

Prirodoslovno - matematički fakultet  
Matematički odsjek  
Združeni doktorski studij matematike

Daniel Šanko

**Međusobno nepristrane Hadamardove matrice i  
asocijacijske sheme**

Zagreb, 17.06.2024.

# Sadržaj

1	Uvod	1
2	Hadamardove matrice Bushovog tipa	2
3	Latinski kvadrati	4
4	Asocijacijske sheme	6
5	Asocijacijske sheme s 5 klasa	8
	Literatura	14
	Prilozi	15

# 1 Uvod

Cilj ovog seminara je pokazati da je egzistencija Hadamardovih matrica Bushovog tipa ekvivalentna egzistenciji asocijacijske sheme s 5 klasa.

Prvo uvodimo pojam Hadamardovih matrica Bushovog tipa. Zatim definiramo međusobno odgovarajuće latinske kvadrate i pokazujemo vezu s Hadamardovim matricama Bushovog tipa, a nakon toga uvodimo i pojam asocijacijske sheme.

U zadnjem poglavlju provodimo dokaze teorema koji govore o ekvivalenciji Hadamardovih matrica Bushovog tipa i asocijacijske sheme s 5 klasa.

## 2 Hadamardove matrice Bushovog tipa

**Definicija 2.1.** Hadamardova matrica reda  $n$  je  $(1, -1)$  - matrica  $H$  za koju je  $HH^T = nI_n$ .

**Primjer 2.2.**

$$H = \begin{bmatrix} - & 1 & 1 & 1 \\ 1 & - & 1 & 1 \\ 1 & 1 & - & 1 \\ 1 & 1 & 1 & - \end{bmatrix},$$

gdje smo radi preglednosti  $s$  - označili  $-1$ .<sup>1</sup>

Dvije Hadamardove matrice  $H_1$  i  $H_2$  reda  $n$  su nepristrane (eng. unbiased) ako je  $H_1H_2^T = \sqrt{n}H_3$ , za neku Hadamardovu matricu  $H_3$ . U tom slučaju je  $n$  nužno potpuni kvadrat. Hadamardovu matricu za koju vrijedi da su sume svih redaka i svih stupaca jednake i iznose  $\sqrt{n}$  nazivamo regularnom.

**Primjer 2.3.** Primjer dviju nepristranih Hadamardovih matrica reda 36 može se naći u [2].

**Teorem 2.4.** [Kharaghani 1985.] Postoji Hadamardova matrica reda  $2n$  ako i samo ako postoji  $2n$   $(1, -1)$  matrica  $C_0, C_1, \dots, C_{2n-1}$  reda  $2n$  takvih da:

1.  $C_i^T = C_i$ ,
2.  $C_iC_j = 0$ ,  $i \neq j$ ,
3.  $C_i^2 = 2nC_i$ ,
4.  $C_0 + C_1 + \dots + C_{2n-1} = 2nI_{2n}$ ,
5. za  $C_0$  možemo uzeti matricu sa svim jedinicama.

*Dokaz.* Neka je  $r_i$   $(i+1)$ -ti redak matrice  $H$ . Stavimo  $C_i = r_i^T r_i$ ,  $i = 0, 1, \dots, 2n-1$ .  $\square$

**Definicija 2.5.** Hadamardova matrica Bushovog tipa je Hadamardova blok matrica  $H = [H_{ij}]$  reda  $4n^2$  s blokovima veličine  $2n$ , takva da vrijedi  $H_{ii} = J_{2n}$  i  $H_{ij}J_{2n} = J_{2n}H_{ij} = 0$ , za  $i \neq j$ ,  $1 \leq i \leq 2n$ ,  $1 \leq j \leq 2n$ , gdje je  $J_{2n}$  matrica reda  $2n$  čiji su svi elementi jednaki 1.

