Sveučilište u Zagrebu

PMF - Matematički odjel

Ante Ćustić

Popločavanje grupa diferencijskim skupovima

Diplomski rad

Zagreb, svibanj 2010.

Sveučilište u Zagrebu

PMF - Matematički odjel

Ante Ćustić

Popločavanje grupa diferencijskim skupovima

Diplomski rad

Voditelj rada:
doc. dr. sc. Vedran Krčadinac

Zagreb, svibanj 2010.

Ovaj diplomski rad obranjen je dana _____ pred nastavničkim povjerenstvom u sastavu:

1. _____ , predsjednik
2. _____ , član
3. _____ , član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

U ovom radu definira se i proučava jedan način popločavanja grupa diferencijskim skupovima.

U prvom poglavlju proučavaju se diferencijski skupovi. Predstavljene su najpoznatije činjenice o diferencijskim skupovima s naglaskom na rezultate koji će se koristiti u drugom poglavlju. Opisana je veza između diferencijskih skupova i simetričnih blokovnih dizajna, navedeno je nekoliko konstrukcija klasičnih familija diferencijskih skupova i obrađen pojam multiplikatora.

U drugom poglavlju definirano je popločavanje grupa diferencijskim skupovima koje nazivamo (v, k, λ)-ogrlicama. Dokazani su neki nužni uvjeti postojanja takvih struktura. Proučena je i prikazana konstrukcija više klasa (v, k, λ)-ogrlica u Abelovim grupama. Za jednu od njih dokazana je beskonačnost. Svi rezultati popraćeni su ilustrativnim primjerima. Priloženi su i primjeri (v, k, λ)-ogrlica u neabelovim grupama pronađeni kompjuterskom pretragom.

Na kraju rada priložen je dodatak u kojem je navedena tablica svih pronađenih (v, k, λ)-ogrlica za $v \leq 200$.

Zahvaljujem profesoru Vedranu Krčadincu na pomoći i savjetima pri izradi rada, a posebno na poticanju mog istrazivanja ove teme.

1 Diferencijski skupovi

1.1 Diferencijski skupovi i simetrični dizajni

Osnovni objekti naših razmatranja su *diferencijski skupovi.* Prvo ćemo navesti definiciju i nekoliko primjera.

Definicija 1.1. *Neka je (G,+) konačna grupa reda v s neutralnim elementom "0". Neka su k i λ pozitivni cijeli brojevi takvi da $2 \leq k < v$. Za $D \subseteq G$ kažemo da je (v, k, λ)-diferencijski skup u (G,+) ako vrijedi:*

1. $|D| = k$,
2. *multiskup $[x - y : x, y \in D, x \neq y]$ sadrži svaki element od $G \setminus \{0\}$ točno λ puta.*

Primjer 1.1

$(13, 4, 1)$-diferencijski skup u $(\mathbb{Z}_{13}, +)$:

$$D = \{0, 1, 3, 9\}.$$

Računajući razlike (modulo 13) svih parova različitih elemenata od D dobijemo sljedeće:

$$\begin{array}{ll} 0 - 1 = 12 & 0 - 3 = 10 \\ 0 - 9 = 4 & 1 - 0 = 1 \\ 1 - 3 = 11 & 1 - 9 = 5 \\ 3 - 0 = 3 & 3 - 1 = 2 \\ 3 - 9 = 7 & 9 - 0 = 9 \\ 9 - 1 = 8 & 9 - 3 = 6 \end{array}$$

Dobili smo svaki element od $\mathbb{Z}_{13}\setminus\{0\}$ točno jednom, dakle, D je $(13, 4, 1)$-diferencijski skup u $(\mathbb{Z}_{13}, +)$. ■

Primjer 1.2

Ne postoji $(16, 6, 2)$-diferencijski skup u grupi $(\mathbb{Z}_{16}, +)$, ali postoji u grupi $(\mathbb{Z}_4 \times \mathbb{Z}_4, +)$:

$$D = \{(0,1), (0,2), (0,3), (1,0), (2,0), (3,0)\}.$$

■

U primjeru 1.1 prikazali smo diferencijski skup u cikličkoj grupi, a u primjeru 1.2 u necikličkoj Abelovoj grupi. Postoje diferencijski skupovi i u neabelovim grupama. Jedan takav vidimo u sljedećem primjeru.

Primjer 1.3

Promotrimo sljedeću grupu, zapisanu multiplikativno:

$$G = \{a^i b^j : a^3 = b^7 = 1, ba = ab^4\}.$$

G je neabelova grupa reda 21, a skup

$$D = \{a, a^2, b, b^2, b^4\}$$

je $(21, 5, 1)$-diferencijski skup u $(G, \cdot)$. ■

Iz definicije vidimo da parovi (i, j) takvi da je $i \neq j$, kojih ima $k(k-1)$, moraju kao razliku dati $v - 1$ nenul elemenata točno λ puta. Stoga, za svaki (v, k, λ)-diferencijski skup mora vrijediti sljedeće:

$$\lambda(v-1) = k(k-1). \tag{1.1.1}$$

Stoga, naprimjer, ne postoji $(16, 6, 5)$-diferencijski skup, jer $5(16-1) \neq 6 \cdot 5$.

Komplement (v, k, λ)-diferencijskog skupa je također diferencijski skup s parametrima $(v, v-k, v-2k+\lambda)$. Zato je dovoljno promatrati samo parametre za koje vrijedi $k \leq \frac{v}{2}$.

Diferencijski skupovi su usko vezani uz *simetrične blokovne dizajne*. Naime, diferencijskim skupom može se konstruirati simetrični BIBD.

Definicija 1.2. *Neka su v, k i λ pozitivni cijeli brojevi takvi da $2 \leq k < v$. Uređeni par $(X, \mathcal{A})$ zovemo (v, k, λ)-blokovni dizajn ($(v, k, \lambda) - BIBD$), ako zadovoljava sljedeća svojstva:*

1. *X je skup od v elemenata koje nazivamo točkama,*
2. *$\mathcal{A}$ je familija podskupova od X koje nazivamo blokovima,*
3. *svaki blok sadrži točno k točaka,*
4. *svaki par različitih točaka je sadržan u točno λ blokova.*

Nadalje, za $(v, k, \lambda) - BIBD$ kažemo da je simetričan ako ima jednak broj točaka i blokova.

Neka je D (v,k,λ)-diferencijski skup u grupi $(G,+)$. Za proizvoljni $g \in G$ definiramo:

$$D+g = \{x+g : x \in D\}.$$

Skup $D+g$ zovemo *translat* od D. S $Dev(D) = \{D+g : g \in G\}$ označimo skup svih v translata od D.

Teorem 1.1. *Neka je D (v,k,λ)-diferencijski skup u Abelovoj grupi $(G,+)$. Tada je $(G, Dev(D))$ simetrični $(v,k,\lambda) - BIBD$.*

Dokaz. Neka su $x, y \in G, x \neq y$. Prvo ćemo dokazati da postoji točno λ elemenata $g \in G$ takvih da je $\{x,y\} \subseteq D+g$.

Označimo $x-y = d$. Postoji točno λ uređenih parova (x',y') takvih da je $x', y' \in D$ i $x'-y' = d$. Označimo te uređene parove s $(x_i, y_i), 1 \leq i \leq \lambda$. Za $1 \leq i \leq \lambda$, definiramo $g_i = -x_i + x$. Tada je $g_i = -y_i + y$ i $\{x,y\} = \{x_i+g_i, y_i+g_i\} \subseteq D+g_i$. Elementi g_i su različiti jer su x_i-ovi različiti, što pokazuje da postoji barem λ vrijednosti $g \in G$ takvih da je $\{x,y\} \subseteq D+g$.

Obratno, pretpostavimo da postoji točno l različitih $g \in G$ takvih da je $\{x,y\} \subseteq D+g$, označimo ih s $g_1, g_2, \ldots, g_l$. Tada je $(x-g_i)+(g_i-y) = x-y = d$ za $1 \leq i \leq l$. Također, $\{x-g_i, y-g_i\} \subseteq D$ za $1 \leq i \leq l$. Svi g_i-ovi su različiti, pa smo našli l uređenih parova $(x',y') \in D$ takvih da je $x'-y' = d$. Postoji točno λ takvih parova, pa je $l \leq \lambda$.

Time smo dokazali da je $l = \lambda$. Svaki blok $D+g$ sadrži k točaka, pa klasa v blokova $\{D+g\colon g \in G\}$ čini simetrični (v,k,λ)-BIBD. □

Može se pokazati da teorem 1.1 vrijedi i za neabelove grupe. Iz sljedeće leme o simetričnim dizajnima i teorema 1.1 vidi se da se svaka dva translata nekog (v,k,λ)-diferencijskog skupa sijeku u točno λ točaka. Dokaz leme može se naći u [1].

Lema 1.1. *Neka je $(X, \mathcal{A})$ simetrični (v,k,λ)-BIBD sa skupom blokova $\mathcal{A} = \{A_1, A_2, \ldots, A_v\}$. Tada za svaki $1 \leq i,j \leq v,\ i \neq j$ vrijedi $|A_i \cap A_j| = \lambda$.*

Korolar 1.1. *Neka je D (v,k,λ)-diferencijski skup u Abelovoj grupi $(G,+)$. Tada se $Dev(D)$ sastoji od v različitih blokova.*

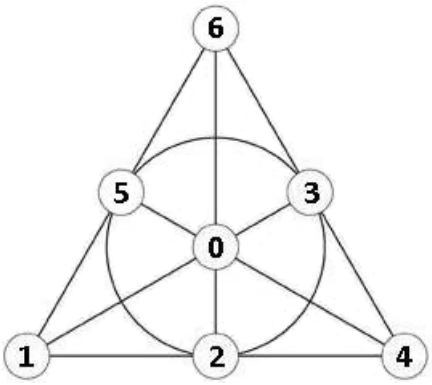
Dokaz. Pretpostavimo da postoje $g_1, g_2 \in G, g_1 \neq g_2$ takvi da je $D+g_1 = D+g_2$. Tada bi simetrični (v,k,λ)-BIBD $(G, Dev(G))$ sadržavao dva bloka koji se sijeku u k točaka. Međutim, iz leme 1.1 sljedi da mu se svaka dva bloka sijeku u λ točaka, a iz (1.1.1) se vidi da ne može vrijediti $k = \lambda$. □

Primjer 1.4

Skup $D = \{1,2,4\}$ je $(7,3,1)$-diferencijski skup u $(\mathbb{Z}_7,+)$. Koristeći teorem 1.1, konstruirat ćemo simetrični $(7,3,1)$-BIBD.

$D = \{1, 2, 4\}$
$Dev(D)$:
$D + 0 = \{1, 2, 4\}$
$D + 1 = \{2, 3, 5\}$
$D + 2 = \{3, 4, 6\}$
$D + 3 = \{0, 4, 5\}$
$D + 4 = \{1, 5, 6\}$
$D + 5 = \{0, 2, 6\}$
$D + 6 = \{0, 1, 3\}$

$(\mathbb{Z}_7, Dev(D))$ je simetrični $(7, 3, 1)$-BIBD poznat kao *Fanova ravnina*, prikazana na slici desno.



Fanova ravnina

■

Definicija 1.3. *Neka su $(X, \mathcal{A})$ i $(Y, \mathcal{B})$ dva dizajna. Kažemo da su $(X, \mathcal{A})$ i $(Y, \mathcal{B})$ izomorfni ako postoji bijekcija $\alpha\colon X \to Y$ takva da*

$$[\{\alpha(x)\colon x \in A\}\colon A \in \mathcal{A}] = \mathcal{B}.$$

Drugim riječima, ako preimenujemo sve točke $x \in X$ sa $\alpha(x)$, tada se $\mathcal{A}$ transformira u $\mathcal{B}$. Bijekciju α zovemo izomorfizam. Ako su $(X, \mathcal{A})$ i $(Y, \mathcal{B})$ jednaki, tada α zovemo automorfizam.

Lako se pokaže da skup svih automorfizama BIBD-a $(X, \mathcal{A})$ s operacijom kompozicije funkcija čini grupu. Tu grupu zovemo grupom automorfizma i označavamo je $Aut(X, \mathcal{A})$. Simetrični BIBD-ovi nastali iz diferencijskih skupova imaju netrivijalnu grupu automorfizama definiranu na očit način. O tome govori sljedeći teorem.

Teorem 1.2. *Neka je $(G, Dev(D))$ simetrični BIBD dobiven od (v, k, λ)-diferencijskog skupa D u grupi $(G, +)$. Tada grupa automorfizama $Aut(G, Dev(D))$ sadrži podgrupu $\widehat{G}$ koja je izomorfna s G i koja djeluje regularno na točke dizajna.*

Dokaz. Za svaki $g \in G$, definiramo preslikavanje $\widehat{g}\colon G \to G$ na sljedeći način:

$$\widehat{g}(x) = x + g$$

za sve $x \in G$. Lako se vidi da je svaki $\widehat{g}$ injekcija i surjekcija, pa je i permutacija od G. Definirajmo $\widehat{G} = \{\widehat{g} : g \in G\}$. $\widehat{G}$ je grupa permutacija. Sad dokažimo sljedeće:

1. $(G, +)$ je izomorfno s $(\widehat{G}, \circ)$, gdje operacija "$\circ$" označava kompoziciju permutacija;

2. $(\widehat{G}, \circ)$ je podgrupa od $Aut(G, Dev(D))$.

Da dokažemo prvu tvrdnju, konstruirajmo izomorfizam između $(G,+)$ i $(\widehat{G},\circ)$. Definiramo $\alpha\colon G \to \widehat{G}$ na očit način: $\alpha(x) = \widehat{g}$ za svaki $g \in G$. Vidimo da je α izomorfizam grupa jer

$$\begin{aligned}(\alpha(g)\circ\alpha(h))(x) &= (\widehat{g}\circ\widehat{h})(x)\\ &= \widehat{h}(\widehat{g}(x))\\ &= \widehat{h}(x+g)\\ &= x+g+h\\ &= \widehat{g+h}(x)\\ &= \alpha(g+h)(x)\end{aligned}$$

vrijedi za sve $g,h,x \in G$, pa $\alpha(g)\circ\alpha(h) = \alpha(g+h)$ vrijedi za sve $g,h \in G$. Nadalje, jasno je da je α surjekcija. Također, α je injekcija jer je $\widehat{g} = \widehat{h}$ ako i samo ako je $g = h$. Dakle, α je izomorfizam grupa.

Da bi dokazali drugu tvrdnju, primjetimo da vrijedi

$$\begin{aligned}\widehat{g}(D+g) &= \{\widehat{g}(x)\colon x \in D+h\}\\ &= \{x+g\colon x \in D+h\}\\ &= \{x+g+h\colon x \in D\}\\ &= D+h+g.\end{aligned}$$

Stoga, za svaku permutaciju $\widehat{g} \in \widehat{G}$ i za svaki blok $D+h \in Dev(D)$ vrijedi da je $\widehat{g}(D+h) \in Dev(D)$. Odnosno, svaki $\widehat{g} \in \widehat{G}$ je automorfizam od $(G, Dev(D))$. Budući da je $\widehat{G}$ grupa, ona je i podgrupa od $Aut(G, Dev(D))$. □

Uz dodatne uvjete vrijedi obrat teorema 1.2. Ovdje ćemo dokazati rezultat tog tipa za diferencijske skupove u cikličkim grupama.

