Konačne grupe, dizajni i kodovi

Andrea Švob
(asvob@math.uniri.hr)

1. veljače 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.

Incidencijske strukture

Definicija

Incidencijska struktura $\mathcal{D}$ *je uređena trojka* $(\mathcal{P}, \mathcal{B}, \mathcal{I})$, *gdje su* $\mathcal{P}$ *i* $\mathcal{B}$ *neprazni disjunktni skupovi i* $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$. *Elementi skupa* $\mathcal{P}$ *se nazivaju* **točke**, *elementi skupa* $\mathcal{B}$ **blokovi**, *a relacija* $\mathcal{I}$ **relacija incidencije**.

Broj blokova koji su incidentni s točkom P naziva se **stupanj točke** P i broj točaka koje su incidentne s blokom x naziva se **stupanj bloka** x.

Za incidencijsku strukturu u kojoj je svaka od v točaka stupnja r i svaki od b blokova stupnja k vrijedi $vr = bk$.

Definicija

Incidencijska struktura je simetrična ako je broj točaka jednak broju blokova tj. $|\mathcal{P}| = |\mathcal{B}|$

Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ konačna incidencijska struktura takva da je $|\mathcal{P}| = v$ i $|\mathcal{B}| = b$. Označimo elemente skupa $\mathcal{P}$ sa $P_1, ..., P_v$ i elemente skupa $\mathcal{B}$ sa $x_1, ..., x_b$. **Matrica incidencije** incidencijske strukture $\mathcal{D}$ je $v \times b$ matrica $\mathbf{M} = (m_{ij})$

$$m_{ij} = \begin{cases} 1, & (P_i, x_j) \in \mathcal{I}, \\ 0, & (P_i, x_j) \notin \mathcal{I}. \end{cases}$$

Dualna struktura

Struktura $\mathcal{D}^* = (\mathcal{P}^*, \mathcal{B}^*, \mathcal{I}^*)$, gdje je $\mathcal{P}^* = \mathcal{B}$, $\mathcal{B}^* = \mathcal{P}$, $\mathcal{I}^* = \{(x, P) | (P, x) \in \mathcal{I}\}$ naziva se **dualna struktura** strukture $\mathcal{D}$.

Komplementarna struktura

Incidencijska struktura $\tilde{\mathcal{D}} = (\mathcal{P}, \mathcal{B}, \tilde{\mathcal{I}})$ gdje je $\tilde{\mathcal{I}} = \mathcal{P} \times \mathcal{B} - \mathcal{I}$, tj. vrijedi $(x, B) \in \tilde{\mathcal{I}} \Leftrightarrow (x, B) \notin \mathcal{I}$, naziva se **komplementarna struktura** strukture $\mathcal{D}$.

Definicija

Neka su $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ *i* $\mathcal{D}' = (\mathcal{P}', \mathcal{B}', \mathcal{I}')$ *incidencijske strukture. Bijektivno preslikavanje* $f : \mathcal{P} \times \mathcal{B} \to \mathcal{P}' \times \mathcal{B}'$ *je* **izomorfizam** *iz* $\mathcal{D}$ *na* $\mathcal{D}'$ *ako vrijedi:*

1. f *preslikava* $\mathcal{P}$ *na* $\mathcal{P}'$ *i* $\mathcal{B}$ *na* $\mathcal{B}'$
2. $(P, x) \in \mathcal{I} \Rightarrow (f(P), f(x)) \in \mathcal{I}', \ \forall P \in \mathcal{P}$ *i* $\forall x \in \mathcal{B}$

Ako je $\mathcal{D}' = \mathcal{D}$*, onda se preslikavanje* f *naziva* **automorfizam**. *Skup svih automorfizama je grupa s obzirom na kompoziciju funkcija i naziva se* **puna grupa automorfizama** *strukture* $\mathcal{D}$.

Samodualna struktura

Struktura $\mathcal{D}$ naziva se samodualna struktura ako je izomorfna svojoj dualnoj strukturi.

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* $\mathcal{B}$.

