Konačne grupe, dizajni i kodovi

Andrea Švob
(asvob@math.uniri.hr)

15. ožujka 2011.

- J. Moori, Finite Groups, Designs and Codes, NATO Science for Peace and Security, Series D: Information and Communication Security, Vol.29 (2011), 202-230.

Dizajni

Definicija

Konačna incidencijska struktura $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ *je* $t - (v, k, \lambda)$ **dizajn** *ako vrijedi sljedeće:*

1. $|\mathcal{P}| = v$,
2. *svaki element skupa* $\mathcal{B}$ *incidentan je s točno* k *elemenata skupa* $\mathcal{P}$,
3. *svakih* t *elemenata skupa* $\mathcal{P}$ *incidentno je s točno* λ *elemenata skupa* $\mathcal{B}$.

Linearni kodovi

Definicija

Neka je q prim broj i neka je F konačno polje reda q te neka je $n \in \mathbb{N}$.
Linearan kod duljine n je linearni podprostor vektorskog prostora F^n.

Kod je binaran za $q = 2$.
Elementi koda zovu se riječi koda.

Oznaka: $[n, k, d]_{|F|}$
n je dimenzija vektorskog prostora
k je dimenzija koda
d je minimalna težina, tj. $d = \min\{w(c) | \, c \in C, \, c \neq 0\}$

Težina riječi koda

Za $x \in F^n$, težina $w(x)$ od x je definirana sa

$$w(x) = d(x, 0) = |\{i \in \mathbb{N} | \, i \leq n, \, x_i \neq 0\}|$$

Djelovanja grupe na skup

Definicija

Grupa G **djeluje** *na konačan skup Ω ako postoji preslikavanje $f : G \times \Omega \to \Omega$ takvo da vrijedi*

1. $f(g_1, f(g_2, x)) = f(g_1 g_2, x),\ \forall x \in \Omega,\ \forall g_1,\ g_2 \in G,$
2. $f(1, x) = x,\ \forall x \in \Omega.$

Slika djelovanja elementa $g \in G$ na element $x \in \Omega$ označava se $g.x$ ili x^g.

Definicija

Skup $G_x = \{g \in G \mid g.x = x\} \leq G$ naziva se **stabilizator** *elementa x za djelovanje grupe G.*

Definicija

Neka je G grupa i $f : G \longrightarrow GL(n, F)$ homomorfizam. Tada kažemo da je f **matrična reprezentacija** *grupe G stupnja n nad poljem F.*

Definicija

Neka je $f : G \longrightarrow GL(n, F)$ reprezentacija grupe G nad poljem F. Preslikavanje $\chi : G \longrightarrow F$ definirana s

$$\chi(g) = tr(f(g)), \forall g \in G$$

zove se **karakter** *od f.*

Definicija

Neka je $t : G \to GL(V)$ *reprezentacija od* G. *Podprostor* W *vektorskog prostora* V *zove se* $G-$**podprostor** *ako je* $wt(g) \in W$, *za sve* $g \in G$ *i sve* $w \in W$.

Definicija

Reprezentacija $t : G \to GL(V)$ *je* **ireducibilna** *nad poljem* F *ako ne postoje netrivijalni* $G-$*podprostori. U suprotnom, reprezentacija je* **reducibilna**. *Kažemo da je potpuno reducibilna ako za svaki* $G-$*podprostor* W *postoji podprostor* W' *takav da je* $V = W \oplus W'$.

Definicija

Ako je $\phi : G \longrightarrow F$ *funkcija koja je konstantna na konjugacijskim klasama od* G*, tj. vrijedi da je* $\phi(g) = \phi(xgx^{-1})$*, za svaki* $x \in G$*, tada kažemo da je* ϕ **funkcija klasa**.

Karakter je funkcija klasa

Vrijedi

$$\chi(hgh^{-1}) = \chi(g), \forall g, h \in G.$$

Karakter χ je konstantan na konjugacijskim klasama grupe G.

Tablica karaktera

Neka je G konačna grupa, F polje. **Tablica karaktera** grupe G je $k \times k$ matrica $X = [\chi_i(g_j)]$ gdje su redovi matrice $\chi_1, \chi_2, ..., \chi_k$ ireducibilni karakteri od G, a stupci matrice $C_1, C_2, ..., C_k$ konjugacijske klase takve da je $g_j \in C_j$.