**Primjer 2.6.** Konstruirajmo Hadamardovu matricu Bushovog tipa koristeći konstrukciju iz dokaza Teorema 2.4.

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ 1 & - & - & 1 \end{bmatrix}$$

---

<sup>1</sup>isti zapis biti će korišten i u ostatku teksta

$$C_0 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}, C_1 = \begin{bmatrix} 1 & 1 & - & - \\ 1 & 1 & - & - \\ - & - & 1 & 1 \\ - & - & 1 & 1 \end{bmatrix}, C_2 = \begin{bmatrix} 1 & - & 1 & - \\ - & 1 & - & 1 \\ 1 & - & 1 & - \\ - & 1 & - & 1 \end{bmatrix}, C_3 = \begin{bmatrix} 1 & - & - & 1 \\ - & 1 & 1 & - \\ - & 1 & 1 & - \\ 1 & - & - & 1 \end{bmatrix}$$

Matrica

$$L = \begin{bmatrix} C_0 & C_1 & C_2 & C_3 \\ C_1 & C_0 & C_3 & C_2 \\ C_2 & C_3 & C_0 & C_1 \\ C_3 & C_2 & C_1 & C_0 \end{bmatrix}$$

je Hadamardova matrica Bushovog tipa reda 16.

Skup  $\{H_1, \dots, H_m\}$ ,  $m \geq 2$ , Hadamardovih matrica Bushovog tipa za koji vrijedi da su svake dvije različite matrice nepristrane naziva se skup *međusobno nepristranih Hadamardovih matrica Bushovog tipa* (eng. *mutually unbiased Bush-type Hadamard matrices* (MUBH)). Jedno važno svojstvo Hadamardovih matrica Bushovog tipa je dano u sljedećoj lemi:

**Lema 2.7.** *Neka su  $H_1$  i  $H_2$  dvije međusobno nepristrane Hadamardove matrice Bushovog tipa reda  $4n^2$ . Neka je  $H_3$   $(1, -1)$  - matrica takva da je  $H_1 H_2^T = 2n H_3$ . Onda je  $H_3$  Hadamardova matrica Bushovog tipa.*

*Dokaz.* Neka je  $X = I_{2n} \otimes J_{2n}$ . Onda je  $H_3$  Hadamardova matrica Bushovog tipa ako i samo ako vrijedi  $H_3 X = X H_3 = 2n X$ . Imamo

$$H_3 X = \frac{1}{2n} H_1 H_2^T X = 2n X.$$

Slično,  $X H_3 = 2n X$ . Dakle,  $H_3$  je Hadamardova matrica Bushovog tipa. □

### 3 Latinski kvadrati

**Definicija 3.1.** Latinski kvadrat reda  $n$  je  $n \times n$  matrica sa svojstvom da se svaki od  $n$  simbola  $a_1, \dots, a_n$  pojavljuje točno jednom u svakom retku i u svakom stupcu.

**Primjer 3.2.**

$$\left[ \begin{matrix} 1 \\ \end{matrix} \right], \left[ \begin{matrix} 1 & 2 \\ 2 & 1 \end{matrix} \right], \left[ \begin{matrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{matrix} \right], \left[ \begin{matrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{matrix} \right]$$

**Definicija 3.3.** Latinski kvadrati  $L_1$  i  $L_2$  reda  $n \geq 2$  su ortogonalni ako su svi uređeni parovi koji se dobiju njihovom superimpozicijom međusobno različiti.

**Primjer 3.4.**

$$L_1 = \left[ \begin{matrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{matrix} \right], L_2 = \left[ \begin{matrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{matrix} \right] \xrightarrow{\text{superimpozicija}} \left[ \begin{matrix} 11 & 22 & 33 \\ 23 & 31 & 12 \\ 32 & 13 & 21 \end{matrix} \right]$$

Skup  $\{L_1, \dots, L_t\}$ ,  $t \geq 2$ , latinskih kvadrata reda  $n$  je ortogonalan ako su svaka dva različita kvadrata ortogonalna. Takav skup ortogonalnih kvadrata naziva se skup međusobno ortogonalnih latinskih kvadrata (eng. *mutually orthogonal latin squares* (MOLS)).

**Definicija 3.5.** Latinski kvadrati  $L_1$  i  $L_2$  reda  $n$  su odgovarajući (eng. *suitable*) ako svaka superimpozicija bilo kojeg retka od  $L_1$  na bilo koji redak od  $L_2$  daje samo jedan element oblika  $(a, a)$ .