Permutaciju k-članog skupa možemo reprezentirati kao produkt disjunktnih cikusa čija je suma duljina jednaka k. Tada multiskup duljina tih ciklusa zovemo cikličkim tipom pripadne permutacije.

Teorem 1.3. *Neka je $(X,\mathcal{A})$ simetrični (v,k,λ)-BIBD, i neka je $\alpha \in Aut(X,\mathcal{A})$. Tada je ciklički tip od α kao permutacije skupa X jednak cikličkom tipu od α kao permutacije skupa $\mathcal{A}$.*

Dokaz ovog teorema može se naći u [1]. Sad možemo dokazati obrat teorema 1.2 za specijalni slučaj.

Teorem 1.4. *Neka je $(X,\mathcal{A})$ simetrični (v,k,λ)-BIBD i α njegov automorfizam koji permutira točke iz X u jednom ciklusu duljine v. Tada postoji (v,k,λ)-diferencijski skup u $(\mathbb{Z}_v,+)$.*

Dokaz. Bez smanjenja općenitosti možemo označiti točke tako da vrijedi $X = \{x_0, x_1, \ldots, x_{v-1}\}$ i $\alpha(x_i) = x_{i+1 \ (mod\ v)}$ za $0 \leq i \leq v-1$, odnosno

$$\alpha = (x_0\ x_1\ \cdots\ x_{v-1}).$$

Izaberimo proizvoljni blok $A \in \mathcal{A}$. Definiramo $A_0 = A$, te za svaki pozitivni cijeli broj definiramo

$$A_j = \{\alpha^j(x) \colon x \in A_0\} = \{x_{i+j \ (mod\ v)} \colon x_i \in A_0\}.$$

Svaki A_j je blok u $\mathcal{A}$ jer je $\alpha^j \in Aut(X, \mathcal{A})$. Također vrijedi $\alpha(A_j) = A_{j+1 \ mod\ v}$. Iz teorema 1.3 znamo da α permutira i blokove iz $\mathcal{A}$ u jednom ciklusu duljine v. Iz toga slijedi da su $A_0, \ldots, A_{v-1}$ različiti, odnosno

$$\mathcal{A} = \{A_j \colon 0 \leq j \leq v-1\},$$

te α permutira blokove iz $\mathcal{A}$ na sljedeći način:

$$\alpha = (A_0\ A_1\ \cdots\ A_{v-1}).$$

Sad definirajmo skup

$$D = \{i \colon x_i \in A_0\},$$

i pokažimo da je skup D naš traženi diferencijski skup. Neka je $g \in \mathbb{Z}_v$, $g \neq 0$. Par $\{x_0, x_g\}$ se pojavljuje u točno λ blokova u $\mathcal{A}$, neka su to $A_{i_1}, \ldots A_{i_\lambda}$. Za svako pojavljivanje para $\{x_0, x_g\} \subseteq A_{i_j}$ postoji par s razlikom g u D. Naime, $(g - i_j) - (-i_j) \equiv g \pmod{v}$, gdje je

$$\{-i_j \pmod{v}, g - i_j \pmod{v}\} \subseteq D.$$

Tih λ parova u D je različito. Stoga, razlika g se pojavljuje λ puta u skupu D za svaki nenul $g \in \mathbb{Z}_v$. Ovim razmatranjem smo uočili svako pojavljivanje elementa g u skupu D, stoga je D diferencijski skup. □

Sljedeći teorem je generalizacija teorema 1.4 za proizvoljne konačne grupe. I on se može dokazati na sličan način kao teorem 1.4.

Teorem 1.5. *Neka je $(X, \mathcal{A})$ simetrični (v, k, λ)-BIBD takav da postoji podgrupa $G \leq Aut(X, \mathcal{A})$ koja djeluje regularno na točke iz X. Tada postoji (v, k, λ)-diferencijski skup u grupi $(G, \circ)$.*

1.2 Singerovi diferencijski skupovi

U ovom odjeljku ćemo pokazati konstrukciju jedne beskonačne klase diferencijskih skupova koji generiraju rubnu klasu simetričnih dizajna - *projektivne ravnine*. Na projektivnu ravninu možemo gledati kao na simetrični dizajn s parametrom $\lambda = 1$, odnosno onaj u kojem se svaki par blokova siječe u jednoj točki.

Definicija 1.4. *Za $(n^2+n+1, n+1, 1)$-BIBD takav da je $n \geq 2$ kažemo da je projektivna ravnina reda n.*

Primijetimo da je *Fanova ravnina* iz primjera 1.4 projektivna ravnina reda 2. Sada ćemo pokazati konstrukciju projektivne ravnine reda q, kada je q prosta potencija.

Teorem 1.6. *Za svaku prostu potenciju $q \geq 2$, postoji $(q^2+q+1, q+1, q)$-BIBD, odnosno projektivna ravnina reda q.*

Dokaz. Neka je q prosta potencija. Neka je $\mathbb{F}_q$ konačno polje reda q, a V trodimenzionalni vektorski prostor nad $\mathbb{F}_q$.

S $\mathcal{V}_1$ označimo skup svih jednodimenzionalnih potprostora od V, a s $\mathcal{V}_2$ skup svih dvodimenzionalnih potprostora od V. Za svaki $B \in \mathcal{V}_2$, definirajmo blok

$$A_B = \{C \in \mathcal{V}_1 \colon C \subseteq B\}.$$

Definirajmo još i

$$\mathcal{A} = \{A_B \colon B \in \mathcal{V}_2\}.$$

Tvrdimo da je $(\mathcal{V}_1, \mathcal{A})$ projektivna ravnina reda q.

Prvo primijetimo da za svaki $C \in \mathcal{V}_1$ vrijedi $|C| = q$ i da sadrži nulvektor: $000 \in C$. Skupovi $C \setminus \{000\}$, $C \in \mathcal{V}_1$ particioniraju skup $V \setminus \{000\}$. Dakle vrijedi

$$|\mathcal{V}_1| = \frac{q^3-1}{q-1} = q^2+q+1.$$

Nadalje, neka je $B \in \mathcal{V}_2$. Jasno je da je $|B| = q^2$. Skupovi $C \setminus \{000\}$ takvi da $C \in \mathcal{V}_1$ i $C \subseteq B$, particioniraju skup $B \setminus \{000\}$. Dakle vrijedi

$$|A_B| = \frac{q^2-1}{q-1} = q+1.$$

Na kraju, uzmimo $C, D \in \mathcal{V}_1,\ C \neq D$. Jasno je da postoji jedinstven dvodimenzionalan potprostor B koji sadrži jednodimenzionalne potprostore C i D. Taj potprostor generira jedinstveni blok A_B koji sadrži točke C i D. □

Dakle, pokazali smo da postoji projektivna ravnina reda n ako je n prosta potencija. Pitanje postoji li projektivna ravnina čiji red nije prosta potencija jedno je od najslavnijih otvorenih pitanja teorije dizajna.

Sada ćemo pokazati da za prostu potenciju q postoji i diferencijski skup kojim možemo generirati projektivnu ravninu reda q. Ti diferencijski skupovi nazivaju se *Singerovim diferencijskim skupovima.* Objasnit ćemo i algoritam konstrukcije takvih diferencijskih skupova.

Teorem 1.7 (Singerovi diferencijski skupovi)**.** *Neka je q prosta potencija. Tada postoji $(q^2+q+1, q+1, 1)$-diferencijski skup u $(\mathbb{Z}_{q^2+q+1}, +)$.*

Dokaz. Prisjetimo se konstrukcije projektivne ravnine iz dokaza teorema 1.6. Neka je V vektorski prostor nad poljem $\mathbb{F}_q$, $\mathcal{V}_1$ skup svih jednodimenzionalnih, a $\mathcal{V}_2 = \mathcal{A}$ skup blokova, odnosno skup svih dvodimenzionalnih potprostora od V.

Iskoristit ćemo važnu činjenicu da je multiplikativna grupa konačnog polja $(\mathbb{F}_q \backslash \{0\}, \cdot)$ ciklička grupa. Generator te grupe, označimo ga s ω, naziva se *pritivnim elementom* polja $\mathbb{F}_q$. Konačno polje $\mathbb{F}_{q^3}$ je trodimenzionalni vektorski prostor nad $\mathbb{F}_q$, pa uzmimo da je $V = \mathbb{F}_{q^3}$. Neka je ω primitivni element od $\mathbb{F}_{q^3}$. Definirajmo preslikavanje $f\colon V \to V$ s $f(z) = \omega z$. Lako se pokaže da je f linearni operator. Naime, za svaki $z_1, z_2 \in V$, i $c \in \mathbb{F}_q$ vrijedi:

$$f(z_1 + z_2) = \omega(z_1 + z_2) = \omega z_1 + \omega z_2 = f(z_1) + f(z_2),$$

$$f(cz_1) = \omega(cz_1) = (\omega c)z_1 = (c\omega)z_1 = c(\omega z_1) = cf(z_1).$$

Zato f preslikava svaki potprostor od V u potprostor od V. Funkcija $f^{-1}(z) = \frac{1}{\omega} z$ je inverz od f, dakle f je bijekcija (tj. regularni linearni operator) pa vrijedi

$$f(\mathcal{V}_1) = \mathcal{V}_1 \qquad \text{i} \qquad f(\mathcal{V}_2) = \mathcal{V}_2,$$

što znači da je f automorfizam naše pripadne projektivne ravnine s parametrima $(q^2 + q + 1, q + 1, 1)$.

$\mathbb{F}_q$ je potpolje od $\mathbb{F}_{q^3}$, pa iz $(q^3 - 1)/(q - 1) = q^2 + q + 1$ slijedi da je

$$\mathbb{F}_q = \{\omega^{(q^2+q+1)i} \colon 0 \leq i \leq q - 2\} \cup \{(0, 0, 0)\}.$$

Tada je jasno da za svaki W potprostor od V vrijedi

$$f^{q^2+q+1}(W) = \omega^{q^2+q+1} W = W$$

jer je ω^{q^2+q+1} skalar iz $\mathbb{F}_q$. Tada, posebno, f^{q^2+q+1} fiksira i sve jednodimenzionalne potprostore od V. Iz toga, iz definicije preslikavanja f i iz činjenice da jednodimenzionalnih potprostora ima $q^2 + q + 1$, slijedi da f permutira točke naše projektivne ravnine u jednom ciklusu. Tada iz teorema 1.4 slijedi da postoji $(q^2 + q + 1, q + 1, 1)$-diferencijski skup u grupi $(\mathbb{Z}_{q^2+q+1}, +)$. □

Opišimo sada konstrukciju Singerovih diferencijskih skupova. Upotrijebiti ćemo istu notaciju kao u gornjem dokazu. Točke projektivne ravnine možemo poredati tako da je $C_i = [\{\omega^i\}]$ za $0 \leq i \leq q^2 + q$, gdje $[S]$ označava linearnu ljusku skupa S. Tada je $f(C_i) = C_{i+1 \pmod{q^2+q+1}}$, $0 \leq i \leq q^2 + q$.

Neka je polje $\mathbb{F}_{q^3}$ konstruirano kao $\mathbb{F}_q[x]/(g(x))$, gdje je $g(x) \in \mathbb{F}_q[x]$ ireducibilan kubni polinom. Tada se elementi od $\mathbb{F}_{q^3}$ mogu reprezentirati kao polinomi iz $\mathbb{F}_q[x]$ stupnja najviše dva.

Za svaki $j \in \mathbb{F}_q$ definirajmo $y_j \in \mathbb{Z}_{q^3-1}$ takav da je $\omega^{y_j} = j + x$. Primijetimo da je $j + x \in \mathbb{F}_{q^3} \setminus \{0\}$, a ω je primitivni element od $\mathbb{F}_{q^3}$, pa je y_j dobro definiran. Sad se lako vidi da je $[\{1\}] = C_0$ i

$$[\{j + x\}] = C_{y_j \pmod{q^2+q+1}}$$

za sve $j \in \mathbb{F}_q$.

Uzmimo dvodimenzionalni potprostor

$$B = [\{1, x\}] = \{i + jx : i, j \in \mathbb{F}_q\},$$

i promatrajmo blok A_B. Tada vrijedi

$$\begin{aligned} A_B =& \{[\{1\}]\} \cup \{[\{j + x\}] : j \in \mathbb{F}_q\} \\ =& \{C_0\} \cup \{C_{y_j \pmod{q^2+q+1}} : j \in \mathbb{F}_q\}. \end{aligned}$$

Tada je skup

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

$(q^2 + q + 1, q + 1, 1)$-diferencijski skup u $(\mathbb{Z}_{q^2+q+1}, +)$.

Pokažimo to na jednom primjeru.

Primjer 1.5

Uzmimo $q = 3$ i konstruirajmo $(13, 4, 1)$-diferencijski skup u $(\mathbb{Z}_{13}, +)$. Tada je $q^3 = 27$, pa promatrajmo polje $\mathbb{F}_{27}$. Njega možemo dobiti kao $\mathbb{Z}_3[x]/(x^3 + 2x^2 + 1)$ jer je $x^3 + 2x^2 + 1$ ireducibilan polinom iz $\mathbb{Z}_3[x]$. Primitivni element pripadnog polja $\mathbb{F}_{27}$ bit će $\omega = x$. Poredajmo nenul elemente od $\mathbb{F}_{27}$ kao potencije od ω.

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	$2x^2 + x$

Sada moramo pronaći sve potencije y_j takve da je $\omega^{y_j} = j + x$ za $j = 0, 1, 2$. Iz gornje tablice vidimo da su to $y_0 = 1$, $y_1 = 18$, i $y_2 = 11$. Gledamo njihove vrijednosti modulo 13, dodamo 0 i dobijemo da je skup $D = \{0, 1, 5, 11\}$ $(13, 4, 1)$-diferencijski skup u $(\mathbb{Z}_{13}, +)$. ■

1.3 Diferencijski skupovi kvadratnog ostatka

U ovom odjeljku predstavit ćemo klasu diferencijskih skupova konstruiranih kvadratnim ostatcima u konačnom polju $\mathbb{F}_q$, gdje je q neparna prosta potencija. *Kvadratni*

ostatci polja $\mathbb{F}_q$ su elementi skupa:

$$QR(q) = \{z^2 : z \in \mathbb{F}_q, z \neq 0\}.$$

Također definiramo i

$$QNR(q) = \mathbb{F}_q \backslash (QR(q) \cup \{0\}).$$

Elemente od $QNR(q)$ nazivamo *kvadratni neostatci* polja $\mathbb{F}_q$.

