Asocijacijske sheme

V. Krčadinac, 2023./24., 60 sati.

Pojam asocijacijske sheme definirali su statističari u 1950-im godinama [3,4]. Do ekvivalentnog pojma pod nazivom "koherentne konfiguracije" dovela su istraživanja permutacijskih grupa i s njima povezanih algebri u 1970-im [9,10]. Neovisno i otprilike u isto vrijeme, sovjetski matematičari došli su do ekvivalentnog pojma "celularnog prstena" [7,11] potaknuti problemima iz teorije grafova. Asocijacijske sheme postale su jedan od središnjih pojmova algebarske kombinatorike objavom disertacije Philippe Delsartea 1973. godine [6], u kojoj ih je povezao s teorijom kodova i teorijom dizajna.

Cilj ovog kolegija je dati pregled najvažnijih rezultata o asocijacijskim shemama i njihovim primjenama u raznim područjima matematike. Osnovna literatura bit će nedavno objavljena knjiga [1], uz klasične knjige [2,5,8] koje imaju stotine citata u istraživačkoj literaturi. Polaganje ispita predviđa se kroz individualne projektne zadatke koji se mogu izložiti usmeno na znanstvenom seminaru ili u obliku pisanog rada.

Literatura

1. E. Bannai, E. Bannai, T. Ito, R. Tanaka, *Algebraic combinatorics*, De Gruyter, 2021.

2. E. Bannai, T. Ito, *Algebraic combinatorics. I. Association schemes*, The Benjamin/Cummings Publishing Co., 1984.

3. R. C. Bose, D. M. Mesner, *On linear associative algebras corresponding to association schemes of partially balanced designs*, Ann. Math. Statist. **30** (1959), 21–38.

4. R. C. Bose, T. Shimamoto, *Classification and analysis of partially balanced incomplete block designs with two associate classes*, J. Amer. Statist. Assoc. **47** (1952), 151–184.

5. A. E. Brouwer, A. M. Cohen, A. Neumaier, *Distance-regular graphs*, Springer-Verlag, 1989.

6. P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. **10** (1973), vi+97 pp.

7. I. A. Faradžev, A. A. Ivanov, M. H. Klin, A. J. Woldar (urednici), *Investigations in algebraic theory of combinatorial objects*, Kluwer Academic Publishers Group, Dordrecht, 1994.

8. C. D. Godsil, *Algebraic combinatorics*, Chapman & Hall, 1993.

9. D. G. Higman, *Coherent configurations. I. Ordinary representation theory*, Geometriae Dedicata **4** (1975), no. 1, 1–32.

10. D. G. Higman, *Coherent configurations. II. Weights*, Geometriae Dedicata **5** (1976), no. 4, 413–424.

11. B. Weisfeiler, A. A. Leman, *Reduction of a graph to a canonical form and an algebra which appears in this process* (na ruskom), Scientific-Technological Investigations **2** (1968), 12–16.

Association schemes

V. Krčadinac, 2023/24, 60 hours.

The concept of association schemes was defined by statisticians in the 1950s [3,4]. Research of permutation groups and related algebras in the 1970s [9,10] lead to the equivalent concept of "coherent configurations". Independently and at about the same time, Soviet mathematicians studied "cellular rings" [7,11], another equivalent concept motivated by problems from graph theory. Association schemes became one of the central concepts of algebraic combinatorics with the publication of Philippe Delsarte's thesis in 1973 [6], in which he established connections with coding theory and design theory.

The goal of this course is to give an overview of the most important results about association schemes and their applications in various parts of mathematics. The main text will be the recently published book [1], along with classic books [2,5,8] which have hundreds of citations in the research literature. The exam will be based on individual project assignments to be presented as scientific seminars or as written essays.

Bibliography

1. E. Bannai, E. Bannai, T. Ito, R. Tanaka, *Algebraic combinatorics*, De Gruyter, 2021.

2. E. Bannai, T. Ito, *Algebraic combinatorics. I. Association schemes*, The Benjamin/Cummings Publishing Co., 1984.

3. R. C. Bose, D. M. Mesner, *On linear associative algebras corresponding to association schemes of partially balanced designs*, Ann. Math. Statist. **30** (1959), 21–38.

4. R. C. Bose, T. Shimamoto, *Classification and analysis of partially balanced incomplete block designs with two associate classes*, J. Amer. Statist. Assoc. **47** (1952), 151–184.

5. A. E. Brouwer, A. M. Cohen, A. Neumaier, *Distance-regular graphs*, Springer-Verlag, 1989.

6. P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. **10** (1973), vi+97 pp.

7. I. A. Faradžev, A. A. Ivanov, M. H. Klin, A. J. Woldar (editors), *Investigations in algebraic theory of combinatorial objects*, Kluwer Academic Publishers Group, Dordrecht, 1994.

8. C. D. Godsil, *Algebraic combinatorics*, Chapman & Hall, 1993.

9. D. G. Higman, *Coherent configurations. I. Ordinary representation theory*, Geometriae Dedicata **4** (1975), no. 1, 1–32.

10. D. G. Higman, *Coherent configurations. II. Weights*, Geometriae Dedicata **5** (1976), no. 4, 413–424.

11. B. Weisfeiler, A. A. Leman, *Reduction of a graph to a canonical form and an algebra which appears in this process* (in Russian), Scientific-Technological Investigations **2** (1968), 12–16.

Asocijacijske sheme

Sadržaj

Verzija 17, 25.4.2024.

1 Definicija i primjeri asocijacijskih shema

Definicija 1.1. Asocijacijska shema s d klasa *sastoji se od grafova* $G_0, \ldots, G_d$ *sa zajedničkim* n*-članim skupom vrhova* X *takvih da vrijedi:*

1. G_0 *je graf koji sadrži sve petlje i nema drugih bridova,*
2. $G_1, \ldots, G_d$ *čine particiju potpunog grafa* K_n*,*
3. *za svaki brid* $\{x, y\}$ *u* G_k*, broj vrhova* z *takvih da je* $\{x, z\}$ *brid u* G_i*, a* $\{z, y\}$ *brid u* G_j *ovisi samo o indeksima* i*,* j*,* k*. Označavamo ga* p_{ij}^k *i zovemo* presječnim brojem *sheme.*

Za vrhove x*,* y *takve da je* $\{x, y\}$ *brid u* G_i *kažemo da su* i-asocirani*. Broj vrhova* n *zovemo* redom *asocijacijske sheme.*

Propozicija 1.2. *Grafovi koji čine asocijacijsku shemu su regularni:* G_i *je stupnja* $n_i = p_{ii}^0$*. Pritom vrijedi* $\sum_{i=0}^{d} n_i = n$*.*

Dokaz. Dokazujemo da je u grafu G_i svaki vrh x stupnja n_i. Petlja $\{x, x\}$ je brid u grafu G_0, pa po 3. svojstvu iz definicije 1.1 imamo točno p_{ii}^0 vrhova z takvih da je $\{x, z\}$ brid u G_i. To su susjedni vrhovi od x u G_i, dakle x je stupnja $n_i = p_{ii}^0$. Ako fiksiramo vrh x_0, svaki vrh $x \in X$ susjedan je s x_0 u jednom od grafova G_i. Vrh x_0 ima n_i susjeda u G_i, pa je $\sum_{i=0}^{d} n_i = |X| = n$. □

Zadatak 1.3. *Neka je* δ *Kroneckerov simbol. Pokažite da presječni brojevi asocijaciske sheme zadovoljavaju:*

(a) $p_{ij}^k = p_{ji}^k$ *(komutativnost),*

(b) $p_{i0}^k = \delta_{ik}$*,*

(c) $p_{ij}^0 = n_i \cdot \delta_{ij}$*,*

(d) $\sum_{j=0}^{d} p_{ij}^k = n_i$*.*

Primjer 1.4 (Poligoni)**.** *Neka je* $X = \mathbb{Z}_n$ *grupa cijelih brojeva modulo* n*. Definiramo da su* x *i* y *susjedni u* G_i *ako je* $x - y = \pm i$*, za* $i = 0, 1, 2, \ldots$*. Tako dobijemo asocijacijsku shemu s* $d = \lfloor n/2 \rfloor$ *klasa koju zovemo* poligonom *reda* n *ili* n-terokutom*.*

Dokaz. Uzmimo dva para vrhova $x, y \in \mathbb{Z}_n$ i $x', y' \in \mathbb{Z}_n$ koji su susjedni u G_k, tj. $x - y = x' - y' = \pm k$. Zamjenom x i y, odnosno x' i y' možemo postići da je $x - y = x' - y' = k$, iz čega slijedi $x' - x = y' - y =: a \in \mathbb{Z}_n$. Želimo vidjeti da je broj vrhova $z \in \mathbb{Z}_n$ koji zadovoljavaju $x - z = \pm i$, $z - y = \pm j$ jednak broju vrhova $z' \in \mathbb{Z}_n$ koji zadovoljavaju $x' - z' = \pm i$, $z' - y' = \pm j$. Definiramo bijekciju $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$, $\alpha(t) = t + a$ tako da vrijedi $\alpha(x) = x'$ i $\alpha(y) = y'$. Ta bijekcija preslikava vrhove z u z' zato što je $\alpha(s) - \alpha(t) = s - t$, $\forall s, t \in \mathbb{Z}_n$. Stoga broj takvih vrhova z ne ovisi o izboru x i y, nego samo o indeksima i, j, k.

Označimo s $N_i(x)$ skup svih susjeda vrha x u grafu G_i. Tada je $n_i = |N_i(x)|$ za bilo koji vrh x. Taj broj je jednak broju rješenja jednadžbe $x - y = \pm i$ (za dane x i i), a njezina rješenja su $y_1 = x + i$, $y_2 = x - i$. Vidimo da je $n_0 = 1$ i $n_1 = \ldots = n_d = 2$. Ako uzmemo bilo koja dva vrha x i y koji su susjedni u G_k, onda je presječni broj sheme $p_{ij}^k = |N_i(x) \cap N_j(y)|$. Budući da su stupnjevi $n_i = |N_i(x)| \in \{1, 2\}$, presječni brojevi zadovoljavaju $p_{ij}^k \in \{0, 1, 2\}$. Možete li precizirati pod kojim uvjetom je $p_{ij}^k = 0$, odnosno $p_{ij}^k = 1$, odnosno $p_{ij}^k = 2$? $\square$

Primjer 1.5 (Johnsonova[1] shema)**.** *Neka su v i d prirodni brojevi takvi da je $2d \le v$. Za skup vrhova uzmimo sve d-člane podskupove od $V = \{1, \ldots, v\}$. Vrhovi $X, Y \subseteq V$ su susjedni u grafu G_i ako je $|X \cap Y| = d - i$. Tako dobijemo* Johnsonovu asocijacijsku shemu *$J(v, d)$ s d klasa, reda $n = \binom{v}{d}$. Grafove G_i iz ove sheme označavamo $J(v, d, i)$ i zovemo* Johnsonovim grafovima.

Dokaz. Uzmimo bilo koja dva d-podskupa $X, Y \subseteq V$ koji su susjedni u G_k, tj. $|X \cap Y| = d - k$. Direktnim prebrojavanjem vidimo da broj d-podskupova $Z \subseteq V$ takvih da je $|X \cap Z| = d - i$, $|Z \cap Y| = d - j$ ne ovisi o X i Y, nego samo o indeksima i, j, k. Da bismo dobili takav podskup Z, prvo biramo l elemenata iz presjeka $X \cap Y$. Zatim biramo $d - i - l$ elemenata iz $X \setminus Y$ i $d - j - l$ elemenata iz $Y \setminus X$. Na kraju dopunimo Z do d elemenata izborom iz $V \setminus (X \cup Y)$. Broj takvih podskupova Z je presječni broj Johnsonove sheme:

$$p_{ij}^k = \sum_{l \ge 0} \binom{d-k}{l} \binom{k}{d-i-l} \binom{k}{d-j-l} \binom{v-d-k}{i+j-d+l}.$$

Stupanj Johnsonovog grafa $G_i = J(v, d, i)$ je $n_i = \binom{d}{i}\binom{v-d}{i}$. $\square$

Johnsonova shema važna je u teoriji kombinatornih dizajna. Dobar uvod u teoriju dizajna je knjiga [120].

Primjer 1.6 (Hammingova[2] shema)**.** *Neka je F skup od q simbola ("slova"). Skup vrhova $X = F^d$ sadrži sve uređene d-torke slova, koje zovemo* riječima. Udaljenost *riječi $x = (x_1, \ldots, x_d)$ i $y = (y_1, \ldots, y_d)$ definiramo kao broj*

[1]Selmer M. Johnson (1916.-1996.), američki matematičar.

[2]Richard W. Hamming (1915.-1998.), američki matematičar.

različitih koordinata: $\partial(x,y) = |\{i \mid x_i \neq y_i\}|$. *Funkcija* $\partial : X \times X \to \mathbb{R}$ *je takozvana* Hammingova metrika. *Neka su riječi* $x, y \in X$ *susjedne u grafu* G_i *ako su na udaljenosti* $\partial(x,y) = i$. *Tako dobijemo* Hammingovu asocijacijsku shemu $H(d,q)$ *s* d *klasa, reda* $n = q^d$.

Dokaz. Uzmimo bilo koje dvije riječi $x, y \in X$ na udaljenosti $\partial(x,y) = k$. Slično kao u prethodnom primjeru, direktnim prebrojavanjem vidimo da broj riječi z takvih da je $\partial(x,z) = i$, $\partial(z,y) = j$ ovisi samo o indeksima i, j, k. Riječi x i y razlikuju se na k koordinata, a podudaraju na $d-k$ koordinata. Prvo biramo l od tih $d-k$ koordinata na kojima se riječ z razlikuje od x i y. Zatim od k koordinata na kojima se x i y razlikuju biramo $k-i+l$ na kojima se z podudara s x te $k-j+l$ na kojima se z podudara s y. Preostale koordinate izaberemo tako da se z razlikuje od x i od y:

$$p_{ij}^k = \sum_{l \geq 0} \binom{d-k}{l} (q-1)^l \binom{k}{i-l} \binom{i-l}{k-j+l} (q-2)^{i+j-2l-k}.$$

Stupanj grafa G_i u Hammingovoj shemi $H(d,q)$ je $n_i = \binom{d}{i}(q-1)^i$. □

Hammingova shema važna je u teoriji kodova za ispravljanje pogrešaka. Dobar uvod u teoriju kodiranja je knjiga [62]. Iduća dva primjera su q-analogoni Johnsonove i Hammingove sheme, tj. analogoni nad konačnim poljem $\mathbb{F}_q$. Neka je V vektorski prostor dimenzije n nad $\mathbb{F}_q$. Prebrojimo koliko V ima k-dimenzionalnih potprostora X. Iz V možemo izabrati k linearno nezavisnih vektora na

$$(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{k-1})$$

načina: prvo biramo bilo koji vektor osim nulvektora, zatim vektor koji nije razapet prvim izabranim vektorom, zatim vektor koji nije razapet s prva dva izabrana vektora itd. Isti potprostor X dobivamo od bilo koje njegove baze, a broj baza je

$$(q^k - 1)(q^k - q)(q^k - q^2) \cdots (q^k - q^{k-1}).$$

Broj potprostora dobijemo dijeljenjem ova dva produkta:

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)\cdots(q^n-q^{k-1})}{(q^k-1)\cdots(q^k-q^{k-1})} = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}.$$

To je takozvani *Gaussov* ili *q-binomni* koeficijent. Chris Godsil u skripti [56] koristi zgodnu notaciju kojom q-binomne koeficijente možemo zapisati analogno kao obične binomne koeficijente. Neka je

$$[n]_q = \frac{q^n - 1}{q - 1} = q^{n-1} + q^{n-2} + \ldots + q + 1$$

suma konačnog geometrijskog reda, a $[n]_q! = [n]_q \cdot [n-1]_q \cdots [1]_q$. U nastavku ćemo podrazumijevati parametar q i pisati samo $[n]$ i $[n]!$. Tada Gaussov koeficijent možemo zapisati kao

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{[n]!}{[k]![n-k]!}.$$

Primjer 1.7 (Grassmannova[3] shema)**.** *Vrhove čine svi d-dimenzionalni potprostori v-dimenzionalnog vektorskog prostora V nad poljem $\mathbb{F}_q$. Vrhovi X i Y su i-asocirani ako je* $\dim(X \cap Y) = d - i$. *Tako dobijemo* Grassmannovu shemu $J_q(v, d)$ *reda* $n = \begin{bmatrix} v \\ d \end{bmatrix}$ *s d klasa.*

Dokaz. Odredimo stupanj n_i grafa G_i Grassmannove sheme. Zadan je d-dimenzionalni potprostor $X \leq V$. Prebrojavamo koliko ima d-dimenzionalnih potprostora $Y \leq V$ takvih da je $\dim(X \cap Y) = d - i$. Prvo biramo $d - i$ linearno nezavisnih vektora iz X, a zatim i linearno nezavisnih vektora iz $V \setminus X$:

$$(q^d - 1)(q^d - q) \cdots (q^d - q^{d-i-1}) \cdot (q^v - q^d)(q^v - q^{d+1}) \cdots (q^v - q^{d+i-1}).$$

Produkt treba podijeliti s brojem baza potprostora Y kojima prvih $d - i$ vektora pripada presjeku $X \cap Y$:

$$(q^{d-i} - 1)(q^{d-i} - q) \cdots (q^{d-i} - q^{d-i-1}) \cdot (q^d - q^{d-i})(q^d - q^{d-i+1}) \cdots (q^d - q^{d-1}).$$

Sređivanjem dobijemo formulu $n_i = q^{i^2} \begin{bmatrix} d \\ i \end{bmatrix} \begin{bmatrix} v-d \\ i \end{bmatrix}$. Pokušajte izvesti formulu za presječne brojeve p_{ij}^k! $\square$

Neka su V i V' vektorski prostori nad poljem $\mathbb{F}$. *Bilinearna forma* je funkcija $f : V \times V' \to \mathbb{F}$ koja je linearna u prvoj i u drugoj koordinati. Ako je $\{e_1, \ldots, e_m\}$ baza od V, a $\{e'_1, \ldots, e'_{m'}\}$ baza od V', bilinearnu formu f možemo identificirati s matricom $A = [a_{ij}] \in M_{mm'}(\mathbb{F})$, $a_{ij} = f(e_i, e'_j)$. Na prostoru bilinearnih formi ili matrica definiramo metriku

$$\partial(A, B) = \operatorname{rk}(A - B),$$

pri čemu je rk rang matrice. Nejednakost trokuta za metriku ∂ slijedi iz nejednakosti $\operatorname{rk}(A + B) \leq \operatorname{rk} A + \operatorname{rk} B$, koju dokazujemo iz definicije ranga.

Primjer 1.8 (Shema bilinearnih formi)**.** *Vrhovi su $m \times m'$ matrice nad konačnim poljem: $X = M_{mm'}(\mathbb{F}_q)$. Matrice A i B su i-asocirane ako je* $\operatorname{rk}(A - B) = i$. *Dobijemo asocijacijsku shemu reda $n = q^{m \cdot m'}$ s* $d = \min\{m, m'\}$ *klasa.*

[3]Hermann Günther Grassmann (1809.-1877.), njemački matematičar, fizičar i lingvist.

Dokaz. Pretpostavimo da je $m \leq m'$. Stupanj n_i grafa G_i dobijemo tako da uzmemo matricu A i prebrojimo koliko ima matrica B takvih da je $\mathrm{rk}(A - B) = i$. Odgovor je isti kao da prebrojavamo matrice $C \in M_{mm'}(\mathbb{F}_q)$ ranga i. Takvu matricu možemo identificirati s linearnim operatorom $C : \mathbb{F}_q^{m'} \to \mathbb{F}_q^m$ kojem je slika potprostor od $\mathbb{F}_q^m$ dimenzije i. Prvo izaberemo sliku $\mathrm{Im}\, C \leq \mathbb{F}_q^m$ na $\left[{m \atop i} \right]$ načina, zatim zadamo djelovanje od C. To je isto kao da biramo $i \times m'$ matricu punog ranga i, tj. njezine retke (i linearno nezavisnih vektora iz $\mathbb{F}_q^{m'}$):

$$n_i = \begin{bmatrix} m \\ i \end{bmatrix} \cdot (q^{m'} - 1)(q^{m'} - q) \cdots (q^{m'} - q^{i-1}) = \begin{bmatrix} m \\ i \end{bmatrix} \cdot \prod_{l=0}^{i-1} (q^{m'} - q^l).$$

Pokušajte izvesti formulu za presječne brojeve p_{ij}^k! □

Asocijacijsku shemu bilinearnih formi proučavao je Philippe Delsarte u članku [41]. Formulu za stupnjeve grafova G_i zapisao je na nešto drugačiji način [41, formula (2.9) na str. 229]:

$$n_i = \prod_{l=0}^{i-1} \frac{(q^m - q^l)(q^{m'} - q^l)}{q^i - q^l}.$$

1.1 Jako regularni grafovi

Jako regularne grafove uveo je R. C. Bose[4] u članku [13].

Definicija 1.9. *Neka je G jednostavan graf koji nije potpun niti prazan. Kažemo da je G* jako regularan *s parametrima $SRG(n, \Bbbk, \lambda, \mu)$ ako vrijedi:*

1. *G je regularan stupnja $\Bbbk$,*

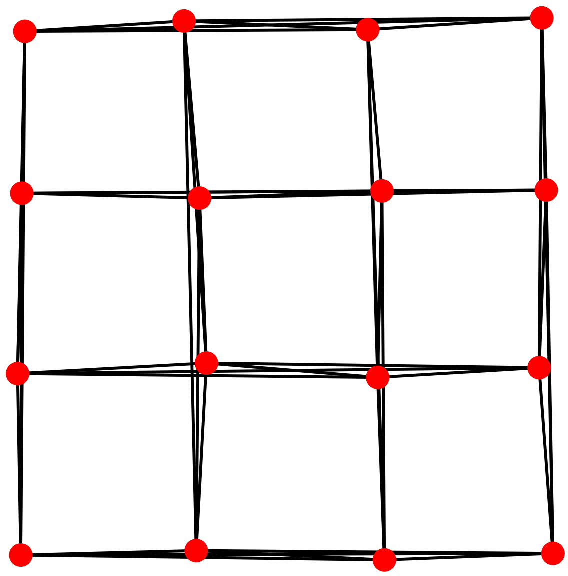
2. *svaka dva susjedna vrha imaju λ zajedničkih susjeda,*

3. *svaka dva nesusjedna vrha imaju μ zajedničkih susjeda.*

U oznakama iz primjera 1.4, za svaka dva vrha x i y takvog grafa vrijedi

$$|N(x) \cap N(y)| = \begin{cases} \Bbbk, & \text{ako je } x = y, \\ \lambda, & \text{ako je } x \sim y, \\ \mu, & \text{ako je } x \not\sim y. \end{cases}$$

[4]Raj Chandra Bose (1901.-1987.), indijsko-američki matematičar i statističar.



Slika 1: Topovski graf za $m = 4$.

Primjer 1.10 (Topovski grafovi)**.** *Neka je $m \in \mathbb{N}$. Za skup vrhova uzmemo $X = \{1, \ldots, m\}^2 = \{(i, j) \mid i, j \in \{1, \ldots, m\}\}$. Vrhovi (i, j) i (i', j') su susjedni ako je $i = i'$ ili $j = j'$ (ali ne oboje). Tako dobijemo jako regularan graf s parametrima $n = m^2$, $\Bbbk = 2m - 2$, $\lambda = m - 2$ i $\mu = 2$ koji se na engleskom zove* rook graph, lattice graph *ili* grid graph*. Zvat ćemo ga $m \times m$* topovskim grafom*; za $m = 4$ prikazan je na slici 1.*

Propozicija 1.11. *Ako je G jako regularan s parametrima $SRG(n, \Bbbk, \lambda, \mu)$, onda je njegov komplement G^c jako regularan s parametrima*

$$SRG(n,\, n - 1 - \Bbbk,\, n - 2\Bbbk + \mu - 2,\, n - 2\Bbbk + \lambda).$$

Dokaz. Komplementarni graf ima isti skup vrhova, a dva vrha su susjedni u G^c ako i samo ako nisu susjedni u G. Očito je G^c regularan stupnja $\overline{\Bbbk} = n - 1 - \Bbbk$. Dva nesusjedna vrha u G imaju μ zajedničkih susjeda, a uz to svaki ima još $\Bbbk - \mu$ susjeda. Znači da oba nisu susjedni s $n - 2 - 2(\Bbbk - \mu) - \mu = n - 2\Bbbk + \mu - 2$ vrhova u G, što je parametar $\overline{\lambda}$ komplementa. Slično dolazimo do parametra $\overline{\mu} = n - 2\Bbbk + \lambda$. □

Na primjer, komplement $m \times m$ topovskog grafa ima parametre $SRG(m^2, (m-1)^2, (m-2)^2, m^2 - 3m + 2)$.

Teorem 1.12. *Asocijacijska shema s dvije klase ekvivalentna je s parom međusobno komplementarnih jako regularnih grafova.*

Dokaz. Ako grafovi G_0, G_1, G_2 čine asocijacijsku shemu, onda su G_1 i G_2 međusobno komplementarni zbog svojstva 2. iz definicije 1.1. Znamo da su G_1 i G_2 regularni stupnja $k_1 = p_{11}^0$ i $k_2 = p_{22}^0$. Vrhovi x i y su susjedni u G_1 ako su 1-asocirani, a nisu susjedni u G_1 ako su 2-asocirani. Broj njihovih zajedničkih susjeda u G_1 u prvom slučaju je $\lambda_1 = p_{11}^1$, a u drugom slučaju $\mu_1 = p_{11}^2$. Na isti način vidimo da je G_2 jako regularan s parametrima $\lambda_2 = p_{22}^2$ i $\mu_2 = p_{22}^1$.

Obrnuto, pretpostavimo da su G_i međusobno komplementarni $SRG(n, k_i, \lambda_i, \mu_i)$ za $i = 1, 2$. Tada G_0, G_1, G_2 zadovoljavaju svojstva 1. i 2. iz definicije 1.1, a za svojstvo 3. već znamo presječne brojeve oblika p_{ii}^k. Treba provjeriti "mješovite" presječne brojeve p_{12}^k. Očito je $p_{12}^0 = 0$, a za p_{12}^1 uzmemo vrhove x i y koji su sudjedni u G_1 i prebrojavamo vrhove z koji su susjedni s x, a nisu susjedni s y (u G_1). Dobijemo $p_{12}^1 = k_1 - \lambda_1 - 1$, a na isti način slijedi $p_{12}^2 = k_2 - \lambda_2 - 1$. S pomoću propozicije 1.11 sve presječne brojeve možemo izraziti preko n, k_1, λ_1 i μ_1. □

Parametri jako regularnog grafa nisu nezavisni:

Propozicija 1.13. *Ako postoji jako regularan graf s parametrima $SRG(n, k, \lambda, \mu)$, onda vrijedi $k(k - \lambda - 1) = (n - k - 1)\mu$.*

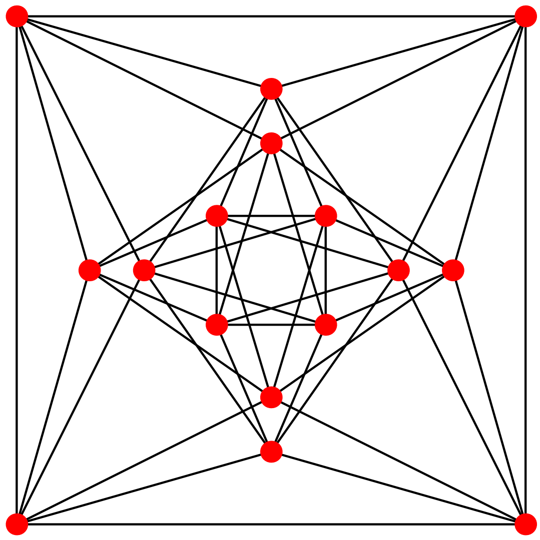
Dokaz. Fiksiramo vrh z i na dva načina prebrojimo parove vrhova

$$\{(x, y) \in X^2 \mid x \sim y,\ x \sim z,\ y \not\sim z\}.$$

□

Poznati su i drugi nužni uvjeti na parametre jako regularnog grafa. Pitanje o egzistenciji jako regularnih grafova s parametrima koji zadovoljavaju nužne uvjete je netrivijalno. Andries Brouwer održava web stranicu [19] s najnovijim rezultatima o egzistenciji i enumeraciji, a nedavno je objavljena monografija [21] o jako regularnim grafovima. U članku [39] matematičari iz Rijeke konstruirali su jako regularne grafove s parametrima $SRG(216, 40, 4, 8)$, $SRG(540, 187, 58, 68)$ i $SRG(540, 224, 88, 96)$ i time eliminirali tri upitnika iz Brouwerove tablice [19]. O broju neizomorfnih jako regularnih grafova Peter Cameron [28] je napisao

> "Strongly regular graphs lie on the cusp between highly structured and unstructured. For example, there is a unique strongly regular graph with parameters $(36, 10, 4, 2)$, but there are 32548 non-isomorphic graphs with parameters $(36, 15, 6, 6)$. (The first assertion is a special case of a theorem of Shrikhande, while the second is the result of a computer search by McKay and Spence.)"



Slika 2: Shrikhandeov graf $SRG(16, 6, 2, 2)$ (preuzeto s [134]).

Drugi spomenuti rezultat objavljen je u [100], a Shrikhandeov[5] teorem u [115]:

Teorem 1.14. *Za $m = 2, 3$ i $m \geq 5$, svaki jako regularan graf s parametrima $SRG(m^2, 2m - 2, m - 2, 2)$ izomorfan je topovskom grafu iz primjera 1.10. Za $m = 4$ postoji još jedan takav graf prikazan na slici 2.*

Graf na slici 2 zovemo *Shrikhandeovim grafom.*

1.2 Distancijsko regularni grafovi

Neka je G graf sa skupom vrhova X. *Put* u G je niz međusobno različitih vrhova $(x_0, x_1, \ldots, x_k)$ takav da je $x_{i-1} \sim x_i$ za svaki $i = 1, \ldots, k$. *Duljina puta* je njegov broj bridova k (a ne broj vrhova $k + 1$). *Udaljenost* vrhova $\partial(x, y)$ je duljina najkraćeg puta od x do y. Ako nema takvih putova, stavljamo $\partial(x, y) = \infty$. Graf u kojem postoji put između svaka dva vrha zovemo *povezanim.* Funkcija ∂ je metrika na skupu vrhova povezanog grafa.

Zadatak 1.15. *Provjerite nejednakost trokuta za Hammingovu metriku iz primjera 1.6, "rang metriku" iz primjera 1.8 i upravo definiranu metriku na vrhovima povezanog grafa.*

[5]Sharadchandra Shankar Shrikhande (1917.-2020.), indijski matematičar.

Najveću moguću udaljenost vrhova $\partial(x,y)$ zovemo *dijametrom* grafa. Jako regularni grafovi su povezani ako je $\mu > 0$ i u tom slučaju imaju dijametar 2. U teoremu 1.12 vidjeli smo da od jako regularnog grafa dobivamo asocijacijsku shemu s dvije klase, a sada to želimo generalizirati na grafove dijametra d. Ako je x vrh, označimo s

$$N_i(x) = \{y \in X \mid \partial(x,y) = i\}$$

skup svih vrhova na udaljenosti i. Tako dobijemo particiju skupa vrhova

$$X = N_0(x) \cup N_1(x) \cup \cdots \cup N_d(x)$$

u kojoj je $N_0(x) = \{x\}$, a $N_1(x) = N(x)$ je skup susjeda od x.

Definicija 1.16. *Neka je G povezan graf dijametra d. Kažemo da je G* distancijsko regularan graf (DRG) *ako broj $|N_i(x) \cap N_j(y)|$ ovisi samo o indeksima i, j te o udaljenosti $\partial(x,y)$, a ne o izboru vrhova $x, y \in X$.*

Teorem 1.17. *Neka je G distancijsko regularan graf dijametra d. Ako za vrhove $x, y \in X$ definiramo da su i-asocirani kad je $\partial(x,y) = i$, dobivamo asocijacijsku shemu s d klasa.*

Dokaz. Od grafa G definirali smo grafove $G_0, G_1, \ldots, G_d$ s istim skupom vrhova; vrhovi x i y su susjedni u G_i ako je $\partial(x,y) = i$. Graf G_0 sadrži petlje, a grafovi $G_1, \ldots, G_d$ particioniraju bridove potpunog grafa jer su svaka dva vrha na nekoj udaljenosti iz $\{1, \ldots, d\}$. Pritom je $G_1 = G$. Za $\partial(x,y) = k$, skup svih vrhova z takvih da su x, z susjedni u G_i, a z, y susjedni u G_j je upravo $N_i(x) \cap N_j(y)$. Stoga su presječni brojevi ove asocijacijske sheme $p_{ij}^k = |N_i(x) \cap N_j(y)|$. $\square$

U knjizi [20] definicija distancijsko regularnog grafa je slabija od definicije 1.16:

Definicija 1.18. *Povezan graf G je* distancijsko regularan *ako je regularan stupnja $\Bbbk$ i za svaka dva vrha na udaljenosti $\partial(x,y) = i$ brojevi $b_i = |N_{i+1}(x) \cap N_1(y)|$ i $c_i = |N_{i-1}(x) \cap N_1(y)|$ su konstantni.*

Skup $N_1(y)$ sadrži susjedne vrhove $z \sim y$. Ako je $\partial(x,y) = i$, udaljenost $\partial(x,z)$ je element skupa $\{i-1, i, i+1\}$. Zato je broj $a_i = |N_i(x) \cap N_1(y)|$ također konstantan i vrijedi $a_i + b_i + c_i = \Bbbk$. Brojeve a_i, b_i, c_i zovemo *presječnim brojevima* distancijsko regularnog grafa. Veza s ranije definiranim presječnim brojevima $p_{ij}^k = |N_i(x) \cap N_j(y)|$ (za $\partial(x,y) = k$) je

$$a_i = p_{i1}^i, \quad b_i = p_{i+1,1}^i, \quad c_i = p_{i-1,1}^i.$$

Još neka svojstva presječnih brojeva sabrana su u sljedećem teoremu.

Teorem 1.19.

(a) *Brojevi* $\hbar_i = |N_i(x)|$ *ne ovise o izboru vrha* x *i vrijedi* $\hbar_0 = 1$, $\hbar_1 = \hbar$, $\hbar_{i+1} = \hbar_i b_i / c_{i+1}$, *za* $i = 0, \ldots, d-1$.

(b) *Ukupan broj vrhova grafa je* $n = 1 + \hbar_1 + \ldots + \hbar_d$.

(c) $1 = c_1 \leq c_2 \leq \cdots \leq c_d$.

(d) $\hbar = b_0 > b_1 \geq \cdots \geq b_{d-1}$.

(e) $c_0 = b_d = 0$.

(f) *Ako je* $i + j \leq d$, *onda je* $c_i \leq b_j$.

Pokazuje se da je slabija definicija distancijsko regularnog grafa 1.18 ekvivalentna jačoj definiciji 1.16. Dake, ako su brojevi $p_{ij}^k = |N_i(x) \cap N_j(y)|$, $k = \partial(x, y)$ konstantni za $j = 1$, $i = k \pm 1$, onda su konstantni za sve izbore i, j, k. U idućem teoremu vidimo kako p_{ij}^k možemo izračunati iz a_i, b_i, c_i.

Teorem 1.20. *Vrijedi* $p_{0j}^k = \delta_{jk}$, $p_{i0}^k = \delta_{ik}$ *i*

$$p_{1j}^k = \begin{cases} c_k, & \textit{za } j = k-1, \\ a_k, & \textit{za } j = k, \\ b_k, & \textit{za } j = k+1, \\ 0, & \textit{inače.} \end{cases}$$

Uz to vrijedi rekurzija

$$p_{i+1,j}^k = \frac{1}{c_{i+1}} \left(p_{i,j-1}^k b_{j-1} + p_{i,j}^k (a_j - a_i) + p_{i,j+1}^k c_{j+1} - p_{i-1,j}^k b_{i-1} \right).$$

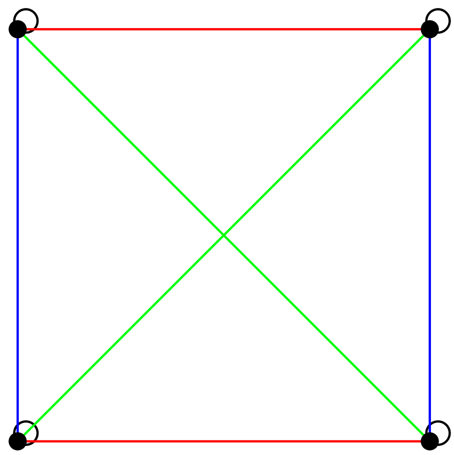
Dokazi teorema nalaze se u knjizi [20]. Budući da brojevi b_i, c_i jednoznačno određuju sve ostale parametre, zapisujemo ih u obliku $\{b_0, \ldots, b_{d-1}; c_1, \ldots, c_d\}$ i zovemo *presječnim nizom* distancijsko regularnog grafa.

Propozicija 1.21. *Povezan graf je jako regularan ako i samo ako je distancijsko regularan dijametra 2. Parametri* $SRG(n, \hbar, \lambda, \mu)$ *odgovaraju presječnom nizu* $\{\hbar, \hbar - \lambda - 1; 1, \mu\}$.

Dokaz. Po teoremu 1.17, od distancijsko regularnog grafa G dijametra $d = 2$ dobivamo asocijacijsku shemu s dvije klase. Po teoremu 1.12, grafovi G_1 i G_2 od kojih se ona sastoji su jako regularni i vrijedi $G = G_1$. Dakle, G je povezan jako regularan graf.

Obrnuto, neka je G povezan jako regularan graf s parametrima $SRG(n, \Bbbk, \lambda, \mu)$. Dijametar od G je $d = 2$ jer vrhovi koji nisu susjedni imaju $\mu > 0$ zajedničkih susjeda, pa su na udaljenosti 2. Presječni broj b_0 je $|N_1(x) \cap N_1(x)| = \Bbbk$, a b_1 je $|N_2(x) \cap N_1(y)|$ za susjedne vrhove $x \sim y$. To je broj vrhova z koji su susjedni s y i nisu susjedni s x i možemo ga izraziti kao $\Bbbk - \lambda - 1$. Slično vidimo da su presječni brojevi $c_1 = 1$ i $c_2 = \mu$. □

Za asocijacijsku shemu koja nastaje od distancijsko regularnog grafa G kao u teoremu 1.17 kažemo da je *metrička* obzirom na G. Općenito, kad je broj klasa $d > 2$, asocijacijska shema ne mora biti metrička obzirom na niti jedan od svojih grafova. Najmanji primjer je asocijacijska shema reda 4 s tri klase prikazana na slici 3. Ona nije metrička jer su grafovi od kojih se sastoji nepovezani. Postoje primjeri asocijacijskih shema koje sadrže povezane grafove (čak mogu biti distancijsko regularni!), ali nisu metričke obzirom na njih. S druge strane, neki od "distancijskih grafova" G_i definiranih od DRG-a kao u teoremu 1.17 mogu biti nepovezani (za $i > 1$).



Slika 3: Asocijacijska shema koja nije metrička.

Zadatak 1.22. *Ako asocijacijska shema s d klasa sadrži povezan graf dijametra d, onda je metrička obzirom na taj graf.*

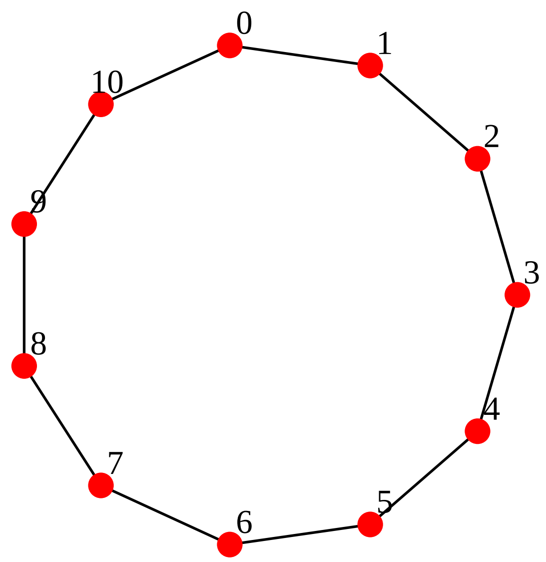
Teorem 1.23. *Asocijacijska shema je metrička obzirom na prvi graf G_1 ako i samo ako njezini presječni brojevi zadovoljavaju sljedeća dva uvjeta:*

1. *ako je $k = i + j$, onda je $p_{ij}^k \neq 0$,*

2. *ako je $p_{ij}^k \neq 0$, onda je $|i - j| \leq k \leq i + j$.*

Dokaz. Sloane [117] kaže da je u Delsarteu [40], ali nisam našao na prvi pogled. Vjerojatno ima u [20]. □

Svi primjeri asocijacijskih shema koje smo do sada susreli su metrički obzirom na G_1. Poligon (primjer 1.4) nastaje od distancijsko regularnog grafa koji se sastoji od jednog ciklusa duljine n, prikazanog na slici 4. Presječni niz poligona je $\{2, 1, \ldots, 1; 1, \ldots, 1, c_d\}$ pri čemu je $c_d = 2$ za parni n i $c_d = 1$ za neparni n.

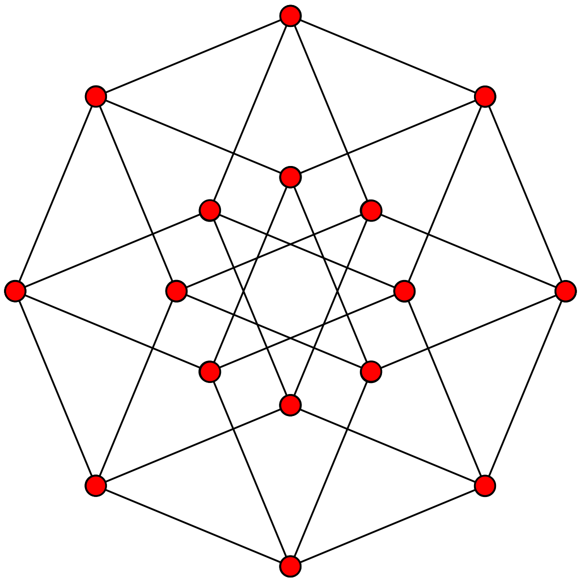


Slika 4: Poligon reda $n = 11$.

Johnsonov graf $G_1 = J(v, d, 1)$ je distancijsko regularan i generira Johnsonovu shemu (primjer 1.5). Naime, za dva d-člana podskupa $X, Y \subseteq V$ vrijedi $|X \cap Y| = d - k$ ako i samo ako najkraći niz međusobno različitih d-podskupova $X = X_0, X_1, \ldots, X_l = Y$ takav da je $|X_{i-1} \cap X_i| = d - 1$, $\forall i = 1, \ldots, l$ ima duljinu $l = k$. Jasno je da možemo napraviti takav niz duljine k: skupovi $X \setminus Y$ i $Y \setminus X$ oba sadrže k elemenata, pa izbacujemo jedan po jedan elemente iz $X \setminus Y$ i dodajemo elemente iz $Y \setminus X$. Ako postoji takav niz duljine k, onda presjek $X \cap Y$ sadrži bar $d - k$ elemenata. U svakom koraku izbacujemo jedan element i dodajemo neki drugi element, pa ne možemo promijeniti više od k elemenata presjeka. Ako nikada ne vraćamo prethodno izbačeni element, niti izbacujemo element kojeg smo prethodno dodali (tj. naš niz je najkraći mogući), onda je $|X \cap Y| = d - k$.

U grafu G_1 Hammingove sheme (primjer 1.6) riječi x i y su susjedne ako se razlikuju na jednoj koordinati. Primijetimo da se Hammingova metrika podudara s metrikom definiranom s pomoću susjedstva u tom grafu. Zato je Hammingova shema $H(d,q)$ metrička obzirom na G_1. Argumentacija je slična za Grassmannovu shemu (primjer 1.7) i shemu bilinearnih formi (primjer 1.8).

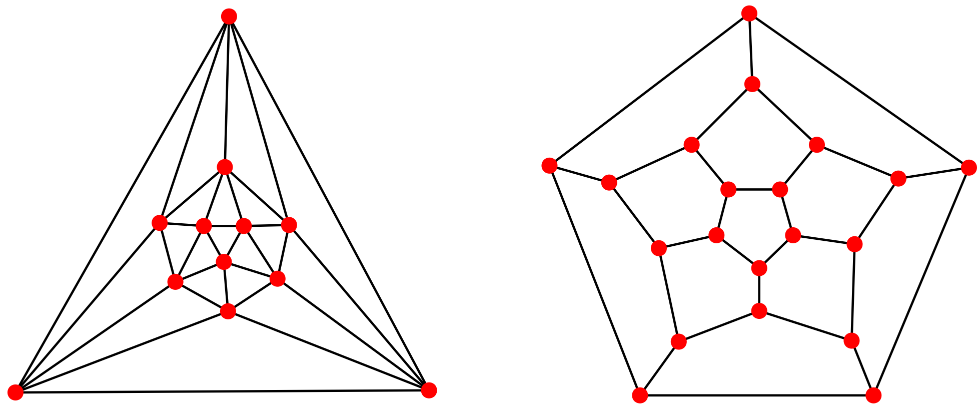
Zadatak 1.24. *Napišite presječni niz Johnsonovog grafa $J(v,d,1)$ i prvog grafa Hammingove sheme $H(d,q)$.*



Slika 5: Hiperkocka dimenzije $d = 4$ (preuzeto s [136]).

Prvi graf binarne Hammingove sheme $H(d,2)$ podudara se s grafom vrhova i bridova d-dimenzionalne hiperkocke (slika 5). "Mreže" nekih drugih pravilnih politopa također su distancijsko regularni grafovi. Mreža d-dimenzionalnog simpleksa je potpun graf K_{d+1} i možemo je interpretirati kao Johnsonov graf $J(d+1,1,1)$. Dual hiperkocke je d-dimenzionalni analogon oktaedra (*ortopleks* ili "*cross-polytope*") i također daje DRG. Drugi pravilni konveksni politopi postoje samo u trodimenzionalnom i četverodimenzionalnom prostoru. Zanimljivo je da su mreže ikosaedra i dodekaedra DRG-ovi, ali od 4-politopa ne dobivamo DRG-ove. To su *oktapleks* (politop kojem su strane 24 oktaedra), *tetrapleks* (strane su 600 tetraedara) i *dodekapleks* (strane su 120 dodekaedara).

Zadatak 1.25. *Napišite presječne nizove ikosaedra, dodekaedra i d-dimenzionalnog ortopleksa.*



Slika 6: Mreže ikosaedra i dodekaedra (preuzeto s [131, 133]).

Prirodan uvjet iz kojeg slijedi da je graf distancijsko regularan je takozvana *distancijska tranzitivnost*. Automorfizam grafa G je bijekcija na skupu njegovih vrhova $\alpha : X \to X$ koja čuva relaciju susjedstva, tj. takva da vrijedi $x \sim y \iff \alpha(x) \sim \alpha(y)$, $\forall x, y \in X$. Skup svih automorfizama od G je grupa obzirom na kompoziciju. Zovemo je *punom grupom automorfizama* od G i označavamo $\mathrm{Aut}(G)$.

Definicija 1.26. *Za graf G kažemo da je* distancijsko tranzitivan *ako za svaka dva para vrhova x, y i x', y' na istoj udaljenosti $\partial(x, y) = \partial(x', y')$ postoji automorfizam $\alpha \in \mathrm{Aut}(G)$ takav da je $\alpha(x) = x'$ i $\alpha(y) = y'$.*

Propozicija 1.27. *Ako je graf G distancijsko tranzitivan, onda je distancijsko regularan.*

Dokaz. Za vrhove x, y, x', y' takve da je $\partial(x, y) = \partial(x', y')$ trebamo pokazati $|N_i(x) \cap N_j(y)| = |N_i(x') \cap N_j(y')|$. Znamo da postoji $\alpha \in \mathrm{Aut}(G)$ koji preslikava $\alpha(x) = x'$ i $\alpha(y) = y'$. Svaki automorfizam čuva udaljenost u grafu, tj. vrijedi $\partial(\alpha(z), \alpha(z')) = \partial(z, z')$, $\forall z, z' \in X$. Zato vrijedi $\alpha(N_i(x)) = N_i(x')$ i $\alpha(N_j(y)) = N_j(y')$, iz čega slijedi $\alpha(N_i(x) \cap N_j(y)) = N_i(x') \cap N_j(y')$. Vidimo da su presječni skupovi jednakobrojni. $\square$

Primijetimo da je funkcija $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$ koju smo koristili u dokazu primjera 1.4 automorfizam grafa n-terokuta. Taj graf je distancijsko tranzitivan, kao i ostali primjeri DRG-ova koje smo spominjali. Svaka permutacija $\alpha \in S_v$ inducira automorfizam Johnsonovog grafa $J(v, d, 1)$ (djelovanje α na d-podskupovima). Za podskupove $X, Y, X', Y' \subseteq V$ takve da je $|X \cap Y| = |X' \cap Y'|$ možemo naći permutaciju $\alpha \in S_v$ koja preslikava

$\alpha(X) = X'$ i $\alpha(Y) = Y'$. Za Hammingovu shemu $H(d,q)$ automorfizmi su permutacije simbola na pojedinim koordinatama (djelovanje direktnog produkta d simetričnih grupa $S_q \times \cdots \times S_q$) i permutacije koordinata (djelovanje simetrične grupe S_d). Zajedno generiraju grupu $S_d \wr S_q$ ("*wreath product*") s kojom možemo preslikati par riječi u bilo koji drugi par riječi na istoj Hammingovoj udaljenosti. Grafovi od kojih dobivamo Grassmanovu shemu i shemu bilinearnih formi također su distancijsko tranzitivni. Najmanji primjer distancijsko regularnog grafa koji nije distancijsko tranzitivan je Shrikhandeov graf (slika 2).

1.3 Simetrični dizajni

Definicija 1.28. *Neka je* $V = \{1, \dots, v\}$ *skup* točaka *i* $\mathcal{D} \subseteq \binom{V}{\Bbbk}$ *familija* $\Bbbk$*-članih podskupova od* V *koje zovemo* blokovima. *Kažemo da je* $\mathcal{D}$ dizajn *s parametrima* $(v, \Bbbk, \lambda)$ *ako za svake dvije točke postoji točno* λ *blokova koji ih sadrže. Dizajn je* simetričan *ako je broj blokova jednak broju točaka:* $|\mathcal{D}| = v$.

Dvostrukim prebrojavanjem vidimo da za svaku točku postoji točno $r = \lambda \cdot \frac{v-1}{\Bbbk-1}$ blokova koji je sadrže, a ukupan broj blokova je $b = |\mathcal{D}| = \lambda \cdot \frac{v(v-1)}{\Bbbk(\Bbbk-1)}$. Iz toga slijedi nužan uvjet za postojanje simetričnih dizajna $\lambda(v-1) = \Bbbk(\Bbbk-1)$. Parametre $(v, \Bbbk, \lambda)$ koji zadovoljavaju taj uvjet zovemo *dopustivim*.

Teorem 1.29. *Ako je dizajn s parametrima* $(v, \Bbbk, \lambda)$ *simetričan, onda se svaka dva bloka tog dizajna sijeku u* λ *točaka. Obrnuto, ako se svaka dva bloka* $(v, \Bbbk, \lambda)$ *dizajna sijeku u konstantnom broju točaka, onda je taj broj* λ, *a dizajn je simetričan.*

Primjer 1.30. *Neka je* q *potencija prostog broja i* $\mathbb{F}_q^{d+1}$ *vektorski prostor dimenzije* $d+1$ *nad konačnim poljem* $\mathbb{F}_q$. *Kao točake uzmimo sve* 1*-dimenzionalne potprostore, a kao blokove skupove točaka sadržane u* d*-dimenzionalnim potprostorima ("hiperravninama"). Tako dobijemo simetrični dizajn s parametrima* $v = \begin{bmatrix} d+1 \\ 1 \end{bmatrix}_q$, $\Bbbk = \begin{bmatrix} d \\ 1 \end{bmatrix}_q$ *i* $\lambda = \begin{bmatrix} d-1 \\ 1 \end{bmatrix}_q$.

Simetrični dizajn s parametrom $\lambda = 1$ zovemo *konačnom projektivnom ravninom.* U tom slučaju parametri su oblika $(n^2+n+1, n+1, 1)$ za neki prirodan broj n koji zovemo *redom* projektivne ravnine. Općenito, red simetričnog dizajna definiramo kao $n = \Bbbk - \lambda$. Konstrukcija iz primjera 1.30 za $d = 2$ daje projektivnu ravninu reda q. Poznate su mnoge druge konstrukcije konačnih projektivnih ravnina, koje daju primjere neizomorfne ravninama iz primjera 1.30, ali svi ti primjeri imaju redove koji su prim potencije. Jedno od najvažnijih otvorenih pitanja o simetričnim dizajnima je

Pitanje 1.31. *Postoji li projektivna ravnina reda koji nije prim potencija?*

Poznat je netrivijalan nužan uvjet za postojanje projektivnih ravnina:

Teorem 1.32 (Bruck[6]-Ryser[7]). *Ako postoji projektivna ravnina reda* $n \equiv 1$ *ili* $2 \pmod 4$*, onda se* n *može prikazati kao zbroj kvadrata dvaju cijelih brojeva.*

Iz teorema slijedi nepostojanje projektivnih ravnina reda $n = 6$, 14, 22 i svih redova oblika $n \equiv 6 \pmod 8$. Poznato je da ne postoji ravnina reda $n = 10$, ali to ne slijedi iz teorema nego je dokazano pomoću računala [89]. Generalizacija Bruck-Ryserova teorema na simetrične dizajne je sljedeći teorem.

Teorem 1.33 (Bruck-Ryser-Chowla[8]). *Neka postoji simetrični* $(v, \Bbbk, \lambda)$ *dizajn.*

1. *Ako je* v *paran, onda je red* $n = \Bbbk - \lambda$ *kvadrat cijelog broja.*
2. *Ako je* v *neparan, onda jednadžba* $n\,x^2 + (-1)^{(v-1)/2}\,\lambda\,y^2 = z^2$ *ima netrivijalno cjelobrojno rješenje* $(x, y, z) \neq (0, 0, 0)$.

Prva tvrdnja poznata je i kao Schützenbergerov[9] teorem. Osim projektivnih ravnina, konstruirane su mnoge beskonačne serije simetričnih dizajna (vidi [67]). Međutim, za svaki čvrsti $\lambda > 1$ poznato je samo konačno mnogo primjera. Još jedno otvoreno pitanje o simetričnim dizajnima je

Pitanje 1.34. *Je li istina da za svaki* $\lambda > 1$ *postoji samo konačno mnogo simetričnih* $(v, \Bbbk, \lambda)$ *dizajna?*

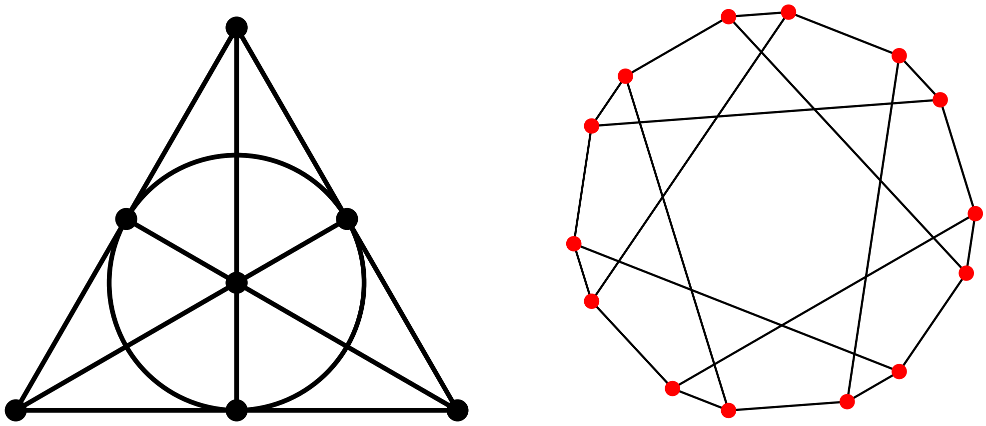
Profesor Janko[10] konstruirao je mnoge sporadične primjere simetričnih dizajna: $(70, 24, 8)$ [75], $(71, 21, 6)$ [76], $(78, 22, 6)$ [77], $(105, 40, 15)$ [70], $(189, 48, 12)$ [71]. U člancima [72] i [74] konstruirao je beskonačne serije simetričnih dizajna, a u članku [73] jako regularne grafove $SRG(936, 375, 150, 150)$ i $SRG(1800, 1029, 588, 588)$ te eliminirao upitnik iz Brouwerove tablice [19]. Analogna tablica o egzistenciji $(v, \Bbbk, \lambda)$ dizajna objavljena je u [99]. Knjige [66] i [90] su monografije posvećene simetričnim dizajnima.

Zadatak 1.35. *Neka je* $\mathscr{D}$ *simetrični* $(v, \Bbbk, \lambda)$ *dizajn. Definiramo bipartitan graf* G *kojem su vrhovi točke i blokovi od* $\mathscr{D}$*, a susjedni su ako točka pripada bloku. Dokažite da je* G *distancijsko regularan graf dijametra* $d = 3$,

[6] Richard Hubert Bruck (1914.-1991.), američki matematičar.
[7] Herbert John Ryser (1923.–1985.), američki matematičar.
[8] Sarvadaman D. S. Chowla (1907.-1995.), indijsko-američki matematičar.
[9] Marcel-Paul Schützenberger (1920.-1996.), francuski matematičar i doktor medicine.
[10] Zvonimir Janko (1932.-2022.), hrvatski matematičar.

odredite mu presječni niz $\{b_0, b_1, b_2; c_1, c_2, c_3\}$ i presječne brojeve p_{ij}^k odgovarajuće asocijacijske sheme. Dolazi li svaka (metrička) asocijacijska shema s tim presječnim brojevima od simetričnog $(v, \Bbbk, \lambda)$ dizajna?

Od projektivne ravnine reda 2, takozvane Fanove[11] ravnine ili simetričnog $(7, 3, 1)$ dizajna, dobijemo Heawoodov[12] graf (slika 7).



Slika 7: Fanova ravnina i Heawoodov graf (preuzeto s [132]).

Rješenje. Presječni niz je $\{\Bbbk, \Bbbk-1, \Bbbk-\lambda; 1, \lambda, \Bbbk\}$. Presječni brojevi su

$$[p_{ij}^0] = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \Bbbk & 0 & 0 \\ 0 & 0 & v-1 & 0 \\ 0 & 0 & 0 & v-\Bbbk \end{bmatrix}, \quad [p_{ij}^1] = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & \Bbbk-1 & 0 \\ 0 & \Bbbk-1 & 0 & v-\Bbbk \\ 0 & 0 & v-\Bbbk & 0 \end{bmatrix},$$

$$[p_{ij}^2] = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & \lambda & 0 & \Bbbk-\lambda \\ 1 & 0 & v-2 & 0 \\ 0 & \Bbbk-\lambda & 0 & v-2\Bbbk+\lambda \end{bmatrix}, \quad [p_{ij}^3] = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & \Bbbk & 0 \\ 0 & \Bbbk & 0 & v-\Bbbk-1 \\ 1 & 0 & v-\Bbbk-1 & 0 \end{bmatrix}.$$

Svaka asocijacijska shema s ovim presječnim brojevima je metrička obzirom na G_1 zbog teorema 1.23. Dakle, G_1 je DRG dijametra $d = 3$ s presječnim nizom $\{\Bbbk, \Bbbk-1, \Bbbk-\lambda; 1, \lambda, \Bbbk\}$. Definiramo incidencijsku strukturu kojoj

[11]Gino Fano (1871.-1952.), talijanski matematičar.
[12]Percy John Heawood (1861.-1955.), britanski matematičar.

je G_1 incidencijski graf: izaberemo bilo koji vrh x_0 i definiramo da su točke vrhovi na parnoj udaljenosti od x_0, a blokovi su vrhovi na neparnoj udaljenosti od x_0. Incidencija između točaka i blokova je susjedstvo u grafu G_1. Stupnjevi grafova sheme su $n_0 = 1$, $n_1 = \Bbbk$, $n_2 = v - 1$, $n_3 = v - \Bbbk$ pa je broj točaka i blokova $n_0 + n_2 = n_1 + n_3 = v$. Kroz svaku točku prolazi $\Bbbk$ blokova i na svakom bloku leži $\Bbbk$ točaka zbog $n_1 = \Bbbk$. Kroz svake dvije točke prolazi $p_{11}^2 = \lambda$ blokova. Dakle, incidencijska struktura je simetrični $(v, \Bbbk, \lambda)$ dizajn. □

1.4 Koherentne konfiguracije

U cjelini 1.2 vidjeli smo da primjeri asocijacijskih shema koje smo spominjali dolaze od grafova koji nisu samo distancijsko regularni, nego i distancijsko tranzitivni. To znači da grupa automorfizama djeluje tranzitivno na svim parovima vrhova koji su na istoj udaljenosti. Propozicija 1.27 i teorem 1.17 pokazuju kako iz tog uvjeta slijede definicijska svojstva asocijacijske sheme. Sada je ideja uzeti bilo koju tranzitivnu permutacijsku grupu G na skupu vrhova X i proglasiti da su parovi vrhova asocirani ako leže u istoj orbiti pod djelovanjem grupe G. Tada su uvjeti iz definicije 1.1 automatski ispunjeni.