Definicija

$2 - (v, k, \lambda)$ *dizajn naziva se* **blok dizajn**.

Definicija

$t - (v, k, \lambda)$ *dizajn takav da je* $v = b$ *naziva se* **simetričan dizajn**.

Grafovi

Definicija

Neka je $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{I})$ konačna incidencijska struktura. $\mathcal{G}$ je **graf** *ako je svaki element skupa $\mathcal{E}$ incidentan s dva (ne nužno različita) elementa iz skupa $\mathcal{V}$. Elementi skupa $\mathcal{V}$ se nazivaju* **vrhovi** *i elementi skupa $\mathcal{E}$* **bridovi**.

Dva vrha u i v su susjedna ako su incidentna s istim bridom. Broj bridova incidentnih s vrhom v naziva se **stupanj vrha** v. Brid e koji spaja vrh v sa samim sobom naziva se **petlja**.

Graf bez petlji u kojemu su svaka dva vrha incidentna najviše s jednim bridom naziva se **jednostavan graf**.

Matrica susjedstva grafa $\mathcal{G}$ s n vrhova $(v_1, ..., v_n)$ je $n \times n$ matrica **A**. Element a_{ij} matrice **A** je broj bridova incidentnih s vrhovima v_i i v_j.

Put u grafu $\mathcal{G}$ je netrivijalan niz $v_0 e_1 v_1 e_2 ... e_k v_k$ u kojemu su svi vrhovi i svi bridovi međusobno različiti, pri čemu su $v_0, ..., v_k$ vrhovi grafa $\mathcal{G}$ i e_i, $i = 1, ..., k$ bridovi koji su incidentni s vrhovima v_{i-1} i v_i.

Graf $\mathcal{G}$ je **povezan graf** ako za svaka dva vrha tog grafa postoji put koji ih povezuje.

Graf u kojem su svi vrhovi jednakog stupnja k naziva se $k-$**regularan graf**.

Definicija

Neka je $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{I})$ graf sa n vrhova. Graf $\mathcal{G}$ je **jako regularan graf** *s parametrima (n, k, λ, μ) ako vrijedi:*

1. *$\mathcal{G}$ je jednostavan $k-$regularan graf,*
2. *svaka dva susjedna vrha imaju točno λ zajedničkih susjednih vrhova,*
3. *svaka dva nesusjedna vrha imaju točno μ zajedničkih susjednih vrhova.*

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. $d = \min\{w(c) | \, c \in C, \, c \neq 0\}$

Hammingova udaljenost

Neka je $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in F^n$.
Broj

$$d(x, y) = |\{i \,|\, 1 \leq i \leq n, x_i \neq y_i\}|$$

se naziva Hammingova udaljenost.

Težina riječi koda

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

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

Generirajuća matrica

Matrica dimenzije $k \times n$ čiji se retci sastoje od vektora baze koda $[n, k, d]$ zove se generirajuća matrica.

Dualni kod

Skalarni produkt

Skalarni produkt vektora $x = (x_1 \dots x_n)$ i $y = (y_1 \dots y_n)$, $x, y \in F^n$ je skalar $\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i \in F$.
Ako je $\langle x, y \rangle = 0$, kažemo da su x i y ortogonalni.

Dualni kod

Za linearni kod $C \subset F^n$ definiramo dualni kod $C^\perp \subset F^n$ sa

$$C^\perp = \{x \in F^n \mid (\forall y \in C)\, \langle x, y \rangle = 0\}$$

Ako je C $[n, k]$ kod, tada je $C^\perp$ $[n, n-k]$ kod.

Paritetna matrica

Neka je $C \subset F^n$ kod. Paritetna matrica za kod C je generirajuća matrica za dualni kod $C^\perp$.

Težinski enumerator

Težinski neumerator koda C je polinom

$$A(x) = \sum_{i=0}^{n} A_i x^i,$$

gdje je A_i broj riječi koda težine i.

Kod je paran ako su sve težine parne, a dvostruko paran (doubly-even) ako su sve težine djeljive s 4.