Primjer (S_3)

	1	3	2
S_3	1	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Teorem

Neka grupa G djeluje na skup Ω. Tada je $\pi : G \to S(\Omega)$, preslikavanje koje svakom elementu g grupe G pridružuje bijekciju $\pi_g : \Omega \to \Omega$, $\pi_g(x) = g.x$, homomorfizam grupa (homomorfizam induciran djelovanjem grupe G na skup Ω). Obrnuto, ako postoji homomorfizam $\pi : G \to S(\Omega)$, onda grupa G djeluje na skup Ω.

Definicija

Homomorfizam $\pi : G \to S(\Omega)$ naziva se **permutacijska reprezentacija** *grupe G.*

Definicija

Djelovanje grupe G na skup Ω definira permutacijsku reprezentaciju π sa odgovarajućim **permutacijskim karakterom** *χ_π, u oznaci $\chi(G|\Omega)$.*

Lema

(i) *Djelovanje grupe G na skup Ω izomorfno je djelovanju grupe G na G/G_α tj. izomorfno je djelovanju na skupu svih lijevih klasa od G_α u G. Vrijedi $\chi(G|\Omega) = \chi(G|G_\alpha)$.*

(ii) *Za svaki g iz G, $\chi(G|\Omega)(g)$ jednak je broju fiksnih točaka u Ω fiksirani s g.*

Lema

Neka je H podgrupa grupe G i neka je Ω skup svih konjugata od H u G. Vrijedi:

(i) $G_H = N_G(H)$, $\chi(G|\Omega) = \chi(G|N_G(H))$.

(ii) *Za bilo koji element g u G, broj konjugata od H u G koje sadrže g dan je s:*

$$\chi(G|\Omega)(g) = \sum_{i=1}^{m} \frac{|C_G(g)|}{|C_{N_G(H)}(x_i)|} = [N_G(H) : H]^{-1} \sum_{i=1}^{k} \frac{|C_G(g)|}{|C_H(h_i)|}.$$

Korolar

Ako je G konačna jednostavna grupa i M maksimalna podgrupa grupe G, tada je broj χ, broj konjugata od M u G koji sadrže g dan s:

$$\chi(G|M)(g) = \sum_{i=1}^{k} \frac{C_G(g)}{C_M(x_i)}.$$

Teorem (Klasifikacija konačnih jednostavnih grupa)

Svaka konačna jednostavna grupa izomorfna je jednoj od sljedećih grupa:

1. *Grupi prostog reda,*
2. *alternirajućoj grupi,* $A_n, n \geq 5$,
3. *konačnoj grupi Lievog tipa,*
4. *jednostavnoj sporadičnoj grupi.*

Pretpostavke:

- G je konačna, jednostavna grupa,
- M je maksimalna podgrupa grupe G,
- Ω je skup svih konjugata od M u G,
- nX je konjugacijska klasa elemenata reda n u grupi G, $g \in nX$, $C_g = [g] = nX$,
- $\chi_M = \chi(G|M)$ je permutacijski karakter dobiven pomoću djelovanja grupe G na skup Ω.

Teorem

Neka je G konačna jednostavna grupa, M maksimalna podgrupa od G, a nX konjugacijska klasa elemenata reda n u G takvih da vrijedi $M \cap nX \neq \emptyset$. Tada je

$$1 - (|nX|, |M \cap nX|, \chi_M(g))$$

dizajn sa skupom blokova

$$\mathcal{B} = \{(M \cap nX)^y | y \in G\}$$

i skupom točaka

$$\mathcal{P} = nX.$$

Grupa G, kao grupa automorfizama dizajna $\mathcal{D}$, djeluje primitivno na skup blokova, a tranzitivno (ne nužno primitivno) na skup točaka.

Napomena 1.

U $1-(v,k,\lambda)$ dizajnu vrijedi relacija $k \cdot b = \lambda \cdot v$. Tada dobivamo

$$k = |M \cap nX| = \frac{\chi_M(g) \cdot |nX|}{[G : M]}.$$

Također, $\widetilde{\mathcal{D}}$ označava komplement dizajna D tj. $\widetilde{\mathcal{D}}$ je dizajn s parametrima $1-(v, v-k, \widetilde{\lambda})$ gdje je $\widetilde{\lambda} = \lambda \cdot \frac{v-k}{k}$.

Napomena 2.