Primjer 1.36 (Schurova[13] konstrukcija)**.** *Neka je $G \leq \mathrm{Sym}(X)$ grupa permutacija na skupu X koja djeluje tranzitivno, tj. tako da vrijedi*

$$(\forall x, y \in X)(\exists g \in G)\ x^g = y.$$

Neka su $R_0, R_1, \ldots, R_d$ orbite pri djelovanju grupe G na skup svih uređenih parova $X \times X$. Možemo pretpostaviti da je $R_0 = \{(x, x) \mid x \in X\}$. Tada vrijedi $\cup_{i=0}^{d} R_i = X \times X$ (disjunktna unija). Nadalje, za svaki izbor indeksa $i, j, k \in \{0, \ldots, d\}$ postoji broj $p_{ij}^k \in \mathbb{N}_0$ takav da je za svaki par $(x, y) \in R_k$ broj vrhova $z \in X$ koji zadovoljavaju $(x, z) \in R_i$ i $(z, y) \in R_j$ jednak p_{ij}^k.

Djelovanje permutacije $g \in G$ zapisujemo zdesna x^g, umjesto funkcijski $g(x)$ kao ranije. Orbitu elementa $x \in X$ označavamo $x^G = \{x^g \mid g \in G\}$, a stabilizator $G_x = \{g \in G \mid x^g = x\}$. Promatramo inducirano djelovanje na parovima $(x, y)^g = (x^g, y^g)$. Orbite na parovima zovemo *orbitalama*, a broj orbitala *rangom* tranzitivne permutacijske grupe G.

Dokaz. Jasno je da skup svih orbitala $R_0, R_1, \ldots, R_d$ particionira Kartezijev kvadrat $X \times X$. Orbitala $R_0 = (x, x)^G$ sadrži sve parove oblika (y, y) zbog tranzitivnosti od G. Ako uzmemo bilo koja dva para (x, y), (x', y') iz iste

[13] Issai Schur (1875.-1941.), ruski matematičar koji je radio u Njemačkoj.

orbitale R_k, onda postoji $g \in G$ takav da je $(x', y') = (x, y)^g$. Vrh z zadovoljava $(x, z) \in R_i$, $(z, y) \in R_j$ ako i samo ako $z' = z^g$ zadovoljava $(x', z') \in R_i$, $(z', y') \in R_j$. Zbog bijektivnosti od g broj takvih vrhova je isti za par (x, y) i par (x', y'). $\square$

Svojstvo koje ne mora biti ispunjeno je simetričnost. Naime, u definiciji 1.1 asocijacijska shema sastoji se od grafova, tj. simetričnih relacija na skupu vrhova X. Sada imamo relacije $R_i \subseteq X \times X$ koje ne moraju biti simetrične, tj. može vrijediti $(x, y) \in R_i$ i $(y, x) \notin R_i$.

Primjer 1.37. *Neka je* $G = \{(), (1\ 2\ 3), (1\ 3\ 2)\}$ *permutacijska grupa reda tri na skupu* $X = \{1, 2, 3\}$. *Schurovom konstrukcijom dobijemo relacije* $R_0 = \{(1, 1), (2, 2), (3, 3)\}$, $R_1 = \{(1, 2), (2, 3), (3, 1)\}$ *i* $R_2 = \{(1, 3), (2, 1), (3, 2)\}$. *Relacije* R_1 *i* R_2 *nisu simetrične, ali presječni brojevi su dobro definirani:*

$$[p^0_{ij}] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad [p^1_{ij}] = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad [p^2_{ij}] = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

Svojstvo koje ipak vrijedi je da za svaku relaciju R_i njoj transponirana relacija $R_i^t = \{(y, x) \mid (x, y) \in R_i\}$ također pripada shemi. Naime, ako je $R_i = (x, y)^G$, onda je $R_i^t = (y, x)^G$. U primjeru 1.37 je $R_0^t = R_0$ i $R_1^t = R_2$. U skladu s preporukom P. Camerona [30], "općenitije asocijacijske sheme" u kojima relacije ne moraju biti simetrične zvat ćemo *koherentnim konfiguracijama.* U knjizi [4] naziv *asocijacijska shema* koristi se za općenitiji pojam.

Definicija 1.38. Koherentna konfiguracija *reda n s d klasa sastoji se od n-članog skupa* vrhova X *i relacija* $R_0, \ldots, R_d \subseteq X \times X$ *takvih da vrijedi:*

1. $R_0 = \{(x, x) \mid x \in X\}$ *je "dijagonala",*
2. $\{R_0, \ldots, R_d\}$ *čine particiju od* $X \times X$,
3. *za svaki indeks i postoji indeks i' takav da je* $R_i^t = R_{i'}$,
4. *za svaki izbor indeksa i, j, k postoji* presječni broj $p^k_{ij} \in \mathbb{N}_0$ *takav da je* $|\{z \in X \mid (x, z) \in R_i,\ (z, y) \in R_j\}| = p^k_{ij}$ *za sve parove* $(x, y) \in R_k$.

Ako su relacije simetrične, tj. u 3. svojstvu uvijek vrijedi $i = i'$, koherentnu konfiguraciju zovemo asocijacijskom shemom. *Ako presječni brojevi zadovoljavaju $p^k_{ij} = p^k_{ji}$ za svaki izbor indeksa, kažemo da je koherentna konfiguracija* komutativna.

U zadatku 1.3 vidjeli smo da iz simetričnosti slijedi komutativnost. Koherentna konfiguracija u primjeru 1.37 nije simetrična, ali je komutativna. Slijedi primjer nekomutativne koherentne konfiguracije.

Primjer 1.39. *Neka je* $G = \langle (1\ 2\ 3)(4\ 5\ 6), (1\ 6)(2\ 5)(3\ 4) \rangle$ *permutacijska grupa na skupu* $X = \{1, 2, 3, 4, 5, 6\}$*. Izomorfna je diedralnoj grupi reda* 6*. Relacije su orbitale* $R_0 = (1,1)^G$*,* $R_1 = (1,2)^G$*,* $\ldots, R_5 = (1,6)^G$*, a presječni brojevi su*

$$[p_{ij}^0] = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad [p_{ij}^1] = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix},$$

$$[p_{ij}^2] = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}, \quad [p_{ij}^3] = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix},$$

$$[p_{ij}^4] = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad [p_{ij}^5] = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Schurova konstrukcija daje asocijacijsku shemu (simetričnu koherentnu konfiguraciju) ako i samo ako grupa G ima svojstvo

$$(\forall x, y \in X)(\exists g \in G)\ x^g = y \text{ i } y^g = x.$$

Takve permutacijske grupe zovemo *obilno tranzitivnim* (eng. *generously transitive*). Primjeri 1.4 (poligon), 1.5 (Johnsonova shema), 1.6 (Hammingova shema), 1.7 (Grassmannova shema) i 1.8 (shema bilinearnih formi) svi nastaju Schurovom konstrukcijom od obilno tranzitivnih grupa. Poligon reda n dobijemo od diedralne grupe D_{2n}. To je grupa izometrija euklidske ravnine koje preslikavaju pravilan n-terokut na samog sebe, restringirana na vrhove. Ona djeluje obilno tranzitivno jer svaki par vrhova možemo međusobno preslikati zrcaljenjem, tj. involucijom.

Zadatak 1.40. *Dokažite da red obilno tranzitivne permutacijske grupe mora biti paran.*

Najmanji primjer koherentne konfiguracije koja nije Schurova, tj. ne nastaje konstrukcijom 1.36 je asocijacijska shema sastavljena od Shrikhandeova grafa (slika 2) i njegova komplementa. Detaljan dokaz dan je u [4, primjer 2.10 na str. 51-52].

Zadatak 1.41. *Definiciju koherentne konfiguracije 1.38 možemo još oslabiti tako da umjesto 1. svojstva zahtijevamo postojanje relacija $R_0, \ldots, R_e$ koje u uniji daju dijagonalu $\{(x,x) \mid x \in X\}$. Takve konfiguracije nastaju Schurovom konstrukcijom od netranzitivnih permutacijskih grupa. U slučaju $e = 0$, kad je dijagonala samo jedna relacija, kažemo da je koherentna konfiguracija* homogena. *Dokažite da iz komutativnosti ($p_{ij}^k = p_{ji}^k$) slijedi homogenost.*

Rješenje. Pretpostavimo da koherentna konfiguracija nije homogena, tj. postoji relacija R_0 koja sadrži par (a,a) i ne sadrži par (b,b) za neke $a, b \in X$. Relacija R_0 u uniji s još nekim relacijama daje dijagonalu $\{(x,x) \mid x \in X\}$, pa ne sadrži niti jedan par oblika (x,y) za $x \neq y$. Postoji relacija R_k koja sadrži par (a,b). Budući da je $a \neq b$, relacija R_k ne sadrži niti jedan par oblika (x,x). Promotrimo presječne brojeve $p_{0k}^k = |\{z \in X \mid (a,z) \in R_0, (z,b) \in R_k\}|$ i $p_{k0}^k = |\{z \in X \mid (a,z) \in R_k, (z,b) \in R_0\}|$. Iz $(a,z) \in R_0$ slijedi $z = a$, ali $(z,a) = (a,a) \notin R_k$ pa je $p_{0k}^k = 0$. S druge strane, iz $(z,b) \in R_0$ slijedi $z = b$. Par (a,b) jest u R_k i vrijedi $p_{k0}^k = 1$. Dakle, $p_{0k}^k \neq p_{k0}^k$ pa ova koherentna konfiguracija nije komutativna. □

Neka je sada G apstraktna grupa reda n (ne nužno grupa permutacija). Za elemente $g_1, g_2 \in G$ kažemo da su *konjugirani* ako postoji $h \in G$ takav da je $g_2 = h^{-1} g_1 h$. Konjugiranost je relacija ekvivalencije na G, a odgovarajuće klase ekvivalencije zovemo *klasama konjugacije* grupe G. U istoj klasi konjugacije su elementi koji se mogu preslikati unutrašnjim automorfizmom grupe G.

Primjer 1.42 (Klase konjugacije grupe)**.** *Neka je G grupa reda n, a $C_0 = \{1\}, C_1, \ldots, C_d$ njezine klase konjugacije. Definiramo relacije $R_i = \{(x,y) \in G \times G \mid y^{-1}x \in C_i\}$. Tako dobijemo koherentnu konfiguraciju reda n s d klasa koja je komutativna.*

Dokaz. Direktni produkt $G \times G$ djeluje na elemente grupe G na sljedeći način: $x^{(g,h)} = g^{-1}xh$. Vrijedi $x^{(g,h)} = x$, $\forall x \in G$ ako i samo ako je $g = h$ i $xg = gx$, $\forall x \in G$, tj. g je element iz centra $Z(G)$. Skup $N = \{(g,g) \mid g \in Z(G)\}$ je normalna podgrupa od $G \times G$. Kvocijent $(G \times G)/N$ možemo identificirati s grupom permutacija na G koja djeluje tranzitivno: za svaki izbor $x, y \in G$ uzmemo $(g, h) = (1, x^{-1}y)$ pa vrijedi $x^{(g,h)} = y$.

Tvrdimo da su relacije R_i definirane s pomoću klasa konjugacije upravo orbitale ove permutacijske grupe. Lako je provjeriti da su relacije invarijantne na djelovanje $G \times G$:

$$\begin{aligned}(x,y)^{(g,h)} \in R_i &\iff (g^{-1}xh, g^{-1}yh) \in R_i \iff h^{-1}y^{-1}xh \in C_i \\ &\iff y^{-1}x \in C_i \iff (x,y) \in R_i.\end{aligned}$$

Nadalje, ako su (x_1, y_1) i (x_2, y_2) parovi iz iste relacije R_i, tj. $y_1^{-1}x_1$ i $y_2^{-1}x_2$ elementi iz iste klase konjugacije C_i, onda postoji h takav da je $h^{-1}y_1^{-1}x_1h = y_2^{-1}x_2$. Ako stavimo $g = x_1hx_2^{-1}$, vidimo da vrijedi $(x_1, y_1)^{(g,h)} = (x_2, y_2)$. Dakle, relacije R_i čine koherentnu konfiguraciju jer nastaju Schurovom konstrukcijom 1.36 od tranzitivne permutacijske grupe.

Da bismo provjerili komutativnost, uzmimo par $(x, y) \in R_k$ i označimo $a = y^{-1}x \in C_k$. Presječni broj p_{ij}^k je broj elemenata $z \in G$ takvih da je $(x, z) \in R_i$, $(z, y) \in R_j$, tj. $z^{-1}x \in C_i$, $y^{-1}z \in C_j$. Prvi uvjet ekvivalentan je sa $z \in xC_i^{-1}$, a drugi sa $z \in yC_j$. Zato vrijedi $p_{ij}^k = |xC_i^{-1} \cap yC_j| = |y(y^{-1}xC_i^{-1} \cap C_j)| = |aC_i^{-1} \cap C_j|$. Koristili smo da za bilo kojo podskup $Y \subseteq G$ i element $g \in G$ vrijedi $|Y| = |gY|$, zbog bijektivnosti pridruživanja $x \mapsto gx$. Na isti način vidimo da je $p_{ji}^k = |aC_j^{-1} \cap C_i|$, a to dalje transformiramo koristeći $|Y| = |Y^{-1}|$ u $p_{ji}^k = |(aC_j^{-1} \cap C_i)^{-1}| = |C_ja^{-1} \cap C_i^{-1}| = |aC_ja^{-1} \cap aC_i^{-1}|$. Budući da je C_j klasa konjugacije, $aC_ja^{-1} = C_j$ i zadnji izraz je jednak $|aC_i^{-1} \cap C_j|$. Dakle, vrijedi komutativnost $p_{ij}^k = p_{ji}^k$. □

Asocijacijska shema na slici 3 nastaje od klasa konjugacije Kleinove[14] četvorne grupe $\mathbb{Z}_2 \times \mathbb{Z}_2$. Općenito, relacije definirane klasama konjugacije ne moraju biti simetrične. Na primjer, koherentna konfiguracija klasa konjugacije cikličke grupe $\mathbb{Z}_n$ za $n \geq 3$ nije asocijacijska shema.

Zadatak 1.43. *Koliko klasa konjugacije ima komutativna grupa reda n? Koliko ih ima simetrična grupa S_n?*

Rješenje. Elementi komutativne grupe su konjugirani samo ako se podudaraju. Klase konjugacije su jednočlane i ima ih n. Permutacije $\pi_1, \pi_2 \in S_n$ su konjugirane ako i samo ako su istog cikličkog tipa (dokažite!). Ciklički tip je multiskup duljina ciklusa u prikazu permutacije kao produkta disjunktinih ciklusa (računajući i cikluse duljine 1, tj. fiksne točke permutacije). Možemo ga identificirati s particijom prirodnog broja n, pa je broj klasa konjugacije od S_n jednak broju particija od n. □

[14]Christian Felix Klein (1849.-1925.), njemački matematičar.

Zadatak 1.44. *Pod kojim uvjetom na grupu G njezine klase konjugacije čine asocijacijsku shemu, tj. simetričnu koherentnu konfiguraciju?*

Rješenje. Simetričnost vrijedi ako i samo ako su klase konjugacije zatvorene na invertiranje, tj. ako je svaki element grupe konjugiran svojem inverzu. Takve grupe zovemo *ambivalentnim.* U grupi $\mathbb{Z}_2 \times \mathbb{Z}_2$ svaki element je jednak svojem inverzu, kao i u svakoj elementarno Abelovoj 2-grupi, pa su to primjeri ambivalentnih grupa. Za konačne grupe ambivalentnost je ekvivalentna uvjetu da svaki karakter grupe nad poljem $\mathbb{C}$ poprima realne vrijednosti. □

Multiplikativna grupa konačnog polja $\mathbb{F}_q^*$ je ciklička reda $q-1$. Njezini generatori su *primivni elementi* polja. Ako je $\omega \in \mathbb{F}_q^*$ primitivni element i $q-1 = r \cdot d$, onda je $H = \langle \omega^d \rangle$ podgrupa od $\mathbb{F}_q^*$ reda r. Susjedne klase $C_i = \omega^{i-1}H$, $i = 1, \ldots, d$ zovemo *klasama ciklotomije* konačnog polja.

Primjer 1.45 (Klase ciklotomije konačnog polja)**.** *Neka je $C_0 = \{0\}$, a $C_1, \ldots, C_d$ klase ciklotomije polja $\mathbb{F}_q$. Definiramo relacije $R_i = \{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q \mid x - y \in C_i\}$. Tako dobijemo koherentnu konfiguraciju reda q s d klasa koja je komutativna.*

Dokaz. Pokažimo da i ovaj primjer nastaje Schurovom konstrukcijom od tranzitivne permutacijske grupe. Neka je G skup svih funkcija s $\mathbb{F}_q$ na sebe zadanih formulom $x^g = ax+b$, za $a \in H$ i $b \in \mathbb{F}_q$. To je podgrupa od $\mathrm{Sym}(\mathbb{F}_q)$ koja djeluje tranzitivno. Lako je provjeriti da su orbitale upravo relacije R_i definirane u primjeru. Za komutativnost pokažemo $p_{ij}^k = |(-C_i+x) \cap (C_j+y)|$, za $x - y \in C_k$, i iskoristimo da za bilo koji podskup $Y \subseteq \mathbb{F}_q$ i element $b \in \mathbb{F}_q$ vrijedi $|Y| = |Y+b| = |-Y|$. □

2 Bose-Mesnerove algebre

U ovom poglavlju za skup vrhova uzimamo $X = \{1, \ldots, n\}$. Relacije $R_0, \ldots, R_d$ od kojih se sastoji koherentna konfiguracija shvaćamo kao $n \times n$ matrice $A_0, \ldots, A_d$:

$$A_i = [a_{xy}^{(i)}], \quad a_{xy}^{(i)} = \begin{cases} 1, & \text{ako je } (x,y) \in R_i, \\ 0, & \text{inače,} \end{cases} \qquad \text{za } i = 0, \ldots, d.$$

U simetričnom slučaju to su matrice susjedstva grafova $G_0, \ldots, G_d$ od kojih se sastoji asocijacijska shema. Ako s I označimo jediničnu matricu, a s J matricu kojoj su svi unosi jedinice, definicijska svojstva koherentne konfiguracije možemo iskazati na sljedeći način.

Definicija 2.1. Koherentna konfiguracija *reda n s d klasa sastoji se od matrica $A_0, \ldots, A_d \in M_n(\mathbb{C})$ popunjenih nulama i jedinicama tako da vrijedi:*

1. $A_0 = I$,
2. $\sum_{i=0}^{d} A_i = J$,
3. *za svaki indeks i postoji indeks i' takav da je $A_i^t = A_{i'}$,*
4. *za svaki izbor indeksa i, j produkt matrica $A_i A_j$ je linearna kombinacija od $A_0, \ldots, A_d$.*

Jasno je da prva tri svojstva odgovaraju svojstvima iz definicije 1.38. Za 4. svojstvo promotrimo kombinatornu interpretaciju elementa na mjestu (x, y) u produktu $A_i A_j$:

$$\sum_{z=1}^{n} a_{xz}^{(i)} a_{zy}^{(j)} = |\{z \mid a_{xz}^{(i)} = 1,\ a_{zy}^{(j)} = 1\}|.$$

Elementi matrica A_i, A_j su nule i jedinice, pa je ova suma broj iz $\mathbb{N}_0$. Jednaka je broju vrhova z takvih da je $a_{xz}^{(i)} = 1$, $a_{zy}^{(j)} = 1$, odnosno $(x, z) \in R_i$, $(z, y) \in R_j$. Ako je $(x, y) \in R_k$, to je upravo presječni broj p_{ij}^k. Dakle, element na mjestu (x, y) produkta $A_i A_j$ podudara se s odgovarajućim elementom linearne kombinacije $\sum_{k=0}^{d} p_{ij}^k A_k$. Uvjet 4. možemo zapisati kao

4. postoje $p_{ij}^k \in \mathbb{N}_0$ takvi da je $A_i A_j = \sum_{k=0}^{d} p_{ij}^k A_k$ za sve indekse i, j.

Sada je jasno da je ovo svojstvo ekvivalentno 4. svojstvu iz definicije 1.38. Štoviše, uvjet komutativnosti $p_{ij}^k = p_{ji}^k$ ekvivalentan komutiranju matrica

($A_iA_j = A_jA_i$), a uvjet simetričnosti ekvivalentan je simetričnosti matrica ($A_i^t = A_i$).

Promotrimo potprostor $\mathcal{A} = \langle A_0, \ldots, A_d \rangle$ od $M_n(\mathbb{C})$ razapet matricama koherentne konfiguracije nad poljem $\mathbb{C}$. Uz implicitnu pretpostavku $A_i \neq 0$ (relacije su neprazne), matrice su linearno nezavisne i $\dim \mathcal{A} = d+1$. Budući da su po 4. svojstvu produkti baznih matrica u $\mathcal{A}$, potprostor je zatvoren i na matrično množenje. Dakle, $\mathcal{A}$ je podalgebra algebre matrica $M_n(\mathbb{C})$ koju zovemo *algebrom koherentne konfiguracije* (u knjizi [4] koristi se naziv *algebra susjedstva*, eng. *adjacency algebra*). Uvjet komutativnosti znači da bazne matrice komutiraju, a u tom slučaju sve matrice iz $\mathcal{A}$ komutiraju. Tada je $\mathcal{A}$ komutativna algebra koju zovemo *Bose-Mesnerovom algebrom koherentne konfiguracije*.

Iz definicije 2.1 direktno slijede ova svostva algebre $\mathcal{A}$:

1. $I \in \mathcal{A}$,

2. $J \in \mathcal{A}$,

3. zatvorenost na transponiranje: $A \in \mathcal{A} \Rightarrow A^t \in \mathcal{A}$.

Osim toga sve matrice iz $\mathcal{A}$ imaju konstantne dijagonale, jer nastaju kao linearne kombinacije matrice I i matrica koje na dijagonali imaju nule.

Uvedimo sada još jednu operaciju na $M_n(\mathbb{C})$, množenje po komponentama: $A \circ B = [a_{ij}b_{ij}]$ za $A = [a_{ij}]$ i $B = [b_{ij}]$. To je *Schurov* ili *Hadamardov*[15] *produkt* matrica, koji Chris Godsil [54] zove "*bad student's product*". Operacija je asocijativna, komutativna i bilinearna: $(A \circ B) \circ C = A \circ (B \circ C)$, $A \circ B = B \circ A$, $(\alpha A + \beta B) \circ C = \alpha A \circ C + \beta B \circ C$. Neutralni element za Schurovo množenje je matrica J. Dakle, $(M_n(\mathbb{C}), +, \circ)$ je komutativna algebra s jedinicom J, dok je $(M_n(\mathbb{C}), +, \cdot)$ samo algebra s jedinicom I jer standardno matrično množenje nije komutativno.

Primijetimo da je algebra koherentne konfiguracije $\mathcal{A}$ zatvorena i na Schurovo množenje. Naime, bazne matrice A_i su idempotentne ($A_i \circ A_i = A_i$) jer sadrže samo nule i jedinice. Za $i \neq j$ produkt $A_i \circ A_j$ je nulmatrica, zbog 2. svojstva iz definicije 2.1. Dakle, vrijedi $A_i \circ A_j = \delta_{ij} A_i$ iz čega slijedi da je $(\mathcal{A}, +, \circ)$ komutativna algebra s jedinicom.

Definicija 2.2. *Za potprostor $\mathcal{A} \leq M_n(\mathbb{C})$ kažemo da je* koherentna algebra *ako sadrži I, J, zatvoren je na transponiranje, matrično množenje i Schurovo množenje te sve matrice iz $\mathcal{A}$ imaju konstantne dijagonale.*

Kasnije ćemo vidjeti da svaka koherentna algebra ima jedinstvenu bazu sastavljenu od 0-1 matrica koje zadovoljavaju uvjete iz definicije 2.1. Dakle,

[15] Jacques Salomon Hadamard (1865.-1963.), francuski matematičar.

svaka koherentna algebra razapeta je matricama koherentne konfiguracije. Uvjet da matrice imaju konstantne dijagonale odgovara homogenosti. Bez tog uvjeta koherentne algebre odgovarale bi općenitijim koherentnim konfiguracijama, kao u zadatku 1.41.

2.1 Centralizatorska algebra permutacijske grupe

Elemente permutacijske grupe $g \in G \leq S_n$ možemo reprezentirati permutacijskim matricama $P(g)$:

$$P(g) = [p_{xy}], \quad p_{xy} = \begin{cases} 1, & \text{ako je } x^g = y, \\ 0, & \text{inače.} \end{cases}$$

Preslikavanje $P : G \to GL(n, \mathbb{C})$ je homomorfizam grupa: $P(gh) = P(g)P(h)$ i $P(g^{-1}) = P(g)^{-1}$. Takvi homomorfizmi proučavaju se u teoriji reprezentacija. *Centralizatorska algebra* $C(G)$ je skup svih matrica $A \in M_n(\mathbb{C})$ koje komutiraju sa svim matricama $P(g)$, $g \in G$.

Propozicija 2.3. *$C(G)$ sadrži I, J i zatvorena je na linearne kombinacije, transponiranje, matrično množenje i Schurovo množenje. Ako je G tranzitivna, onda matrice u $C(G)$ imaju konstantne dijagonale.*

Dokaz. Zatvorenost $C(G)$ na transponiranje vrijedi jer su permutacijske matrice ortogonalne: $P(g)^t = P(g)^{-1}$. Ovako se provjeri zatvorenost na Schurov produkt:

$$P(g)(A \circ B) = (P(g)A) \circ (P(g)B) = (AP(g)) \circ (BP(g)) = (A \circ B)P(g).$$

"Distributivnost" standardnog i Schurovog množenja $P(A \circ B) = (PA) \circ (PB)$ i $(A \circ B)P = (AP) \circ (BP)$ vrijedi za sve permutacijske matrice P. Ako je $A = [a_{xy}]$ i vrijedi $x^g = y$, matrica $P(g)A$ na mjestu (x, y) ima element a_{yy}, a matrica $AP(g)$ na tom mjestu ima a_{xx}. Zato iz tranzitivnosti i $A \in C(G)$ slijedi konstantnost dijagonale: $a_{xx} = a_{yy}$, $\forall x, y \in \{1, \ldots, n\}$. Ostale tvrdnje lako je provjeriti. □

Uzmimo matricu $A = [a_{xy}]$ i promotrimo element matrice $P(g)AP(g^{-1})$ na mjestu (x, y). Matrica $P(g)A$ ima elemente $\sum_z p_{xz} a_{zy} = a_{x^g y}$, jer $p_{xz} = 1$ za $z = x^g$, a inače je $p_{xz} = 0$. Slično vidimo da $AP(g^{-1})$ na mjestu (x, y) ima element a_{xy^g}. Dakle, $P(g)AP(g^{-1})$ na mjestu (x, y) ima $a_{x^g y^g}$. Matrica A komutira s $P(g)$ ako i samo ako je $P(g)AP(g^{-1}) = A$. Zaključujemo da je A iz centralizatorske algebre ako i samo ako vrijedi $a_{x^g y^g} = a_{xy}$ za svaki $g \in G$, tj. A je konstantna na orbitalama grupe G (parovima indeksa koje G preslikava jedne u druge). Time smo dokazali sljedeću propoziciju.

Propozicija 2.4. *Centralizatorska algebra $C(G)$ podudara se s algebrom koherentne konfiguracije dobivene Schurovom konstrukcijom od G (kao u primjeru 1.36).*

Rang od G (broj orbitala) je dimenzija centralizatorske algebre, odnosno broj klasa koherentne konfiguracije uvećan za 1 (zato što "dijagonalu" R_0 ne brojimo kao klasu).

2.2 Schurove idempotente

U prethodnoj cjelini vidjeli smo da centralizatorska algebra ima bazu sastavljenu od 0-1 matrica koje čine koherentnu konfiguraciju. Sada ćemo proširiti taj rezultat na proizvoljnu koherentnu algebru, tj. svaki potprostor $\mathscr{A} \leq M_n(\mathbb{C})$ koji sadrži I, J, zatvoren je na transponiranje, množenje, Schurovo množenje i matrice iz $\mathscr{A}$ imaju konstantne dijagonale (definicija 2.2).

Lema 2.5. *Neka je $\mathscr{A} \leq M_n(\mathbb{C})$ potprostor koji je zatvoren na Schurovo množenje. Onda postoji baza $\{A_0, \ldots, A_d\}$ od $\mathscr{A}$ takva da vrijedi*

$$A_i \circ A_j = \delta_{ij} A_i. \tag{1}$$

Baza s tim svojstvom je jedinstvena do na poredak matrica.

Dokaz. Nosač (eng. *support*) matrice $A = [a_{ij}]$ je skup $\operatorname{supp} A = \{(i,j) \mid a_{ij} \neq 0\}$. Za $\alpha \in \mathbb{C}$, $\alpha \neq 0$ vrijedi $\operatorname{supp}(\alpha A) = \operatorname{supp} A$, $\operatorname{supp}(A \circ B) = \operatorname{supp} A \cap \operatorname{supp} B$ i $\operatorname{supp}(A \circ A) = \operatorname{supp} A$. Za matricu $A \in \mathscr{A}$ kažemo da je *minimalna* ako je $A \neq 0$ i ne postoji matrica $B \in \mathscr{A}$, $B \neq 0$ takva da je $\operatorname{supp} B \subset \operatorname{supp} A$. Ako je $A \in \mathscr{A}$ minimalna, onda za svaku matricu $B \in \mathscr{A}$ vrijedi $\operatorname{supp} A \subseteq \operatorname{supp} B$ ili $\operatorname{supp} A \cap \operatorname{supp} B = \emptyset$. Ako su $A, B \in \mathscr{A}$ minimalne i $\operatorname{supp} A = \operatorname{supp} B$, onda je $B = \alpha A$ za neki $\alpha \neq 0$. U suprotnom mogli bismo linearnom kombinacijom $\alpha A + \beta B$ poništiti neki, ali ne sve elemente iz zajedničkog nosača od A i B, što je kontradikcija s minimalnosti. Iz toga slijedi da su svi nenul elementi minimalne matrice $A \in \mathscr{A}$ jednaki. Naime, matrica $A \circ A$ je također minimalna i nosač joj se podudara s A, pa iz $A \circ A = \alpha A$ slijedi da su nenul elementi od A svi jednaki α.

Dakle, minimalnu matricu možemo *normalizirati*, tj. pomnožiti skalarom tako joj svi nenul elementi budu 1. Neka je $\{A_0, \ldots, A_d\}$ skup svih normaliziranih minimalnih matrica iz $\mathscr{A}$. Taj skup očito zadovoljava relacije (1), iz čega slijedi linearna nezavisnost. Za proizvoljnu matricu $A \in \mathscr{A}$ matrica $A \circ A_i$ je nulmatrica ili je minimalna matrica s istim nosačem kao A_i. U prvom slučaju stavimo $\alpha_i = 0$, a u drugom slučaju postoji $\alpha_i \neq 0$ takav da je $A \circ A_i = \alpha_i A_i$. Tada vrijedi $A = \sum_{i=0}^{d} \alpha_i A_i$, pa je $\{A_0, \ldots, A_d\}$ baza od $\mathscr{A}$.

Uzmimo bilo koju bazu od $\mathscr{A}$ koja zadovoljava relaciju (1). Jedinstvenost vrijedi zato što bazne matrice moraju biti normalizirane (zbog $A_i \circ A_i = A_i$) i minimalne. Kad bi postojala matrica $A \in \mathscr{A}$, $A \neq 0$ takva da je $\operatorname{supp} A \subset \operatorname{supp} A_i$, onda je ne bismo mogli prikazati kao linearnu kombinaciju od $A_0, \ldots, A_d$. □

Matrice koje zadovoljavaju relaciju (1) zovemo *Schurovim idempotentama*. Po lemi 2.5, koherentna algebra $\mathscr{A}$ ima jedinstvenu bazu $\{A_0, \ldots, A_d\}$ sastavljenu od Schurovih idempotenta. Pokažimo da je ta baza koherentna konfiguracija u smislu definicije 2.1.

Zbog idempotentnosti ($A_i \circ A_i = A_i$) elementi matrica A_i su nule i jedinice. Zbog $I \in \mathscr{A}$ i pretpostavke da matrice u $\mathscr{A}$ imaju konstantne dijagonale, jedinična matrica I je jedna od Schurovih idempotenta. Možemo pretpostaviti $A_0 = I$, pa vrijedi svojstvo 1. iz definicije 2.1. Slično, zbog ortogonalnosti ($A_i \circ A_j = 0$ za $i \neq j$) i $J \in \mathscr{A}$ slijedi svojstvo 2. iz definicije 2.1. Zbog zatvorenosti na transponiranje, $\{A_0^t, \ldots, A_d^t\}$ je baza od $\mathscr{A}$. Ta baza također zadovoljava relaciju (1): $A_i^t \circ A_j^t = (A_i \circ A_j)^t = \delta_{ij} A_i^t$. Svojstvo 3. sada slijedi iz jedinstvenosti u lemi 2.5. Konačno, svojstvo 4. slijedi direktno iz zatvorenosti $\mathscr{A}$ na matrično množenje. Time smo dokazali:

Teorem 2.6. *Svaka koherentna algebra $\mathscr{A}$ ima jedinstvenu bazu $\{A_0, \ldots, A_d\}$ sastavljenu od Schurovih idempotenta. Ta baza je koherentna konfiguracija u smislu definicije 2.1.*

U knjizi [4] teorem je dokazan na drugi način. Preuzeli smo dokaz iz skripte [124], a u skripti [55] dan je sličan dokaz u općenitijem kontekstu. Neka je $\mathscr{A} \leq M_n(\mathbb{C})$ potprostor kompleksnih $n \times n$ matrica i $\star$ binarna operacija takva da je $(\mathscr{A}, \star)$ komutativna i asocijativna algebra s jedinicom E. Operacija $\star$ može biti Schurov produkt (u tom slučaju je $E = J$), ali može biti i standardno množenje matrica na nekom potprostoru matrica koje komutiraju (za $E = I$) ili neka druga operacija. Matrice koje zadovoljavaju $A \star A = A$ zovemo *idempotentama*. Ako za idempotente vrijedi $A \star B = 0$, kažemo da su *ortogonalne*. Na skupu svih idempotenta definiramo parcijalni uređaj: $A \leq B$ ako je $A \star B = A$. *Minimalna idempotenta* je minimalni element u parcijalno uređenom skupu svih idempotenta različitih od 0. Ako su A i B idempotente, onda je $A \star B \leq A$ i $A \star B \leq B$. Iz toga slijedi da su minimalne idempotente ortogonalne, ako su različite. Potenciranje u algebri $(\mathscr{A}, \star)$ označavamo $A^{\star k} = A \star \ldots \star A$ (k faktora), uz $A^{\star 0} = E$.

U slučaju kad je operacija $\star$ Schurov produkt, idempotente su 0-1 matrice. Ortogonalnost znači da nemaju jedinice na istim mjestima, a parcijalni uređaj definiran s pomoću operacije podudara se s parcijalnim uređajem kojeg smo koristili u dokazu leme 2.5. Naime, $A \circ B = A$ vrijedi ako i samo ako je $\operatorname{supp} A \subseteq \operatorname{supp} B$.

Promotrimo sada slučaj kad je $\mathcal{A}$ neki potprostor matrica koje komutiraju, a operacija $\star$ standardno množenje matrica. Označimo s $\operatorname{Im} A = \{Ax \mid x \in \mathbb{C}^n\}$ *sliku* matrice A, tj. potprostor od $\mathbb{C}^n$ razapet stupcima od A. Neka je $\operatorname{Ker} A = \{x \in \mathbb{C}^n \mid Ax = 0\}$ *jezgra* matrice A. Ako je A idempotenta, onda za $x \in \operatorname{Im} A$ vrijedi $Ax = x$. Iz toga slijedi $\operatorname{Im} A \cap \operatorname{Ker} A = \{0\}$, pa je A matrica linearnog operatora projekcije na potprostor $\operatorname{Im} A$ duž potprostora $\operatorname{Ker} A$. Slijedi da su svojstvene vrijednosti od A samo nule i jedinice. Matrica A može se dijagonalizirati, a trag joj se podudara s rangom. Vrijedi $A \le B$, odnosno $AB = A$ ako i samo ako je $\operatorname{Im} A \le \operatorname{Im} B$. Ortogonalnost $AB = 0$ znači da je $\operatorname{Im} B \le \operatorname{Ker} A$ i $\operatorname{Im} A \le \operatorname{Ker} B$ (zbog komutativnosti).

Teorem 2.7. *Neka je $(\mathcal{A}, \star)$ komutativna i asocijativna algebra kvadratnih matrica nad $\mathbb{C}$ s jedinicom E. Ako u $\mathcal{A}$ nema nilpotentnih elemenata osim 0 (tj. vrijedi $N^{\star k} = 0 \Rightarrow N = 0$), onda $\mathcal{A}$ ima bazu sastavljenu od međusobno ortogonalnih idempotenta. Ta baza je jedinstvena do na poredak matrica.*

Dokaz. Prvo pokažimo da je svaki element $A \in \mathcal{A}$ linearna kombinacija međusobno ortogonalnih idempotenta. Neka je $m \in \mathbb{N}$ najmanji broj takav da su matrice $A^{\star 0}, \ldots, A^{\star m}$ linearno zavisne. Onda postoje $\alpha_0, \ldots, \alpha_{m-1} \in \mathbb{C}$ takvi da je $A^{\star m} + \alpha_{m-1} A^{\star(m-1)} + \ldots + \alpha_1 A + \alpha_0 E = 0$, a $\psi(t) = t^m + \alpha_{m-1} t^{m-1} + \ldots + \alpha_1 t + \alpha_0$ je *minimalni polinom* matrice A. Rastavimo ga na linearne faktore

$$\psi(t) = \prod_{i=1}^{k} (t - \theta_i)^{m_i}, \qquad \sum_{i=1}^{k} m_i = m$$

i neka je

$$\psi_i(t) = \frac{\psi(t)}{(t - \theta_i)^{m_i}}.$$

Polinomi $\psi_1, \ldots, \psi_k$ su relativno prosti ($M(\psi_1, \ldots, \psi_k) = 1$), pa postoje polinomi $f_1, \ldots, f_k \in \mathbb{C}[t]$ takvi da je $\sum_{i=1}^{k} f_i(t)\psi_i(t) = 1$. Slijedi

$$\sum_{i=1}^{k} f_i(A) \star \psi_i(A) = E. \tag{2}$$

Za $i \ne j$ polinom ψ dijeli $\psi_i \psi_j$, pa je $\psi_i(A) \star \psi_j(A) = 0$. Ako pomnožimo obje strane (2) s $f_i(A) \star \psi_i(A)$, dobijemo

$$(f_i(A) \star \psi_i(A))^2 = f_i(A) \star \psi_i(A).$$

Prema tome, matrice $A_i = f_i(A) \star \psi_i(A)$ su međusobno ortogonalne idempotente, a jednadžbu (2) možemo zapisati kao

$$A_1 + \ldots + A_k = E. \tag{3}$$

Polinom $\psi(t)$ dijeli $(t-\theta_i)^{m_i} f_i(t)\psi_i(t)$, pa je

$$(A - \theta_i E)^{\star m_i} \star A_i = 0 \Rightarrow [(A - \theta_i E) \star A_i]^{\star m_i} = 0.$$

Iz pretpostavke da nema nilpotentnih elemenata slijedi $(A - \theta_i E) \star A_i = 0$, tj. $A \star A_i = \theta_i A_i$. Množenjem (3) s A dobijemo

$$A = A \star A_1 + \ldots + A \star A_k = \theta_1 A_1 + \ldots + \theta_k A_k.$$

Time smo prikazali A kao linearnu kombinaciju međusobno ortogonalnih idempotenta.

Idući korak je dokazati postojanje minimalnih idempotenta. Ako je $\star$ Schurov produkt, to vrijedi jer matrice imaju konačne nosače. Ako je $\star$ standardno matrično množenje, iz $BA = A$ i $A \neq B$ slijedi da je $\operatorname{Im} A$ pravi potprostor od $\operatorname{Im} B$. Stoga niz $A_1 \leq \cdots \leq A_m$ različitih idempotenta može biti duljine najviše $m = n + 1$. Čini mi se da Godsil u [55, teorem 1.4.1] koristi taj argument u općem slučaju, ali ne znam zašto vrijedi za proizvoljnu operaciju $\star$. U algebrama koje nas zanimaju, $(\mathscr{A}, \circ)$ i $(\mathscr{A}, \cdot)$, minimalne idempotente postoje jer su strogo padajući nizovi idempotenta konačni.

Zatim dokazujemo da svaku idempotentu možemo prikazati kao sumu minimalnih idempotenta. Neka je A minimalna idempotenta, a B idempotenta. Ako je $A \star B \neq 0$, onda je $A \star B \leq A$ pa zbog minimalnosti slijedi $A \star B = A$. Iz toga također slijedi ortogonalnost različitih minimalnih idempotenta. Neka je sada B bilo koja idempotenta, a B_0 suma svih minimalnih idempotenta A takvih da je $A \leq B$. Tada je B_0 idempotenta, kao suma međusobno ortogonalnih minimalnih idempotenta. Ako je $B \neq B_0$, na sličan način vidimo da je $B - B_0$ idempotenta. No tada postoji minimalna idempotenta $A \leq B - B_0$, što je kontradikcija s definicijom matrice B_0. Dakle, svaka idempotenta je suma minimalnih idempotenta, a svaka matrica iz $\mathscr{A}$ je linearna kombinacija idempotenta. Zaključujemo da je $\mathscr{A}$ razapet minimalnim idempotentama. Skup svih minimalnih idempotenta je konačan, jer je linearno nezavisan, i čini bazu od $\mathscr{A}$.

Preostaje dokazati jedinstvenost. Neka je $\{A_0, \ldots, A_d\}$ bilo koja baza sastavljena od međusobno ortogonalnih idempotenta, takva da vrijedi $A_i \star A_j = \delta_{ij} A_i$. Dokazujemo da se sastoji od minimalnih idempotenta, što znači da se podudara s bazom koju smo konstruirali. Pretpostavimo da je A idempotenta za koju vrijedi $A \leq A_i$, odnosno $A \star A_i = A$. Tvrdimo da je tada

$A = 0$ ili $A = A_i$, što znači da je A_i minimalna. Raspišimo A u bazi: $A = \sum_{i=0}^{d} \alpha_i A_i$. Množenjem s A_i vidimo da je $A = \alpha_i A_i$. Zbog idempotentnosti od A i A_i slijedi $\alpha_i A_i = A = A \star A = (\alpha_i A_i) \star (\alpha_i A_i) = \alpha_i^2 A_i$. Dakle, $\alpha_i = \alpha_i^2$, tj. $\alpha_i = 0$ ili $\alpha_i = 1$, tj. $A = 0$ ili $A = A_i$. Dokazali smo da su A_i minimalne idempotente i time je teorem dokazan. $\square$

Zadatak 2.8. *Dokažite da je u algebri $(\mathscr{A}, \star)$ uvjet $N^{\star k} = 0 \Rightarrow N = 0$ ekvivalentan uvjetu $N^{\star 2} = 0 \Rightarrow N = 0$.*

Schurovo množenje očito nema nilpotentnih elemenata osim nulmatrice, pa je lema 2.5 specijalni slučaj teorema 2.7. Važan rezultat iz linearne algebre kaže da se matrica može dijagonalizirati ako i samo ako je normalna. To je također posljedica teorema 2.7. Matrica A je *normalna* ako komutira s adjungiranom matricom: $AA^* = A^*A$. Zvjezdica znači adjungiranje, tj. transponiranje i konjugiranje: $A^* = \overline{A^t}$.

Zadatak 2.9. *Dokažite: ako je $N \in M_n(\mathbb{C})$ normalna i nilpotentna, onda je $N = 0$.*

Rješenje. Dokazat ćemo da za normalnu matricu iz $N^k = 0$ slijedi $N^{k-1} = 0$. Iz toga indukcijom slijedi $N = 0$. Matrica $M = N^{k-1}$ je normalna i vrijedi $M^2 = 0$ (jer je $2k - 2 \geq k$). Koristimo normu izvedenu iz standardnog skalarnog produkta na $\mathbb{C}^n$: $\|x\| = \sqrt{x^*x}$. Za proizvoljan vektor $x \in \mathbb{C}^n$ vrijedi $\|M^*Mx\|^2 = (M^*Mx)^*(M^*Mx) = x^*M^*MM^*Mx = x^*(M^*)^2M^2x = 0$. Dakle, $M^*M = 0$ iz čega slijedi $\|Mx\|^2 = (Mx)^*(Mx) = x^*M^*Mx = 0$ za svaki vektor x, tj. $M = 0$. $\square$

Teorem 2.10. *Ako je $A \in M_n(\mathbb{C})$ normalna, onda se može dijagonalizirati.*

Dokaz. Neka je $\mathscr{A}$ najmanja algebra koja sadrži I, A i A^*. Ona je komutativna i zatvorena na adjungiranje. To znači da su sve matrice u $\mathscr{A}$ normalne, a po prethodnom zadatku jedina normalna nilpotentna matrica je 0. Dakle, zadovoljene su pretpostavke teorema 2.7 i $\mathscr{A}$ ima bazu $\{E_0, \ldots, E_d\}$ sastavljenu od međusobno ortogonalnih idempotenta.

Tvrdimo da su matrice E_i hermitske: $E_i^* = E_i$. Skup $\{E_0^*, \ldots, E_d^*\}$ također je baza sastavljena od međusobno ortogonalnih idempotenta, pa se zbog jedinstvenosti u teoremu 2.7 podudara s bazom $\{E_0, \ldots, E_d\}$. Stoga je $E_i^* = E_{i'}$ za neki indeks i'. Primijetimo da je trag $\operatorname{tr}(M^*M)$ suma kvadrata apsolutnih vrijednosti elemenata matrice M i može biti nula samo za $M = 0$. Zbog ortogonalnosti je $\operatorname{tr}(E_{i'}E_i) = 0$ za $i' \neq i$, a E_i nije nulmatrica. Zaključujemo da je $i' = i$.

Matrica E_i je idempotenta obzirom na standardno matrično množenje. To znači da je E_i matrica projekcije na $\operatorname{Im} E_i$ duž $\operatorname{Ker} E_i$, a suma ta dva potprostora je direktna. Vidjeli smo da je E_i hermitska matrica, iz čega slijedi da je suma $\operatorname{Im} E_i \oplus \operatorname{Ker} E_i$ ortogonalna. Zaista, za $x \in \operatorname{Im} E_i$ i $y \in \operatorname{Ker} E_i$ vrijedi $E_i x = x$ i $E_i y = 0$, pa je njihov skalarni produkt $x^* y = (E_i x)^* y = x^* E_i^* y = x^* E_i y = x^* 0 = 0$. Ortogonalnost $E_i E_j = 0$ za $i \neq j$ znači da je $\operatorname{Im} E_i \leq \operatorname{Ker} E_j$ i $\operatorname{Im} E_j \leq \operatorname{Ker} E_i$, iz čega slijedi ortogonalnost sume potprostora $\operatorname{Im} E_0 \oplus \ldots \oplus \operatorname{Im} E_d$. Tvrdimo da je suma jednaka cijelom $\mathbb{C}^n$.

Jediničnu matricu možemo prikazati u bazi: $I = \alpha_0 E_0 + \ldots + \alpha_d E_d$. Množenjem s E_i vidimo da je $E_i = \alpha_i E_i$, iz čega slijedi $\alpha_i = 1$. Dakle, $I = E_0 + \ldots + E_d$ pa svaki vektor $x \in \mathbb{C}^n$ možemo prikazati kao $x = Ix = E_0 x + \ldots + E_d x$, pri čemu je $E_i x \in \operatorname{Im} E_i$. Time smo dokazali da vrijedi $\operatorname{Im} E_0 \oplus \ldots \oplus \operatorname{Im} E_d = \mathbb{C}^n$.

Ako prikažemo našu matricu u bazi: $A = \lambda_0 E_0 + \ldots + \lambda_d E_d$, vidimo da su λ_i svojstvene vrijednosti od A s pridruženim svojstvenim potprostorima $\operatorname{Im} E_i$. Izaberemo ortonormirane baze potprostora $\operatorname{Im} E_i$, pa je njihova unija ortonormirana baza za cijeli $\mathbb{C}^n$ u kojoj je matrica A dijagonalna. Dakle, matrica A je unitarno slična dijagonalnoj matrici. $\square$

Primjeri matrica koje se ne mogu dijagonalizirati su upravo nilpotentne matrice, npr. matrica koja ima jedinice na nekoj od dijagonala iznad glavne dijagonale, a svi ostali elementi su nule:

$$N = \begin{bmatrix} 0 & \cdots & 1 & \cdots & 0 \\ & \ddots & & \ddots & \vdots \\ & & \ddots & & 1 \\ & 0 & & \ddots & \vdots \\ & & & & 0 \end{bmatrix}.$$

Zbog $N^k = 0$ minimalni polinom je t^k i jedina svojstvena vrijednost te matrice je nula. Jedina dijagonalna matrica sa spektrom $\{0\}$ je nulmatrica, pa N nije slična dijagonalnoj matrici.

2.3 Primitivne idempotente

Neka je $\mathscr{A}$ koherentna algebra. Po definiciji 2.2 zatvorena je na transponiranje, a po teoremu 2.6 ima bazu sastavljenu od realnih matrica (točnije, 0-1 matrica) pa je zatvorena i na konjugiranje. Dakle, $\mathscr{A}$ je zatvorena na adjungiranje: za svaku matricu $A \in \mathscr{A}$ vrijedi $A^* \in \mathscr{A}$.

U ovoj cjelini i u nastavku pretpostavljamo da matrice iz $\mathscr{A}$ komutiraju: $AB = BA$, $\forall A, B \in \mathscr{A}$. Komutativne koherentne algebre nazivamo *Bose-Mesnerovim algebrama*. Ako su p_{ij}^k presječni brojevi koherentne konfiguracije koja razapinje $\mathscr{A}$, komutativnost je ekvivalentna uvjetu $p_{ij}^k = p_{ji}^k$. Zbog zatvorenosti na adjungiranje, matrice iz Bose-Mesnerove algebre $\mathscr{A}$ su normalne. Po teoremu 2.10 možemo ih dijagonalizirati, a zbog komutativnosti vrijedi i više: matrice iz $\mathscr{A}$ možemo simultano dijagonalizirati. To znači da postoji baza od $\mathbb{C}^n$ u kojoj su sve matrica iz $\mathscr{A}$ dijagonalne, tj. elementi baze su svojstveni vektori svih matrica iz $\mathscr{A}$. Dokažimo prvo direktno taj rezultat iz linearne algebre.

Lema 2.11. *Neka je $\mathscr{A} \subseteq M_n(\mathbb{C})$ skup matrica koje međusobno komutiraju. Onda postoji $x \in \mathbb{C}^n$, $x \neq 0$ koji je svojstveni vektor svih matrica iz $\mathscr{A}$.*

Dokaz. Prvo primijetimo da je tvrdnju dovoljno dokazati za potprostore od $M_n(\mathbb{C})$, jer ako matrice iz potprostora $\langle \mathscr{A} \rangle$ imaju zajednički svojstveni vektor, onda je on svojstveni vektor i za matrice iz $\mathscr{A}$. Zbog konačnodimenzionalnosti dovoljno je dokazati tvrdnju za konačne skupove matrica. Neka je $\{A_0, \ldots, A_d\}$ baza od $\langle \mathscr{A} \rangle$ i neka matrice baze imaju zajednički svojstveni vektor $x \in \mathbb{C}^n$, $x \neq 0$ takav da je $A_i x = \lambda_i x$ za $i = 0, \ldots, d$. Tada je x ujedno svojstve vektor njihove linearne kombinacije: $(\sum_{i=0}^{d} \alpha_i A_i)x = (\sum_{i=0}^{d} \alpha_i \lambda_i)x$.

Polje $\mathbb{C}$ je algebarski zatvoreno, pa matrica A_0 sigurno ima svojstvenu vrijednost $\lambda_0 \in \mathbb{C}$. Označimo s $E_{A_0}(\lambda_0) = \{x \in \mathbb{C}^n \mid A_0 x = \lambda_0 x\}$ odgovarajući svojstveni potprostor. Zbog komutativnosti taj potprostor je A_1-invarijantan: $x \in E_{A_0}(\lambda_0) \Rightarrow A_0 A_1 x = A_1 A_0 x = A_1(\lambda_0 x) = \lambda_0 A_1 x \Rightarrow A_1 x \in E_{A_0}(\lambda_0)$. Restringirani linearni operator $A_1 : E_{A_0}(\lambda_0) \to E_{A_0}(\lambda_0)$ ima svojstvenu vrijednost $\lambda_1 \in \mathbb{C}$, a odgovarajući svojstveni vektor je zajednički svojstveni vektor od A_0 i A_1. Sada promotrimo presjek svojsvenih potprostora $E_{A_0}(\lambda_0) \cap E_{A_1}(\lambda_1)$. On je A_2-invarijantan jer A_2 komutira s A_0 i A_1, pa restrikcijom dobijemo svojstvenu vrijednost λ_2 od A_2 i zajednički svojstveni vektor od A_0, A_1 i A_2. Iteriranjem dolazimo do zajedničkog svojstvenog vektora svih matrica $A_0, \ldots, A_d$. □

Lema 2.12. *Neka je $\mathscr{A} \subseteq M_n(\mathbb{C})$ skup matrica koji je zatvoren na adjungiranje i matrice iz $\mathscr{A}$ međusobno komutiraju. Onda se matrice iz $\mathscr{A}$ mogu simultano dijagonalizirati, tj. postoji baza od $\mathbb{C}^n$ kojoj su elementi svojstveni vektori svih matrica iz $\mathscr{A}$.*

Dokaz. Iz pretpostavke slijedi da su matrice iz $\mathscr{A}$ normalne, pa se pojedinačno mogu dijagonalizirati. Neka je V suma svih zajedničkih svojstvenih potprostora matrica iz $\mathscr{A}$. Želimo dokazati da je $V = \mathbb{C}^n$. Pretpostavimo suprotno, da je ortogonalni komplement $V^\perp = \{x \in \mathbb{C}^n \mid x^* y = 0, \forall y \in V\}$ netrivijalan. Potprostor V je po definiciji $\mathscr{A}$-invarijantan, a zbog pretpostavke o zatvorenosti na adjungiranje potprostor $V^\perp$ je također $\mathscr{A}$-invarijantan. Naime, za proizvoljne $x \in V^\perp$, $A \in \mathscr{A}$, $y \in V$ vrijedi $A^* \in \mathscr{A} \Rightarrow A^* y \in V \Rightarrow (Ax)^* y = x^* A^* y = 0$, pa je $Ax \in V^\perp$. Po prethodnoj lemi matrice iz $\mathscr{A}$ imaju zajednički svojstveni vektor u $V^\perp$. Taj vektor bi po definiciji trebao biti i u V, što je nemoguće. Iz dokaza je jasno da možemo naći ortonormiranu bazu od $\mathbb{C}^n$ u kojoj su matrice iz $\mathcal{A}$ dijagonalne. Drugim riječima, postoji unitarna matrica $U \in M_n(\mathbb{C})$ takva da je matrica U^*AU dijagonalna za svaku matricu $A \in \mathcal{A}$. □

Sada dokažimo analogon leme 2.5 za standardno matrično množenje.

Lema 2.13. *Neka je $\mathcal{A} \leq M_n(\mathbb{C})$ potprostor koji je zatvoren na matrično množenje i adjungiranje te matrice iz $\mathcal{A}$ međusobno komutiraju. Onda postoji baza $\{E_0, \ldots, E_d\}$ od $\mathcal{A}$ takva da vrijedi*

$$E_i E_j = \delta_{ij} E_i. \tag{4}$$

Baza s tim svojstvom je jedinstvena do na poredak matrica, a sadrži hermitske matrice, tj. vrijedi $E_i^* = E_i$ za $i = 0, \ldots, d$.

Dokaz. Zbog zatvorenosti na adjungiranje i komutativnosti, matrice iz $\mathcal{A}$ su normalne. Po zadatku 2.9, nulmatrica je jedina nilpotentna matrica u $\mathcal{A}$. Prema tome, egzistencija i jedinstvenost baze koja zadovoljava (4) slijedi iz teorema 2.7. Dokažimo ipak egzistenciju direktno, pomoću rezultata iz linearne algebre. Po prethodnoj lemi postoji regularna matrica U takva da je $U^{-1}\mathcal{A}U$ potprostor od $M_n(\mathbb{C})$ koji sadrži samo dijagonalne matrice. Za dijagonalne matrice A i B Schurov produkt i standardni matrični produkt se podudaraju: $AB = A \circ B$. Stoga je potprostor $U^{-1}\mathcal{A}U$ zatvoren na Schurovo množenje, pa po lemi 2.5 ima bazu $\{A_0, \ldots, A_d\}$ sastavljenu od Schurovih idempotenta. Stavimo $E_i = UA_iU^{-1}$, pa je $\{E_0, \ldots, E_d\}$ baza od $\mathcal{A}$ koja zadovoljava (4). Jedinstvenost takve baze slijedi isto kao u dokazu teorema 2.7, a činjenica da su matrice E_i hermitske isto kao u dokazu teorema 2.10. □

Matrice koje zadovoljavaju relaciju (4) zovemo *primitivnim idempotentama*. Dakle, prema lemi 2.13 Bose-Mesnerova algebra $\mathcal{A}$ ima drugu istaknutu bazu $\{E_0, \ldots, E_d\}$ sastavljenu od primitivnih idempotenta. Izvedimo svojstva te baze koja odgovaraju svojstvima baze Schurovih idempotenta, odnosno svojstvima iz definicije 2.1.

Kao prvo, po definiciji 2.2 vrijedi $J \in \mathcal{A}$. Primijetimo da je matrica $\frac{1}{n}J \in \mathcal{A}$ idempotentna obzirom na standardno množenje. Budući da je ranga 1, ta matrica je minimalna idempotenta. Zato se podudara s nekom od primitivnih idempotenta i možemo pretpostaviti da je $E_0 = \frac{1}{n}J$.

Drugo, vrijedi $I \in \mathcal{A}$ pa jediničnu matricu možemo prikazati u bazi primitivnih idempotenta: $I = \sum_{j=0}^{d} \alpha_j E_j$. Vrijedi

$$E_i = E_i I = E_i \sum_{j=0}^{d} \alpha_j E_j \stackrel{(4)}{=} \alpha_i E_i$$

iz čega slijedi $\alpha_i = 1$. Dakle, $E_0 + \ldots + E_d = I$.

Treće, primitivne idempotente su hermitske, pa vrijedi $E_i^t = \overline{E}_i$. Skup $\{E_0^t, \ldots, E_d^t\}$ je također baza od $\mathscr{A}$ i zadovoljava (4), pa se zbog jedinstvenosti podudara s bazom primitivnih idempotenta. Za svaki indeks i postoji indeks $\hat{\imath}$ takav da je $E_i^t = E_{\hat{\imath}} = \overline{E}_i$.

Četvrto, $\mathscr{A}$ je zatvorena na Schurovo množenje. Zato $E_i \circ E_j$ možemo prikazati u bazi primitivnih idempotenta, tj. postoje $\alpha_{ij}^k \in \mathbb{C}$ takvi da je $E_i \circ E_j = \sum_{k=0}^d \alpha_{ij}^k E_k$. Ako označimo $q_{ij}^k = n\,\alpha_{ij}^k$, vrijedi

$$E_i \circ E_j = \frac{1}{n} \sum_{k=0}^{d} q_{ij}^k E_k. \tag{5}$$

Time smo dokazali:

Teorem 2.14. *Bose-Mesnerova algebra $\mathscr{A}$ ima jedinstvenu bazu $\{E_0, \ldots, E_d\}$ sastavljenu od primitivnih idempotenta, koje zadovoljavaju* (4)*. Ta baza ima sljedeća svojstva:*

1. $E_0 = \frac{1}{n} J$,
2. $\sum_{i=0}^d E_i = I$,
3. *za svaki indeks i postoji indeks $\hat{\imath}$ takav da je $E_i^t = E_{\hat{\imath}} = \overline{E}_i$,*
4. *postoje $q_{ij}^k \in \mathbb{C}$ takvi da je $E_i \circ E_j = \frac{1}{n} \sum_{k=0}^d q_{ij}^k E_k$ za sve indekse i, j.*

Brojeve q_{ij}^k iz 4. svojstva zovemo *Kreinovim*[16] *parametrima* Bose-Mesnerove algebre, odnosno komutativne koherentne konfiguracije. Zbog komutativnosti Schurova produkta, oni uvijek zadovoljavaju $q_{ij}^k = q_{ji}^k$. Za razliku od presječnih brojeva p_{ij}^k, Kreinovi parametri nemaju kombinatornu interpretaciju i ne moraju biti prirodni niti cijeli brojevi. Vidjet ćemo da ipak ne mogu biti bilo koji elementi iz $\mathbb{C}$, nego su nenegativni realni brojevi. Uočimo dualnost između teorema 2.14 i teorema 2.6. Ako zamijenimo Schurov i matrični produkt te njihove neutralne elemente J i I, svojstva Schurovih idempotenta iz definicije 2.1 prelaze u svojstva primitivnih idempotenta iz teorema 2.14. Presječni brojevi p_{ij}^k prelaze u Kreinove parametre q_{ij}^k, uz odgovarajuću normalizaciju (dijeljenje s n).