Skup  $\{L_1, \dots, L_t\}$ ,  $t \geq 2$ , latinskih kvadrata reda  $n$  za koji vrijedi da su svaka dva različita kvadrata odgovarajuća naziva se skup međusobno odgovarajućih latinskih kvadrata (eng. *mutually suitable latin squares* (MSLS)). Ekivalencija MOLS i MSLS dana je u sljedećoj lemi:

**Lema 3.6.** Postoji  $m$  MOLS reda  $n$  ako i samo ako postoji  $m$  MSLS reda  $n$ .

*Dokaz.* Neka su  $L_1$  i  $L_2$  ortogonalni latinski kvadrati reda  $n$  sa elementima  $\{1, 2, \dots, n\}$ . Neka  $((i, j), k)$  označava element na poziciji  $(i, j)$ . Transformacijom  $((i, j), k) \Rightarrow ((k, j), i)$  dobivamo par odgovarajućih latinskih kvadrata. Transformacijom unatrag dobili bi ponovno ortogonalne latinske kvadrate.  $\square$

**Primjer 3.7.** Primjer tri međusobno odgovarajuća latinska kvadrata reda 4:

$$L_1 = \left[ \begin{matrix} 0 & 2 & 3 & 1 \\ 2 & 0 & 1 & 3 \\ 3 & 1 & 0 & 2 \\ 1 & 3 & 2 & 0 \end{matrix} \right], L_2 = \left[ \begin{matrix} 0 & 3 & 1 & 2 \\ 3 & 0 & 2 & 1 \\ 1 & 2 & 0 & 3 \\ 2 & 1 & 3 & 0 \end{matrix} \right], L_3 = \left[ \begin{matrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{matrix} \right]$$

**Propozicija 3.8.** *Ako postoji  $m$  MSLS reda  $2n$ , gdje je  $2n$  red Hadamardove matrice  $H$ , tada postoji  $m$  MUBH reda  $4n^2$ .*

*Dokaz.* Neka su  $C_0, C_1, \dots, C_{2n-1}$  matrice koje odgovaraju normaliziranoj<sup>2</sup> Hadamardovoj matrici  $H$  reda  $2n$ . Neka su svi latinski kvadrati nad skupom elemenata  $\{0, 1, \dots, 2n-1\}$ . Zamjenimo li element  $i$  svakog latinskog kvadrata s matricom  $C_i$ ,  $0 \leq i \leq 2n-1$ , dobili bi  $m$  MUBH reda  $4n^2$ .  $\square$

---

<sup>2</sup>H je normalizirana ako su joj svi elementi u prvom retku i prvom stupcu jednaki 1.

## 4 Asocijacijske sheme

**Definicija 4.1.** Simetrična asocijacijska shema s  $d$  klasa sa  $n$ -članim skupom vrhova  $X$  sastoji se od nenul simetričnih  $(0, 1)$  - matrica  $A_0, A_1, \dots, A_d$  čiji su retci i stupci indeksirani elementima skupa  $X$  takvih da vrijedi:

1.  $A_0 = I_n$ , gdje je  $I_n$  jedinična matrica reda  $n$ .
2.  $\sum_{i=0}^d A_i = J_n$ , gdje je  $J_n$  matrica reda  $n$  čiji su svi elementi jednaki 1.
3. 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  $i, j$ .

Iz svojstva 3. slijedi da matrice  $A_i$  komutiraju. Vektorski prostor razapet tim matricama tvori komutativnu algebru koju ćemo označavati sa  $\mathcal{A}$  i zvat ćemo ju *Bose-Mesnerova algebra*. Postoji baza za  $\mathcal{A}$  sastavljena od primitivnih idempotenta,  $E_0 = (1/n)J_n, E_1, \dots, E_d$ . Kako su  $\{A_0, A_1, \dots, A_d\}$  i  $\{E_0, E_1, \dots, E_d\}$  dvije baze za  $\mathcal{A}$ , onda postoje matrice prijelaza  $P = (P_{ij})_{i,j=0}^d$  i  $Q = (Q_{ij})_{i,j=0}^d$  takve da vrijedi

$$A_j = \sum_{i=0}^d P_{ij} E_i, \quad E_i = \frac{1}{n} \sum_{j=0}^d Q_{ij} A_j.$$