Koristeći činjenicu da je $x^2 = (-x)^2$, nije teško pokazati da preslikavanje $z \mapsto z^2$ preslika dva elementa u jedan, za $z \in \mathbb{F}_q \backslash \{0\}$ i q neparan. Iz toga se može pokazati da je $QR(q)$ multiplikativna podgrupa od $\mathbb{F}_q \backslash \{0\}$ s indeksom dva, i $QNR(q)$ je suskup od $QR(q)$. Tada sljedeće činjenice slijede kao posljedice:

$$\begin{aligned} xy &\in QR(q) && \text{ako } x, y \in QR(q) \\ xy &\in QR(q) && \text{ako } x, y \in QNR(q) \\ xy &\in QNR(q) && \text{ako } x \in QR(q), y \in QNR(q). \end{aligned}$$

Sada ćemo okarakterizirati kvadratne ostatke i neostatke na drugačiji način. Jasno, element $\omega \in \mathbb{F}_q$ je primitivni element ako i samo ako

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

Očito je skup

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

podskup od $QR(q)$. Zato što je

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

dokazali smo sljedeći rezultat.

Lema 1.2. *Neka je q neparna prosta potencija i ω primitivni element od $\mathbb{F}_q$. Tada je*

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

Sada ćemo iskazati i dokazati koristan korolar leme 1.2.

Korolar 1.2. *Neka je q neparna prosta potencija. Tada je $-1 \in QR(q)$ ako i samo ako je $q \equiv 1 \pmod 4$.*

Dokaz. Neka je $\omega \in \mathbb{F}_q$ primitivni element, i neka je $\gamma = \omega^{(q-1)/2}$. Tada je $\gamma^2 = \omega^{(q-1)} = 1$ i $\gamma \neq 1$, pa je $\gamma = -1$. Rezultat sada slijedi iz iz leme 1.2. □

Sada je jasno da u slučaju kad je prosta potencija $q \equiv 3 \pmod 4$ vrijedi da je $x \in QR(q)$ ako i samo ako je $-x \in QNR(q)$.

Sljedeći rezultat nam daje beskonačnu klasu diferencijskih skupova koje zovemo *diferencijskim skupovima kvadratnih ostataka*.

Teorem 1.8 (Diferencijski skupovi kvadratnih ostataka)**.** *Neka je* $q \equiv 3 \pmod 4$ *prosta potencija. Tada je* $QR(q)$ $(q, (q-1)/2, (q-3)/4)$*-diferencijski skup u* $(\mathbb{F}_q, +)$.

Dokaz. Označimo $D = QR(q)$. Već smo pokazali da $|D| = (q-1)/2$. Preostaje pokazati da se svaki nenul element od $\mathbb{F}_q$ pojavljuje $(q-3)/4$ puta kao razlika dvaju elementa iz D.

Za svaki $d \in \mathbb{F}_q \backslash \{0\}$, definiramo

$$a_d = |\{(x, y) \colon x, y \in D, x - y = d\}|.$$

Jasno je da $gx - gy = g(x - y)$ za svaki g, x, y, pa je broj pojavljivanja razlike d u D jednak broju pojavljivanja razlike gd u gD, gdje je $gD = \{gx \colon x \in D\}$. Neka je $g \in QR(q)$. Tada je lako vidjeti da $gD = D$, pa je tada $a_d = a_{gd}$ za svaki $g \in QR(q)$. Dakle, postoji konstanta λ takva da je $a_d = \lambda$ za svaki $d \in QR(q)$.

Sada pretpostavimo da je $d \in QNR(q)$ i neka je $e = -d$. Iz korolara 1.2. znamo da je $-1 \in QNR(q)$, stoga je $e \in QR(q)$. Primijetimo da je $a_d = a_e$, jer $x - y = d$ ako i samo ako je $y - x = e$. Iz toga slijedi da je $a_d = \lambda$ za svaki $d \in \mathbb{F}_q \backslash \{0\}$, dakle D je $(q, (q-1)/2, \lambda)$-diferencijski skup. Iz $\lambda(v-1) = k(k-1)$ dobijemo da je $\lambda = (q-3)/4$, kao što smo i htjeli. □

Prikažimo ovo na jednom primjeru.

Primjer 1.6

Pronađimo $(19, 9, 4)$-diferencijski skup u $(\mathbb{Z}_{19}, +)$. Izračunajmo kvadrate: $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 16$, $5^2 = 6$, $6^2 = 17$, $7^2 = 11$, $8^2 = 7$, $9^2 = 5$. Ostali kvadrati se ponavljaju. Iz teorema 1.8 slijedi,

$$QR(19) = \{1, 4, 5, 6, 7, 9, 11, 16, 17\}$$

je $(19, 9, 4)$-diferencijski skup u $(\mathbb{Z}_{19}, +)$. ■

Korolar 1.3. *Neka je* $q \equiv 3 \pmod 4$. *Tada je* $QNR(q)$ $(q, (q-1)/2, (q-3)/4)$*-diferencijski skup u* $(\mathbb{F}_q, +)$.

Dokaz. Iz teorema 1.8 slijedi da je $QR(q)$ $(q, (q-1)/2, (q-3)/4)$-diferencijski skup u $(\mathbb{F}_q, +)$, pa za svaki $d \in \mathbb{F}_q \backslash \{0\}$ postoje $x_i, y_i \in QR(q)$, $1 \leq i \leq (q-3)/4$ takvi da je $x_i - y_i = d$. Kao posljedica korolara 1.2, vrijedi da su $-x_i, -y_i \in QNR(q)$, $1 \leq i \leq (q-3)/4$. Za njih vrijedi da $(-y_i) - (-x_i) = x_i - y_i = d$, $1 \leq i \leq (q-3)/4$. Tada iz $|QR(q)| = |QNR(q)|$ slijedi da je i $QNR(q)$ $(q, (q-1)/2, (q-3)/4)$-diferencijski skup u $(\mathbb{F}_q, +)$. □

1.4 Multiplikatori

U ovom odjeljku ograničit ćemo se na Abelove grupe. Jako koristan koncept u proučavanju diferencijskih skupova u Abelovim grupama je pojam *multiplikatora*, koji ćemo sad definirati.

Definicija 1.5. *Neka je D (v,k,λ)-diferencijski skup u Abelovoj grupi $(G,+)$ reda v. Za prirodan broj m definiramo*

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

gdje je mx suma m kopija od x. Tada m zovemo multiplikatorom od D ako je $mD = D + g$ za neki $g \in G$. Također kažemo da je D fiksiran multiplikatorom m ako je $mD = D$.

Primjer 1.7

Skup $D = \{2,3,5,11\}$ je $(13,4,1)$-diferencijski skup u $(\mathbb{Z}_{13},+)$. Lako se vidi da je $3D = \{2,6,7,9\} = D + 4$, dakle, 3 je multiplikator od D. ■

Lema 1.3. *Neka je m multiplikator (v,k,λ)-diferencisjkog skupa D u Abelovoj grupi $(G,+)$ reda v. Tada je $NZD(m,v) = 1$.*

Dokaz. Pretpostavimo da je $NZD(m,v) > 1$. Neka je p prosti djelitelj od m i v. Neka je $d \in G$ reda p. Moraju postojati $x, y \in D$ takvi da je $x - y = d$. Tada je $mx - my = md = 0$. Dakle, $mx = my$, pa je $mD \neq D + g$ za svaki g. Dakle, m nije multiplikator od D, kontradikcija. □

Lema 1.4. *Neka je m multiplikator (v,k,λ)-diferencijskog skupa D u Abelovoj grupi $(G,+)$ reda v. Definirajmo funkciju $\alpha \colon G \to G$ s pravilom $\alpha(x) = mx$. Tada je $\alpha \in Aut(G, Dev(D))$.*

Dokaz. Znamo da je $mD = D + g$ za neki $g \in G$. Promatrajmo što se događa kad djelujemo s α na proizvoljni blok dizajna $(G, Dev(D))$:

$$\alpha(D + h) = m(D + h) = mD + mh = D + g + mh \in Dev(D).$$

Dakle, α svaki blok preslika u blok, kao što smo htjeli. □

Sada navodimo važan rezultat poznat kao *teorem o multiplikatoru* koji utvrđuje postojanje multiplikatora diferencijskog skupa u ovisnosti o njegovim parametrima. Dokaz se može pronaći u [1].

Teorem 1.9 (Teorem o multiplikatoru)**.** *Neka postoji (v,k,λ)-diferencijski skup D u Abelovoj grupi $(G,+)$ reda v. Ako su zadovoljena sljedeća četiri uvjeta:*

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

tada je p multiplikator od D.

Primijetimo da multiplikator p iz teorema ne ovisi o grupi u kojoj je diferencijski skup, nego samo o njegovim parametrima. Napomenimo još da se vjeruje da uvjet "$k > \lambda$" u teoremu nije potreban, ali nije poznat dokaz teorema bez te pretpostavke.

Sljedeći rezultati će nam olakšati korištenje teorema o multiplikatoru.

Teorem 1.10. *Neka je m multiplikator (v, k, λ)-diferencijskog skupa D u Abelovoj grupi $(G, +)$ reda v. Tada postoji translat od D koji je fiksiran multiplikatorom m.*

Dokaz. Definirajmo $\alpha(x) = mx$ za svaki $x \in G$. U lemi 1.4 smo pokazali da je $\alpha \in Aut(G, Dev(D))$. Jasno je da je $\alpha(0) = 0$, dakle α fiksira barem jednu točku, pa po teoremu 1.3 α fiksira i barem jedan blok od $Dev(D)$. Drugim riječima, postoji translat od D koji je fiksiran multiplikatorom m. □

Dokazat ćemo jači rezultat kada je $NZD(v, k) = 1$. Definirajmo prvo pojam *normaliziranosti*.

Definicija 1.6. *Za diferencijski skup D u Abelovoj grupi $(G, +)$ kažemo da je normaliziran, ako mu je suma elemenata jednaka 0.*

Lema 1.5. *Neka je $NZD(v, k) = 1$ i neka postoji (v, k, λ)-diferencijski skup D u Abelovoj grupi $(G, +)$ reda v. Tada postoji jedinstveni normalizirani translat od D.*

Dokaz. Neka je

$$s = \sum_{x \in D} x.$$

Lako se pokaže da vrijedi jednakost:

$$\sum_{x \in D+g} x = s + kg. \tag{1.4.1}$$

Sada pretpostavimo da je $s + kg = s + kh$, gdje su $g, h \in G$ i $g \neq h$. Tada je $k(g-h) = 0$, pa red od $g-h$ dijeli k. Međutim, u svakoj konačnoj grupi, red svakog elementa dijeli red grupe. Dakle, red od $g - h$ djeli v. Iz $NZD(v, k) = 1$ slijedi da je $g - h = 0$, kontradikcija.

Pokazali smo da je preslikavanje $g \mapsto s + kg$ injekcija. To preslikavanje je sa G u G, pa mora biti i surjekcija, pa stoga postoji jedinstveni $g \in G$ takav da je $s + kg = 0$. Dakle, iz jednakosti (1.4.1), postoji jedinstveni $g \in G$ takav da je

$$\sum_{x \in D+g} x = 0.$$

□

Lema 1.6. *Neka je D (v, k, λ)-diferencijski skup u Abelovoj grupi $(G, +)$. Ako postoji jedinstveni $g \in G$ takav da je $D + g$ normaliziran, tada je $D + g$ fiksiran svakim multiplikatorom.*

Dokaz. Pretpostavimo da je $D + g$ jedinstveni normalizirani translat od D. Neka je m proizvoljan multiplikator od D. Tada je m također multiplikator od $D + g$ i vrijedi

$$\sum_{x \in m(D+g)} x = m \sum_{x \in D+g} x = 0.$$

Diferencijski skup $D + g$ je jedinstveni translat od D čija je suma elemenata jednaka 0, iz čega slijedi da je $m(D + g) = D + g$. Dakle, $D + g$ je fiksiran svim multiplikatorima m. □

Teorem 1.11. *Neka je $NZD(v, k) = 1$ i neka postoji (v, k, λ)-diferencijski skup D u Abelovoj grupi $(G, +)$ reda v. Tada postoji translat od D koji je fiksiran svakim multiplikatorom m.*

Dokaz. Po lemi 1.5 postoji jedinstveni $g \in G$ takav da je $D + g$ normaliziran. Tada po lemi 1.6 slijedi da je $D + g$ fiksiran svakim multiplikatorom. □

S teoremom 1.11 pokazali smo da postoji jedinstveni normalizirani translat svakog (v, k, λ)-diferencijskog skupa D u Abelovoj grupi reda v kad je $NZD(v, k) = 1$ i taj translat je fiksiran svakim multiplikatorom od D. Zato u tom slučaju, svaki (v, k, λ)-diferencijski skup D možemo na jedinstven način prikazati u obliku $D_n + g$, gdje je D_n njegov jedinstven normalizirani translat, a $g \in G$. Normalizirani translat je prirodan reprezentant cijele klase translata.

Ilustrirajmo teorem 1.9 i gornja razmatranja jednim primjerom.

Primjer 1.8

Pronađimo sve $(21, 5, 1)$-diferencijske skupove u $(\mathbb{Z}_{21}, +)$. Primijetimo da $p = 2$ zadovoljava uvjete teorema 1.9, dakle, 2 je multiplikator svakog takvog diferencijskog skupa. Po teoremu 1.10 znamo da možemo tražiti samo diferencijske skupove koji su fiksirani multiplikatorom 2, jer sve ostale možemo dobiti njihovom translacijom. Jasno je da je diferencijski skup u grupi $(\mathbb{Z}_{21}, +)$ fiksiran muptiplikatorom 2 ako i samo ako je unija cijelih ciklusa premutacije $x \mapsto 2x \pmod{21}$. Ciklički zapis te permutacije je:

$$(0)\ (1\ 2\ 4\ 8\ 16\ 11)\ (3\ 6\ 12)\ (5\ 10\ 20\ 19\ 17\ 13)\ (7\ 14)\ (9\ 18\ 15).$$

Naši traženi diferencijski skupovi su kardinaliteta 5, a moraju biti unija gornjih ciklusa. To je moguće samo unijom jednog ciklusa duljine 3 i jednog duljine 2. Dvije su takve kombinacije koje daju ova dva skupa:

$$D_1 = \{3, 6, 7, 12, 14\}$$

$$D_2 = \{7, 9, 14, 15, 18\}$$

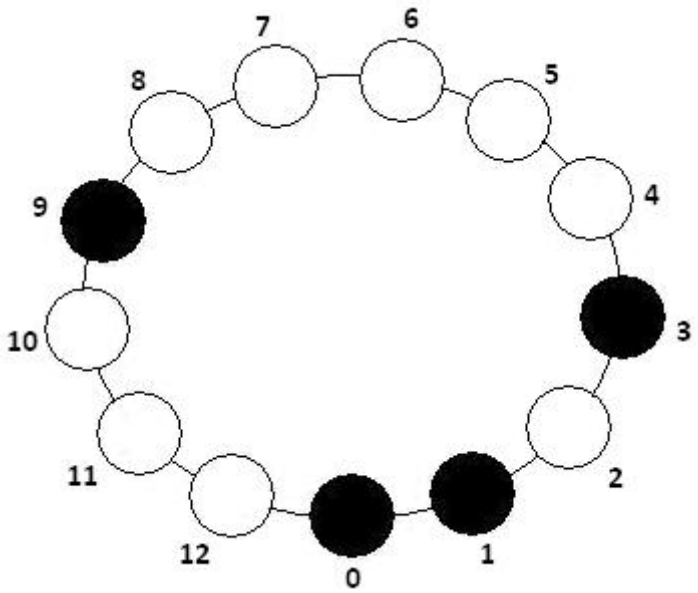
Provjerom lako utvrdimo da su oba ta skupa diferencijski skupovi, a suma im je 0, odnosno normalizirani su. Tada zbog $NZD(v, k) = 1$ znamo da naša dva nađena diferencijska skupa nisu translat jedan drugog. Dakle, njihovom translacijom dobit ćemo sva $2 \cdot 21 = 42$ $(21, 5, 1)$-diferencijska skupa u grupi $(\mathbb{Z}_{21}, +)$. ■

2 Popločavanje grupa

U ovom poglavlju ćemo se poslužiti diferencijskim skupovima da konstruiramo složenije strukture. Definirat ćemo jedan način popločavanja grupa diferencijskim skupovima.

