Johnsonova shema

Šupe, Katarina

Sveučilište u Zagrebu
Prirodoslovno-matematički fakultet
Matematički odsjek

Katarina Šupe

Johnsonova shema

Diplomski rad

Voditelj rada:
izv. prof. dr. sc. Vedran Krčadinac

Zagreb, rujan 2021.

Ovaj diplomski rad obranjen je dana ____________________ pred ispitnim povjerenstvom u sastavu:

1. ______________________________ , predsjednik
2. ______________________________ , član
3. ______________________________ , član

Povjerenstvo je rad ocijenilo ocjenom ______________________ .

Potpisi članova povjerenstva:

1. ______________________________
2. ______________________________
3. ______________________________

Sadržaj

1 Uvod

U ovom radu ćemo najprije definirati Johnsonove grafove $J(v,k,i)$, $i = 0,\ldots,k$ i ilustrirati ih pomoću primjera. Temeljito ćemo proučiti odgovarajuće matrice susjedstva $A_0,\ldots,A_k$. Dokazat ćemo da te matrice imaju nekoliko zanimljivih svojstava: simetrične su, u sumi daju matricu ispunjenu jedinicama te je A_0 jedinična matrica. Cilj poglavlja je pokazati da je vektorski prostor $\mathcal{A}$, razapet matricama $A_0,\ldots,A_k$, komutativna algebra. U tu svrhu ćemo definirati novu familiju matrica $W_{t,k}$, pomoću koje uvodimo matrice $C_0,\ldots,C_k$, takve da je $C_i = W_{i,k}^{\tau} \cdot W_{i,k}$. One također razapinju vektorski prostor $\mathcal{A}$ te će odigrati glavnu ulogu u dokazivanju da je $\mathcal{A}$ komutativna algebra.

U trećem poglavlju ćemo definirati t-(v,k,λ_t) dizajne. Također, vidjet ćemo da dizajn ima snagu barem t ako i samo ako njegov karakteristični vektor zadovoljava jednadžbu $W_{t,k} \cdot f = \lambda_t \mathbf{1}$, za neku konstantu λ_t. Dakle, povezat ćemo matrice iz prethodnog poglavlja s dizajnima. Cilj poglavlja je dokazati Ray-Chaudhurijev i Wilsonov teorem koji govori o donjoj granici kardinaliteta skupa blokova t-dizajna. Da bismo ga dokazali, potrebno je uvesti matrice $W_i(\mathcal{B})$, koje sadrže redom sve stupce matrice $W_{i,k}$ koji odgovaraju blokovima dizajna te dokazati linearnu nezavisnost redaka tih matrica. Za to će biti potrebno definirati komplement dizajna te familiju matrica $\overline{W}_{t,k}$. Kada dokažemo bitna svojstva tih matrica, moći ćemo dokazati Ray-Chaudhurijev i Wilsonov teorem iz kojeg će slijediti Fishereova nejednakost.

U četvrtom poglavlju ćemo se napokon upoznati s pojmom Johnsonove sheme. Osim što ćemo vidjeti da je Johnsonova shema primjer asocijacijske sheme, sve što smo prethodno dokazali za matrice susjedstva Johnsonovih grafova $J(v,k,i)$, poslužit će za bolje razumijevanje naizgled komplicirane definicije asocijacijske sheme. Definirat ćemo Bose-Mesnerovu algebru sheme, dokazati da je zatvorena na Schurov produkt i zaključiti da je algebra $\mathcal{A}$, iz prvog poglavlja, zapravo Bose-Mesnerova algebra Johnsonove sheme. Za asocijacijske sheme će još biti bitno spomenuti svojstvene i dualne svojstvene vrijednosti sheme te presječne brojeve i Kreinove parametre.

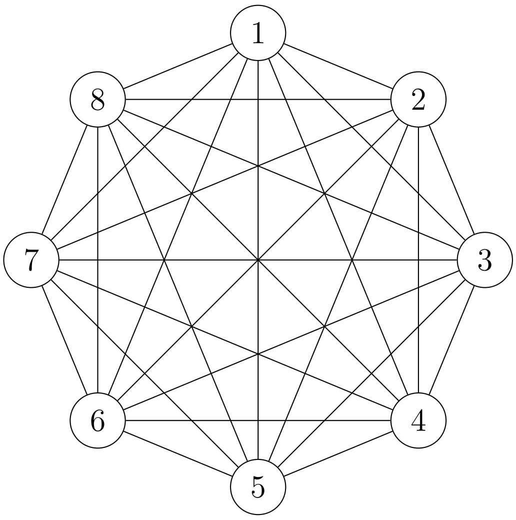
U zadnjem poglavlju bavit ćemo se parametrima Johnsonove sheme, kao konkretnim primjerom parametara neke asocijacijske sheme. Dokazat ćemo bitan rezultat o svojstvenim potprostorima Johnsonove sheme koji će povlačiti glavni rezultat četvrtog poglavlja – Delsarteov teorem koji povezuje t-(v,k,λ_t) dizajne iz trećeg poglavlja sa svojstvenim potprostorima Johnsonove sheme.

2 Johnsonovi grafovi

Da bismo definirali Johnsonove grafove potrebno je najprije prisjetiti se nekih osnovnih pojmova.

Definicija 2.1. Graf *je uređen par* $G = (V, E)$*, pri čemu je* V *konačan skup vrhova, a* E *skup jednočlanih ili dvočlanih podskupova od* V *koje zovemo bridovima. Jednočlane bridove zovemo* petljama. *Kažemo da su vrhovi* $u, v \in V$ susjedni *ako postoji brid* $e = \{u, v\} \in E$*. Kažemo da je vrh* v incidentan *s bridom* e *ukoliko je* $e = \{v\}$ *ili* $e = \{u, v\}$*, za neki vrh* $u \in V$*.*

Definicija 2.2. *Neka je* $G = (V, E)$ *graf,* $|V| = n \in \mathbb{N}$ *te* $E = \binom{V}{2}$ *skup svih dvočlanih podskupova od* V*. Tada kažemo da je graf* G potpuni graf *te ga označavamo s* K_n*.*

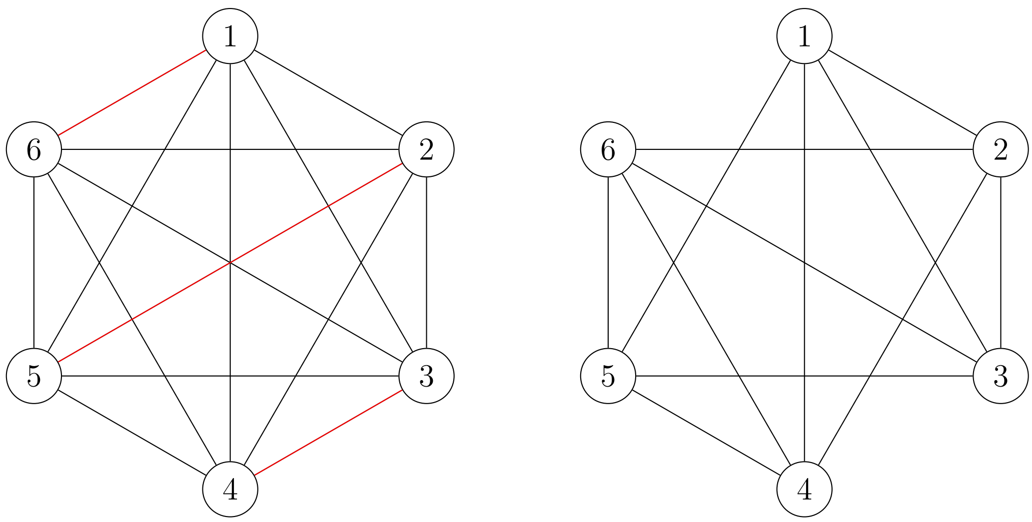


Slika 1: Potpuni graf K_8

Definicija 2.3. *Neka je* V *skup od* v *elemenata i* $\Omega = \binom{V}{k}$ *familija svih* k*-članih podskupova od* V*.* Generalizirani Johnsonov graf $J(v, k, i)$ *ima* Ω *kao skup vrhova, a dva vrha su susjedna ako se sijeku u* $k - i$ *elemenata.*

Graf $J(v, k, 1)$ označavat ćemo s $J(v, k)$ te ga zvati Johnsonovim grafom. Dakle, dva vrha su susjedna u Johnsonovu grafu, ako se sijeku u $k - 1$ elemenata. Očito je onda $J(n, 1)$ potpuni graf K_n.

Primjer 2.4. *Neka je* $V = \{a, b, c, d\}$ *zadani skup. Tada je* $\Omega = \{\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}\}$ *familija svih dvočlanih podskupova od* V*, tj.* Ω *je skup vrhova Johnsonova grafa* $J(4, 2)$*. Susjedni vrhovi su oni koji imaju točno jedan zajednički element. Označimo šest elemenata skupa* Ω *redom brojevima od* 1 *do* 6*. Pogledajmo zatim sliku 2. Lijevo, na slici 2a imamo nacrtan potpuni graf* K_6*. Iz definicije 2.2 znamo da su u tom grafu svi vrhovi susjedni. Pogledajmo stoga koji vrhovi iz potpunog grafa nisu susjedni u Johnsonovom grafu* $J(4, 2)$*. Takvi bridovi označeni su crvenom bojom. Desno, na slici 2b, ti bridovi su uklonjeni te je ostao Johnsonov graf* $J(4, 2)$*.*



(a) Potpuni graf K_6 (b) Johnsonov graf $J(4, 2)$

Slika 2: Johnsonov graf kao razapinjući podgraf potpunog grafa.

Definicija 2.5. Podgraf *grafa* $G = (V, E)$ *je graf* $G' = (V', E')$*, pri čemu je* $V' \subseteq V$ *i* $E' \subseteq E$*.* Razapinjući podgraf *je podgraf oblika* $G' = (V, E')$*.*

Dakle, u razapinjućem podgrafu nekog grafa $G = (V, E)$ skup vrhova je jednak skupu V, dok je skup bridova neki podskup od E. Možemo zaključiti da je Johnsonov graf $J(4, 2)$ na slici 2b razapinjući podgraf grafa na slici 2a.

Definicija 2.6. *Grafovi* $G_1 = (V_1, E_1)$ *i* $G_2 = (V_2, E_2)$ *su* izomorfni *ukoliko postoji bijekcija* $\Theta \colon V_1 \to V_2$*, takva da za sve vrhove* u *i* v *iz* V_1 *vrijedi da su* u *i* v *susjedni u* G_1 *ako i samo ako su vrhovi* $\Theta(u)$ *i* $\Theta(v)$ *susjedni u* G_2*.*

Grafovi $J(v, k)$ i $J(v, v-k)$ su izomorfni. Izomorfizam je preslikavanje $\Theta \colon \binom{V}{k} \to \binom{V}{v-k}$ koje k-članom podskupu $\alpha \subseteq V$ pridružuje njegov komplement, odnosno $\Theta(\alpha) = V \setminus \alpha$. Dva vrha iz $J(v, k)$, tj. podskupa $\alpha, \beta \subseteq V$, $|\alpha| = |\beta| = k$, su susjedna ako i samo ako je $|\alpha \cap \beta| = k - 1$. To je ekvivalentno s $|(V \setminus \alpha) \cap (V \setminus \beta)| = v - k - 1$, odnosno da su slike $\Theta(\alpha)$ i $\Theta(\beta)$ susjedne u $J(v, v-k)$. Zbog njihove izomorfnosti, za Johnsonov graf $J(v,k)$, često ćemo pretpostavljati da je $v \geq 2k$.

Definicija 2.7. *Neka je $G = (V, E)$ te $V = \{v_1, \ldots, v_n\}$, $n \in \mathbb{N}$.* Matrica susjedstva *grafa G je matrica $A = [a_{ij}]_{n \times n}$, takva da je*

$$a_{i,j} = \begin{cases} 1, & \textit{ako je } \{v_i, v_j\} \in E \\ 0, & \textit{inače.} \end{cases}$$

Neka je I jedinična matrica, a J kvadratna matrica reda $n = \binom{v}{k}$ ispunjena jedinicama, dimenzija jednakih dimenzijama matrica $A_0, A_1, \ldots, A_k$, koje su redom matrice susjedstva grafova $J(v,k,i)$. One zadovoljavaju sljedeće uvjete:

- $A_i^\tau = A_i$, $i = 0, \ldots, k$.

  Matrice A_i su simetrične, jer je relacija susjedstva u Johnsonovu grafu simetrična, tj. ako je vrh α susjedan vrhu β, tada je očito i vrh β susjedan vrhu α i obratno. Dakle, vrijedi $A_i^\tau = A_i$ za svaki $i = 0, \ldots, k$.

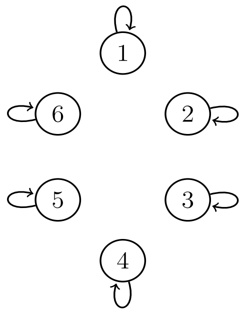
- $A_0 = I$.

  Graf $J(v,k,0)$ je Johnsonov graf u kojem su dva vrha susjedna ako se sijeku u k elemenata. Kako se skup vrhova Ω takvog grafa sastoji od k-članih podskupova nekog v-članog skupa, tada se samo dva jednaka podskupa od Ω mogu sjeći u točno k elemenata. Stoga zaključujemo da su bridovi grafa $J(v,k,0)$ isključivo petlje na svakom vrhu tog grafa, tj. matrica susjedstva A_0 je očito jedinična matrica I, za svaki v i k.

- $\sum_{i=0}^{k} A_i = J$.

  U matrici susjedstva A_i na nekom mjestu se nalazi jedinica, ako pripadni vrhovi imaju $k - i$ zajedničkih elemenata. Dakle, matrice A_i su očito različite za svaki i. Primijetimo da unija bridova grafova $J(v,k,i)$, za $i \neq 0$, čini skup bridova potpunog grafa K_n. Iz toga slijedi da je zbroj matrica susjedstva $A_1, \ldots, A_k$ jednak matrici susjedstva potpunog grafa K_n, koja je $n \times n$ matrica s nulama na dijagonali i jedinicama na preostalim mjestima, jer graf K_n ne sadrži petlje. Pribrojimo li toj matrici matricu A_0, dobit ćemo matricu J. Stoga, $\sum_{i=0}^{k} A_i = J$.