Zadatak 2.15. *Iz 3. svojstva u definiciji 2.1 dobivamo involuciju $i \mapsto i'$ (permutaciju stupnja* 2*) na skupu svih indeksa* $\{0, \ldots, d\}$*. Dualno, iz 3. svojstva u teoremu 2.14 dobivamo involuciju $i \mapsto \hat{\imath}$. Dokažite da možemo numerirati*

[16] Marko Grigorovič Krein (1907.-1989.), sovjetski matematičar.

Schurove idempotente $A_0, \ldots, A_d$ i primitivne idempotente $E_0, \ldots, E_d$ tako da se te dvije involucije podudaraju, tj. da obje involucije imaju isti broj fiksnih točaka i transpozicija.

Proučimo sada pobliže svojstva presječnih brojeva i dualna svojstva Kreinovih parametara. Skup vrhova je $X = \{1, \ldots, n\}$, a relacije od kojih se sastoji komutativna koherentna konfiguracija su $R_0, \ldots, R_d$. Za $x \in X$ i $i \in \{0, \ldots, d\}$ označavamo $N_i(x) = \{z \in X \mid (x, z) \in R_i\}$. Tada je $N_{i'}(x) = \{z \in X \mid (z, x) \in R_i\}$ i kombinatorna interpretacija presječnih brojeva je $p_{ij}^k = |N_i(x) \cap N_{j'}(y)|$, za bilo koji par $(x, y) \in R_k$. *Stupanj* relacije R_i je $n_i = p_{ii'}^0 = |N_i(x)|$, za bilo koji vrh x.

Propozicija 2.16. *Stupnjevi koherentne konfiguracije zadovoljavaju*

1. $n_0 = 1$,
2. $n_0 + \ldots + n_d = n$,
3. $n_i = n_{i'}$.

Dokaz. Po definiciji je $n_0 = |N_0(x)| = |\{z \in X \mid (x, z) \in R_0\}|$. Zbog 1. svojstva u definiciji 1.38 postoji samo jedan takav vrh $z \in X$, naime $z = x$, pa je $n_0 = 1$. Slično, zbog 2. svojstva u definiciji 1.38 skupovi $N_0(x), \ldots, N_d(x)$ čine particiju od X, pa je $n_0 + \ldots + n_d = n$. Treća tvrdnja slijedi iz komutativnosti: $n_i = p_{ii'}^0 = p_{i'i}^0 = n_{i'}$, ali vrijedi i u koherentnim konfiguracijama koje nisu komutativne. Primijetimo da je n_i suma bilo kojeg retka matrice A_i. Zbog $A_i^t = A_{i'}$ slijedi da su sume stupaca od A_i jednake $n_{i'}$. Suma svih elemenata matrice A_i je $nn_i = nn_{i'}$, iz čega slijedi $n_i = n_{i'}$. □

Prva dva svojstva iz prethodne propozicije također možemo dokazati matrično, pomoću Schurovih idempotenta $A_0, \ldots, A_d$. Ako je $\mathbb{1} = (1, \ldots, 1)$ vektor iz $\mathbb{C}^n$ kojem su sve komponente jedinice, vrijedi $A_i \mathbb{1} = n_i \mathbb{1}$. Vidimo da je $\mathbb{1}$ svojstveni vektor od A_i pridružen svojstvenoj vrijednosti n_i. Iz $A_0 = I$ odmah slijedi $n_0 = 1$, a iz $A_0 + \ldots + A_d = J$ slijedi $n_0 + \ldots + n_d = n$.

Zadatak 2.17. *Za koherentnu konfiguraciju kažemo da je* tanka *(eng.* thin*) ako su svi stupnjevi jednaki* 1. *Zbog 2. tvrdnje propozicije 2.16, to je ekvivalentno s $n = d + 1$. Dokažite da sve tanke koherentne konfiguracije nastaju Schurovom konstrukcijom (primjer 1.36) od permutacijskih grupa koje djeluju strogo tranzitivno:* $(\forall x, y \in X)(\exists! g \in G)\ x^g = y$. *Dokažite da za strogo tranzitivne permutacijske grupe vrijedi: G je Abelova ako i samo ako je odgovarajuća Schurova koherentna konfiguracija komutativna. Nađite protuprimjer za tranzitivne grupe koje ne djeluju strogo i dokažite implikaciju koja vrijedi za sve tranzitivne permutacijske grupe.*

Rješenje. $G = \langle (1,2,3,4), (1,4)(2,3) \rangle$ je trazitivna permutacijska grupa stupnja 4 izomorfna diedralnoj grupi D_8, koja nije Abelova. Schur(G) ima dvije klase i simetrična je, dakle i komutativna. $H = \langle (1,2,3)(4,5,6), (1,4)(2,5) \rangle$ je tranzitivna permutacijska grupa stupnja 6 izomorfna alternirajućoj grupi A_4, koja nije Abelova. Schur(H) ima tri klase koje nisu simetrične, ali je komutativna. Implikacija G Abelova $\Rightarrow$ Schur(G) komutativna vrijedi za sve tranzitivne permutacijske grupe $G \leq S_n$. Naime, iz Abelovosti slijedi $|G| = n$, tj. stroga tranzitivnost od G. □

Postavlja se pitanje kako definirati parametre dualne stupnjevima koherentne konfiguracije $n_0, \ldots, n_d$? Dualiziranjem jednakosti $n_i = p_{ii'}^0$ dobivamo brojeve $m_i = q_{i\hat{i}}^0$, koje zovemo *kratnostima* koherentne konfiguracije. Da bismo odgonetnuli njihov smisao, uvedimo oznaku za sumu svih elemenata matrice $A = [a_{ij}] \in M_n(\mathbb{C})$:

$$\operatorname{sum} A = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij}.$$

Lema 2.18. *Za sve matrice $A, B, C \in M_n(\mathbb{C})$ vijedi*

$$\operatorname{sum}(A \circ B) = \operatorname{tr}(AB^t), \tag{6}$$

$$\begin{aligned} \operatorname{sum}(A \circ B \circ C) &= \operatorname{tr}((A \circ B)C^t) = \operatorname{tr}((B \circ C)A^t) = \operatorname{tr}((C \circ A)B^t) \\ &= \operatorname{tr}((A^t \circ B^t)C) = \operatorname{tr}((B^t \circ C^t)A) = \operatorname{tr}((C^t \circ A^t)B). \end{aligned} \tag{7}$$

Dokaz. Element na i-tom mjestu dijagonale matrice AB^t je $\sum_{j=1}^n a_{ij}b_{ij}$, pa joj je trag $\operatorname{sum}(A \circ B)$. Relacija (7) slijedi iz (6), komutativnosti Schurova produkta i svojstava $\operatorname{sum}(A) = \operatorname{sum}(A^t)$, $(A \circ B)^t = A^t \circ B^t$. □

Po definiciji Kreinovih parametara vrijedi $E_i \circ E_{\hat{i}} = \frac{1}{n} \sum_{k=0}^n q_{i\hat{i}}^k E_k$. Matričnim množenjem s $E_0 = \frac{1}{n}J$ slijedi

$$(E_i \circ E_{\hat{i}})E_0 = \frac{1}{n} q_{i\hat{i}}^0 E_0 \quad \Rightarrow \quad (E_i \circ E_{\hat{i}})J = \frac{1}{n} q_{i\hat{i}}^0 J.$$

Trag matrice na desnoj strani je $m_i = q_{i\hat{i}}^0$, a na lijevoj strani primjenom relacije (7) dobijemo

$$\operatorname{tr}((E_i \circ E_{\hat{i}})J) = \operatorname{tr}((J \circ E_i)E_{\hat{i}}^t) = \operatorname{tr}(E_i E_i) = \operatorname{tr}(E_i).$$

Dakle, kratnosti komutativne koherentne konfiguracije jednake su tragu primitivnih idempotenta, $m_i = \operatorname{tr}(E_i)$.

Propozicija 2.19. *Kratnosti komutativne koherentne konfiguracije zadovoljavaju*

1. $m_0 = 1$,
2. $m_0 + \ldots + m_d = n$,
3. $m_i = m_{\hat{i}}$.

Dokaz. Zbog 1. svojstva u teoremu 2.14 je $m_0 = \mathrm{tr}(E_0) = \mathrm{tr}(\frac{1}{n}J) = 1$. Slično, zbog 2. svojstva u teoremu 2.14 i linearnosti traga je $\sum_{i=0}^{d} m_i = \sum_{i=0}^{d} \mathrm{tr}(E_i) = \mathrm{tr}(\sum_{i=0}^{d} E_i) = \mathrm{tr}(I) = n$. Iz 3. svojstva slijedi $m_i = m_{\hat{i}}$, budući da matrice E_i i E_i^t imaju isti trag. $\square$

Presječne brojeve možemo na sljedeći način izraziti pomoću Schurovih idempotenta, a Kreinove parametre pomoću primitivnih idempotenta.

Lema 2.20. *Vrijedi*

$$p_{ij}^k = \frac{1}{n\, n_k} \mathrm{tr}(A_i A_j A_k^t), \tag{8}$$

$$q_{ij}^k = \frac{n}{m_k} \mathrm{tr}((E_i \circ E_j) E_k). \tag{9}$$

Dokaz. Osnovnu relaciju $A_i A_j = \sum_{k=0}^{n} p_{ij}^k A_k$ pomnožimo Schurovo s A_k i dobijemo $p_{ij}^k A_k = (A_i A_j) \circ A_k$. Zbrajanjem elemenata matrice slijedi $p_{ij}^k \,\mathrm{sum}\, A_k = p_{ij}^k\, n\, n_k = \mathrm{sum}((A_i A_j) \circ A_k) \overset{(6)}{=} \mathrm{tr}(A_i A_j A_k^t)$. Dualnu relaciju $E_i \circ E_j = \frac{1}{n} \sum_{k=0}^{n} q_{ij}^k E_k$ pomnožimo matrično s E_k i dobijemo $\frac{1}{n}\, q_{ij}^k E_k = (E_i \circ E_j) E_k$. Računanjem traga slijedi $\frac{1}{n}\, q_{ij}^k \,\mathrm{tr}\, E_k = \frac{m_k}{n}\, q_{ij}^k = \mathrm{tr}((E_i \circ E_j) E_k)$. $\square$

Korolar 2.21. *Kreinovi parametri su realni brojevi.*

Dokaz. Iz relacije (9) slijedi

$$\begin{aligned}
\overline{q_{ij}^k} &= \frac{n}{m_k} \mathrm{tr}((\overline{E}_i \circ \overline{E}_j) \overline{E}_k) = \frac{n}{m_k} \mathrm{tr}((E_i^t \circ E_j^t) E_k^t) = \frac{n}{m_k} \mathrm{tr}((E_i \circ E_j)^t E_k^t) \\
&= \frac{n}{m_k} \mathrm{tr}((E_k (E_i \circ E_j))^t) = \frac{n}{m_k} \mathrm{tr}(E_k (E_i \circ E_j)) = q_{ij}^k.
\end{aligned}$$

$\square$

Zadatak 2.22. *Pokažite primjerom da Kreinovi parametri ne moraju biti racionalni brojevi.*

Rješenje. Heawoodov graf (slika 7) je distancijsko regularan graf s 14 vrhova i presječnim nizom $\{3, 2, 2; 1, 1, 3\}$. Odgovarajuća asocijacijska shema ima 3 klase i Kreinove parametre

$$[q_{ij}^0] = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 6 \end{bmatrix}, \qquad [q_{ij}^1] = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 6 \\ 0 & 0 & 6 & 0 \end{bmatrix},$$

$$[q_{ij}^2] = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & \frac{10+\sqrt{2}}{4} & \frac{10-\sqrt{2}}{4} \\ 0 & 1 & \frac{10-\sqrt{2}}{4} & \frac{10+\sqrt{2}}{4} \end{bmatrix}, \ [q_{ij}^3] = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & \frac{10-\sqrt{2}}{4} & \frac{10+\sqrt{2}}{4} \\ 1 & 0 & \frac{10+\sqrt{2}}{4} & \frac{10-\sqrt{2}}{4} \end{bmatrix}.$$

□

Zadatak 2.23. *Dokažite da su Kreinovi parametri jako regularnog grafa (asocijacijske sheme s dvije klase) racionalni brojevi. Moraju li biti cijeli brojevi?*

Svojstva presječnih brojeva dokazujemo na dva načina: prebrojavanjem, iz kombinatorne interpretacije $p_{ij}^k = |N_i(x) \cap N_{j'}(y)|$ za $(x, y) \in R_k$, te matrično, iz definicijskog svojstva $A_i A_j = \sum_{k=0}^{d} p_{ij}^k A_k$ ili relacije (8).

Propozicija 2.24. *Presječni brojevi zadovoljavaju*

1. $p_{i0}^k = \delta_{ik}$,
2. $p_{0j}^k = \delta_{jk}$,
3. $p_{ij}^0 = n_i \delta_{ij'}$,
4. $p_{ij}^k = p_{j'i'}^{k'}$,
5. $\sum_{j=0}^{d} p_{ij}^k = n_i$,
6. $n_k p_{ij}^k = n_j p_{i'k}^j = n_i p_{kj'}^i$,
7. $\sum_{a=0}^{d} p_{ij}^a p_{ka}^b = \sum_{a=0}^{d} p_{ki}^a p_{aj}^b$.

Dokaz. 1. Za bilo koji par $(x,y) \in R_k$ je $p_{i0}^k = |\{z \mid (x,z) \in R_i,\ (z,y) \in R_0\}|$. Relacija R_0 je dijagonala, pa mora biti $y = x$. Zato vrijedi $p_{i0}^k = 1$ ako je $(x,y) \in R_i$, a $p_{i0}^k = 0$ ako $(x,y) \notin R_i$. Zbog disjunktnosti relacija prvi slučaj nastupa za $i = k$, a drugi za $i \neq k$. Na drugi način, iz svojstva Schurovih idempotenta dobivamo $A_i = A_i I = A_i A_0 = \sum_{k=0}^d p_{i0}^k A_k$. Lijevo i desno imamo prikaz matrice A_i u bazi $\{A_0, \ldots, A_d\}$, pa uspoređivanjem koeficijenata slijedi $p_{i0}^k = \delta_{ik}$.

2. Druga tvrdnja slijedi iz prve tvrdnje i komutativnosti, ali može se dokazati i za nekomutativne koherentne konfiguracije isto kao prva.

3. Za svaki vrh x je $(x,x) \in R_0$ i vrijedi $p_{ij}^0 = |\{z \mid (x,z) \in R_i,\ (z,x) \in R_j\}| = |\{z \mid (x,z) \in R_i,\ (x,z) \in R_{j'}\}|$. Za $i \neq j'$ dobivamo 0, a za $i = j'$ dobivamo $|N_i(x)| = n_i$. Na drugi način, iz relacije (8) slijedi

$$p_{ij}^0 = \frac{1}{n\, n_0} \operatorname{tr}(A_i A_j A_0^t) = \frac{1}{n} \operatorname{tr}(A_i A_j) \overset{(6)}{=} \frac{1}{n} \operatorname{sum}(A_i \circ A_j^t) = \frac{1}{n} \operatorname{sum}(A_i \circ A_{j'}).$$

Ponovo za $i \neq j'$ dobivamo 0, a za $i = j'$ dobivamo $\frac{1}{n} \operatorname{sum}(A_i) = \frac{n\, n_i}{n} = n_i$.

4. Neka je $(x,y) \in R_k$, tj. $(y,x) \in R_{k'}$. Kombinatorno odmah slijedi $p_{ij}^k = |\{z \mid (x,z) \in R_i,\ (z,y) \in R_j\}| = |\{z \mid (z,x) \in R_{i'},\ (y,z) \in R_{j'}\}| = p_{j'i'}^{k'}$. Matrično iz relacije (8) slijedi

$$\begin{aligned} p_{ij}^k &= \frac{1}{n\, n_k} \operatorname{tr}(A_i A_j A_k^t) \overset{(6)}{=} \frac{1}{n\, n_k} \operatorname{sum}((A_i A_j) \circ A_k) = \frac{1}{n\, n_k} \operatorname{sum}(((A_i A_j) \circ A_k)^t) \\ &= \frac{1}{n\, n_k} \operatorname{sum}((A_i A_j)^t \circ A_k^t) = \frac{1}{n\, n_k} \operatorname{sum}((A_j^t A_i^t) \circ A_k^t) \\ &= \frac{1}{n\, n_{k'}} \operatorname{sum}((A_{j'} A_{i'}) \circ A_{k'}) \overset{(6)}{=} \frac{1}{n\, n_{k'}} \operatorname{tr}(A_{j'} A_{i'} A_{k'}^t) = p_{j'i'}^{k'}. \end{aligned}$$

Koristili smo svojstva $\operatorname{sum}(A) = \operatorname{sum}(A^t)$, $(A \circ B)^t = A^t \circ B^t$, $(AB)^t = B^t A^t$ i svojstvo 3. iz propozicije 2.16. Primijetimo da formula $p_{ij}^k = p_{j'i'}^{k'}$ vrijedi i za nekomutativne koherentne konfiguracije, a za komutativne je $p_{ij}^k = p_{i'j'}^{k'}$.

5. Znamo da je $n_i = |N_i(x)|$. Uzmemo $(x,y) \in R_k$ i rastavimo skup $N_i(x)$ tako da ga presijecamo s blokovima particije $\{N_{j'}(y) \mid j = 0, \ldots, d\}$ od X. Slijedi $n_i = |\cup_{j=0}^d (N_i(x) \cap N_{j'}(y))| = \sum_{j=0}^d |N_i(x) \cap N_{j'}(y)| = \sum_{j=0}^d p_{ij}^k$. Matrični dokaz dobijemo iz relacije (8) i linearnosti traga:

$$\begin{aligned} \sum_{j=0}^d p_{ij}^k &= \sum_{j=0}^d \frac{1}{n\, n_k} \operatorname{tr}(A_i A_j A_k^t) = \frac{1}{n\, n_k} \operatorname{tr}(\sum_{j=0}^d A_i A_j A_k^t) = \frac{1}{n\, n_k} \operatorname{tr}(A_i (\sum_{j=0}^d A_j) A_k^t) \\ &= \frac{1}{n\, n_k} \operatorname{tr}(A_i J A_k^t) = \frac{1}{n\, n_k} \operatorname{tr}(n_i n_k J) = \frac{n_i n_k}{n\, n_k} \operatorname{tr}(J) = \frac{n_i \cancel{n_k n}}{\cancel{n\, n_k}} = n_i. \end{aligned}$$

6. Prebrojavamo sljedeći skup uređenih trojki vrhova na tri načina:

$$\{(x,y,z) \mid (x,y) \in R_k,\ (x,z) \in R_i,\ (z,y) \in R_j\}.$$

Prvo ga zapišemo kao

$$\bigcup_{x \in X} \bigcup_{y \in N_k(x)} \{(x,y,z) \mid (x,z) \in R_i,\ (z,y) \in R_j\}$$

i primijetimo da za fiksne x i y uređenih trojki ima isto kao vrhova u skupu $\{z \mid (x,z) \in R_i,\ (z,y) \in R_j\} = N_i(x) \cap N_{j'}(y)$. Zato je ukupan broj trojki $n\, n_k p_{ij}^k$. Iz drugog zapisa

$$\bigcup_{z \in X} \bigcup_{y \in N_j(z)} \{(x,y,z) \mid (x,y) \in R_k,\ (x,z) \in R_i\}$$

slijedi da je broj trojki $n\, n_j p_{i'k}^j$, a iz trećeg zapisa

$$\bigcup_{x \in X} \bigcup_{z \in N_i(x)} \{(x,y,z) \mid (x,y) \in R_k,\ (z,y) \in R_j\}$$

slijedi da je broj trojki $n\, n_i p_{kj'}^i$. Tvrdnja slijedi izjednačavanjem broja trojki i dijeljenjem s n. Za matrični dokaz prvo iz relacije (8) izrazimo

$$\begin{aligned}
n_k p_{ij}^k &= \frac{1}{n} \operatorname{tr}(A_i A_j A_k^t), \\
n_j p_{i'k}^j &= \frac{1}{n} \operatorname{tr}(A_{i'} A_k A_j^t) = \frac{1}{n} \operatorname{tr}(A_i^t A_k A_j^t), \\
n_i p_{kj'}^i &= \frac{1}{n} \operatorname{tr}(A_k A_{j'} A_i^t) = \frac{1}{n} \operatorname{tr}(A_k A_j^t A_i^t).
\end{aligned}$$

Sada koristimo važno svojstvo traga $\operatorname{tr}(AB) = \operatorname{tr}(BA)$ da bismo pokazali $\operatorname{tr}(A_i^t A_k A_j^t) = \operatorname{tr}((A_i^t A_k A_j^t)^t) = \operatorname{tr}(A_j A_k^t A_i) = \operatorname{tr}((A_j A_k^t) A_i) = \operatorname{tr}(A_i (A_j A_k^t)) = \operatorname{tr}(A_i A_j A_k^t)$. Na sličan način vidimo $\operatorname{tr}(A_k A_j^t A_i^t) = \operatorname{tr}(A_i A_j A_k^t)$, pa su sva tri izraza jednaka.

7. Za kombinatorni dokaz zadnje tvrdnje fiksiramo par $(x,y) \in R_b$ i prebrojimo sljedeći skup parova vrhova na dva načina:

$$\begin{aligned}
&\{(z,w) \mid (z,w) \in R_i,\ (x,z) \in R_k,\ (w,y) \in R_j\} = \\
&= \bigcup_{a=0}^{d} \bigcup_{z \in N_k(x) \cap N_{a'}(y)} \{(z,w) \mid (z,w) \in R_i,\ (w,y) \in R_j\} \\
&= \bigcup_{a=0}^{d} \bigcup_{w \in N_a(x) \cap N_{j'}(y)} \{(z,w) \mid (z,w) \in R_i,\ (x,z) \in R_k\}.
\end{aligned}$$

Matrični dokaz je prirodniji i slijedi iz asocijativnosti množenja matrica $A_k(A_iA_j) = (A_kA_i)A_j$. Primijenimo na lijevoj strani definicijsko svojstvo presječnih brojeva $A_iA_j = \sum_{a=0}^d p_{ij}^a A_a$, pa dobijemo

$$\begin{aligned} A_k(A_iA_j) &= A_k \sum_{a=0}^d p_{ij}^a A_a = \sum_{a=0}^d p_{ij}^a A_k A_a \\ &= \sum_{a=0}^d p_{ij}^a \sum_{b=0}^d p_{ka}^b A_b = \sum_{b=0}^d \left(\sum_{a=0}^d p_{ij}^a p_{ka}^b \right) A_b. \end{aligned}$$

Slično na desnoj strani dobijemo

$$(A_kA_i)A_j = \sum_{b=0}^d \left(\sum_{a=0}^d p_{ki}^a p_{aj}^b \right) A_b.$$

Tvrdnja slijedi izjednačavanjem koeficijenata. □

Dualna svojstva Kreinovih parametara dokazujemo samo matrično, budući da Kreinovi parametri nemaju kombinatornu interpretaciju.

Propozicija 2.25. *Kreinovi parametri zadovoljavaju*

1. $q_{i0}^k = \delta_{ik}$,
2. $q_{0j}^k = \delta_{jk}$,
3. $q_{ij}^0 = m_i \delta_{i\hat{j}}$,
4. $q_{ij}^k = q_{\hat{i}\hat{j}}^{\hat{k}}$,
5. $\sum_{j=0}^d q_{ij}^k = m_i$,
6. $m_k q_{ij}^k = m_j q_{\hat{i}k}^j = m_i q_{k\hat{j}}^i$,
7. $\sum_{a=0}^d q_{ij}^a q_{ka}^b = \sum_{a=0}^d q_{ki}^a q_{aj}^b$.

Dokaz. 1. Iz svojstva primitivnih idempotenta slijedi $E_i = E_i \circ J = n(E_i \circ E_0) = n(\frac{1}{n} \sum_{k=0}^d q_{i0}^k E_k) = \sum_{k=0}^d q_{i0}^k E_k$. Lijevo i desno imamo prikaz od E_i u bazi $\{E_0, \ldots, E_d\}$, pa usporedbom koeficijenata dobijemo $q_{i0}^k = \delta_{ik}$.

2. Slijedi iz "komutativnosti" Kreinovih parametara $q_{0j}^k = q_{j0}^k = \delta_{jk}$.

3. Iz relacije (9) slijedi

$$q_{ij}^0 = \frac{n}{m_0}\operatorname{tr}((E_i \circ E_j)E_0) = \cancel{n}\operatorname{tr}((E_i \circ E_j)\frac{1}{\cancel{n}}J) \overset{(6)}{=} \operatorname{sum}(E_i \circ E_j \circ J^t)$$

$$= \operatorname{sum}(E_i \circ E_j) \overset{(6)}{=} \operatorname{tr}(E_i E_j^t) = \operatorname{tr}(E_i E_{\hat{j}}).$$

Za $i \neq \hat{j}$ dobijemo 0, a za $i = \hat{j}$ dobijemo $\operatorname{tr} E_i = m_i$.

4. Koristimo relacije (9), (7) i svojstvo 3. iz propozicije 2.19:

$$q_{ij}^k = \frac{n}{m_k}\operatorname{tr}((E_i \circ E_j)E_k) \overset{(7)}{=} \frac{n}{m_k}\operatorname{tr}((E_i^t \circ E_j^t)E_k^t) = \frac{n}{m_{\hat{k}}}\operatorname{tr}((E_{\hat{i}} \circ E_{\hat{j}})E_{\hat{k}}) = q_{\hat{i}\hat{j}}^{\hat{k}}.$$

5. Iz relacije (9), linearnosti traga te distributivnosti matričnog i Schurovog produkta prema zbrajanju matrica slijedi

$$\sum_{j=0}^{d} q_{ij}^k = \sum_{j=0}^{d} \frac{n}{m_k}\operatorname{tr}((E_i \circ E_j)E_k) = \frac{n}{m_k}\operatorname{tr}\left(\sum_{j=0}^{d}(E_i \circ E_j)E_k\right)$$

$$= \frac{n}{m_k}\operatorname{tr}\left(\left(E_i \circ \sum_{j=0}^{d} E_j\right) E_k\right) = \frac{n}{m_k}\operatorname{tr}\left((E_i \circ I)\, E_k\right).$$

Matrica $E_i \circ I$ na dijagonali ima iste elemente kao E_i, a izvan dijagonale ima nule. Vidimo da je $\operatorname{tr}(E_i \circ I) = \operatorname{tr} E_i = m_i$. S druge strane, $E_i \circ I$ je matrica iz Bose-Mesnerove algebre i ima konstantnu dijagonalu. Zaključujemo da je $E_i \circ I = \frac{m_i}{n} I$, pa uvrštavanjem u gonju jednakost dobivamo

$$\sum_{j=0}^{d} q_{ij}^k = \frac{\cancel{n}}{m_k}\operatorname{tr}\left(\left(\frac{m_i}{\cancel{n}} I\right) E_k\right) = \frac{m_i}{m_k}\operatorname{tr}(E_k) = \frac{m_i}{m_k} m_k = m_i.$$

6. Iz relacije (9) izrazimo

$$\begin{aligned}
m_k q_{ij}^k &= n\operatorname{tr}((E_i \circ E_j)E_k),\\
m_j q_{\hat{i}k}^j &= n\operatorname{tr}((E_{\hat{i}} \circ E_k)E_j) = n\operatorname{tr}((E_i^t \circ E_k)E_j),\\
m_i q_{k\hat{j}}^i &= n\operatorname{tr}((E_k \circ E_{\hat{j}})E_i) = n\operatorname{tr}((E_k \circ E_j^t)E_i).
\end{aligned}$$

Sada iz relacije (7) i komutativnosti Schurovog množenja slijedi da se izrazi podudaraju.

7. Slijedi iz asocijativnosti Schurovog množenja $E_k \circ (E_i \circ E_j) = (E_k \circ E_i) \circ E_j$ i svojstva $E_i \circ E_j = \frac{1}{n} \sum_{a=0}^{d} q_{ij}^a E_a$:

$$E_k \circ (E_i \circ E_j) = E_k \circ \left(\frac{1}{n} \sum_{a=0}^{d} q_{ij}^a E_a \right) = \frac{1}{n} \sum_{a=0}^{d} q_{ij}^a (E_k \circ E_a)$$
$$= \frac{1}{n} \sum_{a=0}^{d} q_{ij}^a \left(\frac{1}{n} \sum_{b=0}^{d} q_{ka}^b E_b \right) = \frac{1}{n^2} \sum_{b=0}^{d} \left(\sum_{a=0}^{d} q_{ij}^a q_{ka}^b \right) E_b.$$

Na desnoj strani dobijemo

$$(E_k \circ E_i) \circ E_j = \frac{1}{n^2} \sum_{b=0}^{d} \left(\sum_{a=0}^{d} q_{ki}^a q_{aj}^b \right) E_b$$

i tvrdnja slijedi izjednačavanjem koeficijenata. $\square$

2.4 Svojstvene vrijednosti

U ovoj cjelini $\mathscr{A} \leq M_n(\mathbb{C})$ je i dalje Bose-Mesnerova algebra s bazom Schurovih idempotenta $A_0, \ldots, A_d$ i bazom primitivnih idempotenta $E_0, \ldots, E_d$. Kratnosti od $\mathscr{A}$ definirali smo kao $m_i = \operatorname{tr} E_i$. Matrice E_i su hermitske i idempotentne ($E_i^* = E_i$, $E_i^2 = E_i$), pa su dijagonalizabilne i svojstvene vrijednosti su im samo nule i jedinice. Zato im se trag podudara s rangom: $m_i = \operatorname{tr} E_i = \operatorname{rk} E_i = \dim \operatorname{Im} E_i$. Označimo $V = \mathbb{C}^n$ i $V_i = \operatorname{Im} E_i \leq V$.

Lema 2.26. *Vrijedi $V = V_0 \oplus \ldots \oplus V_d$ (ortogonalna suma).*

Dokaz. Iz relacije $I = E_0 + \ldots + E_d$ slijedi da se svaki vektor $x \in V$ može zapisati kao $x = x_0 + \ldots + x_d$ za $x_i = E_i x \in V_i$. Ortogonalnost sume slijedi zato što je $E_i E_j = 0$ za $i \neq j$. Skalarni produkti pribrojnika su $x_i^* x_j = (E_i x)^* (E_j x) = x^* E_i^* E_j x = x^* E_i E_j x = x^* 0 x = 0$. $\square$

Uzmimo bilo koju matricu $A \in \mathscr{A}$ i prikažimo je u bazi primitivnih idempotenta: $A = \lambda_0 E_0 + \ldots + \lambda_d E_d$. Za svaki vektor $x \in V_i$ vrijedi $E_i x = x$ i $E_j x = 0$ za $j \neq i$, pa je $Ax = \lambda_i x$. Dakle, λ_i je svojstvena vrijednost matrice A, a V_i je odgovarajući svojstveni potprostor. Lema 2.26 daje nam dekompoziciju prostora V na zajedničke svojstvene potprostore matrica iz Bose-Mesnerove algebre, a $m_i = \dim V_i$ su geometrijske kratnosti odgovarajućih svojstvenih vrijednosti.

Raspišimo Schurove idempotente u bazi primitivnih idempotenta:

$$A_j = \sum_{i=0}^{d} P_j(i) E_i, \quad j = 0, \ldots, d. \tag{10}$$

Brojevi $P_j(0), \dots, P_j(d) \in \mathbb{C}$ su svojstvene vrijednosti od A_j pridružene zajedničkim svojstvenim potprostorima $V_0, \dots, V_d$. Zovemo ih *svojstvenim vrijednostima Bose-Mesnerove algebre* $\mathscr{A}$. Može se dogoditi da se neki od brojeva $P_j(0), \dots, P_j(d)$ podudaraju. Dualno, raspišimo primitivne idempotente u bazi Schurovih idempotenta:

$$E_j = \frac{1}{n} \sum_{i=0}^{d} Q_j(i) A_i, \quad j = 0, \dots, d. \tag{11}$$

Brojeve $Q_j(0), \dots, Q_j(d) \in \mathbb{C}$ zovemo *dualnim svojstvenim vrijednostima Bose-Mesnerove algebre* $\mathscr{A}$. Matricu $P = [P_j(i)] \in M_{d+1}(\mathbb{C})$, kojoj je unos na mjestu (i, j) jednak $P_j(i)$, zovemo *svojstvenom matricom* ili *prvom tablicom karaktera* od $\mathscr{A}$. Svojstvena matrica u j-tom stupcu ima svojstvene vrijednosti od A_j, a retke i stupce indeksiramo s $0, \dots, d$. Na taj način definiramo i matricu $Q = [Q_j(i)] \in M_{d+1}(\mathbb{C})$, koju zovemo *dualnom svojstvenom matricom* ili *drugom tablicom karaktera* od $\mathscr{A}$. Budući da je P matrica prijelaza iz baze $\{E_i\}$ u bazu $\{A_i\}$, a $\frac{1}{n}Q$ je matrica prijelaza iz baze $\{A_i\}$ u bazu $\{E_i\}$, vrijedi sljedeća tvrdnja.

Propozicija 2.27. *$PQ = QP = nI$.*

Pritom je I jedinična matrica reda $d + 1$ (do sada smo s I označavali jediničnu matricu reda n). Vidimo da poznavanje jedne od matrica P i Q jednoznačno određuje drugu: $Q = nP^{-1}$ i $P = nQ^{-1}$. Štoviše, ako su Schurove idempotente simetrične matrice (tj. ako radimo s asocijacijskom shemom), svojstvene vrijednosti su im realne i P je realna matrica. Tada je i Q realna matrica, kao inverz realne matrice. Izvest ćemo još jednu vezu između matrica P i Q.

Formulom $\langle A, B\rangle = \operatorname{tr}(AB^*)$ zadan je skalarni produkt na vektorskom prostoru kvadratnih matrica. Stoga su $M_n(\mathbb{C})$ i naša Bose-Mesnerova algebra $\mathscr{A}$ unitarni prostori. Zbog relacije (6) skalarni produkt možemo zapisati i kao $\langle A, B\rangle = \operatorname{sum}(A \circ \overline{B})$. Dakle, imamo dva izraza za skalarni produkt:

$$\langle A, B\rangle = \operatorname{tr}(AB^*) = \operatorname{sum}(A \circ \overline{B}). \tag{12}$$

Iz toga slijedi da su obje baze Schurovih i primitivnih idempotenta ortogonalne:

$$\langle A_i, A_j\rangle = \operatorname{sum}(A_i \circ \overline{A_j}) = \operatorname{sum}(A_i \circ A_j) = \operatorname{sum}(\delta_{ij} A_i) = \delta_{ij} n\, n_i,$$

$$\langle E_i, E_j\rangle = \operatorname{tr}(E_i E_j^*) = \operatorname{tr}(E_i E_j) = \operatorname{tr}(\delta_{ij} E_i) = \delta_{ij} m_i.$$

U skalarnom kvadratu Schurovih idempotenta pojavljuje se dodatni faktor n, kojeg nema u skalarnom kvadratu primitivnih idempotenta. To je razlog zašto smo u definiciji Kreinovih parametara (5) i na drugim mjestima množili s $\frac{1}{n}$. Da zamijenimo primitivne idempotente s bazom $\{\sqrt{n}E_i\}$, vrijedilo bi $\langle\sqrt{n}E_i, \sqrt{n}E_j\rangle = \delta_{ij} n\, m_i$ (analogno kao za Schurove idempotente), a definicija Kreinovih parametara glasila bi $\sqrt{n}E_i \circ \sqrt{n}E_j = \sum_{k=0}^{d} q_{ij}^k E_k$ (bez faktora $\frac{1}{n}$ s desne strane, kao i za presječne brojeve).

Lema 2.28.

1. $$A_i E_j = P_i(j) E_j, \tag{13}$$

2. $$A_i \circ E_j = \frac{1}{n} Q_j(i) A_i. \tag{14}$$

Dokaz. Prvu relaciju dobijemo matričnim množenjem (10) s E_i i zamjenom indeksa $i \leftrightarrow j$, a drugu relaciju Schurovim množenjem (11) s A_i. Relaciju (13) možemo interpretirati na sljedeći način. Na lijevoj strani je matrica kompozicije linearnih operatora, pri čemu prvo djeluje ortogonalni projektor na svojstveni potprostor V_j s matricom E_j, a zatim linearni operator s matricom A_i. Svojstvena vrijednost od A_i na tom potprostoru je $P_i(j)$, pa je rezultat isti kao da djelujemo projektorom E_j i množimo skalarom $P_i(j)$. $\square$

Zbog dvostruke formule za skalarni produkt (12) možemo na dva načina izračunati međusobne umnoške Schurovih i primitivnih idempotenta:

$$\langle A_i, E_j\rangle = \mathrm{tr}(A_i E_j^*) = \mathrm{tr}(A_i E_j) \overset{(13)}{=} \mathrm{tr}(P_i(j) E_j) = P_i(j) m_j$$

$$= \mathrm{sum}(A_i \circ \overline{E_j}) = \mathrm{sum}(\overline{A_i \circ E_j}) \overset{(14)}{=} \mathrm{sum}(\tfrac{1}{n}\overline{Q_j(i)} A_i) = \overline{Q_j(i)} n_i.$$

Izjednačavanjem dobivamo drugu vezu između svojsvenih vrijednosti i dualnih svojstvenih vrijednosti:

Teorem 2.29. $\dfrac{Q_j(i)}{m_j} = \dfrac{\overline{P_i(j)}}{n_i}$.

Zapišimo tu vezu matrično, pomoću dijagonalnih matrica $N, M \in M_{d+1}(\mathbb{C})$ koje na dijagonali imaju stupnjeve, odnosno kratnosti od $\mathscr{A}$:

$$N = \begin{bmatrix} n_0 & & 0 \\ & \ddots & \\ 0 & & n_d \end{bmatrix}, \quad M = \begin{bmatrix} m_0 & & 0 \\ & \ddots & \\ 0 & & m_d \end{bmatrix}. \tag{15}$$

Množenje matrice A dijagonalnom matricom D zdesna AD je množenje stupaca od A redom s elementima na dijagonali od D, a s lijeva DA je množenje redaka od A. Vidimo da vrijedi $NQ = P^* M$ i time smo dokazali

Propozicija 2.30. $Q = N^{-1}P^*M, \quad P = M^{-1}Q^*N.$

Raspisivanjem matrične jednakosti iz propozicije 2.27 po komponentama dobivamo takozvane *relacije ortogonalnosti.*

Teorem 2.31. *Svojstvene vrijednosti zadovoljavaju prvu i drugu relaciju ortogonalnosti:*

1. $$\sum_{k=0}^{d} \frac{1}{n_k} P_k(i)\overline{P_k(j)} = \frac{n}{m_i}\delta_{ij},$$

2. $$\sum_{k=0}^{d} m_k P_i(k)\overline{P_j(k)} = n\, n_i \delta_{ij}.$$

Dokaz. 1. Element na mjestu (i,j) u matričnoj jednakosti $PQ = nI$ je $\sum_{k=0}^{d} P_k(i)Q_j(k) = n\delta_{ij}$. Iz teorema 2.29 izrazimo $Q_j(k) = \frac{m_j}{n_k}\overline{P_k(j)}$. Uvrštavanjem dobijemo prvu relaciju ortogonalnosti.

2. Element na mjestu (j,i) u matričnoj jednakosti $QP = nI$ je $\sum_{k=0}^{d} Q_k(j)P_i(k) = n\delta_{ij}$. Iz teorema 2.29 izrazimo $Q_k(j) = \frac{m_k}{n_j}\overline{P_j(k)}$ i dobijemo drugu relaciju ortogonalnosti. $\square$

Zadatak 2.32. *Izvedite prvu i drugu relaciju ortogonalnosti za dualne svojstvene vrijednosti.*

Rješenje. $$\sum_{k=0}^{d} \frac{1}{m_k} Q_k(i)\overline{Q_k(j)} = \frac{n}{n_i}\delta_{ij}, \qquad \sum_{k=0}^{d} n_k Q_i(k)\overline{Q_j(k)} = n\, m_i \delta_{ij}.$$ $\square$

Uzmimo bilo koju matricu $A \in M_n(\mathbb{C})$ i označimo s $\widehat{A}$ njezinu ortogonalnu projekciju na Bose-Mesnerovu algebru $\mathscr{A}$. Budući da su obje baze $\{A_0, \ldots, A_d\}$ i $\{E_0, \ldots, E_d\}$ ortogonalne, lako izračunamo prikaze od $\widehat{A}$ u tim bazama:

$$\begin{aligned} \widehat{A} &= \sum_{i=0}^{d} \alpha_i A_i, \quad \alpha_i = \frac{\langle A_i, A\rangle}{\langle A_i, A_i\rangle} = \frac{\langle A_i, A\rangle}{n\, n_i} \\ &= \sum_{i=0}^{d} \lambda_i E_i, \quad \lambda_i = \frac{\langle E_i, A\rangle}{\langle E_i, E_i\rangle} = \frac{\langle E_i, A\rangle}{m_i}. \end{aligned}$$

Koeficijenti α_i su unosi matrice $\widehat{A}$, a koeficijenti λ_i su svojstvene vrijednosti matrice $\widehat{A}$. U nastavku dokazujemo još neka svojstva prve i druge tablice karaktera P i Q.

Propozicija 2.33.

1. $P_0(i) = 1$,
2. $Q_0(i) = 1$,
3. $P_j(0) = n_j$,
4. $Q_j(0) = m_j$.

Dokaz. 1. Vrijedi $A_0 = I = E_0 + \ldots + E_d$, pa iz (10) slijedi $P_0(i) = 1$.

2. Dualno, iz $E_0 = \frac{1}{n}J = \frac{1}{n}(A_0 + \ldots + A_d)$ i (11) slijedi $Q_0(i) = 1$.

3. U propoziciji 2.16 vidjeli smo da su sume redaka i stupaca od A_j jednake n_j, što možemo zapisati kao $A_j J = J A_j = n_j J$. Stoga je $E_0 A_j = \frac{1}{n} J A_j = \frac{n_j}{n} J = n_j E_0$. S druge strane, iz (13) je $E_0 A_j = A_j E_0 = P_j(0) E_0$. Izjednačavanjem slijedi $P_j(0) = n_j$.

4. Kratnosti smo definirali kao $m_j = \operatorname{tr} E_j$. Matrica A_0 je jedinična matrica, a ostale Schurove idempotente na dijagonali imaju nule, pa je $\operatorname{tr}(A_i) = n\delta_{i0}$. Iz linearnosti traga i (11) slijedi

$$m_j = \operatorname{tr} E_j = \operatorname{tr}\left(\frac{1}{n}\sum_{i=0}^{d} Q_j(i) A_i\right) = \frac{1}{n}\sum_{i=0}^{d} Q_j(i)\operatorname{tr}(A_i) = Q_j(0).$$

□

Dakle, tablice karaktera su ovog oblika:

$$P = \begin{bmatrix} 1 & n_1 & \cdots & n_d \\ 1 & & & \\ \vdots & & & \\ 1 & & & \end{bmatrix}, \quad Q = \begin{bmatrix} 1 & m_1 & \cdots & m_d \\ 1 & & & \\ \vdots & & & \\ 1 & & & \end{bmatrix}.$$

Na primjer, za Heawoodov graf (slika 7, zadatak 2.22) vrijedi

$$P = \begin{bmatrix} 1 & 3 & 6 & 4 \\ 1 & -3 & 6 & -4 \\ 1 & \sqrt{2} & -1 & -\sqrt{2} \\ 1 & -\sqrt{2} & -1 & \sqrt{2} \end{bmatrix}, \quad Q = \begin{bmatrix} 1 & 1 & 6 & 6 \\ 1 & -1 & 2\sqrt{2} & -2\sqrt{2} \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -\frac{3}{\sqrt{2}} & \frac{3}{\sqrt{2}} \end{bmatrix}.$$

Stupnjevi su $(n_0, n_1, n_2, n_3) = (1, 3, 6, 4)$, a kratnosti su $(m_0, m_1, m_2, m_3) = (1, 1, 6, 6)$. U ovom primjeru sve svojstvene vrijednosti i dualne svojstvene vrijednosti su realni brojevi jer su Schurove idempotente simetrične, tj. imamo asocijacijsku shemu. U primjeru 1.37 koherentna konfiguracija dobivena Schurovom konstrukcijom od permutacijske grupe $G = \langle(1,2,3)\rangle$ nije simetrična, ali jest komutativna. Njezine tablice karaktera sadrže kompleksne brojeve:

$$P = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \frac{-1+i\sqrt{3}}{2} & \frac{-1-i\sqrt{3}}{2} \\ 1 & \frac{-1-i\sqrt{3}}{2} & \frac{-1+i\sqrt{3}}{2} \end{bmatrix}, \quad Q = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \frac{-1-i\sqrt{3}}{2} & \frac{-1+i\sqrt{3}}{2} \\ 1 & \frac{-1+i\sqrt{3}}{2} & \frac{-1-i\sqrt{3}}{2} \end{bmatrix}.$$

Stupnjevi i kratnosti su $(1,1,1)$, pa ovo je primjer tanke koherentne konfiguracije (zadatak 2.17). Primijetimo da su Schurove idempotente tankih koherentnih konfiguracija permutacijske matrice.

Zadatak 2.34. *Odredite svojstvene vrijednosti permutacijske matrice.*

Kao što smo vidjeli u primjeru 1.39, odgovarajuća koherentna konfiguracija ne mora biti komutativna, a tada ne možemo govoriti o njezinim svojstvenim vrijednostima (jer Schurove idempotente nemaju zajedničke svojstvene potprostore). U primjeru 1.37 sve (dualne) svojstvene vrijednosti imaju apsolutnu vrijednost 1. Za Heawoodov graf apsolutna vrijednost $|P_j(i)|$ je manja ili jednaka od stupnja n_j, a $|Q_j(i)|$ od kratnosti m_j (prvih elementa u j-tom stupcu). Tvrdnja vrijedi općenito.

Propozicija 2.35.

1. $|P_j(i)| \leq n_j$,
2. $|Q_j(i)| \leq m_j$.

Dokaz. Neka je $A \in M_n(\{0,1\})$ matrica s unosima iz $\{0,1\}$ i točno k jedinica u svakom retku. Tada je $A\mathbb{1} = k\mathbb{1}$, tj. k je svojstvena vrijednost od A pridružena svojstvenom vektoru $\mathbb{1}$. Tvrdimo da za svaku svojstvenu vrijednost λ od A vrijedi $|\lambda| \leq k$, tj. k je maksimalna svojstvena vrijednost. Neka je $x \in V = \mathbb{C}^n$, $x \neq 0$ svojstveni vektor pridružen λ. Neka je x_i najveća koordinata od x po apsolutnoj vrijednosti: $|x_i| \geq |x_j|$, $\forall j = 1, \ldots, n$. Računamo apsolutnu vrijednost i-te koordinate od $Ax = \lambda x$:

$$|\lambda||x_i| = |\lambda x_i| = \left|\sum_{j=1}^{n} a_{ij}x_j\right| \leq \sum_{j=1}^{n} a_{ij}|x_j| \leq \sum_{j=1}^{n} a_{ij}|x_i| = \sum_{\{j|a_{ij}=1\}} |x_i| = k|x_i|.$$

Dijeljenjem s $|x_i| \neq 0$ dobijemo $|\lambda| \leq k$. Posebno, u regularnom grafu stupanj regularnosti k je maksimalna svojstvena vrijednost matrice susjedstva (tvrdnju smo dokazali i za nesimetrične matrice A). Prvu tvrdnju propozicije dobijemo ako za A uzmemo Schurovu idempotentu A_j, a drugu tvrdnju dobijemo iz teorema 2.29:

$$|Q_j(i)| = \left|\frac{m_j}{n_i}\overline{P_i(j)}\right| = \frac{m_j}{n_i}|P_i(j)| \leq m_j.$$

□

Propozicija 2.36.

1. $P_{j'}(i) = \overline{P_j(i)}$,
2. $Q_{\hat{j}}(i) = \overline{Q_j(i)}$.

Dokaz. 1. Direktno iz (10) je $A_{j'} = \sum_{i=0}^{d} P_{j'}(i)E_i$. S druge strane, $A_{j'} = A_j^t = A_j^* \overset{(10)}{=} \left(\sum_{i=0}^{d} P_j(i)E_i\right)^* = \sum_{i=0}^{d} \overline{P_j(i)}E_i^* = \sum_{i=0}^{d} \overline{P_j(i)}E_i$. Uspoređivanjem koeficijenata vidimo da je $P_{j'}(i) = \overline{P_j(i)}$.

2. Dualno, iz (11) je $E_{\hat{j}} = \frac{1}{n}\sum_{i=0}^{d} Q_{\hat{j}}(i)A_i$. S druge strane vrijedi $E_{\hat{j}} = \overline{E_j} \overset{(11)}{=} \overline{\frac{1}{n}\sum_{i=0}^{d} Q_j(i)A_i} = \frac{1}{n}\sum_{i=0}^{d} \overline{Q_j(i)}A_i$. Uspoređivanjem koeficijenata vidimo da je $Q_{\hat{j}}(i) = \overline{Q_j(i)}$. □

Teorem 2.37.

1. $P_i(\ell)P_j(\ell) = \sum\limits_{k=0}^{d} p_{ij}^k P_k(\ell)$,
2. $Q_i(\ell)Q_j(\ell) = \sum\limits_{k=0}^{d} q_{ij}^k Q_k(\ell)$.

Dokaz. 1. U jednadakosti $A_iA_j = \sum_{k=0}^{d} p_{ij}^k A_k$ primijenimo (10) na lijevoj i na desnoj strani:

$$A_iA_j = \left(\sum_{\ell=0}^{d} P_i(\ell)E_\ell\right)\left(\sum_{k=0}^{d} P_j(k)E_k\right) = \sum_{\ell=0}^{d} P_i(\ell)P_j(\ell)E_\ell,$$

$$\sum_{k=0}^{d} p_{ij}^k A_k = \sum_{k=0}^{d} p_{ij}^k \sum_{\ell=0}^{d} P_k(\ell)E_\ell = \sum_{\ell=0}^{d}\left(\sum_{k=0}^{d} p_{ij}^k P_k(\ell)\right)E_\ell.$$

Tvrdnja slijedi izjednačavanjem koeficijenata uz E_ℓ.

2. U jednadakosti $E_i \circ E_j = \frac{1}{n}\sum_{k=0}^{d} q_{ij}^k E_k$ primijenimo (11) na lijevoj i na desnoj strani:

$$E_i \circ E_j = \left(\frac{1}{n}\sum_{\ell=0}^{d} Q_i(\ell)A_\ell\right) \circ \left(\frac{1}{n}\sum_{k=0}^{d} Q_j(k)A_k\right) = \frac{1}{n^2}\sum_{\ell=0}^{d} Q_i(\ell)Q_j(\ell)A_\ell,$$

$$\frac{1}{n}\sum_{k=0}^{d} q_{ij}^k E_k = \frac{1}{n}\sum_{k=0}^{d} q_{ij}^k \left(\frac{1}{n}\sum_{\ell=0}^{d} Q_k(\ell)A_\ell\right) = \frac{1}{n^2}\sum_{\ell=0}^{d}\left(\sum_{k=0}^{d} q_{ij}^k Q_k(\ell)\right) A_\ell.$$

Tvrdnja slijedi izjednačavanjem koeficijenata uz A_ℓ. □

Teorem 2.38.

1. $P_i(j)Q_j(\ell) = \sum_{k=0}^{d} p_{ik}^\ell Q_j(k)$,

2. $Q_i(j)P_j(\ell) = \sum_{k=0}^{d} q_{ik}^\ell P_j(k)$.

Dokaz. 1. Na dva načina raspišemo produkt A_iE_j i izjednačimo koeficijente uz A_ℓ:

$$A_iE_j \overset{(13)}{=} P_i(j)E_j \overset{(11)}{=} P_i(j)\left(\frac{1}{n}\sum_{\ell=0}^{d} Q_j(\ell)A_\ell\right) = \frac{1}{n}\sum_{\ell=0}^{d} P_i(j)Q_j(\ell)A_\ell,$$

$$\begin{aligned} A_iE_j &\overset{(11)}{=} A_i\left(\frac{1}{n}\sum_{k=0}^{d} Q_j(k)A_k\right) = \frac{1}{n}\sum_{k=0}^{d} Q_j(k)A_iA_k \\ &= \frac{1}{n}\sum_{k=0}^{d} Q_j(k)\sum_{\ell=0}^{d} p_{ik}^\ell A_\ell = \frac{1}{n}\sum_{\ell=0}^{d}\left(\sum_{k=0}^{d} p_{ik}^\ell Q_j(k)\right) A_\ell. \end{aligned}$$

2. Na dva načina raspišemo Schurov produkt $E_i \circ A_j$ i izjednačimo koeficijente uz E_ℓ:

$$E_i \circ A_j \overset{(14)}{=} \frac{1}{n}Q_i(j)A_j \overset{(10)}{=} \frac{1}{n}Q_i(j)\left(\sum_{\ell=0}^{d} P_j(\ell)E_\ell\right) = \frac{1}{n}\sum_{\ell=0}^{d} Q_i(j)P_j(\ell)A_\ell,$$

$$\begin{aligned} E_i \circ A_j &\overset{(10)}{=} E_i \circ \left(\sum_{k=0}^{d} P_j(k)E_k\right) = \sum_{k=0}^{d} P_j(k)E_i \circ E_k \\ &= \sum_{k=0}^{d} P_j(k)\left(\frac{1}{n}\sum_{\ell=0}^{d} q_{ik}^\ell E_\ell\right) = \frac{1}{n}\sum_{\ell=0}^{d}\left(\sum_{k=0}^{d} q_{ik}^\ell P_j(k)\right) E_\ell. \end{aligned}$$

□

Na kraju ove cjeline pokažimo kako presječne brojeve i Kreinove parametre možemo izraziti preko (dualnih) svojstvenih vrijednosti.

Teorem 2.39.

1. $$p_{ij}^k = \frac{1}{n\,n_k}\sum_{\ell=0}^{d} m_\ell P_i(\ell)P_j(\ell)\overline{P_k(\ell)} \tag{16}$$

$$= \frac{n_i n_j}{n}\sum_{\ell=0}^{d} \frac{1}{m_\ell^2} Q_\ell(i)Q_\ell(j)\overline{Q_\ell(k)}, \tag{17}$$

2. $$q_{ij}^k = \frac{1}{n\,m_k}\sum_{\ell=0}^{d} n_\ell Q_i(\ell)Q_j(\ell)\overline{Q_k(\ell)} \tag{18}$$

$$= \frac{m_i m_j}{n}\sum_{\ell=0}^{d} \frac{1}{n_\ell^2} P_\ell(i)P_\ell(j)\overline{P_\ell(k)}. \tag{19}$$

Dokaz. 1. Uvrstimo (10) u relaciju (8):

$$p_{ij}^k = \frac{1}{n\,n_k}\operatorname{tr}\left(A_iA_jA_k^t\right) = \frac{1}{n\,n_k}\operatorname{tr}\left(A_iA_jA_{k'}\right) =$$
$$= \frac{1}{n\,n_k}\operatorname{tr}\left(\sum_{\ell_1=0}^{d} P_i(\ell_1)E_{\ell_1}\sum_{\ell_2=0}^{d} P_j(\ell_2)E_{\ell_2}\sum_{\ell_3=0}^{d} P_{k'}(\ell_3)E_{\ell_3}\right).$$

Produkt $E_{\ell_1}E_{\ell_2}E_{\ell_3}$ je 0, osim za $\ell_1 = \ell_2 = \ell_3 = \ell$. Koristimo 1. tvrdnju iz propozicije 2.36, linearnost traga i definiciju kratnosti $m_\ell = \operatorname{tr} E_\ell$:

$$p_{ij}^k = \frac{1}{n\,n_k}\operatorname{tr}\left(\sum_{\ell=0}^{d} P_i(\ell)P_j(\ell)P_{k'}(\ell)\,E_\ell\right) = \frac{1}{n\,n_k}\sum_{\ell=0}^{d} P_i(\ell)P_j(\ell)\overline{P_k(\ell)}\operatorname{tr} E_\ell$$
$$= \frac{1}{n\,n_k}\sum_{\ell=0}^{d} m_\ell P_i(\ell)P_j(\ell)\overline{P_k(\ell)}.$$

Za drugi izraz koristimo teorem 2.29:

$$p_{ij}^k = \frac{1}{n\,\cancel{n_k}}\sum_{\ell=0}^{d} \cancel{m_\ell}\frac{n_i}{\cancel{m_\ell}}\overline{Q_\ell(i)}\frac{n_j}{m_\ell}\overline{Q_\ell(j)}\frac{\cancel{n_k}}{m_\ell}Q_\ell(k)$$
$$= \frac{n_i n_j}{n}\sum_{\ell=0}^{d} \frac{1}{m_\ell^2}\overline{Q_\ell(i)Q_\ell(j)}Q_\ell(k).$$

Presječni brojevi su realni, pa je $p_{ij}^k = \overline{p_{ij}^k} = \frac{n_i n_j}{n} \sum_{\ell=0}^{d} \frac{1}{m_\ell^2} Q_\ell(i) Q_\ell(j) \overline{Q_\ell(k)}$.

2. Dokazuje se dualno, uvrštavanjem (11) u relaciju (9). □

Vidjeli smo da svojstvene vrijednosti komutativne koherentne konfiguracije jednoznačno određuju sve ostale parametre: stupnjeve, kratnosti, dualne svojstvene vrijednosti, presječne brojeve i Kreinove parametre. Mnoge primjene ove teorije zasnivaju se na toj činjenici. Ako uspijemo izračunati svojstvenu matricu P, možemo napisati izraze za n_i, m_i i p_{ij}^k, a oni moraju biti nenegativni cijeli brojevi. Također možemo izraziti q_{ij}^k, a u idućoj cjelini dokazujemo da su i oni nenegativni.

2.5 Kreinov uvjet i presječne matrice

Uvjet nenegativnosti Kreinovih parametara q_{ij}^k poznat je kao *Kreinov uvjet.* Prezentirat ćemo dokaz koji autori knjige [4] pripisuju N. Biggsu [11]. U knjizi [21] Kreinov uvjet pripisuje se L. L. Scottu [111, 112]. U knjizi [4] izložen je još jedan dokaz iz Delsarteove disertacije [40], a C. Godsil daje alternativni dokaz u [55, Lema 2.4.3]. M. G. Krein je do uvjeta došao u kontekstu funkcionalne analize i konveksnosti [87, 88].

Ponovimo prvo osnovne činjenice o hermitskim matricama. Za matricu $A \in M_n(\mathbb{C})$ kažemo da je *hermitska* ako je $A^* = A$. Na primjer, primitivne idempotente Bose-Mesnerove algebre $E_0, \ldots, E_d$ su hermitske matrice. Ako su matrice A i B hermitske, onda je $A + B$ hermitska. Produkt AB ne mora biti hermitska matrica, osim ako A i B komutiraju. Schurov produkt $A \circ B$ je uvijek hermitska matrica. Hermitske matrice su normalne, pa se po teoremu 2.10 mogu dijagonalizirati.

Zadatak 2.40. *Dokažite da su svojstvene vrijednosti hermitske matrice realni brojevi.*

Rješenje. Neka je $\langle x, y \rangle = y^* x$ skalarni produkt na vektorskom prostoru $\mathbb{C}^n$ (vektore shvaćamo kao jednostupčane matrice). Tada za hermitsku matricu A vrijedi $\langle Ax, y \rangle = y^* A x = y^* A^* x = (Ay)^* x = \langle x, Ay \rangle$. Neka je λ svojstvena vrijednost pridružena svojstvenom vektoru $x \neq 0$, tj. $Ax = \lambda x$. Tada je $\langle Ax, x \rangle = \langle \lambda x, x \rangle = \lambda \langle x, x \rangle = \lambda \|x\|^2$. S druge strane, $\langle x, Ax \rangle = \langle x, \lambda x \rangle = \overline{\lambda} \langle x, x \rangle = \overline{\lambda} \|x\|^2$. Izjednačavanjem slijedi $\lambda = \overline{\lambda}$, tj. $\lambda \in \mathbb{R}$. □

Zadatak 2.41. *Dokažite da su svojstveni vektori pridruženi različitim svojstvenim vrijednostima hermitske matrice ortogonalni.*

Rješenje. Neka su $\lambda, \mu \in \mathbb{R}$ različite svojstvene vrijednosti, a $x, y \in \mathbb{C}^n$ odgovarajući svojstveni vektori: $Ax = \lambda x$, $Ay = \mu y$. Tada je $\lambda \langle x, y \rangle =$

$\langle \lambda x, y\rangle = \langle Ax, y\rangle = \langle x, Ay\rangle = \langle x, \mu y\rangle = \mu\langle x, y\rangle$. Vrijedi $(\lambda - \mu)\langle x, y\rangle = 0$, iz čega zbog $\lambda \neq \mu$ slijedi $\langle x, y\rangle = 0$. Dakle, svojstveni vektori x i y su ortogonalni. □

Znamo da je $\langle x, y\rangle = \overline{\langle y, x\rangle}$. Zato je za hermitsku matricu A i bilo koji vektor $x \in \mathbb{C}^n$ skalarni produkt $\langle Ax, x\rangle$ realan broj: $\overline{\langle Ax, x\rangle} = \langle x, Ax\rangle = \langle Ax, x\rangle$. Za A kažemo da je *pozitivno semidefinitna* ako je hermitska i vrijedi $\langle Ax, x\rangle \geq 0$, $\forall x \in \mathbb{C}^n$.