2.1 Motivacija i definicija ogrlice

Diferencijski skupovi u cikličkim grupama mogu se prikazati pomoću ogrlica. Naprimjer, $(13, 4, 1)$-diferencijski skup u $(\mathbb{Z}_{13}, +)$ $D = \{0, 1, 3, 9\}$ izgledao bi ovako:



$(13, 4, 1)$-diferencijski skup

Elementi cikličke grupe poredani u krug na očit način čine ogrlicu, a elementi diferencijskog skupa označeni su crnim kuglicama. Tada se za skup D svojstvo diferencijskog skupa očituje u tome da za svaki broj $d \in \mathbb{Z}_{13} \setminus \{0\}$ postoji jedinstven par crnih kuglica koje su udaljene za d. Pri tome podrazumijevamo da svaki par kuglica ima dvije udaljenosti, gledano u smjeru kazaljke na satu, i obrnuto od smjera kazaljke na satu. Dakle, svaki (v, k, λ)-diferencijski skup u cikličkoj grupi reda v možemo prikazati kao ogrlicu od v kuglica, od kojih je k crno obojanih tako da vrijedi da za svaki broj $d \in \mathbb{Z}_v \setminus \{0\}$ postoji λ parova čija je udaljenost d.

Primijetimo da translate diferencijskih skupova u ovakvom prikazu dobijemo jednostavno rotacijom ogrlice. Npr. za $(13, 4, 1)$-diferencijski skup D sa slike 1.2, njegov

translat $D+2$ dobijemo rotacijom za $2\frac{2\pi}{13}$ u obrnutom smjeru od kazaljke na satu.

Pokušajmo napraviti šareniju ogrlicu, odnosno, na jednoj ogrlici prikazati više diferencijskih skupova istih parametara koji se ne preklapaju, svakog u svojoj boji. Prirodno se postavlja pitanje, možemo li popločati cijelu ogrlicu sa diferencijskim skupovima jednakih parametara. Odgovor je ne.

Propozicija 2.1. *Za prirodne brojeve v, k, λ ne postoji popločavanje grupe reda v s (v, k, λ)-diferencijskim skupovima.*

Dokaz. Iz relacije za diferencijske skupove

$$\lambda(v-1) = k(k-1) \tag{2.1.1}$$

slijedi da je

$$v = k\Big(\frac{k-1}{\lambda} + \frac{1}{k}\Big).$$

Iz gornje jednakosti slijedi da nam treba $\frac{k-1}{\lambda} + \frac{1}{k}$ diferencijskih skupiva kardinaliteta k da bismo popločali grupu reda v, odnosno $\frac{k-1}{\lambda} + \frac{1}{k}$ bi morao biti cijeli broj. Iz (2.1.1) i definicije diferencijskog skupa slijedi da je $1 \leq \lambda < k$. Ako je $\frac{k-1}{\lambda}$ cijeli broj, tada $\frac{k-1}{\lambda} + \frac{1}{k}$ nije cijeli broj. Ako $\frac{k-1}{\lambda}$ nije cijeli broj, tada je najmanja vrijednost koja mu treba biti zbrojena da bi postao cijeli broj $\frac{1}{\lambda}$. Zbog $\lambda < k$ vrijedi da je $\frac{1}{\lambda} > \frac{1}{k}$, pa $\frac{k-1}{\lambda} + \frac{1}{k}$ ne može biti cijeli broj. □

Promotrimo maksimalni broj disjunktnih Singerovih diferencijskih skupova s parametrom $\lambda = 1$. Tada, po jednakosti (2.1.1) bi s $k-1$ disjunktnih diferencijskih skupova mogli popločati cijelu grupu osim jednog elementa. Sljedeći primjer daje takvo popločavanje.

Primjer 2.1

Skupovi D_1, D_2, D_3, D_4 i D_5 su $(31, 6, 1)$-diferencijski skupovi u $(\mathbb{Z}_{31}, +)$. Disjunktni su i popločavaju sve nenul elemente pripadne grupe i tako generiraju donju šarenu ogrlicu. Diferencijski skupovi su prikazani različitim bojama, a crna kuglica predstavlja neutralni element.

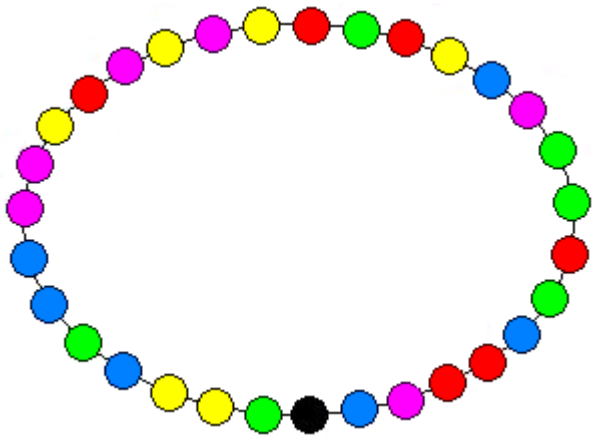
$D_1 = \{1, 5, 11, 24, 25, 27\}$

$D_2 = \{2, 10, 17, 19, 22, 23\}$

$D_3 = \{3, 4, 7, 13, 15, 20\}$

$D_4 = \{6, 8, 9, 14, 26, 30\}$

$D_5 = \{12, 16, 18, 21, 28, 29\}$



$(31, 6, 1)$-ogrlica

Dakle, za svaki broj $d \in \mathbb{Z}_{31} \setminus \{0\}$ i svaku boju postoji jedinstveni par kuglica te boje udaljen za d. ■

Iz primjera 2.1 vidimo da popločavanje nenul elemenata grupe diferencijskim skupovima ima smisla. Definirajmo tu strukturu, ali malo općenitije nego u primjeru 2.1. Nećemo gledati samo diferencijske skupove kojima je $\lambda = 1$, nego za proizvoljni λ, i nećemo promatrati samo cikličke grupe, nego općenite konačne grupe.

Definicija 2.1. *Neka su v, k i λ prirodni brojevi. Neka je $(G, +)$ grupa reda v. Tada skup $\mathcal{A} = \{D_1, D_2, \ldots, D_a\}$ zovemo (v, k, λ)-ogrlicom u grupi $(G, +)$ ako sadrži međusobno disjunktne (v, k, λ)-diferencijske skupove u $(G, +)$ i ako je $\bigcup_{i=1}^{a} D_i = G \setminus \{0\}$.*

U primjeru 2.1 smo prikazali $(31, 6, 1)$-ogrlicu u grupi $(\mathbb{Z}_{31}, +)$. Postoje (v, k, λ)-ogrlice i u necikličkim grupama, i kada je $\lambda > 1$. Dakle, naša definicija (v, k, λ)-ogrlice ima smisla.

Primjer 2.2

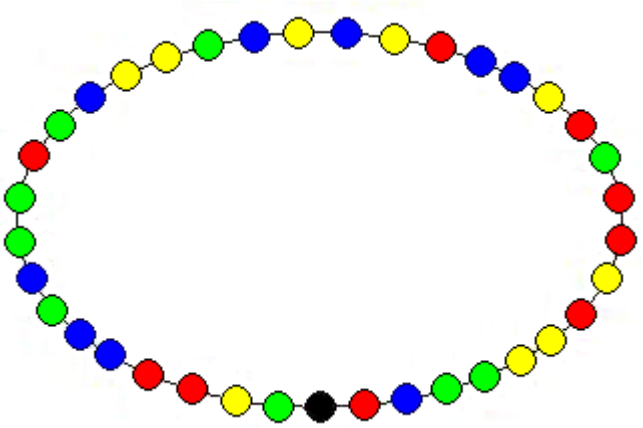
Skupovi

$D_1 =$
$\{1, 7, 9, 10, 12, 16, 26, 33, 34\}$,

$D_2 =$
$\{2, 14, 15, 18, 20, 24, 29, 31, 32\}$,

$D_3 =$
$\{3, 4, 11, 21, 25, 27, 28, 30, 36\}$,

$D_4 =$
$\{5, 6, 8, 13, 17, 19, 22, 23, 35\}$



$(37, 9, 2)$-ogrlica

su $(37, 9, 2)$-diferencijski skupovi u $(\mathbb{Z}_{37}, +)$, pa je $\{D_1, D_2, D_3, D_4\}$ $(37, 9, 2)$-ogrlica u $(\mathbb{Z}_{37}, +)$. ■

Primjer 2.3

Skupovi

$$
\begin{aligned}
D_1 = \{\ & (0,0,1)\ (2,2,1)\ (0,2,2)\ (2,1,1)\ (1,2,1)\ (0,2,1)\ (0,2,0) \\
& (1,0,2)\ (1,1,0)\ (2,0,2)\ (1,1,1)\ (1,2,0)\ (1,0,0)\ \}, \\
D_2 = \{\ & (0,0,2)\ (0,1,0)\ (0,1,1)\ (0,1,2)\ (1,0,1)\ (1,1,2)\ (1,2,2) \\
& (2,0,0)\ (2,0,1)\ (2,1,0)\ (2,1,2)\ (2,2,0)\ (2,2,2)\ \}
\end{aligned}
$$

su $(27, 13, 6)$-diferencijski skupovi u grupi $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. Disjunktni su i ne sadrže $(0, 0, 0)$, pa je $\{D_1, D_2\}$ $(27, 13, 6)$-ogrlica u $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. ■

Primjer 2.4

Postoji $(27, 13, 6)$-ogrlica i u jednoj neabelovoj grupi, semidirektnom produktu $\mathbb{Z}_3 \cdot \mathbb{Z}_9$. Tu grupu možemo zadati s pomoću generatora i relacija na sljedeći način: $G = \langle a, b \,|\, a^3 = b^9 = 1,\, ba = ab^7 \rangle$. Elementi od G su oblika $a^i b^x$ i možemo ih identificirati s uređenim parovima (i, x), za $i = 0, 1, 2$, $x = 0, 1, \ldots, 8$. Tada se elementi množe prema sljedećem pravilu:

$$(i, x) \cdot (j, y) = (i + j, 7^j x + y),$$

pri čemu se na prvoj koordinati računa modulo 3, a na drugoj koordinati modulo 9. Ovo su $(27, 13, 6)$-diferencijski skupovi u grupi G:

$$D_1 = \{a, b^2, ab^2, a^2b^2, b^3, ab^3, b^4, a^2b^4, ab^5, a^2b^5, ab^6, ab^7, b^8\},$$
$$D_2 = \{a^2, b, ab, a^2b, a^2b^3, ab^4, b^5, b^6, a^2b^6, b^7, a^2b^7, ab^8, a^2b^8\}.$$

Budući da su disjunktni i ne sadrže neutralni element 1, ta dva skupa čine $(27, 13, 6)$-ogrlicu u G. ■

Primjer 2.5

Promotrimo grupu $G = \langle a, b \,|\, a^3 = b^{19} = 1,\, ba = ab^7 \rangle$. Riječ je o neabelovoj grupi reda 57 (semidirektnom produktu $\mathbb{Z}_3 \cdot \mathbb{Z}_{19}$). Ako element $a^i b^x$ identificiramo s uređenim parom (i, x), elementi se množe prema istoj formuli kao u prethodnom primjeru, samo se na drugoj koordinati računa modulo 19. Sljedećih sedam skupova su $(57, 8, 1)$ diferencijski skupovi u G:

$$D_1 = \{a, b, a^2, b^2, ab^4, ab^{10}, b^{13}, b^{18}\},$$
$$D_2 = \{ab, ab^5, a^2b^6, a^2b^{13}, b^{15}, a^2b^{14}, ab^{15}, ab^{18}\},$$
$$D_3 = \{a^2b, a^2b^7, a^2b^8, ab^9, ab^{12}, b^{14}, ab^{14}, a^2b^{16}\},$$
$$D_4 = \{ab^2, b^4, a^2b^3, b^9, a^2b^9, b^{11}, b^{12}, a^2b^{18}\},$$
$$D_5 = \{b^3, a^2b^2, b^5, b^8, a^2b^{10}, a^2b^{11}, ab^{17}, a^2b^{17}\},$$
$$D_6 = \{ab^3, b^6, ab^6, ab^8, b^{10}, b^{16}, a^2b^{15}, b^{17}\},$$
$$D_7 = \{a^2b^4, a^2b^5, b^7, ab^7, ab^{11}, a^2b^{12}, ab^{13}, ab^{16}\}.$$

Disjunktni su i ne sadrže neutralni element 1, pa čine $(57, 8, 1)$-ogrlicu u neabelovoj grupi G. Zanimljivo je da ne postoji ogrlica s tim parametrima u cikličkoj grupi $\mathbb{Z}_{57}$. ■

Navedimo sada neke nužne uvjete za postojanje ogrlica u konačnim grupama.

Propozicija 2.2. *Ako postoji (v, k, λ)-ogrlica $\mathcal{A}$, tada λ dijeli $k-1$.*

Dokaz. Iz (2.1.1) slijedi

$$v - 1 = k\frac{k-1}{\lambda}.$$

Dakle, broj diferencijskih skupova u (v, k, λ)-ogrlici je

$$a := \frac{k-1}{\lambda}.$$

To mora biti prirodan broj, pa je nužan uvjet postojanja (v, k, λ)-ogrlice

$$\lambda \mid k - 1.$$

□

Primjer 2.6

U Primjeru 1.2 pokazali smo da postoje $(16, 6, 2)$-diferencijski skupovi u nekim grupama, međutim, ne postoji $(16, 6, 2)$-ogrlica ni u jednoj grupi jer

$$2 \nmid 6 - 1.$$

■

Korolar 2.1. *Ako postoji (v, k, λ)-ogrlica, onda vrijedi $NZD(v, k) = 1$.*

Dokaz. Primijetimo još da za svake dopustive parametre za (v, k, λ)-ogrlicu, vrijedi

$$v - 1 = k \cdot a,$$

gdje je $a = \frac{k-1}{\lambda}$ prirodan broj. Budući da $v - 1$ relativno prost s v, tada je $k \cdot a$ relativno prost s v, pa je i k relativno prost s v. □

Dakle, uvijek ćemo za naše dopustive parametre (v, k, λ), po teoremu 1.11, moći pretpostaviti da za svaki (v, k, λ)-diferencijski skup, postoji jedinstveni normalizirani translat koji je fiksiran svim svojim multiplikatorima.