Kod C je samoortogonalan, ako vrijedi: $C \subset C^{\perp}$

Kod C je samodualan, ako je $C = C^{\perp}$

Izomorfni kodovi

Dva koda iste duljine i nad istim poljem su **ekvivalentna** ako se jedan može dobiti iz drugoga permutacijom koordinata u svim riječima koda i množenjem koordinatne pozicije s ne-nul elementom polja.

Dva koda iste duljine i nad istim poljem su **izomorfna** ako se jedan može dobiti iz drugoga permutacijom koordinata u svim riječima koda.

Automorfizam koda C je bilo koja permutacija koordinatnih pozicija koja preslikava riječi koda u riječi koda.

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.*

Na skupu Ω na kojeg djeluje grupa G može se definirati relacija

$$x \sim y \Leftrightarrow (\exists g \in G)\text{t.d.je} g.x = y.$$

Relacija $\sim$ je relacija ekvivalencije na skupu Ω.

Klasa ekvivalencije elementa x s obzirom na relaciju $\sim$,
$G.x = \{g.x \mid g \in G\}$, naziva se **orbita** elementa x za djelovanje grupe G.
Dugi način zapisa: $x^G = \{x^g, g \in G\}$

Definicija

Grupa G djeluje **tranzitivno** *na skup Ω ako postoji element $x \in \Omega$ takav da je $G.x = \Omega$. Odnosno, cijeli skup Ω je jedna orbita. Grupa G je tranzitivna ako za svaki par točaka $\alpha, \beta \in \Omega$ postoji $g \in G$ takav da je $\alpha^g = \beta$.*

Propozicija

Neka grupa G djeluje na skup Ω i neka je G_x stabilizator elementa $x \in \Omega$ za djelovanje grupe G. Tada je $G_{g.x} = gG_xg^{-1}$, $\forall g \in G$. Posebno, ako G djeluje tranzitivno na skup Ω, onda su svi stabilizatori međusobno konjugirani.

Neka grupa G djeluje na skup Ω. Proširimo to djelovanje na skup podskupova skupa Ω na sljedeći način:

$$g.X = \{g.x \mid x \in X\},\ X \subseteq \Omega.$$

Definicija

Neka grupa G djeluje tranzitivno na skup Ω i neka je $\Delta \subseteq \Omega$. Ako za svaki $g \in G$ vrijedi $g.\Delta = \Delta$ ili $g.\Delta \cap \Delta = \emptyset$, onda se skup Δ naziva **blok**.

Trivijalni blokovi:

- Ω,
- $\{x\}$, za svaki $x \in \Omega$.

Definicija

Ako grupa G djeluje tranzitivno na skup Ω tako da ne postoje netrivijalni blokovi, onda kažemo da je djelovanje **primitivno** *i da je G* **primitivna grupa**.

Teorem

Neka grupa G djeluje tranzitivno na skup Ω. To djelovanje je primitivno ako i samo ako je G_x maksimalna podgrupa grupe G za svaki $x \in \Omega$.

Definicija

Označimo sa $S(\Omega)$ skup svih bijekcija na skupu Ω. Skup S s obzirom na kompoziciju preslikavanja tvori grupu. Za konačan skup Ω, bijekcije na skupu Ω se nazivaju **permutacije** *skupa Ω.*

Definicija

Grupa svih permutacija skupa Ω zove se **simetrična grupa** *i označava S_n, $n = |\Omega|$. Podgrupa grupe S_n naziva se* **permutacijska grupa**.

Broj svih permutacija skupa Ω: $|S_n| = n!$

Korolar (Cayleyev teorem)

Grupa G je izomorfna podgrupi grupe $S(G)$. Posebno, svaka konačna grupa G reda n je izomorfna nekoj permutacijskoj grupi.

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.*

J. D. Key, J. Moori:
Codes, Designs and Graphs from the Janko Groups J_1 and J_2
J. Combin. Math. Combin. Comput. 40 (2002), 143-159.