Zadatak 2.42. *Dokažite da je hermitska matrica A pozitivno semidefinitna ako i samo ako su joj sve svojstvene vrijednosti nenegativne.*

Rješenje. Neka je λ svojstvena vrijednost i $x \neq 0$ odgovarajući svojstveni vektor. Zbog pozitivne semidefinitnosti je $\langle Ax, x\rangle \geq 0$, a s druge strane je $\langle Ax, x\rangle = \langle \lambda x, x\rangle = \lambda\|x\|^2$. Iz $\lambda\|x\|^2 \geq 0$ slijedi $\lambda \geq 0$. Obrnuto, neka je $\{x_1, \ldots, x_n\}$ ortonormirana baza sastavljena od svojstvenih vektora. Odgovarajuće svojstvene vrijednosti označimo $\lambda_1, \ldots, \lambda_n$ i pretpostavimo da su nenegativne. Bilo koji vektor $x \in \mathbb{C}^n$ prikažimo u bazi $x = \sum_{i=1}^n \alpha_i x_i$ i računamo:

$$\langle Ax, x\rangle = \left\langle \sum_{i=1}^n \alpha_i A x_i, \sum_{j=1}^n \alpha_j x_j \right\rangle = \left\langle \sum_{i=1}^n \alpha_i \lambda_i x_i, \sum_{j=1}^n \alpha_j x_j \right\rangle$$

$$= \sum_{i=1}^n \sum_{j=1}^n \lambda_i \alpha_i \overline{\alpha_j} \langle x_i, x_j\rangle = \sum_{i=1}^n \lambda_i |\alpha_i|^2 \geq 0.$$

Dakle, A je pozitivno semidefinitna. □

Primitivne idempotente $E_0, \ldots, E_d$ za svojstvene vrijednosti imaju nule i jedinice, pa su po prethodnom zadatku pozitivno semidefinitne. *Glavna podmatrica* od A je podmatrica dobivena izbacivanjem nekih redaka i odgovarajućih stupaca (s istim indeksima).

Zadatak 2.43. *Ako je A hermitska matrica, dokažite da je svaka njezina glavna podmatrica hermitska.*

Rješenje. Ako je $A = [a_{ij}]$, hermitskost znači da je $a_{ij} = \overline{a_{ji}}$ za sve indekse i, j. Posebno, to vrijedi za indekse koji odgovaraju recima i stupcima glavne podmatrice, pa je i ona hermitska. □

Zadatak 2.44. *Ako je A pozitivno semidefinitna, dokažite da je svaka njezina glavna podmatrica pozitivno semidefinitna.*

Rješenje. Neka je $A \in M_n(\mathbb{C})$ i $B \in M_m(\mathbb{C})$ njezina glavna podmatrica dobivena restringiranjem na retke i stupce indeksirane s $I \subseteq \{1, \ldots, n\}$, $|I| = m$. Za bilo koji vektor $y \in \mathbb{C}^m$ možemo naći vektor $x \in \mathbb{C}^n$ kojem su komponente $x_i = 0$ ako $i \notin I$, a ostale komponente redom se podudaraju s komponentama od y. Tada je $\langle By, y\rangle = \langle Ax, x\rangle \geq 0$, pa je i B pozitivno semidefinitna. $\square$

Kroneckerov produkt matrice A tipa $m \times n$ i matrice B tipa $p \times q$ je matrica

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix}$$

tipa $mp \times nq$. Operacija je linearna u obje varijable:

$$(\alpha A + \beta B) \otimes C = \alpha(A \otimes C) + \beta(B \otimes C),$$

$$A \otimes (\beta B + \gamma C) = \beta(A \otimes B) + \gamma(A \otimes C).$$

Za konjugiranje, transponiranje i adjungiranje vrijedi

$$\overline{A \otimes B} = \overline{A} \otimes \overline{B}, \quad (A \otimes B)^t = A^t \otimes B^t, \quad (A \otimes B)^* = A^* \otimes B^*.$$

Prema tome, Kroneckerov produkt hermitskih matrica je hermitska matrica. Kroneckerov produkt se dobro ponaša prema standardnom i Schurovom množenju matrica.

Propozicija 2.45. *Ako su definirani produkti AC i BD, onda vrijedi*

$$(A \otimes B)(C \otimes D) = AC \otimes BD. \tag{20}$$

Ako su definirani Schurovi produkti $A \circ C$ i $B \circ D$, onda vrijedi

$$(A \otimes B) \circ (C \otimes D) = (A \circ C) \otimes (B \circ D). \tag{21}$$

Neka je A kvadratna matrica reda n, a B kvadratna matrica reda m i neka vrijedi $Ax = \lambda x$, $By = \mu y$. Iz (20) slijedi $(A \otimes B)(x \otimes y) = Ax \otimes By = \lambda x \otimes \mu y = (\lambda\mu)(x \otimes y)$. Iz toga slijedi

Propozicija 2.46. *Neka je $A \in M_n(\mathbb{C})$ matrica sa svojstvenim vrijednostima $\{\lambda_1, \ldots, \lambda_n\}$, a $B \in M_m(\mathbb{C})$ matrica sa svojstvenim vrijednostima $\{\mu_1, \ldots, \mu_m\}$. Tada $A \otimes B$ ima svojstvene vrijednosti $\{\lambda_i\mu_j \mid i = 1, \ldots, n,\ j = 1, \ldots, m\}$.*

Korolar 2.47. *Ako su A i B pozitivno semidefinitne, onda je $A \otimes B$ pozitivno semidefinitna.*

Dokaz. Slijedi iz prethodne propozicije i zadatka 2.42. □

Korolar 2.48. *Za $A \in M_n(\mathbb{C})$ i $B \in M_m(\mathbb{C})$ vrijedi* $\operatorname{tr}(A \otimes B) = \operatorname{tr}(A)\operatorname{tr}(B)$ *i* $\det(A \otimes B) = (\det A)^m (\det B)^n$.

Dokaz. Trag je zbroj svojstvenih vrijednosti, a determinanta umnožak svojstvenih vrijednosti. □

Lema 2.49. *Ako su $A, B \in M_n(\mathbb{C})$ pozitivno semidefinitne matrice, onda je njihov Schurov produkt $A \circ B$ pozitivno semidefinitna matrica.*

Dokaz. Prema korolaru 2.47, $A \otimes B$ je pozitivno semidefinitna matrica. Retke i stupce Kroneckerova produkta indeksiramo sa $\{(i,j) \mid i,j \in \{1,\ldots,n\}\}$. Ako je $r = (x,y)$ i $s = (u,v)$, onda $A \otimes B$ na mjestu (r,s) ima $a_{xu} b_{yv}$. Vidimo da je Schurov produkt $A \circ B = [a_{ij} b_{ij}]$ glavna podmatrica od $A \otimes B$ kojoj su reci i stupci indeksirani sa $\{(i,i) \mid i \in \{1,\ldots,n\}\}$. Prema zadatku 2.44, $A \circ B$ je pozitivno semidefinitna matrica. □

Sada znamo da su i Schurovi produkti primitivnih idempotenta $E_i \circ E_j$ pozitivno semidefinitne matrice. Iz toga lako slijedi Kreinov uvjet.

Teorem 2.50 (Kreinov uvjet)**.** *Kreinovi parametri su nenegativni: $q_{ij}^k \geq 0$.*

Dokaz. Po definiciji Kreinovih parametara vrijedi $E_i \circ E_j = \frac{1}{n} \sum_{k=0}^{d} q_{ij}^k E_k$. Kad matricu iz Bose-Mesnerove algebre prikažemo u bazi primitivnih idempotenta, koeficijenti su svojstvene vrijednosti te matrice. Prema tome, $\frac{1}{n} q_{ij}^k$, $k = 0, \ldots, d$ su svojstvene vrijednosti pozitivno semidefinitne matrice $E_i \circ E_j$. Iz zadatka 2.42 slijedi $q_{ij}^k \geq 0$. □

U teoremu 2.39 vidjeli smo da presječne brojeve p_{ij}^k i Kreinove parametre q_{ij}^k možemo izračunati iz tablica karaktera P ili Q. Idući cilj je pokazati da P i Q možemo izračunati iz presječnih brojeva ili Kreinovih parametara. U zadatku 1.35 i u primjerima 1.37 i 1.39 trodimenzionalnu tablicu presječnih brojeva p_{ij}^k rastavili smo na kvadratne matrice fiksiranjem indeksa k. Tako smo postupili da bude vidljiva (ne)komutativnost, no korisnije je fiksirati indeks i.

Definicija 2.51. *Neka je $B_i \in M_{d+1}(\mathbb{C})$ matrica kojoj je unos na mjestu (j,k) jednak p_{ij}^k. Matrice $B_0, \ldots, B_d$ zovemo* presječnim matricama *komutativne koherentne konfiguracije.*

U zadatku 2.22 Kreinove parametre složili smo u matrice fiksiranjem indeksa k, a sada ih slažemo fiksiranjem indeksa i.

Definicija 2.52. *Neka je* $B_i^\circ \in M_{d+1}(\mathbb{C})$ *matrica kojoj je unos na mjestu* (j,k) *jednak* q_{ij}^k. *Matrice* $B_0^\circ, \ldots, B_d^\circ$ *zovemo* dualnim presječnim matricama *komutativne koherentne konfiguracije.*

Propozicija 2.53. *Presječne matrice zadovoljavaju*

1. $B_0 = I$,

2. *nulti redak od* B_i *je vektor* e_i *kanonske baze od* $\mathbb{C}^{d+1}$*, koji na* i*-toj koordinati ima* 1*, a na ostalim koordinatama* 0*,*

3. *matrice* $B_0, \ldots, B_d$ *su linearno nezavisne,*

4. $B_i B_j = \sum_{k=0}^d p_{ij}^k B_k$,

5. $B_i B_j = B_j B_i$,

6. $(B_i)^t = N^{-1} B_{i'} N$*, gdje je matrica* N *definirana s* (15)*.*

Dokaz. 1. Element na mjestu (j,k) od B_0 je p_{0j}^k, a po 2. tvrdnji propozicije 2.24 to je δ_{jk}.

2. Element na mjestu $(0,k)$ od B_i je p_{i0}^k, a po 1. tvrdnji propozicije 2.24 to je δ_{ik}.

3. Slijedi iz prethodne tvrdnje.

4. Uz zamjenu oznaka $a \leftrightarrow k$ i korištenjem komutativnosti $p_{ij}^k = p_{ji}^k$, tvrdnju 7. propozicije 2.24 možemo zapisati kao $\sum_{k=0}^d p_{ij}^k p_{ka}^b = \sum_{k=0}^d p_{ia}^k p_{jk}^b$. Na lijevoj strani je (a,b)-unos matrice $\sum_{k=0}^d p_{ij}^k B_k$, a na desnoj strani je (a,b)-unos matrice $B_i B_j$. Prema tome, te dvije matrice se podudaraju.

5. Slijedi iz prethodne tvrdnje i komutativnosti $p_{ij}^k = p_{ji}^k$.

6. Iz 6. tvrdnje propozicije 2.24 slijedi $N(B_i)^t = B_{i'} N$. □

Propozicija 2.54. *Dualne presječne matrice zadovoljavaju*

1. $B_0^\circ = I$,

2. *nulti redak od* B_i° *je vektor* e_i *kanonske baze od* $\mathbb{C}^{d+1}$*, koji na* i*-toj koordinati ima* 1*, a na ostalim koordinatama* 0*,*

3. *matrice* $B_0^\circ, \ldots, B_d^\circ$ *su linearno nezavisne,*

4. $B_i^\circ B_j^\circ = \sum_{k=0}^d q_{ij}^k B_k^\circ$,

5. $B_i^\circ B_j^\circ = B_j^\circ B_i^\circ$,

6. $(B_i^\circ)^t = M^{-1} B_{\hat{i}}^\circ M$, *gdje je matrica* M *definirana s* (15).

Dokaz. Dokazuje se na isti način iz propozicije 2.25. □

Neka je $\mathscr{B} = \langle B_0, \ldots, B_d \rangle$ potprostor od $M_{d+1}(\mathbb{C})$ razapet presječnim matricama. Zbog propozicije 2.53, $\mathscr{B}$ je zatvoren na množenje matrica (4. tvrdnja), matrice iz $\mathscr{B}$ komutiraju (5. tvrdnja) i $\mathscr{B}$ sadrži neutralni element (1. tvrdnja). Dakle, $\mathscr{B}$ je komutativna algebra s jedinicom obzirom na množenje matrica, koju zovemo *presječnom algebrom* komutativne koherentne konfiguracije. Na isti način definiramo *dualnu presječnu algebru* $\mathscr{B}^\circ = \langle B_0^\circ, \ldots, B_d^\circ \rangle$, koja je također komutativna algebra s jedinicom obzirom na množenje matrica.

Teorem 2.55. *Presječna algebra* $\mathscr{B}$ *izomorfna je Bose-Mesnerovoj algebri* $(\mathscr{A}, \cdot)$ *s operacijom matričnog množenja. Dualna presječna algebra* $\mathscr{B}^\circ$ *izomorfna je Bose-Mesnerovoj algebri* $(\mathscr{A}, \circ)$ *s operacijom Schurovog množenja.*

Dokaz. Pridruživanje baza $B_i \mapsto A_i$ prošireno po linearnosti je izomorfizam vektorskih prostora. Zbog 4. tvrdnje propozicije 2.53 i definicijskog svojstva presječnih brojeva $A_i A_j = \sum_{k=0}^{d} p_{ij}^k A_k$, ujedno je izomorfizam algebri $\mathscr{B}$ i $(\mathscr{A}, \cdot)$. Dualno pridruživanje $B_i^\circ \mapsto nE_i$ daje izomorfizam algebri $\mathscr{B}^\circ$ i $(\mathscr{A}, \circ)$. □

Matrice iz presječne algebre $\mathscr{B}$ i dualne presječne algebre $\mathscr{B}^\circ$ su reda $d+1$, a matrice iz Bose-Mesnerove algebre $\mathscr{A}$ su reda n. Broj klasa d komutativne koherentne konfiguracije može biti puno manji od broja vrhova n, a tada je lakše računati u $\mathscr{B}$ i $\mathscr{B}^\circ$ nego u $\mathscr{A}$. Operacije $\cdot$ i $\circ$ definirane na Bose-Mesnerovoj algebri "prenijeli" smo na manje matrične algebre, ali $\mathscr{B}$ i $\mathscr{B}^\circ$ su općenito **različiti** potprostori od $M_{d+1}(\mathbb{C})$, a Bose-Mesnerova algebra $\mathscr{A}$ je **jedan** potprostor od $M_n(\mathbb{C})$ na kojem imamo dvije operacije množenja.

Iz teorema 2.55 vidimo razlog zašto presječni brojevi jednoznačno određuju svojstvene vrijednosti komutativne koherentne konfiguracije. Imamo izomorfizam algebri koji preslikava matrice $B_i \mapsto A_i$, pa B_i ima isti minimalni polinom kao A_i. Zato ima i iste svojstvene vrijednosti. Taj argument ne vrijedi za dualne presječne matrice, pa dokazujemo vezu između presječnih matrica i tablice karatera P koju možemo prenijeti i na dualni slučaj. Označimo s $\operatorname{diag}(\alpha_0, \ldots, \alpha_d) \in M_{d+1}(\mathbb{C})$ dijagonalnu matricu koja na dijagonali ima redom brojeve $\alpha_0, \ldots, \alpha_d$.

Teorem 2.56. *Presječne matrice i dualne presječne matrice zadovoljavaju*

1. $P(B_i)^t P^{-1} = \operatorname{diag}(P_i(0), \ldots, P_i(d))$,

2. $Q(B_i^\circ)^t Q^{-1} = \mathrm{diag}(Q_i(0), \ldots, Q_i(d))$.

Dokaz. 1. Neka je $A \in \mathscr{A}$ i $L_A : \mathscr{A} \to \mathscr{A}$ linearni operator zadan sa $L_A(B) = AB$. Tada vrijedi $L_{A_i}(A_j) = A_i A_j = \sum_{k=0}^d p_{ij}^k A_k$, pa je $(B_i)^t$ matrica linearnog operatora L_{A_i} u bazi Schurovih idempotenta $\{A_0, \ldots, A_d\}$. S druge strane, $L_{A_i}(E_j) = A_i E_j \overset{(10)}{=} \left(\sum_{k=0}^d P_i(k) E_k\right) E_j = P_i(j) E_j$, pa je $\mathrm{diag}(P_i(0), \ldots, P_i(d))$ matrica istog linearnog operatora u bazi primitivnih idempotenta $\{E_0, \ldots, E_d\}$. Prva tvrdnja vrijedi jer je P matrica prijelaza iz baze $\{E_i\}$ u bazu $\{A_i\}$.

2. Neka je $A \in \mathscr{A}$ i $L_A^\circ : \mathscr{A} \to \mathscr{A}$ linearni operator zadan sa $L_A^\circ(B) = A \circ B$. Tada vrijedi $L_{E_i}(E_j) = E_i \circ E_j = \frac{1}{n} \sum_{k=0}^d q_{ij}^k E_k$, pa je $\frac{1}{n}(B_i^\circ)^t$ matrica linearnog operatora $L_{E_i}^\circ$ u bazi primitivnih idempotenta $\{E_0, \ldots, E_d\}$. S druge strane, $L_{E_i}^\circ(A_j) = E_i \circ A_j \overset{(11)}{=} \left(\frac{1}{n} \sum_{k=0}^d Q_i(k) A_k\right) \circ A_j = \frac{1}{n} Q_i(j) A_j$, pa je $\frac{1}{n}\,\mathrm{diag}(Q_i(0), \ldots, Q_i(d))$ matrica istog linearnog operatora u bazi Schurovih idempotenta $\{A_0, \ldots, A_d\}$. Druga tvrdnja vrijedi jer je $\frac{1}{n}Q$ matrica prijelaza iz baze $\{A_i\}$ u bazu $\{E_i\}$. □

Korolar 2.57. *Spektar presječne matrice B_i je $\{P_i(0), \ldots, P_i(d)\}$ i podudara se sa spektrom Schurove idempotente A_i. Spektar dualne presječne matrice B_i° je $\{Q_i(0), \ldots, Q_i(d)\}$.*

Dokaz. Spektar dijagonalne matrice su brojevi na dijagonali, a spektri transponirane matrice $(B_i)^t$ i njoj slične matrice $P(B_i)^t P^{-1}$ podudaraju se sa spektrom od B_i. □

Na kraju ovog poglavlja dokazujemo još jedan uvjet djeljivosti stupnjeva i kratnosti komutativne koherentne konfiguracije. Iz propozicije 2.27 znamo da je $PQ = nI$, a po propoziciji 2.30 je $Q = N^{-1} P^* M$. Uvrštavanjem dobijemo $PN^{-1}P^*M = nI$, a računanjem determinante slijedi

$$\det(PP^*) = n^{d+1} \frac{\det N}{\det M} = n^{d+1} \prod_{i=0}^d \frac{n_i}{m_i}. \tag{22}$$

Ovaj izraz poznat je kao *Frameov*[17] *kvocijent* [51]. Pomoću skalarnog produkta na prostoru matrica (12) možemo ga izraziti i kao omjer skalarnih kvadrata Schurovih i primitivnih idempotenta:

$$\det(PP^*) = \prod_{i=0}^d \frac{\langle A_i, A_i \rangle}{\langle E_i, E_i \rangle}.$$

[17] J. Sutherland Frame (1907.-1997.), američki matematičar.

Teorem 2.58. *Frameov kvocijent* (22) *je prirodan broj.*

Dokaz. Matrice P i P^* sadrže svojstvene vrijednosti Schurovih idempotenta $A_0, \dots, A_d$. One su 0-1 matrice, pa im karakteristični polinomi imaju cjelobrojne koeficijente i vodeći koeficijent ± 1. Prema tome, svojstvene vrijednosti su algebarski cijeli brojevi. Poznato je da algebarski cijeli brojevi čine prsten, pa je i $\det(PP^*)$ algebarski cijeli broj. S desne strane izraza (22) je pozitivan racionalan broj, koji po sljedećoj lemi mora biti prirodan broj. $\square$

Lema 2.59. *Ako je algebarski cijeli broj racionalan, onda je cijeli broj.*

Dokaz. Neka je x algebarski cijeli broj, tj. nultočka polinoma $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ s cjelobrojnim koeficijentima $a_0, \dots, a_{n-1} \in \mathbb{Z}$. Pretpostavimo da je $x = \frac{a}{b}$ za $a \in \mathbb{Z} \setminus \{0\}$, $b \in \mathbb{N}$ i $M(a, b) = 1$. Tvrdimo da je tada $b = 1$, tj. $x \in \mathbb{Z}$. U suprotnom postoji prost broj p koji dijeli nazivnik b, a ne dijeli brojnik a. Uvrštavanjem x u polinom vidimo da je $a^n + a_{n-1}a^{n-1}b + \ldots + a_1 a b^{n-1} + a_0 b^n = 0$, tj. $a^n = -b(a_{n-1}a^{n-1} + \ldots + a_1 a b^{n-2} + a_0 b^{n-1})$. Broj p dijeli desnu stranu, a ne dijeli lijevu stranju, što je kontradikcija. $\square$

Zadatak 2.60. *Dokažite da je skup algebarskih cijelih brojeva zatvoren na zbrajanje, množenje i konjugiranje.*

U dokazu teorema 2.58 vidjeli smo da su svojsvene vrijednosti komutativne koherentne konfiguracije algebarski cijeli brojevi.

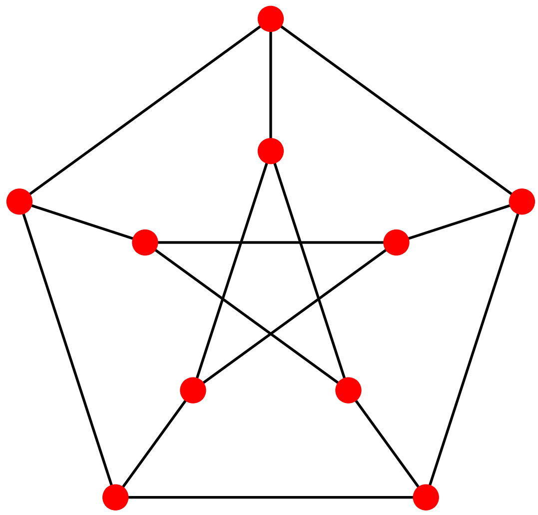
Propozicija 2.61. *Ako su sve svojstvene vrijednosti komutativne koherentne konfiguracije racionalni brojevi (prema tome i cijeli brojevi), onda je Frameov kvocijent* (22) *kvadrat prirodnog broja.*

Dokaz. U tom slučaju na lijevoj strani je $\det(PP^*) = \det(P)^2$. Po teoremu 2.58 to je prirodan broj, pa mora biti kvadrat prirodnog broja. $\square$

3 Asocijacijske sheme s dvije klase

3.1 Tablica dopustivih parametara

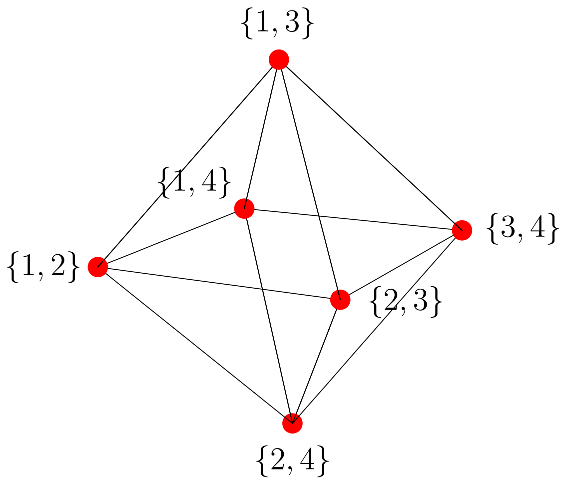
U cjelini 1.1 upoznali smo pojam jako regularnog grafa (definicija 1.9). Vidjeli smo primjer $m \times m$ topovskog grafa (primjer 1.10) s parametrima $SRG(m^2, 2m-2, m-2, 2)$. Shrikhandeov graf (slika 2) ima odgovarajuće parametre za $m = 4$, ali nije izomorfan 4×4 topovskom grafu. Poligon s n vrhova (slika 4) je jako regularan samo za $n = 4$ i $n = 5$. U tom slučaju parametri su $SRG(4, 2, 0, 2)$ i $SRG(5, 2, 0, 1)$. Petersenov graf (slika 8) također je jako regularan s parametrima $SRG(10, 3, 0, 1)$.



Slika 8: Petersenov graf je $SRG(10, 3, 0, 1)$.

Primjer 3.1 (Trokutni grafovi)**.** *Neka je $m \in \mathbb{N}$, $m \geq 4$. Za skup vrhova uzmemo dvočlane podskupove od $\{1, \ldots, m\}$, tj. $X = \{\{x, y\} \mid 1 \leq x < y \leq m\}$. Vrhovi $\{x, y\}$ i $\{x', y'\}$ su susjedni ako je $|\{x, y\} \cap \{x', y'\}| = 1$. Tako dobijemo jako regularan graf s parametrima $SRG(\binom{m}{2}, 2(m-2), m-2, 4)$. Zovemo ga* trokutnim grafom *(eng.* triangular graph*) i označavamo $T(m)$.*

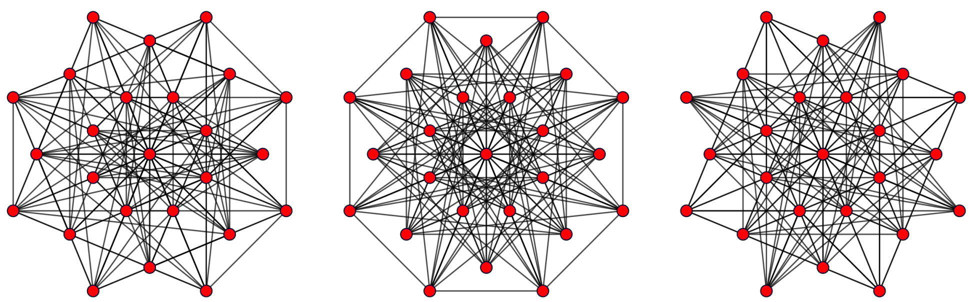
Trokutni graf $T(m)$ podudara se s Johnsonovim grafom $J(m, 2, 1)$ (primjer 1.5). Graf $T(4)$ je graf vrhova i bridova oktaedra (slika 9). Graf $T(5)$ je komplement Petersenova grafa. Za graf G sa skupom bridova B, *linijski graf* $L(G)$ (eng. *line graph*) ima B kao skup vrhova, a susjedni su ako su incidentni s istim vrhom iz G. Alternativno, $T(m)$ možemo definirati kao linijski graf potpunog grafa $L(K_m)$. Slično, $m \times m$ topovski graf je linijski graf potpunog bipartitnog grafa $L(K_{m,m})$. Još jedna sličnost je da su trokutni grafovi



Slika 9: Trokutni graf $T(4)$.

određeni svojim parametrima do na izomorfizam, osim u jednom slučaju. Sljedeći teorem analogan je Shrikhandeovu teoremu 1.14.

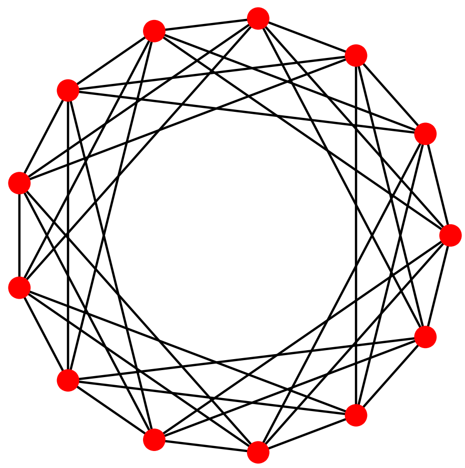
Teorem 3.2 (L. C. Chang [35, 36])**.** *Za $m \neq 8$, svaki jako regularan graf s parametrima $SRG(\binom{m}{2}, 2(m-2), m-2, 4)$ izomorfan je trokutnom grafu $T(m)$ iz primjera 3.1. Za $m = 8$ postoje još tri takva grafa prikazana na slici 10, koje zovemo* Changovim grafovima.



Slika 10: Changovi grafovi s parametrima $SRG(28, 12, 6, 4)$ (preuzeto s [135]).

Idući primjer jako regularnih grafova nazvan je po engleskom matematičaru R. E. A. C. Paleyu (1907.-1933.), a uveli su ih H. Sachs [110] te P. Erdős i A. Rényi [46]. Paley je na sličan način konstruirao Hadamardove matrice pomoću kvadrata u konačnom polju [104].

Primjer 3.3 (Paleyevi grafovi)**.** *Neka je $q \equiv 1 \pmod 4$ potencija prostog broja. Za skup vrhova uzmemo elemente konačnog polja $\mathbb{F}_q$. Vrhovi x i y su susjedni ako je $x - y$ kvadrat u $\mathbb{F}_q \setminus \{0\}$. Tako dobijemo jako regularan graf s parametrima $SRG(q, \frac{1}{2}(q-1), \frac{1}{4}(q-5), \frac{1}{4}(q-1))$.*



Slika 11: Paleyev graf $SRG(13, 6, 2, 3)$.

Zadatak 3.4. *Dokažite da konstrukcija iz primjera 3.3 zaista daje jako regularne grafove.*

Za male parametre Paleyevi grafovi također su jedinstveno određeni parametrima, ali za veće q broj neizomorfnih grafova $SRG(q, \frac{1}{2}(q-1), \frac{1}{4}(q-5), \frac{1}{4}(q-1))$ naglo raste. Točan broj poznat je do $q = 29$ [119], a za $q = 37$ i $q = 41$ poznate su donje ocjene [100, 38, 94]. Brojevi i ocjene navedene su u sljedećoj tablici.

Parametri	Broj	Parametri	Broj
$SRG(5, 2, 0, 1)$	1	$SRG(25, 12, 5, 6)$	15
$SRG(9, 4, 1, 2)$	1	$SRG(29, 14, 6, 7)$	41
$SRG(13, 6, 2, 3)$	1	$SRG(37, 18, 8, 9)$	$\geq$6802
$SRG(17, 8, 3, 4)$	1	$SRG(41, 20, 9, 10)$	$\geq$18439

Tablica 1: Broj neizomorfnih SRG-ova s Paleyevim parametrima.

Svi dosadašnji primjeri jako regularnih grafova su povezani. Primjer nepovezanog jako regularnog grafa je disjunktna unija $r > 1$ kopija potpunog grafa K_m, u oznaci $r \cdot K_m$. Taj graf ima parametre $SRG(rm, m-1, m-2, 0)$. Uočimo da je parametar $\mu = 0$.

Propozicija 3.5. *Jako regularan graf ima parametar $\mu = 0$ ako i samo ako je oblika $r \cdot K_m$.*

Dokaz. Zbog uvjeta $\mu = 0$, relacija susjedstva na skupu svih vrhova je tranzitivna. Možemo je proširiti do relacije ekvivalencije dodavanjem parova (x, x). Klase ekvivalencije particioniraju vrhove na disjunktnu uniju potpunih grafova, koji su jednako veliki zbog regularnosti. □

Propozicija 3.6. *Jako regularan graf s parametrima $SRG(n, \Bbbk, \lambda, \mu)$ je povezan ako i samo ako je $\mu > 0$.*

Dokaz. Svaka dva susjedna vrha povezana su šetnjom duljine 1. Nesusjedne vrhove zbog $\mu > 0$ povezuje šetnja duljine 2. Obrnuto, povezan jako regularan graf ne može imati parametar $\mu = 0$ jer bi po prethodnoj propoziciji bio oblika $r \cdot K_m$, a taj graf nije povezan. □

Komplement grafa $r \cdot K_m$ je potpuni multipartitini graf $K_{m,\ldots,m}$ (r indeksa m) s parametrima $SRG(rm, (r-1)m, (r-2)m, (r-1)m)$. Uočimo da mu parametri zadovoljavaju $\mu = \Bbbk$.

Propozicija 3.7. *Jako regularan graf $SRG(n, \Bbbk, \lambda, \mu)$ zadovoljava $\mu = \Bbbk$ ako i samo ako je izomorfan potpunom multipartitnom grafu $K_{m,\ldots,m}$.*

Dokaz. Neka je G jako regularan graf s $\mu = \Bbbk$. Tvrdimo da njegov komplement G^c ima parametar $\overline{\mu} = 0$. Po propoziciji 3.5, graf G^c je tada $r \cdot K_m$, pa je G potpuni multipartitni graf $K_{m,\ldots,m}$. Pretpostavimo suprotno, da u G^c postoje dva nesusjedna vrha x i y koja imaju zajedničkog susjeda z (tj. da je $\overline{\mu} > 0$). U grafu G tada vrijedi $x \sim y$ i $x \not\sim z \not\sim y$. Zbog uvjeta $\mu = \Bbbk$, skup svih susjeda $N(x)$ podudara se sa skupom $N(z)$. To je kontradikcija s $y \in N(x)$ i $y \notin N(z)$. □

Time smo potpuno karakterizirali jako regularne grafove s $\mu = 0$ ili $\mu = \Bbbk$, koje zovemo *imprimitivnima*. Zanimljiviji su *primitivni* jako regularni grafovi, koji zadovoljavaju $0 < \mu < \Bbbk$. U nastavku je cilj izvesti nužne uvjete na parametre jako regularnog grafa $SRG(n, \Bbbk, \lambda, \mu)$. U propoziciji 1.13 dvostrukim prebrojavanjem dokazali smo jednakost

$$\Bbbk(\Bbbk - \lambda - 1) = (n - \Bbbk - 1)\mu. \tag{23}$$

Zadatak 3.8. *Neka jako regularan graf G ima broj vrhova oblika $n = p + 1$, pri čemu je p prost broj. Dokažite da je tada G imprimitivan.*

Rješenje. Iz jednadžbe (23) slijedi $\Bbbk(\Bbbk - \lambda - 1) = (p - \Bbbk)\mu$. Zbog toga što je p prost, vidimo da je $M(\Bbbk, p - \Bbbk) = 1$. Zato $\Bbbk$ dijeli μ, pa iz $\mu \leq \Bbbk$ slijedi $\mu = \Bbbk$ ili $\mu = 0$. □

Mnoge nužne uvjete za egzistenciju jako regularnih grafova ne možemo dokazati kombinatorno. Snažan alat su algebarski dokazi koji se zasnivaju na činjenici da su jako regularni grafovi ekvivalentni asocijacijskim shemama s dvije klase (teorem 1.12). Ako je A matrica susjedstva grafa s parametrima $SRG(n, \Bbbk, \lambda, \mu)$, matrice $A_0 = I$, $A_1 = A$ i matrica susjedsva komplementarnog grafa $A_2 = J - I - A$ su Schurove idempotente asocijacijske sheme s dvije klase. Stupnjevi te sheme su $n_0 = 1$, $n_1 = \Bbbk$ i $n_2 = n - 1 - \Bbbk$. U dokazu teorema 1.12 vidjeli smo da su presječni brojevi

$$p_{11}^0 = \Bbbk, \qquad p_{11}^1 = \lambda, \qquad p_{11}^2 = \mu.$$

Iz 4. svojstva u definiciji 2.1 slijedi da matrica susjedstva zadovoljava

$$A^2 = \Bbbk I + \lambda A + \mu(J - I - A). \tag{24}$$

Relacija (24) slijedi i direktno iz sljedeće važne leme iz teorije grafova.

Lema 3.9. *Neka je A matrica susjedstva grafa G. Element na mjestu (i, j) potencije A^k jednak je broju šetnji duljine k od i-tog do j-tog vrha u grafu G.*

Broj šetnji duljine 2 od vrha do samog sebe jednak je stupnju tog vrha, pa za regularan graf matrica A^2 na dijagonali ima stupanj $\Bbbk$. Za $i \neq j$, broj šetnji duljine 2 jednak je broju zajedničkih susjeda i-tog i j-tog vrha. Ako je graf jako regularan, matrica A^2 izvan dijagonale ima λ ako su i-ti i j-ti vrh susjedni, a inače ima μ. Vidimo da je relacija (24) matrični zapis definicijskih svojstava jako regularnog grafa.

Za $\Bbbk$-regularan graf, vektor jedinica $\mathbb{1}$ je svojstveni vektor matrice susjedstva A pridružen svojstvenoj vrijednosti $\Bbbk$. Množenjem relacije (24) s $\mathbb{1}$ dobijemo $\Bbbk^2 \mathbb{1} = (\Bbbk + \lambda \Bbbk + \mu(n - 1 - \Bbbk))\mathbb{1}$, tj. $\Bbbk(\Bbbk - 1 - \lambda) = \mu(n - 1 - \Bbbk)$. To je algebarski dokaz relacije (23).

Neka je $x \neq \Bbbk$ neka druga svojstvena vrijednost od A i e odgovarajući svojstveni vektor. Matrica A je simetrična, pa su svojstveni vektori e i $\mathbb{1}$ ortogonalni, jer su pridruženi različitim svojstvenim vrijednostima. Zato je $Je = 0$ (reci matrice J su $\mathbb{1}$ i ortogonalni su na e). Množenjem relacije (24) s e dobijemo $x^2 e = \Bbbk e + \lambda x e + \mu(-e - xe) = (\Bbbk + \lambda x - \mu - \mu x)e$, tj.

$$x^2 + (\mu - \lambda)x + \mu - \Bbbk = 0. \tag{25}$$

Ako je graf povezan i nije potpun, pokazuje se da osim $\Bbbk$ ima bar još dvije svojstvene vrijednosti. Tada su oba rješenja kvadratne jednadžbe (25) svojstvene vrijednosti i možemo ih zapisati kao

$$\begin{aligned} r &= \frac{\lambda - \mu + \sqrt{(\lambda - \mu)^2 + 4(\Bbbk - \mu)}}{2}, \\ s &= \frac{\lambda - \mu - \sqrt{(\lambda - \mu)^2 + 4(\Bbbk - \mu)}}{2}. \end{aligned} \tag{26}$$

Vieteove formule daju nam vezu između parametara i svojstvenih vrijednosti jako regularnog grafa:

$$r + s = \lambda - \mu, \qquad rs = \mu - \Bbbk. \tag{27}$$

Iz druge jednadžbe vidimo da su za primitivan graf (s $0 < \mu < \Bbbk$) svojstvene vrijednosti suprotnog predznaka. Uobičajeno je označiti ih kao u (26), tako da je $s < 0 < r$.

Zadatak 3.10. *Odredite spektar nepovezanog jako regularnog grafa (s $\mu = 0$) te imprimitivnog jako regularnog grafa s $\mu = \Bbbk$.*

Zadatak 3.11. *Neka je $G \neq K_n$ povezan $\Bbbk$-regularan graf. Dokažite da je G jako regularan ako i samo ako ima točno tri svojstvene vrijednosti (od kojih je jedna $\Bbbk$).*

U slučaju jako regularnog grafa, jednadžbe (10) svode se na

$$A_0 = E_0 + E_1 + E_2, \qquad A_1 = \Bbbk E_0 + rE_1 + sE_2.$$

Budući da je $A_2 = J - I - A_1 = nE_0 - E_0 - E_1 - E_2 - A_1$, dobivamo

$$A_2 = (n - 1 - \Bbbk)E_0 - (r + 1)E_1 - (s + 1)E_2.$$

Time smo odredili svojstvenu matricu jako regularnog grafa:

$$P = \begin{bmatrix} 1 & \Bbbk & n-1-\Bbbk \\ 1 & r & -r-1 \\ 1 & s & -s-1 \end{bmatrix}. \tag{28}$$

Iz propozicije 2.27 možemo izračunati dualnu svojstvenu matricu:

$$Q = \begin{bmatrix} 1 & \frac{-\Bbbk-(n-1)s}{r-s} & \frac{\Bbbk+(n-1)r}{r-s} \\ 1 & \frac{n-\Bbbk+s}{r-s} & \frac{\Bbbk-n-r}{r-s} \\ 1 & \frac{s-\Bbbk}{r-s} & \frac{\Bbbk-r}{r-s} \end{bmatrix} = \begin{bmatrix} 1 & f & g \\ 1 & f\,\frac{r}{\Bbbk} & g\,\frac{s}{\Bbbk} \\ 1 & -f\,\frac{r+1}{n-1-\Bbbk} & -g\,\frac{s+1}{n-1-\Bbbk} \end{bmatrix}. \tag{29}$$

U prvom retku matrice Q su kratnosti $m_0 = 1$, $m_1 = \frac{-\Bbbk-(n-1)s}{r-s}$ i $m_2 = \frac{\Bbbk+(n-1)r}{r-s}$. Uobičajeno je kratnost svojstvenih vrijednosti r i s označiti redom $f = m_1$ i $g = m_2$. Uvrštavanjem (26) i sređivanjem dobivamo formule

$$\begin{aligned} f &= \frac{1}{2}\left(n - 1 + \frac{(n-1)(\mu-\lambda) - 2\Bbbk}{\sqrt{(\lambda-\mu)^2 + 4(\Bbbk-\mu)}}\right), \\ g &= \frac{1}{2}\left(n - 1 - \frac{(n-1)(\mu-\lambda) - 2\Bbbk}{\sqrt{(\lambda-\mu)^2 + 4(\Bbbk-\mu)}}\right). \end{aligned} \tag{30}$$

Iz činjenice da su kratnosti prirodni brojevi dobivamo snažan uvjet za egzistenciju jako regularnog grafa.

Propozicija 3.12. *Ako postoji jako regularan graf* $SRG(n, \mathscr{k}, \lambda, \mu)$*, onda su izrazi* (30) *prirodni brojevi.*

Prva stranica Brouwerowe tablice [19] sadrži dopustive parametre jako regularnih grafova s $n \leq 50$ vrhova. Da bismo ih generirali, uzimamo redom $n = 4, \ldots, 50$. Za svaki n, uzimamo $\mathscr{k} = 2, \ldots, \lfloor n/2 \rfloor$. Ograničit ćemo se na jedan od dva međusobno komplementarna grafa, pa možemo pretpostaviti $2k \leq n$. Brouwerova tablica sadrži parove komplementarnih parametara na uzastopnim mjestima. Za svaki n i $\mathscr{k}$, uzimamo $\lambda = 0, \ldots, \mathscr{k}$ i iz (23) izračunamo $\mu = \frac{\mathscr{k}(\mathscr{k}-\lambda-1)}{n-\mathscr{k}-1}$. Tako dobivamo 6052 četvorki $(n, \mathscr{k}, \lambda, \mu)$, ali u mnogima parametar μ nije cijeli broj. Ako izbacimo sve takve četvorke i sve četvorke koje odgovaraju imprimitivnim grafovima (s $\mu = 0$ ili $\mu = \mathscr{k}$), ostaje 480 četvorki. To su mogući parametri primitivnih jako regularnih grafova koji zadovoljavaju uvjet (23). Uvjet iz propozicije 3.12 elimina sve osim 37 od tih 480 četvorki. Među njima je jedan par komplementarnih četvorki $(21, 10, 3, 6)$ i $(21, 10, 4, 5)$ s istim parametrom $\mathscr{k}$, od kojih izbacimo drugu. Preostalih 36 četvorki odgovara parovima komplementarnih parametara na prvoj stranici Brouwerove tablice [19]. Navodimo ih u tablici 2.

Rbr	n	$\mathscr{k}$	λ	μ	r	s	f	g	Broj	Napomena
1	5	2	0	1	$\frac{-1\pm\sqrt{5}}{2}$		2	2	1	Paley(5)
2	9	4	1	2	1	-2	4	4	1	Paley(9)
3	10	3	0	1	1	-2	5	4	1	Petersen= $T(5)^c$
4	13	6	2	3	$\frac{-1\pm\sqrt{13}}{2}$		6	6	1	Paley(13)
5	15	6	1	3	1	-3	9	5	1	$T(6)^c$
6	16	5	0	2	1	-3	10	5	1	
7	16	6	2	2	2	-2	6	9	2	4×4, Shrikhande
8	17	8	3	4	$\frac{-1\pm\sqrt{17}}{2}$		8	8	1	Paley(17)
9	21	10	3	6	1	-4	14	6	1	$T(7)^c$
10	21	10	4	5	$\frac{-1\pm\sqrt{21}}{2}$		10	10	0	Tm. 3.18
11	25	8	3	2	3	-2	8	16	1	5×5
12	25	12	5	6	2	-3	12	12	15	Paley(25)

Tablica 2: Dopustivi parametri primitivnih SRG-ova.

Rbr	n	k	λ	μ	r	s	f	g	Broj	Napomena
13	26	10	3	4	2	-3	13	12	10	
14	27	10	1	5	1	-5	20	6	1	
15	28	9	0	4	1	-5	21	6	0	(32), Prop. 3.21
16	28	12	6	4	4	-2	7	20	4	$T(8)$, Chang
17	29	14	6	7	$\frac{-1\pm\sqrt{29}}{2}$		14	14	41	Paley(29)
18	33	16	7	8	$\frac{-1\pm\sqrt{33}}{2}$		16	16	0	Tm. 3.18
19	35	16	6	8	2	-4	20	14	3854	
20	36	10	4	2	4	-2	10	25	1	6×6
21	36	14	4	6	2	-4	21	14	180	
22	36	14	7	4	5	-2	8	27	1	$T(9)$
23	36	15	6	6	3	-3	15	20	32548	
24	37	18	8	9	$\frac{-1\pm\sqrt{37}}{2}$		18	18	$\geq$6802	Paley(37)
25	40	12	2	4	2	-4	24	15	28	
26	41	20	9	10	$\frac{-1\pm\sqrt{41}}{2}$		20	20	$\geq$18439	Paley(41)
27	45	12	3	3	3	-3	20	24	78	
28	45	16	8	4	6	-2	9	35	1	$T(10)$
29	45	22	10	11	$\frac{-1\pm 3\sqrt{5}}{2}$		22	22	+	[97]
30	49	12	5	2	5	-2	12	36	1	7×7
31	49	16	3	6	2	-5	32	16	0	[22]
32	49	18	7	6	4	-3	18	30	$\geq$727	[37]
33	49	24	11	12	3	-4	24	24	+	Paley(49)
34	50	7	0	1	2	-3	28	21	1	
35	50	21	4	12	1	-9	42	7	0	Prop. 3.21
36	50	21	8	9	3	-4	25	24	+	

Tablica 2: Dopustivi parametri primitivnih SRG-ova.

Prvo navodimo redni broj i parametre (n, k, λ, μ), zatim svojstvene vrijednosti r i s izračunate iz (26) te kratnosti f i g izračunate iz (30). Slijedi broj neizomorfnih grafova s tim parametrima prepisan iz Brouwerove tablice [19] (oznaka "+" znači da postoji barem jedan graf) te napomena. Zeleno su obojani reci s grafovima za koje smo opisali konstrukciju u nekom od primjera. Topovski graf iz primjera 1.10 označen je $m \times m$, trokutni graf iz primjera 3.1 $T(m)$, a Paleyev graf iz primjera 3.3 Paley(q). Bijeli su reci u kojima je poznato da grafovi postoje, ali nismo ih susreli u primjerima. Konačno, u crvenim recima poznato je da grafovi ne postoje, iako parametri zadovoljavaju uvjete koje smo do sada spomenuli. Propozicije 1.13 i 3.12 su samo nužni, ali ne i dovoljni uvjeti za egzistenciju jako regularnih grafova.

3.2 Još neki nužni uvjeti za jako regularne grafove

Promotrimo parametre $SRG(28, 9, 0, 4)$ u 15. retku tablice 2. Iz formula (26) izračunamo svojstvene vrijednosti $r = 1$, $s = -5$ i tada znamo prvu tablicu karaktera

$$P = \begin{bmatrix} 1 & 9 & 18 \\ 1 & 1 & -2 \\ 1 & -5 & 4 \end{bmatrix}.$$

Iz formula (30) dobivamo kratnosti $f = 21$ i $g = 6$. Sada iz formula (19) možemo izračunati Kreinove parametre. Parametar $q_{22}^2 = -4/9$ je negativan, pa po teoremu 2.50 zaključujemo da jako regularni grafovi s tim parametrima ne postoje. Za komplementarne parametre $SRG(28, 18, 12, 10)$ negativan je Kreinov parametar $q_{11}^1 = -4/9$.

Za opće parametre $SRG(n, \Bbbk, \lambda, \mu)$, po formuli (19) dobivamo

$$q_{11}^1 = \frac{f^2}{n}\left(1 + \frac{r^3}{\Bbbk^2} - \frac{(r+1)^3}{(n-1-\Bbbk)^2}\right), \quad q_{22}^2 = \frac{g^2}{n}\left(1 + \frac{s^3}{\Bbbk^2} - \frac{(s+1)^3}{(n-1-\Bbbk)^2}\right).$$

Po Kreinovu uvjetu, izrazi u zagradi moraju biti nenegativni:

$$(r+1)^3\Bbbk^2 \leq (n-1-\Bbbk)^2(\Bbbk^2 + r^3),$$
$$(s+1)^3\Bbbk^2 \leq (n-1-\Bbbk)^2(\Bbbk^2 + s^3).$$

Uvjeti se mogu zapisati na ekvivalentan način.

Propozicija 3.13. *Ako postoji jako regularan graf $SRG(n, \Bbbk, \lambda, \mu)$ sa svojstvenim vrijednostima r i s, onda vrijedi*

$$(r+1)(\Bbbk + r + 2rs) \leq (\Bbbk + r)(s+1)^2, \tag{31}$$
$$(s+1)(\Bbbk + s + 2rs) \leq (\Bbbk + s)(r+1)^2. \tag{32}$$

Za ostale Kreinove parametre dobivamo formule koje su uvijek nenegativne. Promotrimo sada pobliže izraze za kratnosti (30). U nazivniku imamo korijen iz diskriminante kvadratne jednadžbe (25). Ako izraz u brojniku

$(n-1)(\mu-\lambda)-2\Bbbk$ nije nula, nazivnik mora biti cijeli broj da bi f i g bili prirodni brojevi, tj. diskriminanta $(\lambda-\mu)^2+4(\Bbbk-\mu)$ mora biti kvadrat prirodnog broja. Tada su svojstvene vrijednosti (26) racionalne. U dokazu teorema 2.58 vidjeli smo da su svojstvene vrijednosti algebarski cijeli brojevi, pa iz leme 2.59 slijedi da su r i s cijeli brojevi. Za takve jako regularne grafove kažemo da su *tipa II*.

Jako regularne grafove za koje je $(n-1)(\mu-\lambda)-2\Bbbk=0$ zovemo *grafovima tipa I*. Tada je $f=g=\frac{n-1}{2}$ i $\Bbbk=\frac{n-1}{2}(\mu-\lambda)$. No kako je $\Bbbk<n-1$, zaključujemo da je $\mu-\lambda=1$ i $\Bbbk=\frac{n-1}{2}$. Iz jednadžbe (23) slijedi $\mu=\frac{\Bbbk}{2}=\frac{n-1}{4}$ i $\lambda=\mu-1=\frac{n-5}{4}$. Parametri su oblika

$$SRG(n,\tfrac{n-1}{2},\tfrac{n-5}{4},\tfrac{n-1}{4})=SRG(4t+1,2t,t-1,t)$$

za prirodan broj t, a svojstvene vrijednosti su $r,s=(-1\pm\sqrt{n})/2$. Grafovi tipa I nazivaju se još i "*half case*" ili *konferencijski grafovi.* Paleyevi grafovi iz primjera 3.3 su tog tipa, pa konferencijski grafovi postoje uvijek kad je broj vrhova n prim potencija.

Zadatak 3.14. *Neka jako regularan graf G ima prost broj $n=p$ kao broj vrhova. Dokažite da je tada G konferencijski graf.*

Rješenje. Pretpostavimo suprotno, da je G graf tipa II. Vidjeli smo da su tada njegove svojstvene vrijednosti cjelobrojne, pa je po propoziciji 2.61 Frameov kvocijent kvadrat prirodnog broja. Za jako regularan graf Frameov kvocijent je

$$n^3\,\frac{n_0n_1n_2}{m_0m_1m_2}=p^3\,\frac{\Bbbk(p-\Bbbk-1)}{fg}.$$

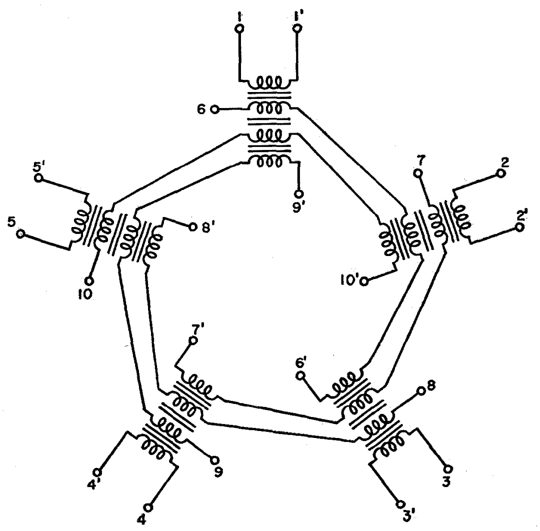
Razlomak u gornjem izrazu je prirodan broj i nije djeljiv s p, jer su u brojniku i u nazivniku faktori manji od p. Zato p ima eksponent 3 u rastavu na proste faktore Frameova kvocijenta, što nije moguće ako je kvadrat. Dakle, G mora biti tipa I, tj. konferencijski graf. $\square$

Kao što vidimo iz retka 29 tablice 2, konferencijski grafovi mogu postojati i kad n nije prim potencija. Najmanji primjeri s parametrima $SRG(45,22,10,11)$ su članovi beskonačne familije koju je konstruirao Rudi Mathon[18] [97]. Najmanji parametri za koje je egzistencija otvorena su $SRG(85,42,20,21)$. Objasnimo sada od kuda potječe naziv "konferencijski grafovi".

Definicija 3.15. Konferencijska matrica *reda n je $C\in M_n(\mathbb{C})$ koja na dijagonali ima 0, a izvan dijagonale ±1, takva da su joj reci međusobno ortogonalni: $CC^t=(n-1)I$.*

[18]Rudolf Anton Mathon (1940.-2022.), češko-kanadski matematičar.

Belgijski matematičar i inženjer elektrotehnike Vitold Belevitch (1921.-1999.) uveo je konferencijske matrice u članku [7], vezano uz problem izrade telefonskih mreža za konferencijske pozive, kod kojih svaki sudionik čuje svakog drugog sudionika. Na slici 12 prikazana je jedna takva mreža iz Belevitcheva članka i konferencijska matrica reda 10.



$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & - & 1 & - & 1 & - & 1 & - \\ 1 & 1 & 0 & 1 & - & 1 & 1 & - & - & - \\ 1 & - & 1 & 0 & - & 1 & - & - & 1 & 1 \\ 1 & 1 & - & - & 0 & 1 & - & 1 & 1 & - \\ 1 & - & 1 & 1 & 1 & 0 & - & 1 & - & - \\ 1 & 1 & 1 & - & - & - & 0 & 1 & - & 1 \\ 1 & - & - & - & 1 & 1 & 1 & 0 & - & 1 \\ 1 & 1 & - & 1 & 1 & - & - & - & 0 & 1 \\ 1 & - & - & 1 & - & - & 1 & 1 & 1 & 0 \end{bmatrix}$$

Slika 12: Idealna konferencijska telefonska mreža (slika preuzeta iz [7]) i konferencijska matrica reda 10.

Množenje redaka i stupaca s -1 čuva definicijska svojstva konferencijske matrice. Tako možemo postići da elementi iz prvog retka i stupca budu jedinice, osim prve nule, a konferencijsku matricu tog oblika zovemo *normaliziranom*. Neka je S matrica dobivena brisanjem prvog retka i stupca normalizirane konferencijske matrice C. Zovemo je *jezgrom* od C.

Teorem 3.16. *Neka je C normalizirana konferencijska matrica reda n i S njezina jezgra. Ako je $n > 1$, onda je n paran. Ako je $n \equiv 2 \pmod 4$, onda je $S = S^t$ simetrična matrica. Ako je $n \equiv 0 \pmod 4$, onda je $S = -S^t$ antisimetrična matrica.*

Dokaz. Prva dva retka matrice C su ovog oblika:

$$\begin{matrix} 0 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 0 & \pm 1 & \pm 1 & \cdots & \pm 1 \end{matrix}$$

U drugom retku na mjestima označenim ± 1 mora biti jednak broj elemenata 1 i -1, da bi bio ortogonalan na prvi redak. Ako je taj broj m, onda je $n = 2m + 2$ paran broj.

Neka je $C = [c_{ij}]$ i neka su $i, j \in \{2, \ldots, n\}$, $i < j$. Pokazat ćemo da vrijede implikacije $c_{ij} = c_{ji} \Rightarrow n \equiv 2 \pmod 4$ i $c_{ij} = -c_{ji} \Rightarrow n \equiv 0 \pmod 4$. Iz toga slijedi da u slučaju $n \equiv 2 \pmod 4$ matrica S mora biti simetrična, a u slučaju $n \equiv 0 \pmod 4$ antisimetrična.

Promotrimo prvi, i-ti i j-ti redak matrice C:

$$\begin{array}{ccccccccc} 0 & 1 & \cdots & 1 & \cdots & 1 & \cdots & 1 \\ 1 & \pm 1 & \cdots & 0 & \cdots & c_{ij} & \cdots & \pm 1 \\ 1 & \pm 1 & \cdots & c_{ji} & \cdots & 0 & \cdots & \pm 1 \end{array}$$

Neka je n_{++} broj stupaca različitih od prvog, i-tog i j-tog stupca, u kojima su u i-om i j-tom retku unosi 1. Slično, n_{+-} je broj takvih stupaca u kojima je u i-tom retku 1, a u j-tom retku -1. Analogno definiramo n_{-+} i n_{--}. Zbog međusobne ortogonalnosti i-tog i j-tog retka vrijedi $n_{+-} + n_{-+} = m$. Ako je $c_{ij} = 1$, onda zbog ortogonalnosti prvog i i-tog retka slijedi $n_{++} + n_{+-} = m - 1$. Ako je $c_{ij} = -1$, onda zbog istog razloga slijedi $n_{++} + n_{+-} = m$. Analogno, zbog ortogonalnosti prvog i j-tog retka vrijedi $c_{ji} = 1 \Rightarrow n_{++} + n_{-+} = m - 1$ te $c_{ji} = -1 \Rightarrow n_{++} + n_{-+} = m$.

Sada pretpostavimo $c_{ij} = c_{ji}$ i uzmimo da je na tim mjestima 1. Tada iz $n_{++} + n_{+-} = m - 1$ i $n_{++} + n_{-+} = m - 1$ slijedi $n_{+-} = n_{-+}$, što uvrštavanjem u jednadžbu $n_{+-} + n_{-+} = m$ daje $m = 2n_{+-}$, odnosno $n = 2m + 2 = 4n_{+-} + 2 \equiv 2 \pmod 4$. Isti zaključak dobivamo za $c_{ij} = c_{ji} = -1$. Ako pak pretpostavimo $c_{ij} = -c_{ji}$, dobivamo $m = 2n_{+-} + 1$ ili $m = 2n_{+-} - 1$, što daje $n \equiv 0 \pmod 4$. $\square$

Teorem 3.17. *Konferencijska matrica C reda $n \equiv 2 \pmod 4$ postoji ako i samo ako postoji konferencijski graf s parametrima $SRG(4t+1, 2t, t-1, t)$, za $t = (n-2)/4$.*

Dokaz. Normaliziramo C i neka je S njezina jezgra. Po prethodnom teoremu, S je simetrična matrica reda $n-1$. Neka je A matrica dobivena iz S zamjenom svih unosa -1 sa 0. Vezu možemo izraziti kao $S = A - (J - I - A) = 2A - J + I$. Iz jednadžbe $CC^t = (n-1)I$ slijedi $S\mathbb{1} = 0$ i $SS^t = (n-1)I - J$. Prva jednadžba znači da u svakom retku od S ima jednak broj jedinica i minus jedinica, koji smo u prethodnom dokazu označili m. Iz prethodnog dokaza također znamo da je $m = 2t$ paran, odnosno $n = 4t + 2$. Sada uvrštavanjem $S = 2A - J + I$ u $SS^t = (n-1)I + J$ dobivamo

$$A^2 = tI - A + tJ = 2tI + (t-1)A + t(J - I - A),$$

a to je upravo jednadžba (24) za $\Bbbk = 2t$, $\lambda = t - 1$ i $\mu = t$. Dakle, A je matrica susjedstva jako regularnog grafa s parametrima $SRG(4t+1, 2t, t-1, t)$.

