 1

2 – (36, 15, 6) dizajn

Točke: $\infty, i_0, i_1, i_2, i_3, i_4, i_5, i_6, i = 1, 2, 3, 4, 5$

Automorfizam: $\rho = (\infty)(i_0, i_1, i_2, i_3, i_4, i_5, i_6), i = 1, 2, 3, 4, 5$

Bazni blokovi:

$\infty 1_0 1_1 1_2 1_3 1_4 1_5 1_6 2_0 2_1 2_2 2_3 2_4 2_5 2_6$

$\infty 1_0 1_1 1_2 1_4 2_0 3_1 3_2 3_4 4_3 4_6 4_5 5_1 5_2 5_4$

$\infty 2_0 2_1 2_2 2_4 1_0 4_1 4_2 4_4 3_3 3_6 3_5 5_1 5_2 5_4$

$1_1 1_2 1_4 2_3 2_6 2_5 3_0 3_3 3_6 3_5 4_0 5_0 5_1 5_2 5_4$

$2_1 2_2 2_4 1_3 1_6 1_5 4_0 4_3 4_6 4_5 3_0 5_0 5_1 5_2 5_4$

$1_1 1_2 1_4 2_1 2_2 2_4 3_0 3_1 3_2 3_4 4_0 4_1 4_2 4_4 5_0$

Unital čini fiksna točka ∞ zajedno s 7 točaka iz orbite 3, 4 ili 5 od ρ , npr.

$\mathcal{U} = \{\infty, 3_0, 3_1, 3_2, 3_3, 3_4, 3_5, 3_6\}$ je unital.

2 – (36, 15, 6) dizajn

Točke: $\infty, i_0, i_1, i_2, i_3, i_4, i_5, i_6, i = 1, 2, 3, 4, 5$

Automorfizam: $\rho = (\infty)(i_0, i_1, i_2, i_3, i_4, i_5, i_6), i = 1, 2, 3, 4, 5$

Bazni blokovi:

$\infty 1_0 1_1 1_2 1_3 1_4 1_5 1_6 2_0 2_1 2_2 2_3 2_4 2_5 2_6$

$\infty 1_0 1_1 1_2 1_4 2_0 3_1 3_2 3_4 4_3 4_6 4_5 5_1 5_2 5_4$

$\infty 2_0 2_1 2_2 2_4 1_0 4_1 4_2 4_4 3_3 3_6 3_5 5_1 5_2 5_4$

$1_1 1_2 1_4 2_3 2_6 2_5 3_0 3_3 3_6 3_5 4_0 5_0 5_1 5_2 5_4$

$2_1 2_2 2_4 1_3 1_6 1_5 4_0 4_3 4_6 4_5 3_0 5_0 5_1 5_2 5_4$

$1_1 1_2 1_4 2_1 2_2 2_4 3_0 3_1 3_2 3_4 4_0 4_1 4_2 4_4 5_0$

Unital čini fiksna točka ∞ zajedno s 7 točaka iz orbite 3, 4 ili 5 od ρ , npr.

$\mathcal{U} = \{\infty, 3_0, 3_1, 3_2, 3_3, 3_4, 3_5, 3_6\}$ je unital.

2-(66,26,10) dizajn [Tran van Trung] Točke: $1_i, \dots, 6_i, i = 0, 1, \dots, 10$

Automorfizmi: $\rho = (1_0, 1_1, \dots, 1_{10}), l = 1, 2, \dots, 6$ i $\sigma = (1_i, 2_i, 3_i, 4_i, 5_i)(6_i)$

Bazni blokovi:

$1_1 1_3 1_4 1_5 1_9 2_2 2_6 2_7 2_8 2_{10} 3_2 3_6 3_7 3_8 3_{10} 4_1 4_3 4_4 4_5 4_9 5_0 6_1 6_3 6_4 6_5 6_9$

$1_2 1_6 1_7 1_8 1_{10} 2_2 2_6 2_7 2_8 2_{10} 3_2 3_6 3_7 3_8 3_{10} 4_2 4_6 4_7 4_8 4_{10} 5_2 5_6 5_7 5_8 5_{10} 6_0$

Unitali: svaka od 6 orbita točaka od ρ čini unital.