Propozicija 2.3. *Diferencijski skupovi koji čine (v, k, λ)-ogrlicu nisu transati jedan drugoga.*

Dokaz. Skup translata diferencijskog skupa čini simetrični BIBD. Po lemi 1.1 se svaka dva bloka simetričnog BIBD-a sijeku u točno λ točaka. Diferencijski skupovi koji čine (v, k, λ)-ogrlicu moraju biti disjunktni, stoga, (v, k, λ)-ogrlica ne može sadržavati niti jedan par diferencijskih skupova koji su međusobni translati. □

Koristeći ovu propoziciju također možemo dokazati nepostojanje ogrlica za određene parametre.

Propozicija 2.4. *Ne postoji $(21, 5, 1)$-ogrlica u grupi $(\mathbb{Z}_{21}, +)$.*

Dokaz. U primjeru 1.8 smo pokazali da postoje samo dva skupa translata $(21, 5, 1)$-diferencijskih skupova u grupi $(\mathbb{Z}_{21}, +)$. Da bismo konstruirali $(21, 5, 1)$-oglicu, treba nam $a = (5 - 1)/1 = 4$ diferencijska skupa. Svaki od ta četiri diferencijska skupa mora biti iz posebnog skupa translata, da bi međusobno bili disjunktni. Mi imamo na raspolaganju samo dva skupa translata, dakle, ne postoji $(21, 5, 1)$-ogrlica u grupi $(\mathbb{Z}_{21}, +)$. □

Propozicija 2.5. *Ne postoji* $(273, 17, 1)$*-ogrlica u grupi* $(\mathbb{Z}_{273}, +)$.

Dokaz. Po teoremu 1.9 vrijedi da je 2 multiplikator svakog $(273, 17, 1)$-diferencijskog skupa. Tražimo diferencijske skupove fiksirane multiplikatorom 2, promatrajući cikluse permutacije $x \mapsto 2x \pmod{273}$:

(0)
(1 2 4 8 16 32 64 128 256 239 205 137)
(3 6 12 24 48 96 192 111 222 171 69 138)
(5 10 20 40 80 160 47 94 188 103 206 139)
(7 14 28 56 112 224 175 77 154 35 70 140)
(9 18 36 72 144 15 30 60 120 240 207 141)
(11 22 44 88 176 79 158 43 86 172 71 142)
(13 26 52 104 208 143)
(17 34 68 136 272 271 269 265 257 241 209 145)
(19 38 76 152 31 62 124 248 223 173 73 146)
(21 42 84 168 63 126 252 231 189 105 210 147)
(23 46 92 184 95 190 107 214 155 37 74 148)
(25 50 100 200 127 254 235 197 121 242 211 149)
(27 54 108 216 159 45 90 180 87 174 75 150)
(29 58 116 232 191 109 218 163 53 106 212 151)
(33 66 132 264 255 237 201 129 258 243 213 153)
(39 78 156)
(41 82 164 55 110 220 167 61 122 244 215 157)
(49 98 196 119 238 203 133 266 259 245 217 161)
(51 102 204 135 270 267 261 249 225 177 81 162)
(57 114 228 183 93 186 99 198 123 246 219 165)
(59 118 236 199 125 250 227 181 89 178 83 166)
(65 130 260 247 221 169)
(67 134 268 263 253 233 193 113 226 179 85 170)
(91 182)

(97 194 115 230 187 101 202 131 262 251 229 185)
(117 234 195).

Diferencijske skupove fiksirane multiplikatorom 2 dobijemo kao unije ovih ciklusa. $(273, 17, 1)$-diferencijski skupovi mogu se dobiti samo unijom dva šesteročlana, jednog tročlanog i jednog dvočlanog ciklusa (6+6+3+2=17), ili unijom jednog dvanaestočlanog, jednog tročlanog i jednog dvočlanog ciklusa (12+3+2=17). Za prvi slučaj imamo jednu kombinaciju, i ona ne daje diferencijski skup. U drugom slučaju imamo četrdeset i dvije ($21 \cdot 2 \cdot 1 = 42$) kombinacije. Provjerom vidimo da samo njih dvanaest daje ove $(273, 17, 1)$-diferencijske skupove:

$\{1, 2, 4, 8, 16, 32, 64, 91, 117, 128, 137, 182, 195, 205, 234, 239, 256\}$
$\{5, 10, 20, 39, 40, 47, 78, 80, 91, 94, 103, 139, 156, 160, 182, 188, 206\}$
$\{11, 22, 43, 44, 71, 79, 86, 88, 91, 117, 142, 158, 172, 176, 182, 195, 234\}$
$\{19, 31, 38, 39, 62, 73, 76, 78, 91, 124, 146, 152, 156, 173, 182, 223, 248\}$
$\{23, 37, 46, 74, 91, 92, 95, 107, 117, 148, 155, 182, 184, 190, 195, 214, 234\}$
$\{39, 59, 78, 83, 89, 91, 118, 125, 156, 166, 178, 181, 182, 199, 227, 236, 250\}$
$\{17, 34, 39, 68, 78, 91, 136, 145, 156, 182, 209, 241, 257, 265, 269, 271, 272\}$
$\{67, 85, 91, 113, 117, 134, 170, 179, 182, 193, 195, 226, 233, 234, 253, 263, 268\}$
$\{39, 78, 91, 97, 101, 115, 131, 156, 182, 185, 187, 194, 202, 229, 230, 251, 262\}$
$\{25, 50, 91, 100, 117, 121, 127, 149, 182, 195, 197, 200, 211, 234, 235, 242, 254\}$
$\{29, 53, 58, 91, 106, 109, 116, 117, 151, 163, 182, 191, 195, 212, 218, 232, 234\}$
$\{39, 41, 55, 61, 78, 82, 91, 110, 122, 156, 157, 164, 167, 182, 215, 220, 244\}$.

Zbrojimo li elemente, vidjet ćemo da su svi ovi diferencijski skupovi normalizirani. Vrijedi $NZD(273, 17) = 1$, pa svaki od njih predstavlja svoju klasu translata. Dakle, postoji samo dvanaest skupova translata, a nama treba $(17-1)/1 = 16$ diferencijskih skupova da napravimo $(273, 17, 1)$-ogrlicu. Stoga, ne postoji $(273, 17, 1)$-ogrlica u $(\mathbb{Z}_{273}, +)$. □

2.2 Ogrlice kvadratnih ostataka

U ovom odjeljku ćemo prikazati konstrukciju jedne beskonačne klase (v, k, λ)-ogrlica koju smo zapravo već susreli.

U odjeljku 1.3 definirali smo kvadratne ostatke i kvadratne neostatke na sljedeći način:

$$QR(q) = \{z^2 : z \in \mathbb{F}_q, z \neq 0\},$$
$$QNR(q) = \mathbb{F}_q \backslash (QR(q) \cup \{0\}).$$

U teoremu 1.8 i korolaru 1.3 pokazali smo da su $QR(q)$ i $QNR(q)$ diferencijski skupovi s parametrima $(q, (q-1)/2, (q-3)/4)$ u aditivnoj grupi polja $\mathbb{F}_q$ za sve proste

potencije $q \equiv 3 \pmod 4$. Iz definicije $QR(q)$ i $QNR(q)$ se vidi da su disjunktni i da je $QR(q) \cup QNR(q) = \mathbb{F}_q \setminus \{0\}$. Dakle, vrijedi sljedeći teorem.

Teorem 2.1. *Neka je $q \equiv 3 \pmod 4$ prosta potencija. Tada je $\{QR(q), QNR(q)\}$ $(q, (q-1)/2, (q-3)/4)$-ogrlica u $(\mathbb{F}_q, +)$.*

Primjer 2.7

Konstruirajmo $(23, 11, 5)$-ogrlicu u $(\mathbb{Z}_{23}, +)$. Broj 23 je prost i vrijedi $23 \equiv 3 \pmod 4$, pa izračunajmo $QR(23)$. Računamo samo prvih jedanaest kvadrata, jer se, zbog $x^2 = (-x)^2$, ostali ponavljaju.

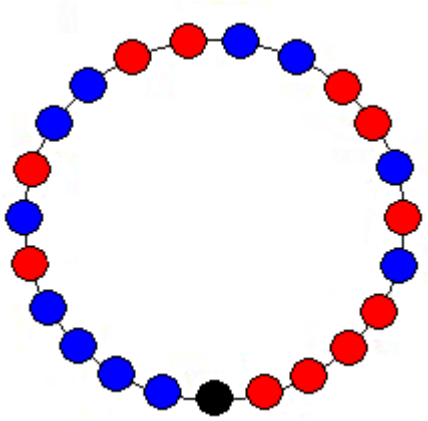
$1^2 = 1, \qquad 2^2 = 4,$

$3^2 = 9, \qquad 4^2 = 16, \qquad 5^2 = 2,$

$6^2 = 13, \qquad 7^2 = 3, \qquad 8^2 = 18,$

$9^2 = 12, \qquad 10^2 = 8, \qquad 11^2 = 6.$

$QR(23) = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$
$QNR(23) = \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}$



$(23, 11, 5)$-ogrlica

$\{QR(23), QNR(23)\}$ je $(23, 11, 5)$-ogrlica u $(\mathbb{Z}_{23}, +)$. ■

Za sljedeći rezultat treba nam *Dirichletov teorem* koji navodimo bez dokaza.

Teorem 2.2 (Dirichletov teorem)**.** *Neka su b, c relativno prosti prirodni brojevi. Tada aritmetički niz $a_n = b + cn$ sadrži beskonačno mnogo prostih brojeva.*

Propozicija 2.6. *Klasa (v, k, λ)-ogrlica u cikličkim grupama dobivena kvadratnim ostatcima je beskonačna.*

Dokaz. Za svaki prost broj q oblika $q = 3 + 4n$ kvadratnim ostatcima dobijemo $(q, (q-1)/2, (q-3)/4)$-ogrlicu u cikličkoj grupi reda q. Brojevi 3 i 4 su relativno prosti pa iz Dirichletovog teorema slijedi da postoji beskonačno takvih cikličkih ogrlica. □

U primjeru 2.3 prikazana je $(27, 13, 6)$-ogrlica u $(\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3, +)$ koja je također dobivena na ovaj način. Aditivna grupa konačnog polja $\mathbb{F}_q$ je ciklička ako je q prost broj, a elementarno Abelova ako je q prava potencija prostog broja. Broj 27 nije prost, pa nismo dobili (v, k, λ)-ogrlicu u cikličkoj, nego u elementarno Abelovoj grupi. Na ovaj način također možemo dobiti $(243, 121, 60)$-ogrlicu u $(\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3, +)$ i $(343, 171, 85)$-ogrlicu u $(\mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_7, +)$.

Navedimo sada definiciju jednog poznatog pojma, o kojem se više može pronaći u [5].

Definicija 2.2. *Za diferencijski skup D u konačnoj grupi $(G,+)$ kažemo da je antisimetrični diferencijski skup (ili "skew Hadamardov" diferencijski skup) ako je G disjunktna unija od D, $-D$ i $\{0\}$.*

Primijetimo da su antisimetrični diferencijski skupovi specijalni slučaj naših (v,k,λ)-ogrlica. Primijetimo i da su ovdje navedeni diferencijski skupovi kvadratnih ostataka primjer antisimetričnih diferencijskih skupova. Preko sedamdeset godina to su bili jedini poznati primjeri. Tek su u [6] i [7] otkrivene dvije nove klase u elementarno Abelovim grupama.

2.3 Kvocijentne ogrlice

Sada ćemo opisati općenitiji način konstruiranja ogrlica. Za početak pokažimo da automorfizam grupe čuva svojstvo *biti diferencijski skup* u pripadnoj grupi.

Lema 2.1. *Neka je D (v,k,λ)-diferencijski skup u konačnoj grupi $(G,+)$, a α automorfizam grupe $(G,+)$. Tada je $\alpha(D)=\{\alpha(x)\colon x\in D\}$ (v,k,λ)-diferencijski skup u $(G,+)$.*

Dokaz. Neka je D (v,k,λ)-diferencijski skup u $(G,+)$, a α automorfizam grupe $(G,+)$. Tada za svaki $d\in G\setminus\{0\}$ postoji točno λ parova $x_i,y_i\in D$, za $1\leq i\leq\lambda$ takvih da je

$$d=x_1-y_1=x_2-y_2=\cdots=x_\lambda-y_\lambda.$$

Tada iz svojstva automorfizma da je $\alpha(-x)=-\alpha(x)$ slijedi da je $\alpha(x-y)=\alpha(x)-\alpha(y)$. Ako automorfizmom α djelujemo na gornju jednakost, dobijemo

$$\alpha(d)=\alpha(x_1)-\alpha(y_1)=\alpha(x_2)-\alpha(y_2)=\cdots=\alpha(x_\lambda)-\alpha(y_\lambda).$$

Automorfizam α je bijekcija i $\alpha(0)=0$, pa iz gornje jednakosti slijedi da je $\alpha(D)$ (v,k,λ)-diferencijski skup u $(G,+)$. □

Promotrimo malo bolje ogrlice kvadratnih ostataka konstruirane u prošlom odjeljku. U odjeljku 1.3 smo pokazali da u slučaju kada je prosta potencija q takva da je $q\equiv 3 \pmod 4$, imamo diferencijski skup $D=QR(q)$ koji je multiplikativna podgrupa polja (u oznaci $\mathbb{F}_q^*$). Tada imamo i drugi diferencijski skup koji je oblika $(-1)D$, dakle njegov suskup. Oni su disjunktni i popločavaju multiplikativnu grupu polja, odnosno tvore ogrlicu, a istovremeno D i $(-1)D$ su elementi kvocijentne grupe $\mathbb{F}_q^*/D$. Općenito vrijedi sljedeća tvrdnja.

Teorem 2.3. *Neka je $\mathbb{F}_q$ konačno polje. Ako postoji diferencijski skup D u $(\mathbb{F}_q,+)$ takav da je D podgrupa od $\mathbb{F}_q^*$, onda postoji ogrlica $\mathcal{A}$ u $(\mathbb{F}_q,+)$, takva da je $\mathcal{A}=\mathbb{F}_q^*/D$.*

Dokaz. Neka je $\mathbb{F}_q$ konačno polje, i neka je D diferencijski skup u grupi $(\mathbb{F}_q, +)$ takav da je i podgrupa od $\mathbb{F}_q^*$. Zbog komutativnosti grupe $\mathbb{F}_q^*$, D je normalna podgrupa od $\mathbb{F}_q^*$. Promotrimo kvocijentnu grupu $\mathcal{A} = \mathbb{F}_q^*/D$. Svaki element od $\mathcal{A}$ je oblika aD za neki $a \in \mathbb{F}_q^*$. Za svaki $a \in \mathbb{F}_q^*$ preslikavanje $x \mapsto ax$ je automorfizam grupe $(\mathbb{F}_q, +)$. Naime, to preslikavanje je bijekcija, a iz distributivnosti množenja prema zbrajanju u polju, vrijedi da za svaki $x, y \in \mathbb{F}_q$ vrijedi

$$a(x + y) = ax + ay.$$

Dakle, pokazali smo da je svaki element kvocijentne grupe $\mathcal{A}$ diferencijski skup s jednakim parametrima kao D. $\mathcal{A}$ se sastoji od međusobno disjunktnih skupova koji u uniji daju $\mathbb{F}_q \setminus \{0\}$, dakle $\mathcal{A}$ je ogrlica u $(\mathbb{F}_q, +)$. □

Dakle, teorem 2.3 nam pokazuje da od diferencijskog skupa u aditivnoj grupi polja koji je podgrupa multiplikativne grupe polja jednostavno možemo konstruirati ogrlicu u aditivnoj grupi polja. Prikazat ćemo to na nekoliko primjera.