Obratno, ako imamo matricu susjedstva A grafa s tim parametrima, zamijenimo nule izvan dijagonale s -1 i "obrubimo" matricu retkom i stupcom jedinica s nulom na prvom mjestu. Tako dobivamo konferencijsku matricu reda $n \equiv 2 \pmod 4$. $\square$

Belevitch [7] je uočio sljedeći nužan uvjet za egzistenciju konferencijske matrice reda $n \equiv 2 \pmod 4$, odnosno konferencijskog grafa.

Teorem 3.18. *Ako postoji jako regularan graf s parametrima $SRG(4t+1, 2t, t-1, t)$, onda je $4t+1$ zbroj kvadrata dvaju cijelih brojeva.*

Raghavarao[19] [106] je dokazao taj uvjet pomoću Hasse[20]-Minkowskijevog[21] teorema o kvadratnim formama. U Rijeci je nedavno održana radionica o ovoj teoriji [103]. Elementarni dokaz dali su van Lint[22] i Seidel[23] [128]. Teorem 3.18 vrlo je sličan Bruck-Ryserovu teoremu 1.32 i oba se dokazuju na slične načine. Iz teorije brojeva poznat je sljedeći kriterij za uvjet iz tih teorema.

Teorem 3.19 (Fermat[24])**.** *Prirodan broj n može se prikazati kao zbroj kvadrata dvaju cijelih brojeva ako i samo ako u rastavu broja n na proste faktore svi faktori oblika $p \equiv 3 \pmod 4$ imaju parne eksponente.*

Na primjer, broj $21 = 3 \cdot 7$ ne može se prikazati kao zbroj dvaju kvadrata jer se faktor 3 javlja s eksponentom 1 (a to se lako provjeri i direktno). Isto vrijedi za broj $33 = 3 \cdot 11$. Zato konferencijski grafovi s parametrima iz 10. i 18. retka tablice 2 ne postoje. Parametri iz 29. retka zadovoljavaju uvjet: $45 = 3^2 + 6^2$. Iz toga ne slijedi direktno postojanje grafova, naime teorem 3.18 je također samo nužan uvjet.

Zadatak 3.20. *U primjeru 3.3 vidjeli smo da konferencijski grafovi postoje uvijek kad je broj vrhova $4t+1$ potencija prostog broja. Iz toga i teorema 3.18 slijedi da se svaka prim potencija tog oblika može prikazati kao zbroj dvaju kvadrata. Dokažite to direktno iz Fermatovog teorema 3.19.*

Još jedan nužan uvjet za postojanje jako regularnih grafova je takozvana *apsolutna ocjena.*

---

[19] Damaraju Raghavarao (1938.-2013.), indijski statističar.
[20] Helmut Hasse (1898.-1979.), njemački matematičar.
[21] Hermann Minkowski (1864.-1909.), njemački matematičar.
[22] Jacobus Hendricus "Jack" van Lint (1932.-2004.), nizozemski matematičar.
[23] Johan Jacob "Jaap" Seidel (1919.-2001.), nizozemski matematičar.
[24] Pierre de Fermat (1607.-1665.), francuski matematičar.

Propozicija 3.21 (Apsolutna ocjena). *Ako postoji primitivan jako regularan graf $SRG(n, \Bbbk, \lambda, \mu)$ s kratnostima f i g, onda vrijedi*

$$n \leq \tfrac{1}{2} f(f+3) \quad i \quad n \leq \tfrac{1}{2} g(g+3). \tag{33}$$

Apsolutna ocjena eliminira grafove s parametrima iz 15. i 35. retka tablice 2, a slijedi iz općenitog uvjeta na kratnosti komutativne koherentne konfiguracije.

Teorem 3.22. *Neka su $m_0, \ldots, m_d$ kratnosti komutativne koherentne konfiguracije s d klasa i neka su zadani $i, j \in \{0, \ldots, d\}$. Tada vrijedi*

$$\sum_{q_{ij}^k \neq 0} m_k \leq \begin{cases} m_i m_j, & \text{ako je } i \neq j, \\ \frac{1}{2} m_i(m_i+1), & \text{ako je } i = j, \end{cases} \tag{34}$$

pri čemu na lijevoj strani sumiramo po svim indeksima $k \in \{0, \ldots, d\}$ za koje Kreinov parametar q_{ij}^k nije jednak nula.

Dokaz. Neka su $E_0, \ldots, E_d$ primitivne idempotente. Sjetimo se da je $m_i = \operatorname{rk} E_i$ i vrijedi $E_i \circ E_j = \frac{1}{n} \sum_{k=0}^{n} q_{ij}^k E_k$. Lijevu stranu od (34) dobijemo kao $\operatorname{rk}(E_i \circ E_j)$. U dokazu leme 2.49 vidjeli smo da je Schurov produkt $E_i \circ E_j$ glavna podmatrica Kroneckerova produkta $E_i \otimes E_j$. Zato je $\operatorname{rk}(E_i \circ E_j) \leq \operatorname{rk}(E_i \otimes E_j) = \operatorname{rk}(E_i) \operatorname{rk}(E_j) = m_i m_j$, što daje nejednakost za $i \neq j$.

Ako je $i = j$, elementi od $E_i \circ E_i$ su kvadrati elemenata od E_i. Neka je $A = [a_{ij}] \in M_n(\mathbb{C})$ proizvoljna matrica ranga r. Označimo njezine retke $a_i = (a_{i1}, \ldots, a_{in})$, $i = 1, \ldots, n$ i bez smanjenja općenitosti pretpostavimo da su prvih r redaka linearno nezavisni. Tada za svaki redak a_i postoje skalari $\beta_1, \ldots, \beta_r \in \mathbb{C}$ takvi da je $a_i = \sum_{k=1}^{r} \beta_k a_k$. Uzmimo j-tu komponentu ove vektorske jednakosti i kvadriramo je:

$$(a_{ij})^2 = \left(\sum_{k=1}^{r} \beta_k a_{kj} \right)^2 = \sum_{k=1}^{r} \beta_k^2 (a_{kj})^2 + \sum_{1 \leq k < \ell \leq r} 2 \beta_k \beta_\ell a_{kj} a_{\ell j}.$$

Ovo vrijedi za $j = 1, \ldots, n$, pa je vektor $a_i \circ a_i$ (i-ti redak Schurova produkta $A \circ A$) linearna kombinacija vektora $a_k \circ a_k$ za $k = 1, \ldots, r$ i vektora $a_k \circ a_\ell$ za $1 \leq k < \ell \leq r$. Prema tome, rang $\operatorname{rk}(A \circ A)$ je manji ili jednak od $r + \binom{r}{2} = \frac{1}{2} r(r+1)$. Primjenom na $A = E_i$ i $r = m_i$ slijedi nejednakost za $i = j$. □

Dokaz propozicije 3.21. Primijenimo prethodni teorem za $i = j = 1$ na primitivan jako regularan graf. Prije propozicije 3.13 izrazili smo Kreinov parametar q_{11}^1, a sada izrazimo još i

$$q_{11}^0 = \frac{f^2}{n} \left(1 + \frac{r^2}{\Bbbk^2} + \frac{(r+1)^2}{(n-1-\Bbbk)^2} \right), \quad q_{11}^2 = \frac{f^2}{n} \left(1 + \frac{r^2 s}{\Bbbk^2} - \frac{(r+1)^2 (s+1)}{(n-1-\Bbbk)^2} \right).$$

Iz prvog izraza odmah vidimo da je $q_{11}^0 > 0$, a iz drugog izraza uz malo više truda vidimo $q_{11}^2 > 0$. S druge strane, $q_{11}^2 = 0$ ako i samo ako graf dostiže Kreinov uvjet (31). Stoga, uvijek vrijedi $m_0 + m_2 \leq \frac{1}{2}m_1(m_1+1)$, tj. $1 + g \leq \frac{1}{2}f(f+1)$. Dodavanjem f na lijevu i desnu stranu dobivamo $n = 1+f+g \leq \frac{1}{2}f(f+3)$. Za grafove koji ne dostižu Kreinov uvjet (31) vrijedi stroža nejednakost $n \leq \frac{1}{2}f(f+1)$. Razmatranjem Kreinovih parametara q_{22}^0, q_{22}^1 i q_{22}^2 na isti način dobivamo $n \leq \frac{1}{2}g(g+3)$. □

Time smo dokazali nepostojanje grafova za sve crvene retke tablice 2, osim za redak 31. Graf $SRG(49, 16, 3, 6)$ eliminirali su Bussemaker, Haemers, Mathon, i Wilbrink [22] 'ad hoc' dokazom koji vrijedi samo za te parametre.

3.3 Euklidska reprezentacija

U ovoj cjelini dat ćemo drugi, "geometrijski" dokaz apsolutne ocjene. Za jako regularne grafove, kao i za druge asocijacijske sheme (simetrične koherentne konfiguracije), Bose-Mesnerovu algebru možemo promatrati nad poljem $\mathbb{R}$ umjesto nad poljem $\mathbb{C}$. Schurove idempotente $A_0, \ldots, A_d$ su simetrične matrice, pa su njihove svojstvene vrijednosti i svojstveni vektori realni. Zato su i primitivne idempotente $E_0, \ldots, E_d$ realne matrice. Matricu susjedstva jako regularnog grafa možemo zapisati kao $A = \Bbbk E_0 + rE_1 + sE_2$. Pritom su E_0, E_1 i E_2 matrice ortogonalnih projekcija na svojstvene potprostore $V_0 = [\mathbb{1}]$, V_1 i V_2, koji su dimenzija 1, f i g. Vrhove grafa možemo identificirati s vektorima $e_1, \ldots, e_n$ kanonske baze od $\mathbb{R}^n$, a i-ti i j-ti vrh su susjedni ako i samo ako je $e_i^t A e_j = 1$ (inače je $e_i^t A e_j = 0$).

Projiciramo vektore kanonske baze na jedan od netrivijalnih svojstvenih potprostora, recimo V_1: $x_i = E_1 e_i$, $i = 1, \ldots, n$. Računamo skalarne produkte tih vektora:

$$\langle x_i, x_j \rangle = x_i^t x_j = (E_1 e_i)^t (E_1 e_j) = e_i^t E_1^t E_1 e_j = e_i^t E_1 e_j.$$

Vidjeli smo da su primitivne idempotente Hermitske, a sada su i realne, pa su simetrične matrice. Stoga je $E_1^t E_1 = E_1^2 = E_1$. Po relaciji (11) raspišimo matricu E_1 u bazi Schurovih idempotenta:

$$\begin{aligned} E_1 &= \frac{1}{n}\Big(Q_1(0)A_0 + Q_1(1)A_1 + Q_1(2)A_2\Big) \\ &= \frac{1}{n}\Big((Q_1(0) - Q_1(2))I + Q_1(2)J + (Q_1(1) - Q_1(2))A\Big). \end{aligned}$$

Znamo da $e_i^t A e_j$ poprima vrijednosti 1 ili 0 ovisno jesu li i-ti i j-ti vrh susjedni. Očito vrijedi $e_i^t I e_j = e_i^t e_j = \delta_{ij}$ i $e_i^t J e_j = e_i^t \mathbb{1} = 1$. Zato skalarni produkt

$\langle x_i, x_j \rangle$ poprima samo tri različite vrijednosti:

$$\langle x_i, x_j \rangle = \begin{cases} \alpha, & \text{ako je } i = j, \\ \beta, & \text{ako su } i\text{-ti i } j\text{-ti vrh susjedni,} \\ \gamma, & \text{ako } i\text{-ti i } j\text{-ti vrh nisu susjedni.} \end{cases}$$

Iz (29) možemo izračunati $\alpha = \frac{1}{n}$, $\beta = \frac{n-\Bbbk+s}{n(r-s)}$ i $\gamma = \frac{s-\Bbbk}{n(r-s)}$. Normiranjem dobivamo jedinične vektore $\overline{x}_i = \frac{1}{\sqrt{\alpha}} x_i = \sqrt{n} x_i$ sa skalarnim produktima

$$\langle \overline{x}_i, \overline{x}_j \rangle = \begin{cases} \frac{n-\Bbbk+s}{r-s}, & \text{ako su } i\text{-ti i } j\text{-ti vrh susjedni,} \\ \frac{s-\Bbbk}{r-s}, & \text{ako } i\text{-ti i } j\text{-ti vrh nisu susjedni.} \end{cases} \tag{35}$$

Vektori $\overline{x}_1, \ldots, \overline{x}_n$ leže na jediničnoj sferi u svojstvenom potprostoru V_1, kojeg identificiramo s $\mathbb{R}^f$. Za primitivne jako regularne grafove pokazuje se da su ti vektori međusobno različiti. Zovemo ih *euklidskom reprezentacijom* jako regularnog grafa.

Zadatak 3.23. *Projicirajte vektore kanonske baze na svojstveni potprostor V_2 i izvedite formulu za skalarni produkt analognu formuli* (35)*.*

Konačne podskupove jedinične sfere u euklidskom prostoru nazivamo *sfernim kodovima*. Skalarni produkt vektora na jediničnoj sferi je kosinus kuta kojeg zatvaraju $\langle x, y \rangle = \cos \measuredangle(x, y)$ i jednoznačno određuje njihovu udaljenost $\|x - y\|^2 = 2 - 2\langle x, y \rangle$. Dobili smo sferni kod veličine n u $\mathbb{R}^f$ čiji vektori zatvaraju samo dva kuta, odnosno nalaze se na samo dvije udaljenosti. Broj različitih kutova ili udaljenosti među vektorima nazivamo *stupnjem* sfernog koda. Dakle, euklidska reprezentacija jako regularnog grafa je sferni kod stupnja dva u $\mathbb{R}^f$ ili $\mathbb{R}^g$. Na analogan način od asocijacijske sheme s d klasa dobivamo sferne kodove stupnja najviše d. Knjiga posvećena sfernim kodovima je [47].

Delsarte, Goethals i Seidel [42, 43] dokazali su ocjenu za veličinu sfernog koda stupnja d, koju također zovemo *apsolutnom ocjenom*. Smisao naziva je da ocjena ne ovisi o iznosima kutova koje zatvaraju vektori sfernog koda, nego samo o broju različitih kutova. Ako su poznate mjere tih kutova, u nekim slučajevima možemo dobiti bolje "relativne" ocjene.

Teorem 3.24 (Apsolutna ocjena)**.** *Neka je $X = \{x_1, \ldots, x_n\}$ sferni kod veličine n i stupnja d u $\mathbb{R}^f$. Tada je*

$$n \leq \binom{f+d-1}{d} + \binom{f+d-2}{d-1}. \tag{36}$$

Za dokaz nam trebaju osnovne činjenice o sfernim polinomima. Promijenit ćemo oznaku i dimenziju prostora označavati m. Jediničnu sferu u $\mathbb{R}^m$ označavamo $S^{m-1} = \{x \in \mathbb{R}^m \mid \|x\| = 1\}$. Polinome u m varijabli $f, g \in \mathbb{R}[z_1, \ldots, z_m]$ smatramo ekvivalentnima ako vrijedi $f(x) = g(x)$ za sve $x \in S^{m-1}$. Klase ekvivalencije zovemo *sfernim polinomima*.

"Običan" polinom iz $\mathbb{R}[z_1, \ldots, z_m]$ možemo na jedinstven način prikazati kao linearnu kombinaciju monoma $z^u = z_1^{u_1} \cdots z_m^{u_m}$, gdje su $u = (u_1, \ldots, u_m) \in \mathbb{N}_0^m$ eksponenti, a $z = (z_1, \ldots, z_m)$ varijable. Stupanj monoma je $\deg z^u = u_1 + \ldots + u_m$, a stupanj polinoma je najveći stupanj monoma koji se javlja u njegovu razvoju. Prikaz sfernog polinoma kao linearne kombinacije monoma **nije** jedinstven. Na primjer, konstantni polinom $f(z_1, \ldots, z_m) = 1$ i kvadratni polinom $g(z_1, \ldots, z_m) = z_1^2 + \ldots + z_m^2 = \|z\|^2$ očito poprimaju iste vrijednosti na jediničnoj sferi S^{m-1}. *Stupanj sfernog polinoma* definiramo kao najmanji stupanj polinoma iz $\mathbb{R}[z_1, \ldots, z_m]$ u toj klase ekvivalencije. Dakle, sferni polinom kojem pripadaju $f(z_1, \ldots, z_m) = 1$ i $g(z_1, \ldots, z_m) = z_1^2 + \ldots + z_m^2$ je stupnja nula, a ne stupnja 2.

Skup svih sfernih polinoma u m varijabli stupnja najviše d označavamo $\mathrm{Pol}(m, d)$. Uz uobičajene operacije zbrajanja i množenja skalarom, to je vektorski prostor i želimo mu odrediti dimenziju. Sferni polinom je *homogen* ako se može prikazati kao linearna kombinacija monoma istog stupnja. Skup svih homogenih sfernih polinoma koji su linearne kombinacije monoma stupnja i označavamo $\mathrm{Hom}(m, i)$. To je također vektorski prostor, potprostor od $\mathrm{Pol}(m, d)$ ako je $i \leq d$. Nadalje, $\mathrm{Hom}(m, i-2)$ je potprostor od $\mathrm{Hom}(m, i)$. Naime, polinomi $f(z)$ i $g(z) = f(z) \cdot \|z\|^2$ su ekvivalentni, a svaki monom u razvoju od f daje m monoma u razvoju od g kojima je stupanj veći za 2.

Lema 3.25. *Vrijedi* $\mathrm{Pol}(m, d) = \mathrm{Hom}(m, d) \oplus \mathrm{Hom}(m, d-1)$ *(direktna suma vektorskih prostora).*

Dokaz. Neka je $f \in \mathrm{Pol}(m, d)$ i z^u neki od monoma u njegovu razvoju. Ako je $\deg z^u = i < d - 1$, možemo ga zamijeniti s ekvivalentnim polinomom $z^u \|z\|^{2j}$ stupnja $i + 2j$ i pritom izabrati j tako da stupanj bude $d - 1$ ili d. Dakle, svaki sferni polinom iz $\mathrm{Pol}(m, d)$ može se prikazati kao suma polinoma iz $\mathrm{Hom}(m, d-1)$ i $\mathrm{Hom}(m, d)$. Taj prikaz je jedinstven, iz čega slijedi da je suma direktna. □

Sada možemo odrediti dimenziju vektorskog prostora sfernih polinoma.

Lema 3.26. $\dim \mathrm{Pol}(m, d) = \binom{m+d-1}{d} + \binom{m+d-2}{d-1}$.

Dokaz. Zbog prethodne leme vrijedi

$$\dim \mathrm{Pol}(m, d) = \dim \mathrm{Hom}(m, d) + \dim \mathrm{Hom}(m, d-1).$$

Različiti monomi stupnja d su linearno nezavisni, nisu ekvivalentni i razapinju $\mathrm{Hom}(m,d)$. Broj takvih monoma jednak je broju cjelobrojnih rješenja jednadžbe $u_1 + \ldots + u_m = d$ uz uvjete $u_1 \geq 0, \ldots, u_m \geq 0$, koji je po "principu kuglica i štapića" jednak $\binom{m+d-1}{d}$. Dakle, $\dim \mathrm{Hom}(m,d) = \binom{m+d-1}{d}$ i $\dim \mathrm{Hom}(m, d-1) = \binom{m+d-2}{d-1}$, iz čega slijedi tvrdnja. $\square$

Dokaz teorema 3.24. Neka je $X = \{x_1, \ldots, x_n\}$ sferni kod veličine n i stupnja d u $\mathbb{R}^f$ te neka je $A = \{s_1, \ldots, s_d\}$ skup svih skalarnih produkata različitih vektora iz X. Za $i \in \{2, \ldots, n\}$ definiramo sljedeći podskup od A:

$$\Delta_i = \{\langle x_i, x_j \rangle \mid j = 1, \ldots, i-1\}.$$

Zatim definiramo polinome u jednoj varijabli t sa $F_1(t) = 1$ i

$$F_i(t) = \prod_{s \in \Delta_i} \frac{t-s}{1-s}, \quad i = 2, \ldots, n.$$

Konačno, definiramo sferne polinome u f varijabli $z = (z_1, \ldots, z_f)$:

$$p_i(z) = F_i(\langle z, x_i \rangle), \quad i = 1, \ldots, n.$$

Stupnjevi od $F_1, \ldots, F_n$ nisu veći od d, pa su $p_1, \ldots, p_n \in \mathrm{Pol}(f,d)$. Vrijedi $p_i(x_j) = 0$ za $j < i$ i $p_i(x_i) = 1$, iz čega slijedi da su $p_1, \ldots, p_n$ linearno nezavisni. Stoga je $n \leq \dim \mathrm{Pol}(f,d) = \binom{f+d-1}{d} + \binom{f+d-2}{d-1}$. $\square$

Propozicija 3.21 je jednostavan korolar teorema 3.24. Euklidska reprezentacija jako regularnog grafa s parametrima $SRG(n, \Bbbk, \lambda, \mu)$ u svojstvenom potprostoru $V_1 \equiv \mathbb{R}^f$ je sferni kod veličine n i stupnja 2. Stoga po teoremu 3.24 vrijedi $n \leq \binom{f+1}{2} + \binom{f}{1} = \frac{f(f+3)}{2}$. Euklidska reprezentacija u drugom svojstvenom potprostoru $V_2 \equiv \mathbb{R}^g$ daje drugu ocjenu $n \leq \frac{g(g+3)}{2}$.

Za sferni kod X kažemo da je *antipodalan* ako za svaki $x \in X$ vrijedi $-x \in X$. Za antipodalne kodove Delsarte, Goethals i Seidel [43] dokazali su nešto jaču ocjenu.

Teorem 3.27. *Neka je X antipodalni sferni kod veličine n i stupnja d u $\mathbb{R}^f$. Tada je*

$$n \leq 2\binom{f+d-2}{d-1}.$$

Dokaz. Vidi [47], teorem 9.5.2 na str. 313. $\square$

U teoriji sfernih kodova, cilj je konstruirati kodove $X \subset S^{m-1}$ što većeg kardinaliteta $n = |X|$, što manje dimenzije m i što veće minimalne udaljenosti $\rho(X) = \min\{\|x-y\|^2 \mid x, y \in X,\ x \neq y\}$. Od jako regularnih grafova dobivamo kodove malog stupnja $d = 2$, u kojima se pojavljuju samo dvije različite udaljenosti. Mnogi od tih kodova imaju dobra metrička svojstva, tj. veliku minimalnu udaljenost $\rho(X)$. Pregled grafova $SRG(n, \Bbbk, \lambda, \mu)$ koji daju dobre sferne kodove s parametrima (m, ρ, n) dan je u knjizi [47, tablica 9.2 na str. 310]. Kratak pregled teorije sfernih kodova dan je u cjelini 5.1.1 knjige [4] (str. 175–178).

Na kraju ovog poglavlja definiramo uvjet regularnosti koji generalizira uvjet za jako regularne grafove. Rezultate navodimo bez dokaza i uglavnom slijedimo [29].

Definicija 3.28. *Neka je $t \in \mathbb{N}_0$. Za graf kažemo da je* t-izoregularan *ili da ima* svojstvo $C(t)$ *ako za svaka dva podskupa vrhova S_1 i S_2 veličine najviše t, takva da su inducirani podgrafovi na S_1 i S_2 izomorfni, broj vrhova susjednih svim vrhovima iz S_1 je jednak broju vrhova susjednih svim vrhovima iz S_2.*

Parametri takvog grafa su brojevi $\lambda(S)$. To je broj vrhova susjednih svakom vrhu induciranog podgrafa izomorfnog sa S, pri čemu S ide po svim klasama izomorfizma grafova s najviše t vrhova. Uvjet $C(t)$ je sve jači što je broj t veći. Uvjet $C(0)$ zadovoljava svaki graf, a $\lambda(\emptyset)$ je ukupan broj vrhova. Uvjet $C(1)$ je "obična regularnost", a $\lambda(\{x\})$ je stupanj. Uvjet $C(2)$ ekvivalentan je definiciji jako regularnog grafa, uključujući potpune i prazne grafove. Ako su parametri $SRG(n, \Bbbk, \lambda, \mu)$, onda je $\lambda(S) = \lambda$ ako se S sastoji od dva susjedna vrha, a $\lambda(S) = \mu$ ako se S sastoji od dva nesusjedna vrha. Cameron [26] je karakterizirao grafove koji zadovoljavaju uvjet $C(5)$.

Teorem 3.29. *Graf koji zadovoljava uvjet $C(5)$ ujedno zadovoljava $C(t)$ za sve $t \in \mathbb{N}_0$. Jedini takvi grafovi su disjunktne unije potpunih grafova $r \cdot K_m$, ciklus C_5 te 3×3 topovski graf i njihovi komplementi.*

Poznata su samo dva grafa koji zadovoljavaju $C(4)$, a ne zadovoljavaju $C(5)$: Schläfijev graf $SRG(27, 10, 1, 5)$ i McLaughlinov graf $SRG(275, 112, 30, 56)$ (i komplementi). Poznato je beskonačno mnogo grafova koji zadovoljavaju svojstvo $C(3)$. Cameron, Goethals i Seidel [33] klasificirali su njihove parametre u tri familije: pseudo latinski kvadrati, negativni latinski kvadrati i grafovi Smithinog tipa. Za opise tih familija vidi [34, str. 110-111]. Parametre "običnih" jako regularnih grafova, koji zadovoljavaju samo uvjet $C(2)$, ne možemo opisati na taj način, tj. klasificirati ih u nekoliko beskonačnih familija. Za gerenriranje tablice dopustivih parametara 2 trebali smo pomoć računala.

Uvjeti regularnosti $C(t)$ povezani su s još jednom vrstom pravilinih konačnih podskupova sfere.

Definicija 3.30. *Za skup vektora* $X = \{x_1, \ldots, x_n\}$ *iz sfere* $\Omega = S^{m-1}$ *kažemo da je* sferni t-dizajn *ako za svaki polinom* $f \in \mathrm{Pol}(m,t)$ *vrijedi*

$$\frac{1}{n}\sum_{i=1}^{n} f(x_i) = \frac{1}{\mathrm{vol}(\Omega)}\int_{\Omega} f(x)\mathrm{d}x.$$

U [47, teorem 9.6.1] uvjet je karakteriziran na šest načina, od kojih svaki može poslužiti kao definicija sfernog t-dizajna. Za male t uvjet ima mehaničku interpretaciju. Zamislimo kruto tijelo koje se sastoji od n jediničnih masa postavljenih na točke iz X. Tada je X sferni 1-dizajn ako i samo ako je centar mase tog tijela u ishodištu. Ako je to ispunjeno, X je sferni 2-dizajn ako i samo ako je elipsoid inercije tog tijela sfera (tj. tijelo ima isti moment inercije obzirom na bilo koju os kroz ishodište).

Teorem 3.31. *Neka je* G *primitivan jako regularan graf i* X *njegova euklidska reprezentacija u jednom od netrivijalnih svojstvenih potprostora* V_1 *ili* V_2.

(a) *X je uvijek sferni* 2*-dizajn.*

(b) *X je sferni* 3*-dizajn ako i samo ako G dostiže odgovarajući Kreinov uvjet:* $q_{11}^1 = 0$ *ako smo projicirali na* V_1, *a* $q_{22}^2 = 0$ *ako smo projicirali na* V_2. *U tom slučaju G zadovoljava uvjet* $C(3)$.

(c) *X je sferni* 4*-dizajn ako i samo ako G dostiže odgovarajuću apsolutnu ocjenu:* $n = \frac{1}{2}f(f+3)$ *za* V_1, *a* $n = \frac{1}{2}g(g+3)$ *za* V_2. *U tom slučaju G zadovoljava uvjet* $C(4)$.

(d) *X nikad nije sferni* 5*-dizajn.*

Apsolutna ocjena je gornja ocjena na veličinu sfernog koda $X \subset S^{m-1}$ stupnja d. Najveći t za koji je X sferni t-dizajn nazivamo *snagom* od X. Delsarte, Goethals i Seidel [43] dali su donju ocjenu na veličinu sfernog koda snage t.

Teorem 3.32. *Neka je* $X \subset S^{m-1}$ *podskup veličine n i snage* $t \geq 4$, *za* $m \geq 3$. *Ako je* $t = 2d$ *paran, onda vrijedi*

$$n \geq \binom{m+d-1}{d} + \binom{m+d-2}{d-1}. \tag{37}$$

Ako je $t = 2d-1$ *neparan, onda vrijedi*

$$n \geq 2\binom{m+d-2}{d-1}. \tag{38}$$

Dokaz. Vidi [47], teorem 9.6.7 na str. 322. □

Od posebng interesa je slučaj kad se dostižu ove ocjene. Za parni t, ako X dostiže ocjenu (37), onda je stupnja d i ujedno dostiže apsolutnu ocjenu iz teorema 3.24. Za neparni t, ako X dostiže ocjenu (38), onda je antipodalan, stupnja d i ujedno dostiže ocjenu iz teorema 3.27. Za takve sferne dizajne kažemo da su *napeti* (eng. *tight*). Kratak pregled teorije sfernih dizajna dan je na početku II. dijela knjige [1] (str. 50–55). Opsežniji pregledi su cjelina 5.1.2 knjige [4] (str. 178–196) i cjelina 9.6 knjige [47] (str. 314–324).

Zadatak 3.33. *Neka je G graf maksimalnog stupnja $\Bbbk$ i dijametra d. Dokažite da broj vrhova n takvog grafa zadovoljava*

$$n \leq 1 + \Bbbk \sum_{i=0}^{d-1} (\Bbbk - 1)^i.$$

Grafove koji dostižu jednakost zovemo Mooreovim grafovima*. Klasificirajte Mooreove grafove dijametra $d = 2$.*

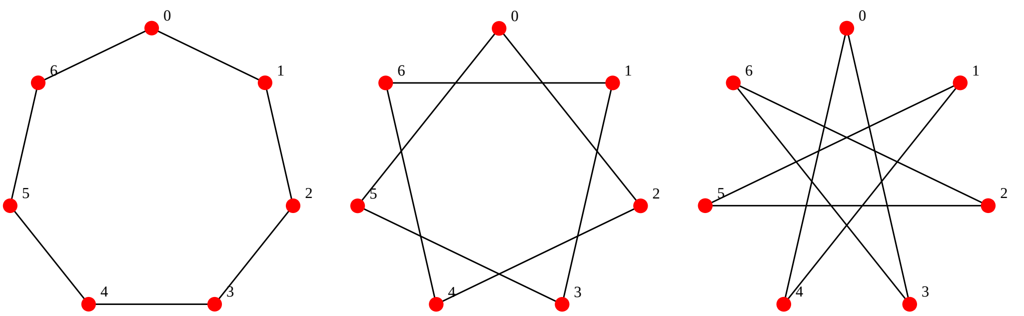
4 Asocijacijske sheme s tri klase

U ovom poglavlju opisat ćemo nekoliko zanimljivih primjera asocijacijskih shema s tri klase. Primjeri su simetrični, pa Bose-Mesnerovu algebru možemo gledati nad poljem $\mathbb{R}$. Prvo definiramo i proučavamo pojam primitivnosti i imprimitivnosti u općem slučaju, za komutativne (ne nužno simetrične) koherentne konfiguracije s d klasa i Bose-Mesnerove algebre nad $\mathbb{C}$.

4.1 Primitivnost i imprimitivnost

U cjelini 3.1 definirali smo da je jako regularan graf G s parametrima $SRG(n, \Bbbk, \lambda, \mu)$ imprimitivan ako je $\mu = 0$ ili $\mu = \Bbbk$, a primitivan ako je $0 < \mu < \Bbbk$. Odgovarajuća asocijacijska shema sastoji se od grafa G i njegovog komplementa G^c. U imprimitivnom slučaju jedan od ta dva grafa ima parametar $\mu = 0$ i nije povezan (propozicija 3.6). U primitivnom slučaju oba grafa su povezana.

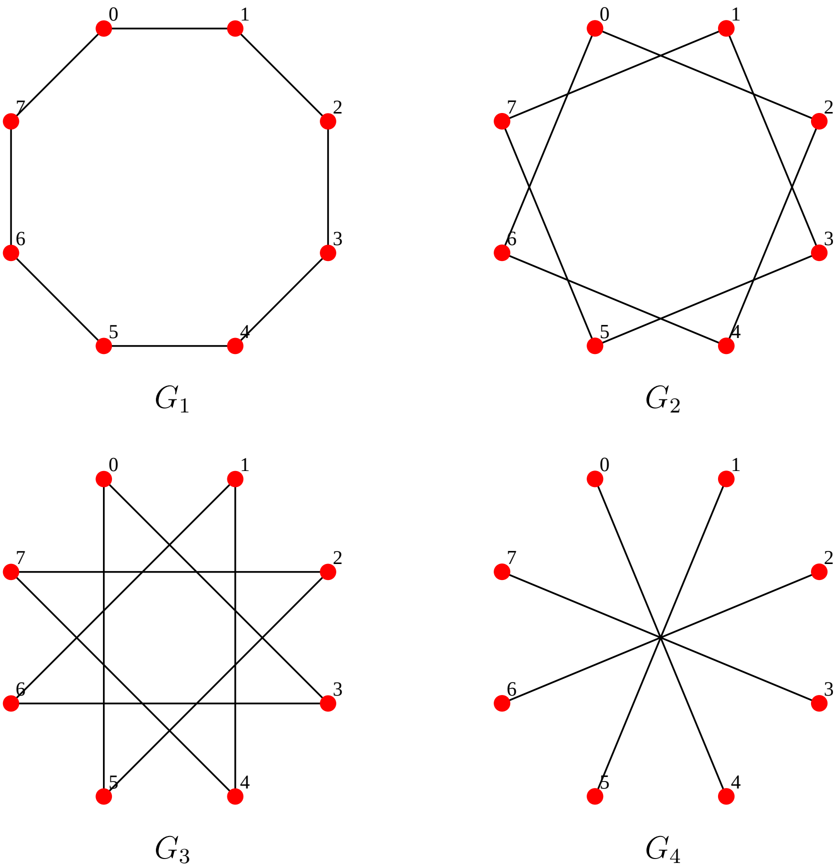
Definicija 4.1. *Neka je $\mathfrak{X}$ koherentna konfiguracija sa skupom vrhova X i relacijama $R_0, R_1, \ldots, R_d$. Kažemo da je $\mathfrak{X}$* primitivna *ako su relacije $R_1, \ldots, R_d$ povezane, a* imprimitivna *ako je bar jedna od tih relacija nepovezana.*



G_1 G_2 G_3

Slika 13: Grafovi poligona reda $n = 7$ (sedmerokuta).

Na slici 13 prikazani su netrivijalni grafovi koji čine poligon reda $n = 7$ (primjer 1.4). Vidimo da su sva tri grafa povezana, pa je sedmerokut primitivna asocijacijska shema. Na slici 14 prikazani su netrivijalni grafovi osmerokuta, poligona reda $n = 8$. Grafovi G_2 i G_4 su nepovezani, pa je osmerokut primjer imprimitivne asocijacijske sheme.



Slika 14: Grafovi poligona reda $n = 8$ (osmerokuta).

Zadatak 4.2. *Dokažite da je poligon reda $n \geq 2$ (primjer 1.4) primitivan ako i samo ako je n prost broj.*

Zadatak 4.3. *Dokažite da klase konjugacije konačne grupe G (primjer 1.42) čine primitivnu koherentnu konfiguraciju ako i samo ako je grupa G jednostavna, tj. ako nema netrivijalnih normalnih podgrupa.*

Objasnimo pobliže pojam povezanosti za nesimetrične relacije. Koristimo terminologiju teorije grafova i relaciju shvaćamo kao usmjereni graf. Ako je par vrhova (x, y) u relaciji, pišemo $x \to y$ (u simetričnom slučaju koristili smo oznaku $x \sim y$ za susjedne vrhove). *Šetnja* od vrha x do vrha y je niz vrhova $x = x_0 \to x_1 \to \ldots \to x_\ell = y$. Broj ℓ je *duljina* šetnje. Ako postoji šetnja od x do y, to zapisujemo $x \twoheadrightarrow y$. Relacija $\twoheadrightarrow$ je tranzitivno zatvorenje relacije $\to$ (najmanja tranzitivna i refleksivna relacija koja sadrži $\to$).

Općenito, za usmjerene grafove razlikujemo pojmove jake i slabe povezanosti. *Jaka povezanost* znači da za svaka dva vrha vrijedi $x \twoheadrightarrow y$. *Slaba* *povezanost* znači da je neusmjereni graf koji dobijemo "zanemarivanjem orijentacije" povezan. Naše relacije čine koherentnu konfiguraciju. Vidjet ćemo da se zbog toga jaka i slaba povezanost podudaraju. Relacija $\twoheadrightarrow$ bit će simetrična, čak i ako krenemo od nesimetrične relacije koherentne kofiguracije.

Uzmimo jednu od relacija koherentne konfiguracije R_i (indeks i je sada fiksiran). Neka je A_i odgovarajuća Schurova idempotenta, tj. 0-1 matrica pridružena relaciji R_i. Sjetimo se oznake $N_i(x) = \{y \in X \mid x \to y\}$ za skup svih susjeda vrha x. Definiramo $N^{(i)}(x) = \{y \in X \mid x \twoheadrightarrow y\}$ kao skup svih vrhova do kojih možemo doći šetnjom koja počinje u x. To je komponenta povezanosti relacije R_i kojoj pripada x. Trebat će nam usmjerena verzija leme 3.9.

Lema 4.4. *Element na mjestu (x, y) potencije A_i^ℓ jednak je broju šetnji duljine ℓ od vrha x do vrha y.*

Dokaz. Indukcijom po ℓ. Za $\ell = 0$, postoji jedna šetnja duljine 0 od x do x i nula šetnji duljine 0 od x do $y \neq x$. To se slaže sa $A_i^0 = I$. Za $\ell = 1$, broj šetnji je jedan ako vrijedi $x \to y$, tj. $[A_i]_{x,y} = 1$, a nula ako ne vrijedi $x \to y$, tj. $[A_i]_{x,y} = 0$. Pretpostavimo da je $[A_i^{\ell-1}]_{x,z}$ broj šetnji duljine $\ell - 1$ od x do z. Šetnje duljine ℓ do vrha y dobivamo tako da dodamo korak $z \to y$, ako su ta dva vrha u relaciji. Prema tome, broj šetnji duljine ℓ od x do y je $\sum\limits_{z \in X} [A_i^{\ell-1}]_{x,z}[A_i]_{z,y}$. To je upravo element na mjestu (x, y) produkta matrica $A_i^{\ell-1} \cdot A_i = A_i^\ell$. $\square$

Propozicija 4.5. *Postoji skup indeksa $\Omega \subseteq \{0, \ldots, d\}$ takav da za svaki vrh x vrijedi $N^{(i)}(x) = \cup_{k\in\Omega} N_k(x)$.*

Dokaz. Po prethodnoj lemi vrijedi

$$N^{(i)}(x) = \{y \in X \mid (\exists \ell \in \mathbb{N}_0)\, [A_i^\ell]_{x,y} > 0\}.$$

Potencije A_i^ℓ pripadaju koherentnoj algebri i možemo ih prikazati u bazi Schurovih idempotenta: $A_i^\ell = \sum_{k=0}^{d} \alpha_k^\ell A_k$. Definiramo

$$\Omega = \{k \in \{0, \ldots, d\} \mid (\exists \ell \in \mathbb{N}_0)\, \alpha_k^\ell > 0\}. \tag{39}$$

Za vrhove x i y, uvjet $(\exists \ell \in \mathbb{N}_0)\, [A_i^\ell]_{x,y} > 0$ ekvivalentan je s $k \in \Omega$ i $[A_k]_{x,y} = 1$, odnosno $k \in \Omega$ i $y \in N_k(x)$. Zato je $N^{(i)}(x) = \cup_{k\in\Omega} N_k(x)$. $\square$

Ključno je da skup Ω definiran s (39) ne ovisi o izboru vrha x, nego samo o relaciji R_i. Iz toga slijede iduće tvrdnje.

Korolar 4.6. *Veličina komponente povezanosti $|N^{(i)}(x)|$ ne ovisi o izboru vrha x.*

Dokaz. Veličina "susjedstva" $|N_k(x)| = n_k$ je stupanj koherentne konfiguracije i ne ovisi o x. Skupovi $N_0(x), \ldots, N_d(x)$ su disjunktni, pa je $|N^{(i)}(x)| = \sum\limits_{k\in\Omega} n_k$, a Ω ne ovisi o x. $\square$

Korolar 4.7. *Relacija $\twoheadrightarrow$ je relacija ekvivalencije. Klasa ekvivalencije kojoj pripada x podudara se s komponentom povezanosti $N^{(i)}(x)$.*

Dokaz. Refleksivnost i tranzitivnost su očite. Dokazujemo simetričnost. Neka vrijedi $x \twoheadrightarrow y$, tj. $y \in N^{(i)}(x)$. Zbog tranzitivnosti tada vrijedi $N^{(i)}(y) \subseteq N^{(i)}(x)$. Iz prethodnog korolara znamo da je $|N^{(i)}(x)| = |N^{(i)}(y)|$, pa je $N^{(i)}(x) = N^{(i)}(y)$. Po refleksivnosti je $x \in N^{(i)}(x)$ i slijedi $x \in N^{(i)}(y)$, tj. $y \twoheadrightarrow x$. $\square$

Korolar 4.8. *Ako je $k \in \Omega$, onda je $k' \in \Omega$. Pritom je Ω skup indeksa iz propozicije 4.5, a k' je indeks za koji vrijedi $A_{k'} = A_k^t$.*

Dokaz. Po propoziciji 4.5, relacija $\twoheadrightarrow$ je unija relacija koherentne konfiguracije: $\cup_{k\in\Omega} R_k$. Neka je $k \in \Omega$ i $(x, y) \in R_k$. Tada vrijedi $x \twoheadrightarrow y$, pa zbog simetričnosti slijedi $y \twoheadrightarrow x$. No tada i par $(y, x) \in R_{k'}$ pripada uniji $\cup_{k\in\Omega} R_k$, pa je $k' \in \Omega$. $\square$

Uzmimo sada bilo koji skup indeksa $\Omega \subseteq \{0, \ldots, d\}$ i promotrimo odgovarajuću uniju relacija $R_\Omega = \cup_{k\in\Omega} R_k$. Na dva trivijalna načina možemo postići da R_Ω bude relacija ekvivalencije. Ako uzmemo $\Omega = \{0\}$, unija je R_0, a to je relacija ekvivalencije u kojoj je svaki vrh ekvivalentan samom sebi i niti jednom drugom vrhu (klase ekvivalencije su jednočlane). Ako uzmemo $\Omega = \{0, \ldots, d\}$, unija je Kartezijev produkt $X \times X$, a to je relacije ekvivalencije u kojoj su svaka dva vrha ekvivalentna (klasa ekvivalencije je cijeli X). Imprimitivne koherentne konfiguracije karakterizirane su na sljedeći način.

Teorem 4.9. *Koherentna konfiguracija sa skupom vrhova X i relacijama $R_0, \ldots, R_d$ je imprimitivna ako i samo ako postoji skup indeksa Ω takav da je $\{0\} \subsetneq \Omega \subsetneq \{0, \ldots, d\}$ i R_Ω je relacija ekvivalencije.*

Dokaz. Neka je koherentna konfiguracija imprimitivna. Po definiciji postoji indeks $i \in \{1, \ldots, d\}$ za koji relacija R_i nije povezana. Skup indeksa Ω iz propozicije 4.5 daje nam relaciju ekvivalencije R_Ω koja se podudara s relacijom $\twoheadrightarrow$ dobivenom iz R_i. Zbog nepovezanosti, R_Ω ima bar dvije klase ekvivalencije, pa je $\Omega \neq \{0, \ldots, d\}$. S druge strane, zbog $i \in \Omega$ je $\Omega \neq \{0\}$.

Obratno, pretpostavimo da postoji netrivijalni Ω za koji je R_Ω relacija ekvivalencije. Zbog $\Omega \neq \{0, \ldots, d\}$ ta relacija ima bar dvije klase ekvivalencije. Zbog $\Omega \neq \{0\}$ postoji $i \in \Omega$, $i \neq 0$. Klase ekvivalencije od R_Ω su disjunktne unije komponenta povezanosti od R_i. Zato relacija R_i ima bar dvije komponente, tj. nije povezana. Dakle, koherentna konfiguracija je imprimitivna. $\square$

Neka je $G \leq \mathrm{Sym}(X)$ tranzitivna permutacijska grupa. Iz teorije grupa poznata je sljedeća definicija (vidi npr. [27, cjelina 1.9]). Kažemo da je G *imprimitivna* ako postoji netrivijalna particija od X koju G preslikava u sebe. U suprotnom, ako G čuva samo trivijalne particije (na jednočlane podskupove i na cijeli X), kažemo da je *primitivna.*

Zadatak 4.10. *Neka je G tranzitivna permutacijska grupa i $\mathcal{X}$ koherentna konfiguracija dobivena Schurovom konstrukcijom od G, kao u primjeru 1.36. Dokažite da je G imprimitivna ako i samo ako je $\mathcal{X}$ imprimitivna.*

Promotrimo konkretan primjer imprimitivne asocijacijske sheme, osmerokut (slika 14). Neka su R_1, R_2, R_3 i R_4 relacije susjedstva grafova G_1, G_2, G_3 i G_4, a R_0 "dijagonala". Netrivijalne relacije ekvivalencije dobivamo na dva načina. Unija $R_0 \cup R_4$ je relacija ekvivalencije s klasama $\{0, 4\}$, $\{1, 5\}$, $\{2, 6\}$ i $\{3, 7\}$. To je relacija kongruencije modulo 4 na skupu $\mathbb{Z}_8$. Unija $R_0 \cup R_2 \cup R_4$ je relacija ekvivalencije s klasama $\{0, 2, 4, 6\}$ i $\{1, 3, 5, 7\}$. To je relacija kongruencije modulo 2.

Sada ćemo vidjeti kako primitivnost i imprimitivnost koherentne konfiguracije prepoznajemo iz presječnih brojeva p_{ij}^k.

Definicija 4.11. *Neka je Δ_i graf sa skupom vrhova $\{0, \ldots, d\}$. Vrhovi j, k su susjedni ($j \to k$) ako je $p_{ij}^k > 0$. Taj graf zovemo i-tim* distribucijskim grafom *koherentne konfiguracije.*

Matricu susjedstva od Δ_i dobivamo iz presječne matrice B_i (definicija 2.51) tako da nenul elemente zamijenimo jedinicama. Distribucijski graf ima petlju $j \to j$ uvijek kad je $p_{ij}^j > 0$. Zbog 2. svojstva iz propozicije 2.24, graf Δ_0 ima sve petlje i nema drugih vrhova. Proučimo pobliže distribucijske grafove $\Delta_1, \ldots, \Delta_d$. Općenito, Δ_i je usmjereni graf, ali ako krenemo od asocijacijske sheme je simetričan.

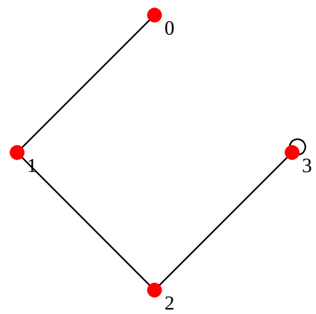
Propozicija 4.12. *Ako je koherentna konfiguracija simetrična, onda su njezini distribucijski grafovi simetrični.*

Dokaz. Za simetričnu koherentnu konfiguraciju je $i = i'$, pa po 6. svojstvu iz propozicije 2.24 vrijedi $n_k p_{ij}^k = n_j p_{ik}^j$. Stoga je $p_{ij}^k > 0$ ako i samo ako je $p_{ik}^j > 0$. $\square$

U nesimetričnom slučaju, pokazuje se da je relacija $\twoheadrightarrow$ postojanja šetnje između vrhova u Δ_i ipak simetrična, kao i za relacije koherentne konfiguracije. Dokaz je raspisan u [4], lemi 2.53 i korolaru 2.54 te u [124], lemi 9.10

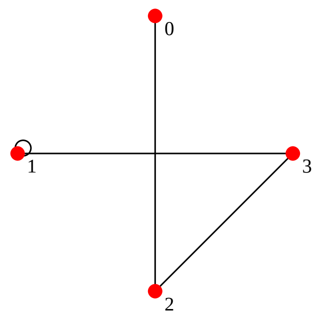
$$B_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Δ_1 :



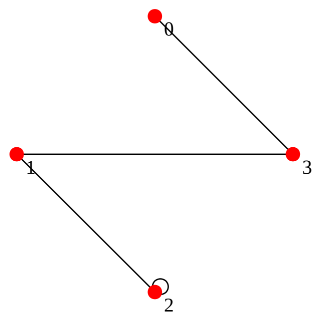
$$B_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 2 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

Δ_2 :



$$B_3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 2 & 1 & 0 & 0 \end{bmatrix}$$

Δ_3 :



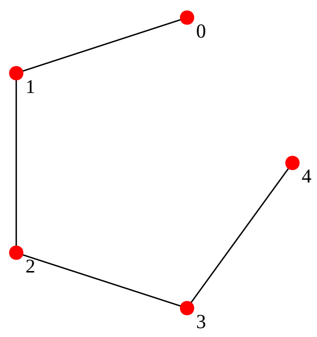
Slika 15: Distribucijski grafovi sedmerokuta.

i korolaru 9.11. Zato se jake i slabe komponente povezanosti distribucijskih grafova podudaraju. Na slici 15 prikazani su distribucijski grafovi sedmerokuta. Vidimo da su grafovi Δ_1, Δ_2 i Δ_3 povezani. Na slici 16 prikazani su distribucijski grafovi osmerokuta. Grafovi Δ_1 i Δ_3 su povezani, a Δ_2 i Δ_4 nepovezani. To se podudara s (ne)povezanosti odgovarajućih relacija koherentne konfiguracije, a zaključak vrijedi i općenito.

Propozicija 4.13. *Distribucijski graf Δ_i je povezan ako i samo ako je relacija R_i komutativne koherentne konfiguracije povezana.*

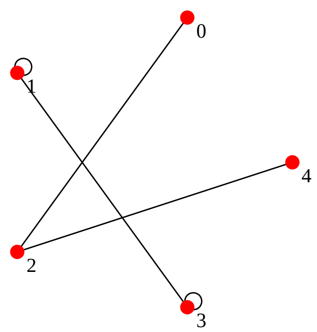
$$B_1 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Δ_1 :



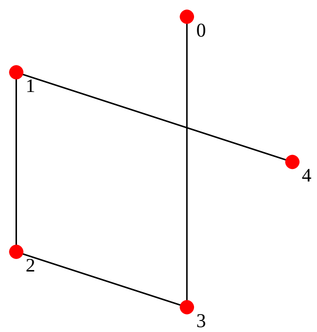
$$B_2 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 2 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Δ_2 :



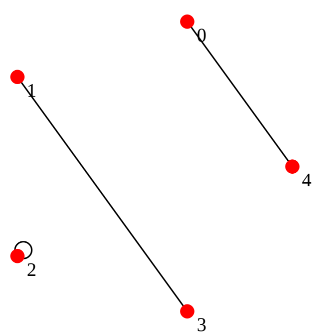
$$B_3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 1 & 0 \\ 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

Δ_3 :



$$B_4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Δ_4 :



Slika 16: Distribucijski grafovi osmerokuta.

Dokaz. Relacija R_i je povezana ako i samo ako je skup indeksa Ω iz propozicije 4.5 cijeli $\{0,\ldots,d\}$. Pokazat ćemo da se skup Ω podudara s komponentom povezanosti grafa Δ_i koja sadrži 0. Iz toga slijedi tvrdnja. Očito je $0 \in \Omega$. Ako je $j \in \Omega$ i postoji brid $j \to k$ u grafu Δ_i, to znači da je $p_{ij}^k > 0$. Zbog komutativnosti, tada je i $p_{ji}^k > 0$. Po definiciji presječnog broja, za svaki vrh y za koji je $(x,y) \in R_k$ postoji vrh z takav da je $(x,z) \in R_j$ i $(z,y) \in R_i$. Budući da je $j \in \Omega$, postoji šetnja u R_i od x do z. Možemo je proširiti korakom (z,y) i dobiti šetnju od x do y, a iz toga zaključujemo da je $k \in \Omega$. Dakle, Ω je najmanji skup indeksa koji sadrži 0 i zatvoren je na "susjedstvo u Δ_i" (ako je $j \in \Omega$ i $j \to k$, onda je $k \in \Omega$). To je upravo komponenta povezanosti od Δ_i koja sadrži 0. □

Prema tome, primitivnost komutativne koherentne konfiguracije ekvivalentna je povezanosti distribucijskih grafova $\Delta_1,\ldots,\Delta_d$, a imprimitivnost nepovezanosti bar jednog od tih grafova. U dokazu propozicije 4.13 koristili smo komutativnost, a u tom slučaju imamo primitivne idempotente $E_0,\ldots,E_d$ i Kreinove parametre $q_{ij}^k \geq 0$. Pomoću Kreinovih parametara možemo definirati grafove na isti način kao od presječnih brojeva.

Definicija 4.14. *Neka je ∇_i graf sa skupom vrhova $\{0,\ldots,d\}$. Vrhovi j, k su susjedni ($j \to k$) ako je $q_{ij}^k > 0$. Taj graf zovemo i-*tim reprezentacijskim grafom *komutativne koherentne konfiguracije.*

Matricu susjedstva od ∇_i dobivamo iz dualne presječne matrice B_i° (definicija 2.52) zamjenom nenul elemenata jedinicama. Reprezentacijski graf ima petlju $j \to j$ ako je $q_{ij}^j > 0$. Zbog 2. svojstva iz propozicije 2.25, graf ∇_0 ima sve petlje i nema drugih vrhova. Proučimo reprezentacijske grafove $\nabla_1,\ldots,\nabla_d$.

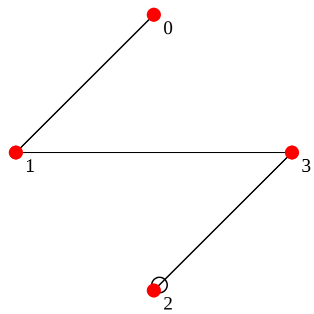
Propozicija 4.15. *Ako je koherentna konfiguracija simetrična, onda su njezini reprezentacijski grafovi simetrični.*

Dokaz. U simetričnom slučaju primitivne idempotente $E_0,\ldots,E_d$ su realne matrice. Znamo da su hermitske, a tada su simetrične ($E_{\hat{i}} = E_i^t = E_i$). Zato je $i = \hat{i}$. Po 6. svojstvu propozicije 2.25 vrijedi $m_k q_{ij}^k = m_j q_{ik}^j$. Stoga je $q_{ij}^k > 0$ ako i samo ako je $q_{ik}^j > 0$. □

U nesimetričnom slučaju, relacija $\twoheadrightarrow$ u grafu ∇_i ipak je simetrična; vidi [124, lema 9.16]. Zato se jake i slabe komponente povezanosti podudaraju i u reprezentacijskim grafovima. Na slici 17 prikazani su reprezentacijski grafovi sedmerokuta; vidimo da su povezani. Na slici 18 prikazani su reprezentacijski grafovi osmerokuta. Grafovi ∇_1 i ∇_2 su nepovezani, a ∇_3 i ∇_4 povezani. Za reprezentacijske grafove ne vrijedi analogon propozicije 4.13 jer

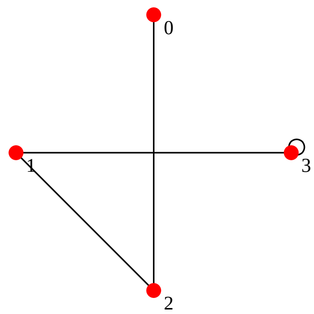
$$B_1^\circ = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

$\nabla_1 :$



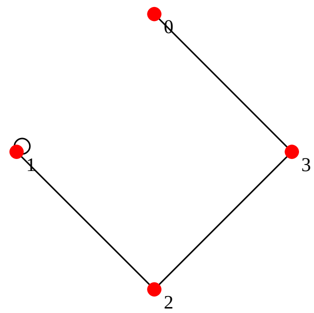
$$B_2^\circ = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

$\nabla_2 :$



$$B_3^\circ = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 2 & 0 & 1 & 0 \end{bmatrix}$$

$\nabla_3 :$

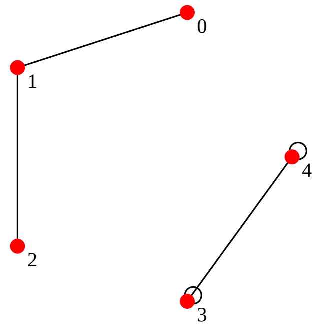


Slika 17: Reprezentacijski grafovi sedmerokuta.

oni ovise o numeraciji primitivnih idempotenta $E_0, \ldots, E_d$. Za razliku od Schurovih idempotenta $A_0, \ldots, A_d$, numeracija primitivnih idempotenta nije jednoznačno određena s numeracijom relacija $R_0, \ldots, R_d$. Broj povezanih i nepovezanih reprezentacijskih grafova ipak se podudara s brojem povezanih i nepovezanih relacija $R_0, \ldots, R_d$. Zato primitivnost i imprimitivnost komutativne koherentne konfiguracije možemo prepoznati i preko njezinih reprezentacijskih grafova.

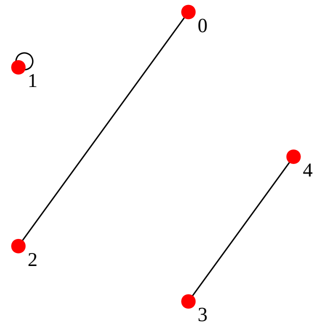
$$B_1^\circ = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 2 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

$\nabla_1 :$



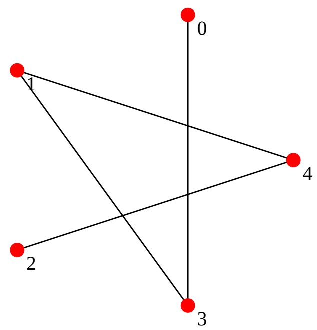
$$B_2^\circ = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$\nabla_2 :$



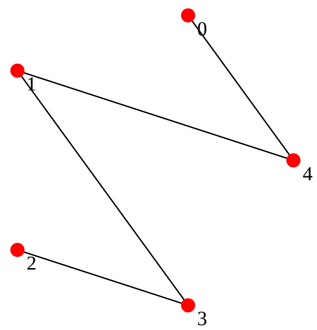
$$B_3^\circ = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \end{bmatrix}$$

$\nabla_3 :$



$$B_4^\circ = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 \end{bmatrix}$$

$\nabla_4 :$



Slika 18: Reprezentacijski grafovi osmerokuta.

Za dokaz te činjenice koristi se još jedna karakterizacija (im)primitivnosti preko svojstvenih vrijednosti i dualnih svojstvenih vrijednosti. Sjetimo se da Schurove idempotente komutativne koherentne konfiguracije možemo simultano dijagonalizirati. Svojstvene vrijednosti od A_j stavljamo u j-ti stupac matrice $P = [P_j(i)]$, a to su ujedno svojstvene vrijednosti presječne matrice B_j (korolar 2.57). Slično, u j-tom stupcu dualne svojstvene matrice $Q = [Q_j(i)]$ je spektar dualne presječne matrice B_j°. Stupnjevi $n_j = P_j(0)$ i kratnosti $m_j = Q_j(0)$ su u nultom retku matrica P, Q i to su svojstvene vrijednosti koje su najveće po apsolutnoj vrijednosti: $|P_j(i)| \le n_j$, $|Q_j(i)| \le m_j$ (propozicija 2.35). Broj komponenta povezanosti grafova Δ_j i ∇_j prepoznajemo po kratnostima tih najvećih svojstvenih vrijednosti.