Primjer 2.8. *Provjerimo zadovoljavaju li matrice susjedstva A_0, A_1 i A_2 grafova $J(4,2,0)$, $J(4,2,1)$ te $J(4,2,2)$ navedene uvjete. Ukoliko promatramo Johnsonov graf $J(4,2,0)$ na slici 3, možemo primijetiti da su svi njegovi bridovi petlje. Tada*



$$A_0 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

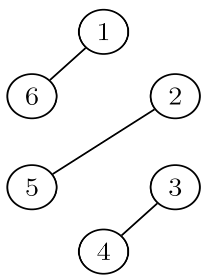
Slika 3: Johnsonov graf $J(4,2,0)$ s pripadnom matricom susjedstva A_0.

je očito $A_0 = I_6$, odnosno jedinična 6×6 matrica. Znamo da je jedinična matrica simetrična, pa vrijedi $A_0^\tau = A_0$.

Johnsonov graf $J(4,2,1)$ je graf $J(4,2)$ na slici 2b. Pripadna matrica susjedstva je

$$A_1 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Matrica A_1 je očito simetrična, tj. $A_1^\tau = A_1$. Na kraju, promatramo A_2, matricu susjedstva Johnsonovog grafa $J(4,2,2)$ na slici 4.



$$A_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Slika 4: Johnsonov graf $J(4,2,2)$ s pripadnom matricom susjedstva A_2.

A_2 je također simetrična matrica, odnosno $A_2^\tau = A_2$. Uočimo još da je suma matrica A_0, A_1 i A_2 matrica ispunjena jedinicama, odnosno matrica J.

Neka je $\mathcal{A}$ vektorski prostor razapet matricama $A_0, A_1, \ldots, A_k$ nad poljem $\mathbb{R}$, tj. $\mathcal{A} = \langle A_0, \ldots, A_k \rangle$. Pokazat ćemo da je vektorski prostor $\mathcal{A}$ zatvoren na matrično množenje, tj. da je matrična algebra. U tu svrhu ćemo najprije definirati važnu familiju matrica.

Definicija 2.9. *Neka su t, k i v fiksni te neka je V skup od v elemenata. Proizvoljno poredajmo t-člane i k-člane podskupove od V. Tada je $W_{t,k}(v)$ $\binom{v}{t} \times \binom{v}{k}$ matrica ispunjena nulama i jedinicama. Na mjestu (i, j) u matrici $W_{t,k}(v)$ se nalazi 1, ako je i-ti t-člani podskup od V sadržan u j-tom k-članom podskupu od V. Inače se na mjestu (i, j) u matrici $W_{t,k}(v)$ nalazi 0.*

Obično će iz konteksta biti jasno na koji v-člani skup V se matrica $W_{t,k}(v)$ odnosi pa ćemo je označavati s $W_{t,k}$. Primijetimo da je $W_{t,k}$ matrica s $\binom{v-t}{k-t}$ jedinica u svakom retku te $\binom{k}{t}$ jedinica u svakom stupcu. Fiksni k-člani podskup od V sadrži i-ti t-člani podskup od V ako je taj t-člani skup njegov podskup. Znamo da je broj t-članih podskupova k-članog skupa jednak $\binom{k}{t}$, stoga slijedi da matrica $W_{t,k}$ ima $\binom{k}{t}$ jedinica u svakom stupcu. Neki k-člani podskup od V možemo kreirati tako da prvo odaberemo t-člani podskup od V koji zatim nadopunimo do k-članog skupa. Za fiksni t-člani podskup od V to možemo napraviti na $\binom{v-t}{k-t}$ načina pa slijedi da matrica $W_{t,k}$ ima $\binom{v-t}{k-t}$ jedinica u svakom retku.

Primjer 2.10. *Prisjetimo se Johnsonovih grafova i njihovih matrica susjedstva iz primjera 2.8. Dakle, $v = 4$, $k = 2$ i neka je $t = 1$ te $V = \{1, 2, 3, 4\}$ skup od v elemenata. Poredajmo t-člane i k-člane podskopove od V na sljedeći način:*

$$\Omega_1 = \{\{1\}, \{2\}, \{3\}, \{4\}\}$$

i

$$\Omega_2 = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}.$$

Najprije pogledajmo kako će izgledati matrica $W_{1,2}$:

$$W_{1,2} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Na mjestu $(1, 1)$ u matrici $W_{1,2}$ nalazi se 1, jer vrijedi $\{1\} \subseteq \{1, 2\}$. Preciznije, prvi t-člani podskup od V, tj. prvi element skupa Ω_1, sadržan je u prvom k-članom podskupu od V, odnosno u prvom elementu skupa Ω_2. Na mjestu $(3, 3)$ u matrici $W_{1,2}$ nalazi se 0, jer $\{3\} \nsubseteq \{1, 4\}$. Analogno za preostale elemente matrice $W_{1,2}$. Primijetimo da matrica $W_{1,2}$ zaista ima $\binom{v-t}{k-t} = \binom{4-1}{2-1} = \binom{3}{1} = 3$ jedinica u svakom retku te $\binom{k}{t} = \binom{2}{1} = 2$ jedinica u svakom stupcu.

Sada definiramo matrice $C_0, \cdots, C_k$ na sljedeći način:

$$C_i = W_{i,k}^{\tau} \cdot W_{i,k}. \tag{1}$$

Primjer 2.11. *Kada transponiramo matricu $W_{1,2}$ iz primjera 2.10 dobijemo*

$$W_{1,2}^{\tau} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

Sada iz jednakosti (1) *zaključujemo da je*

$$C_1 = W_{1,2}^{\tau} \cdot W_{1,2} = \begin{bmatrix} 2 & 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 1 & 1 & 0 & 1 \\ 1 & 1 & 2 & 0 & 1 & 1 \\ 1 & 1 & 0 & 2 & 1 & 1 \\ 1 & 0 & 1 & 1 & 2 & 1 \\ 0 & 1 & 1 & 1 & 1 & 2 \end{bmatrix}.$$

Dijagonala matrice C_1 ispunjena je dvojkama, jer je svaki dvočlani skup iz Ω_2 nadskup dva jednočlana skupa iz Ω_1. Primijetimo da je $C_1 = 2A_0 + A_1$, pri čemu su A_0 i A_1 matrice susjedstva Johnsonovih grafova iz primjera 2.8.

Propozicija 2.12. *Za sve $i \in \{0, \ldots, k\}$ vrijedi sljedeća jednakost*

$$C_i = \sum_{r \geq i} \binom{r}{i} A_{k-r}. \tag{2}$$

Dokaz. Neka su $\alpha, \beta \in \Omega = \binom{V}{k}$. Promotrimo mjesto (α, β) u matrici $C_i = W_{i,k}^{\tau} \cdot W_{i,k}$. Po definiciji množenja matrica, to je suma po svim $\gamma \in \binom{V}{i}$ produkta $(W_{i,k}^{\tau})_{\alpha,\gamma} \cdot (W_{i,k})_{\gamma,\beta}$. Produkt je 1 ako je $\gamma \subseteq \alpha$ i $\gamma \subseteq \beta$, tj. $\gamma \subseteq \alpha \cap \beta$, a inače je 0. Dakle, na mjestu (α, β) u matrici C_i je broj i-članih podskupova od $\alpha \cap \beta$, tj. $(C_i)_{\alpha,\beta} = \binom{|\alpha \cap \beta|}{i}$. S druge strane, element na mjestu (α, β) u matrici A_{k-r} je 1 ako je $|\alpha \cap \beta| = r$, a inače je 0. Zato je i $\left(\sum_{r \geq i} \binom{r}{i} A_{k-r}\right)_{\alpha,\beta} = \sum_{r \geq i} \binom{r}{i} (A_{k-r})_{\alpha,\beta} = \binom{|\alpha \cap \beta|}{i}$. Time smo dokazali da je $C_i = \sum_{r \geq i} \binom{r}{i} A_{k-r}$. □

Lema 2.13. *Vrijedi*

$$\binom{n}{j}\binom{j}{k} = \binom{n}{k}\binom{n-k}{j-k}. \tag{3}$$

Dokaz. Jednakost ćemo dokazati kombinatornim argumentom. Recimo da imamo n kuglica u nekoj posudi. Na lijevoj strani jednakosti najprije biramo j kuglica od n na $\binom{n}{j}$ načina. Nakon toga od tih j kuglica biramo k kuglica koje stavljamo u ladicu, a preostale u kutiju. Dakle, u kutiji je ukupno $j-k$ kuglica. Na desnoj strani jednakosti biramo kuglice tako da prvo odaberemo njih k koje stavljamo u ladicu te zatim od preostalih $n-k$ kuglica biramo $j-k$ kuglica koje idu u kutiju. □

Teorem 2.14 (Relacija ortogonalnosti za binomne koeficijente)**.** *Vrijedi sljedeća relacija:*

$$\delta_{nk} = \sum_{j=k}^{n} (-1)^{j-k} \binom{n}{j} \binom{j}{k}. \tag{4}$$

Dokaz. δ_{nk} je Kroneckerov simbol, koji je definiran za svaki par prirodnih brojeva (n,k) na sljedeći način:

$$\delta_{nk} = \begin{cases} 1, & \text{ako je } n = k \\ 0, & \text{ako je } n \neq k. \end{cases}$$

Kada raspišemo desnu stranu jednakosti (4) dobijemo:

$$\begin{aligned}
\sum_{j=k}^{n} (-1)^{j-k} \binom{n}{j} \binom{j}{k} &= \sum_{j=k}^{n} (-1)^{j-k} \binom{n}{k} \binom{n-k}{j-k} \\
&= \binom{n}{k} \sum_{j=0}^{n-k} (-1)^{j} \binom{n-k}{j} \\
&= \binom{n}{k} \sum_{j=0}^{n-k} \binom{n-k}{j} 1^{n-k-j} (-1)^{j} \\
&= \binom{n}{k} (1-1)^{n-k} \\
&= \delta_{nk}.
\end{aligned}$$

U prvoj jednakosti koristili smo identitet (3), dok smo u predzadnjoj jednakosti koristili binomni teorem. □

Teorem 2.15 (Binomna inverzija)**.** *Za svake dvije funkcije $f, g\colon \{0,1,\ldots,n\} \to M_m$ ekvivalentno je*

1. $g(i) = \sum_{j=0}^{i} \binom{i}{j} f(j)$, $\forall i \in \{0,1,\ldots,n\}$,

2. $f(i) = \sum_{j=0}^{i} (-1)^{i-j} \binom{i}{j} g(j)$, $\forall i \in \{0,1,\ldots,n\}$.

Dokaz. Pokažimo da je $\sum_{j=0}^{i}(-1)^{i-j}\binom{i}{j}g(j)$ uistinu $f(i)$:

$$\begin{aligned}
\sum_{j=0}^{i}(-1)^{i-j}\binom{i}{j}g(j) &= \sum_{j=0}^{i}(-1)^{i-j}\binom{i}{j}\sum_{k=0}^{j}\binom{j}{k}f(k) \\
&= \sum_{j=0}^{i}\sum_{k=0}^{j}(-1)^{i-j}\binom{i}{j}\binom{j}{k}f(k) \\
&= \sum_{k=0}^{j}\sum_{j=0}^{i}(-1)^{i-j}\binom{i}{j}\binom{j}{k}f(k) \\
&= \sum_{k=0}^{j}\sum_{j=k}^{i}(-1)^{i-j}\binom{i}{j}\binom{j}{k}f(k) \\
&= \sum_{k=0}^{i}\sum_{j=k}^{i}(-1)^{i-j}\binom{i}{j}\binom{j}{k}f(k) \\
&= \sum_{k=0}^{i}f(k)\sum_{j=k}^{i}(-1)^{i-j}\binom{i}{j}\binom{j}{k} \\
&= \sum_{k=0}^{i}f(k)\delta_{ik} \\
&= f(i).
\end{aligned}$$

U prvoj jednakosti koristili smo formulu 1. Zatim smo unutar druge sumacije ubacili sve što ne ovisi o k, nakon čega smo zamijenili poredak sumacije. Drugu sumaciju po j smo pomakli da kreće od k, jer za $j < k$ je $\binom{j}{k} = 0$. Nakon toga smo prvu sumaciju po k proširili do i, što ne utječe na ukupnu sumu, jer je $\binom{j}{k} = 0$, za $k > j$. U šestoj jednakosti smo izlučili $f(k)$ ispred sume po j, a zatim smo primijenili relaciju ortogonalnosti (4). Na sličan način se dokazuje da formula 1 implicira formulu 2. □

Upravo dokazani teorem je tvrdnja poznata kao *binomna inverzija.* Funkciju g nazivamo *binomnom transformacijom* funkcije f.

Korolar 2.16. *Za sve $i \in \{0, \dots, k\}$ vrijedi sljedeća jednakost*

$$A_{k-i} = \sum_{r \geq i}(-1)^{r-i}\binom{r}{i}C_r. \tag{5}$$

Dokaz. Slijedi iz teorema 2.15, jer je binomna inverzija formule (2) formula (5). □

Dakle, matrice C_i također razapinju vektorski prostor $\mathcal{A}$, tj. $\mathcal{A} = \langle C_0, C_1, \ldots, C_k \rangle$. Dokažimo prvo neke rezultate koji će nam, zajedno s matricama C_i, pomoći pri dokazivanju da je $\mathcal{A}$ komutativna algebra.