Ako je $\lambda = 1$, tada je $\mathcal{D}$, $1-(v,k,1)$ dizajn. Budući da je nX disjunktna unija b blokova, za svaki blok veličine k, vrijedi:
$Aut(\mathcal{D}) = S_k \wr S_b = (S_k^b) : S_b$. Tada, za svaki p vrijedi
$C = C_p(\mathcal{D}) = [|nX|, b, k]_p$, $Aut(C) = Aut(\mathcal{D})$.

Napomena 3.

Dizajni $\mathcal{D}$ konstruirani na ovaj način ne moraju biti simetrični dizajni.
Dizajn $\mathcal{D}$ će biti simetričan ako i samo ako vrijedi

$$b = |\mathcal{B}| = v = |\mathcal{P}| \iff [G : M] = |nX| \iff$$

$$[G : M] = [G : C_G(g)] \iff |M| = |C_G(g)|.$$

Alternirajuća grupa

- Konačna, jednostavna grupa parnih permutacija definirana na konačnom skupu $\{1, ..., n\}$,
- ima 5 konjugacijskih klasa maksimalnih podgrupa, te 9 konjugacijskih klasa elemenata.

No.	Struktura	Index	Red
Max[1]	A_6	7	360
Max[2]	$PSL_2(7)$	15	168
Max[3]	$PSL_2(7)$	15	168
Max[4]	S_5	21	120
Max[5]	$(A_4 \times 3) : 2$	35	72

nX	$\lvert nX \rvert$	$C_G(g)$	Max.centralizator
$2A$	105	$D_8 : 3$	Ne
$3A$	70	$A_4 \times 3 \cong (2^2 \times 3) : 3$	Ne
$3B$	280	3×3	Ne

Primjer (Konstrukcija dizajna)

Neka je $G = A_7, M = A_6, nX = 3A$. *Tada imamo:*

- $b = [G : M] = 7, v = |3A| = 70, k = |M \cap 3A| = 40,$
- *koristeći tablicu karaktera od* A_7, *imamo:* $\chi_M = \chi_1 + \chi_2 = 1a + 6a$, $g \in 3A$, $\chi_M(g) = 1 + 3 = 4 = \lambda$,
- *konstruiran je* **nesimetričan,** $1 - (70, 40, 4)$ **dizajn** $\mathcal{D}$,
- *grupa* A_7 *djeluje primitivno na* 7 *blokova,*
- $C_{A_7}(g) = A_4 \times 3$ *nije maksimalna podgrupa u* A_7, *pa vrijedi da* A_7 *djeluje neprimitivno na* 70 *točaka,*
- $\widetilde{\mathcal{D}}$ *je* $1 - (70, 30, 3)$, $Aut(\mathcal{D}) \cong 2^{35} : S_7 \cong 2^5 \wr S_7$, $|Aut(\mathcal{D})| = 2^{39}.3^2.5.7.$

Primjer (Konstrukcija kodova)

- *Kod C konstruiranog dizajna je binaran,* $[70, 6, 32]_2$ *kod,*
- *kod je samoortogonalan sa težinskom distribucijom* $< 0, 1 >, < 32, 35 >, < 40, 28 >$,
- *kod C je ireducibilna reprezentacija grupe G,*
- $Aut(C) \cong 2^{35} : S_8, |Aut(C)| = 2^{42}.3^2.5.7$,
- $Aut(C) \geq Aut(\mathcal{D})$, $Aut(\mathcal{D})$ *nije normalna podgrupa* $Aut(C)$,
- $C^{\perp} = [70, 64, 2]$.

Ostali rezultati:

M	nX	Dizajn	$Aut(\mathcal{D})$	Kod	$Aut(C)$
A_6	$3A$	$1-(70,40,4)$	$25 \wr S_7$	$[70,6,32]_2$	$2^{35} : S_8$
A_6	$2A$	$1-(105,45,3)$	$S_3^5 \wr S_7$	$[105,7,45]_2$	$S_3^5 \wr S_7$
S_5	$2A:1$	$1-(105,25,5)$			
PSL_2^7	$2A:1$	$1-(105,21,3)$			
PSL_2^7	$3B:1$	$1-(280,56,3)$			

Vrijedi teorem:

Teorem

Za projektivnu specijalnu linearnu grupu,

$$PSL_2(p^k) = SL_2(p^k)/Z(SL_2(p^k)),$$

vrijedi

1. $PSL_2(p^k)$ *je jednostavna grupa za* $p^k > 3$,
2.

$$|PSL_2(p^k)| = \begin{cases} (p^k+1)p^k(p^k-1), & p = 2, \\ \frac{1}{2}(p^k+1)p^k(p^k-1), & p = \textit{neparan, prost}. \end{cases}$$

- $|PSL_2(11)| = 660 = 2^2 \times 3 \times 5 \times 11$
- ima 4 konjugacijske klase maksimalnih podgrupa te 8 konjugacijskih klasa elemenata.