Teorem 4.16. *Broj komponenta povezanosti distribucijskog grafa Δ_j jednak je $|\{i \in \{0,\dots,d\} \mid P_j(i) = n_j\}|$. Broj komponenta povezanosti reprezentacijskog grafa ∇_j jednak je $|\{i \in \{0,\dots,d\} \mid Q_j(i) = m_j\}|$.*

Ovaj teorem je posljedica Perron[25]-Frobeniusove[26] teorije o matricama s nenegativnim unosima (vidi 8. poglavlje knjige [63] ili 7. poglavlje knjige [101]). Dokaz je raspisan u [124, propozicija 9.17] i [4, propozicija 2.59]. Pomoću GAP paketa *AssociationSchemes* [2] možemo izračunati (dualne) svojstvene vrijednosti sedmerokuta i osmerokuta. Za sedmerokut dobivamo

$$P = \begin{bmatrix} 1 & 2 & 2 & 2 \\ 1 & e_7^2 + e_7^5 & e_7^3 + e_7^4 & e_7 + e_7^6 \\ 1 & e_7 + e_7^6 & e_7^2 + e_7^5 & e_7^3 + e_7^4 \\ 1 & e_7^3 + e_7^4 & e_7 + e_7^6 & e_7^2 + e_7^5 \end{bmatrix}$$

$$\approx \begin{bmatrix} 1 & 2 & 2 & 2 \\ 1 & -0.445042 & -1.80194 & 1.24698 \\ 1 & 1.24698 & -0.445042 & -1.80194 \\ 1 & -1.80194 & 1.24698 & -0.445042 \end{bmatrix},$$

$$Q = \begin{bmatrix} 1 & 2 & 2 & 2 \\ 1 & e_7^2 + e_7^5 & e_7 + e_7^6 & e_7^3 + e_7^4 \\ 1 & e_7^3 + e_7^4 & e_7^2 + e_7^5 & e_7 + e_7^6 \\ 1 & e_7 + e_7^6 & e_7^3 + e_7^4 & e_7^2 + e_7^5 \end{bmatrix}$$

$$\approx \begin{bmatrix} 1 & 2 & 2 & 2 \\ 1 & -0.445042 & 1.24698 & -1.80194 \\ 1 & -1.80194 & -0.445042 & 1.24698 \\ 1 & 1.24698 & -1.80194 & -0.445042 \end{bmatrix}.$$

[25] Oskar Perron (1880.-1975.), njemački matematičar.
[26] Ferdinand Georg Frobenius (1849.-1917.), njemački matematičar.

Ovdje je $e_7 = e^{2\pi i/7} = \cos(2\pi/7) + i\sin(2\pi/7)$ primitivni sedmi korijen jedinice. Primitivni osmi korijen jedinice možemo jednostavnije zapisati kao $e_8 = e^{\pi i/4} = \frac{1+i}{\sqrt{2}}$. Za osmerokut dobivamo

$$P = \begin{bmatrix} 1 & 2 & 2 & 2 & 1 \\ 1 & 0 & -2 & 0 & 1 \\ 1 & -2 & 2 & -2 & 1 \\ 1 & \sqrt{2} & 0 & -\sqrt{2} & -1 \\ 1 & -\sqrt{2} & 0 & \sqrt{2} & -1 \end{bmatrix}, \quad Q = \begin{bmatrix} 1 & 2 & 1 & 2 & 2 \\ 1 & 0 & -1 & \sqrt{2} & -\sqrt{2} \\ 1 & -2 & 1 & 0 & 0 \\ 1 & 0 & -1 & -\sqrt{2} & \sqrt{2} \\ 1 & 2 & 1 & -2 & -2 \end{bmatrix}.$$

U nultom stupcu svojstvena vrijednost 1 ponavlja se $d+1$ puta, što odgovara činjenici da grafovi Δ_0 i ∇_0 imaju $d+1$ komponenta povezanosti (izoirane vrhove spojene petljom samo sa sobom). Za sedmerokut, dvojke se pojavljuju samo u nultom retku od P i Q, pa su Δ_1, Δ_2, Δ_3 i ∇_1, ∇_2, ∇_3 povezani. Za osmerokut, prvi i treći stupac matrice P sadrže samo jednu svojstvenu vrijednost 2, pa su Δ_1 i Δ_3 povezani. Drugi stupac sadrži dvije svojstvene vrijednosti 2 i Δ_2 ima dvije komponente povezanosti, a četvrti stupac sadrži tri svojstvene vrijednosti 1 i Δ_4 ima tri komponente povezanosti. U matrici Q treći i četvrti stupac sadrže samo jedan unos 2, a grafovi ∇_3 i ∇_4 su povezani. Prvi i drugi stupac sadrže redom dvije i tri najveće svojstvene vrijednosti, što odgovara broju komponenta povezanosti od ∇_1 i ∇_2.

Korolar 4.17. *Ekvivalentno je:*

(a) bar jedan od distribucijskih grafova $\Delta_1, \ldots, \Delta_d$ je nepovezan,

(b) bar jedan od reprezentacijskih grafova $\nabla_1, \ldots, \nabla_d$ je nepovezan.

Dokaz. Iz teorema 2.29 znamo da je $\frac{Q_j(i)}{m_j} = \frac{\overline{P_i(j)}}{n_i}$. Prema tome, vrijedi $P_i(j) = n_i$ ako i samo ako vrijedi $Q_j(i) = m_j$. Tvrdnja korolara slijedi iz teorema 4.16. □

Dakle, komutativna koherentna konfiguracija je imprimitivna ako i samo ako je bar jedan od reprezentacijskih grafova $\nabla_1, \ldots, \nabla_d$ nepovezan. Zadnja karakterizacija imprimitivnosti koju ćemo obraditi temelji se na operaciji množenja podskupova indeksa $\Omega, \Omega' \subseteq \{0, \ldots, d\}$:

$$\Omega\Omega' = \{k \in \{0, \ldots, d\} \mid \text{ postoje } i \in \Omega,\ j \in \Omega' \text{ takvi da je } p_{ij}^k > 0\}. \quad (40)$$

Propozicija 4.18. *Operacija množenja podskupova indeksa ima svojstva:*

1. *podskup $\{0\}$ je neutralni element,*

2. *asocijativnost: $(\Omega\Omega')\Omega'' = \Omega(\Omega'\Omega'')$,*

3. komutativnost: $\Omega\Omega' = \Omega'\Omega$ *(za komutativne koherentne konfiguracije).*

Dokaz. 1. Iz propozicije 2.24 znamo da je $p_{i0}^k = \delta_{ik}$ i $p_{0j}^k = \delta_{jk}$. Slijedi $\{0\}\Omega = \Omega\{0\} = \Omega$ za svaki podskup Ω.

2. Uzmimo indeks $b \in (\Omega\Omega')\Omega''$. To znači da postoje indeksi $a \in \Omega\Omega'$, $j \in \Omega''$ takvi da je $p_{aj}^b > 0$. Dalje, zbog $a \in \Omega\Omega'$ postoje indeksi $k \in \Omega$, $i \in \Omega'$ takvi da je $p_{ki}^a > 0$. Slijedi $p_{ki}^a p_{aj}^b > 0$, a to je jedan član sume na desnoj strani 7. svojstva iz propozicije 2.24. Suma na desnoj strani je pozitivna, pa je i suma na lijevoj strani pozitivna. Zato bar jedan član te sume mora biti pozitivan, dakle postoji indeks c takav da je $p_{ij}^c p_{kc}^b > 0$. No tada je $p_{ij}^c > 0$, pa je $c \in \Omega'\Omega''$. Osim toga je $p_{kc}^b > 0$, pa je $b \in \Omega(\Omega'\Omega'')$. Time smo dokazali inkluziju $(\Omega\Omega')\Omega'' \subseteq \Omega(\Omega'\Omega'')$, a obratna inkluzija dokazuje se slično.

3. Uz pretpostavku komutativnosti, vrijedi $p_{ij}^k > 0$ ako i samo ako vrijedi $p_{ji}^k > 0$. Zato je $\Omega\Omega' = \Omega'\Omega$. □

Operacija množenja podskupova indeksa detaljnije je obrađena u prvom poglavlju knjige [142], u općenitijem kontekstu i u drugim oznakama. Koristili smo oznaku $R_\Omega = \cup_{k\in\Omega} R_k$ za uniju relacija, a sada uvodimo oznaku $A_\Omega = \sum_{k\in\Omega} A_k$ za sumu Schurovih idempotenta.

Lema 4.19. $\Omega\Omega' = \{k \in \{0,\ldots,d\} \mid (A_\Omega A_{\Omega'}) \circ A_k \neq 0\}$.

Dokaz. Vrijedi $A_\Omega A_{\Omega'} = (\sum_{i\in\Omega} A_i)(\sum_{j\in\Omega'} A_j) = \sum_{i\in\Omega}\sum_{j\in\Omega'} A_i A_j = \sum_{i\in\Omega}\sum_{j\in\Omega'}\sum_{\ell=0}^{d} p_{ij}^\ell A_\ell$. Schurovim množenjem dobijemo $(A_\Omega A_{\Omega'}) \circ A_k = \sum_{i\in\Omega}\sum_{j\in\Omega'} p_{ij}^k A_k$. Ova matrica nije nulmatrica ako i samo ako postoje $i \in \Omega$, $j \in \Omega'$ takvi da je $p_{ij}^k > 0$. Dakle, skup iz iskaza leme podudara se sa skupom iz definicije produkta (40). □

Za podskup indeksa Ω kažemo da je *zatvoren* ako vrijedi $\Omega^2 = \Omega$. Pritom je $\Omega^2 = \Omega\Omega$ množenje definirano s (40).

Teorem 4.20. *Neprazan podskup indeksa* $\Omega \subseteq \{0,\ldots,d\}$ *je zatvoren ako i samo ako je* R_Ω *relacija ekvivalencije.*

Dokaz. Vidi [4, lema 2.63]. □

Dakle, koherentna konfiguracija je imprimitivna ako i samo ako postoji zatvoreni podskup Ω koji je netrivijalan: $\{0\} \subsetneq \Omega \subsetneq \{0,\ldots,d\}$.

Zadatak 4.21. Tanki radikal *(eng.* thin radical*) koherentne konfiguracije je skup svih indeksa za koje su stupnjevi jednaki jedan:*

$$\Omega_1 = \{k \in \{0,\ldots,d\} \mid n_k = 1\}.$$

Dokažite da je Ω_1 *zatvoren i da množenje indeksa iz* Ω_1 *čini grupu. Produkt indeksa* i, j *shvaćamo kao produkt jednočlanih podskupova* $\{i\}\{j\}$*.*

Zadatak 4.22. *Operaciju množenja podskupova indeksa $\Omega, \Omega' \subseteq \{0, \dots, d\}$ možemo definirati na dualan način s pomoću Kreinovih parametara:*

$$\Omega \circ \Omega' = \{k \in \{0, \dots, d\} \mid \text{ postoje } i \in \Omega,\ j \in \Omega' \text{ takvi da je } q_{ij}^k > 0\}.$$

Ispitajte svojstva te operacije!

4.2 Potkonfiguracije i kvocijentne konfiguracije

Neka je $\mathfrak{X} = (X, \{R_i\}_{i=0}^d)$ komutativna koherentna konfiguracija sa Schurovim idempotentama $A_0, \dots, A_d$ i primitivnim idempotentama $E_0, \dots, E_d$. U ovoj cjelini pretpostavljamo da je $\mathfrak{X}$ imprimitivna. Po teoremu 4.9 i teoremu 4.20, postoji zatvoreni skup indeksa $\{0\} \subsetneq \Omega \subsetneq \{0, \dots, d\}$ takav da je $R_\Omega = \cup_{k \in \Omega} R_k$ relacija ekvivalencije. Neka je $\Sigma = \{X_1, \dots, X_r\}$ particija skupa vrhova X na klase ekvivalencije od R_Ω. Particiju Σ zovemo *sustavom imprimitivnosti* od $\mathfrak{X}$, a klase ekvivalencije *vlaknima* (eng. *fibers*). U korolarima 4.6 i 4.7 vidjeli smo da je veličina svakog vlakna $|X_i| = \sum_{k \in \Omega} n_k$. Veličinu vlakna označavat ćemo m. Broj vrhova je tada

$$n = |X| = \sum_{i=1}^{r} |X_i| = r \cdot m.$$

Lema 4.23.

1. *Ako su $i, j \in \Omega$ i $p_{ij}^k > 0$, onda je $k \in \Omega$.*

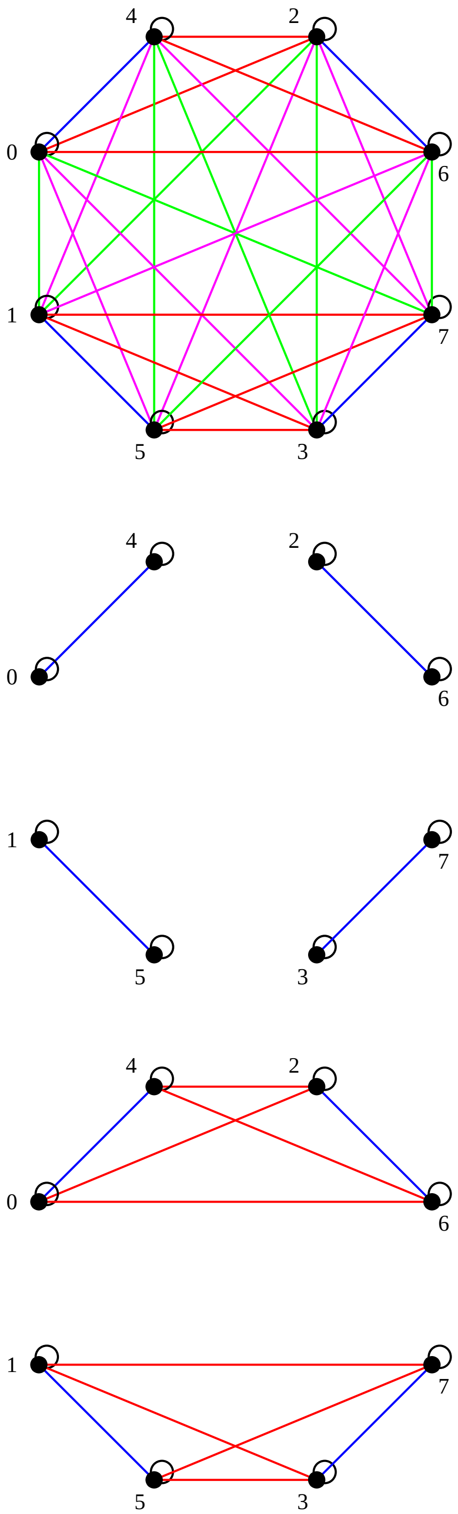
2. *Ako je $i \in \Omega$, onda je $i' \in \Omega$.*

Dokaz. 1. Neka je $(x, y) \in R_k$. Zbog $p_{ij}^k > 0$, postoji vrh z takav da je $(x, z) \in R_i$ i $(z, y) \in R_j$. Iz $i, j \in \Omega$ slijedi (x, z), $(z, y) \in R_\Omega$, pa je zbog tranzitivnosti relacije R_Ω i par $(x, y) \in R_\Omega$. Zaključujemo da je $k \in \Omega$. Ovo svojstvo je zapravo zatvorenost skupa indeksa Ω, tj. $\Omega^2 = \Omega$.

2. Slijedi na sličan način iz simetričnosti relacije R_Ω. $\square$

Prema zadatku 4.3, u koherentnoj konfiguraciji klasa konjugacije konačne grupe G imprimitivnost znači da postoji netrivijalna normalna podgrupa $N \trianglelefteq G$. Od normalne podgrupe dobivamo kvocijentnu grupu G/N. U ovoj cjelini vidjet ćemo da na sustavu imprimitivnosti možemo definirati takozvanu kvocijentnu koherentnu konfiguraciju. Pogledajmo prvo kako imprimitivna koherentna konfiguracija inducira potkonfiguracije na vlaknima.

Ako je $|\Omega| = s + 1$, možemo permutirati relacije $R_0, \dots, R_d$ tako da bude $\Omega = \{0, \dots, s\}$. U nastavku pretpostavljamo takvu numeraciju.



R_0, R_1, R_2, R_3, R_4

$\Omega = \{0, 4\}$

$R_\Omega = R_0 \cup R_4$

Vlakna: $\{0, 4\}$, $\{1, 5\}$, $\{2, 6\}$, $\{3, 7\}$

$\Omega = \{0, 2, 4\}$

$R_\Omega = R_0 \cup R_2 \cup R_4$

Vlakna: $\{0, 2, 4, 6\}$, $\{1, 3, 5, 7\}$

Slika 19: Osmerokut i njegovi sustavi imprimitivnosti.

Teorem 4.24. *Neka je $Y \subseteq X$ jedno od vlakna imprimitivne koherentne konfiguracije. Tada je $\mathcal{Y} = (Y, \{R_i|_{Y\times Y}\}_{i=0}^s)$ komutativna koherentna konfiguracija reda m sa s klasa. Presječni brojevi i stupnjevi od $\mathcal{Y}$ i $\mathcal{X}$ se podudaraju: $p_{ij}^k(\mathcal{Y}) = p_{ij}^k(\mathcal{X})$ i $n_i(\mathcal{Y}) = n_i(\mathcal{X})$ za $i, j, k \in \{0, \ldots, s\}$. Ako je $\mathcal{X}$ simetrična, onda je i $\mathcal{Y}$ simetrična.*

Dokaz. Provjeravamo svojstva iz definicije 1.38 za $\mathcal{Y}$. Restrikcija $R_0|_{Y\times Y} = \{(y, y) \mid y \in Y\}$ je dijagonala od Y. Restringirane relacije $\{R_i|_{Y\times Y}\}_{i=0}^s$ čine particiju od $Y \times Y$. Vrijedi $Y \times Y \subseteq R_\Omega$, pa za bilo koji par $(x, y) \in Y \times Y$ postoji $i \in \{0, \ldots, s\}$ takav da je $(x, y) \in R_i$. U prethodnoj lemi vidjeli smo da iz $i \in \{0, \ldots, s\}$ slijedi $i' \in \{0, \ldots, s\}$, a očito je $(R_i|_{Y\times Y})^t = R_i^t|_{Y\times Y}$. Konačno, ako su $i, j, k \in \{0, \ldots, s\}$ i vrhovi $x, y \in Y$ su u relaciji R_k, presječni broj u $\mathcal{X}$ je

$$p_{ij}^k(\mathcal{X}) = |\{z \in X \mid (x, z) \in R_i, (z, y) \in R_j\}|.$$

Svaki element z iz tog skupa je u relaciji R_Ω sa x i y, pa leži u istoj klasi ekvivalencije Y. Zato se taj presječni broj podudara s

$$p_{ij}^k(\mathcal{Y}) = |\{z \in Y \mid (x, z) \in R_i, (z, y) \in R_j\}|.$$

Iz komutativnosti od $\mathcal{X}$ direktno slijedi komutativnost od $\mathcal{Y}$, a stupnjevi se podudaraju zbog $n_i(\mathcal{Y}) = p_{ii'}^0 = n_i(\mathcal{X})$, za $i \in \{0, \ldots, s\}$. Također, iz simetričnosti od $\mathcal{X}$ direktno slijedi simetričnost od $\mathcal{Y}$. □

Na slici 19 prikazani su sustavi imprimitivnosti osmerokuta. Vrhovi su raspoređeni tako da vlakna budu razdvojena. Od zatvorenog skupa $\Omega = \{0, 4\}$ dobivamo četiri vlakna veličine $m = 2$ na kojima su inducirane podsheme s jednom klasom. Od zatvorenog skupa $\Omega = \{0, 2, 4\}$ dobivamo dva vlakna veličine $m = 4$ na kojima su inducirane podsheme izomorfne četverokutu. Promotrimo sada odnos Bose-Mesnerove algebre konfiguracije $\mathcal{X}$, tj. $\mathcal{A} = \langle A_0, \ldots, A_d\rangle$, i Bose-Mesnerove algebre potkonfiguracije $\mathcal{Y}$.

Lema 4.25. *Schurove idempotente $A_0, \ldots, A_s$ razapinju podalgebru $\mathcal{A}_\Omega$ algebre $\mathcal{A}$. To je potprostor vektorskog prostora zatvoren na matrično množenje, Schurovo množenje, transponiranje i kompleksno konjugiranje. Neutralni element za Schurovo množenje u $\mathcal{A}_\Omega$ je $A_\Omega = \sum_{i\in\Omega} A_i$.*

Dokaz. Zatvorenost na matrično množenje slijedi iz 1. tvrdnje leme 4.23, a zatvorenost na transponiranje iz 2. tvrdnje te leme. Ostale tvrdnje su očite. □

Ako indeksiramo matrice tako da vrhovi iz vlakna $X_1, \ldots, X_r$ budu uzastopni, onda su matrice iz podalgebre $\mathcal{A}_\Omega$ blok dijagonalne s r blokova veličine $m \times m$ na dijagonali. Na primjer, ako vrhovi osmerokuta idu redom 0, 4, 2, 6, 7, 3, 5, 1 (kao na slici 19), Schurove idempotene koje odgovaraju nepovezanim relacijama R_4 i R_2 su blok dijagonalne s četiri bloka veličine 2×2, odnosno dva bloka veličine 4×4 na dijagonali:

$$A_4 = \begin{bmatrix} 0&1&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&1&0 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 0&0&1&1&0&0&0&0 \\ 0&0&1&1&0&0&0&0 \\ 1&1&0&0&0&0&0&0 \\ 1&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&1 \\ 0&0&0&0&0&0&1&1 \\ 0&0&0&0&1&1&0&0 \\ 0&0&0&0&1&1&0&0 \end{bmatrix}.$$

Neutralni element za Schurovo množenje u podalgebri $\mathcal{A}_{\{0,4\}}$ je zbroj $A_{\{0,4\}} = A_0 + A_4$, a u podalgebri $\mathcal{A}_{\{0,2,4\}}$ je zbroj $A_{\{0,2,4\}} = A_0 + A_2 + A_4$:

$$A_{\{0,4\}} = \begin{bmatrix} 1&1&0&0&0&0&0&0 \\ 1&1&0&0&0&0&0&0 \\ 0&0&1&1&0&0&0&0 \\ 0&0&1&1&0&0&0&0 \\ 0&0&0&0&1&1&0&0 \\ 0&0&0&0&1&1&0&0 \\ 0&0&0&0&0&0&1&1 \\ 0&0&0&0&0&0&1&1 \end{bmatrix}, \; A_{\{0,2,4\}} = \begin{bmatrix} 1&1&1&1&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 0&0&0&0&1&1&1&1 \\ 0&0&0&0&1&1&1&1 \\ 0&0&0&0&1&1&1&1 \\ 0&0&0&0&1&1&1&1 \end{bmatrix}.$$

Općenito, neutralni element za Schurovo množenje je Kroneckerov produkt $A_\Omega = I \otimes J$ jedinične matrice I reda r i matrice J popunjene jedinicama reda m. To je blok dijagonalna matrica s r blokova J na dijagonali.

Lema 4.26. *Neka je $\mathcal{Y} = (Y, \{R_i|_{Y\times Y}\}_{i=0}^s)$ potkonfiguracija inducirana na vlaknu imprimitivne koherentne konfiguracije $\mathfrak{X} = (X, \{R_i\}_{i=0}^d)$.*

1. *Schurove idempotente od $\mathcal{Y}$ su rekstrikcije $A_i|_{Y\times Y}$, $i = 0, \ldots, s$.*
2. *Bose-Mesnerova algebra od $\mathcal{Y}$ je restrikcija podalgebre $\mathcal{A}_\Omega|_{Y\times Y}$.*
3. *Preslikavanje $A \mapsto A|_{Y\times Y}$ je izomorfizam između podalgebre $\mathcal{A}_\Omega$ i $\mathcal{A}_\Omega|_{Y\times Y}$ (obzirom na matrično množenje i obzirom na Schurovo množenje).*
4. *Izomorfizam šalje $\frac{1}{m}A_\Omega$ u trivijalnu primitivnu idempotentu $\frac{1}{m}J$ Bose-Mesnerove algebre od $\mathcal{Y}$.*

Dokaz. Sve tvrdnje su očite. □

Podalgebra $\mathcal{A}_\Omega \leq \mathcal{A}$ je zatvorena na matrično množenje i adjungiranje te matrice iz $\mathcal{A}_\Omega$ međusobno komutiraju. Po lemi 2.13, $\mathcal{A}_\Omega$ ima bazu sastavljenu od primitivnih idempotenta.

Teorem 4.27. *Postoji particija $\{\Lambda_0, \ldots, \Lambda_s\}$ skupa $\{0, \ldots, d\}$ takva da su primitivne idempotente podalgebre $\mathcal{A}_\Omega$ sume primitivnih idempotenta od $\mathcal{A}$:*

$$E_{\Lambda_i} = \sum_{\ell \in \Lambda_i} E_\ell, \quad i = 0, \ldots, s.$$

Možemo pretpostaviti da je $0 \in \Lambda_0$, a tada je $E_{\Lambda_0} = \frac{1}{m} A_\Omega$.

Zadatak 4.28. *Dokažite teorem 4.27. U GAP paketu* AssociationSchemes *[2] izračunajte primitivne idempotente osmerokuta i odredite particije $\{\Lambda_0, \Lambda_1\}$ i $\{\Lambda_0, \Lambda_1, \Lambda_2\}$ od kojih dobivamo primitivne idempotente od $\mathcal{A}_\Omega$, za $\Omega = \{0, 4\}$ i $\Omega = \{0, 2, 4\}$.*

Primitivne idempotente potkonfiguracije $\mathcal{Y}$ dobivamo restrikcijom primitivnih idempotenta podalgebre $\mathcal{A}_\Omega$: $E_i(\mathcal{Y}) = (E_{\Lambda_i})|_{Y \times Y}$. Kreinovi parametri potkonfiguracije su brojevi $q_{ij}^k(\mathcal{Y})$ za koje vrijedi

$$E_{\Lambda_i} \circ E_{\Lambda_j} = \frac{1}{m} \sum_{k=0}^{s} q_{ij}^k(\mathcal{Y}) E_{\Lambda_k}.$$

Takvi brojevi postoje jer je podalgebra $\mathcal{A}_\Omega$ zatvorena na Schurovo množenje. Izaberemo indeks $h \in \Lambda_k$ i pomnožimo prethodnu relaciju s E_h, pa dobijemo vezu Kreinovih parametara konfiguracije i potkonfiguracije:

$$q_{ij}^k(\mathcal{Y}) = \frac{1}{r} \sum_{a \in \Lambda_i} \sum_{b \in \Lambda_j} q_{ab}^h(\mathcal{X}), \qquad i, j, k \in \{0, \ldots, s\}.$$

Element $\Lambda = \Lambda_0$ particije iz teorema 4.27 zatvoren je na "Schurovo množenje" podskupova indeksa iz zadatka 4.22, tj. vrijedi $\Lambda \circ \Lambda = \Lambda$.

U idućem teoremu definiramo kvocijentnu koherentnu konfiguraciju.

Teorem 4.29. *Neka je $\Omega = \{0, \ldots, s\}$ netrivijalni zatvoren skup i $\Sigma = \{X_1, \ldots, X_r\}$ odgovarajući sustav imprimitivnosti komutativne koherentne konfiguracije $\mathcal{X} = (X, \{R_i\}_{i=0}^d)$. Definiramo relacije na Σ:*

$$\tilde{R}_i = \{(X_a, X_b) \mid (\exists x \in X_a)(\exists y \in X_b)\ (x, y) \in R_i\}.$$

Tada je $\mathbb{Q} = (\Sigma, \{\tilde{R}_i\})$ komutativna koherentna konfiguracija reda r sa t klasa, pri čemu je $1 \leq t \leq d - s$. Ako je $\mathcal{X}$ simetrična, onda je i $\mathbb{Q}$ simetrična.

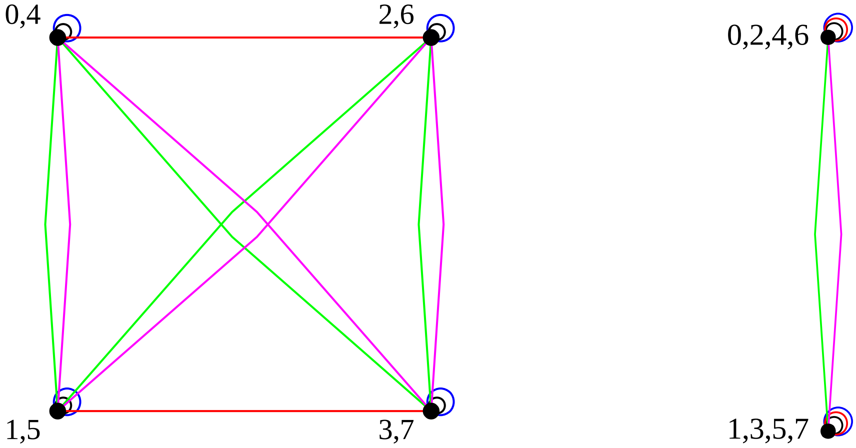
Skica dokaza. Broj relacija kvocijentne konfiguracije je manji od d jer se neke od relacija $\tilde{R}_0, \ldots, \tilde{R}_d$ podudaraju. Na primjer, za svaki $i \in \{0, \ldots, s\}$ relacija $\tilde{R}_i$ je "dijagonala" od Σ, tj. trivijalna relacija kvocijentne konfiguracije. Relacije $\tilde{R}_i$, $\tilde{R}_j$ se ili podudaraju, ili su disjunktne. Tako dobivamo parciju $\{\Omega_0, \ldots, \Omega_t\}$ skupa indeksa $\{0, \ldots, d\}$, pri čemu su u istom bloku indeksi i, j za koje je $\tilde{R}_i = \tilde{R}_j$. Pritom je $\Omega_0 = \Omega$ i particija $\{\Omega_0, \ldots, \Omega_t\}$ se sastoji od komponenta povezanosti jednog od distribucijskih grafova konfiguracije $\mathfrak{X}$. Dualno, particija $\{\Lambda_0, \ldots, \Lambda_s\}$ iz teorema 4.27 sastoji se od komponenta povezanosti jednog od reprezentacijskih grafova. Vrijedi $|\Lambda_0| = 1+t$ i primitivne idempotente možemo permutirati tako da bude $\Lambda_0 = \{0, \ldots, t\}$. U nastavku pretpostavljamo takvu numeraciju primitivnih idempotenta i pišemo $\Lambda = \Lambda_0$.

Lako je provjeriti svojstva 1.-3. iz definicije 1.38 za kvocijentnu konfiguraciju $\mathbb{Q}$. Da bismo provjerili 4. svojstvo, promotrimo podalgebru $\mathscr{A}_\Lambda^\circ$ Bose-Mesnerove algebre $\mathscr{A}$ razapetu primitivnim idempotentama $E_0, \ldots, E_t$. Prema lemi 2.5, ona ima bazu Schurovih idempotenta $\tilde{A}_0, \ldots, \tilde{A}_t$ takvu da je $\tilde{A}_i = A_{\Omega_i} = \sum_{k \in \Omega_i} A_k$. Schurove idempotente $\tilde{A}_i$ su konstantne na vlaknima sustava imprimitivnosti, tj. svi unosi od $\tilde{A}_i|_{X_a \times X_b}$ su ili 0 ili 1. Zato ih možemo prikazati kao Kroneckerove produkte $\tilde{A}_i = D_i \otimes J$, $i = 0, \ldots, t$. Ovdje je J matrica popunjena jedinicama dimenzija $m \times m$, a $D_0, \ldots, D_t$ su $r \times r$ matrice popunjene nulama ili jedinicama. To su upravo Schurove idempotente kvocijentne konfiguracije, tj. incidencijske matrice relacija $\tilde{R}_i$. Pridruživanje $\tilde{A}_i \mapsto D_i$ proširuje se po linearnosti do izomorfizma između podalgebre $\mathscr{A}_\Lambda^\circ$ i Bose-Mesnerove algebre kvocijentne konfiguracije $\mathbb{Q}$. Kreinovi parametri i kratnosti od $\mathbb{Q}$ i $\mathfrak{X}$ se podudaraju: $q_{ij}^k(\mathbb{Q}) = q_{ij}^k(\mathfrak{X})$ i $m_i(\mathbb{Q}) = m_i(\mathfrak{X})$ za $i, j, k \in \{0, \ldots, t\}$. Red kvocijentne konfiguracije je $r = \sum_{i=0}^t m_i$, a presječne brojeve dobivamo na dualan način kao Kreinove parametre potkonfiguracija:

$$p_{ij}^k(\mathbb{Q}) = \frac{1}{m} \sum_{a \in \Omega_i} \sum_{b \in \Omega_j} p_{ab}^h(\mathfrak{X}), \quad i, j, k \in \{0, \ldots, t\}, \quad h \in \Omega_k.$$

□

Na slici 20 prikazane su kvocijentne konfiguracije osmerokuta. Na lijevoj strani sustav imprimitivnosti dobiven je od zatvorenog skupa $\Omega = \{0, 4\}$, a na desnoj strani od zatvorenog skupa $\Omega = \{0, 2, 4\}$. Vlakna sa slike 19 stisnuta su u vrhove kvocijentne konfiguracije. Relacije $\tilde{R}_i$ dobivene su od relacija osmerokuta kao u teoremu 4.29 i generiraju particiju skupa indeksa $\{\Omega_0, \Omega_1, \Omega_2\}$, odnosno $\{\Omega_0, \Omega_1\}$. Lijeva kvocijentna konfiguracija izomorfna je četverokutu, a desna trivijalnoj asocijacijskoj shemi s dva vrha i jednom relacijom.



$\Omega = \Omega_0 = \{0, 4\}$, $\Omega_1 = \{2\}$, $\Omega_2 = \{1, 3\}$ $\qquad$ $\Omega = \Omega_0 = \{0, 2, 4\}$, $\Omega_1 = \{1, 3\}$

Slika 20: Kvocijentne konfiguracije osmerokuta.

4.3 Imprimitivne sheme s tri klase

U propozicijama 3.5 i 3.7 karakterizirali smo imprimitivne jako regularne grafove s $\mu = 0$ i $\mu = \Bbbk$. Odgovarajuća asocijacijska shema ima dvije klase: R_1 je relacija susjedstva grafa s $\mu = 0$, a R_2 njegovog komplementa s $\mu = \Bbbk$. Sada možemo objasniti ovu karakterizaciju pomoću podshema i kvocijentne sheme u specijalnom slučaju shema s dvije klase.

Neka je $\mathcal{X}$ asocijacijska shema s dvije klase. Do na numeraciju relacija R_1 i R_2, jedini mogući netrivijalan zatvoren skup je $\Omega = \{0, 1\}$. Podsheme na vlaknima imaju samo jednu netrivijalnu relaciju, restrikciju od R_1, pa su izomorfne potpunom grafu K_m. Zato je R_1 disjunktna unija potpunih grafova $r \cdot K_m$. S druge strane, kvocijentna shema također ima samo jednu relaciju i izomorfna je potpunom grafu K_r. Iz toga slijedi da je R_2 relacija susjedstva potpunog multipartitnog grafa $K_{m,\ldots,m}$ (r indeksa m).

U ovoj cjelini proučit ćemo imprimitivne asocijacijske sheme s tri klase R_1, R_2 i R_3. Do na njihovu numeraciju, mogućnosti za zatvorene skupove su A: $\Omega = \{0, 1, 2\}$ ili B: $\Omega = \{0, 1\}$. U slučaju A kvocijentna shema ima samo jednu klasu i R_3 je relacija susjedstva od $K_{m,\ldots,m}$. Podsheme na vlaknima imaju dvije netrivijalne klase, restrikcije od R_1 i R_2. Prema tome, svaka od podshema ekvivalentna je jako regularnom grafu i njegovu komplementu. Inducirani grafovi na različitim vlaknima imaju iste parametre $SRG(m, \Bbbk, \lambda, \mu)$ i $SRG(m, m - 1 - \Bbbk, m - 2\Bbbk + \mu - 2, m - 2\Bbbk + \lambda)$, ali ne moraju biti izomorfni.

Ako postoji jako regularan graf $SRG(m, \mathscr{k}, \lambda, \mu)$, za svaki $r \geq 2$ možemo napraviti r kopija takvog grafa na disjunktnim skupovima vrhova i tako dobiti relaciju R_1. Za R_2 uzmemo relaciju susjedstva disjunktne unije komplemenata tih grafova, a za R_3 relaciju susjedstva od $K_{m,\ldots,m}$, grafa sa svim bridovima između vlakna. Tako dobijemo imprimitivnu asocijacijsku shemu tipa A. Ako postoji više neizomorfnih grafova $SRG(m, \mathscr{k}, \lambda, \mu)$, možemo ih neovisno birati na svakom vlaknu i napraviti puno kombinatorno neizomorfnih asocijacijskih shema. Međutim, sve su "algebarski izomorfne", što znači da su im Bose-Mesnerove algebre izomorfne. To slijedi zato što sve imaju iste parametre: presječne brojeve, Kreinove parametre, svojstvene vrijednosti i dualne svojstvene vrijednosti. Dovoljno je izračunati svojstvenu matricu $P = [P_j(i)]_{i,j=0}^3$ jer prema rezultatima iz poglavlja 2 sve ostale parametre možemo izraziti preko svojstvenih vrijednosti.

U poglavlju 3 odredili smo svojstvenu matricu jako regularnog grafa (28). Zamijenimo broj vrhova n s veličinom vlakna m, a svojstvene vrijednosti iz formula (26) označimo $\mathscr{r}$ i $\mathscr{s}$ jer nam slovo r sada označava broj vlakna.

Propozicija 4.30. *Neka je asocijacijska shema s tri klase imprimitivna tipa A. Ako je dobivena od r disjunktnih grafova* $SRG(m, \mathscr{k}, \lambda, \mu)$*, onda je njezina svojstvena matrica*

$$P = \begin{bmatrix} 1 & \mathscr{k} & m-1-\mathscr{k} & (r-1)m \\ 1 & \mathscr{k} & m-1-\mathscr{k} & -m \\ 1 & \mathscr{r} & -\mathscr{r}-1 & 0 \\ 1 & \mathscr{s} & -\mathscr{s}-1 & 0 \end{bmatrix}.$$

Dokaz. Označimo s A i $\bar{A}$ matrice susjedstva grafa $SRG(m, \mathscr{k}, \lambda, \mu)$ i njegova komplementa. Svojstvene vrijednosti matrice A su $\mathscr{k}$, $\mathscr{r}$ i $\mathscr{s}$, a matrice $\bar{A}$ su $m-1-\mathscr{k}$, $-\mathscr{r}-1$ i $-\mathscr{s}-1$. Pritom je zajednički svojstveni vektor koji odgovara $\mathscr{k}$ i $m-1-\mathscr{k}$ jednak $\mathbb{1}_m = (1, \ldots, 1)$ (m komponenta), a druga dva zajednička svojstvena potprostora sadržana su u $\langle \mathbb{1}_m \rangle^\perp$. Prve dvije Schurove idempotente naše asocijacijske sheme su Kroneckerovi produkti $A_1 = I_r \otimes A$ i $A_2 = I_r \otimes \bar{A}$. Po propoziciji 2.46, te dvije matrice imaju iste svojstvene vrijednosti kao A i $\bar{A}$. Treća Schurova idempotenta je $A_3 = (J_r - I_r) \otimes J_m$. To je matrica susjedstva potpunog multipartitnog grafa $K_{m,\ldots,m}$. Matrica J_m ima spektar $\{m, 0\}$ sa svojstvenim potprostorima $\langle \mathbb{1}_m \rangle$ i $\langle \mathbb{1}_m \rangle^\perp$, a matrica $J_r - I_r$ ima spektar $\{r-1, -1\}$ sa svojstvenim potprostorima $\langle \mathbb{1}_r \rangle$ i $\langle \mathbb{1}_r \rangle^\perp$. Po propoziciji 2.46, svojstvene vrijednosti od A_3 na potprostoru $\mathbb{R}^r \otimes \mathbb{1}_m$, na kojem A_1 i A_2 imaju svojstvene vrijednosti $\mathscr{k}$ i $m-1-\mathscr{k}$, su $(r-1)m$ i $-m$. Ostale svojstvene vrijednosti od A_3 su 0. Dakle, svojstvena matrica P ima unose kao u iskazu propozicije. $\square$

U dokazu smo računali sa shemom dobivenom od r kopija istog grafa, ali zaključak vrijedi i ako su inducirani grafovi na vlaknima neizomorfni. Promotrimo sada imprimitivne sheme tipa B, sa zatvorenim skupom $\Omega = \{0, 1\}$. Inducirane sheme na vlaknima imaju jednu klasu i izomorfne su s K_m. Relacija R_1 je susjedstvo u disjunktnoj uniji $r \cdot K_m$, a pripadna Schurova idempotenta je $A_1 = I_r \otimes J_m - I_{rm}$. Kvocijentna shema ima $t = 1$ ili $t = 2$ relacija, a odgovarajuće slučajeve označavamo B_1 i B_2.

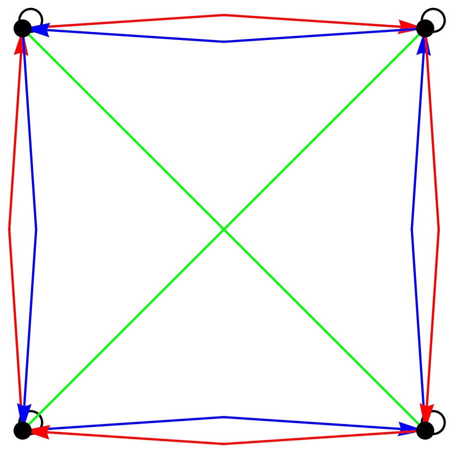
Slučaj B_2 je jednostavniji. Kvocijentna shema sastoji se od jako regularnog grafa $SRG(r, \mathscr{k}, \lambda, \mu)$ i njegova komplementa s matricama susjedstva A i $\bar{A}$. Odgovarajuće Schurove idempotente su $A_2 = A \otimes J_m$ i $A_3 = \bar{A} \otimes J_m$. Kao i kod tipa A, imprimitivnu shemu tipa B_2 možemo napraviti od svakog jako regularnog grafa $SRG(r, \mathscr{k}, \lambda, \mu)$ i za svaki $m \geq 2$. Sličnim zaključivanjem kao u dokazu prethodne propozicije izračunavamo svojstvenu matricu.

Propozicija 4.31. *Neka je asocijacijska shema s tri klase imprimitivna tipa B_2. Ako ima vlakna veličine m i kvocijentni graf je $SRG(r, \mathscr{k}, \lambda, \mu)$, onda je njezina svojstvena matrica*

$$P = \begin{bmatrix} 1 & m-1 & m\mathscr{k} & m(r-1-\mathscr{k}) \\ 1 & m-1 & m\mathscr{r} & m(-\mathscr{r}-1) \\ 1 & m-1 & m\mathscr{s} & m(-\mathscr{s}-1) \\ 1 & -1 & 0 & 0 \end{bmatrix}.$$

Kad bismo znali sve jako regularne grafove, opisanim konstrukcijama mogli bismo dobiti sve imprimitivne sheme tipa A i tipa B_2. Ta dva slučaja smatramo degeneriranim jer se svode na proučavanje jako regularnih grafova. Slučaj B_1 je kompliciraniji i zanimljiviji. Kao i u slučaju B_2, relacija R_1 odgovara susjedstvu u $r \cdot K_m$, a relacije R_2 i R_3 u uniji daju susjedstvo u $K_{m,\ldots,m}$. Između svaka dva vlakna sada imamo bridove iz R_2 i iz R_3, pa kvocijentna shema ima samo jednu klasu i izomorfna je potpunom grafu K_r. Za konstrukciju takvih shema trebali bismo rastaviti $K_{m,\ldots,m}$ na dva bridno disjunktna razapinjuća podgrafa tako da budu zadovoljena svojstva iz definicije 1.1. Za to nemamo jednostavan recept.

Jedan mali primjer asocijacijske sheme tipa B_1 vidjeli smo na slici 3. Nastaje Schurovom konstrukcijom od permutacijske grupe $G_1 = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle$ ili od klasa konjugacije te grupe, izomorfne sa $\mathbb{Z}_2 \times \mathbb{Z}_2$. Shema ima tri zatvorena skupa $\Omega_1 = \{0, 1\}$, $\Omega_2 = \{0, 2\}$, $\Omega_3 = \{0, 3\}$. Dobivamo $r = 2$ vlakna veličine $m = 2$ i na svakom od njih podshemu s dva vrha i jednom relacijom, a takva je i kvocijentna shema. Sličan, ali nesimetričan primjer nastaje od cikličke grupe $G_2 = \langle (1\ 2\ 3\ 4) \rangle$. Koherentna konfiguracija dobivena Schurovom konstrukcijom od G_2 ili pomoću klasa konjugacije



Slika 21: Imprimitivna koherentna konfiguracija tipa B_1.

cikličke grupe $\mathbb{Z}_4$ prikazana je na slici 21. Ima samo jedan zatvoren skup $\Omega = \{0, 2\}$, a potkonfiguracije i kvocijentna konfiguracija su iste kao za G_1.

Još dva sporadična prijera shema tipa B_1 su trodimenzionalna kocka, tj. Hammingova shema $H(3, 2)$, te Johnsonova shema $J(6, 3)$ (primjeri 1.5 i 1.6). Općenito, $H(3, q)$ i $J(v, 3)$ su asocijacijske sheme s tri klase, ali za $q > 2$ i za $v > 6$ su primitivne.

Zadatak 4.32. *Proučite sustave imprimitivnosti od $H(3, 2)$ i $J(6, 3)$ i uvjerite se da su to sheme tipa B_1. Dokažite da su $H(3, q)$, $q > 2$ i $J(v, 3)$, $v > 6$ primitivne.*

Zadatak 4.33. *Ispitajte (im)primitivnost Grassmannove sheme i sheme bilinearnih formi (primjeri 1.7 i 1.8) u slučajevima kad imaju tri klase.*

Beskonačnu familiju shema tipa B_1 dobivamo od incidencijskih grafova simetričnih dizajna, kao u zadatku 1.35. Neka je $\mathcal{D}$ simetrični $(v, \Bbbk, \lambda)$ dizajn i A njegova incidencijska matrica. To je $v \times v$ matrica kojoj su reci indeksiranim točkama od $\mathcal{D}$, a stupci blokovima. Na (i, j)-tom mjestu ima 1 ako je i-ta točka incidentna s j-tim blokom, a 0 inače. Činjenica da je $\mathcal{D}$ simetrični $(v, \Bbbk, \lambda)$ dizajn ekvivalentna je sa $AA^t = A^tA = (\Bbbk - \lambda)I + \lambda J$. Incidencijski graf dizajna $\mathcal{D}$ ima točke i blokove kao vrhove, a susjedni su ako su incidentni. To je bipartitan graf s matricom susjedstva

$$A_1 = \begin{bmatrix} 0 & A \\ A^t & 0 \end{bmatrix}.$$

U zadatku 1.35 pokazali smo da je taj graf distancijsko regularan dijametra $d = 3$. Schurove idempotente koje odgovaraju vrhovima na udaljenosti 2 i 3 su redom

$$A_2 = \begin{bmatrix} J - I & 0 \\ 0 & J - I \end{bmatrix} \quad \text{i} \quad A_3 = \begin{bmatrix} 0 & J - A \\ J - A^t & 0 \end{bmatrix}.$$

Graf kojemu je A_2 matrica susjedstva je nepovezan i izomorfan s $2 \cdot K_v$. Sustav imprimitivnosti sastoji se od $r = 2$ vlakna veličine $m = v$, a kvocijentna shema od dva vrha i jedne relacije. Dakle, to je imprimitivna asocijacijska shema tipa B_1 s tri klase. U zadatku 1.35 odredili smo joj presječne brojeve, a sada je cilj odrediti svojstvenu matricu.

Lema 4.34. *Neka je $M = (\Bbbk - \lambda)I + \lambda J$ kvadratna matrica reda v s elementima $\Bbbk$ na dijagonali i λ izvan dijagonale. Matrica M ima svojstvenu vrijednost $\Bbbk + (v-1)\lambda$ kratnosti 1 i $\Bbbk - \lambda$ kratnosti $v - 1$.*

Dokaz. Direktno provjerimo da je $M\mathbb{1} = (\Bbbk - (v-1)\lambda)\mathbb{1}$. Nadalje, za vektor $x \in \mathbb{R}^v$ i $\lambda \neq 0$ vidimo da je $Mx = (\Bbbk - \lambda)x$ ekvivalentno s $Jx = 0$, tj. $x \in \langle \mathbb{1} \rangle^\perp$. □

Propozicija 4.35. *Asocijacijska shema iz zadatka 1.35 ima svojstvenu matricu*

$$P = \begin{bmatrix} 1 & \Bbbk & v-1 & v-\Bbbk \\ 1 & -\Bbbk & v-1 & \Bbbk - v \\ 1 & \sqrt{\Bbbk - \lambda} & -1 & -\sqrt{\Bbbk - \lambda} \\ 1 & -\sqrt{\Bbbk - \lambda} & -1 & \sqrt{\Bbbk - \lambda} \end{bmatrix}.$$

Dokaz. Neka je $\mathbb{1} = (1, \ldots, 1)$ vektor iz $\mathbb{R}^v$. Računamo:

$$A_1 \begin{bmatrix} \mathbb{1} \\ \mathbb{1} \end{bmatrix} = \begin{bmatrix} 0 & A \\ A^t & 0 \end{bmatrix} \begin{bmatrix} \mathbb{1} \\ \mathbb{1} \end{bmatrix} = \begin{bmatrix} A\mathbb{1} \\ A^t\mathbb{1} \end{bmatrix} = \Bbbk \begin{bmatrix} \mathbb{1} \\ \mathbb{1} \end{bmatrix},$$

$$A_2 \begin{bmatrix} \mathbb{1} \\ \mathbb{1} \end{bmatrix} = \begin{bmatrix} J - I & 0 \\ 0 & J - I \end{bmatrix} \begin{bmatrix} \mathbb{1} \\ \mathbb{1} \end{bmatrix} = \begin{bmatrix} (J-I)\mathbb{1} \\ (J-I)\mathbb{1} \end{bmatrix} = (v-1) \begin{bmatrix} \mathbb{1} \\ \mathbb{1} \end{bmatrix},$$

$$A_3 \begin{bmatrix} \mathbb{1} \\ \mathbb{1} \end{bmatrix} = \begin{bmatrix} 0 & J - A \\ J - A^t & 0 \end{bmatrix} \begin{bmatrix} \mathbb{1} \\ \mathbb{1} \end{bmatrix} = \begin{bmatrix} (J-A)\mathbb{1} \\ (J-A^t)\mathbb{1} \end{bmatrix} = (v-\Bbbk) \begin{bmatrix} \mathbb{1} \\ \mathbb{1} \end{bmatrix}.$$

Dakle, $\begin{bmatrix} \mathbb{1} \\ \mathbb{1} \end{bmatrix}$ je zajednički svojstveni vektor od kojeg dobivamo prvi redak matrice P. Slično vidimo da od vektora $\begin{bmatrix} \mathbb{1} \\ -\mathbb{1} \end{bmatrix}$ dobivamo drugi redak od P. Neka je $M = AA^t = A^tA$ i uzmimo neki vektor $x \in \langle \mathbb{1} \rangle^\perp$. Po prethodnoj lemi je $Mx = (k-\lambda)x$, a očito je $Jx = 0$. Definiramo $y = \frac{1}{\sqrt{{\mathchar'26\mkern-9mu k}-\lambda}} A^t x$. Tada je $A^t x = \sqrt{k-\lambda}\, y$ i $Ay = \frac{1}{\sqrt{{\mathchar'26\mkern-9mu k}-\lambda}} Mx = \sqrt{{\mathchar'26\mkern-9mu k}-\lambda}\, x$. Budući da J komutira s A^t, vrijedi $Jy = 0$. Računamo:

$$A_1 \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 & A \\ A^t & 0 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} Ay \\ A^t x \end{bmatrix} = \sqrt{{\mathchar'26\mkern-9mu k}-\lambda} \begin{bmatrix} x \\ y \end{bmatrix},$$

$$A_2 \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} J-I & 0 \\ 0 & J-I \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} (J-I)x \\ (J-I)y \end{bmatrix} = - \begin{bmatrix} x \\ y \end{bmatrix},$$

$$A_3 \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 & J-A \\ J-A^t & 0 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} (J-A)y \\ (J-A^t)x \end{bmatrix} = -\sqrt{{\mathchar'26\mkern-9mu k}-\lambda} \begin{bmatrix} x \\ y \end{bmatrix}.$$

Dakle, vektori oblika $\begin{bmatrix} x \\ y \end{bmatrix}$ čine zajednički $(v-1)$-dimenzionalni svojstveni potprostor od kojeg dobivamo treći redak matrice P. Sličnim računom vidimo da od vektora oblika $\begin{bmatrix} x \\ -y \end{bmatrix}$ dobivamo četvrti redak od P. $\square$

Zanimljivo je da spektar matrica A_1 i A_3 ovisi samo o parametrima dizajna $(v, {\mathchar'26\mkern-9mu k}, \lambda)$. Spektar incidencijske matrice A nije jednoznačno određen s parametrima, nego ovisi čak o numeraciji točaka i blokova dizajna, naravno i o tome koji dizajn s parametrima $(v, {\mathchar'26\mkern-9mu k}, \lambda)$ uzmemo. Budući da ima beskonačno mnogo simetričnih dizajna s beskonačno mnogo različitih parametara $(v, {\mathchar'26\mkern-9mu k}, \lambda)$, konstruirali smo beskonačnu seriju imprimitivnih shema tipa B_1. Međutim, sve imaju samo dva vlakna. Za tip A imprimitivnih shema mogli smo proizvoljno zadati broj vlakna r, a za tip B_2 broj vlakna je broj vrhova jako regularnog grafa od kojeg dobivamo kvocijentnu shemu i također može biti po volji velik. Smisao sljedeće definicije je generalizacija shema tipa B_1, kakve smo konstruirali u zadatku 1.35, na veći broj vlakna.

Definicija 4.36. Sustav spojenih simetričnih dizajna $SSSD(v, {\mathchar'26\mkern-9mu k}, \lambda; r)$ *(eng.* linked system of symmetric designs, *LSSD) je graf sa skupom vrhova* $X = X_1 \cup \cdots \cup X_r$ *(disjunktna unija). Skupove* X_i *zovemo* vlaknima *i svaki ima* v *vrhova, pa je ukupan broj vrhova* $n = rv$*. Bridovi zadovoljavaju:*

1. *svaki brid ima krajeve u različitim vlaknima;*

2. *za sve* $i, j \in \{1, \ldots, r\}$*,* $i \neq j$*, inducirani podgraf na* $X_i \cup X_j$ *je incidencijski graf nekog* $(v, {\mathchar'26\mkern-9mu k}, \lambda)$ *dizajna;*

3. *postoje konstante* μ *i* ν *takve da za različite* $i, j, k \in \{1, \ldots, r\}$ *i za svaki izbor vrhova* $x \in X_i$*,* $y \in X_j$*, broj zajedničkih susjeda od* x *i* y *u vlaknu* X_k *je* μ *ako su* x *i* y *susjedni, a* ν *ako nisu susjedni.*

Prvi uvjet iz definicije kaže da je SSSD r-partitni graf. *Multipartitni komplement* dobivamo tako da zamijenimo susjedstvo i nesusjedstvo vrhova iz različitih vlakna, a vrhove iz istog vlakna ostavimo nesusjednima.

Lema 4.37. *Multipartitni komplement grafa* $SSSD(v, \Bbbk, \lambda; r)$ *je graf* $SSSD(v, v-\Bbbk, v-2\Bbbk+\lambda; r)$. *Pritom su za komplement konstante iz trećeg uvjeta definicije* $\bar{\mu} = v - 2\Bbbk + \nu$ *i* $\bar{\nu} = v - 2\Bbbk + \mu$.

Dokaz. Vrijedi zato što je komplement simetričnog $(v, \Bbbk, \lambda)$ dizajna simetrični $(v, v-\Bbbk, v-2\Bbbk+\lambda)$ dizajn. Komplementarne parametre $\bar{\lambda} = v-2\Bbbk+\lambda$, $\bar{\mu}$ i $\bar{\nu}$ dobijemo iz formule uključivanja-isključivanja. □

Ako je broj vlakna $r = 2$, treći uvjet iz definicije 4.36 ispunjen je "na prazno", a $SSSD(v, \Bbbk, \lambda; 2)$ je ekvivalentan incidencijskom grafu jednog simetričnog dizajna. To je upravo distancijsko regularni graf iz zadatka 1.35. U nastavku pretpostavljamo da je $r \geq 3$. Tada parametri $(v, \Bbbk, \lambda)$, osim nužnog uvjeta $\lambda(v-1) = \Bbbk(\Bbbk-1)$ za postojanje simetričnog dizajna, zadovoljavaju vrlo jake dodatne uvjete. Iz definicije vidimo da je graf $SSSD(v, \Bbbk\ \lambda; r)$ ako i samo ako je svaki njegov inducirani podgraf na tri vlakna $SSSD(v, \Bbbk, \lambda; 3)$. Zato se za dokazivanje nužnih uvjeta možemo ograničiti na $r = 3$.

Teorem 4.38. *Neka postoji* $SSSD(v, \Bbbk, \lambda; 3)$. *Tada vrijedi:*

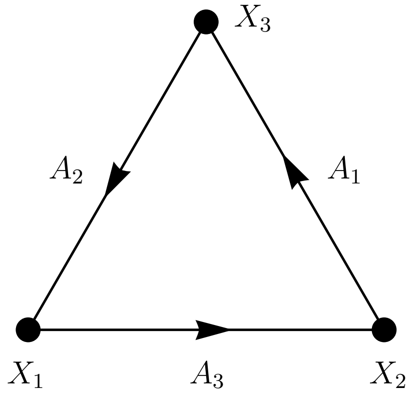
1. *red simetričnog dizajna* $\Bbbk - \lambda$ *je kvadrat prirodnog broja,*
2. $\nu = \frac{\Bbbk(\Bbbk \pm \sqrt{\Bbbk-\lambda})}{v}$ *i* $\mu = \nu \mp \sqrt{\Bbbk - \lambda}$,
3. $M(v, k) > 1$ *i* $M(v, \sqrt{\Bbbk - \lambda}) > 1$ *(M je najveći zajednički djelitelj),*
4. v *dijeli točno jedan od brojeva* $\Bbbk(\Bbbk + \sqrt{\Bbbk - \lambda})$, $\Bbbk(\Bbbk - \sqrt{\Bbbk - \lambda})$.

Dokaz. Neka je A_1 incidencijska matrica simetričnog dizajna kojem su točke vrhovi iz vlakna X_2, a blokovi vrhovi iz X_3. Incidencija je susjedstvo u induciranom podgrafu na $X_2 \cup X_3$. Slično, neka je A_2 incidencijska matrica između X_3 i X_1, a A_3 između X_1 i X_2 (slika 22). Znamo da vrijedi $A_i J = J A_i = \Bbbk J$ i $A_i A_i^t = A_i^t A_i = (\Bbbk - \lambda) I + \lambda J$ za $i = 1, 2, 3$. U produktu matrica $A_2 A_1$, element na mjestu (i, j) je broj vrhova iz X_3 koji su zajednički susjedi i-tog vrha iz X_2 i j-tog vrha iz X_1. Po trećem uvjetu iz definicije 4.36, taj broj je μ ako A_3^t na (i, j)-tom mjestu ima 1, a ν ako ima 0. Time smo dokazali

$$A_2 A_1 = \mu A_3^t + \nu(J - A_3^t) = \nu J + (\mu - \nu) A_3^t. \tag{41}$$

Na sličan način vidimo da vrijedi

$$A_3 A_2 = \nu J + (\mu - \nu) A_1^t. \tag{42}$$



Slika 22: Incidencijske matrice između vlakna. Strelice idu od točaka prema blokovima.

Pomnožimo (41) zdesna sa J i iskoristimo $J^2 = vJ$, pa dobijemo $\Bbbk^2 J = \nu v J + (\mu - \nu)\Bbbk J$, odnosno

$$\nu v = \Bbbk(\Bbbk + \nu - \mu). \tag{43}$$

Zatim pomnožimo (41) s lijeva sa A_2^t i iskoristimo (42):

$$\begin{aligned}(\Bbbk - \lambda)A_1 + \lambda\Bbbk J &= \nu\Bbbk J + (\mu - \nu)A_2^t A_3^t = \nu\Bbbk J + (\mu - \nu)(A_3 A_2)^t \\ &= \nu\Bbbk J + (\mu - \nu)\left[\nu J + (\mu - \nu)A_1\right] \\ &= (\mu - \nu)^2 A_1 + \left[\nu\Bbbk + (\mu - \nu)\nu\right] J.\end{aligned}$$

Iz linearne nezavisnosti A_1 i J slijedi $\Bbbk - \lambda = (\mu - \nu)^2$ i time smo dokazali prvu tvrdnju teorema. Ako označimo $\nu - \mu = \pm\sqrt{\Bbbk - \lambda}$, iz (43) slijedi druga tvrdnja.

Za treću tvrdnju pretpostavimo da je $1 < k < \frac{v}{2}$; u suprotnom napravimo multipartitni komplement. Tada je $k \pm \sqrt{\Bbbk - \lambda} < v$, pa iz $\nu = \frac{\Bbbk(\Bbbk \pm \sqrt{\Bbbk - \lambda})}{v} \in \mathbb{N}$ vidimo da je $M(v, \Bbbk) > 1$. Dalje, nužan uvjet za postojanje simetričnog dizajna možemo zapisati kao $\lambda v = k^2 - (\Bbbk - \lambda)$. To transformiramo u

$$\lambda = \frac{\Bbbk(\Bbbk \pm \sqrt{\Bbbk - \lambda})}{v} \mp \frac{\sqrt{\Bbbk - \lambda}(\Bbbk \pm \sqrt{\Bbbk - \lambda})}{v}. \tag{44}$$

U jednoj od ove dvije jednadžbe prvi razlomak je prirodan broj, pa je i drugi razlomak prirodan broj. Iz $\frac{\sqrt{\Bbbk - \lambda}(\Bbbk \pm \sqrt{\Bbbk - \lambda})}{v} \in \mathbb{N}$ i $k \pm \sqrt{\Bbbk - \lambda} < v$ isto kao ranije zaključujemo da je $M(v, \sqrt{\Bbbk - \lambda}) > 1$ i time je treća tvrdnja dokazana.