Propozicija 2.17 (Vandermondeova konvolucija)**.** *Vrijedi*

$$\sum_{k=0}^{r} \binom{m}{k} \binom{n}{r-k} = \binom{m+n}{r}. \tag{6}$$

Dokaz. Kombinatornim argumentom možemo jednostavno dokazati gornju jednakost. Interpretirajmo najprije desnu stranu jednakosti. Promotrimo skup koji ima $m+n$ obojanih elemenata. Neka je m elemenata obojano crvenom, a n elemenata plavom bojom. Recimo da želimo odabrati r elemenata iz tog skupa. To možemo učiniti na $\binom{m+n}{r}$ načina, jer nam nije važno koje elemente odabiremo, već nam je dovoljno da ih je točno r. S druge strane, biramo elemente $(m+n)$-članog skupa tako da najprije odaberemo nekoliko crvenih elemenata i zatim preostale plave elemente. Stoga prvo odabiremo k crvenih elemenata na $\binom{m}{k}$ načina i onda od n plavih elemenata biramo preostalih $r-k$ elemenata na $\binom{n}{r-k}$ načina, za svaki $k = 0, \ldots, r$. Takav odabir možemo napraviti na ukupno $\binom{m}{0}\binom{n}{r} + \binom{m}{1}\binom{n}{r-1} + \cdots + \binom{m}{r-1}\binom{n}{1} + \binom{m}{r}\binom{n}{0}$ načina, što je lijeva strana jednakosti (6). $\square$

Propozicija 2.18. *Vrijedi*

$$W_{s,k} W_{t,k}^{\tau} = \sum_{i=0}^{t} \binom{v-s-t}{v-k-i} W_{i,s}^{\tau} W_{i,t}. \tag{7}$$

Dokaz. Neka je α s-člani podskup i β t-člani podskup v-članog skupa V. Na mjestu (i,j) u matrici $W_{s,k}$ se nalazi 1, ako je i-ti s-člani podskup od V sadržan u j-tom k-članom podskupu od V. Inače se na mjestu (i,j) u matrici $W_{s,k}$ nalazi 0. Na mjestu (i,j) u matrici $W_{t,k}$ se nalazi 1, ako je i-ti t-člani podskup od V sadržan u j-tom k-članom podskupu od V. Inače se na mjestu (i,j) u matrici $W_{t,k}$ nalazi 0. Kada transponiramo matricu $W_{t,k}$ te je slijeva pomnožimo s matricom $W_{s,k}$, možemo primijetiti da se u dobivenoj matrici $W_{s,k}W_{t,k}^{\tau}$ na mjestu (α, β) nalazi broj k-članih podskupova od V koji su nadskupovi skupova α i β. Takav k-člani skup možemo odabrati tako da prvo odaberemo sve elemente koji se nalaze u skupovima α i β, a njih je ukupno $|\alpha \cup \beta|$, te zatim od preostalih $v - |\alpha \cup \beta|$ elemenata biramo $k - |\alpha \cup \beta|$ elemenata na $\binom{v-|\alpha\cup\beta|}{k-|\alpha\cup\beta|}$ načina. Dakle, na mjestu (α, β) u matrici $W_{s,k}W_{t,k}^{\tau}$ nalazi se

$$\binom{v - |\alpha \cup \beta|}{k - |\alpha \cup \beta|}.$$

Analogno, na mjestu (α, β) u matrici $W_{i,s}^{\tau} W_{i,t}$ nalazi se broj i-članih podskupova v-članog skupa koji se nalaze u presjeku skupova α i β. Dakle od $|\alpha \cap \beta|$ elemenata možemo odabrati njih i na $\binom{|\alpha\cap\beta|}{i}$ načina pa se na mjestu (α, β) u matrici $W_{i,s}^{\tau} W_{i,t}$ nalazi

$$\binom{|\alpha \cap \beta|}{i}.$$

Kada promatramo desnu stranu jednakosti (7), sada vidimo da na mjestu (α, β) imamo

$$\sum_{i=0}^{t} \binom{v-s-t}{v-k-i} \binom{|\alpha \cap \beta|}{i}.$$

Raspišimo dobivenu sumu, koristeći se Vandermondeovom konvolucijom u prvom koraku, tako da dobijemo vrijednost s lijeve strane jednakosti:

$$\begin{aligned}
\sum_{i=0}^{t} \binom{v-s-t}{v-k-i} \binom{|\alpha \cap \beta|}{i} &= \binom{v-s-t+|\alpha \cap \beta|}{v-k} \\
&= \binom{v-(s+t-|\alpha \cap \beta|)}{v-k} \\
&= \binom{v-(|\alpha|+|\beta|-|\alpha \cap \beta|}{v-k} \\
&= \binom{v-|\alpha \cup \beta|}{v-k} \\
&= \binom{v-|\alpha \cup \beta|}{v-|\alpha \cup \beta|-(v-k)} \\
&= \binom{v-|\alpha \cup \beta|}{v-|\alpha \cup \beta|-v+k} \\
&= \binom{v-|\alpha \cup \beta|}{k-|\alpha \cup \beta|}.
\end{aligned}$$

Na kraju smo dobili vrijednost na mjestu (α, β) u matrici $W_{s,k} W_{t,k}^{\tau}$, stoga smo pokazali da jednakost (7) vrijedi. $\square$

Propozicija 2.19. *Ako je $s \leq t \leq k$, onda vrijedi*

$$W_{s,t} W_{t,k} = \binom{k-s}{t-s} W_{s,k}. \tag{8}$$

Dokaz. Ako je α s-člani, a β k-člani podskup od V, tada se na mjestu (α, β) u matrici $W_{s,t} W_{t,k}$ nalazi broj t-članih podskupova od V koji sadrže α te se nalaze u β. To je upravo jednako $\binom{k-s}{t-s}$. $\square$

Sada ćemo pokazati da zatvorenost na množenje i komutativnost vrijedi za matrice C_i iz čega će slijediti da je $\mathcal{A}$ komutativna algebra.

Teorem 2.20. *Vrijedi*

$$C_iC_j = \sum_{r\leq i,j} \binom{v-i-j}{v-k-r}\binom{k-r}{i-r}\binom{k-r}{j-r}C_r. \tag{9}$$

Dokaz.

$$\begin{aligned}
C_iC_j &= W_{i,k}^{\tau}W_{i,k}W_{j,k}^{\tau}W_{j,k} \\
&= W_{i,k}^{\tau}\left(\sum_{r\leq i,j}\binom{v-i-j}{v-k-r}W_{r,i}^{\tau}W_{r,j}\right)W_{j,k} \\
&= \sum_{r\leq i,j}\binom{v-i-j}{v-k-r}(W_{i,k}^{\tau}W_{r,i}^{\tau})(W_{r,j}W_{j,k}) \\
&= \sum_{r\leq i,j}\binom{v-i-j}{v-k-r}(W_{r,i}W_{i,k})^{\tau}\binom{k-r}{j-r}W_{r,k} \\
&= \sum_{r\leq i,j}\binom{v-i-j}{v-k-r}\binom{k-r}{i-r}W_{r,k}^{\tau}\binom{k-r}{j-r}W_{r,k} \\
&= \sum_{r\leq i,j}\binom{v-i-j}{v-k-r}\binom{k-r}{i-r}\binom{k-r}{j-r}W_{r,k}^{\tau}W_{r,k} \\
&= \sum_{r\leq i,j}\binom{v-i-j}{v-k-r}\binom{k-r}{i-r}\binom{k-r}{j-r}C_r
\end{aligned}$$

U prvoj i zadnjoj jednakosti koristili smo definiciju matrica C_i, tj. jednakost (1), u drugoj jednakosti primijenili smo propoziciju 2.18, dok smo u četvrtoj i petoj jednakosti koristili propoziciju 2.19. □

Korolar 2.21. $C_iC_j = C_jC_i$*, za bilo koje* i*,* j*.*

Dokaz. Slijedi direktno iz činjenice da je desna strana jednakosti (9) simetrična s obzirom na i i j. □

Teorem 2.22. $\mathcal{A}$ *je komutativna algebra.*

Dokaz. Definirali smo da je $\mathcal{A} = \langle A_0, \dots, A_k \rangle$. Iz propozicije 2.12 i korolara 2.16 slijedi da je $\mathcal{A} = \langle C_0, \dots, C_k \rangle$. Također vrijedi:

$$\begin{aligned}\sum_{i=0}^{k} a_i C_i \cdot \sum_{j=0}^{k} b_j C_j &= \sum_{i=0}^{k} \sum_{j=0}^{k} (a_i C_i \cdot b_j C_j) \\ &= \sum_{i=0}^{k} \sum_{j=0}^{k} (a_i b_j \cdot C_i C_j),\end{aligned}$$

gdje su a_i i b_j neki skalari. U teoremu 2.20 pokazali smo da je $C_i C_j \in \mathcal{A}$, a dobivena sumacija je neka linearna kombinacija matrica C_i pa zaključujemo da je $\mathcal{A}$ zatvorena na množenje. Iskoristimo li komutativnost matrica C_i iz korolara 2.21 i nastavimo raspisivati dobiveni umnožak, dobijemo:

$$\begin{aligned}\sum_{i=0}^{k} a_i C_i \cdot \sum_{j=0}^{k} b_j C_j &= \sum_{i=0}^{k} \sum_{j=0}^{k} (a_i b_j \cdot C_j C_i) \\ &= \sum_{i=0}^{k} \sum_{j=0}^{k} (b_j C_j \cdot a_i C_i) \\ &= \sum_{j=0}^{k} \sum_{i=0}^{k} (b_j C_j \cdot a_i C_i) \\ &= \sum_{j=0}^{k} b_j C_j \cdot \sum_{i=0}^{k} a_i C_i.\end{aligned}$$

Dakle, množenje u $\mathcal{A}$ je komutativno.

□

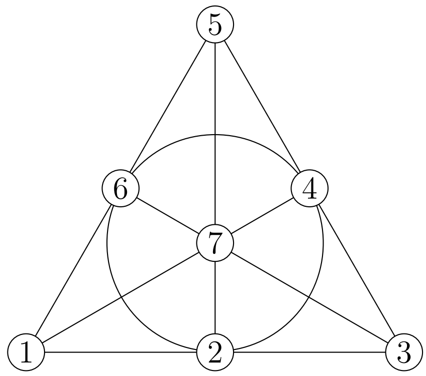
3 Dizajni

Definicija 3.1. *Neka je V neki fiksni v-člani skup te neka je $\mathcal{B}$ familija k-članih podskupova od V. Uređeni par $(V, \mathcal{B})$ nazivamo* dizajn*, gdje je V skup* točaka*, a $\mathcal{B}$ skup* blokova *ili* pravaca*. Nadalje, kažemo da $(V, \mathcal{B})$ ima* snagu *barem t ako postoji konstanta λ_t takva da svaki t-člani podskup od V leži u točno λ_t blokova. Dizajn $(V, \mathcal{B})$ koji ima snagu barem t nazivat ćemo t-(v, k, λ_t) dizajn.*

Primjer 3.2. *Neka je $V = \{1,2,3,4,5,6,7\}$, a $\mathcal{B}$ sljedeći skup tročlanih podskupova od V:*

$$\{\{1,2,3\},\{1,4,7\},\{1,5,6\},\{2,4,6\},\{2,5,7\},\{3,4,5\},\{3,6,7\}\}.$$

Tvrdimo da je tada dizajn $(V,\mathcal{B})$ zapravo 2-$(7,3,1)$ dizajn. Zaista, ukupan broj točaka je broj elemenata skupa V, tj. 7. Također, u svakom bloku leže točno 3 točke. Na kraju, lako se provjeri da su svi dvočlani podskupovi od V sadržani u točno jednom bloku (npr. skup $\{2,5\}$ je sadržan samo u bloku $\{2,5,7\}$), odnosno $t = 2$ i $\lambda_t = 1$. Taj dizajn prikazujemo kao Fanovu ravninu na slici 5, koja je konačna projektivna ravnina reda 2 sa 7 točaka i 7 pravaca (blokova). Na svakom pravcu nalaze se 3 točke, a kroz svaku točku prolaze 3 pravca.



Slika 5: Fanova ravnina.

Primijetimo da je broj točaka jednak broju blokova. Takve dizajne nazivamo *simetričnim dizajnima.*

Sada ćemo vidjeti da su matrice $W_{t,k}$ iz definicije 2.9 važne i za dizajne. Neka je V neki v-člani skup, Ω familija svih k-članih podskupova od V, kao i ranije. Ako je $\mathcal{B}$ neki podskup od Ω, tada ga možemo predstaviti kao vektor stupac f duljine $\binom{v}{k}$. Vektor f na i-tom mjestu ima 1, ako je i-ti element iz Ω sadržan u $\mathcal{B}$, a inače na tom mjestu ima 0. Vektor f zovemo *karakterističnim vektorom* dizajna $(V,\mathcal{B})$. Dizajn ima snagu barem t ako i samo ako njegov karakteristični vektor zadovoljava jednadžbu

$$W_{t,k} \cdot f = \lambda_t \mathbf{1}, \tag{10}$$

za neku konstantu λ_t. Ovdje je $\mathbf{1}$ vektor stupac duljine $\binom{v}{t}$ kojem su svi unosi 1. Dakle, t-(v,k,λ_t) dizajni odgovaraju $\{0,1\}$-rješenjima jednadžbe (10).

Primjer 3.3. *Prisjetimo se primjera 2.10. Pokažimo da je sada jednostavno naći neki* t-(v,k,λ_t) *dizajn. Tražimo* $\{0,1\}$*-rješenja jednadžbe*

$$W_{1,2} \cdot f = \lambda_t \mathbf{1}.$$

gdje je $f = \begin{bmatrix} f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \end{bmatrix}$. *Odatle imamo*

$$\begin{bmatrix} f_1+f_2+f_3 \\ f_1+f_4+f_5 \\ f_2+f_4+f_6 \\ f_3+f_5+f_6 \end{bmatrix} = \lambda_t \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}.$$

Jedno rješenje dane jednadžbe je $f = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$, *za* $\lambda_t = 1$. *Taj* f *određuje dizajn* $(V,\mathcal{B})$, *odnosno* 1-$(4,2,1)$ *dizajn, gdje je* $\mathcal{B}$ *sljedeći skup:*

$$\mathcal{B} = \{\{1,2\},\{3,4\}\}.$$

Uistinu, svaki jednočlani podskup od V *nalazi se u točno jednom bloku. Još jedno rješenje dane jednadžbe za* $\lambda_t = 2$ *je* $f = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}$. *Taj* f *određuje dizajn* $(V,\mathcal{B})$, *odnosno* 1-$(4,2,2)$ *dizajn, gdje je* $\mathcal{B}$ *sljedeći skup:*

$$\{\{1,2\},\{1,4\},\{2,3\},\{3,4\}\}.$$

Primijetimo da se svaki jednočlani podskup od V *nalazi u točno dva bloka.*

Lema 3.4. *Ako je* $s \le t$ *i* $(V,\mathcal{B})$ *neki* t-(v,k,λ_t) *dizajn, tada je* $(V,\mathcal{B})$ *i* s*-dizajn, gdje je*

$$\lambda_s = \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}} \lambda_t.$$

Dokaz. Danu tvrdnju ćemo dokazati na dva načina:

1. Neka je $S \subseteq V$ bilo koji s-člani skup točaka. Označimo sa λ_s broj blokova koji sadrže S. Dvostrukim prebrojavanjem parova u skupu $\{(T,B)\colon S \subseteq T \subseteq B, |T| = t, B \in \mathcal{B}\}$ dobivamo jednakost $\binom{v-s}{t-s} \cdot \lambda_t = \lambda_s \cdot \binom{k-s}{t-s}$. Slijedi da λ_s ne ovisi o izboru skupa S, nego samo o njegovoj kardinalnosti s i možemo ga izraziti kao u iskazu leme.

