Jankove grupe kao dizajni i jako regularni grafovi

Vedrana Mikulić (vmikulic@math.uniri.hr)

Odjel za matematiku
Sveučilište u Rijeci

9. listopad 2008.

Djelovanje grupe na skup

Definicija

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

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

Slika djelovanja elementa $g \in G$ na element $x \in X$ označava se $g.x$.

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

Na skupu X na kojega djeluje grupa G može se definirati relacija

$$x \sim y \Leftrightarrow (\exists g \in G) g.x = y.$$

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

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.

Propozicija

Ako konačna grupa G djeluje na skup X, onda za svaki $x \in X$ vrijedi $|G.x| = [G : G_x]$.

Grupa G djeluje **tranzitivno** na skup X ako postoji element $x \in X$ takav da je $G.x = X$.

Propozicija

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

Teorem

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

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

Korolar

(Caylejev teorem) Svaka konačna grupa je izomorfna nekoj permutacijskoj grupi.

Primjer

Promotrimo djelovanje konačne grupe G množenjem slijeva na lijevi kvocijentni skup $G/H = \{gH \mid g \in G\}$, $H \leq G$. Preslikavanje

$$f_x : G/H \to G/H, \; f_x(gH) = (xg)H,$$

je bijekcija te je preslikavanje

$$F : G \to S(G/H), \; g \mapsto f_g,$$

monomorfizam. Definirano djelovanje je vjerno. Za svaka dva elementa $g_1H \in G/H$ i $g_2H \in G/H$ vrijedi

$$g_1H = g_1g_2^{-1}g_2H = (g_1g_2^{-1}).g_2H$$

pa je definirano djelovanje tranzitivno i vrijedi

$$|G.(gH)| = |G/H| \Rightarrow |G_H| = |H|$$

$$G_H = \{g \in G \mid gH = H\} = \{g \in G \mid g \in H\} \subseteq H.$$

Primitivne grupe

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

$$x.S = \{x.s \mid s \in S\},\ S \subseteq X.$$

Definicija

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

Trivijalni blokovi:

- X,
- $\{x\}$, za svaki $x \in X$.

Definicija

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

Primjer

Grupa S_3 *djeluje na skup* $X = \{1, 2, 3\}$*:*

$$g.x = g(x), \forall g \in S_3, \forall x \in X.$$

$S_3.1 = X \Rightarrow$ *tranzitivnost*

Stabilizator svakog elementa je grupa reda dva. Podgrupe reda dva grupe S_3 *su maksimalne pa je opisano djelovanje primitivno.*

Primjer

Neka je H *maksimalna podgrupa konačne grupe* G*.*

Grupa G *djeluje tranzitivno množenjem slijeva na lijevi kvocijentni skup* G/H *i* $G_H = H$*, odnosno stabilizator od* H *je maksimalna podgrupa grupe* G*. Zbog tranzitivnosti, svi stabilizatori* $G_{gH}, g \in G$*, su međusobno konjugirani pa je definirano djelovanje primitivno.*

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* $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$*.*

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

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

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

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 $\mathbf{M} = (m_{ij})$

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

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* $\mathcal{B}$.

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

Primjer

$2 - (6, 3, 2)$ dizajn

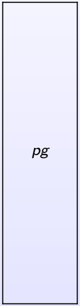
$t-(v,k,\lambda)$ dizajn takav da je $v=b$ naziva se **simetričan dizajn**.

Stupanj svake točke simetričnog dizajna jednak je stupnju svakog bloka tog dizajna, odnosno vrijedi $k=r$.

Propozicija

Ako je $t-(v,k,\lambda)$ simetričan dizajn, onda je $t\leq 2$.

Primjer



$2-(7,3,1)$ 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 $\mathcal{V}$.*

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 $\mathbf{A}$. Element a_{ij} matrice $\mathbf{A}$ 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.*

Primjer

Primjer

Neka grupa G djeluje tranzitivno na skup X. Tada grupa G djeluje na skup $X \times X$ na sljedeći način:

$$g.(x_1, x_2) = (g.x_1, g.x_2).$$

Skup $\{(x, x) \mid x \in X\}$ *naziva se* **dijagonala skupa** X.
Broj orbita skupa $X \times X$ *za djelovanje grupe* G *naziva se* **rang grupe** G.
Za orbitu O *skupa* $X \times X$ *za djelovanje grupe* G *kažemo da je* **simetrična orbita** *ako vrijedi*

$$(x, y) \in O \Rightarrow (y, x) \in O.$$

Neka je G grupa parnog reda. Tada postoji barem jedna simetrična orbita D (različita od dijagonale) na skupu $X \times X$. G je grupa automorfizama grafa $\mathcal{G}(D)$ kojemu je X skup vrhova i D skup bridova.
Ako je G grupa ranga tri, onda je $\mathcal{G}(D)$ jako regularan graf.