Iz formule za ν jasno je da v dijeli bar jedan od brojeva $\Bbbk(\Bbbk \pm \sqrt{\Bbbk - \lambda})$. Za četvrtu tvrdnju treba dokazati da ne dijeli oba broja. U suprotnom, iz (44) slijedi da v dijeli oba broja $\sqrt{\Bbbk-\lambda}(\Bbbk \pm \sqrt{\Bbbk-\lambda})$, a tada dijeli i njihovu razliku $2(\Bbbk-\lambda)$. No tada je $v \leq 2(\Bbbk-\lambda) < 2\Bbbk$, što je kontradikcija s pretpostavkom $k < \frac{v}{2}$. $\square$

Iz teorema slijedi da su konstante μ i ν jednoznačno određene s parametrima $(v, \Bbbk, \lambda)$. Broj $\sqrt{\Bbbk-\lambda}$ jednak je jednom od brojeva $\mu-\nu$ ili $\nu-\mu$. U prvom slučaju vrijedi $\mu > \nu$ i za SSSD kažemo da je *μ-naglašen*, a u drugom slučaju vrijedi $\nu > \mu$ i kažemo da je *ν-naglašen* (eng. *μ-heavy, ν-heavy*). Iz formula za $\bar{\mu}$ i $\bar{\nu}$ u lemi 4.37 vidimo da je multipartitni komplement μ-naglašenog SSSD-a ν-naglašen, i obrnuto. Tablica [99] sadrži 199 trojki $(v, \Bbbk, \lambda)$ koje zadovoljavaju $k \leq \frac{v}{2}$ i $\Bbbk \leq 41$. Od toga samo šest trojki zadovoljava sve nužne uvjete iz teorema 4.38. Navodimo ih u tablici 3 lijevo. Trojka $(36, 15, 6)$ je μ-naglašena, a ostalih pet trojki lijevo su ν-naglašene. Desno navodimo parametre multipartitnih komplementa.

$(v, \Bbbk, \lambda)$	μ	ν	$(v, \bar{\Bbbk}, \bar{\lambda})$	$\bar{\mu}$	$\bar{\nu}$	Tip	Noda
$(16, 6, 2)$	1	3	$(16, 10, 6)$	7	5	Opt	$r \leq 8$
$(36, 15, 6)$	8	5	$(36, 21, 12)$	11	14	Pes	–
$(45, 12, 3)$	1	4	$(45, 33, 24)$	25	22	Opt	$r \leq 50/7$
$(64, 28, 12)$	10	14	$(64, 36, 20)$	22	18	Opt	$r \leq 32$
$(96, 20, 4)$	1	5	$(96, 76, 60)$	61	57	Opt	$r \leq 54/7$
$(175, 30, 5)$	1	6	$(175, 145, 120)$	121	116	Opt	$r \leq 196/23$

Tablica 3: Dopustivi parametri SSSD-ova i njihovih komplementa.

Teorem 4.39. *Neka postoji sustav spojenih simetričnih dizajna s r vlakna veličine v. Tada postoji asocijacijska shema s tri klase koja je imprimitivna tipa B_1 i netrivijalne klase su joj:*

- *R_1 je relacija susjedstva μ-naglašenog $SSSD(v, \Bbbk, \lambda; r)$-a,*
- *R_2 je relacija susjedstva disjunktne unije potpunih grafova na vlaknima,*
- *R_3 je relacija susjedstva ν-naglašenog $SSSD(v, v-\Bbbk, v-2\Bbbk+\lambda; r)$-a.*

Grafovi od kojih su dobivene relacije R_1 i R_3 su multipartitni komplementi.

Dokaz. Neka je G_1 graf $SSSD(v, \Bbbk, \lambda; r)$, G_2 graf $r \cdot K_v$, a G_3 multipartitni komplement od G_1. Možemo pretpostaviti da je G_1 μ-naglašen, a G_3 ν-naglašen. U suprotonom ih zamijenimo, uz zamjenu parametara $(v, \Bbbk, \lambda)$ s komplementarnim parametrima. Provjeravamo da zajedno s trivijalnom relacijom R_0 relacije susjedstva R_1, R_2, R_3 ta tri grafa čine asocjacijsku shemu reda $n = rv$. Relacije su simetrične, disjunktne i u uniji daju skup svih parova $X \times X$. Da bismo provjerili 4. svojstvo iz definicije 1.38, izaberemo par $(x, y) \in R_k$ i brojimo vrhove z takve da je $(x, z) \in R_i$ i $(z, y) \in R_j$. Zbog simetričnosti možemo se ograničiti na $i \leq j$.

Za $k = 0$ je $x = y$ i presječni broj je $p^0_{ij} = 0$ ako je $i \neq j$. Za $i = j$ dobivamo stupnjeve relacija: $p^0_{00} = n_0 = 1$, $p^0_{11} = n_1 = (r-1)\Bbbk$ (jer u G_1 vrh x ima $\Bbbk$ susjeda u svakom vlaknu kojem ne pripada), $p^0_{22} = n_2 = v - 1$ (jer je u G_2 vrh x susjedan sa svim drugim vrhovima u vlaknu kojem pripada) i $p^0_{33} = n_3 = (r-1)(v-\Bbbk)$ (isto objašnjenje kao za G_1 u komplementarnom grafu G_3).

Za $k = 1$ vrhovi x i y su susjedni u G_1 (1-*susjedni*). Ako je $i = 0$, očito je $p^1_{0j} = \delta_{j1}$. Za $i = 1$ presječni brojevi su $p^1_{11} = (r-2)\mu$ (po trećem svojstvu iz definicije 4.36, vrhovi x i y imaju μ zajedničkih 1-susjeda u svakom od $r-2$ vlakna koja ne sadrže ni x ni y), $p^1_{12} = \Bbbk - 1$ (y je 2-susjedan sa svim vrhovima iz svojeg vlakna, a x u tom vlaknu ima još $\Bbbk - 1$ 1-susjeda osim y) i $p^1_{13} = (r-2)(\Bbbk - \mu)$ (u svakom vlaknu kojem ne pripadaju x i y, vrh x ima $\Bbbk$ 1-susjeda, od kojih su μ zajednički 1-susjedi; preostalih $\Bbbk - \mu$ su 3-susjedi od y). Za $i = 2$ presječni brojevi su $p^1_{22} = 0$ (x i y su iz različitih vlakna, a 2-susjedi su u istom vlaknu) i $p^1_{23} = v - \Bbbk$ (2-susjedi od x su preostali vrhovi u istom vlaknu, a među njima y ima $v - \Bbbk$ 3-susjeda). Za $i = 3$ imamo presječni broj $p^1_{33} = (r-2)(v - 2\Bbbk + \mu)$ (u svakom vlaknu kojem ne pripadaju x i y, zajedničke 3-susjede dobijemo iz formule uključivanja-isključivanja).

Za $k = 2$ vrhovi x i y su 2-susjedni, što znači da su u istom vlaknu. Za $i = 0$ kao i ranije imamo $p^2_{0j} = \delta_{j2}$. Za $i = 1$ dobivamo presječne brojeve $p^2_{11} = (r-1)\lambda$ (u svakom drugom vlaknu x i y imaju λ zajedničkih 1-susjeda jer inducirani podgraf odgovara simetričnom dizajnu), $p^2_{12} = 0$ (2-susjedi od y su u istom vlaknu, a x nema 1-susjeda u tom vlaknu) i $p^2_{13} = (r-1)(\Bbbk - \lambda)$ (u svakom drugom vlaknu x ima $\Bbbk$ 1-susjeda, od kojih su λ zajednički 1-susjedi, a preostalih $\Bbbk - \lambda$ su 3-susjedi od y). Dalje, za $i = 2$ presječni brojevi su $p^2_{22} = v - 2$ (svi preostali vrhovi iz vlakna od x i y su njihovi zajednički 2-susjedi) i $p^2_{23} = 0$ (2-susjedi od x su u istom vlaknu, a y nema 3-susjeda u tom vlaknu). Konačno, za $i = 3$ presječni broj je $p^2_{33} = (r-1)(v - 2\Bbbk + \lambda)$ (za svako drugo vlakno inducirani podgraf od G_3 odgovara komplementarnom simetričnom $(v, v - \Bbbk, v - 2\Bbbk + \lambda)$ dizajnu).

Za $k = 3$ argumentacija je slična kao za $k = 1$ i dobivamo presječne brojeve $p^3_{0j} = \delta_{j3}$, $p^3_{11} = (r-2)\nu$, $p^3_{12} = \Bbbk$, $p^3_{13} = (r-2)(\Bbbk - \nu)$, $p^3_{22} = 0$, $p^3_{23} = v - \Bbbk - 1$ i $p^3_{33} = (r-2)(v - 2\Bbbk + \nu)$. Time smo provjerili sve slučajeve i dokazali da imamo asocijacijsku shemu. Imprimitivost slijedi jer je graf G_2 nepovezan, a tip je B_1 jer između svaka dva vlakna imamo bridove iz G_1

i G_3. □

U dokazu teorema odredili smo sve presječne brojeve. Zapišimo ih u presječne matrice.

Korolar 4.40. *Asocijacijska shema iz teorema 4.39 ima presječne matrice*

$$M_0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \qquad M_1 = \begin{bmatrix} 0 & (r-1)\Bbbk & 0 & 0 \\ 1 & (r-2)\mu & \Bbbk - 1 & (r-2)(\Bbbk - \mu) \\ 0 & (r-1)\lambda & 0 & (r-1)(\Bbbk - \lambda) \\ 0 & (r-2)\nu & \Bbbk & (r-2)(\Bbbk - \nu) \end{bmatrix},$$

$$M_2 = \begin{bmatrix} 0 & 0 & v-1 & 0 \\ 0 & \Bbbk - 1 & 0 & v - \Bbbk \\ 1 & 0 & v-2 & 0 \\ 0 & \Bbbk & 0 & v - \Bbbk - 1 \end{bmatrix},$$

$$M_3 = \begin{bmatrix} 0 & 0 & 0 & (r-1)(v-\Bbbk) \\ 0 & (r-2)(\Bbbk - \mu) & v - \Bbbk & (r-2)(v - 2\Bbbk + \mu) \\ 0 & (r-1)(\Bbbk - \lambda) & 0 & (r-1)(v - 2\Bbbk + \lambda) \\ 1 & (r-2)(\Bbbk - \nu) & v - \Bbbk - 1 & (r-2)(v - 2\Bbbk + \nu) \end{bmatrix}.$$

Propozicija 4.41. *Ako su relacije numerirane kao u teoremu 4.39, tako da je R_1 relacija susjedstva μ-naglašenog $SSSD(v, \Bbbk, \lambda; r)$, onda asocijacijska shema ima svojstvene matrice*

$$P = \begin{bmatrix} 1 & (r-1)\Bbbk & v-1 & (r-1)(v-\Bbbk) \\ 1 & -\Bbbk & v-1 & \Bbbk - v \\ 1 & (r-1)\sqrt{\Bbbk - \lambda} & -1 & (1-r)\sqrt{\Bbbk - \lambda} \\ 1 & -\sqrt{\Bbbk - \lambda} & -1 & \sqrt{\Bbbk - \lambda} \end{bmatrix}, \tag{45}$$

$$Q = \begin{bmatrix} 1 & r-1 & v-1 & (r-1)(v-1) \\ 1 & -1 & \frac{v-\Bbbk}{\sqrt{\Bbbk-\lambda}} & \frac{\Bbbk - v}{\sqrt{\Bbbk-\lambda}} \\ 1 & r-1 & -1 & 1-r \\ 1 & -1 & \frac{-\Bbbk}{\sqrt{\Bbbk-\lambda}} & \frac{\Bbbk}{\sqrt{\Bbbk-\lambda}} \end{bmatrix}. \tag{46}$$

Dokaz. Vidi [98, formulu (7)] ili [82, formulu (6)]. □

Konstrukcija iz teorema 4.39 je generalizacija zadatka 1.35, ali za $r > 2$ shema ne nastaje od distancijsko regularnog grafa. Grafovi G_1 i G_2 su dijametra 2, a ne dijametra 3 kao u slučaju $r = 2$. Naša motivacija za definiciju 4.36 je generalizacija shema tipa B_1 dobivenih od simetričnih dizajna na više od dva vlakna. Sustave spojenih simetričnih dizajna prvi je definirao Cameron [23], a njegova motivacija bila je proučavnje grupa koje imaju više 2-tranzitivnih permutacijskih reprezentacija s istim karakterima, koje su u parovima neekvivalentne.

Zadatak 4.42. *Vidjeli smo da graf $SSSD(v, \Bbbk, \lambda; r)$ za $r > 2$ ima dijametar 2. Uz koji uvjet je jako regularan i koji su mu tada parametri?*

Rješenje. Graf ima $n = rv$ vrhova i svi su stupnja $(r-1)\Bbbk$. Po definiciji, susjedni vrhovi imaju μ zajedničkih susjeda u svakom vlaknu kojem ne pripada niti jedan od njih, dakle ukupno $(r-2)\mu$ zajedničkih susjeda. Nesusjedni vrhovi mogu biti iz istog vlakna i tada imaju $(r-1)\lambda$ zajedničkih susjeda. Ako su iz različitih vlakna, imaju $(r-2)\nu$ zajedničkih susjeda. Da bi graf bio jako regularan, ta dva broja moraju se podudarati: $(r-1)\lambda = (r-2)\nu$. Ako je to ispunjeno, parametri su $SRG(rv, (r-1)\Bbbk, (r-2)\mu, (r-2)\nu)$. $\square$

Za fiksne parametre jako regularnog grafa $SRG(m, \Bbbk, \lambda, \mu)$, imprimitivna shema s tri klase tipa A može imati proizvoljno mnogo vlakna r. Slično, za fiksne parametre $SRG(r, \Bbbk, \lambda, \mu)$, imprimitivna shema tipa B_2 može imati proizvoljnu veličinu vlakna m. Postavlja se pitanje može li, za fiksne parametre $(v, \Bbbk, \lambda)$, broj vlakna r sustava spojenih simetričnih dizajna biti po volji velik? Ryuzaburo Noda [102] dokazao je nejednakost koja ograničava r.

Teorem 4.43 (Nodina nejednakost)**.** *Ako postoji $SSSD(v, \Bbbk, \lambda; r)$, onda je*

$$(r-1)\left[(\Bbbk-2)\lambda\binom{\Bbbk}{3} - (v-2)\left[(v-\Bbbk)\binom{\nu}{3} + \Bbbk\binom{\mu}{3}\right]\right] \leq$$

$$\leq (v-2)\left[(v-1)\binom{\lambda}{3} + \binom{\Bbbk}{3} - \left[(v-k)\binom{\nu}{3} + \Bbbk\binom{\mu}{3}\right]\right].$$

Jednakost se dostiže ako i samo ako $(X_1, X_2 \cup \cdots \cup X_r)$ čini 3-dizajn.

Za karakterizaciju dostizanja, vrhovi iz X_1 su točke, a iz ostalih vlakna blokovi dizajna. Incidencija između točaka i blokova određena je susjedstvom u grafu. Broj točaka je v, a broj blokova je $(r-1)v$. Svaki blok sadrži $\Bbbk$ točaka i kroz svaku točku prolazi $(r-1)\Bbbk$ blokova. Uvjet da imamo 3-dizajn znači da kroz svake tri točke prolazi konstantan broj blokova; taj broj ćemo označavati Λ. Naravno, bilo koje vlakno mogli smo uzeti za skup točaka (ne samo prvo vlakno X_1), a uniju ostalih vlakna za skup blokova.

Dokaz. Za tri točke $x, y, z \in X_1$, neka je $\Lambda_{x,y,z}$ broj blokova koji ih sadrže. Prebrojavamo na dva načina skup svih parova $(\{x,y,z\}, B)$, pri čemu je $\{x,y,z\}$ tročlan skup točaka sadržan u bloku B. Dobivamo jednadžbu

$$\sum_{x,y,z\in X_1} \Lambda_{x,y,z} = (r-1)v\binom{\hbar}{3}. \tag{47}$$

Zatim prebrojavamo parove $(\{x,y,z\}, \{B_1, B_2\})$, gdje je $\{x,y,z\}$ tročlan skup točaka sadržan u blokovima B_1 i B_2. Na lijevoj strani prvo biramo skup točaka, a zatim dva bloka kroz te točke:

$$\sum_{x,y,z\in X_1} \binom{\Lambda_{x,y,z}}{2} = \frac{1}{2}(r-1)v\left[(v-1)\binom{\lambda}{3} + (r-2)(v-\hbar)\binom{\nu}{3} + (r-2)\hbar\binom{\mu}{3}\right]. \tag{48}$$

Na desnoj strani prvo biramo blokove B_1 i B_2, a zatim tri zajedničke točke. Ako su iz istog vlakna, imaju λ zajedničkih točaka. Ako su iz različitih vlakna i nisu susjedni, imaju ν zajedničkih točaka. Ako su iz različitih vlakna i susjedni su, imaju μ zajedničkih točaka. Sada definiramo $\Lambda = (r-1)v\binom{\hbar}{3}/\binom{v}{3}$ i promatramo sumu $S = \sum\limits_{x,y,z\in X_1} (\Lambda - \Lambda_{x,y,z})^2$. Očito je $S \geq 0$ i vrijedi $S = 0$ ako i samo ako imamo 3-dizajn. Računamo:

$$\begin{aligned}
S &= \sum \left(\Lambda^2 - (2\Lambda - 1)\Lambda_{x,y,z} + \Lambda_{x,y,z}(\Lambda_{x,y,z} - 1)\right) \\
&= \binom{v}{3}\Lambda^2 - (2\Lambda - 1)\sum \Lambda_{x,y,z} + 2\sum \binom{\Lambda_{x,y,z}}{2} \\
&\overset{(47),(48)}{=} \frac{(r-1)^2 v^2 \binom{\hbar}{3}^2}{\binom{v}{3}} - \frac{2(r-1)v\binom{\hbar}{3} - \binom{v}{3}}{\binom{v}{3}}(r-1)v\binom{\hbar}{3} \\
&\qquad + (r-1)v\left[(v-1)\binom{\lambda}{3} + (r-2)(v-\hbar)\binom{\nu}{3} + (r-2)\hbar\binom{\mu}{3}\right] \\
&= \frac{(r-1)v}{\binom{v}{3}}\left[-(r-1)v\binom{\hbar}{3}^2 + \binom{v}{3}\binom{\hbar}{3} + \binom{v}{3}(v-1)\binom{\lambda}{3}\right. \\
&\qquad \left. + \binom{v}{3}(r-2)(v-\hbar)\binom{\nu}{3} + \binom{v}{3}(r-2)\hbar\binom{\mu}{3}\right].
\end{aligned}$$

U prvom članu uglate zagrade raspišemo $\binom{\hbar}{3} = \frac{\hbar(\hbar-1)(\hbar-2)}{6}$ i iskoristimo uvjet $\hbar(\hbar-1) = \lambda(v-1)$. U ostalim članovima raspišemo $\binom{v}{3} = \frac{v(v-1)(v-2)}{6}$, pa iz svih članova izlučimo $\frac{v(v-1)}{6}$:

$$S = \frac{(r-1)v^2(v-1)}{6\binom{v}{3}} \left[-(r-1)(\bar{k}-2)\lambda\binom{\bar{k}}{3} + (v-2)\binom{\bar{k}}{3} \right.$$
$$\left. +(v-2)(v-1)\binom{\lambda}{3} + (v-2)(r-2)(v-\bar{k})\binom{\nu}{3} + (v-2)(r-2)\bar{k}\binom{\mu}{3} \right].$$

Uglata zagrada je nenegativna i može se "srediti" do nejednakosti iz teorema.
$\square$

Nodina nejednakost daje ograničenje na broj vlakna samo za SSSD-ove koji su ν-naglašeni i imaju $2k \leq v$, ili su μ-naglašeni i imaju $2k \geq v$. Brian Kodalen [82] takve SSSD-ove zove *optimističnim*, a u suprotnom (ako su ν-naglašeni i imaju $2k \geq v$ ili su μ-naglašeni i imaju $2k \leq v$) zove ih *pesimističnim*. Na primjer, parametri iz prvog retka tablice 3 su optimistični i Nodina nejednakost daje ocjenu $r \leq 8$. Parametri iz drugog retka su pesimistični i Nodina nejednakost daje $r \geq -16$, što je uvijek ispunjeno. Ostali parametri u tablici 3 su optimistični i navedena je ocjena na broj vlakna koju dobivamo iz Nodine nejednakosti.

Mathon [98] je uočio da je Nodina nejednakost ekvivalentna Kreinovom uvjetu $q_{22}^2 \geq 0$. Uz pretpostavku da je SSSD μ-naglašen, uvrštavanjem svojstvenih vrijednosti (45) u formulu (19) dobivamo

$$\begin{aligned}
q_{22}^2 &= \frac{m_2^2}{n}\left[\frac{1}{n_0^2}P_0(2)^3 + \frac{1}{n_1^2}P_1(2)^3 + \frac{1}{n_2^2}P_2(2)^3 + \frac{1}{n_3^2}P_3(2)^3\right] \\
&= \frac{(v-1)^2}{rv}\left[1 + \frac{(r-1)^{\cancel{3}}(\sqrt{\bar{k}-\lambda})^3}{\cancel{(r-1)^2}\,\bar{k}^2} - \frac{1}{(v-1)^2} - \frac{(r-1)^{\cancel{3}}(\sqrt{\bar{k}-\lambda})^3}{\cancel{(r-1)^2}(v-\bar{k})^2}\right] \\
&= \frac{(v-1)^2}{rv}\left[(r-1)(\sqrt{\bar{k}-\lambda})^3\left(\frac{1}{\bar{k}^2} - \frac{1}{(v-\bar{k})^2}\right) + 1 - \frac{1}{(v-1)^2}\right] \\
&= \frac{(v-1)^2}{r\cancel{v}}\left[(r-1)(\sqrt{\bar{k}-\lambda})^3\,\frac{\cancel{v}(v-2\bar{k})}{\bar{k}^2(v-\bar{k})^2} + \frac{\cancel{v}(v-2)}{(v-1)^2}\right].
\end{aligned}$$

Iskoristimo uvjet $\bar{k}(v-\bar{k}) = (\bar{k}-\lambda)(v-1)$, koji je ekvivalentan s $\lambda(v-1) = \bar{k}(\bar{k}-1)$:

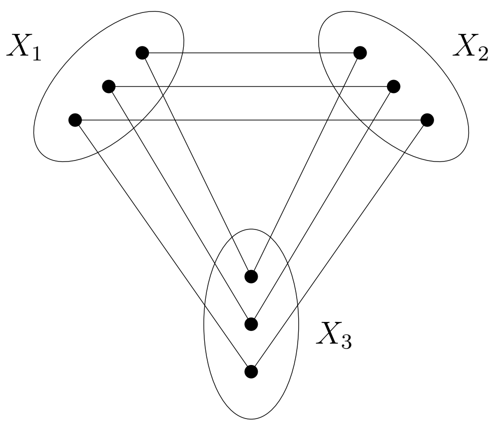
$$\begin{aligned}
q_{22}^2 &= \frac{\cancel{(v-1)^2}}{r}\left[(r-1)(\sqrt{\bar{k}-\lambda})^3\,\frac{v-2\bar{k}}{(\bar{k}-\lambda)^2\cancel{(v-1)^2}} + \frac{v-2}{\cancel{(v-1)^2}}\right] \\
&= \frac{1}{r}\left[(r-1)\frac{v-2\bar{k}}{\sqrt{\bar{k}-\lambda}} + v - 2\right] \geq 0.
\end{aligned}$$

Iz ovog dobivamo jednostavniju nejednakost $(r-1)(2\bar{k}-v) \leq (v-2)\sqrt{\bar{k}-\lambda}$, koja je za μ-naglašene SSSD-ove ekvivalentna s Nodinom nejednakosti. U pesimističnom slučaju lijeva strana je negativna i ne dobivamo ograničenje na r. U optimističnom slučaju slijedi

$$r \leq \frac{(v-2)\sqrt{\Bbbk - \lambda}}{2\Bbbk - v} + 1. \tag{49}$$

Kodalen [82] je pokazao da teorem 3.22 (apsolutna ocjena) daje ograničenje na broj vlakna u optimističnom i u pesimističnom slučaju. Iz propozicije 2.25 znamo da je $q_{22}^0 = m_2 > 0$, a sličnim računom kao za q_{22}^2 vidimo da je $q_{22}^1 = 0$ i $q_{22}^3 > 0$. Ako se ne dostiže Nodina nejednakost, onda je i $q_{22}^2 > 0$ pa uvrštavanjem $i = j = 2$ u teorem 3.22 slijedi $m_0 + m_2 + m_3 \leq \frac{1}{2}m_2(m_2+1)$. Kratnosti m_i očitamo iz nultog retka matrice (46). Uvrštavanjem dobijemo $r \leq \frac{1}{2}v - \frac{1}{v-1}$, iz čega slijedi $r \leq \frac{v-1}{2}$. Ako se dostiže Nodina nejednakost, onda je $q_{22}^2 = 0$ i teorem 3.22 daje $m_0 + m_3 \leq \frac{1}{2}m_2(m_2+1)$. Iz toga na sličan način dobijemo $r \leq \frac{v+1}{2}$. Ove nejednakosti su za optimistične parametre iz prvog i četvrtog retka tablice 3 ekvivalentne Nodinoj nejednakosti, a za optimistične parametre iz trećeg, petog i šestog retka su slabije od Nodine nejednakosti. Za pesimistične parametre $(36, 15, 6)$ u drugom retku dobivamo ograničenje $r \leq 17$. Međutim, za te parametre nije poznat niti primjer sa $r = 3$.

Do sada nismo rekli ništa o egzistenciji SSSD-ova za $r \geq 3$. Trivijalni primjer možemo napraviti za bilo koju veličinu vlakna $v \geq 3$ i broj vlakna r tako da za G_1 uzmemo uniju v disjunktnih potpunih grafova K_r, od kojih svaki sadrži po jedan vrh iz svakog vlakna (slika 23). Inducirani podgraf na bilo koja dva vlakna je incidencijski graf trivijalnog simetričnog $(v, 1, 0)$ dizajna, a konstante iz trećeg uvjeta definicije 4.36 su $\mu = 1$ i $\nu = 0$. Ovo je μ-naglašen SSSD i ima $2\Bbbk < v$, pa je pesimističan. Broj vlakna r možemo izabrati po volji. Za apsolutnu ocjenu implicitno smo koristili pretpostavku



Slika 23: Trivijalni $SSSD(v, 1, 0; r)$.

da su parametri simetričnog dizajna netrivijalni, tj. $\Bbbk \geq 3$. Trivijalni SSSD-ovi su jedini poznati pesimistični primjeri.

U optimističnom slučaju poznata je "klasična serija" primjera, koju su konstruirali Jean-Marie Goethals [57] te Peter Cameron i Jaap Seidel [31]. Bazirani su na simetričnim dizajnima s parametrima $v = 2^{2m}$, $\Bbbk = 2^{m-1}(2^m + 1)$, $\lambda = 2^{m-1}(2^{m-1} + 1)$ reda $\Bbbk - \lambda = 2^{2(m-1)}$. Konstante iz trećeg uvjeta definicije 4.36 su $\mu = 2^{m-2}(2^m + 3)$ i $\nu = 2^{m-2}(2^m + 1)$. Vidimo da je $\mu > \nu$ i $2k > v$, pa su zaista optimistični. Od binarnog linearnog Reed-Mullerovog koda drugog reda $RM(m, 2)$ dobivamo SSSD sa $r = 2^m$ vlakna, a od nelinearnog Kerdockovog koda dobivamo SSSD sa $r = 2^{2m-1}$ vlakna koji dostiže Nodinu nejednakost. Na primjer, za $m = 2$ dobivamo $SSSD(16, 10, 6; 8)$ sa $\mu = 7$, $\nu = 5$, a za $m = 3$ dobivamo $SSSD(64, 36, 20; 32)$ sa $\mu = 22$, $\nu = 18$ (parametri iz prvog i četvrtog retka tablice 3). Mathon [98] je potpuno klasificirao najmanje netrivijalne primjere s $v = 16$ pomoću računala. Za $r = 2$ i $r = 3$ dobio je 3 neizomorfna primjera, za $r = 4$ dobio je 12 primjera, a za $r = 5, 6, 7, 8$ samo po jedan primjer do na izomorfizam. Davis, Martin i Polhill [32] te Jedwab, Li i Simon [78] konstruirali su daljnje primjere optimističnih SSSD-ova pomoću diferencijskih skupova u 2-grupama. Svi do sada spomenuti primjeri imaju parametar v koji je potencija od 2. Kodalen [82] uspio je konstruirati primjere kojima v nije potencija od 2, a broj vlakna r može biti po volji velik. Definirao je takozvane "spojene simplekse" i uspostavio vezu s regularnim nepristranim Hadamardovim matricama (eng. regular unbiased Hadamard matrices).

Detalje konstrukcije klasične serije SSSD-ova upoznat ćemo u sljedećem poglavlju, kad obradimo osnove teorije kodiranja. Upoznat ćemo i primjere primitivnih asocijaciskih shema s tri klase, koje su povezane s kombinatornim dizajnima. Vodeći ekspert za asocijacijske sheme s tri klase je Edwin van Dam, koji ih je proučavao u svojoj disertaciji [126] i u članku [127].

5 Podskupovi Johnsonove i Hammingove sheme

5.1 Kombinatorni dizajni

U primjeru 1.5 definirali smo Johnsonovu shemu $J(v, d)$ sa skupom vrhova $\binom{V}{d}$ (skup svih d-članih podskupova od $V = \{1, \ldots, v\}$). Vrhovi X i Y su i-asocirani ako je $|X \cap Y| = d - i$. Vidjeli smo da je $J(v, d)$ asocijacijska shema s d klasa. U ovoj cjelini umjesto d koristimo oznaku $\Bbbk$, koja je tradicionalna u teoriji dizajna.

Definicija 5.1. *Za podskup vrhova Johnsonove sheme $\mathcal{D} \subseteq \binom{V}{\Bbbk}$ kažemo da je* kombinatorni dizajn *s parametrima t-$(v, \Bbbk, \lambda)$ ako za svaki t-člani podskup od V postoji točno λ elemenata iz $\mathcal{D}$ koji ga sadrže. Elemente od V zovemo* točkama*, a elemente od $\mathcal{D}$* blokovima *dizajna.*

Propozicija 5.2. *Ako je $\mathcal{D}$ dizajn s parametrima t-$(v, \Bbbk, \lambda)$, onda je i s-$(v, \Bbbk, \lambda_s)$ dizajn za $s = 0, \ldots, t$, pri čemu je $\lambda_s = \lambda\binom{v-s}{t-s}/\binom{\Bbbk-s}{t-s}$.*

Dokaz. Neka je $S \subseteq V$ bilo koji s-člani skup točaka. Označimo sa $\lambda(S) = |\{X \in \mathcal{D} \mid S \subseteq X\}|$ broj blokova koji sadrže S. Dvostrukim prebrojavanjem parova $\{(T, X) \mid T \in \binom{V}{t},\ X \in \mathcal{D},\ S \subseteq T \subseteq X\}$ vidimo da vrijedi $\binom{v-s}{t-s}\lambda = \lambda(S)\binom{\Bbbk-s}{t-s}$. Iz toga slijedi da $\lambda(S)$ ne ovisi o izboru skupa S, nego samo o njegovoj kardinalnosti s. Dakle, $\mathcal{D}$ je ujedno s-dizajn s parametrom λ_s. □

Ukupan broj blokova dizajna je $b = |\mathcal{D}| = \lambda_0 = \lambda\binom{v}{t}/\binom{\Bbbk}{t}$. Izrazi za $\lambda_0, \ldots, \lambda_t$ moraju biti prirodni brojevi:

Korolar 5.3. *Ako postoji t-$(v, \Bbbk, \lambda)$ dizajn, onda $\binom{\Bbbk-s}{t-s}$ dijeli $\lambda\binom{v-s}{t-s}$, za svaki $s = 0, \ldots, t$.*

Da bismo izbjegli trivijalne slučajeve, pretpostavljamo da parametri dizajna zadovoljavaju $2 \le t \le \Bbbk$ i $3 \le \Bbbk < v$. Zbog sljedeće propozicije možemo se ograničiti na $\Bbbk \le \frac{v}{2}$.

Propozicija 5.4. *Neka je $\mathcal{D}$ dizajn s parametrima t-$(v, \Bbbk, \lambda)$ i neka vrijedi $t \le v - \Bbbk$. Tada je familija $\overline{\mathcal{D}} = \{V \setminus X \mid X \in \mathcal{D}\}$, dobivena komplementiranjem blokova, dizajn s parametrima t-$(v, v - \Bbbk, \bar{\lambda})$ za $\bar{\lambda} = \sum_{s=0}^{t}(-1)^s\binom{t}{s}\lambda_s = \lambda\binom{v-t}{\Bbbk}/\binom{v-t}{\Bbbk-t}$.*

Dokaz. Izaberemo bilo koji t-člani podskup točaka $T = \{x_1, \ldots, x_t\} \subseteq V$. Želimo prebrojati blokove koji su disjunktni s T. Označimo $A_i = \{Y \in \mathcal{D} \mid$

$x_i \in Y\}$ i $A_S = \cap_{i\in S} A_i$. Iz formule uključivanja-isključivanja slijedi

$$\bar{\lambda} = |(A_1 \cup \cdots \cup A_t)^c| = \sum_{S\subseteq\{1,\ldots,t\}} (-1)^{|S|} |A_S| = \sum_{s=0}^{t} (-1)^s \binom{t}{s} \lambda_s.$$

Sada znamo da broj $\bar{\lambda}$ ne ovisi o izboru skupa T, pa dvostrukim prebrojavanjem parova $\{(T,X) \mid T \in \binom{V}{t},\ X \in \mathscr{D},\ T\cap X = \emptyset\}$ dobijemo $\binom{v}{t}\bar{\lambda} = b\binom{v-\Bbbk}{t}$. Uvrštavanjem formule za $b = \lambda_0$ iz propozicije 5.2 slijedi $\bar{\lambda} = \lambda\binom{v-\Bbbk}{t}/\binom{\Bbbk}{t} = \lambda\binom{v-t}{\Bbbk}/\binom{v-t}{\Bbbk-t}$. □

Zadatak 5.5. *Neka je $\mathscr{D}$ dizajn s parametrima t-$(v,\Bbbk,\lambda)$, a $I \in \binom{V}{i}$, $J \in \binom{V}{j}$, $I \cap J = \emptyset$ disjunktni skupovi točaka takvi da je $i + j \le t$. Dokažite da broj $\lambda_{i,j} = |\{X \in \mathscr{D} \mid I \subseteq X,\ J \cap X = \emptyset\}|$ ne ovisi o izboru skupova I, J, nego samo o njihovim kardinalnostima i, j. Dokažite formulu $\lambda_{i,j} = \lambda\binom{v-i-j}{\Bbbk-i}/\binom{v-t}{\Bbbk-t}$ te rekurziju $\lambda_{i,j+1} = \lambda_{i,j} - \lambda_{i+1,j}$.*

Cijeli skup vrhova Johnsonove sheme $J(v,\Bbbk)$, tj. $\mathscr{D} = \binom{V}{\Bbbk}$, je $\Bbbk$-$(v,\Bbbk,1)$ dizajn. To je takozvani *potpuni dizajn*. Od interesa su *nepotpuni* dizajni: pravi podskupovi $\mathscr{D} \subsetneq \binom{V}{\Bbbk}$ koji su t-dizajni za što veći $t < \Bbbk$. Najveći t za koji to vrijedi nazivamo *snagom* od $\mathscr{D}$.

Statističari su u 1930-im godinama [50, 141, 12] koristili dizajne snage $t = 2$ za planiranje eksperimenata, uglavnom u poljoprivredi. Cilj je usporediti v vrsta gnojiva (*varieties* ili *treatments*) na b polja (*blocks*) na kojima raste neka poljoprivredna kultura. Ako na svakom polju uspoređujemo jedan par gnojiva (podijelimo ga na dvije polovice i na svakoj primijenimo jednu vrstu gnojiva), potrebno je $b = \binom{v}{2}$ polja. Taj broj raste kao kvadrat od v, što može biti nepraktično. Ako na svakom polju primijenimo svih v vrsta gnojiva, nema ograničenja na b, ali polja dijelimo na prevelik broj malih parcela. Zato svako polje dijelimo na $\Bbbk$ parcela, $2 < \Bbbk < v$, te na svakom primijenimo nekih $\Bbbk$ vrsta gnojiva. Eksperiment želimo organizirati tako da svaki par gnojiva uspoređujemo jednako mnogo puta, recimo λ. To je uvjet *balansiranosti*. Tako dolazimo do definicije 2-$(v,\Bbbk,\lambda)$ dizajna, koji se još nazivaju *balansiranim nepotpunim blokovnim dizajnima* (eng. *balanced incomplete block designs*, BIBD). Kraći naziv je *blokovni dizajni*, a parametre nekad zapisujemo BIBD$(v,b,r,\Bbbk,\lambda)$. Parametar $r = \lambda_1$ je broj blokova kroz zadanu točku (*replication number*). Postavlja se pitanje koji je najmanji mogući broj blokova 2-$(v,\Bbbk,\lambda)$ dizajna?

Teorem 5.6 (Fisherova[27] nejednakost)**.** *U svakom* 2-$(v,\Bbbk,\lambda)$ *dizajnu vrijedi*

$$b \ge v.$$

[27]Sir Ronald Aylmer Fisher (1890.-1962.), britanski matematičar, statističar, biolog i genetičar.

Nejednakost se može dokazati s pomoću linearne algebre, vidi [121, teorem 2.17] ili [120, teorem 1.33]. Fisherov originalni dokaz [49] koristi dvostruko prebrojavanje. Dakle, najmanji mogući broj blokova imaju upravo simetrični dizajni, koje smo susreli u cjelini 1.3.

Motivacija za proučavanje kombnatornih dizajna snage $t > 2$ bile su višestruko tranzitivne permutacijske grupe [139, 140, 64]. Za $G \leq \mathrm{Sym}(V)$ kažemo da je *t-tranzitivna* ako za svake dvije uređene t-torke $(x_1, \ldots, x_t)$, $(y_1, \ldots, y_t)$ međusobno različitih elemenata iz V postoji permutacija $g \in G$ takva da je $(x_1, \ldots, x_t)^g = (x_1^g, \ldots, x_t^g) = (y_1, \ldots, y_t)$. Za G kažemo da je *t-homogena* ako za svaka dva t-člana podskupa $\{x_1, \ldots, x_t\}$, $\{y_1, \ldots, y_t\} \subseteq V$ postoji permutacija $g \in G$ takva da je $\{x_1, \ldots, x_t\}^g = \{x_1^g, \ldots, x_t^g\} = \{y_1, \ldots, y_t\}$. Iz t-tranzitivnosti očito slijedi t-homogenost. Za $t \geq 5$ vrijedi i obrat.

Teorem 5.7 (Livingstone, Wagner [92]). *Neka je $G \leq \mathrm{Sym}(V)$ permutacijska grupa i neka vrijedi $5 \leq t \leq v/2$. Ako je G t-homogena, onda je i t-tranzitivna.*

Za $2 \leq t \leq 4$, Kantor [79] je klasificirao sve permutacijske grupe koje su t-homogene, a nisu t-tranzitivne. Od t-homogenih grupa direktno dobivamo dizajne snage t.

Zadatak 5.8. *Neka je $G \leq \mathrm{Sym}(V)$ permutacijska grupa koja je t-homogena. Ako je $X \in \binom{V}{\Bbbk}$ bilo koji $\Bbbk$-člani skup točaka, dokažite da je $\mathscr{D} = X^G$ (orbita pri djelovanju G na podskupove) dizajn s parametrima t-$(v, \Bbbk, \lambda)$ za $\lambda = |G|\binom{\Bbbk}{t}/(|G_X|\binom{v}{t})$. Pritom je $G_X = \{g \in G \mid X^g = X\}$ stabilizator skupa X.*

Iz klasifikacije konačnih jednostavnih grupa slijedi da su jedine 6-tranzitivne permutacijske grupe simetrične i alternirajuće grupe S_v i A_v [27, teorem 4.11]. One nisu zanimljive za konstrukciju dizajna jer od njih dobivamo samo potpune dizajne na v točaka. Nadalje, jedine 5-tranzitivne grupe (osim alternirajućih i simetričnih) su Mathieuove[28] grupe M_{12} i M_{24} [95, 96]. Od njih dobivamo Wittove[29] dizajne 5-$(12, 6, 1)$ i 5-$(24, 8, 1)$ [140]. Postavlja se pitanje postoje li nepotpuni dizajni snage $t > 5$, budući da ih ne možemo dobiti od t-tranzitivnih grupa?

Prvi netrivijalni primjer 6-dizajna konstruirali su Spyros S. Magliveras i David W. Leavitt 1984. godine [93]. Luc Teirlinck [123] je 1987. dokazao postojanje nepotpunih dizajna proizvoljno velike snage t. Njegovi dizajni imaju parametre oblika t-$(v, t+1, (t+1)!^{2t+1})$, $v \equiv t \pmod{(t+1)!^{2t+1}}$.

[28]Émile Léonard Mathieu (1835.-1890.), francuski matematičar.

[29]Ernst Witt (1911.-1991.), njemački matematičar.

Broj točaka v i parametar λ jako naglo rastu s porastom t. Već za $t = 7$ Teirlinckovi dizajni imaju više od $1.2 \cdot 10^{69}$ točaka. Primjere dizajna snage $t = 7, 8, 9$ s malim brojem točaka konstruirali su matematičari sa sveučilišta Bayreuth u drugoj polovici 1990-ih [8, 10, 9, 91]. Svi spomenuti dizajni imaju parametar $\lambda > 1$. Dizajne s $\lambda = 1$ zovemo *Steinerovim*[30] i znatno ih je teže konstruirati. Do danas nije poznat niti jedan eksplicitni primjer Steinerovog dizajna snage $t > 5$, iako njihova egzistencija slijedi iz asimptotskih rezultata Petera Keewasha [80, 81] za proizvoljno velike t.

Članak [5] naglašava analogije između sfernih dizajna, konačnih podskupova sfere S^{m-1} koji dobro aproksimiraju cijelu sferu u smislu definicije 3.30, i kombinatornih dizajna:

> "The concept of combinatorial t-design is to find subsets which approximate the whole space $\binom{V}{\mathscr{k}}$ ..."

Analogon teorema 3.32 i generalizacija Fisherove nejednakosti je sljedeća nejednakost Dijen K. Ray-Chaudhurija i Ricka Wilsona [107, 108].

Teorem 5.9 (Ray-Chaudhuri, Wilson)**.** *Neka je $\mathscr{D}$ kombinatorni t-$(v, \mathscr{k}, \lambda)$ dizajn s $b = |\mathscr{D}|$ blokova. Ako je $t = 2d$ paran i vrijedi $v \geq \mathscr{k} + d$, onda je*

$$b \geq \binom{v}{d}.$$

Ako je $t = 2d + 1$ neparan i vrijedi $v - 1 \geq \mathscr{k} + d$, onda je

$$b \geq 2\binom{v-1}{d}.$$

Dokaz iz [108] je linearnoalgebarski i raspisan je u skripti [84, teorem 1.15 i korolar 1.16]. Wilson je kasnije dokazivao nejednakost na druge načine [137, 138, 44]. Posljedica nejednakosti je da netrivijalni simetrični dizajni mogu biti najviše snage $t = 2$. Stupanj konačnog podskupa sfere definirali smo kao broj različitih kutova ili udaljenosti između vektora iz tog podskupa. Analogno, *stupanj kombinatornog dizajna* je broj različitih veličina presjeka blokova tog dizajna. Veličine presjeka blokova nazivamo *presječnim brojevima* dizajna.

Primjer 5.10 (Mali Wittov dizajn)**.** *Konstruirajmo* 5-(12, 6, 1) *dizajn u sustavu za računalnu algebru GAP [52]. Odredimo mu presječne brojeve i stupanj.*

[30] Jakob Steiner (1796.-1863.), švicarski matematičar.

Rješenje. Ovako u GAP-u dobijemo Mathieuovu grupu M_{12} i ispitamo njezina svojstva:

```
gap> M12:=MathieuGroup(12);
Group([ (1,2,3,4,5,6,7,8,9,10,11), (3,7,11,8)(4,10,5,6),
  (1,12)(2,11)(3,6)(4,8)(5,9)(7,10) ])
gap> Size(M12);
95040
gap> Transitivity(M12);
5
```

Vidimo da je $M_{12} \leq S_{12}$ permutacijska grupa reda $95040 = 2^6 \cdot 3^3 \cdot 5 \cdot 11$ i da je 5-tranzitivna. Prema zadatku 5.8, orbita bilo kojeg 6-članog podskupa od $\{1, \ldots, 12\}$ pod djelovanjem M_{12} je 5-$(12, 6, \lambda)$ dizajn. Da bismo dobili Steinerov dizajn ($\lambda = 1$), moramo pronaći podskup sa stabilizatorom odgovarajuće veličine.

```
gap> sub6:=Combinations([1..12],6);; Size(sub6);
924
gap> Collected(List(sub6,x->Size(Stabiliser(M12,x,OnSets))));
[ [ 120, 792 ], [ 720, 132 ] ]
```

Od $\binom{12}{6} = 924$ podskupova, 792 imaju stabilizatore reda 120. Orbite tih podskupova su blokovi 5-$(12, 6, 6)$ dizajna. Preostalih 132 podskupova imaju stablizatore reda 720 i njihove orbite su 5-$(12, 6, 1)$ dizajni.

```
gap> st:=Filtered(sub6,x->Size(Stabiliser(M12,x,OnSets))=720);;
gap> Size(st);
132
gap> Orbit(M12,st[1],OnSets);
[ [ 1, 2, 3, 4, 5, 7 ], [ 2, 3, 4, 5, 6, 8 ], [ 1, 2, 6, 7, 10, 11 ],
  [ 6, 8, 9, 10, 11, 12 ], [ 3, 4, 5, 6, 7, 9 ], [ 2, 3, 4, 6, 7, 10 ],
  [ 3, 4, 6, 8, 9, 11 ], [ 1, 2, 3, 7, 8, 11 ], [ 1, 2, 4, 5, 8, 11 ],
  [ 2, 3, 7, 10, 11, 12 ], [ 1, 7, 9, 10, 11, 12 ], [ 3, 4, 5, 8, 9, 12 ],
  [ 4, 5, 6, 7, 8, 10 ], [ 4, 6, 7, 9, 10, 11 ], [ 3, 5, 6, 8, 9, 10 ],
  [ 3, 4, 5, 7, 8, 11 ], [ 2, 4, 5, 7, 10, 11 ], [ 3, 6, 7, 8, 10, 11 ],
  [ 1, 4, 5, 7, 9, 10 ], [ 3, 4, 7, 8, 9, 10 ], [ 1, 2, 3, 4, 8, 9 ],
  [ 2, 4, 6, 10, 11, 12 ], [ 1, 2, 3, 5, 6, 9 ], [ 1, 2, 3, 6, 8, 10 ],
  [ 2, 4, 8, 9, 11, 12 ], [ 1, 3, 4, 8, 11, 12 ], [ 2, 5, 7, 8, 11, 12 ],
  [ 1, 2, 8, 10, 11, 12 ], [ 1, 5, 8, 9, 11, 12 ], [ 1, 2, 5, 7, 10, 12 ],
  [ 4, 5, 6, 9, 10, 12 ], [ 3, 6, 7, 9, 10, 12 ], [ 1, 4, 5, 6, 8, 9 ],
  [ 5, 6, 7, 8, 9, 11 ], [ 3, 4, 5, 6, 10, 11 ], [ 1, 5, 7, 8, 10, 11 ],
  [ 4, 5, 8, 9, 10, 11 ], [ 2, 3, 5, 7, 8, 10 ], [ 2, 4, 6, 8, 9, 10 ],
  [ 1, 3, 5, 6, 8, 11 ], [ 2, 5, 6, 8, 10, 11 ], [ 2, 7, 8, 9, 10, 11 ],
  [ 1, 4, 7, 8, 9, 11 ], [ 1, 5, 6, 9, 10, 11 ], [ 5, 7, 8, 9, 10, 12 ],
  [ 3, 5, 7, 9, 10, 11 ], [ 2, 3, 4, 5, 9, 10 ], [ 1, 2, 3, 7, 9, 10 ],
```

```
[ 4, 5, 6, 8, 11, 12 ], [ 1, 3, 5, 7, 11, 12 ], [ 2, 4, 5, 8, 10, 12 ],
[ 1, 2, 4, 6, 7, 9 ], [ 3, 5, 6, 9, 11, 12 ], [ 2, 3, 4, 7, 9, 11 ],
[ 3, 4, 6, 7, 11, 12 ], [ 1, 3, 5, 9, 10, 12 ], [ 2, 3, 8, 9, 10, 12 ],
[ 1, 2, 4, 5, 9, 12 ], [ 1, 3, 7, 8, 10, 12 ], [ 1, 2, 4, 6, 8, 12 ],
[ 1, 3, 6, 8, 9, 12 ], [ 2, 3, 6, 8, 11, 12 ], [ 1, 2, 4, 9, 10, 11 ],
[ 1, 2, 3, 9, 11, 12 ], [ 1, 2, 3, 5, 8, 12 ], [ 1, 2, 4, 7, 11, 12 ],
[ 1, 2, 6, 9, 10, 12 ], [ 1, 2, 5, 6, 11, 12 ], [ 5, 6, 7, 10, 11, 12 ],
[ 1, 3, 5, 7, 8, 9 ], [ 4, 7, 8, 10, 11, 12 ], [ 4, 5, 7, 9, 11, 12 ],
[ 1, 3, 5, 6, 7, 10 ], [ 2, 5, 6, 7, 9, 10 ], [ 1, 3, 4, 6, 9, 10 ],
[ 1, 6, 7, 8, 9, 10 ], [ 1, 4, 5, 6, 7, 11 ], [ 2, 3, 6, 7, 8, 9 ],
[ 1, 2, 6, 8, 9, 11 ], [ 2, 4, 7, 9, 10, 12 ], [ 2, 4, 5, 7, 8, 9 ],
[ 2, 3, 5, 6, 7, 11 ], [ 1, 3, 4, 6, 7, 8 ], [ 2, 3, 4, 6, 9, 12 ],
[ 1, 3, 6, 7, 9, 11 ], [ 1, 3, 8, 9, 10, 11 ], [ 2, 3, 5, 8, 9, 11 ],
[ 1, 2, 5, 8, 9, 10 ], [ 2, 3, 5, 7, 9, 12 ], [ 1, 4, 6, 8, 10, 11 ],
[ 2, 3, 4, 8, 10, 11 ], [ 1, 2, 5, 7, 9, 11 ], [ 1, 5, 6, 7, 9, 12 ],
[ 3, 4, 6, 8, 10, 12 ], [ 1, 6, 7, 8, 11, 12 ], [ 2, 3, 5, 6, 10, 12 ],
[ 3, 5, 8, 10, 11, 12 ], [ 1, 4, 6, 7, 10, 12 ], [ 4, 6, 7, 8, 9, 12 ],
[ 1, 3, 4, 5, 8, 10 ], [ 1, 4, 5, 7, 8, 12 ], [ 3, 4, 9, 10, 11, 12 ],
[ 1, 2, 3, 4, 10, 12 ], [ 1, 3, 4, 7, 9, 12 ], [ 1, 3, 4, 5, 6, 12 ],
[ 2, 3, 4, 7, 8, 12 ], [ 1, 2, 3, 4, 6, 11 ], [ 1, 2, 3, 5, 10, 11 ],
[ 1, 2, 7, 8, 9, 12 ], [ 1, 2, 3, 6, 7, 12 ], [ 1, 4, 6, 9, 11, 12 ],
[ 1, 2, 4, 7, 8, 10 ], [ 1, 5, 6, 8, 10, 12 ], [ 2, 4, 6, 7, 8, 11 ],
[ 2, 4, 5, 6, 9, 11 ], [ 3, 5, 6, 7, 8, 12 ], [ 1, 3, 4, 5, 9, 11 ],
[ 3, 4, 5, 7, 10, 12 ], [ 1, 2, 5, 6, 7, 8 ], [ 2, 3, 4, 5, 11, 12 ],
[ 2, 5, 9, 10, 11, 12 ], [ 2, 3, 6, 9, 10, 11 ], [ 1, 3, 4, 7, 10, 11 ],
[ 2, 4, 5, 6, 7, 12 ], [ 2, 6, 7, 9, 11, 12 ], [ 2, 6, 7, 8, 10, 12 ],
[ 1, 4, 5, 10, 11, 12 ], [ 2, 5, 6, 8, 9, 12 ], [ 1, 3, 6, 10, 11, 12 ],
[ 1, 4, 8, 9, 10, 12 ], [ 1, 2, 4, 5, 6, 10 ], [ 3, 7, 8, 9, 11, 12 ] ]
```

U GAP paketu DESIGN [118] možemo provjeriti da smo dobili 5-dizajne i izračunati im parametre $\lambda_0, \ldots, \lambda_5$.

```
gap> LoadPackage("Design");
âââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââ
Loading  GRAPE 4.8.3 (GRaph Algorithms using PErmutation groups)
by Leonard H. Soicher (http://www.maths.qmul.ac.uk/~lsoicher/).
Homepage: https://gap-packages.github.io/grape
Report issues at https://github.com/gap-packages/grape/issues
âââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââ
âââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââ
Loading  DESIGN 1.7 (The Design Package for GAP)
by Leonard H. Soicher (http://www.maths.qmul.ac.uk/~lsoicher/).
Homepage: https://gap-packages.github.io/design
Report issues at https://github.com/gap-packages/design/issues
âââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââ
true
gap> diz1:=BlockDesign(12,[st[1]],M12);;
```

```
gap> AllTDesignLambdas(diz1);
[ 132, 66, 30, 12, 4, 1 ]
gap> notst:=Difference(sub6,st);;
gap> diz2:=BlockDesign(12,[notst[1]],M12);;
gap> AllTDesignLambdas(diz2);
[ 792, 396, 180, 72, 24, 6 ]
```

U GAP paketu PAG [85] postoji naredba za presječne brojeve dizajna.

```
gap> LoadPackage("PAG");
âââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââ
Loading  PAG 0.2.2 (Prescribed Automorphism Groups)
by Vedran Krcadinac (https://web.math.pmf.unizg.hr/~krcko/homepage.html).
Homepage: https://vkrcadinac.github.io/PAG
Report issues at https://github.com/vkrcadinac/PAG/issues
âââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââ
true
gap> IntersectionNumbers(diz1);
[ 0, 2, 3, 4 ]
gap> IntersectionNumbers(diz2);
[ 0, 1, 2, 3, 4, 5 ]
```

Mali Wittov dizajn ima presječne brojeve $\{0,2,3,4\}$ i stupanj $d=4$. U dizajnu s parametrima 5-$(12,6,6)$ pojavljuju se svi mogući presječni brojevi i stupanj mu je $d=6$. Presječne brojeve 5-$(12,6,1)$ dizajna $\mathcal{D}$ možemo dobiti direktnim prebrojavanjem. Prvo iz propozicije 5.2 izračunamo $(\lambda_0,\lambda_1,\lambda_2,\lambda_3,\lambda_4,\lambda_5)=(132,66,30,12,4,1)$. Ukupan broj blokova je $b=\lambda_0=132$. Fiksiramo blok $X_0\in\mathcal{D}$ i označimo s b_i broj blokova koji ga sijeku u točno i točaka. Nadalje, neka je a_i broj parova u skupu $\{(I,X)\mid I\in\binom{V}{i},\ X\in\mathcal{D},\ X\neq X_0,\ I\subseteq X\cap X_0\}$. Ako prvo biramo $I\subseteq X_0$, a zatim blok $X\neq X_0$ kroz I, dobijemo $a_i=\binom{6}{i}(\lambda_i-1)$. Slijedi $(a_0,a_1,a_2,a_3,a_4,a_5)=(131,390,435,220,45,0)$. Ako prvo biramo blok X, pa onda podskup $I\subseteq X\cap X_0$, dobijemo $a_i=\sum_{j=i}^5 b_j\binom{j}{i}$. Redom možemo izračunati $b_5=a_5=0$, $b_4=a_4-\binom{5}{4}b_5=45$, $b_3=a_3-\binom{5}{3}b_5-\binom{4}{3}b_4=40$, $b_2=a_2-\sum_{j=3}^5\binom{j}{2}b_j=45$, $b_1=a_1-\sum_{j=2}^5\binom{j}{1}b_j=0$, $b_0=a_0-\sum_{j=1}^5 b_j=1$. Vidimo da X može sijeći X_0 u 0, 2, 3 ili 4 točke, a ne može u 1 ili 5 točaka. Stupanj 5-$(12,6,1)$ dizajna je $d=4$ jer se javljaju četiri različita presječna broja. □

Primjer 5.11 (Veliki Wittov dizajn). *Konstruirajmo* 5-$(24,8,1)$ *dizajn i odredimo mu presječne brojeve i stupanj.*

Rješenje. Veliki Wittov dizajn dobivamo od Mathieuove grupe M_{24}.

```
gap> M24:=MathieuGroup(24);
```

```
Group([ (1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23),
  (3,17,10,7,9)(4,13,14,19,5)(8,18,11,12,23)(15,20,22,21,16), (1,24)
  (2,23)(3,12)(4,16)(5,18)(6,10)(7,20)(8,14)(9,21)(11,17)(13,22)
  (15,19) ])
gap> Size(M24);
244823040
gap> Transitivity(M24);
5
```

Red grupe je $244823040 = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$ i 5-tranzitivna je. Broj podskupova $\binom{24}{8} = 735471$ je prevelik da bismo im računali stabilizatore. Steinerov dizajn konstruiramo u paketu PAG [85].

```
gap> diz3:=KramerMesnerSearch(5,24,8,1,M24)[1];;
gap> AllTDesignLambdas(diz3);
[ 759, 253, 77, 21, 5, 1 ]
gap> IntersectionNumbers(diz3);
[ 0, 2, 4 ]
```

Dizajn 5-$(24, 8, 1)$ ima presječne brojeve $\{0, 2, 4\}$ i stupanj mu je $d = 3$. Do toga također možemo doći direktnim prebrojavanjem, vidi [84, lema 1.28]. □

Naredba `KramerMesnerSearch`$(t, v, \Bbbk\ \lambda, G)$ traži dizajne sa zadanim parametrima i grupom automorfizama G takozvanom Kramer-Mesnerovom metodom [83]. Ako je grupa t-homogena, svaka orbita $\Bbbk$-članih podskupova je t-dizajn (zadatak 5.8), ali takav dizajn ponekad možemo konstruirati i od grupa manjeg stupnja homogenosti. Ideja je uzeti uniju nekoliko orbita kao blokove dizajna. Biranje orbita koje čine t-$(v, \Bbbk, \lambda)$ dizajn svodi se na rješavanje sustava linearnih jednadžbi nad $\{0, 1\}$.

Apsolutna ocjena (teorem 3.24) daje najveću moguću veličinu sfernog koda zadanog stupnja. Analogni teorem za kombinatorne dizajne dokazali su Ray-Chaudhuri i Wilson [108]. Dokaz je također raspisan u skripti [84, teorem 1.18].

Teorem 5.12. *Neka je $\mathfrak{D} \subseteq \binom{V}{\Bbbk}$ kombinatorni dizajn stupnja d. Tada broj blokova od $\mathfrak{D}$ zadovoljava $b \leq \binom{v}{d}$.*

Primijetimo da se u prethodnom teoremu ne spominje snaga od $\mathfrak{D}$. Ocjena vrijedi i za $t = 0$, tj. $\mathfrak{D}$ može biti bilo koja familija $\Bbbk$-članih podskupova od V. Ako imamo dizajn parne snage $t = 2d$ i vrijedi $v \geq \Bbbk + d$, onda je po teoremu 5.9 broj blokova ograničen odozdo: $b \geq \binom{v}{d}$. Slijedi da takav dizajn mora biti stupnja barem d, inače bi po teoremu 5.12 imao manje od $\binom{v}{d}$ blokova. Ray-Chaudhuri i Wilson [108] dokazali su da je dizajn snage $t = 2d$

koji dostiže ocjenu $b = \binom{v}{d}$ stupnja točno d. Za takve dizajne kažemo da su *napeti* (eng. *tight*), kao i za sferne dizajne koji dostižu ocjene (36) i (37).