Primjer 2.8

$(\mathbb{Z}_{73}, +, *)$ je konačno polje reda 73, a

$$D = \{1, 2, 4, 8, 16, 32, 37, 55, 64\}$$

je $(73, 9, 1)$-diferencijski skup u $(\mathbb{Z}_{73}, +)$. Ako pokažemo da je D podgrupa od $\mathbb{Z}_{73}^*$ po teoremu 2.3 moći ćemo konstruirati ogrlicu. Prisjetimo se činjenice da je multiplikativna grupa polja ciklička, pa je i svaka njena podgrupa ciklička. Sada lako možemo uočiti da je $D = \langle 2 \rangle$. Dakle, uvjeti teorema 2.3 su ispunjeni. Izračunajmo sada elemente od $\mathbb{Z}_{73}^*/D$. Skup D ne sadrži 3, pa izračunajmo $3D$:

$$3D = \{3, 6, 12, 19, 23, 24, 38, 46, 48\}.$$

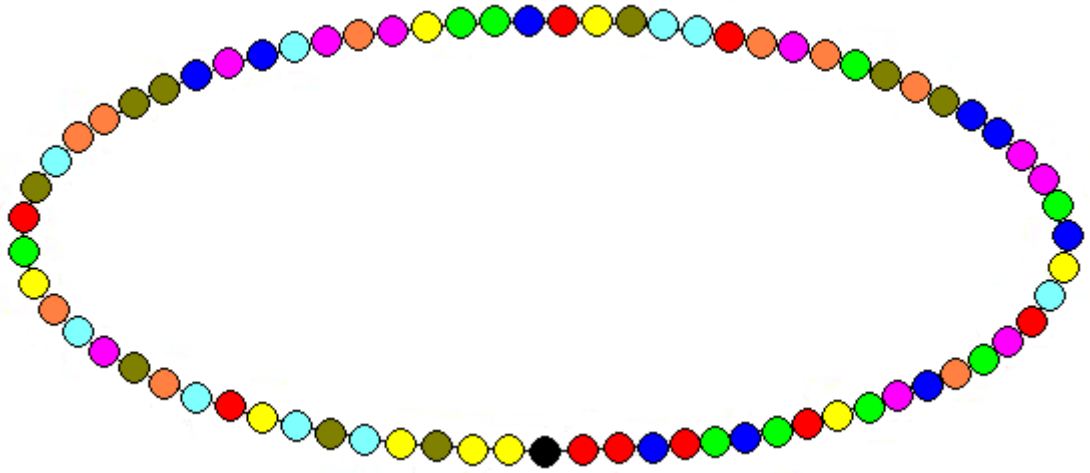
Skupovi D i $3D$ ne sadrže 5, pa izračunajmo $5D$:

$$5D = \{5, 7, 10, 14, 20, 28, 39, 40, 56\}.$$

Analogno dobijemo i ostale diferencijske skupove kvocijentne ogrlice $\mathbb{Z}_{73}^*/D$:

$$\begin{aligned}
9D &= \{9, 18, 36, 41, 57, 65, 69, 71, 72\}, \\
11D &= \{11, 15, 21, 22, 30, 42, 44, 47, 60\}, \\
13D &= \{13, 26, 29, 31, 43, 51, 52, 58, 62\}, \\
17D &= \{17, 33, 34, 45, 53, 59, 63, 66, 68\}, \\
25D &= \{25, 27, 35, 49, 50, 54, 61, 67, 70\}.
\end{aligned}$$

Dakle, $\{D, 3D, 5D, 9D, 11D, 13D, 17D, 25D\}$ je $(73, 9, 1)$-ogrlica u grupi $(\mathbb{Z}_{73}, +)$.



$(73, 9, 1)$-ogrlica u $(\mathbb{Z}_{73}, +)$

■

Općenito, proizvoljni diferencijski skup ne mora biti multiplikativna podgrupa polja, niti multiplikativna podgrupa polja mora biti diferencijski skup. Zato ćemo u sljedećem primjeru probati iskoristiti teorem o Singerovim diferencijskim skupovima i teorem o multiplikatoru kako bismo našli diferencijske skupove.

Primjer 2.9

Po teoremu 1.7 znamo da za prostu potenciju $q = p^n$ postoji $(q^2+q+1, q+1, 1)$-diferencijski skup u $(\mathbb{Z}_{q^2+q+1}, +)$. Tada po teoremu 1.9 znamo da je p multiplikator takvog diferencijskog skupa. Normalizirani translat tog diferencijskog skupa je fiksiran s p, pa mora biti unija ciklusa permutacije $x \mapsto px \pmod{q^2+q+1}$. Kada je q^2+q+1 prost broj, tada se ciklusi te permutacije sastoje od istih elemenata kao i elementi kvocijentne grupe $\mathbb{Z}^*_{q^2+q+1}/\langle p \rangle$. Zato, kada je $|\langle p \rangle| = q+1$, jedan element od $\mathbb{Z}^*_{q^2+q+1}/\langle p \rangle$ mora biti $(q^2+q+1, q+1, 1)$-diferencijski skup u $(\mathbb{Z}_{q^2+q+1}, +)$. Tada su i svi ostali elementi od $\mathbb{Z}^*_{q^2+q+1}/\langle p \rangle$ $(q^2+q+1, +)$-diferencijski skupovi u $(\mathbb{Z}_{q^2+q+1}, +)$ i čine $(q^2+q+1, q+1, 1)$-ogrlicu u $(\mathbb{Z}_{q^2+q+1}, +)$.

Pogledajmo sad kada je ispunjeno da je $|\langle p \rangle| = q+1$. Tražimo najmanji r takav da je $p^r \equiv 1 \pmod{q^2+q+1}$, odnosno da je

$$(p^r - 1)/(p^{2n} + p^n + 1)$$

cijeli broj. Primijetimo da za $r = 3n$ vrijedi

$$p^{3n} - 1 = (p^n)^3 - 1 = (p^n - 1)(p^{2n} + p^n + 1)$$

što je djeljivo s $p^{2n} + p^n + 1$. Dakle, za naš traženi r vrijedi da je $r \leq 3n$, pa je

$$q + 1 = p^n + 1 \leq 3n.$$

Postoje samo tri rješenja te nejednakosti:

$p = 2,\ \ n = 1 \ \dashrightarrow \ \ q^2 + q + 1 = 7$

$p = 2,\ \ n = 2 \ \dashrightarrow \ \ q^2 + q + 1 = 21$ Nije prost!

$p = 2,\ \ n = 3 \ \dashrightarrow \ \ q^2 + q + 1 = 73$

Dakle, na ovaj način mogu se dobiti samo dvije ogrlice: $(73, 9, 1)$-ogrlica prikazana u prethodnom primjeru 2.8 i $(7, 3, 1)$-ogrlica $\mathcal{A}$ u grupi $(\mathbb{Z}_7, +)$, gdje je

$$\begin{aligned}\mathcal{A} =& \{\langle 2\rangle, 3\langle 2\rangle\}\\ =& \big\{\{1, 2, 4\},\ \{3, 5, 6\}\big\}.\end{aligned}$$

Primjetimo da se ova $(7, 3, 1)$-ogrlica može dobiti i kvadratnim ostatcima. ■

Sada ćemo navesti dvije konstrukcije diferencijskih skupova koje će nam koristiti za konstruiranje ogrlica. Konstrukcije su slične diferencijskim skupovima kvadratnih ostataka, samo sada ne gledamo druge, nego četvrte i osme potencije elemenata konačnog polja. Ti diferencijski skupovi, zajedno s diferencijskim skupovima kvadratnih ostataka, spadaju u klasu *ciklotomskih diferencijskih skupova*. Više o ciklotomskim diferencijskim skupovima i dokaz sljedeće činjenice može se pronaći u [5].

Teorem 2.4. *Podskupovi konačnog polja* $\mathbb{F}_q$

- $\mathbb{F}_q^{(4)} = \big\{x^4 \ : x \in \mathbb{F}_q \setminus \{0\}\big\}$, $q = 4t^2 + 1$, *t neparan;*
- $\mathbb{F}_q^{(8)} = \big\{x^8 \ : x \in \mathbb{F}_q \setminus \{0\}\big\}$, $q = 8t^2 + 1 = 64u^2 + 9$, *t, u neparni*

su diferencijski skupovi u aditivnoj grupi polja $\mathbb{F}_q$ *redom s parametrima* $(q, (q - 1)/4, (q - 5)/16)$ *i* $(q, (q - 1)/8, (q - 9)/64)$.

Ovi diferencijski skupovi su nam korisni jer su oni multiplikativne podgrupe polja, odnosno vrijedi sljedeći korolar.

Korolar 2.2. *Neka je* $\mathbb{F}_q$ *konačno polje reda* q.

- *Ako postoji neparan prirodan broj* t, *takav da je* $q = 4t^2 + 1$, *tada je* $\mathbb{F}_q^*/\mathbb{F}_q^{(4)}$ $(q, (q - 1)/4, (q - 5)/16)$*-ogrlica u* $(\mathbb{F}_q, +)$.
- *Ako postoje neparni prirodani brojevi* t, u, *takavi da je* $q = 8t^2 + 1 = 64u^2 + 9$, *tada je* $\mathbb{F}_q^*/\mathbb{F}_q^{(8)}$ $(q, (q - 1)/8, (q - 9)/64)$*-ogrlica u* $(\mathbb{F}_q, +)$.

Dokaz. Pokažimo da su $\mathbb{F}_q^{(4)}$ i $\mathbb{F}_q^{(8)}$ multiplikativne podgrupe polja $\mathbb{F}_q$.

Za svaki $x^4 \in \mathbb{F}_q^{(4)}$ vrijedi da je njegov multiplikativni inverz $(x^{-1})^4$ jer zbog komutativnosti vrijedi da je

$$x^4(x^{-1})^4 = xx^{-1}xx^{-1}xx^{-1}xx^{-1} = 1.$$

Neka su x^4 i y^4 proizvoljni elementi iz $\mathbb{F}_q^{(4)}$. Tada vrijedi da je i $x^4(y^4)^{-1}$ element od $\mathbb{F}_q^{(4)}$, jer opet zbog komutativnosti vrijedi

$$x^4(y^4)^{-1} = x^4(y^{-1})^4 = xy^{-1}xy^{-1}xy^{-1}xy^{-1} = (xy^{-1})^4.$$

Dakle $\mathbb{F}_q^{(4)}$ je mutiplikativna podgrupa polja. Analogno se pokaže i za $\mathbb{F}_q^{(8)}$. Tada po teoremu 2.3 slijedi tvrdnja korolara. □

Primijetimo da ovako dobivene ogrlice sadrže četiri, odnosno osam diferencijskih skupova, odnosno boja. Može se pokazati da je za ove dvije klase q uvijek prost broj, dakle, dobit ćemo samo ogrlice u cikličkim grupama, a ne i u necikličkim kao s kvadratnim ostatcima. Više o tome može se pročitati u [4].

$(37, 9, 2)$-ogrlica iz primjera 2.2 dobivena je pomoću diferencijskog skupa $\mathbb{F}_{37}^{(4)}$. Sljedeći primjer daje još jednu tako dobivenu ogrlicu.

Primjer 2.10

Za $q = 101$ vrijedi da je $q = 4 \cdot 5^2 + 1$, a 5 je neparan broj. Dakle, $\mathbb{F}_{101}^{(4)}$ je $(101, 25, 6)$-differencijski skup. Izračunajmo sve četvrte potencije konačnog polja $\mathbb{Z}_{101}$.

$1^4 = \mathbf{1}$	$2^4 = \mathbf{16}$	$3^4 = \mathbf{81}$	$4^4 = \mathbf{54}$	$5^4 = \mathbf{19}$	$6^4 = \mathbf{84}$	$7^4 = \mathbf{78}$
$8^4 = \mathbf{56}$	$9^4 = \mathbf{97}$	$10^4 = 1$	$11^4 = 97$	$12^4 = \mathbf{31}$	$13^4 = \mathbf{79}$	$14^4 = \mathbf{36}$
$15^4 = \mathbf{24}$	$16^4 = \mathbf{88}$	$17^4 = \mathbf{95}$	$18^4 = \mathbf{37}$	$19^4 = 31$	$20^4 = 16$	$21^4 = 56$
$22^4 = 37$	$23^4 = \mathbf{71}$	$24^4 = \mathbf{92}$	$25^4 = \mathbf{58}$	$26^4 = \mathbf{52}$	$27^4 = \mathbf{80}$	$28^4 = 71$
$29^4 = 79$	$30^4 = 81$	$31^4 = 78$	$32^4 = 95$	$33^4 = 80$	$34^4 = \mathbf{5}$	$35^4 = \mathbf{68}$
$36^4 = \mathbf{87}$	$37^4 = 5$	$38^4 = 92$	$39^4 = 36$	$40^4 = 54$	$41^4 = 84$	$42^4 = 88$
$43^4 = 52$	$44^4 = 87$	$45^4 = \mathbf{25}$	$46^4 = 25$	$47^4 = 68$	$48^4 = 58$	$49^4 = 24$
$50^4 = 19$	$51^4 = 19$	$52^4 = 24$	$53^4 = 58$	$54^4 = 68$	$55^4 = 25$	$56^4 = 25$
$57^4 = 87$	$58^4 = 52$	$59^4 = 88$	$60^4 = 84$	$61^4 = 54$	$62^4 = 36$	$63^4 = 92$
$64^4 = 5$	$65^4 = 87$	$66^4 = 68$	$67^4 = 5$	$68^4 = 80$	$69^4 = 95$	$70^4 = 78$
$71^4 = 81$	$72^4 = 79$	$73^4 = 71$	$74^4 = 80$	$75^4 = 52$	$76^4 = 58$	$77^4 = 92$
$78^4 = 71$	$79^4 = 37$	$80^4 = 56$	$81^4 = 16$	$82^4 = 31$	$83^4 = 37$	$84^4 = 95$
$85^4 = 88$	$86^4 = 24$	$87^4 = 36$	$88^4 = 79$	$89^4 = 31$	$90^4 = 97$	$91^4 = 1$
$92^4 = 97$	$93^4 = 56$	$94^4 = 78$	$95^4 = 84$	$96^4 = 19$	$97^4 = 54$	$98^4 = 81$
$99^4 = 16$	$100^4 = 1$					

Dobili smo dvadeset i pet različitih četvrtih potencija, točno koliko smo i trebali. Te potencije čine $(101, 25, 6)$-diferencijski skup D u $(\mathbb{Z}_{101}, +)$:

$$D = \{1, 5, 16, 19, 24, 25, 31, 36, 37, 52, 54, 56, 58, 68, 78,$$
$$78, 79, 80, 81, 84, 87, 88, 92, 95, 97\}$$

Primjenom teorema 2.3 dobijemo i ostale diferencijske skupove koji čine ogrlicu:

$$\begin{aligned}
2D = \{&2, 3, 7, 10, 11, 15, 32, 35, 38, 41, 48, 50, 55, 57, 59, 61,\\
&62, 67, 72, 73, 74, 75, 83, 89, 93\},\\
4D = \{&4, 6, 9, 13, 14, 17, 20, 21, 22, 23, 30, 33, 43, 45, 47, 49,\\
&64, 65, 70, 76, 77, 82, 85, 96, 100\},\\
8D = \{&8, 12, 18, 26, 27, 28, 29, 34, 39, 40, 42, 44, 46, 51, 53, 60,\\
&63, 66, 69, 86, 90, 91, 94, 98, 99\}.
\end{aligned}$$

Dakle, $\{D, 2D, 4D, 8D\}$ je $(101, 25, 6)$-ogrlica u $(\mathbb{Z}_{101}, +)$. ■

Pomoću diferencijskih skupova $\mathbb{F}_q^{(4)}$ dobijemo još npr. i cikličke ogrlice s parametrima $(197, 49, 12)$, $(677, 169, 42)$, $(2917, 729, 182)$, $(4357, 1089, 272)$ (kompjuterskom pretragom našao sam ukupno sto pedeset i dvije za $q < 10\ 000\ 000$).