No.	Struktura	Index	Red
Max[1]	$F_{55} = 11 : 5$	12	55
Max[2]	A_5	11	60
Max[3]	A_5	11	60
Max[4]	D_{12}	55	12

nX	$\|nX\|$	$C_G(g)$	Max.centralizator
$2A$	55	D_{12}	Da
$3A$	110	Z_6	Ne
$5A$	132	Z_5	Ne
$5B$	132	Z_5	Ne
$6A$	110	Z_6	Ne
$11A$	60	Z_{11}	Ne
$11B$	60	Z_{11}	Ne

Rezultati dobiveni iz grupe $PSL_2(11)$:

Dizajn	$Aut(\mathcal{D})$	Kod	$Aut(C)$
$1-(132,22,2)$	$2^{66}:S_{12}$	$[132,11,22]_2$	$2^{66}:S_{12}$
$1-(60,5,1)$	$(S_5)^{12}:S_{12}$	$[60,12,5]_2$	$(S_5)^{12}:S_{12}$
$1-(55,15,3)$	$PSL_2(11)$	$[55,11,15]_2$	$PSL_2(11):2$
$1-(110,20,2)$	$2^{55}:S_{11}$	$[110,10,20]_2$	$2^{55}:S_{11}$
$1-(132,12,1)$	$(S_{12})^{11}:S_{11}$	$[132,121,2]_2$	$(S_{12})^{11}:S_{11}$
$1-(55,7,7)$	$PSL_2(11):2$	$[55,35,4]_2$	$PSL_2(11):2$
$1-(110,2,1)$	$2^{55}:S_{55}$	$[110,55,2]_2$	$2^{55}:S_{55}$

Pretpostavke:

- $G = PSL_2(q)$, M je maksimalna podgrupa grupe G, Ω je skup svih konjugata podgrupe M u grupi G,
- G djeluje strogo $2-$ tranzitivno na Ω,
- $M = F_q : F_q^* = F_q : Z_{q-1}$, q =paran,
- $M = F_q : F_{\frac{q-1}{2}}$, q =neparan,
- $\chi = 1 + \psi$, χ =permutacijski karakter djelovanja, ψ =ireducibilni karakter,
- djelovanje je strogo 2-tranzitivno, jedini element koji fiksira 3 različita elementa skupa Ω je 1_G tj:

$$\forall g \in G, g \neq 1_G \Rightarrow \lambda = \chi(g) \in \{0, 1, 2\}.$$

Propozicija

Neka je $G = PSL_2(q)$, M *maksimalna podgrupa grupe* G *indeksa* $q+1$, *a* Ω *skup svih konjugata podgrupe* M *u grupi* G. *Pretpostavimo da je* $g \in nX \subseteq G$ *element koji fiksira točno jednu točku i ne smanjujući općenitost možemo pretpostaviti da* $g \in M$. *Tada za konstruirani dizajn vrijedi* $r = \lambda = 1$. *Također, vrijedi:*

(i) *Ako je* q *neparan, tada je* $|g^G| = \frac{1}{2}(q^2-1), |M \cap g^G| = \frac{1}{2}(q-1)$ *i* $\mathcal{D}$ *je*

$$1 - (\frac{1}{2}(q^2-1), \frac{1}{2}(q-1), 1)$$

dizajn sa $q+1$ *blokova. Vrijedi* $Aut(\mathcal{D}) = S_{\frac{1}{2}(q-1)} \wr S_{q+1} = (S_{\frac{1}{2}(q-1)})^{q+1} : S_{q+1}$. *Za svaki* p, $C = C_p(\mathcal{D}) = [\frac{1}{2}(q^2-1), q+1, \frac{1}{2}(q-1)]_p$ *s* $Aut(C) = Aut(\mathcal{D})$.