Teorem 5.13. *Ako postoji napeti $2d$-$(v, \Bbbk, \lambda)$ dizajn, onda ima točno d različitih presječnih brojeva. Presječni brojevi su pozitivni i nultočke su sljedećeg polinoma stupnja d:*

$$\Psi_d(x) = \sum_{i=0}^{d} (-1)^{d-i} \frac{\binom{v-d}{i}\binom{\Bbbk-i}{d-i}\binom{\Bbbk-1-i}{d-i}}{\binom{d}{i}} \binom{x}{i}.$$

Napeti dizajni snage $t = 2$ su upravo simetrični dizajni. U teoremu 1.29 već smo vidjeli da im je stupanj $d = 1$, tj. imaju samo jedan presječni broj λ. Napeti dizajni snage $t = 4$ su stupnja $d = 2$. Imaju dva presječna broja, koja označavamo $x < y$. Postoji samo jedan takav dizajn s parametrima 4-$(23, 7, 1)$ i presječnim brojevima $x = 1$, $y = 3$ [68, 69, 45, 18]. Pojednostavljeni dokaz dan je u [4, teorem 3.32]. Napeti dizajni snage $t = 6$ i stupnja $d = 3$ ne postoje [105]. Eiichi Bannai [3] dokazao je da za $d \geq 4$ postoji samo konačno mnogo napetih dizajna snage $t = 2d$ (skicu dokaza vidi u [4, teorem 3.28]).

Općenito, dizajne stupnja $d = 2$ zovemo *kvazisimetričnim* i posvećena im je knjiga [114] i skripta [84]. Snaga im je ograničena s $t \leq 4$ (vidi [84, teorem 1.21]). Za $t = 3$ i $x = 0$, Cameron [25] je opisao sve dopustive parametre (vidi propoziciju 1.31 i teorem 1.36 u [84]). Za $t = 3$ i $x > 0$, Mohan Shrikhande postavio je hipotezu da jedini takvi dizajni imaju parametre 3-$(23, 7, 5)$ i 3-$(22, 7, 4)$ te presječne brojeve $x = 1$, $y = 3$ [113, conjecture 48.20]. Drugi primjeri nisu poznati, a hipoteza je dokazana samo uz neke dodatne pretpostavke. Kvazisimetričnih dizajna snage $t = 2$ ima beskonačno mnogo i dopustive parametre ne možemo klasificirati u nekoliko jednostavnih familija. Situacija je slična kao za simetrične dizajne. Tablice malih parametara kvazisimetričnih dizajna s podacima o egzistenciji dane su u [129, tablica 1.3] (za $v \leq 150$) i [21, tablica 8.2] (za $v \leq 100$).

5.2 Cameron-Delsarteov teorem

U ovoj cjelini cilj je pokazati da kombinatorni dizajn dovoljno velike snage i malog stupnja čini asocijacijsku shemu, podshemu Johnsonove sheme. Vrhovi su blokovi dizajna, a klase su određene veličinom presjeka, kao i u Johnsonovoj shemi $J(v, \Bbbk)$. Teorem su neovisno dokazali Peter Cameron [24] i Philippe Delsarte [40, teorem 5.25].

Teorem 5.14 (Cameron, Delsarte)**.** *Neka je $\mathscr{D}$ kombinatorni t-$(v, \Bbbk, \lambda)$ dizajn stupnja d s presječnim brojevima $x_1 > \ldots > x_d \geq 0$. Stavimo $x_0 = \Bbbk$ i* *za blokove $X, Y \in \mathcal{D}$ definiramo da su i-asocirani ako je $|X \cap Y| = x_i$. Ako vrijedi $t \geq 2d - 2$, onda tako dobivamo asocijacijsku shemu s d klasa.*

Za dizajn kojem blokovi čine asocijacijsku shemu obzirom na relacije iz teorema kažemo da je *shematski*. Uvjet $t \geq 2d - 2$ je dovoljan da bi dizajn bio shematski, a kasnije ćemo vidjeti da nije nužan. Dokaz smo preuzeli iz [54, teorem 5.1]. Prije dokaza teorema uvodimo notaciju i dokazujemo pomoćne rezultate. Neka je $W_{t\Bbbk}$ matrica kojoj su reci indeksirani t-članim podskupovima od V, a stupci $\Bbbk$-članim podskupovima od V. Za $T \in \binom{V}{t}$ i $K \in \binom{V}{\Bbbk}$ matrica na mjestu (T, K) ima 1 ako je $T \subseteq K$, a inače ima 0. Dakle, $W_{t\Bbbk}$ je 0-1 matrica tipa $\binom{v}{t} \times \binom{v}{\Bbbk}$ koju zovemo *inkluzijskom matricom.* Rick Wilson je koristio te matrice u [137] i u drugim radovima.

Skup vrhova Johnsonove sheme $J(v, \Bbbk)$ u nastavku označavamo $\Omega = \binom{V}{\Bbbk}$. Dizajn je podskup $\mathcal{D} \subseteq \Omega$ i možemo ga identificirati s indikatorskom funkcijom $f : \Omega \to \{0, 1\}$, $f(X) = 1$ ako je $X \in \mathcal{D}$, a $f(X) = 0$ inače.

Propozicija 5.15. *Indikatorska funkcija $f : \Omega \to \{0, 1\}$ predstavlja t-$(v, \Bbbk, \lambda)$ dizajn ako i samo ako vrijedi $W_{t\Bbbk} \cdot f = \lambda \mathbb{1}$. Ovdje je $\mathbb{1}$ vektor visine $\binom{v}{t}$ popunjen jedinicama.*

Dokaz. Produkt $W_{t\Bbbk} \cdot f$ je vektor visine $\binom{v}{t}$ koji u retku indeksiranom s $T \in \binom{V}{t}$ ima broj blokova iz $\mathcal{D}$ koji sadrže T. □

Time smo problem egzistencije t-$(v, \Bbbk, \lambda)$ dizajna sveli na rješavanje sustava linearnih jednadžbi nad $\{0, 1\}$, poznati NP-potpuni problem. Naš sustav ima $\binom{v}{\Bbbk}$ nepoznanica, previše za rješavanje na računalu i za male parametre v i $\Bbbk$. U Kramer-Mesnerovoj metodi [83] pretpostavljamo grupu automorfizama $G \leq S(V)$. Matricu $W_{t\Bbbk}$ zamijenimo "kondenziranom" matricom, kojoj su reci indeksirani orbitama t-podskupova, a stupci orbitama $\Bbbk$-podskupova. Ako dovoljno smanjimo sustav, ponekad ga možemo riješiti na računalu.

Propozicija 5.16. *Za $i \leq j \leq \Bbbk$ vrijedi* $W_{ij} \cdot W_{j\Bbbk} = \dbinom{\Bbbk - i}{j - i} W_{i\Bbbk}$.

Dokaz. Element produkta $W_{ij} \cdot W_{j\Bbbk}$ u retku indeksiranom s $I \in \binom{V}{i}$ i stupcu indeksiranom s $K \in \binom{V}{\Bbbk}$ je broj podskupova $J \in \binom{V}{j}$ takvih da je $I \subseteq J \subseteq K$. Ako je $I \subseteq K$, broj takvih podskupova je $\binom{\Bbbk - i}{j - i}$, a inače je 0. □

Iz propozicija 5.15 i 5.16 slijedi matrični dokaz propozicije 5.2, vidi [54, lema 2.2]. U Godsilovoj skripti na sličan način dokazana je i propozicija 5.4, vidi [54, lema 3.4]. Transponiranje u ovom poglavlju označavamo s τ jer je slovo t rezervirano za snagu dizajna.

Propozicija 5.17. *Vrijedi*

$$W_{i\Bbbk} \cdot W_{j\Bbbk}^{\tau} = \sum_{k=0}^{t} \binom{v-i-j}{v-\Bbbk-k} W_{ki}^{\tau} \cdot W_{kj}.$$

Dokaz. Neka je $I \in \binom{V}{i}$ i $J \in \binom{V}{j}$. Na lijevoj strani produkt $W_{i\Bbbk} \cdot W_{j\Bbbk}^{\tau}$ ima na mjestu (I,J) broj podskupova iz Ω koji sadrže I i J, a to je $\binom{v-|I\cup J|}{\Bbbk-|I\cup J|}$. Na odgovarajućem mjestu produkta $W_{ki}^{\tau} \cdot W_{kj}$ je broj podskupova $K \in \binom{V}{k}$ koji su sadržani u I i J, dakle $\binom{|I\cap J|}{k}$. U sumi na desnoj strani element na mjestu (I,J) je

$$\sum_{k=0}^{t} \binom{v-i-j}{v-\Bbbk-k}\binom{|I\cap J|}{k} = \binom{v-i-j+|I\cap J|}{v-\Bbbk}$$

(koristimo Vandermondeovu[31] konvoluciju). Po formuli uključivanja-isključivanja vrijedi $|I\cup J| = i+j-|I\cap J|$, pa se lijeva i desna strana podudaraju. □

Neka su $A_0,\ldots,A_{\Bbbk}$ Schurove idempotente Johnsonove sheme $J(v,\Bbbk)$. To su kvadratne matrice indeksirane s Ω takve da A_i na mjestu $(X,Y) \in \Omega\times\Omega$ ima 1 ako je $|X\cap Y| = \Bbbk - i$, a inače 0. One razapinju Bose-Mesnerovu algebru $\mathscr{A} = \langle A_0,\ldots,A_{\Bbbk}\rangle$ od $J(v,\Bbbk)$. Uvedimo sada još jedan skup matrica $C_i = W_{i\Bbbk}^{\tau} \cdot W_{i\Bbbk}$, $i = 0,\ldots,\Bbbk$, za koje ćemo pokazati da također čine bazu od $\mathscr{A}$. Produkt $W_{i\Bbbk}^{\tau} \cdot W_{i\Bbbk}$ na mjestu (X,Y) ima broj podskupova $I \in \binom{V}{i}$ koji su sadržani u X i Y. Stoga, ako je $|X\cap Y| = j$, element $(C_i)_{X,Y}$ je $\binom{j}{i}$ i vrijedi

$$C_i = \sum_{j\geq i} \binom{j}{i} A_{\Bbbk-j}, \quad i = 0,\ldots,\Bbbk.$$

Invertiranjem ovog sustava jednakosti dobivamo

$$A_{\Bbbk-i} = \sum_{j\geq i} (-1)^{j-i}\binom{j}{i} C_j, \quad i = 0,\ldots,\Bbbk,$$

što pokazuje da zaista vrijedi $\mathscr{A} = \langle C_0,\ldots,C_{\Bbbk}\rangle$. U ovoj bazi lakše je dokazati da je $\mathscr{A}$ komutativna algebra.

Propozicija 5.18. *Vrijedi*

$$C_iC_j = \sum_{k\leq i,j} \binom{v-i-j}{v-\Bbbk-k}\binom{\Bbbk-k}{i-k}\binom{\Bbbk-k}{j-k} C_k.$$

[31] Alexandre-Théophile Vandermonde (1735.-1796.), francuski matematičar, glazbenik i kemičar.

Dokaz.

$$\begin{aligned}
C_iC_j &= W_{i\Bbbk}^{\tau} W_{i\Bbbk} W_{j\Bbbk}^{\tau} W_{j\Bbbk} = \text{(propozicija 5.17)} = \\
&= W_{i\Bbbk}^{\tau} \left(\sum_k \binom{v-i-j}{v-\Bbbk-k} W_{ki}^{\tau} W_{kj} \right) W_{j\Bbbk} = \\
&= \sum_k \binom{v-i-j}{v-\Bbbk-k} (W_{ki}W_{i\Bbbk})^{\tau} W_{kj} W_{j\Bbbk} = \text{(propozicija 5.16)} = \\
&= \sum_k \binom{v-i-j}{v-\Bbbk-k} \binom{\Bbbk-k}{i-k} W_{k\Bbbk}^{\tau} \binom{\Bbbk-k}{j-k} W_{k\Bbbk} = \\
&= \sum_k \binom{v-i-j}{v-\Bbbk-k} \binom{\Bbbk-k}{i-k} \binom{\Bbbk-k}{j-k} C_k.
\end{aligned}$$

□

Desna strana je simetrična u i, j te vrijedi $C_iC_j = C_jC_i \in \mathscr{A}$, pa je potprostor $\mathscr{A}$ zatvoren na množenje i matrice iz $\mathscr{A}$ komutiraju. Ovo je matrični dokaz da $J(v,\Bbbk)$ čini asocijacijsku shemu. U primjeru 1.5 to smo dokazali računanjem presječnih brojeva. Baza $C_0, \ldots, C_\Bbbk$ kasnije će nam pomoći odrediti svojstvene vrijednosti Johnsonove sheme.

Neka je sada $\mathscr{D} \subseteq \Omega = \binom{V}{\Bbbk}$ kombinatorni dizajn s $b = |\mathscr{D}|$ blokova, a $W_i(\mathscr{D})$ podmatrica inkluzijske matrice $W_{i\Bbbk}$ koja se sastoji od stupaca iz $\mathscr{D}$. To je 0-1 matrica tipa $\binom{v}{i} \times b$.

Propozicija 5.19. *Ako je $\mathscr{D}$ t-dizajn i vrijedi $i+j \leq t$, onda je*

$$\frac{1}{b} W_i(\mathscr{D}) \cdot W_j(\mathscr{D})^{\tau} = \frac{1}{\binom{v}{\Bbbk}} W_{i\Bbbk} \cdot W_{j\Bbbk}^{\tau}.$$

Dokaz. Za $I \in \binom{V}{i}$, $J \in \binom{V}{j}$ označimo veličinu njihove unije $s = |I \cup J|$. Element na mjestu (I,J) produkta $W_i(\mathscr{D}) \cdot W_j(\mathscr{D})^{\tau}$ je broj blokova dizajna $\mathscr{D}$ koji sadrže $I \cup J$. Budući da je $s \leq i+j \leq t$, taj broj je λ_s iz propozicije 5.2. Odgovarajući element produkta $W_{i\Bbbk} \cdot W_{j\Bbbk}^{\tau}$ je broj svih $\Bbbk$-članih podskupova od V koji sadrže $I \cup J$, što je $\binom{v-s}{\Bbbk-s}$. Dakle, trebamo dokazati da je $\frac{\lambda_s}{b} = \frac{\binom{v-s}{\Bbbk-s}}{\binom{v}{\Bbbk}}$. Uvrštavanjem izraza za λ_s i b iz propozicije 5.2 na lijevoj strani dobivamo $\frac{\lambda_s}{b} = \frac{\binom{v-s}{t-s}\binom{\Bbbk}{t}}{\binom{v}{t}\binom{\Bbbk-s}{t-s}}$. Izjednačavanje s desnom stranom daje identitet $\binom{v-s}{t-s}\binom{v}{\Bbbk}\binom{\Bbbk}{t} = \binom{v}{t}\binom{v-s}{\Bbbk-s}\binom{\Bbbk-s}{t-s}$, koji slijedi iz formule $\binom{m}{n}\binom{n}{k} = \binom{m}{k}\binom{m-k}{n-k}$. □

Ova propozicija pokazuje da je t-$(v,\Bbbk,\lambda)$ dizajn "dobra aproksimacija" Johnsonove sheme $J(v,\Bbbk)$. Produkti restrikcija inkluzijskih matrica na blokove dizajna $W_i(\mathscr{D}) \cdot W_j(\mathscr{D})^{\tau}$ proporcionalni su produktima cijelih inkluzijskih matrica $W_{i\Bbbk} \cdot W_{j\Bbbk}^{\tau}$. Konstanta proporcionalnosti je omjer broja blokova dizajna i broja vrhova Johnsonove sheme $b/\binom{v}{k}$. Tvrdnja vrijedi za tim više indeksa $i+j \le t$ što je snaga dizajna veća.

Promotrimo vektorski prostor $\mathbb{R}^\Omega = \{f : \Omega \to \mathbb{R}\}$ svih realnih funkcija definiranih na skupu vrhova Johnsonove sheme. Za fiksni $T \subseteq V$ definiramo *inkluzijsku funkciju*

$$f_T : \Omega \to \mathbb{R}, \quad f_T(X) = \begin{cases} 1, & \text{ako je } T \subseteq X, \\ 0, & \text{inače.} \end{cases}$$

Funkcije f_T za $T \in \binom{V}{t}$ zapravo su reci inkluzijske matrice W_{tk}. Neka je $\mathrm{Pol}(\Omega, t)$ potprostor od $\mathbb{R}^\Omega$ razapet svim funkcijama f_S za $S \subseteq V$, $|S| \le t$. Uz uobičajenu definiciju množenja funkcija "po točkama", za $S, T \subseteq V$ vrijedi $f_S f_T = f_{S \cup T}$. Zato inkluzijsku funkciju f_S, $S \in \binom{V}{s}$ možemo prikazati kao produkt s inkluzijskih funkcija točaka $f_{\{x\}}$, $x \in V$. Prostor $\mathrm{Pol}(\Omega, t)$ je skup svih polinoma stupnja najviše t u varijablama $f_{\{x\}}$, $x \in V$. Iduća karakterizacija kombinatornih dizajna (teorem 7.1 u Godsilovoj skripti [54]) je još jedna analogija s definicijom sfernih dizajna 3.30.

Propozicija 5.20. *Familija $\mathcal{D} \subseteq \binom{V}{k}$ je t-(v, k, λ) dizajn ako i samo ako za svaku funkciju $f \in \mathrm{Pol}(\Omega, t)$ vrijedi*

$$\frac{1}{b} \sum_{X \in \mathcal{D}} f(X) = \frac{1}{\binom{v}{k}} \sum_{X \in \Omega} f(X).$$

Dokaz. Neka je $\mathcal{D}$ dizajn s parametrima t-(v, k, λ). Dovoljno je provjeriti tvrdnju za funkcije koje razapinju $\mathrm{Pol}(\Omega, t)$, inkluzijske funkcije f_S za $S \subseteq V$, $s = |S| \le t$. Po propoziciji 5.2 skup S je sadržan u točno λ_s blokova od $\mathcal{D}$, pa je prosječna vrijednost f_S po blokovima dizajna

$$\frac{1}{b} \sum_{X \in \mathcal{D}} f_S(X) = \frac{\lambda_s}{b} = \frac{\binom{v-s}{k-s}}{\binom{v}{k}}.$$

Drugu jednakost provjerili smo u dokazu propozicije 5.19. S druge strane, prosječna vrijednost f_S po svim $X \in \Omega = \binom{V}{k}$ je

$$\frac{1}{\binom{v}{k}} \sum_{X \in \Omega} f_S(X) = \frac{\binom{v-s}{k-s}}{\binom{v}{k}}.$$

Vidimo da se prosječne vrijednosti podudaraju.

Obrnuto, ako se prosječne vrijednosti podudaraju za sve funkcije $f \in \mathrm{Pol}(\Omega, t)$, onda se podudaraju i za sve inkluzijske funkcije f_T, $T \in \binom{V}{t}$:

$$\frac{1}{b} \sum_{X \in \mathcal{D}} f_T(X) = \frac{1}{\binom{v}{k}} \sum_{X \in \Omega} f_T(X) = \frac{\binom{v-t}{k-t}}{\binom{v}{k}}.$$

Uvrštavanjem izraza $b = \lambda\binom{v}{t}/\binom{k}{t}$ dobijemo

$$\sum_{X\in\mathcal{D}} f_T(X) = b\,\frac{\binom{v-t}{k-t}}{\binom{v}{k}} = \lambda\,\frac{\binom{v}{t}\binom{v-t}{k-t}}{\binom{v}{k}\binom{k}{t}} = \lambda,$$

a to znači da je T sadržan u točno λ blokova od $\mathcal{D}$. Dakle, $\mathcal{D}$ je t-(v,k,λ) dizajn. □

Za dokaz teorema 5.14 trebamo još i sljedeći rezultat o determinanti sličnoj Vandermondeovoj.

Lema 5.21. *Determinanta*

$$\begin{vmatrix} \binom{x_0}{0} & \binom{x_1}{0} & \cdots & \binom{x_d}{0} \\ \binom{x_0}{1} & \binom{x_1}{1} & \cdots & \binom{x_d}{1} \\ \vdots & \vdots & & \vdots \\ \binom{x_0}{d} & \binom{x_1}{d} & \cdots & \binom{x_d}{d} \end{vmatrix}$$

jednaka je 0 *ako i samo ako je* $x_i = x_j$ *za neke* $i \neq j$.

Dokaz. Elementarnim transformacijama nad recima možemo je svesti na Vandermondeovu determinantu. □

Sada smo spremni dokazati Cameron-Delsarteov teorem.

Dokaz teorema 5.14. Sjetimo se, $\mathcal{D}$ je t-(v,k,λ) dizajn s presječnim brojevima $x_1 > \cdots > x_d \geq 0$, a $x_0 = k$. Neka je A_i matrica tipa $b\times b$ indeksirana blokovima dizajna $\mathcal{D}$ koja na mjestu (X,Y) ima 1 ako je $|X\cap Y| = x_i$, a inače ima 0. Uz pretpostavku $t \geq 2d-2$, želimo dokazati da matrice $A_0,\ldots,A_d$ čine asocijacijsku shemu, tj. simetričnu koherentnu konfiguraciju u smislu definicije 2.1. Prva dva svojstva iz definicije i simetričnost matrica A_i je očita. Za četvrto svojstvo trebamo provjeriti da je potprostor $\mathcal{A} = \langle A_0,\ldots,A_d\rangle$ zatvoren na množenje. Nakon propozicije 5.17 uveli smo drugu bazu Bose-Mesnerove algebre Johnsonove sheme, u kojoj je bilo lakše provjeriti zatvorenost na množenje. Slično, sada uvodimo matrice $C_i(\mathcal{D}) = W_i(\mathcal{D})^\tau \cdot W_i(\mathcal{D})$ tipa $b\times b$. Element te matrice na mjestu $(X,Y)\in\mathcal{D}\times\mathcal{D}$ je broj i-članih podskupova presjeka $X\cap Y$. Ako je $|X\cap Y| = x_j$, to je binomni koeficijent $\binom{x_j}{i}$. Prema tome, vrijedi

$$C_i(\mathcal{D}) = \sum_{j=0}^{d} \binom{x_j}{i} A_j, \quad i = 0,\ldots,d.$$

Prema lemi 5.21 matrica koeficijenata ovog sustava je regularna, pa možemo prikazati $A_0, \ldots, A_d$ kao linearne kombinacije od $C_0(\mathscr{D}), \ldots, C_d(\mathscr{D})$. Zato je to druga baza od $\mathscr{A}$. Matricu $C_d(\mathscr{D})$ te baze možemo zamijeniti s jediničnom matricom $I = A_0$, budući da je koeficijent u prikazu A_0 uz $C_d(\mathscr{D})$ različit od nule. To se provjeri računanjem "adjunkte", tj. kofaktora elementa $\binom{x_0}{d}$ determinante iz leme 5.21.

Dakle, vrijedi $\mathscr{A} = \langle I, C_0(\mathscr{D}), \ldots, C_{d-1}(\mathscr{D})\rangle$. Da bismo provjerili zatvorenost na množenje, trebamo pokazati $C_i(\mathscr{D})C_j(\mathscr{D}) \in \mathscr{A}$ za sve $i, j < d$. Matrica $C_i(\mathscr{D})$ je restrikcija od $C_i = W_{i\hbar}^\tau W_{i\hbar}$ na blokove dizajna. Retke i stupce simetrične matrice C_i možemo tumačiti kao funkcije iz $\mathrm{Pol}(\Omega, i)$. Stupac koji odgovara $Y \in \Omega$ je funkcija $f : \Omega \to \mathbb{R}$, $f(X) = (C_i)_{X,Y} = \binom{|X\cap Y|}{i}$. Možemo je prikazati kao $f(X) = \sum_{S\in\binom{Y}{i}} f_S(X)$, pa pripada prostoru $\mathrm{Pol}(\Omega, i)$. Za indekse $i, j < d$ reci i stupci od C_i, C_j su funkcije iz $\mathrm{Pol}(\Omega, d-1)$, a reci i stupci od $C_i(\mathscr{D})$, $C_j(\mathscr{D})$ njihove restrikcije na blokove dizajna. Produkt dvije takve funkcije je iz $\mathrm{Pol}(\Omega, 2d-2) \subseteq \mathrm{Pol}(\Omega, t)$, zbog pretpostavke $t \geq 2d-2$.

Element $(C_i(\mathscr{D})C_j(\mathscr{D}))_{X,Y}$ je "skalarni produkt" retka od $C_i(\mathscr{D})$ indeksiranog s $X \in \Omega$ i stupca od $C_j(\mathscr{D})$ indeksiranog s $Y \in \Omega$. To je suma produkta odgovarajućih funkcija iz $\mathrm{Pol}(\Omega, d-1)$ po blokovima dizajna. Element $(C_iC_j)_{X,Y}$ je suma produkta tih funkcija po svim elementima iz Ω. Po propoziciji 5.20 vrijedi

$$\frac{1}{b}(C_i(\mathscr{D})C_j(\mathscr{D}))_{X,Y} = \frac{1}{\binom{v}{\hbar}}(C_iC_j)_{X,Y}.$$

Sada primijenimo propoziciju 5.18:

$$\begin{aligned}(C_i(\mathscr{D})C_j(\mathscr{D}))_{X,Y} &= \frac{b}{\binom{v}{\hbar}}(C_iC_j)_{X,Y}\\ &= \frac{b}{\binom{v}{\hbar}}\sum_{k\leq i,j}\binom{v-i-j}{v-\hbar-k}\binom{\hbar-k}{i-k}\binom{\hbar-k}{j-k}(C_k)_{X,Y}\\ &= \frac{b}{\binom{v}{\hbar}}\sum_{k\leq i,j}\binom{v-i-j}{v-\hbar-k}\binom{\hbar-k}{i-k}\binom{\hbar-k}{j-k}(C_k(\mathscr{D}))_{X,Y}.\end{aligned}$$

U zadnjem retku mogli smo zamijeniti C_k sa $C_k(\mathscr{D})$ jer je $(X, Y) \in \mathscr{D} \times \mathscr{D}$. Dakle, produkt $C_i(\mathscr{D})C_j(\mathscr{D})$ je linearna kombinacija od $C_0(\mathscr{D}), \ldots, C_{d-1}(\mathscr{D})$ i sadržan je u $\mathscr{A}$. Time je teorem dokazan. $\square$

Ako je stupanj $d = 1$, asocijacijsku shemu dobivamo već od dizajna snage $t = 0$, tj. od bilo koje familije $\mathscr{D} \subseteq \binom{V}{\hbar}$ u kojoj se svaka dva bloka sijeku u istom broju točaka. Shema je trivijalna jer ima samo jednu klasu. Zato za simetrične dizajne ne dobivamo nikakve dodatne uvjete na parametre.

Za stupanj $d = 2$, iz teorema slijedi da su dizajni snage $t \geq 2d-2 = 2$ shematski. Asocijacijska shema ima dvije klase i ekvivalentna je jako regularnom grafu i njegovu komplementu. To je takozvani *blokovni graf* kvazisimetričnog dizajna. Vrhovi su blokovi dizajna, a susjedni su ako se sijeku u y točaka ($x < y$ su presječni brojevi dizajna). Kao korolar Cameron-Delsarteova teorema dobili smo poznati rezultat da je blokovni graf kvazisimetričnog dizajna jako regularan [116, 58]. Direktni dokaz tog teorema dan je u [84, teorem 2.3], a uobičajeni "sprektralni dokaz" u [84, teorem 2.16]. Zbog jake regularnosti blokovnog grafa dobivamo dodatne uvjete na parametre kvazisimetričnog 2-dizajna i njegove presječne brojeve, povrh standardnih nužnih uvjeta za egzistenciju 2-dizajna (uvjeti djeljivosti iz korolara 5.3 i Fisherova nejednakost, teorem 5.6). Tablica dopustivih parametara kvazisimetričnih dizajna izvodi se iz tih uvjeta, vidi cjelinu 2.4 u [84].

Promotrimo sada dizajne stupnja $d = 3$ kojima blokovi tvore asocijacijsku shemu s tri klase. Po teoremu 5.14, dovoljan uvjet je snaga dizajna $t \geq 2d - 2 = 4$. U članku [86] izračunate su svojstvene vrijednosti sheme $P = [P_j(i)]_{i,j=0}^3$ iz parametara 4-$(v, \Bbbk, \lambda)$ i presječnih brojeva $x < y < z$. Znamo da je $P_0(i) = 1$, a ostale svojstvene vrijednosti možemo izraziti s pomoću

$$\theta_j(i) = \lambda \binom{v-i-j}{\Bbbk - j}\binom{\Bbbk - i}{j-i} \Big/ \binom{v-4}{\Bbbk-4}$$

kao

$$\begin{aligned} P_1(i) &= \frac{yz\theta_0(i) + (1-y-z)\theta_1(i) + 2\theta_2(i) - (y-\Bbbk)(z-\Bbbk)}{(y-x)(z-x)}, \\ P_2(i) &= \frac{xz\theta_0(i) + (1-x-z)\theta_1(i) + 2\theta_2(i) - (x-\Bbbk)(z-\Bbbk)}{(x-y)(z-y)}, \\ P_3(i) &= \frac{xy\theta_0(i) + (1-x-y)\theta_1(i) + 2\theta_2(i) - (x-\Bbbk)(y-\Bbbk)}{(x-z)(y-z)}. \end{aligned} \tag{50}$$

Kratnosti su $m_i = \binom{v}{i} - \binom{v}{i-1}$ za $i = 0, 1, 2$ i $m_3 = b - \binom{v}{2}$. Iz uvjeta cjelobrojnosti svojstvenih vrijednosti i presječnih brojeva određeni su u [86] svi dopustivi parametri takvih dizajna s $v \leq 1000$ točaka. Postoji samo 11 takvih parametara, navedenih u tablici 4. Dizajni iz prvih pet redaka postoje, a za ostale je egzistencija otvorena. Parametri u sivim recima tablice pripadaju beskonačnoj seriji dopustivih parametara

$$\begin{aligned} v &= 8n^2 - 1, \\ k &= 4n^2 - 1 = (2n-1)(2n+1), \\ \lambda &= 4n^4 - 7n^2 + 3 = (n-1)(n+1)(4n^2-3), \end{aligned} \tag{51}$$

Rbr	v	k	λ	x	y	z	Egzistencija
1	11	5	1	1	2	3	$\exists$
2	23	8	4	0	2	4	$\exists$
3	23	11	48	3	5	7	$\exists$
4	24	8	5	0	2	4	$\exists$
5	47	11	8	1	3	5	$\exists$
6	71	35	264	14	17	20	?
7	199	99	2328	44	49	54	?
8	391	195	9264	90	97	104	?
9	647	323	25680	152	161	170	?
10	659	329	390874	153	164	175	?
11	967	483	57720	230	241	252	?

Tablica 4: Dopustivi parametru shematskih 4-dizajna za $v \leq 1000$.

$$\begin{aligned} x &= 2n^2 - n - 1 = (n-1)(2n+1), \\ y &= 2n^2 - 1, \\ z &= 2n^2 + n - 1 = (n+1)(2n-1), \end{aligned}$$

za neparne $n \in \mathbb{N}$. Proučimo pobliže dizajne i asocijacijske sheme iz prvih pet redaka tablice 4.

Primjer 5.22. *Dizajn* 4-$(11, 5, 1)$ *s presječnim brojevima* $x = 1$, $y = 2$, $z = 3$ *je derivirani dizajn malog Wittovog dizajna iz primjera 5.10. O deriviranim i rezidualnim dizajnima vidi [84], definiciju 1.26 i propoziciju 1.27. Broj blokova je* $b = 66$, *dakle dobivamo asocijacijsku shemu reda* 66 *s tri klase koja je primitivna. Koristimo naredbu* `BlockScheme` *iz GAP paketa PAG [85]:*

```
gap> diz4:=DerivedBlockDesign(diz1,1);;
gap> AllTDesignLambdas(diz4);
[ 66, 30, 12, 4, 1 ]
gap> IntersectionNumbers(diz4);
[ 1, 2, 3 ]
gap> shema4:=BlockScheme(diz4);
< 3-class association scheme of order 66 >
gap> IsPrimitive(shema4);
true
```

Naredba `IsPrimitive` *je iz paketa AssociationSchemes [2]. Svojstvene vrijednosti možemo izračunati pomoću naredbe* `MatrixOfEigenvalues` *ili iz for-*

mula (50)*:*

$$P = \begin{bmatrix} 1 & 15 & 20 & 30 \\ 1 & -7 & -2 & 8 \\ 1 & 2 & -2 & -1 \\ 1 & -3 & 8 & -6 \end{bmatrix}.$$

Primjer 5.23. *Dizajn* 4-$(23, 8, 4)$ *s presječnim brojevima* $x = 0$*,* $y = 2$*,* $z = 4$ *je rezidualni dizajn velikog Wittovog dizajna iz primjera 5.11.*

```
gap> diz5:=ResidualBlockDesign(diz3,1);;
gap> AllTDesignLambdas(diz5);
[ 506, 176, 56, 16, 4 ]
gap> IntersectionNumbers(diz5);
[ 0, 2, 4 ]
gap> shema5:=BlockScheme(diz5);
< 3-class association scheme of order 506 >
gap> IsPrimitive(shema5);
true
```

Asocijacijska shema je primitivna, reda 506 *s tri klase i svojstvenim vrijednostima*

$$P = \begin{bmatrix} 1 & 15 & 280 & 210 \\ 1 & -8 & -42 & 49 \\ 1 & 4 & -6 & 1 \\ 1 & -3 & 8 & -6 \end{bmatrix}.$$

Primjer 5.24. *Dizajn* 4-$(23, 11, 48)$ *s presječnim brojevima* $x = 3$*,* $y = 5$*,* $z = 7$ *dobivamo od Mathieuove grupe* M_{23}*.*

```
gap> diz6:=KramerMesnerSearch(4,23,11,48,MathieuGroup(23))[1];;
gap> AllTDesignLambdas(diz6);
[ 1288, 616, 280, 120, 48 ]
gap> IntersectionNumbers(diz6);
[ 3, 5, 7 ]
gap> shema6:=BlockScheme(diz6);
< 3-class association scheme of order 1288 >
gap> IsPrimitive(shema6);
true
```

Odgovarajuća shema je primitivna, reda 1288 *s tri klase i svojstvenim vrijednostima*

$$P = \begin{bmatrix} 1 & 165 & 792 & 330 \\ 1 & -65 & -36 & 100 \\ 1 & 19 & -36 & 16 \\ 1 & -3 & 8 & -6 \end{bmatrix}.$$

Primjer 5.25. *Dizajn* 4-$(24, 8, 5)$ *s presječnim brojevima* $x = 0$, $y = 2$, $z = 4$ *je veliki Wittov dizajn iz primjera 5.11 promatran kao* 4*-dizajn. Shema je primitivna, reda* 759 *s tri klase i svojstvenim vrijednostima*

$$P = \begin{bmatrix} 1 & 30 & 448 & 280 \\ 1 & -15 & -56 & 70 \\ 1 & 7 & -12 & 4 \\ 1 & -3 & 8 & -6 \end{bmatrix}.$$

Primjer 5.26. *Dizajn* 4-$(47, 11, 8)$ *s presječnim brojevima* $x = 1$, $y = 3$, $z = 5$ *povezan je s kodom kvadratnih ostataka* $QR(47, 2)$ *s parametrima* $[47, 24, 11]_2$*. Dobiva se kao derivirani dizajn* 5-$(48, 12, 8)$ *dizajna spomenutog na kraju članka [125]. Shema je primitivna, reda* 4324 *s tri klase i svojstvenim vrijednostima*

$$P = \begin{bmatrix} 1 & 1386 & 2475 & 462 \\ 1 & -259 & 125 & 133 \\ 1 & 29 & -55 & 25 \\ 1 & -6 & 15 & -10 \end{bmatrix}.$$

U članku [65] postavljena je hipoteza da je jedini dizajn stupnja $d = 3$ i snage $t = 5$ veliki Wittov dizajn 5-$(24, 8, 1)$. Tvrdnja je dokazana uz neke dodatne pretpostavke, ali općenito je i dalje otvorena. Za snagu $t = 4$ poznato je samo pet spomenutih primjera. Dopustivih parametara ima beskonačno mnogo (51), ali nažalost u članku [86] nije dokazana klasifikacija parametara poput Cameronove [25] za kvazisimetrične 3-dizajne s $x = 0$. Ako zadržimo stupanj $d = 3$ i spustimo snagu na $t = 3$, više nije zadovoljen uvjet $t \geq 2d - 2$ iz Cameron-Deslarteova teorema i dizajn ne mora biti shematski. Poznato je beskonačno mnogo takvih dizajna, a neki od njih ipak su shematskih. Jedna serija primjera dobiva se od klasičnih SSSD-ova [31, 57] koji dostižu Nodinu nejednakost, na način opisan u teoremu 4.43. Odgovarajuće asocijacijske sheme s tri klase su imprimitivne. Ova serija pokazuje da uvjet $t \geq 2d - 2$ iz Cameron-Delsarteova teorema nije nužan da bi dizajn bio shematski. Druga serija takvih primjera su Steinerovi dizajni 3-$(n^2 + 1, n + 1, 1)$ za parne n, takozvane inverzijske ravnine parnog reda.

Zadatak 5.27. *Dokažite da su dizajni* 3-$(n^2 + 1, n + 1, 1)$ *za parne* n *shematski i ispitajte (im)primitivnost odgovarajućih asocijacijskih shema. Ispitajte (im)primitivnost asocijacijskih shema dobivenih od* 4*-dizajna s parametrima* (51) *za neparne* n*.*

U Grassmannovoj asocijacijskoj shemi (primjer 1.7) nije teško formulirati definiciju analognu definiciji 5.1. To su takozvani q-analogoni dizajna ili dizajni nad konačnim poljima $\mathbb{F}_q$, kojima parametre označavamo t-$(v, k, \lambda)_q$. U članku [17] dan je pregled rezultata o q-analogonima dizajna. Prvi i do sada jedini primjeri Steinerovih dizajna nad $\mathbb{F}_q$ su 2-$(13, 3, 1)_2$ dizajni konstruirani u [16]. Pitanje egzistencije 2-$(7, 3, 1)_2$ dizajna je otvoreno.

Literatura

[1] B. Bajnok, *Additive combinatorics. A menu of research problems*, CRC Press, Boca Raton, FL, 2018.

[2] J. Bamberg, A. Hanaki, J. Lansdown, *AssociationSchemes, A GAP package for working with association schemes and homogeneous coherent configurations*, verzija 3.0.0, 2023. `http://www.jesselansdown.com/AssociationSchemes`

[3] E. Bannai, *On tight designs*, Quart. J. Math. Oxford Ser. (2) **28** (1977), no. 112, 433–448.

[4] E. Bannai, E. Bannai, T. Ito, R. Tanaka, *Algebraic combinatorics*, De Gruyter, 2021.

[5] E. Bannai, E. Bannai, H. Tanaka, Y. Zhu, *Design theory from the viewpoint of algebraic combinatorics*, Graphs Combin. **33** (2017), no. 1, 1–41.

[6] E. Bannai, T. Ito, *Algebraic combinatorics. I. Association schemes*, The Benjamin/Cummings Publishing Co., 1984.

[7] V. Belevitch, *Theory of $2n$-terminal networks with applications to conference telephony*, Electrical Communication **27** (1950), 231–244. `http://archivodigital.coit.es/uploads/documentos/ec/1948-1954/vol27-1950-03.pdf`

[8] A. Betten, A. Kerber, R. Laue, A. Wassermann, *Es gibt* 7*-Designs mit kleinen Parametern!*, Bayreuth. Math. Schr. **49** (1995), 213.

[9] A. Betten, A. Kerber, R. Laue, A. Wassermann, *Simple* 8*-designs with small parameters*, Des. Codes Cryptogr. **15** (1998), no. 1, 5–27.

[10] A. Betten, R. Laue, A. Wassermann, *Simple* 6*- and* 7*-designs on* 19 *to* 33 *points*, Congr. Numer. **123** (1997), 149–160.

[11] N. Biggs, *Automorphic graphs and the Krein condition*, Geometriae Dedicata **5** (1976), no. 1, 117–127.

[12] R. C. Bose, *On the construction of balanced incomplete block designs*, Ann. Eugen. **9** (1939), 353–399. https://doi.org/10.1111/j.1469-1809.1939.tb02219.x

[13] R. C. Bose, *Strongly regular graphs, partial geometries and partially balanced designs*, Pacific J. Math. **13** (1963), 389–419.

[14] R. C. Bose, D. M. Mesner, *On linear associative algebras corresponding to association schemes of partially balanced designs*, Ann. Math. Statist. **30** (1959), 21–38.

[15] R. C. Bose, T. Shimamoto, *Classification and analysis of partially balanced incomplete block designs with two associate classes*, J. Amer. Statist. Assoc. **47** (1952), 151–184.

[16] M. Braun, T. Etzion, P. R. J. Östergard, A. Vardy, A. Wassermann, *Existence of q-analogs of Steiner systems*, Forum Math. Pi **4** (2016), e7, 14 str.

[17] M. Braun, M. Kiermaier, A. Wassermann, *q-analogs of designs: subspace designs*, u *Network coding and subspace designs* (ur. M. Greferath, M. O. Pavčević, N. Silberstein, M. Á. Vázquez-Castro), Springer, 2018., str. 171–211.

[18] A. Bremner, *A Diophantine equation arising from tight* 4*-designs*, Osaka J. Math. **16** (1979), 353–356.

[19] A. E. Brouwer, *Parameters of strongly regular graphs*, https://www.win.tue.nl/~aeb/graphs/srg/srgtab.html (pristupljeno 10.2.2024.)

[20] A. E. Brouwer, A. M. Cohen, A. Neumaier, *Distance-regular graphs*, Springer-Verlag, 1989.

[21] A. E. Brouwer, H. Van Maldeghem, *Strongly regular graphs*, Cambridge University Press, 2022. https://homepages.cwi.nl/~aeb/math/srg/rk3/srgw.pdf

[22] F. C. Bussemaker, W. H. Haemers, R. Mathon, H. A. Wilbrink, *A* $(49, 16, 3, 6)$ *strongly regular graph does not exist*, European J. Combin. **10** (1989), no. 5, 413–418.

[23] P. J. Cameron, *On groups with several doubly-transitive permutation representations*, Math. Z. **128** (1972), 1–14.

[24] P. J. Cameron, *Near-regularity conditions for designs*, Geometriae Dedicata **2** (1973), 213–223.

[25] P. J. Cameron, *Extending symmetric designs*, J. Combinatorial Theory Ser. A **14** (1973), 215–220.

[26] P. J. Cameron, 6-*transitive graphs*, J. Combin. Theory Ser. B **28** (1980), no. 2, 168–179.

[27] P. J. Cameron, *Permutation groups*, Cambridge University Press, 1999.

[28] P. J. Cameron, *Random strongly regular graphs?*, Discrete Math. **273** (2003), no. 1-3, 103–114.

[29] P. J. Cameron, *Strongly regular graphs*, u *Topics in algebraic graph theory* (ed. L. W. Beineke, R. J. Wilson), Cambridge University Press, Cambridge, 2004.

[30] P. J. Cameron, *Terminology: association scheme or coherent configuration?*, `https://cameroncounts.wordpress.com/2014/06/08/terminology-association-scheme-or-coherent-configuration/` (pristupljeno 10.11.2023.)

[31] P. J. Cameron, J. J. Seidel, *Quadratic forms over $GF(2)$*, Nederl. Akad. Wetensch. Proc. Ser. A **76** Indag. Math. **35** (1973), 1–8.

[32] J. A. Davis, W. J. Martin, J. B. Polhill, *Linking systems in nonelementary abelian groups*, J. Combin. Theory Ser. A **123** (2014), 92–103.

[33] P. J. Cameron, J.-M. Goethals, J. J. Seidel, *Strongly regular graphs having strongly regular subconstituents*, J. Algebra **55** (1978), no. 2, 257–280.

[34] P. J. Cameron, J. H. van Lint, *Designs, graphs, codes and their links*, Cambridge University Press, Cambridge, 1991.

[35] L. C. Chang, *The uniqueness and nonuniqueness of the triangular association schemes*, Sci. Record (N.S.) **3** (1959), 604–613.

[36] L. C. Chang, *Association schemes of partially balanced designs with parameters $v = 28$, $n_1 = 12$, $n_2 = 15$ and $p^2_{11} = 4$*, Sci. Record (N.S.) **4** (1960), 12–18.

[37] D. Crnković, M. Maksimović, *Construction of strongly regular graphs having an automorphism group of composite order*, Contrib. Discrete Math. **15** (2020), no. 1, 22–41.

[38] D. Crnković, M. Maksimović, *Strongly regular graphs with parameters* $(37, 18, 8, 9)$ *having nontrivial automorphisms*, Art Discrete Appl. Math. **3** (2020), no. 2, Paper No. 2.10.

[39] D. Crnković, S. Rukavina, A. Švob, *New strongly regular graphs from orthogonal groups* $O^+(6,2)$ *and* $O^-(6,2)$, Discrete Math. **341** (2018), no. 10, 2723–2728.

[40] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. **10** (1973), vi+97 pp.

[41] P. Delsarte, *Bilinear forms over a finite field, with applications to coding theory*, J. Combin. Theory Ser. A **25** (1978), no. 3, 226–241.

[42] P. Delsarte, J.-M. Goethals, J. J. Seidel, *Bounds for systems of lines, and Jacobi polynomials*, Philips Research Reports **30** (1975), 91–105. Nalazi se također u *Geometry and combinatorics. Selected works of J. J. Seidel* (ed. D. G. Corneil, R. Mathon), Academic Press, Inc., Boston, MA, 1991.

[43] P. Delsarte, J.-M. Goethals, J. J. Seidel, *Spherical codes and designs*, Geometriae Dedicata **6** (1977), no. 3, 363–388.

[44] P. Dukes, R.M. Wilson, *The cone condition and* t*-designs*, European J. Combin. **28** (2007), 1610–1625.

[45] H. Enomoto, N. Ito, R. Noda, *Tight* 4*-designs*, Osaka J. Math. **16** (1979), 39–43.

[46] P. Erdős, A. Rényi, *Asymmetric graphs*, Acta Math. Acad. Sci. Hungar. **14** (1963), 295–315.

[47] T. Ericson, V. Zinoviev, *Codes on Euclidean spheres*, North-Holland Publishing Co., Amsterdam, 2001.

[48] I. A. Faradžev, A. A. Ivanov, M. H. Klin, A. J. Woldar (urednici), *Investigations in algebraic theory of combinatorial objects*, Kluwer Academic Publishers Group, Dordrecht, 1994.

[49] R. A. Fisher, *An examination of the different possible solutions of a problem in incomplete blocks*, Ann. Eugen. **10** (1940), 52–75. `https://doi.org/10.1111/j.1469-1809.1940.tb02237.x`

[50] R. A. Fisher, *The design of experiments (9th ed.)*, Macmillan, 1971. (prvo izdanje 1935.).

[51] J. S. Frame, *The double cosets of a finite group*, Bull. Amer. Math. Soc. **47** (1941), 458–467.

[52] The GAP Group, *GAP – Groups, Algorithms, and Programming*, Version 4.12.2, 2022. `https://www.gap-system.org`

[53] C. D. Godsil, *Algebraic combinatorics*, Chapman & Hall, 1993.

[54] C. D. Godsil, *Linear algebra and designs*, University of Waterloo, 1995.

[55] C. Godsil, *Association schemes*, University of Waterloo, 2010. `https://www.math.uwaterloo.ca/~cgodsil/pdfs/assoc2.pdf`

[56] C. Godsil, *Finite geometry*, University of Waterloo, 2004. `https://www.math.uwaterloo.ca/~cgodsil/pdfs/fgeom.pdf`

[57] J.-M. Goethals, *Nonlinear codes defined by quadratic forms over* $GF(2)$, Information and Control **31** (1976), no. 1, 43–74.

[58] J.-M. Goethals, ; J. J. Seidel, *Strongly regular graphs derived from combinatorial designs*, Canadian J. Math. **22** (1970), 597–614.

[59] A. Herman, *Seminar notes: Algebraic aspects of association schemes and scheme rings*, University of Regina, 2011. `https://uregina.ca/~hermana/ASSR-Lecture9.pdf`

[60] D. G. Higman, *Coherent configurations. I. Ordinary representation theory*, Geometriae Dedicata **4** (1975), no. 1, 1–32.

[61] D. G. Higman, *Coherent configurations. II. Weights*, Geometriae Dedicata **5** (1976), no. 4, 413–424.

[62] R. Hill, *A first course in coding theory*, Clarendon Press, Oxford, 1986.

[63] R. A. Horn, C. B. Johnson, *Matrix analysis. Second edition*, Cambridge University Press, 2013.

[64] D. R. Hughes, *On* t*-designs and groups*, Amer. J. Math. **87** (1965), 761–778.

[65] Y. J. Ionin, M. S. Shrikhande, 5*-designs with three intersection numbers*, J. Combin. Theory Ser. A **69** (1995), no. 1, 36–50.

[66] Y. J. Ionin, M. S. Shrikhande, *Combinatorics of symmetric designs*, Cambridge University Press, 2006.

[67] Y. J. Ionin, T. V. Tran, *Symmetric designs*, u: *The Handbook of Combinatorial Designs, Second Edition* (urednici C.J. Colbourn i J.H. Dinitz), CRC Press, 2007., str. 110–124.

[68] N. Ito, *On tight* 4*-designs*, Osaka J. Math. **12** (1975), 493–522.

[69] N. Ito, *Corrections and supplements to: "On tight 4-designs"*, Osaka J. Math. 15 (1978), 693–697.

[70] Z. Janko, *The existence of symmetric designs with parameters* $(105, 40, 15)$, J. Combin. Des. **7** (1999), no. 1, 17–19.

[71] Z. Janko, *The existence of symmetric designs with parameters* $(189, 48, 12)$, J. Combin. Theory Ser. A **80** (1997), no. 2, 334–338.

[72] Z. Janko, *The existence of a Bush-type Hadamard matrix of order* 36 *and two new infinite classes of symmetric designs*, J. Combin. Theory Ser. A **95** (2001), no. 2, 360–364.

[73] Z. Janko, H. Kharaghani, *A block negacyclic Bush-type Hadamard matrix and two strongly regular graphs*, J. Combin. Theory Ser. A **98** (2002), no. 1, 118–126.

[74] Z. Janko, H. Kharaghani, V. D. Tonchev, *The existence of a Bush-type Hadamard matrix of order* 324 *and two new infinite classes of symmetric designs*, Des. Codes Cryptogr. **24** (2001), no. 2, 225–232.

[75] Z. Janko, T. V. Tran, *The existence of a symmetric block design for* $(70, 24, 8)$, Mitt. Math. Sem. Giessen No. **165** (1984), 17–18.

[76] Z. Janko, T. V. Tran, *Construction of two symmetric block designs for* $(71, 21, 6)$, Discrete Math. **55** (1985), no. 3, 327–328.

[77] Z. Janko and T. V. Tran, *Construction of a new symmetric block design for* $(78, 22, 6)$ *with the help of tactical decompositions*, J. Combin. Theory Ser. A, **40** (1985), 451–455.

[78] J. Jedwab, S. Li, S. Simon, *Linking systems of difference sets*, J. Combin. Des. **27** (2019), no. 3, 161–187.

[79] W. M. Kantor, *k-homogeneous groups*, Math. Z. **124** (1972), 261–265.

[80] P. Keevash, *The existence of designs*, 2014. (novija verzija 2019.). `https://arxiv.org/abs/1401.3665`

[81] P. Keevash, *The existence of designs II*, 2018. https://arxiv.org/abs/1802.05900

[82] B. G. Kodalen, *Linked systems of symmetric designs*, Algebr. Comb. **2** (2019), no. 1, 119–147.

[83] E. S. Kramer, D. M. Mesner, *t-designs on hypergraphs*, Discrete Math. **15** (1976), no. 3, 263–296.

[84] V. Krčadinac, *Kvazisimetrični dizajni*, skripta, Sveučilište u Zagrebu, 2017. https://web.math.pmf.unizg.hr/~krcko/nastava/kvazisim.pdf

[85] V. Krčadinac, *PAG, Prescribed Automorphism Groups*, verzija 0.2.2, 2023. https://vkrcadinac.github.io/PAG

[86] V. Krčadinac, R. Vlahović Kruc, *Schematic* 4*-designs*, Discrete Math. **346** (2023), no. 7, članak 113385, 7 str.

[87] M. G. Krein, *Hermitian-positive kernels on homogeneous spaces. I* (na ruskom), Ukrain. Mat. Žurnal **1** (1949), no. 4, 64–98.

[88] M. G. Krein, *Hermitian-positive kernels in homogeneous spaces. II*, (na ruskom), Ukrain. Mat. Žurnal **2** (1950), 10–59.

[89] C. W. H. Lam, L. Thiel, S. Swiercz, *The nonexistence of finite projective planes of order* 10, Canad. J. Math. **41** (1989), no. 6, 1117–1123.

[90] E.S. Lander, *Symmetric designs: an algebraic approach*, Cambridge University Press, 1983.

[91] R. Laue, *Constructing objects up to isomorphism, simple* 9*-designs with small parameters*, u: *Algebraic combinatorics and applications (Gößweinstein, 1999)* (ur. A. Betten, A. Kohnert, R. Laue, A. Wassermann), Springer-Verlag, 2001., str. 232–260.

[92] D. Livingstone, A. Wagner, *Transitivity of finite permutation groups on unordered sets*, Math. Z. **90** (1965), 393–403.

[93] S. S. Magliveras, D. W. Leavitt, *Simple* 6-$(33, 8, 36)$ *designs from* $P\Gamma L_2(32)$, u: *Computational group theory* (ur. M. D. Atkinson), Academic Press, Inc., 1984., str. 337–352.

[94] M. Maksimović, S. Rukavina, *New regular two-graphs on* 38 *and* 42 *vertices*, Math. Commun. **27** (2022), no. 2, 151–161.

[95] É. Mathieu, *Mémoire sur l'étude des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariables*, Journal de Mathématiques Pures et Appliquées **6** (1863), 241–323.

[96] É. Mathieu, *Sur la fonction cinq fois transitive de* 24 *quantités*, Journal de Mathématiques Pures et Appliquées **18** (1873), 25–46.

[97] R. Mathon, *Symmetric conference matrices of order* $pq^2 + 1$, Canadian J. Math. **30** (1978), no. 2, 321–331.

[98] R. Mathon, *The systems of linked* 2-$(16, 6, 2)$ *designs*, Ars Combin. **11** (1981), 131–148.

[99] R. Mathon, A. Rosa, 2-(v, k, λ) *designs of small order*, u: *The Handbook of Combinatorial Designs, Second Edition* (urednici C.J. Colbourn i J.H. Dinitz), CRC Press, 2007., str. 25–58.

[100] B. D. McKay, E. Spence, *Classification of regular two-graphs on* 36 *and* 38 *vertices*, Australas. J. Combin. **24** (2001), 293–300.

[101] C. D. Meyer, *Matrix analysis and applied linear algebra. Second edition*, Society for Industrial and Applied Mathematics (SIAM), 2023.

[102] R. Noda, *On homogeneous systems of linked symmetric designs*, Math. Z. **138** (1974), 15–20.

[103] P. Ó Catháin, R. Egan, P. Browne, *Equivalence of quadratic forms*, srpanj 2023. Materijal s radionice "Workshop in Linear Algebra" (Rijeka, 8.7.2023.).

[104] R. E. A. C. Paley, *On orthogonal matrices*, Journal of Mathematics and Physics **12** (1933), 311–320.

[105] C. Peterson, *On tight* 6*-designs*, Osaka J. Math. **14** (1977), 417–435.

[106] D. Raghavarao, *Some aspects of weighing designs*, Ann. Math. Statist. **31** (1960), 878–884.

[107] D. Ray-Chaudhuri, R. Wilson, *Generalisation of Fisher's inequality to* t*-designs*, Notices Amer. Math. Soc. **18** (1971), 805.

[108] D. Ray-Chaudhuri, R. Wilson, *On* t*-designs*, Osaka J. Math. **12** (1975), 737–744.

[109] L. Relić, *Asocijacijske sheme*, diplomski rad, Sveučilište u Zagrebu, 2022. `https://urn.nsk.hr/urn:nbn:hr:217:373687`

[110] H. Sachs, *Über selbstkomplementäre Graphen*, Publ. Math. Debrecen **9** (1962), 270–288.

[111] L. L. Scott, *A condition on Higman's parameters*, Notices Amer. Math. Soc. **20** (1973), A-97 (701-20-45).

[112] L. L. Scott, *Some properties of character products*, J. Algebra **45** (1977), no. 2, 259–265.

[113] M. S. Shrikhande, *Quasi-symmetric designs*, u: *The Handbook of Combinatorial Designs, Second Edition* (ur. C. J. Colbourn, J. H. Dinitz), CRC Press, 2007, str. 578–582.

[114] M. S. Shrikhande, S. S. Sane, *Quasi-symmetric designs*, Cambridge University Press, 1991.

[115] S. S. Shrikhande, *The uniqueness of the L_2 association scheme*, Ann. Math. Statist. **30** (1959), 781–798.

[116] S. S. Shrikhande, Bhagwandas, *Duals of incomplete block designs*, J. Indian Statist. Assoc. **3** (1965), 30–37.

[117] N. J. A. Sloane, *An introduction to association schemes and coding theory*, u: *Theory and application of special functions* (ur. R. A. Askey), Academic Press, Inc., 1975., str. 225–260.

[118] L. H. Soicher, *DESIGN, The Design Package for GAP*, verzija 1.7, 2019. `https://gap-packages.github.io/design`

[119] E. Spence, *Strongly regular graphs on at most* 64 *vertices*, `http://www.maths.gla.ac.uk/~es/srgraphs.php` (pristupljeno 10.2.2024.).

[120] D. R. Stinson, *Combinatorial designs: constructions and analysis*, Springer-Verlag, 2004.

[121] J. Šiftar, V. Krčadinac, *Konačne geometrije*, skripta, Sveučilište u Zagrebu, 2013. `https://web.math.pmf.unizg.hr/~krcko/nastava/kg-skripta.pdf`

[122] K. Škufca, *Distancijsko regularni grafovi*, diplomski rad, Sveučilište u Zagrebu, 2022. `https://urn.nsk.hr/urn:nbn:hr:217:810981`

[123] L. Teirlinck, *Nontrivial t-designs without repeated blocks exist for all t*, Discrete Math. **65** (1987), no. 3, 301–311.

[124] P. Terwilliger, *Algebraic combinatorics: association schemes*, University of Wisconsin, 2023. https://people.math.wisc.edu/~pmterwil/Htmlfiles/asAll.pdf

[125] V. D. Tonchev, *Quasi-symmetric* 2-$(31, 7, 7)$ *designs and a revision of Hamada's conjecture*, J. Combin. Theory Ser. A **42** (1986), no. 1, 104–110.

[126] E. R. van Dam, *Graphs with few eigenvalues. An interplay between combinatorics and algebra*, doktorska disertacija, Tilburg University, 1996. https://cage.ugent.be/geometry/Theses/30/evandam.pdf

[127] E. R. van Dam, *Three-class association schemes*, J. Algebraic Combin. **10** (1999), no. 1, 69–107.

[128] J. H. van Lint, J. J. Seidel, *Equilateral point sets in elliptic geometry*, Nederl. Akad. Wetensch. Proc. Ser. A **69** Indag. Math. **28** (1966), 335–348.

[129] R. Vlahović Kruc, *Neki rezultati o kvazisimetričnim dizajnima s iznimnim parametrima*, disertacija, Sveučilište u Zagrebu, 2019. https://urn.nsk.hr/urn:nbn:hr:217:446211

[130] B. Weisfeiler, A. A. Leman, *Reduction of a graph to a canonical form and an algebra which appears in this process* (na ruskom), Scientific-Technological Investigations **2** (1968), 12–16.

[131] E. W. Weisstein, *Dodecahedral graph*, From MathWorld – A Wolfram Web Resource, https://mathworld.wolfram.com/DodecahedralGraph.html (pristupljeno 9.11.2023.).

[132] E. W. Weisstein, *Heawood graph*, From MathWorld – A Wolfram Web Resource, https://mathworld.wolfram.com/HeawoodGraph.html (pristupljeno 9.11.2023.).

[133] E. W. Weisstein, *Icosahedral graph*, From MathWorld – A Wolfram Web Resource, https://mathworld.wolfram.com/IcosahedralGraph.html (pristupljeno 9.11.2023.).

[134] E. W. Weisstein, *Shrikhande graph*, From MathWorld – A Wolfram Web Resource, https://mathworld.wolfram.com/ShrikhandeGraph.html (pristupljeno 2.11.2023.).

[135] Wikipedia, *Chang graphs*, https://en.wikipedia.org/wiki/Chang_graphs (pristupljeno 10.2.2024.).

[136] Wikipedia, *Hypercube graph*, https://en.wikipedia.org/wiki/Hypercube_graph (pristupljeno 2.11.2023.).

[137] R. M. Wilson, *Incidence matrices of t-designs*, Linear Algebra Appl. **46** (1982), 73–82.

[138] R. M. Wilson, *Inequalities for t-designs*, J. Combin. Theory Ser. A **34** (1983), 313–324.

[139] E. Witt, *Die* 5*-fach transitiven Gruppen von Mathieu*, Abh. Math. Semin. Univ. Hambg. **12** (1938), 256–264.

[140] E. Witt, *Über Steinersche Systeme*, Abh. Math. Semin. Univ. Hambg. **12** (1938), 265–275.

[141] F. Yates, *Incomplete randomized blocks*, Ann. Eugen. **7(2)** (1936), 121–140. https://doi.org/10.1111/j.1469-1809.1936.tb02134.x

[142] P.-H. Zieschang, *Theory of association schemes*, Springer-Verlag, 2005.