2. Pretpostavimo da je $(V, \mathcal{B})$ neki t-(v, k, λ_t) dizajn. Tada karakteristični vektor f familije $\mathcal{B}$ zadovoljava jednadžbu (10) te vrijedi:

$$\binom{k-s}{t-s} W_{s,k} \cdot f = W_{s,t} \cdot W_{t,k} \cdot f = W_{s,t} \cdot \lambda_t \mathbf{1} = \lambda_t W_{s,t} \cdot \mathbf{1} = \lambda_t \binom{v-s}{t-s} \mathbf{1}.$$

U prvoj jednakosti smo koristili propoziciju 2.19, a u drugoj jednakosti smo koristili činjenicu da je f rješenje jednadžbe (10). Pri definiranju matrice $W_{s,t}$ rekli smo da ima $\binom{v-s}{t-s}$ jedinica u svakom retku, što koristimo u zadnjoj jednakosti. Iz gornjih jednakosti slijedi da je

$$W_{s,k} \cdot f = \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}} \lambda_t \mathbf{1}.$$

$(V, \mathcal{B})$ je sada očito i s-dizajn, gdje je $\lambda_s = \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}} \lambda_t$.

□

Primijetimo da λ_s mora biti cijeli broj, za bilo koji $s \in \{0, 1, \ldots, t\}$ pa smo dobili i koristan nužan uvjet na parametre t-dizajna.

Ako je $\mathcal{B}$ poskup od Ω, tada s $W_i(\mathcal{B})$ označavamo podmatricu matrice $W_{i,k}$, formiranu tako da matrica $W_i(\mathcal{B})$ sadrži redom sve stupce matrice $W_{i,k}$ koji odgovaraju elementima skupa $\mathcal{B}$.

Primjer 3.5. *Neka je $\mathcal{B} = \{\{1,2\},\{1,4\},\{2,3\},\{3,4\}\}$, iz primjera 3.3. Tada matrica $W_1(\mathcal{B})$ sadrži prvi, treći, četvrti i šesti stupac matrice $W_{1,2}$, jer ti stupci redom odgovaraju elementima skupa $\mathcal{B}$. Dakle,*

$$W_1(\mathcal{B}) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

Sada promotrimo skup $\mathcal{B}$ iz primjera 3.2. Matrica $W_{1,3}$ je $\binom{7}{1} \times \binom{7}{3} = 7 \times 35$ matrica. Matrica $W_1(\mathcal{B})$ sadrži samo one stupce koji odgovaraju blokovima u $\mathcal{B}$. Matricu $W_1(\mathcal{B})$ nazivamo incidencijskom matricom *dizajna $(V, \mathcal{B})$. Matrica $W_{2,3}$ je $\binom{7}{2} \times \binom{7}{3} = 21 \times 35$ matrica. Matrica $W_2(\mathcal{B})$ također sadrži samo one stupce koji odgovaraju blokovima u*

$\mathcal{B}$. *Dakle,*

$$W_1(\mathcal{B}) = \begin{bmatrix} 1&1&1&0&0&0&0\\ 1&0&0&1&1&0&0\\ 1&0&0&0&0&1&1\\ 0&1&0&1&0&1&0\\ 0&0&1&0&1&1&0\\ 0&0&1&1&0&0&1\\ 0&1&0&0&1&0&1 \end{bmatrix}, \text{ te } W_2(\mathcal{B}) = \begin{bmatrix} 1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0\\ 0&1&0&0&0&0&0\\ 0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0\\ 0&1&0&0&0&0&0\\ 1&0&0&0&0&0&0\\ 0&0&0&1&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&1&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&1&0\\ 0&0&0&0&0&1&0\\ 0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1\\ 0&0&0&0&0&1&0\\ 0&0&0&1&0&0&0\\ 0&1&0&0&0&0&0\\ 0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1 \end{bmatrix}.$$

Teorem 3.6. *Neka je $(V, \mathcal{B})$ t-dizajn te $i + j \leq t$. Tada vrijedi*

$$|\mathcal{B}|^{-1} W_i(\mathcal{B}) W_j(\mathcal{B})^\tau = \binom{v}{k}^{-1} W_{i,k} W_{j,k}^\tau.$$

Dokaz. Označimo s $b = |\mathcal{B}|$, što je ujedno broj λ_0 iz leme 3.4. Neka je α neki i-člani podskup od V, a β neki j-člani podskup od V i neka je $|\alpha \cup \beta| = s$. Tada je na mjestu koje odgovara paru (α, β) u matrici $W_i(\mathcal{B}) \cdot W_j(\mathcal{B})^\tau$ broj blokova iz $\mathcal{B}$ koji su nadskupovi od α i β, odnosno broj blokova koji sadrže α i β. Budući da je $s \leq i + j \leq t$, taj broj je λ_s iz leme 3.4. S druge strane, na mjestu koje odgovara paru (α, β) u matrici $W_{i,k} \cdot W_{j,k}^\tau$ nalazi se broj k-članih podskupova od V koji su nadskupovi od $\alpha \cup \beta$, a taj broj je $\binom{v-s}{k-s}$. Da bismo provjerili jednakost iz teorema, treba vidjeti da je $\frac{\lambda_s}{b} = \frac{\binom{v-s}{k-s}}{\binom{v}{k}}$. Iz leme 3.4 slijedi da je lijeva strana $\frac{\lambda_s}{b} = \frac{\lambda_s}{\lambda_0} = \frac{\binom{k}{s}}{\binom{v}{s}}$, pa se jednakost svodi na $\binom{v}{k}\binom{k}{s} = \binom{v}{s}\binom{v-s}{k-s}$, a to smo dokazali u lemi 2.13. □

Upravo dokazani teorem pomoći će nam pri dokazivanju linearne nezavisnosti redaka matrica $W_i(\mathcal{B})$, što ćemo koristiti u dokazu teorema 3.15.

Definicija 3.7. Komplement dizajna $(V, \mathcal{B})$ *je dizajn sa skupom vrhova* V *i skupom blokova* $V \setminus \beta$, *gdje* β *ide po svim blokovima iz* $\mathcal{B}$.

Definicija 3.8. *Neka su* t, k *i* v *fiksni te uzmimo proizvoljno poredane* t*-člane i* k*-člane podskupove fiksnog* v*-članog skupa. Tada definiramo* $\overline{W}_{t,k}$ *kao* $\binom{v}{t} \times \binom{v}{k}$ *matricu koja na mjestu* (i, j) *ima* 1, *ako su* i*-ti* t*-člani i* j*-ti* k*-člani podskupovi od* V *međusobno disjunktni, a* 0 *inače.*

Neka je α neki t-člani podskup od V, a β neki k-člani podskup od V. Primijetimo da vrijedi $\alpha \cap \beta = \emptyset$ ako i samo ako je $\alpha \subseteq V \setminus \beta$. Zato matricu $\overline{W}_{t,k}$ dobijemo permutacijom stupaca matrice $W_{t,v-k}$ koja odgovara komplementiranju. Štoviše, $\overline{W}_{k,v-k}$ je permutacijska matrica.

Primjer 3.9. *Neka je* $V = \{1, 2, 3, 4, 5\}$ *te neka je* Ω_1 *familija svih jednočlanih,* Ω_2 *familija svih dvočlanih te* Ω_3 *familija svih tročlanih podskupova od* V, *tj.*

$$\begin{aligned}
\Omega_1 &= \{\{1\}, \{2\}, \{3\}, \{4\}, \{5\}\}, \\
\Omega_2 &= \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{1, 5\}, \{2, 3\}, \{2, 4\}, \{2, 5\}, \{3, 4\}, \{3, 5\}, \{4, 5\}\} \\
\Omega_3 &= \{\{1, 2, 3\}, \{1, 2, 4\}, \{1, 2, 5\}, \{1, 3, 4\}, \{1, 3, 5\}, \{1, 4, 5\}, \{2, 3, 4\}, \\
&\quad \{2, 3, 5\}, \{2, 4, 5\}, \{3, 4, 5\}\}.
\end{aligned}$$

Tada imamo

$$\overline{W}_{1,2} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

te

$$W_{1,3} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Ako se u matrici $W_{1,3}$ *na mjestu* (α, γ) *nalazi* 1, *tada je* $\alpha \subseteq \gamma$. *Također, znamo da postoji* $\beta \in \Omega_2$ *takav da je* $\gamma = V \setminus \beta$. *Slijedi da su* γ *i* β *međusobno disjunktni skupovi, pa su posebno i* α *i* β *međusobno disjunktni skupovi. Dakle, na mjestu* (α, β) *u matrici* $\overline{W}_{1,2}$ *također se nalazi* 1. *Inače, ako se u matrici* $W_{1,3}$ *na mjestu* (α, γ) *nalazi* 0, *tada* α *nije sadržan u* γ *pa su* α *i* γ *dva međusobno disjunktna skupa. Kako je* γ *tročlani podskup od* V, *znamo da postoji* $\beta \in \Omega_2$, *takav da je* $\beta = V \setminus \gamma$. *S obzirom na to da su* α *i* γ *međusobno disjunktni, slijedi da je* $\alpha \subseteq V \setminus \gamma = \beta$, *odnosno* *skupovi α i β nisu disjunktni pa se na mjestu (α, β) u matrici $\overline{W}_{1,2}$ također nalazi 0. Sada je očito je da se $\overline{W}_{1,2}$ razlikuje od $W_{1,3}$ za permutaciju njezinih stupaca, a matrica permutacije je 10×10 matrica s jedinicama na sporednoj dijagonali, što upravo odgovara matrici $\overline{W}_{2,3}$.*

Lema 3.10. *Vrijedi*

1. $\overline{W}_{t,k} = \sum_i (-1)^i W_{i,t}^\tau W_{i,k}$,
2. $W_{t,k} = \sum_i (-1)^i W_{i,t}^\tau \overline{W}_{i,k}$.

Dokaz. Neka je α t-člani podskup od V te neka je β k-člani podskup od V. Na mjestu (α, β) u matrici $\overline{W}_{t,k}$ nalazi se 1, ako je α disjunktan s β, a 0 inače. Kao što smo već objasnili u dokazu propozicije 2.18, na mjestu (α, β) u matrici $W_{i,t}^\tau W_{i,k}$ nalazi se $\binom{|\alpha\cap\beta|}{i}$. Ako su α i β međusobno disjunktni skupovi, tada je $|\alpha \cap \beta| = 0$ pa je $\binom{|\alpha\cap\beta|}{i} = 0$, za svaki $i > 0$. U slučaju kada je $i = 0$, tada je $\binom{|\alpha\cap\beta|}{i} = 1$. Ako je $\alpha \cap \beta \neq \emptyset$ te ako stavimo $s := |\alpha \cap \beta|$, tada koristeći binomni teorem dobijemo

$$\sum_{i=0}^{s} (-1)^i \binom{s}{i} = (1 + (-1))^s = 0.$$

Stoga desnu stranu jednakosti tvrdnje 1 možemo zapisati kao

$$\sum_i (-1)^i \binom{|\alpha \cap \beta|}{i} = \begin{cases} 1, & \text{ako je } \alpha \cap \beta = \emptyset \\ 0, & \text{inače.} \end{cases}$$

Kako se s desne strane dobivene jednakosti nalaze odgovarajuće vrijednosti za matricu $\overline{W}_{t,k}$, pokazali smo da tvrdnja 1 vrijedi.

Nadalje, znamo da se na mjestu (α, β) u matrici $W_{t,k}$ nalazi 1 ako je t-člani podskup od V sadržan u k-članom podskupu od V, a inače se na tom mjestu nalazi 0. Na mjestu (α, β) u matrici $W_{i,t}^\tau \overline{W}_{i,k}$ nalazi se broj i-članih podskupova od V koji su podskupovi od α, a disjunktni su s β. Takvih skupova ima $\binom{|\alpha\setminus\beta|}{i}$. Ako je $\alpha \subseteq \beta$, tada je $|\alpha \setminus \beta| = 0$, pa je $\binom{|\alpha\setminus\beta|}{i} = 0$, za svaki $i > 0$. U slučaju kada je $i = 0$, tada je $\binom{|\alpha\setminus\beta|}{i} = 1$. Inače, ako α nije podskup skupa β te $r := |\alpha \setminus \beta|$, koristeći binomni teorem dobijemo

$$\sum_{i=0}^{r} (-1)^i \binom{r}{i} = (1 + (-1))^r = 0.$$

Stoga desnu stranu jednakosti tvrdnje 2 možemo zapisati kao

$$\sum_i (-1)^i \binom{|\alpha \setminus \beta|}{i} = \begin{cases} 1, & \text{ako je } \alpha \subseteq \beta \\ 0, & \text{inače.} \end{cases}$$

S desne strane očito imamo odgovarajuće vrijednosti za matricu $W_{t,k}$ pa smo dokazali tvrdnju 2. $\square$

Lema 3.11. *Vrijedi*

$$W_{i,t}\overline{W}_{t,k} = \binom{v-k-i}{t-i}\overline{W}_{i,k}.$$

Dokaz. Neka je V neki fiksni skup od v elemenata te neka je α i-člani i β k-člani podskup od V. Tada se na mjestu (α, β) u matrici $W_{i,t}\overline{W}_{t,k}$ nalazi broj t-članih podskupova od V koji sadrže α i disjunktni su s β. Ako α i β nisu disjunktni, takvi t-člani podskupovi ne postoje, pa je na lijevoj strani 0, kao i u matrici $\overline{W}_{i,k}$ na desnoj strani. Ako su α i β disjunktni, od $v-k-i$ elemenata koji nisu niti u α niti u β biramo $t-i$ elemenata da bismo nadopunili α do t-članog podskupa disjunktnog s β. Tada je na lijevoj i na desnoj strani $\binom{v-k-i}{t-i}$. $\square$