Propozicija (nastavak)

(ii) *Ako je q paran, tada je $|g^G| = (q^2-1), |M \cap g^G| = (q-1)$ i $\mathcal{D}$ je*

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

dizajn sa $q+1$ blokova. Vrijedi
$Aut(\mathcal{D}) = S_{(q-1)} \wr S_{q+1} = (S_{(q-1)})^{q+1} : S_{q+1}$. Za svaki p,
$C = C_p(\mathcal{D}) = [(q^2-1), q+1, (q-1)]_p$ s $Aut(C) = Aut(\mathcal{D})$.

Propozicija

Neka je $G = PSL_2(q)$, M maksimalna podgrupa grupe G indeksa $q+1$, a Ω skup svih konjugata podgrupe M u grupi G. Neka je $M = G_1$. Pretpostavimo da je $g \in nX \subseteq G$ element koji fiksira točno dvije točke i ne smanjujući općenitost možemo pretpostaviti da je $g \in G_1$ i $g \in G_2$. Tada za konstruirani dizajn vrijedi $r = \lambda = 2$. Također, vrijedi:

(i) *Ako je g involucija, tako da je $q \equiv 1 (mod 4)$ tada je dizajn $\mathcal{D}$ $1-(\frac{1}{2}q(q+1), q, 2)$ dizajn sa $q+1$ blokova. Vrijedi $Aut(\mathcal{D}) = S_{q+1}$. Također, $C_2(\mathcal{D}) = [\frac{1}{2}q(q+1), q, q]_2, C_p(\mathcal{D}) = [\frac{1}{2}q(q+1), q+1, q]_p$, ako je p neparan prost i $Aut(C_p(\mathcal{D})) = Aut(\mathcal{D}) = S_{q+1}$, za svaki p.*

Propozicija (nastavak)

(ii) *Ako g nije involucija, tada je dizajn $\mathcal{D}$ $1-(q(q+1), 2q, 2)$ dizajn sa $q+1$ blokova. Vrijedi $Aut(\mathcal{D}) = 2^{\frac{1}{2}q(q+1)} : S_{q+1}$. Također, $C_2(\mathcal{D}) = [q(q+1), q, 2q]_2, C_p(\mathcal{D}) = [q(q+1), q+1, 2q]_p$, ako je p neparan prost i $Aut(C_p(\mathcal{D})) = Aut(\mathcal{D}) = 2^{\frac{1}{2}q(q+1)} : S_{q+1}$, za svaki p.*

Primjer ($PSL_2(16)$)

Dizajn	*Kod*
$1-(255,15,1)$	$[255,17,15]_p$
$1-(272,32,2)$	$[272,16,32]_2, [272,17,32]_p$

Primjer ($PSL_2(17)$)

Dizajn	*Kod*
$1-(144,8,1)$	$[144,18,8]_p$
$1-(153,17,2)$	$[153,17,17]_2, [153,18,17]_p$
$1-(306,34,2)$	$[306,17,34]_2, [306,18,34]_p$

Primjer ($PSL_2(19)$)

Dizajn	*Kod*
$1-(180,9,1)$	$[180,20,9]_p$
$1-(380,38,2)$	$[360,19,38]_2, [360,20,38]_p$

- Jankova grupa J_1 je jednostavna grupa reda 175560,
- $\mathrm{Aut}J_1 \cong J_1$,
- Grupa J_1 ima 7 konjugacijskih klasa maksimalnih podgrupa, te 15 konjugacijskih klasa elemenata.

No.	Struktura	Index	Red
Max[1]	$PSL(2,11)$	266	660
Max[2]	$2^3:7:3$	1045	168
Max[3]	$2 \times A_5$	1463	120
Max[4]	$19:6$	1540	114
Max[5]	$11:10$	1596	110
Max[6]	$D_6 \times D_{10}$	2926	60
Max[7]	$7:6$	4180	42

nX	$\lvert nX\rvert$	$C_G(g)$	Max.centralizator
$2A$	1463	$2 \times A_5$	Da
$3A$	5852	$D_6 \times 5$	Ne

Rezultati dobiveni iz Jankove grupe J_1:

M	nX	Dizajn
$PSL_2(11)$	$2A:1$	$1-(1463,55,10)$
$2\times A_5$	$2A:1$	$1-(1463,31,31)$
$PSL_2(11)$	$3A:1$	$1-(5852,110,5)$
$PSL_2(11)$	$3A:1$	$1-(5852,20,5)$