$(73, 9, 1)$-ogrlica iz primjera 2.8 se također može dobiti na ovaj način kvocijentnom grupom iz $\mathbb{F}_{73}^{(8)}$. U [4] se može vidjeti da najmanja sljedeća ogrlica dobivena kao $\mathbb{F}_q^*/\mathbb{F}_q^{(8)}$ ima parametre $(104411704393, 13051463049, 1631432881)$.

Kao što smo već spomenuli, multiplikativa grupa konačnog polja je ciklička. Za konačnu cikličku grupu reda n postoji njena podgrupa reda m ako i samo ako m dijeli n. Štoviše, postoji jedinstvena takva podgrupa. Očito, ako je ω generator početne grupe, onda je $\omega^{\frac{n}{m}}$ generator tražene podgrupe. Promatajmo tada dopustive parametre (v, k, λ) gdje je v prosta potencija. Za ne prevelike parametre, koristeći gornje činjenice možemo otkriti postoji li (v, k, λ)-diferencijski skup koji zadovoljava teorem 2.3. Naime, nađemo podgrupu od $\mathbb{F}_v^*$ reda k. Ako je ta podgrupa (v, k, λ)-diferencijski skup u $(\mathbb{F}_v, +)$ tada je teorem 2.3 zadovoljen. U suprotnom, zbog jedinstvenosti takve podgrupe, teorem ne može biti zadovoljen za parametre (v, k, λ). Te činjenice nam mogu poslužiti za kompjutersko traženje ogrlica. Izvršio sam takvo traženje cikličkih ogrlica, odnosno za prost v. Dobije se da za $v \leq 100\ 000$ sve cikličke ogrlice koje se mogu dobiti teoremom 2.3 spadaju u jednu od tri ovdje navedene klase (kvadratnih ostataka, $\mathbb{F}_q^{(4)}$, $\mathbb{F}_q^{(8)}$).

2.4 Cikličke ogrlice normaliziranih diferencijskih skupova

Sve do sad pronađene Abelove ogrlice bile su u aditivnim grupama konačnih polja i sastojale su se od normaliziranih diferencijskih skupova koji se međusobno mogu dobiti djelovanjem automorfizama. U ovom odjeljku promatrat ćemo takav slučaj, ali samo za cikličke grupe.

Definicija 2.3. *Za diferencijske skupove D_1 i D_2 u grupi $(G, +)$ kažemo da su ekvivalentni ako postoji automorfizam α grupe $(G, +)$ i $g_1, g_2 \in G$ takvi da je $\alpha(D_1 + g_1) = D_2 + g_2$.*

Skup svih multiplikatora nekog diferencijskog skupa čini grupu i lako se može pokazati sljedeća činjenica.

Lema 2.2. *Grupe multiplikatora ekvivalentnih Abelovih diferencijskih skupova su jednake.*

Dakle, za prost broj v i (v, k, λ)-diferencijski skup D pokušajmo s njemu ekvivalentnim normaliziranim diferencijskim skupovima konstruirati (v, k, λ)-ogrlicu u grupi $(\mathbb{Z}_v, +)$. Prikažimo to na jednom primjeru.

Primjer 2.11

Skup $\{2, 6, 12, 25, 26, 28\}$ je $(31, 6, 1)$-diferencijski skup u $\mathbb{Z}_{31}$. Taj skup ima dopustive parametre i 31 je prost broj, pa pokušajmo pomoću njega konstruirati ogrlicu od normaliziranih i njemu ekvivalentinih diferencijskih skupova. Negov pripadni normalizirani translat je $D = \{1, 5, 11, 24, 25, 27\}$. D nije podgrupa od $\mathbb{Z}_{31}^*$ pa ne možemo iskoristiti teorem 2.3, ali ćemo pokušati provesti malo općenitiju konstrukciju. Po teoremu 1.9 vidimo da je 5 multiplikator od D. Tada je jasno da je i svaki element od $\langle 5\rangle$ multiplikator. Može se vidjeti da su mu to svi multiplikatori, odnosno $\langle 5\rangle$ je grupa multiplikatora od D. Automorfizmi od $(\mathbb{Z}_v, +)$ su množenje modulo v. Ako je suma elemenata od D jednaka 0, tada za automorfizam α vrijedi da je i suma elemenata od $\alpha(D)$ jednaka 0. Dakle, sve ekvivaletne normalizirane diferencijske skupove od D dobit ćemo množenjem skupa D elementima iz $\mathbb{Z}_{31}^*$. Po lemi 2.2 znamo da je $\langle 5\rangle$ grupa multiplikatora i svakog diferencijskog skupa ekvivalentnog skupu D. Iz toga slijedi da je svaki normalizirani diferencijski skup koje je ekvivalentan s D šesteročlana unija orbita djelovanja grupe $\langle 5\rangle$ na $\mathbb{Z}_{31}$ (gdje je djelovanje definirano kao množenje modulo 31). To slijedi iz činjenice da su normalizirani diferencijski skupovi fiksirani multiplikatorima. Broj 31 je prost pa će te orbite biti $\{0\}$ i elementi kvocijentne grupe $\mathbb{Z}_{31}^*/\langle 5\rangle$. Svi elementi od $\mathbb{Z}_{31}^*/\langle 5\rangle$ su tročlani, naši diferencijski skupovi imaju šest elemenata, pa se normalizirani diferencijski skupovi sastoje od dva elementa te kvocijentne grupe. Primijetimo da kada $|\langle 5\rangle|$ ne bi dijelilo k nego $k-1$, tada ne bismo mogli ovako konstruirati ogrlicu jer bi svaki skup sadržavao 0 pa ne bi bili disjunktni. Tako je naš skup D jednak

$$D = \langle 5\rangle \cup 11\langle 5\rangle.$$

Multiplikativna grupa konačnog polja je ciklička, u našem slučaju generator od $\mathbb{Z}_{31}^*$ je $g = 3$. Upišimo u tablicu sve elemente od $\mathbb{Z}_{31}^*$ kao potencije od 3 i označimo u njoj diferencijski skup D.

g^0	g^1	g^2	g^3	g^4	g^5	g^6	g^7	g^8	g^9
1	3	9	**27**	19	26	16	17	20	29
g^{10}	g^{11}	g^{12}	g^{13}	g^{14}	g^{15}	g^{16}	g^{17}	g^{18}	g^{19}
25	13	8	**24**	10	30	28	22	4	12
g^{20}	g^{21}	g^{22}	g^{23}	g^{24}	g^{25}	g^{26}	g^{27}	g^{28}	g^{29}
5	15	14	**11**	2	6	18	23	7	21

Grupa $\langle 5\rangle$ je reda 3, pa je

$$\langle 5\rangle = \{g^{0\frac{30}{3}}, g^{1\frac{30}{3}}, g^{2\frac{30}{3}}\} = \{g^0, g^{10}, g^{20}\},$$

a diferencijski skup D je

$$D = \langle 5\rangle \cup\ g^3\langle 5\rangle = \{g^0, g^3, g^{10}, g^{13}, g^{20}, g^{23}\}.$$

Množenje skupa s g^n u tablici se očituje kao ciklički pomak u desno za n mjesta. Zbog toga se popločavanje $\mathbb{Z}_{31}^*$ s ekvivalentnim normaliziranim diferencijskim skupovima od D svodi na popločavanje skupa $\{0, 1, \ldots, 29\}$ s translatima (modulo 30) skupa eksponenata $\{0, 3, 10, 13, 20, 23\}$. Skupovi eksponenata uvijek imaju period $\frac{v-1}{|\langle m\rangle|}$, gdje je $\langle m\rangle$ pripadna grupa multiplikatora. U našem slučaju period je 10, pa problem možemo reducirati na popločavanje skupa $\{0, 1, \ldots, 9\}$ s translatima (modulo 10) skupa $\{0, 3\}$. Dakle, želimo pronaći brojeve $b_1, b_2, \ldots, b_5 \in \{0, 1, \ldots, 9\}$ tako da vrijedi

$$\{0 + b_1, 0 + b_2, \ldots, 0 + b_5, 3 + b_1, 3 + b_2, \ldots, 3 + b_5\} = \{0, 1, \ldots, 9\} \ \ (mod\ 10).$$

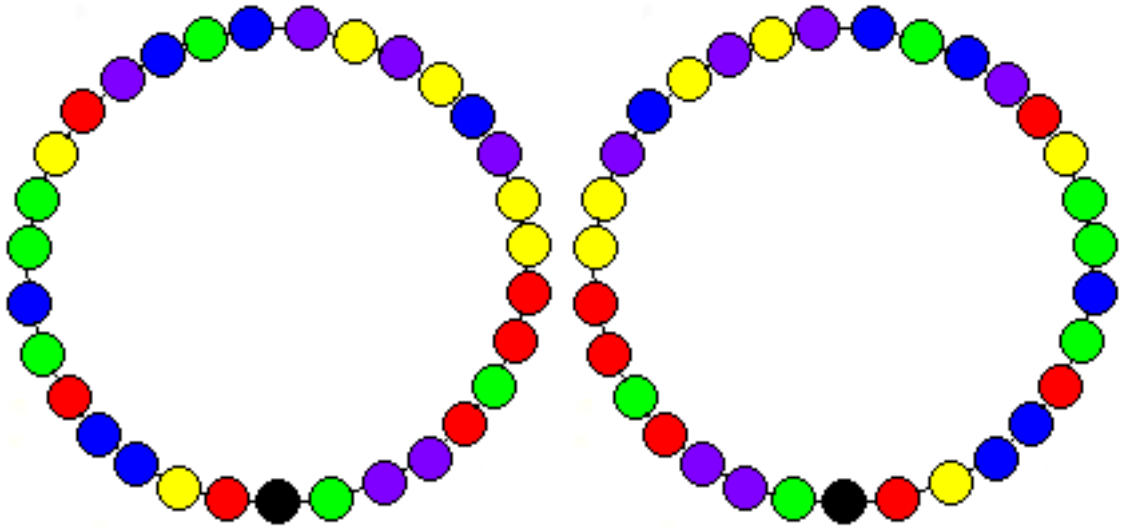
Brojevi b_i predstavljaju automorfizme, točnije automorfizmi su množenje s 3^{b_i}. Ovaj problem ima dva rješenja:

$$0, 2, 4, 6, 8 \quad i \quad 1, 3, 5, 7, 9.$$

Ta rješenja predstavljaju $(31, 6, 1)$-ogrlice $\mathcal{A}_1$ i $\mathcal{A}_2$ u grupi $(\mathbb{Z}_{31}, +)$, prikazane u nastavku.

$D_1 = \{1, 5, 11, 24, 25, 27\}$
$D_2 = \{2, 10, 17, 19, 22, 23\}$
$D_3 = \{3, 4, 7, 13, 15, 20\}$
$D_4 = \{6, 8, 9, 14, 26, 30\}$
$D_5 = \{12, 16, 18, 21, 28, 29\}$
$\mathcal{A}_1 = \{D_1, D_2, D_3, D_4, D_5\}$

$D_6 = \{1, 5, 17, 22, 23, 25\}$
$D_7 = \{2, 3, 10, 13, 15, 19\}$
$D_8 = \{4, 6, 7, 20, 26, 30\}$
$D_9 = \{8, 9, 12, 14, 21, 29\}$
$D_{10} = \{11, 16, 18, 24, 27, 28\}$
$\mathcal{A}_2 = \{D_6, D_7, D_8, D_9, D_{10}\}$



$(31, 6, 1)$-ogrlice $\mathcal{A}_1$ i $\mathcal{A}_2$ u $(\mathbb{Z}_{31}, +)$

Primijetimo da su $(31, 6, 1)$-ogrlice $\mathcal{A}_1$ i $\mathcal{A}_2$ jednake ako ih gledamo kao stvarne ogrlice, odnosno predmet, jer se jedna od druge dobiju okretanjem. To se na slici očituje zrcaljenjem, a skupovno množenjem s -1. Primijetimo još da se kvocijentne ogrlice zrcaljenjem preslikaju same u sebe. ■

Razmišljanja iz gornjeg primjera saželi smo u sljedećoj propoziciji.

Propozicija 2.7. *Neka je p prost broj i D (p, k, λ)-diferencijski skup u $(\mathbb{Z}_p, +)$. Neka je $\langle m \rangle$ grupa multiplikatora od D takva da $|\langle m \rangle| = r$ dijeli k. Neka je $n = \frac{p-1}{r}$, g primitivni element od $\mathbb{Z}_p$ i neka je*

$$D_n = g^{c_1}\langle m \rangle \cup \ g^{c_2}\langle m \rangle \cup \cdots \cup g^{c_{\frac{k}{r}}}\langle m \rangle$$

normalizirani translat od D, pri čemu su $c_1, c_2, \ldots, c_{\frac{k}{r}} \in \{0, 1, \ldots, n-1\}$. Tada postoji (p, k, λ)-ogrlica nastala od normaliziranih diferencijskih skupova ekvivalentnih s D ako i samo ako postoje brojevi $b_1, b_2, \ldots, b_{\frac{k-1}{\lambda}} \in \{0, 1, \ldots, n-1\}$ takvi da

$$b_i - b_j \not\equiv c_u - c_v \ (mod\ n)$$

za sve različite $i, j \in \{1, 2, \ldots, \frac{k-1}{\lambda}\}$ i različite $u, v \in \{1, 2, \ldots, \frac{k}{r}\}$.