Lema 3.12. *Ako je $t \leq k \leq v-t$, onda je prostor razapet retcima matrice $W_{t,k}$ jednak prostoru razapetom retcima matrice $\overline{W}_{t,k}$ nad $\mathbb{Q}$.*

Dokaz. Potrebno je pokazati da je svaki redak matrice $\overline{W}_{t,k}$ linearna kombinacija redaka matrice $W_{t,k}$ te da je svaki redak matrice $W_{t,k}$ linearna kombinacija redaka matrice $\overline{W}_{t,k}$. Iz propozicije 2.19 imamo

$$W_{i,t}W_{t,k} = \binom{k-i}{t-i}W_{i,k}.$$

Kada podijelimo gornju jednakost sa $\binom{k-i}{t-i}$ dobijemo

$$W_{i,k} = \binom{k-i}{t-i}^{-1}W_{i,t}W_{t,k},$$

pa iz tvrdnje 1 leme 3.10 slijedi

$$\overline{W}_{t,k} = \sum_i (-1)^i W_{i,t}^\tau \binom{k-i}{t-i}^{-1} W_{i,t}W_{t,k}.$$

Kada sredimo dobivenu jednakost dobijemo

$$\overline{W}_{t,k} = \left(\sum_i (-1)^i \binom{k-i}{t-i}^{-1} W_{i,t}^\tau W_{i,t}\right) W_{t,k},$$

jer matrica $W_{t,k}$ ne ovisi o i te je $W_{i,t}^\tau \binom{k-i}{t-i}^{-1} = \binom{k-i}{t-i}^{-1} W_{i,t}^\tau$. Iz toga slijedi da je svaki redak matrice $\overline{W}_{t,k}$ linearna kombinacija redaka matrice $W_{t,k}$. Nadalje, iz leme 3.11 vrijedi

$$W_{i,t}\overline{W}_{t,k} = \binom{v-k-i}{t-i}\overline{W}_{i,k},$$

pa tvrdnja 2 leme 3.10 povlači jednakost

$$W_{t,k} = \left(\sum_i (-1)^i \binom{v-k-i}{t-i}^{-1} W_{i,t}^{\tau} W_{i,t} \right) \overline{W}_{t,k}.$$

Dakle, svaki redak matrice $W_{t,k}$ možemo prikazati kao linearnu kombinaciju redaka matrice $\overline{W}_{t,k}$.

□

Teorem 3.13. *Dizajn i njegov komplement imaju jednaku snagu.*

Dokaz. U lemi 3.12 smo pokazali da postoje matrice G i H takve da vrijedi

$$\overline{W}_{t,k} = G \cdot W_{t,k} \quad \text{i} \quad W_{t,k} = H \cdot \overline{W}_{t,k}.$$

Sume redaka matrica G i H su konstante pa ako vrijedi da je $W_{t,k} \cdot x = \lambda \mathbf{1}$, tada je $\overline{W}_{t,k} \cdot x = G \cdot W_{t,k} \cdot x = G \cdot \lambda \mathbf{1} = \lambda G \cdot \mathbf{1} = c\mathbf{1}$, za neku konstantu c. S obzirom na to da se matrica $W_{t,v-k}$ dobiva iz matrice $\overline{W}_{t,k}$ permutacijom njezinih stupaca, slijedi da komplement dizajna snage t ima snagu barem t.

□

Teorem 3.14. *Ako je $t \leq k$, rang matrice $W_{t,k}$ nad $\mathbb{Q}$ je $min\{\binom{v}{t}, \binom{v}{k}\}$.*

Dokaz. Pretpostavimo da je $t \leq k \leq v-t$. Prvo razmotrimo slučaj kad je $v = t + k$. Tada su $W_{t,v-t}$ i $\overline{W}_{t,k}$ kvadratne matrice istog reda. Kako je $\overline{W}_{t,v-t}$ permutacijska matrica, ona je regularna. S obzirom da su prostori razapeti retcima matrica $\overline{W}_{t,v-t}$ i $W_{t,v-t}$ jednaki, što smo pokazali u lemi 3.12, vrijedi da one imaju isti rang pa je matrica $W_{t,v-t}$ regularna. Sada razmotrimo slučaj kada je $t \leq h \leq v-t$. Tada iz leme 3.11 imamo

$$W_{t,h} W_{h,v-t} = \binom{v-2t}{h-t} W_{t,v-t}.$$

Kako je matrica s desne strane jednadžbe regularna, slijedi da su retci matrice $W_{t,h}$ linearno nezavisni.

□

Teorem 3.15 (Ray-Chaudhuri i Wilson)**.** *Neka je $(V, \mathcal{B})$ t-dizajn takav da je $t < k \leq v-t$. Tada je $|\mathcal{B}| \geq \binom{v}{\lfloor t/2 \rfloor}$.*

Dokaz. Označimo $i \coloneqq \lfloor t/2 \rfloor$. Dovoljno je pokazati da $W_i(\mathcal{B})$ ima linearno nezavisne retke. Kako je $\frac{t}{2} + \frac{t}{2} = t$, iz teorema 3.6 slijedi jednakost

$$|\mathcal{B}|^{-1} W_i(\mathcal{B}) W_i(\mathcal{B})^{\tau} = \binom{v}{k}^{-1} W_{i,k} W_{i,k}^{\tau}.$$

U teoremu 3.14 pokazali smo da su za $k \leq v - t$ retci matrice $W_{i,k}$ linearno nezavisni pa je $W_{i,k}W_{i,k}^{\tau}$ regularna. Slijedi da je matrica $W_i(\mathcal{B})W_i(\mathcal{B})^{\tau}$ regularna pa su retci matrice $W_i(\mathcal{B})$ linearno nezavisni. □

Korolar 3.16 (Fisherova nejednakost)**.** *Neka je $(V, \mathcal{B})$ 2-dizajn takav da je $2 < k \leq v - 2$. Tada je $|\mathcal{B}| \geq v$.*

Dokaz. Slijedi iz teorema 3.15, za $t = 2$. □

Korolar 3.17. *Ako je $(V, \mathcal{B})$ dizajn snage barem $2s$, tada su retci matrice $W_s(\mathcal{B})$ linearno nezavisni.*

Dokaz. Slijedi iz dokaza teorema 3.15. □

4 Asocijacijske sheme

Dosad smo promatrali Johnsonove grafove i pokazali koja svojstva zadovoljavaju njihove matrice susjedstva. Ukoliko promatramo skup bilo kojih grafova s odgovarajućim svojstvima, doći ćemo do definicije asocijacijske sheme koju će sada biti jednostavnije razumjeti.

Definicija 4.1. *Asocijacijska shema s d klasa na n-članom skupu V je skup grafova $G_0, G_1, \ldots, G_d$ sa skupom vrhova V, takav da vrijedi:*

- *Graf G_0 sadrži samo petlje, odnosno sve jednočlane bridove.*
- *Ako su x i y dva različita vrha u V, tada postoji točno jedan graf G_i u kojem je $\{x, y\}$ brid.*
- *Neka su $i, j, k \in \{0, \ldots, d\}$ i $x, y \in V$ elementi takvi da je $\{x, y\}$ brid u G_k. Tada broj elemenata $z \in V$ takvih da je $\{x, z\}$ brid u G_i te $\{y, z\}$ brid u G_j ne ovisi o izboru elemenata x i y, nego samo o indeksima i, j, k. Taj broj je nenegativna konstanta $p_{i,j}^k$ koju zovemo presječnim brojem sheme.*

Kažemo da je graf G_i i-ta klasa sheme, tj. klasu poistovjećujemo s grafom. Zajednički skup vrhova grafova G_i nazivamo skupom vrhova sheme. Za dva susjedna vrha u grafu G_i kažemo da su i-asocirani. Asocijacijska shema određuje particiju skupa bridova potpunog grafa na d razapinjućih podgrafova $G_1, \ldots, G_d$. Definiciju 4.1 možemo izreći i u terminima matrica. Za matrice $A_0, \ldots, A_d$, koje su redom matrice susjedstva grafova $G_0, \ldots, G_d$ vrijedi:

1. $A_i^{\tau} = A_i$, $i = 0, \ldots, k$,

2. $A_0 = I$,

3. $\sum_{i=0}^{d} A_i = J$,

4. $A_i A_j = A_j A_i$, za sve i, j,

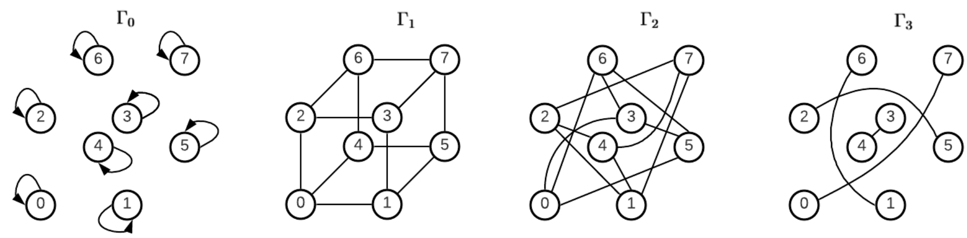
5. Produkt matrica $A_i A_j$ je linearna kombinacija matrica $A_0, \ldots, A_d$, za sve i, j.

Skup $\{0,1\}$-matrica tipa $n \times n$, različitih od nulmatrice, koje zadovoljavaju gore navedene uvjete, nazivamo asocijacijskom shemom s d klasa. Zbog 3. svojstva očito je da su matrice $A_0, \ldots, A_d$ linearno nezavisne, pa razapinju potprostor vektorskog prostora $M_n(\mathbb{R})$ dimenzije $d+1$. Iz 4. i 5. svojstva slijedi da je taj vektorski prostor komutativna algebra s jedinicom koju nazivamo Bose-Mesnerovom algebrom sheme. Objasnimo još vezu između 5. svojstva te presječnih brojeva iz definicije 4.1. Matricu $A_i A_j$ možemo prikazati kao linearnu kombinaciju matrica $A_0, \ldots, A_d$, tj.

$$A_i A_j = \sum_{k=0}^{d} \alpha_{i,j}^k A_k.$$

S lijeve strane jednakosti imamo cjelobrojnu matricu s nenegativnim vrijednostima te svaka matrica A_i ima jedinice na različitim mjestima pa zaključujemo da su koeficijenti $\alpha_{i,j}^k$ nužno nenegativni cijeli brojevi. Nadalje, na mjestu (x, y) u matrici $A_i A_j$ nalazi se broj vrhova z koji su susjedi s x u G_i te susjedi s y u G_j. Možemo zaključiti da je takva interpretacija ekvivalentna 5. svojstvu iz definicije 4.1, tj. koeficijenti $\alpha_{i,j}^k$ su presječni brojevi sheme.

Primjer 4.2. *Neka je $V = \{0, \ldots, 7\}$. Tada grafovi $\Gamma_0, \ldots, \Gamma_3$ sa slike 6 čine asocijacijsku shemu poznatu pod nazivom 3-kocka.*



Slika 6: Četiri grafa 3-kocke.

Uzmimo sada za primjer brid $\{0, 7\}$ iz grafa Γ_3. Provjerimo koliko iznosi presječni broj $p_{1,2}^3$. Vrh 0 je u grafu Γ_1 susjed s tri vrha, tj. u grafu Γ_1 imamo bridove $\{0, 1\}$,

$\{0,2\}$ te $\{0,4\}$. Pogledajmo postoje li u grafu Γ_2 bridovi $\{1,7\}$, $\{2,7\}$ te $\{4,7\}$. Vidimo da ti bridovi postoje, stoga postoje tri vrha z takva da je $\{0,z\}$ brid u Γ_1 te $\{z,7\}$ brid u Γ_3. Lako se provjeri da isto vrijedi za sve bridove u Γ_3, odnosno neovisno o odabiru brida u Γ_3, vrijedi da je $p^3_{1,2} = 3$. Uvjerimo se sada još da je ekvivalentna definicija s matricama ispravna, tako što ćemo provjeriti umnožak matrica susjedstva grafova Γ_1 i Γ_2, odnosno A_1 i A_2. Tvrdimo da je $A_1 \cdot A_2 = \sum_{k=0}^{3} p^k_{1,2} A_k$. Iz grafova na slici 6 vidimo da je $p^0_{1,2} = 0$, $p^1_{1,2} = 2$, $p^2_{1,2} = 0$, a pokazali smo da je $p^3_{1,2} = 3$. Dakle, imamo:

$$A_1 \cdot A_2 = p^0_{1,2}A_0 + p^1_{1,2}A_1 + p^2_{1,2}A_2 + p^3_{1,2}A_3 = 2A_1 + 3A_3.$$

Uistinu,

$$A_1 \cdot A_2 = \begin{bmatrix} 0 & 2 & 2 & 0 & 2 & 0 & 0 & 3 \\ 2 & 0 & 0 & 2 & 2 & 3 & 2 & 0 \\ 2 & 0 & 0 & 2 & 0 & 3 & 2 & 0 \\ 0 & 2 & 2 & 0 & 3 & 0 & 0 & 2 \\ 2 & 0 & 0 & 3 & 0 & 2 & 2 & 0 \\ 0 & 2 & 3 & 0 & 2 & 0 & 0 & 2 \\ 0 & 3 & 2 & 0 & 2 & 0 & 0 & 2 \\ 3 & 0 & 0 & 2 & 0 & 2 & 2 & 0 \end{bmatrix} = 2A_1 + 3A_3.$$

Primjer 4.3. *Prethodno smo definirali matrice $A_1, \ldots, A_k$ kao matrice susjedstva Johnsonovih grafova $J(v,k,i)$. Matrice $A_1, \ldots, A_k$ zajedno s matricom A_0 čine asocijacijsku shemu s k klasa na skupu od $n = \binom{v}{k}$ vrhova. Stoga je skup koji sadrži grafove $G_i = J(v,k,i)$, $i = 0, \ldots, k$ asocijacijska shema koju nazivamo* Johnsonovom shemom *te označavamo s $J(v,k)$. Dakle, $\mathcal{A} = \langle A_0, A_1, \ldots, A_k \rangle$ je Bose-Mesnerova algebra Johnsonove sheme.*

Primjer 4.4. *Drugi važan primjer asocijacijske sheme je Hammingova shema $H(k,q)$. Skup vrhova ove sheme su sve riječi duljine k nad alfabetom veličine q.* Hammingova udaljenost *između dvije riječi u i v je broj indeksa r takvih da je $u_r \neq v_r$. Neka je G_i graf s riječima kao vrhovima. Dva vrha su susjedna ako i samo ako je Hammingova udaljenost među njima i. Tada skup koji sadrži grafove $G_0, \ldots, G_k$ čini asocijacijsku shemu s k klasa na skupu od $n = q^k$ vrhova koju nazivamo* Hammingovom shemom. *Primijetimo da su dva vrha susjedna u G_i ako i samo ako su na udaljenosti i u grafu G_1. Hammingova shema je veoma važna u teoriji kodiranja. Uočimo da je primjer 4.2 zapravo Hammingova shema $H(3,2)$. U toj shemi imamo vrhove koji su riječi duljine* 3 *nad alfabetom duljine* 2. *Ukoliko uzmemo za alfabet $\{0,1\}$, tada su vrhovi riječi* 000, 001, 010, 011, 100, 101, 110 *te* 111. *Pridružimo li svakoj riječi odgovarajući broj u dekadskom sustavu, dobivamo upravo vrhove u grafovima Γ_i. Očito je i da su bridovi u grafovima Γ_i odgovarajući. Primjerice, u grafu G_3 Hammingove sheme dva su vrha* *susjedna ako i samo ako je Hammingova udaljenost među njima* 3. *Iz toga slijedi da je skup bridova grafa* G_3 *jednak* $\{\{000, 111\}, \{001, 110\}, \{010, 101\}, \{011, 100\}\}$, *što je ekvivalentno bridovima* $\{\{0, 7\}, \{1, 6\}, \{2, 5\}, \{3, 4\}\}$ *u* Γ_3.