Teorem (Key, Moori)

Neka je Ω $n-$člani skup, α element skupa Ω i neka je G konačna grupa koja djeluje primitivno na skup Ω. Neka je $\Delta \neq \{\alpha\}$, orbita za djelovanje stabilizatora G_α na neki element $\beta \in \Omega$, $\Delta = \{g.\beta \mid g \in G_\alpha\}$. Ako je $\mathcal{B} = \{g.\Delta \mid g \in G\}$, $\delta \in \Delta$ i $\mathcal{E} = \{g.\{\alpha, \delta\} \mid g \in G\}$, tada je $\mathcal{D} = (\Omega, \mathcal{B})$ simetričan $1-(n, |\Delta|, |\Delta|)$ dizajn. Ako je Δ samosparena orbita od G_α, tada je $\Gamma = (\Omega, \mathcal{E})$ regularan povezan graf stupnja $|\Delta|$, dizajn $\mathcal{D}$ je samodualan i grupa G,kao grupa automorfizama, djeluje primitivno na svaku od ovih struktura.

Ovom metodom moguće je konstruirati samo simetrične $1-$ dizajne.

Neka su $\beta_1, ..., \beta_s$ elementi skupa Ω i neka je

$$\Delta = G_\alpha.\beta_1 \cup ... \cup G_\alpha.\beta_s,$$

uz uvjet da je $\Delta \neq \Omega$.
Tada je

$$\mathcal{B} = \{g.\Delta \mid g \in G\}$$

skup blokova samodualnog simetričnog $1-$dizajna na kojega grupa G djeluje primitivno kao grupa automorfizama.

Lema

Ako grupa G djeluje primitivno na simetričan dizajn $\mathcal{D}$, onda se dizajn $\mathcal{D}$ može konstruirati na način opisan teoremom KM.

Lema

Neka je G jednostavna primitivna permutacijska grupa. Tada postoji samo jedna trivijalna orbita za djelovanje stabilizatora G_α, $\alpha \in G$.

Općenito o grupama J_1 i J_2

- Jankova grupa J_1 je jednostavna grupa reda 175560,
- $\mathrm{Aut}J_1 \cong J_1$,
- Grupa J_1 ima sedam maksimalnih podgrupa, do na konjugaciju i odgovarajuće primitivne permutacijske reprezentacije na 266, 1045, 1463, 1540, 1596, 2926 i 4180 točaka.

- Jankova grupa J_2 je jednostavna grupa reda 604800,
- Puna grupa automorfizama grupe J_2 je izomorfna grupi $J_2 : Z_2$,
- Grupa J_2 ima devet maksimalnih podgrupa, do na konjugaciju i devet primitivnih permutacijskih reprezentacija na 100, 280, 315, 525, 840 1008, 1800, 2016 i 10080 točaka.

1−dizajni i grafovi konstruirani iz grupe J_1

Propozicija

Postoji točno 245 neizomorfnih samodualnih dizajna konstruiranih iz grupe J_1, na način opisan teoremom. Grupa J_1 djeluje primitivno kao puna grupa automorfizama na konstruirane dizajne.

Autori ističu da su provjerili jaku regularnost konstruiranih grafova za neke od primitivnih reprezentacija grupe J_1, ali nisu dobili niti jedan jako regularan graf.

1−dizajni i grafovi konstruirani iz grupe J_2

Propozicija

Postoji točno 51 neizomorfnih samodualnih dizajna konstruiranih iz grupe J_2, na način opisan teoremom. Grupa J_2 djeluje primitivno na sve konstruirane dizajne. Konstruirani dizajni imaju punu grupu automorfizama izomorfnu grupi J_2 ili grupi $AutJ_2$. Za svaki dizajn kojemu je puna grupa automorfizama izomorfna grupi $AutJ_2$ konstruiran je njemu izomorfan dizajn iz orbite iste duljine.