Dokaz. Iz razmatranja u primjeru 2.11 vidimo da se ogrlica može konstruirati ako i samo ako postoje $b_1, b_2, \ldots, b_{\frac{k-1}{\lambda}}$ takvi da je

$$\{c_1 + b_1, c_1 + b_2, \ldots, c_1 + b_{\frac{k-1}{\lambda}}, \ldots, c_{\frac{k}{r}} + b_1, c_{\frac{k}{r}} + b_2, \ldots, c_{\frac{k}{r}} + b_{\frac{k-1}{\lambda}}\} = \{0, 1, \ldots, n-1\}.$$

Gornja skupovna jednakost je zadovoljena ako i samo ako je

$$c_u + b_i \not\equiv c_v + b_j \ \ (mod\ n)$$

za sve različite $i, j \in \{1, 2, \ldots, \frac{k-1}{\lambda}\}$ i različite $u, v \in \{1, 2, \ldots, \frac{k}{r}\}$. To je ekvivalentno s

$$b_i - b_j \not\equiv c_u + c_v \ \ (mod\ n)$$

za sve različite $i, j \in \{1, 2, \ldots, \frac{k-1}{\lambda}\}$ i različite $u, v \in \{1, 2, \ldots, \frac{k}{r}\}$. □

A Tablica poznatih popločavanja

U prvoj tablici navedene su poznate Abelove (v, k, λ)-ogrlice za $v \leq 200$. U stupcu "a" upisan je broj diferencijskih skupova u (v, k, λ)-ogrlici, odnosno broj $(k-1)/\lambda$. U stupcu "TIP" označen je tip diferencijskog skupa i način na koji je (v, k, λ)-ogrlica konstruirana, gdje oznake imaju sljedeća značenja:

- $QR(q)$ - Ogrlica kvadratnih ostataka u konačnom polju reda q (odjeljak 2.2, str. 22).
- $\mathbb{F}_q^{(4)}$ - Kvocijentna ogrlica $\mathbb{F}_q^*/\mathbb{F}_q^{(4)}$. (str. 27)
- $\mathbb{F}_q^{(8)}$ - Kvocijentna ogrlica $\mathbb{F}_q^*/\mathbb{F}_q^{(8)}$. (str. 27)
- ★ - Cikličke ogrlice opisane u odjeljku 2.4

U stupcu "OGRLICA" navedena je ogrlica. U slučaju kvocijentnih ogrlica ($QR(q)$,$\mathbb{F}_q^{(4)}$ i $\mathbb{F}_q^{(8)}$) upisan je samo diferencijski skup koji je multiplikativna podgrupa pomoću koje se gradi kvocijentna grupa. U slučaju ★, upisani su svi diferencijski skupovi koji čine ogrlicu. Elementi iz $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ zapisani su skraćeno ((a,b,c) → abc).

(v, k, λ)	a	GRUPA	TIP	OGRLICA
$(7, 3, 1)$	2	$\mathbb{Z}_7$	$QR(7)$	$\{1, 2, 4\}$
$(11, 5, 2)$	2	$\mathbb{Z}_{11}$	$QR(11)$	$\{1, 3, 4, 5, 9\}$
$(19, 9, 4)$	2	$\mathbb{Z}_{19}$	$QR(19)$	$\{1, 4, 5, 6, 7, 9, 11, 16, 17\}$
$(23, 11, 5)$	2	$\mathbb{Z}_{23}$	$QR(23)$	$\{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$
$(27, 13, 6)$	2	$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	$QR(27)$	$\{001, 221, 022, 211, 121, 021, 020, 102,$ $110, 202, 111, 120, 100\}$
$(31, 6, 1)$	5	$\mathbb{Z}_{31}$	★	$\{1, 5, 11, 24, 25, 27\}$ $\{3, 4, 7, 13, 15, 20\}$ $\{2, 10, 17, 19, 22, 23\}$ $\{6, 8, 9, 14, 26, 30\}$ $\{12, 16, 18, 21, 28, 29\}$
		$\mathbb{Z}_{31}$	★	$\{1, 5, 17, 22, 23, 25\}$ $\{2, 3, 10, 13, 15, 19\}$ $\{4, 6, 7, 20, 26, 30\}$ $\{8, 9, 12, 14, 21, 29\}$ $\{11, 16, 18, 24, 27, 28\}$
$(31, 15, 7)$	2	$\mathbb{Z}_{31}$	$QR(31)$	$\{1, 2, 3, 4, 6, 8, 12, 15, 16, 17, 23, 24, 27,$ $29, 30\}$
$(37, 9, 1)$	4	$\mathbb{Z}_{37}$	$\mathbb{F}_{37}^{(4)}$	$\{1, 7, 9, 10, 12, 16, 26, 33, 34\}$

(v,k,λ)	a	GRUPA	TIP	OGRLICA
$(43,21,10)$	2	$\mathbb{Z}_{43}$	$QR(43)$	$\{1,4,6,9,10,11,13,14,15,16,17,21,23,24,25,31,32,34,36,38,40,41\}$
$(47,23,11)$	2	$\mathbb{Z}_{47}$	$QR(47)$	$\{1,2,3,4,6,7,8,9,12,14,16,17,18,21,24,25,27,28,32,34,36,37,42\}$
$(59,29,14)$	2	$\mathbb{Z}_{59}$	$QR(59)$	$\{1,3,4,5,7,9,12,15,16,17,19,20,21,22,25,26,27,28,29,35,36,41,45,46,48,49,51,53,57\}$
$(67,33,16)$	2	$\mathbb{Z}_{67}$	$QR(67)$	$\{1,4,6,9,10,14,15,16,17,19,21,22,23,24,25,26,29,33,35,36,37,39,40,47,49,54,55,56,59,60,62,64,65\}$
$(71,35,17)$	2	$\mathbb{Z}_{71}$	$QR(71)$	$\{1,2,3,4,5,6,8,9,10,12,15,16,18,19,20,24,25,27,29,30,32,26,37,38,40,43,45,48,49,50,54,57,58,60,64\}$
$(73,9,1)$	8	$\mathbb{Z}_{73}$	$\mathbb{F}_{73}^{(8)}$	$\{1,2,4,8,16,32,37,55,64\}$
$(79,39,19)$	2	$\mathbb{Z}_{79}$	$QR(79)$	$\{1,2,4,5,8,9,10,11,13,16,18,19,20,21,22,23,25,26,31,32,36,38,40,42,44,45,46,49,50,51,52,55,62,64,65,67,72,73,76\}$
$(83,41,20)$	2	$\mathbb{Z}_{83}$	$QR(83)$	$\{1,3,4,7,9,10,11,12,16,17,21,23,25,26,27,28,29,30,31,33,36,37,38,40,41,44,48,49,51,59,61,63,64,65,68,69,70,75,77,78,81\}$
$(101,25,6)$	4	$\mathbb{Z}_{101}$	$\mathbb{F}_{101}^{(4)}$	$\{1,5,16,19,24,25,31,36,37,52,54,56,58,68,71,78,79,80,81,84,87,88,92,95,97\}$
$(103,51,25)$	2	$\mathbb{Z}_{103}$	$QR(103)$	$\{1,2,4,7,8,9,13,14,15,16,17,18,19,23,25,26,28,29,30,32,33,34,36,38,41,46,49,50,52,55,56,58,59,60,61,63,64,66,68,72,76,79,81,82,83,91,92,93,97,98,100\}$
$(107,53,26)$	2	$\mathbb{Z}_{107}$	$QR(107)$	$\{1,3,4,9,10,11,12,13,14,16,19,23,25,27,29,30,33,34,35,36,37,39,40,41,42,44,47,48,49,52,53,56,57,61,62,64,69,75,76,79,81,83,85,86,87,89,90,92,99,100,101,102,105\}$
$(127,63,31)$	2	$\mathbb{Z}_{127}$	$QR(127)$	$\{1,2,4,8,9,11,13,15,16,17,18,19,21,22,25,26,30,31,32,34,35,36,37,38,41,42,44,47,49,50,52,60,61,62,64,68,69,70,71,72,73,74,76,79,81,82,84,87,88,94,98,99,100,103,104,107,113,115,117,120,121,122,124\}$

(v,k,λ)	a	GRUPA	TIP	OGRLICA
$(131,65,32)$	2	$\mathbb{Z}_{131}$	$QR(131)$	$\{1,3,4,5,7,9,11,12,13,15,16,20,21,25,$ $27,28,33,34,35,36,38,39,41,43,44,45,46,$ $48,49,52,53,55,58,59,60,61,62,63,64,65,$ $74,75,77,80,81,84,89,91,94,99,100,101,$ $102,105,107,108,109,112,113,114,117,$ $121,123,125,129\}$
$(139,69,34)$	2	$\mathbb{Z}_{139}$	$QR(139)$	$\{1,4,5,6,7,9,11,13,16,20,24,25,28,29,$ $30,31,34,35,36,37,38,41,42,44,45,46,47,$ $49,51,52,54,55,57,63,64,65,66,67,69,71,$ $77,78,79,80,81,83,86,89,91,96,99,100,$ $106,107,112,113,116,117,118,120,121,$ $122,124,125,127,129,131,136,137\}$
$(151,75,37)$	2	$\mathbb{Z}_{151}$	$QR(151)$	$\{1,2,4,5,8,9,10,11,16,17,18,19,20,21,$ $22,25,29,31,32,34,36,37,38,39,40,42,43,$ $44,45,47,49,50,55,58,59,62,64,68,69,72,$ $74,76,78,80,81,84,85,86,88,90,91,94,95,$ $97,98,99,100,103,105,110,116,118,121,$ $123,124,125,127,128,136,137,138,139,$ $144,145,148\}$
$(163,81,40)$	2	$\mathbb{Z}_{163}$	$QR(163)$	$\{1,4,6,9,10,14,15,16,21,22,24,25,26,33,$ $34,35,36,38,39,40,41,43,46,47,49,51,53,$ $54,55,56,57,58,60,61,62,64,65,69,71,74,$ $77,81,83,84,85,87,88,90,91,93,95,96,97,$ $100,104,111,113,115,118,119,121,126,$ $131,132,133,134,135,136,140,143,144,$ $145,146,150,151,152,155,156,158,160,$ $161\}$
$(167,83,41)$	2	$\mathbb{Z}_{167}$	$QR(167)$	$\{1,2,3,4,6,7,8,9,11,12,14,16,18,19,21,$ $22,24,25,27,28,29,31,32,33,36,38,42,44,$ $47,48,49,50,54,56,57,58,61,62,63,64,65,$ $66,72,75,76,77,81,84,85,87,88,89,93,94,$ $96,97,98,99,100,107,108,112,114,115,$ $116,121,122,124,126,127,128,130,132,$ $133,137,141,144,147,150,152,154,157,$ $162\}$
$(179,89,44)$	2	$\mathbb{Z}_{179}$	$QR(179)$	$\{1,3,4,5,9,12,13,14,15,16,17,19,20,22,$ $25,27,29,31,36,39,42,43,45,46,47,48,49,$ $51,52,56,57,59,60,61,64,65,66,67,68,70,$ $74,75,76,77,80,81,82,83,85,87,88,89,93,$ $95,100,101,106,107,108,110,116,117,121,$ $124,125,126,129,135,138,139,141,142,$ $144,145,146,147,149,151,153,155,156,$ $158,161,168,169,171,172,173,177\}$

(v,k,λ)	a	GRUPA	TIP	OGRLICA
$(191,95,47)$	2	$\mathbb{Z}_{191}$	$QR(191)$	$\{1,2,3,4,5,6,8,9,10,12,13,15,16,17,18,$ $20,23,24,25,26,27,30,32,34,36,39,40,43,$ $45,46,48,49,50,51,52,54,59,60,64,65,67,$ $68,69,72,75,77,78,79,80,81,85,86,90,92,$ $96,97,98,100,102,103,104,107,108,109,$ $115,117,118,120,121,125,128,129,130,$ $133,134,135,136,138,144,147,149,150,$ $153,154,156,158,160,162,163,169,170,$ $172,177,180,184\}$
$(197,49,12)$	4	$\mathbb{Z}_{197}$	$\mathbb{F}_{197}^{(4)}$	$\{1,16,23,24,28,29,34,36,37,40,42,49,51,$ $53,54,59,60,61,63,70,76,81,85,88,90,$ $100,101,104,105,114,132,133,135,142,$ $150,154,156,158,164,171,172,175,178,$ $182,187,188,190,191,193\}$
$(199,99,49)$	2	$\mathbb{Z}_{199}$	$QR(199)$	$\{1,2,4,5,7,8,9,10,13,14,16,18,20,23,25,$ $26,28,29,31,32,33,35,36,40,43,45,46,47,$ $49,50,51,52,53,56,57,58,61,62,63,64,65,$ $66,70,72,79,80,81,86,89,90,91,92,94,98,$ $100,102,103,104,106,111,112,114,115,$ $116,117,121,122,123,124,125,126,128,$ $130,131,132,139,140,144,145,151,155,$ $157,158,160,161,162,165,169,172,175,$ $177,178,180,182,184,187,188,193,196\}$

U sljedećoj tablici su primjeri poznatih neabelovih (v,k,λ)-ogrlica. Dobiveni su kompjuterskom pretragom u grupama malog reda.

parametri	$(27,13,6)$
grupa	$\langle a,b : a^3=b^9=1,\ ba=ab^7\rangle$
ogrlica	$\{a,b^2,ab^2,a^2b^2,b^3,ab^3,b^4,a^2b^4,ab^5,a^2b^5,ab^6,ab^7,b^8\}$ $\{a^2,b,ab,a^2b,a^2b^3,ab^4,b^5,b^6,a^2b^6,b^7,a^2b^7,ab^8,a^2b^8\}$

parametri	$(57,8,1)$
grupa	$\langle a,b : a^3=b^{19}=1,\ ba=ab^7\rangle$
ogrlica	$\{a,b,a^2,b^2,ab^4,ab^{10},b^{13},b^{18}\}$ $\{ab,ab^5,a^2b^6,a^2b^{13},b^{15},a^2b^{14},ab^{15},ab^{18}\}$ $\{a^2b,a^2b^7,a^2b^8,ab^9,ab^{12},b^{14},ab^{14},a^2b^{16}\}$ $\{ab^2,b^4,a^2b^3,b^9,a^2b^9,b^{11},b^{12},a^2b^{18}\}$ $\{b^3,a^2b^2,b^5,b^8,a^2b^{10},a^2b^{11},ab^{17},a^2b^{17}\}$ $\{ab^3,b^6,ab^6,ab^8,b^{10},b^{16},a^2b^{15},b^{17}\}$ $\{a^2b^4,a^2b^5,b^7,ab^7,ab^{11},a^2b^{12},ab^{13},ab^{16}\}$

Bibliografija

[1] Douglas R. Stinson: *Combinatorial Designs: Construction and Analysis*, Springer, New York, 2004.

[2] Charles J. Colbourn, Jeffrey H. Dintz: *Handbook of Combinatorial Designs, Second Edition*, Chapman & Hall, 2007.

[3] Darko Veljan: *Kombinatorna i diskretna matematika*, Algoritam, Zagreb, 2001.

[4] Jeffrey H. Dinitz, Douglas R. Stinson: *Contemporary Design Theory: A Collection of Surveys*, Wiley, New Jersey, 1992.

[5] Leonard D. Baumert: *Cyclic Difference Sets*, Springer-Verlag, 1971.

[6] Cunsheng Ding, Jin Yuan: *A family of skew Hadamard difference sets*, Journal of Combinatorial Theory, Series A 113 (2006) 1526-1535

[7] Cunsheng Ding, Zeying Wang, Qing Xiang: *Skew Hadamard difference sets from the Ree-Tits slice symplectic spreads in* $PG(3, 3^{2h+1})$, Journal of Combinatorial Theory, Series A 114 (2007) 867-887