Primjer 4.5. *Skup vrhova sheme* $J(n, k)$ *možemo povezati sa skupom riječi težine* k *u Hammingovoj shemi* $H(n, 2)$. *Kažemo da je riječ* w *težine* k, *ako se sastoji od* k *znakova različitih od* 0. *Neka je* $n = 4$, $k = 3$ *te uzmimo alfabet* $\{0, 1\}$. *Tada je skup riječi težine* 2 *iz skupa vrhova Hammingove sheme* $H(4, 2)$ *jednak* $\{0011, 0101, 0110, 1001, 1010, 1100\}$. *S druge strane, prisjetimo se primjera 2.4 te skup riječi težine* 2 *interpretirajmo tako da svaka riječ određuje brid u* $J(4, 2)$ *na sljedeći način:*

$$
\begin{gathered}
0011 \to \{c, d\} \\
0101 \to \{b, d\} \\
\vdots
\end{gathered}
$$

Tada očito dobijemo pripadni skup bridova Ω.

Pokazali smo već da je Bose-Mesnerova algebra $\mathcal{A}$ asocijacijske sheme zatvorena na matrično množenje. Sada ćemo definirati Schurov produkt te pokazati da je $\mathcal{A}$ zatvorena i na takvo množenje.

Definicija 4.6. *Neka su* A *i* B *dvije matrice istih dimenzija.* Schurov *produkt matrica* A *i* B *označava se sa* $A \circ B$ *i definira kao*

$$(A \circ B)_{i,j} = (A)_{i,j}(B)_{i,j}.$$

Schurov produkt često se naziva i Hadamardov produkt.

Propozicija 4.7. *Bose-Mesnerova algebra je zatvorena na Schurov produkt.*

Dokaz. Neka je $\mathcal{A} = \langle A_0, A_1, \ldots A_d \rangle$ Bose-Mesnerova algebra dimenzije $d+1$. Matrice A_i su matrice asocijacijske sheme s d klasa pa vrijedi

$$\sum_{i=0}^{d} A_i = J.$$

Iz toga vidimo da matrica J, koja je neutralni element za Schurovo množenje, leži u $\mathcal{A}$. Vrijedi sljedeća jednakost:

$$A_i \circ A_j = \begin{cases} A_i, & \text{ako je } i = j, \\ 0, & \text{inače.} \end{cases} \tag{11}$$

Element na mjestu (i,j) matrice $A \circ B$ jednak je produktu elemenata na mjestu (i,j) matrica A i B. Pokažimo da je tada Schurov produkt dvije linearne kombinacije matrica $A_0, \ldots, A_d$ također linearna kombinacija tih matrica:

$$\left(\sum_{i=0}^{d} \alpha_i A_i\right) \circ \left(\sum_{j=0}^{d} \beta_j A_j\right) = \sum_{i=0}^{d} \sum_{j=0}^{d} \alpha_i \beta_j A_i \circ A_j = \sum_{i=0}^{d} \alpha_i^2 A_i \in \mathcal{A}.$$

Dakle, algebra razapeta matricama $A_0, \ldots A_d$ je zatvorena na Schurov produkt pa je Bose-Mesnerova algebra $\mathcal{A}$ zatvorena na Schurov produkt. □

Iz (11) slijedi da su matrice A_i idempotentne s obzirom na Schurov produkt pa ih zovemo Schurovim idempotentama sheme. Sljedeći teorem ćemo samo iskazati kao važnu karakterizaciju Bose-Mesnerove algebre, a dokaz može se naći u knjizi [1] na 57. stranici.

Teorem 4.8. *Svaki potprostor vektorskog prostora simetričnih matrica koji sadrži I i J te je zatvoren na matrično i Schurovo množenje je Bose-Mesnerova algebra neke asocijacijske sheme.*

Osim matričnog i Schurovog produkta, na Bose-Mesnerovoj algebri možemo definirati i skalarni produkt.

Propozicija 4.9. *Bose-Mesnerova algebra asocijacijske sheme je unitaran prostor, sa skalarnim produktom*

$$\langle A, B \rangle = \mathrm{tr}(AB),$$

gdje AB predstavlja matrično množenje.

Dokaz. Produkt $\langle A, B \rangle = \mathrm{tr}(AB^\tau)$ je skalarni produkt na vektorskom prostoru matrica $M_n(\mathbb{R})$, a u našem slučaju, zbog simetričnosti matrica asocijacijske sheme, vrijedi jednakost $\mathrm{tr}(AB^\tau) = \mathrm{tr}(AB)$ pa je zadani produkt također skalaran. □

Prethodno definirani skalarni produkt alternativno možemo zapisati pomoću Schurovog produkta.

Propozicija 4.10. *Neka je $sum(A)$ suma svih elemenata matrice A. Tada za svake dvije simetrične matrice $A, B \in M_n(\mathbb{R})$ vrijedi:*

$$\langle A, B \rangle = sum(A \circ B).$$

Dokaz. Vrijedi:

$$
\begin{aligned}
\langle A, B\rangle &= \operatorname{tr}(AB)\\
&= \operatorname{tr}\left(\left[\sum_{k=1}^{n}(A)_{i,k}(B)_{k,j}\right]\right)\\
&= \sum_{i=1}^{n}\sum_{k=1}^{n}(A)_{i,k}(B)_{k,i}\\
&= \sum_{i=1}^{n}\sum_{k=1}^{n}(A)_{i,k}(B)_{i,k}\\
&= \sum_{i=1}^{n}\sum_{k=1}^{n}(A \circ B)_{i,k}\\
&= \operatorname{sum}(A \circ B).
\end{aligned}
$$

□

Schurove idempotente A_i su u parovima ortogonalne s obzirom na Schurov produkt te čine bazu za $\mathcal{A}$. Pokazat ćemo da postoji druga baza za $\mathcal{A}$ koju čine idempotentne matrice koje su u parovima ortogonalne s obzirom na matrično množenje. Prije toga, prisjetimo se nekih pojmova iz linearne algebre. Neka su $A, B \in M_n$ kvadratne matrice istog reda. Za matricu A kažemo da je regularna ako postoji matrica B takva da vrijedi $AB = BA = I$. Tada matricu B nazivamo inverz matrice A i označavamo s A^{-1}. Kažemo da je matrica A ortogonalna ako vrijedi $AA^{\tau} = A^{\tau}A = I$. Tada je očito svaka ortogonalna matrica regularna, gdje je $A^{-1} = A^{\tau}$. Kažemo da je matrica A slična matrici B, ako postoji regularna matrica $T \in M_n$ takva da je $B = T^{-1}AT$. Za kvadratnu matricu kažemo da je dijagonalizabilna ako je slična nekoj dijagonalnoj matrici. Za daljnje tvrdnje potrebno je još iskazati sljedeći važan teorem, čiji se dokaz može naći u [15].

Teorem 4.11. *Kvadratnu realnu matricu A možemo prikazati u Schurovoj formi $A = URU^{\tau}$, gdje je U ortogonalna, a R gornjetrokutasta matrica.*

Sada ćemo vidjeti da se sve simetrične matrice mogu dijagonalizirati. Štoviše, za simetrične matrice postoje ortogonalne matrice koje ih dijagonaliziraju.

Teorem 4.12. *Matrica $A \in M_n$ se može ortogonalno dijagonalizirati ako i samo ako je simetrična.*

Dokaz. Pretpostavimo da se A može ortogonalno dijagonalizirati. To znači da postoji ortogonalna matrica L takva je $D = L^\tau AL$ dijagonalna. Pomnožimo sada taj izraz s L slijeva i L^τ zdesna. Tada imamo:

$$LDL^\tau = LL^\tau ALL^\tau.$$

S obzirom da je L ortogonalna, onda vrijedi da je $LL^\tau = I$ pa dobijemo:

$$LDL^\tau = A.$$

Pokažimo sada da to povlači da je matrica A nužno simetrična.

$$A^\tau = L^\tau D^\tau (L^\tau)^\tau = L^\tau DL = A.$$

S druge strane, pretpostavimo da je A simetrična i pokažimo da se ona tada može ortogonalno dijagonalizirati. Matricu A možemo zapisati u Schurovoj formi pa imamo da je $A = LRL^\tau$, gdje je L ortogonalna i R gornjetrokutasta matrica. Zbog pretpostavke da je A simetrična, vrijedi:

$$LRL^\tau = A = A^\tau = (L^\tau)^\tau R^\tau L^\tau = LR^\tau L^\tau.$$

Da bi jednakost vrijedila, gornjetrokutasta matrica R mora biti simetrična, iz čega slijedi da je dijagonalna. $\square$

Korolar 4.13. *$\{0,1\}$-matrice $A_0, \ldots, A_d$ dimenzije $n \times n$ koje čine asocijacijsku shemu mogu se ortogonalno dijagonalizirati.*

Dokaz. S obzirom da su matrice $A_0, \ldots, A_d$ simetrične, tvrdnja slijedi iz teorema 4.12. $\square$

Iskažimo sada važan teorem o simultanoj dijagonalizaciji, čiji se dokaz može pronaći u [2] na 9. stranici.

Teorem 4.14 (Simultana dijagonalizacija)**.** *Neka su $A_1, \ldots, A_r$ realne matrice takve da je svaka matrica A_i dijagonalizabilna. Tada se $A_1, \ldots, A_r$ mogu simultano dijagonalizirati ako i samo ako matrice A_i međusobno komutiraju.*

Teorem 4.15. *Neka $\{0,1\}$-matrice $A_0, \ldots, A_d$ dimenzije $n \times n$ čine asocijacijsku shemu te neka je $\mathcal{A} = \langle A_0, A_1, \ldots A_d \rangle$ pripadna Bose-Mesnerova algebra dimenzije $d+1$. Tada postoji skup u parovima ortogonalnih idempotentnih matrica $E_0, \ldots, E_d$ i realni brojevi $p_i(j)$ takvi da:*

1. $\sum_{j=0}^{d} E_j = I$,

2. $A_i E_j = p_i(j) E_j$,

3. $E_0 = \frac{1}{n} J$,

4. $\{E_0, \dots E_d\}$ *je baza za* $\mathcal{A}$.

Dokaz. Iz teorema 4.14 slijedi da postoji ortogonalna matrica L, takva da su $D_i := L^\tau A_i L$ dijagonalne matrice, za $i = 0, \dots, d$. Matrice D_i razapinju $(d+1)$-dimenzionalnu algebru $\mathcal{B}$ dijagonalnih matrica izomorfnu Bose-Mesnerovoj algebri $\mathcal{A}$. Na dijagonali matrice D_i nalaze se svojstvene vrijednosti matrice A_i. Promotrimo sada elemente na dijagonalama matrica $D_0, \dots, D_d$ na sljedeći način:

$$\begin{aligned} s_0 &:= (\lambda_{0,0}, \lambda_{1,0}, \dots, \lambda_{d,0}) \\ s_1 &:= (\lambda_{0,1}, \lambda_{1,1}, \dots, \lambda_{d,1}) \\ &\vdots \\ s_d &:= (\lambda_{0,d}, \lambda_{1,d}, \dots, \lambda_{d,d}), \\ &\vdots \\ s_n &:= (\lambda_{0,n}, \lambda_{1,n}, \dots, \lambda_{d,n}), \end{aligned}$$

gdje je $\lambda_{i,j}$ j-ta vrijednost na dijagonali matrice D_i. Među n uređenih $(d+1)$-torki postoji $d+1$ različitih zbog dimenzije algebre $\mathcal{B}$; označimo ih s $t_0, \dots, t_d$. Definiramo matricu F_i tako da se na mjestu (j, j) nalazi 1, ako je $s_j = t_i$. Na preostalim mjestima se nalaze nule. Za matrice F_i vrijedi da je $\sum_{i=0}^d F_i = I$ te $F_i F_j = 0$, za sve $i \neq j$. Matrice F_i su $\{0,1\}$-matrice koje čine bazu algebre $\mathcal{B}$. Sada definiramo matrice E_i kao $E_i := L F_i L^\tau$. Tada za matrice E_i vrijedi:

$$E_i E_j = \begin{cases} E_i, & \text{ako je } i = j \\ 0, & \text{inače} \end{cases}$$

i

$$\sum_{j=0}^{d} E_j = I. \tag{12}$$

Dakle, matrice E_i su idempotentne i u parovima ortogonalne s obzirom na obično matrično množenje. Neka je $U_i = \{E_i x \colon x \in \mathbb{R}^n\}$. Za vektore $u \in U_i$, zbog idempotentnosti matrica E_i, postoji vektor $v \in \mathbb{R}^n$ takav da je:

$$u = E_i v = E_i^2 v = E_i(E_i v) = E_i u.$$

Stoga, vektore iz U_i matrica E_i ostavlja fiksnima. Za $w \in U_i^\perp$ vrijedi:

$$\langle E_i w, E_i w\rangle = \langle E_i^2 w, w\rangle = \langle E_i w, w\rangle = 0,$$

jer je $E_i w \in U_i$, a $w \in U_i^\perp$ pa je $E_i w$ nulvektor. Vektor $x \in \mathbb{R}^n$ možemo zapisati kao $x = y + z$, gdje je $y \in U_i$ te $z \in U_i^\perp$. Tada vrijedi:

$$E_i x = E_i y + E_i z = y + E_i z.$$

S obzirom da je $E_i z$ nulvektor, slijedi da je $y = E_i x$ pa matrica E_i predstavlja ortogonalnu projekciju na potprostor od $\mathbb{R}^n$. Pokažimo da to mora biti svojstveni potprostor za bilo koju matricu $A \in \mathcal{A}$, odnosno $A = \sum_{j=0}^d \alpha_j E_j$. Neka je $y \in U_i$ pa je $y = E_i x$, za $x \in \mathbb{R}^n$. Pomnožimo li y s A slijeva, dobijemo:

$$Ay = AE_i x = \sum_{j=0}^{d} \alpha_j E_j E_i x = \alpha_i E_i E_i x = \alpha_i E_i x = \alpha_i y.$$