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 (KM)

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 $\beta \in \Omega$, $\Delta = \{g.\beta \mid g \in G_\alpha\}$. Tada je

(1) *$\mathcal{B} = \{g.\Delta \mid g \in G\}$ $n-$člani skup blokova simetričnog samodualnog $1-(n, |\Delta|, |\Delta|)$ dizajna na kojega grupa G primitivno djeluje kao grupa automorfizama,*

(2) *za $\delta \in \Omega$, skup $\mathcal{E} = \{g.\{\alpha, \delta\} \mid g \in G\}$ je skup bridova povezanog $|\Delta|-$regularnog grafa sa n vrhova na kojega grupa G primitivno djeluje kao grupa automorfizama.*

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

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

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.

Dokaz iz članka:

Neka je $\mathcal{D}$ simetričan $1-(v,k,k)$ dizajn i neka je $\mathcal{B}$ skup blokova dizajna $\mathcal{D}$. Tada je $\mathcal{B} = G.B$ za neki blok $B \in B$. Slijedi da je $|G| = |\mathcal{B}| \cdot |G_B|$.

G djeluje primitivno na dizajn $\mathcal{D}$ pa je G_B maksimalna podgrupa i $G_B = G_\alpha$ za neku točku α dizajna $\mathcal{D}$. Zaključujemo da G_α fiksira blok B te je B unija nekih G_α orbita.

$\square$

Dodatne napomene

- Alternativna definicija ranga grupe:
  rang tranzitivne permutacijske grupe G je broj orbita za djelovanje stabilizatora $G_x, \ x \in G$.
  Slijedi da je graf iz grupe ranga tri konstruiran na način opisan teoremom KM jako regularan graf.
- Neka je G jednostavna primitivna permutacijska grupa. Tada postoji samo jedna trivijalna orbita za djelovanje stabilizatora $G_x, \ x \in G$.

Grupe J_1 i J_2

Jankova grupa J_1 je jednostavna grupa reda 175560 te je $\mathrm{Aut}J_1 \cong J_1$. 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.

Primjer u programskom paketu Magma

$1-$*dizajni i grafovi konstruirani iz grupe* J_1

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

Autori ističu da su testirali 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

Postoji točno 51 neizomorfnih samodualnih dizajna konstruiranih iz grupe J_2 (na način opisan teoremom KM). 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. Konstruirana su i tri jako regularna grafa s parametrima:

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

Graf na 100 vrhova konstruiran je iz permutacijske reprezentacije ranga tri, a grafovi na 280 vrhova iz permutacijske reprezentacije ranga četiri.

Hipoteza

Autori pretpostavljaju da svaki dizajn $\mathcal{D}$ konstruiran na opisani način iz grupe G ima grupu Aut$G$ kao punu grupu automorfizama, osim u slučaju da je iz iste grupe konstruiran dizajn izomorfan dizajnu $\mathcal{D}$. U tom slučaju je, prema njihovoj pretpostavci, grupa automorfizama izomorfna podgrupi grupe Aut$G$.

Kodovi iz incidencijskih struktura

Neka je $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ incidencijska struktura i $\mathbf{M}$ matrica incidencije strukture $\mathcal{D}$. Stupci matrice $\mathbf{M}$ su vektori incidencije.

Linearni kod $\mathcal{C}$ iz dizajna $\mathcal{D}$ je potprostor vektorskog prostora dimenzije $|\mathcal{P}|$ nad konačni poljem $\mathbb{F}$ razapet vektorima incidencije dizajna.

Oznaka: $[n, k, d]_{|\mathbb{F}|}$
n je dimenzija vektorskog prostora
k je dimenzija potprostora razapetog vektorima incidencije
d je najmanja težina (udaljenost od nul vektora)

Automorfizam koda je permutacija komponetni vektora koda koja čuva potprostor.

Kodovi konstruirani iz grupe J_2

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