Dobivena tri jako regularna grafa:

- (100,36,14,12)
- (280,135,70,60)
- (280,36,8,4)

Kodovi konstruirani iz grupa J_1 i J_2

- Autori ističu dobivene samoortogonalne dvostruko parne kodove:

Iz grupe J_1:

dizajn	kod	grupa automorfizama
$1-(1045, 421, 421)$	$[1045, 20, 456]_2$	J_1

Iz grupe J_2:

dizajn	kod	grupa automorfizama
$1-(100, 36, 36)$	$[100, 36, 16]_2$	$J_2 : Z_2$
$1-(280, 108, 108)$	$[280, 14, 108]_2$	$J_2 : Z_2$
$1-(315, 64, 64)$	$[315, 28, 64]_2$	$J_2 : Z_2$
$1-(315, 80, 80)$	$[315, 36, 80]_2$	$J_2 : Z_2$

Oktade i dodekade

Neka je $\Omega = \{1, 2, 3, ..., 24\}$. Promatramo Steinerov sustav $S(5, 8, 24)$ definiran na ovom skupu. Svaki blok Steinerovog sustava zove se **oktada** i označava s 8^0.

- Postoji 759 oktada.
- Svake dvije oktade, O_1 i O_2 sijeku se u skupu čiji je kardinalni broj $0, 2, 4, 8$.
- Ako vrijedi $|O_1 \cap O_2| = 2$ tada se $O_1 \Delta O_2$ zove **dodekada** i označava s 12^0.
- Postoji 2576 dodekada u $S(5, 8, 24)$.

Općenito o grupi Co_2 - Conway grupa

Leech-ova rešetka

Leech-ova rešetka, Λ, je 24 dimenzionalan Euklidski prostor R^{24} čija je grupa automorfizama jednaka $2 \cdot Co_1$. Pronašao ju je John Leech, a opisao u člancima iz 1964., 1965. i 1967. Povezana je s zatvorenim pokrivanjem sfere u u dimenziji 24.

Λ se sastoji od $(x_1, x_2, ..., x_{24}) \in Z^{24}$ t.d. vrijedi:

(i) $\sum_{i=1}^{24} x_i \equiv 4m(mod8)$

(ii) $x_i \equiv m(mod2)$

(iii) $\{i : x_i \equiv m(mod4)\}$ za bilo koji zadani m jednak je praznom skupu, $8^0, 12^0$ ili njihovim komplementima.

Conway grupa

Leech-ova grupa je grupa $Aut(\Lambda) = Co_0$

Conway je dokazao da vrijedi:

(i) Grupa $N = 2^{12}.M_{24}$ je maksimalna podgrupa od Co_0.

(ii) $|Co_0| = 2^{22}3^9 5^4 7^2 \times 11 \times 13 \times 23$

(iii) Co_0 je nova savršena grupa, $|Z(Co_0)| = 2$.

(iv) $Co_0/Z(Co_0)$ je nova jednostavna grupa, Co_1.

Neka je $\Lambda_n = \{x \in \Lambda t.d. ||x|| = 4\sqrt{n}\}$. Grupa Co_0 djeluje tranzitivno na $\Lambda_i, i = 2, 3, 4$.

Vrijedi:

- $|\Lambda_2| = 196560$, $(Co_0)_{\Lambda_2} = Co_2$, nova jednostavna grupa
- $|\Lambda_3| = 16737120$, $(Co_0)_{\Lambda_3} = Co_3$, nova jednostavna grupa
- $|\Lambda_4| = 3980034000$, $(Co_0)_{\Lambda_4} = Co_4 = 2^{11}.M_{23}$, nije jednostavna grupa

Rezultati dobiveni iz grupe Co_2

- J.Moori, B.G. Rodrigues, Some designs and codes invariant under the simple group Co_2, Journal of Algebra 316(2007)649 – 661
- Dobiveni dizajni su samodualni simetrični, a kodovi samoortogonalni dvostruko parni.

dizajn	grupa automorfizama	kod	grupa automorfizama
$1-(2300, 892, 892)$	Co_2	$[2300, 23, 892]$	Co_2
$1-(2300, 1408, 1408)$	Co_2	$[2300, 22, 1024]$	Co_2