U trećoj jednakosti iskoristili smo ortogonalnost matrica E_i, tj. $E_i E_j = 0$, za $i \neq j$. Jedini sumandi koji ostaju su za $j = i$, a onda u četvrtoj jednakosti koristimo idempotentnost matrica E_i, zbog čega je $E_i E_i = E_i$. Na kraju, $\alpha_i y$ je također u U_i pa zaključujemo da matrica A preslikava prostor U_i u njega samoga. Onda postoje realni brojevi $p_i(j)$ takvi da je

$$A_i E_j = p_i(j) E_j \tag{13}$$

pa iz (12) dobijemo:

$$A_i = A_i I = A_i \sum_j E_j = \sum_j A_i E_j = \sum_j p_i(j) E_j,\ i = 0, \dots, d. \tag{14}$$

Zaključujemo da je svaka matrica A_i linearna kombinacija matrica E_j. S obzirom da su E_j u parovima ortogonalne, one su linearno nezavisne pa je $\{E_0, \dots E_d\}$ baza za $\mathcal{A}$. Preostalo nam je pokazati da je $E_0 = \frac{1}{n} J$. Znamo da je $J \in \mathcal{A}$ pa slijedi da J komutira sa svakom idempotentom E_j. Stoga, $JE_j = \gamma E_j$, gdje je γ suma stupca matrice E_j. Također, γ mora biti svojstvena vrijednost od J pa je $\gamma = 0$ ili $\gamma = n$. Iz toga zaključujemo da jedna od idempotenti E_j mora biti jednaka $\frac{1}{n}J$, a možemo pretpostaviti da je to E_0.

□

Sve matrice E_i leže u $\mathcal{A}$ pa također postoje i realni brojevi $q_i(j)$ takvi da je

$$E_i = \frac{1}{n} \sum_j q_i(j) A_j,\ i = 0, \dots, d. \tag{15}$$

Dakle, $E_i \circ A_j = \frac{1}{n} q_i(j) A_j$ te $A_i \circ E_j = \frac{1}{n} q_j(i) A_i$.

Definicija 4.16. *Realne brojeve $p_i(j)$ nazivamo* svojstvenim vrijednostima*, a realne brojeve $q_i(j)$ zovemo* dualnim svojstvenim vrijednostima *asocijacijske sheme. Matrice E_i nazivamo* glavnim idempotentama *sheme.*

Sada nas zanima odnos između svojstvenih i dualnih svojstvenih vrijednosti sheme.

Definicija 4.17. *Neka je P $(d+1) \times (d+1)$ matrica takva da je $(P)_{ij} = p_j(i)$. Matricu P nazivamo* matricom svojstvenih vrijednosti asocijacijske sheme*. Također definiramo matricu Q s $(Q)_{ij} = q_j(i)$ te je nazivamo* matricom dualnih svojstvenih vrijednosti asocijacijske sheme*.*

Ako u (14) uvrstimo (15) umjesto E_j, dobivamo $\sum_{k=0}^{d} p_i(l)q_l(j) = n\delta_{ij}$, tj.

$$PQ = nI. \tag{16}$$

Postoji još jedna važna veza između P i Q.

Definicija 4.18. Stupanj *ili* valenciju *vrha x grafa G definiramo kao broj bridova grafa G koji sadrže vrh x. Ukoliko svaki vrh grafa ima isti stupanj, kažemo da je graf* regularan*.*

Kada je graf regularan onda možemo pričati o stupnju grafa, pritom misleći na stupanj svakog vrha tog grafa. Neka je n_i zbroj elemenata u retku matrice A_i, tj. stupanj grafa G_i, za $i > 0$. Neka je m_j dimenzija svojstvenog potprostora koji je jednak prostoru U_i razapetom stupcima matrice E_j. Tada je očito m_j rang matrice E_j. Kako je E_j idempotentna, onda vrijedi da je $E_j^2 - E_j = 0$ pa su sve svojstvene vrijednosti jednake 0 ili 1. Iz toga slijedi da je $\mathrm{tr}(E_j) = r(E_j) = m_j$.

Definicija 4.19. *Realne brojeve $m_0, \ldots, m_d$ nazivamo* kratnostima sheme*.*

Sada koristeći jednakost (13) te propozicije 4.9 i 4.10 imamo:

$$p_i(j)\mathrm{tr}(E_j) = \mathrm{tr}(p_i(j)E_j) = \mathrm{tr}(A_iE_j) = \langle A_i, E_j \rangle = \mathrm{sum}(A_i \circ E_j).$$

Vidjeli smo ranije da je $A_i \circ E_j = p_i(j)E_j$ te $m_j = tr(E_j)$ pa konačno vrijedi:

$$p_i(j)m_j = p_i(j)\mathrm{tr}(E_j) = \frac{1}{n}q_j(i)\mathrm{sum}(A_i). \tag{17}$$

Znamo da $\mathrm{sum}(A_i)$ predstavlja sumu svih elemenata matrice A_i. Tada je $\frac{1}{n}$ $\mathrm{sum}(A_i)$ suma retka matrice A_i, odnosno n_i. Gornja jednakost može se zapisati kao

$$p_i(j)m_j = q_j(i)n_i.$$

Označimo s Δ_n $(d+1)\times(d+1)$ dijagonalnu matricu s brojevima n_i na dijagonali te s Δ_m $(d+1)\times(d+1)$ dijagonalnu matricu s brojevima m_i na dijagonali. Tada prethodnu jednakost možemo zapisati u terminima matrica P i Q:

$$P^\tau \Delta_m = \Delta_n Q.$$

Osim $p_i(j)$ i $q_j(i)$ kao dualnog para familije parametara povezanih s asocijacijskom shemom, postoji još jedan zanimljiv par. Znamo da je $A_iA_j \in \mathcal{A}$ pa postoje brojevi $p^k_{i,j}$ takvi da je

$$A_iA_j = \sum_{r=0}^{d} p^r_{i,j} A_r. \tag{18}$$

Njih smo prethodno definirali kao presječne brojeve i objasnili zašto su nenegativni cijeli brojevi. Također, s obzirom na to da je $E_i \circ E_j \in \mathcal{A}$, postoje brojevi $q^k_{i,j}$ takvi da je

$$E_i \circ E_j = \frac{1}{n}\sum_{r=0}^{d} q^r_{i,j} E_r.$$

Definicija 4.20. *Brojeve $q^k_{i,j}$ nazivamo* Kreinovim parametrima *asocijacijske sheme.*

Parametre $p^k_{i,j}$ i $q^k_{i,j}$ možemo zapisati u terminima svojstvenih vrijednosti $p_i(j)$. Iz (18) i idempotentnosti matrica A_i imamo:

$$(A_iA_j)\circ A_k = p^k_{i,j}A_k,$$

iz čega slijedi da je

$$\begin{aligned} p^k_{i,j}\cdot\ \mathrm{sum}A_k &= \mathrm{sum}((A_iA_j)\circ A_k) \\ &= \mathrm{tr}((A_iA_j)A_k) \\ &= \mathrm{tr}\left(\sum_{r=0}^{d} p_i(r)p_j(r)p_k(r)E_r\right) \\ &= \sum_{r=0}^{d} p_i(r)p_j(r)p_k(r)m_r. \end{aligned}$$

Na sličan način dobivamo da je

$$\frac{1}{n}q^k_{i,j}m_k = \frac{1}{n^3}\sum_{r=0}^{d} q_i(r)q_j(r)q_k(r)\ \mathrm{sum}A_r,$$

odnosno, ako iskoristimo jednakost (17), imamo

$$q_{i,j}^k = nm_im_j \sum_{r=0}^{d} \frac{p_r(i)p_r(j)p_r(k)}{(\mathrm{sum}A_r)^2}. \tag{19}$$

Sada ćemo dokazati važan rezultat poznat kao Kreinov uvjet.

Definicija 4.21. *Neka su $A = (a_{ij})$ i $B = (b_{ij})$ matrice. Tada se zamjenom elementa a_{ij} matrice A s matricom $a_{ij}B$, za sve i i j, dobiva* Kroneckerov produkt $A \otimes B$.

Teorem 4.22 (Kreinov uvjet)**.** *Kreinovi parametri $q_{i,j}^k$ asocijacijske sheme su nenegativni.*

Dokaz. Znamo da je $E_i \circ E_j = \frac{1}{n}\sum_{k=0}^{d} q_{i,j}^k E_k$, odakle slijedi da su $\frac{1}{n}q_{i,j}^k$ svojstvene vrijednosti od $E_i \circ E_j$. Nadalje,

$$(E_i \otimes E_j)^2 = E_i^2 \otimes E_j^2 = E_i \otimes E_j,$$

stoga su sve svojstvene vrijednosti od $E_i \otimes E_j$ jednake 0 ili 1. S obzirom da su E_i i E_j simetrične, onda je i $E_i \otimes E_j$ simetrična. Iz toga slijedi da je $E_i \otimes E_j$ pozitivno semidefinitna. Matrica $E_i \circ E_j$ je iz definicije očito glavna minora matrice $E_i \otimes E_j$ pa je također semidefinitna. Dakle, sve svojstvene vrijednosti od $E_i \circ E_j$ su nenegativne, što povlači nenegativnost Kreinovih parametara. □

S jedne strane imamo presječne brojeve, matrice A_i te matricu P, dok s druge strane imamo Kreinove parametre, matrice E_i i matricu Q. Ukoliko su presječni brojevi neke asocijacijske sheme $\mathcal{A}$ jednaki Kreinovim parametrima asocijacijske sheme $\mathcal{B}$, tada vrijedi i da su presječni brojevi sheme $\mathcal{B}$ jednaki Kreinovim parametrima sheme $\mathcal{A}$. Kažemo da su takve sheme formalno međusobno dualne.

5 Parametri Johnsonove sheme

Johnsonovu shemu smo spominjali kao važan primjer asocijacijske sheme te smo pronašli vezu s Hammingovom shemom. Pričali smo općenito o parametrima asocijacijske sheme, a sada ćemo vidjeti da za Johnsonovu shemu možemo dati formulu za izračun presječnih brojeva.

Propozicija 5.1. *Presječni brojevi Johnsonove sheme $J(v,k)$ jednaki su*

$$p_{i,j}^l = \sum_{m=0}^{k-l} \binom{k-l}{m}\binom{l}{k-i-m}\binom{l}{k-j-m}\binom{v-k-l}{i+j+m-k}.$$

Dokaz. Neka je V v-člani skup te neka su X i Y dva k-člana podskupa od V koja se sijeku u $k-l$ elemenata. Tada je očito u skupovima X i Y ostalo po l elemenata koji se ne nalaze u njihovom presjeku. Da bismo dobili presječni broj $p^l_{i,j}$, prebrojavamo koliko ima k-članih podskupova Z od V koji se sijeku s X u $k-i$ te s Y u $k-j$ elemenata. Takav skup Z se može sjeći s različitim brojem elemenata iz presjeka skupova X i Y. Označimo taj broj elemenata s m te zatim prebrojavamo u ovisnosti o m. Odabir m elemenata iz skupa $X \cap Y$, koji će biti sadržani u skupu Z, možemo napraviti na $\binom{k-l}{m}$ načina. Trebamo još odabrati $k-i-m$ elemenata iz X i $k-j-m$ iz Y koji se ne nalaze u $X \cap Y$. To možemo napraviti na $\binom{l}{k-i-m}\binom{l}{k-j-m}$ načina. Preostalo je nadopuniti skup Z do k-članog skupa, a to radimo s elementima iz $V \setminus (X \cup Y)$. Elemenata iz $V \setminus (X \cup Y)$ ima $v-(k-l)-l-l = v-k+l-2l = v-k-l$, a preostalo je odabrati $k-(2k-i-j-m) = i+j+m-k$ elemenata. □

Pokazali smo da je za dobivanje matrice svojstvenih vrijednosti P neke asocijacijske sheme potrebno odrediti svojstvene vrijednosti $p_i(j)$. Pomoću formule (16), iz matrice P lako dobijemo i matricu Q koja sadrži dualne svojstvene vrijednosti asocijacijske sheme. Za Johnsonovu shemu možemo izračunati svojstvene vrijednosti pomoću matrica C_i i $W_{i,k}$, koje smo definirali u drugom poglavlju.

Teorem 5.2. *Za Johnsonovu shemu $J(v,k)$ vrijedi:*

$$p_i(j) = \sum_{r=0}^{i} (-1)^{i-r} \binom{k-r}{i-r} \binom{v-k+r-j}{r} \binom{k-j}{r}.$$

Dokaz. Najprije trebamo odrediti svojstvene potprostore Johnsonove sheme da bismo dobili matricu svojstvenih vrijednosti Johnsonove sheme. Sa U_i označimo prostor razapet stupcima matrice $W^{\tau}_{i,k}$. Retci matrice $W_{i,k}$ su linearno nezavisni, pa se U_i podudara s prostorom razapetim stupcima matrice C_i. Iz propozicije 2.19 znamo da je

$$W_{i,j} W_{j,k} = \binom{k-i}{j-i} W_{i,k},$$

iz čega slijedi da je U_{i-1} potprostor od U_i. S T_i označimo ortogonalni komplement od U_{i-1} u U_i. Dimenzija prostora T_i je $\binom{v}{i} - \binom{v}{i-1}$. Tvrdimo da su T_i svojstveni potprostori Johnsonove sheme $J(v,k)$. Iz teorema 2.20 znamo da vrijedi

$$C_i C_j = \sum_{r \le i,j} \binom{v-i-j}{v-k-r} \binom{k-r}{i-r} \binom{k-r}{j-r} C_r. \tag{20}$$

Iz toga slijedi da je U_j C_i-invarijantan, za svaki j. S obzirom na to da su C_i simetrične matrice, slijedi da je prostor T_j C_i-invarijantan. Neka matrica E_j predstavlja ortogonalnu projekciju na T_j. Onda je $C_r E_j = 0$, za $r < j$. Stoga, ako pretpostavimo da je $i \geq j$ te obe strane jednadžbe (20) pomnožimo s E_j zdesna, dobijemo:

$$C_i C_j E_j = \binom{v-i-j}{v-k-j}\binom{k-j}{i-j} C_j E_j.$$

Prostor razapet stupcima matrice $C_j E_j$ je svojstveni potprostor od C_i te kako je prostor razapet stupcima matrice $C_j E_j$ jednak T_j, zaključujemo da su $\binom{v-i-j}{v-k-j}\binom{k-j}{i-j}$ svojstvene vrijednosti od C_i geometrijske kratnosti $\binom{v}{j} - \binom{v}{j-1}$, za $j = 0, \ldots, i$. Budući da C_i ima rang $\binom{v}{k}$, vidimo da je i 0 svojstvena vrijednost s geometrijskom kratnošću $\binom{v}{k} - \binom{v}{i}$. Suma geometrijskih kratnosti svojstvenih vrijednosti koje smo našli je $\binom{v}{k}$ pa zaključujemo da smo pronašli sve svojstvene vrijednosti od C_i s odgovarajućim svojstvenim potprostorima. Sad kada imamo svojstvene vrijednosti od C_i, koristeći korolar 2.16 lako možemo dobiti matricu svojstvenih vrijednosti za $J(v,k)$. Dakle, imamo

$$p_{k-i}(j) = \sum_{r=i}^{k} (-1)^{r-i} \binom{r}{i} \binom{v-r-j}{v-k-j} \binom{k-j}{r-j},$$

iz čega slijedi tvrdnja teorema. $\square$

Primjer 5.3. *Presječne brojeve neke Johnsonove sheme možemo izračunati direktno iz definicije Johnsonove sheme. Tako za Johnsonovu shemu $J(4,2)$, čije smo grafove uz pripadne matrice susjedstva prikazali u primjeru 2.8, dobijemo sljedeće matrice presječnih brojeva:*

$$M_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \; M_1 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \; M_2 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 4 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

U matrici M_k na mjestu (i,j) nalazi se presječni broj $p^k_{i,j}$. S obzirom da vrijedi da je $p^k_{i,j} = p^k_{j,i}$, onda to možemo zapisati i u sažetom obliku u tablici:

k	$p^k_{0,0}$	$p^k_{0,1}$	$p^k_{0,2}$	$p^k_{1,1}$	$p^k_{1,2}$	$p^k_{2,2}$
0	1	0	0	4	0	1
1	0	1	0	2	1	0
2	0	0	1	4	0	0

Sada je lako vidjeti da je primjerice $A_1 \cdot A_2 = p^0_{1,2}A_0 + p^1_{1,2}A_1 + p^2_{1,2}A_2 = A_1$. *Pokažimo da presječne brojeve možemo izračunati i pomoću teorema 5.2. Za to će nam biti potrebna veza presječnih brojeva sa svojstvenim vrijednostima, koju smo spomenuli u prethodnom poglavlju:*

$$p^k_{i,j} sumA_k = \sum_{r=0}^{d} p_i(r)p_j(r)p_k(r)m_r.$$

Za izračun kratnosti imamo zgodnu formulu $\sum_{k=0}^{d} \frac{(p_k(i))^2}{n_k} = \frac{n}{m_i}$, *gdje je u našem slučaju* $n = \binom{4}{2} = 6$. *Brojevi* n_i *redom predstavljaju stupnjeve grafova* G_i *pa je* $n_0 = 1$, $n_1 = 4$, $n_2 = 1$. *Broj* $sumA_k$ *jednak je sumi elemenata matrice* A_k. *Sad kada imamo sve potrebne formule, izračunajmo presječni broj* $p^0_{1,1}$. *Imamo:*

$$\begin{aligned} p^0_{1,1} sumA_0 &= \sum_{r=0}^{2} p_1(r)p_1(r)p_0(r)m_r \\ &= \sum_{r=0}^{2} (p_1(r))^2 m_r \\ &= (p_1(0))^2 m_0 + (p_1(1))^2 m_1 + (p_1(2))^2 m_2. \end{aligned}$$

U drugoj jednakosti koristili smo činjenicu da je $p_0(j) = 1$, *za svaki* j. *Naglasimo još da je* $p_i(0)$ *broj nenul elemenata u bilo kojem retku matrice* A_i *pa ujedno i stupanj grafa* G_i, *tj.* n_i. *Dakle,* $p_1(0) = n_1 = 4$. *Sada možemo pomoću teorema 5.2 izračunati svojstvene vrijednosti koje nam trebaju.*

$$\begin{aligned} p_1(1) &= \sum_{r=0}^{1} (-1)^{1-r} \binom{2-r}{1-r} \binom{4-2+r-1}{r} \binom{2-1}{r} = -2+2=0 \\ p_1(2) &= \sum_{r=0}^{1} (-1)^{1-r} \binom{2-r}{1-r} \binom{2+r-2}{r} \binom{2-2}{r} = -2 \\ p_2(2) &= \sum_{r=0}^{2} (-1)^{2-r} \binom{2-r}{2-r} \binom{2+r-2}{r} \binom{2-2}{r} = 1 \end{aligned}$$

Osim svojstvenih vrijednosti, još moramo odrediti kratnosti m_i.

$$\frac{6}{m_0} = \sum_{k=0}^{2} \frac{(p_k(0))^2}{n_k} = \frac{(p_0(0))^2}{n_0} + \frac{(p_1(0))^2}{n_1} + \frac{(p_2(0))^2}{n_2}$$
$$\frac{6}{m_1} = \sum_{k=0}^{2} \frac{(p_k(1))^2}{n_k} = \frac{(p_0(1))^2}{n_0} + \frac{(p_1(1))^2}{n_1} + \frac{(p_2(1))^2}{n_2}$$
$$\frac{6}{m_2} = \sum_{k=0}^{2} \frac{(p_k(2))^2}{n_k} = \frac{(p_0(2))^2}{n_0} + \frac{(p_1(2))^2}{n_1} + \frac{(p_2(2))^2}{n_2}$$

Odatle slijedi da je $m_0 = 1$, $m_1 = 3$ te $m_2 = 2$. Sada se vratimo na izračun presječnog broja $p^0_{1,1}$. Kada uvrstimo izračunate vrijednosti, dobijemo:

$$p^0_{1,1} = \frac{4^2 \cdot 1 + 0 \cdot 3 + (-2)^2 \cdot 2}{6} = \frac{24}{6} = 4.$$

Usporedimo li dobiveni presječni broj s onim iz tablice, vidimo da smo uistinu dobili istu vrijednost. Analogno bismo računali i preostale presječne brojeve. Za Kreinove parametre sheme $J(4,2)$ koristili bismo formulu (19) te na sličan način došli do odgovarajućih vrijednosti.

Iz primjera 5.3 vidimo da ukoliko imamo zadanu matricu svojstvenih vrijednosti P, lako dobijemo i presječne brojeve i Kreinove parametre sheme. Iz propozicije 5.1 je $p^1_{1,1} = \binom{2-1}{0}\binom{1}{2-1-0}\binom{1}{2-1-0} + \binom{2-1}{1}\binom{1}{2-1-1}\binom{1}{2-1-1} = 2$, što je jednako prethodno izračunatoj vrijednosti u tablici.

Osim jednog od načina za izračun svojstvenih vrijednosti Johnsonove sheme, teorem 5.2 donio nam je važno znanje o svojstvenim potprostorima Johnsonove sheme te je njegova posljedica Delsarteov teorem.

Teorem 5.4 (Delsarte)**.** *Neka je Ω skup svih k-članih podskupova v-članog skupa V te neka je f karakteristična funkcija dizajna $\mathcal{D}$, kojeg promatramo kao podskup od Ω. Tada dizajn $\mathcal{D}$ ima snagu barem t ako i samo ako $E_i f = 0$, za $i = 1, \ldots, t$.*

Dokaz. Pretpostavimo da f ima snagu barem t. Tada je

$$W_{t,k} f = \lambda_t \mathbf{1}$$

za neki λ_t. Dakle, ako su u i v neka dva retka matrice $W_{t,k}$, tada vrijedi jednakost

$$\langle u - v, f \rangle = 0,$$

pa je f ortogonalna na prostor razapet razlikama redaka matrice $W_{t,k}$. Taj prostor je ortogonalni komplement od $\mathbf{1}$, tj. projekcija od f na T_i je jednaka nula za $1 \leq i \leq t$ pa je naš uvjet nužan. Lako se vidi da vrijedi i obrat. $\square$

Literatura

[1] A. E. Brouwer, A. M. Cohen, A. Neumaier, *Distance-Regular Graphs*, Springer-Verlag, 1989.

[2] K. Conrad, *The minimal polynomial and some applications*, dostupno na: `https://kconrad.math.uconn.edu/blurbs/linmultialg/minpolyandappns.pdf` (kolovoz 2021.).

[3] C. D. Godsil, *Algebraic combinatorics*, Chapman & Hall, 1993.

[4] C. D. Godsil, *Linear algebra and designs*, University of Waterloo, 1995.

[5] K. Horvatić, *Linearna algebra*, Golden marketing - Tehnička knjiga, 2004.

[6] Y. J. Ionin, M. S. Shrikhande, *Combinatorics of Symmetric Designs*, Cambridge University Press, 2006.

[7] V. Krčadinac, *Kombinatorika*, predavanja, Sveučilište u Zagrebu, 2021., dostupno na: `https://web.math.pmf.unizg.hr/~krcko/nastava/komb/komb-skripta.pdf` (srpanj 2021.).

[8] V. Krčadinac, *Kvazisimetrični dizajni*, skripta, Sveučilište u Zagrebu, 2017., dostupno na: `https://web.math.pmf.unizg.hr/~krcko/nastava/kvazisim.pdf` (lipanj 2021.).

[9] G. Medina, *How might I typeset the Fano plane in LaTeX?*, Stack Exchange, dostupno na: `https://tex.stackexchange.com/questions/208894/how-might-i-typeset-the-fano-plane-in-latex` (lipanj 2021.).

[10] I. Nakić, *Diskretna matematika*, skripta, Sveučilište u Zagrebu, 2012., dostupno na: `https://web.math.pmf.unizg.hr/nastava/komb/predavanja/predavanja.pdf` (svibanj 2021.).

[11] B. M. Scott, *Prove inversion formula involving binomial coefficients*, *Stack Exchange*, dostupno na: `https://math.stackexchange.com/questions/3834828/prove-inversion-formula-involving-binomial-coefficients` (svibanj 2021.).

[12] M. Spivey, *Beautiful identity*, *Stack Exchange*, dostupno na:
https://math.stackexchange.com/questions/4175/beautiful-identity-sum-k-mn-1k-m-binomkm-binomnk-delta (svibanj 2021.).

[13] R. P. Stanley, *Algebraic Combinatorics*, Springer, 2018.

[14] J. Šiftar, V. Krčadinac, *Konačne geometrije*, skripta, Sveučilište u Zagrebu, 2013., dostupno na:
https://web.math.pmf.unizg.hr/nastava/kg/kg-skripta.pdf (svibanj 2021.).

[15] D. H. Wagner, *Proof of Schur's theorem*, dostupno na:
https://www.math.uh.edu/~wagner/2331/Schurs_theorem.pdf (kolovoz 2021.).

[16] egreg, *Prove that a self adjoint and idempotent matrix is a orthogonal projection matrix*, dostupno na:
https://math.stackexchange.com/questions/2580848/prove-that-a-self-adjoint-and-idempotent-matrix-is-a-orthogonal-projection-matri (kolovoz 2021.).

Sažetak

Neka je V skup od v elemenata i $\Omega = \binom{V}{k}$ familija svih k-članih podskupova od V. Johnsonov graf $J(v, k, i)$ ima Ω kao skup vrhova, a dva vrha su susjedna ako se sijeku u $k - i$ elemenata. Johnsonovi grafovi imaju zanimljiva svojstva koja ih čine asocijacijskom shemom. Skup koji sadrži grafove $G_i = J(v, k, i)$, $i = 0, \ldots, k$ nazivamo Johnsonovom shemom i označavamo s $J(v, k)$. U ovom radu promatramo vezu između Johnsonovih grafova i dizajna, uz pomoć koje dokazujemo Ray-Chaudhurijev i Wilsonov teorem. Na kraju izvodimo parametre Johnsonove sheme i dokazujemo Delsarteov teorem koji povezuje dizajne sa svojstvenim potprostorima Johnsonove sheme.

Summary

Let V be a set of v points and let Ω denote the set of all k-subsets of V. The Johnson graph $J(v, k, i)$ has Ω as vertex set and two vertices are adjacent if they intersect in exactly $k - i$ points. Johnson graphs have interesting properties that make them an association scheme. The set consisting of $G_i = J(v, k, i)$, $i = 0, \ldots, k$ is called Johnson scheme and denoted by $J(v, k)$. In this thesis we explore the relationship between Johnson graphs and designs, with the help of which we prove Ray-Chaudhuri and Wilson's theorem. In the end, we determine parameters of the Johnson scheme and prove Delsarte's theorem, connecting designs with eigenspaces of the Johnson scheme.

Životopis

Katarina Šupe rođena je u Šibeniku 3. srpnja 1995. godine. Završila je Osnovnu školu Juraj Dalmatinac te opći smjer Gimnazije Antuna Vrančića u Šibeniku. U Zagreb se preselila 2013. godine te je upisala preddiplomski sveučilišni studij Matematika na Prirodoslovno-matematičkom fakultetu. Nakon što je 2019. godine završila preddiplomski studij, upisala je diplomski sveučilišni studij Računarstvo i matematika.