Nadalje, kako matrice  $A_i$  tvore bazu za  $\mathcal{A}$  slijedi da je  $\mathcal{A}$  zatvorena obzirom na množenje po komponentama  $\circ$  (tzv. *Schurov* ili *Hadamardov produkt*). Definiramo *Kreinove parametre*  $q_{ij}^k$  sa

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

Onda je *Kreinova matrica*  $B_i^\circ$  definirana sa  $B_i^\circ = (q_{ij}^k)_{j,k=0}^d$ .

Matrice  $A_i$  su matrice susjedstva grafova  $\mathcal{G}_i$  bez višestrukih bridova. Za asocijacijsku shemu kažemo da je *imprimitivna* ako je barem jedan od grafova  $\mathcal{G}_i$ ,  $i \neq 0$ , nepovezan. Tada postoji skup indeksa  $\mathcal{I}$  takav da su 0 i odgovarajući indeks  $i$  elementi skupa  $\mathcal{I}$ , te vrijedi  $\sum_{j \in \mathcal{I}} A_j = I_p \otimes J_q$ , za neke  $p$  i  $q$  takve da je  $1 < p < n$ . Dakle,  $n$ -člani skup vrhova  $X$  je particioniran na  $p$  podskupova veličine  $q$  koje zovemo *vlakna*. Skup  $\mathcal{I}$  definira relaciju ekvivalencije  $\sim$  na skupu  $\{0, 1, \dots, d\}$ ,  $j \sim k$  ako i samo ako je  $p_{ij}^k \neq 0$  za neki  $i \in \mathcal{I}$ . Neka su  $\mathcal{I}_0 = \mathcal{I}, \mathcal{I}_1, \dots, \mathcal{I}_t$  klase ekvivalencije na  $\{0, 1, \dots, d\}$  obzirom na relaciju  $\sim$ . Onda iz Teorema 9.4 u [3] slijedi da postoje  $(0, 1)$  - matrice  $\bar{A}_j$  ( $0 \leq j \leq t$ ) takve da vrijedi

$$\sum_{i \in \mathcal{I}_j} A_i = \bar{A}_j \otimes J_q,$$

i te matrice definiraju asocijacijsku shemu nad skupom vlakana koju zovemo *kvocijentna asocijacijska shema* obzirom na  $\mathcal{I}$ .

Za vlakna  $U$  i  $V$  označimo sa  $\mathcal{I}(U, V)$  skup indeksa matrica susjedstva  $A_i$  sa  $(A_i)_{u,v}$  za neke  $u \in U, v \in V$ . Definiramo  $(0, 1)$  - matricu  $A_i^{UV}$  sa

$$(A_i^{UV})_{xy} = \begin{cases} 1, & \text{ako je } (A_i)_{xy} = 1, x \in U, y \in V, \\ 0, & \text{inače.} \end{cases}$$



**Definicija 4.2.** Za imprimitivnu asocijacijsku shemu kažemo da je uniformna ako pripadna kvocijentna asocijacijska shema ima jednu klasu i postoje cijeli brojevi  $a_{ij}^k$  takvi da za sva vlakna  $U, V, W$ ,  $i \in \mathcal{I}(U, V)$ ,  $j \in \mathcal{I}(V, W)$  imamo

$$A_i^{UV} A_j^{VW} = \sum_k a_{ij}^k A_k^{UW}.$$

## 5 Asocijacijske sheme s 5 klasa

Neka je  $\{H_1, H_2, \dots, H_m\}$ ,  $m \geq 2$ , skup međusobno nepristranih regularnih Hadamardovih matrica (MURH) reda  $4n^2$ . Označimo sa

$$M = \begin{bmatrix} I \\ H_1/2n \\ H_2/2n \\ \vdots \\ H_m/2n \end{bmatrix} \begin{bmatrix} I & H_1^\tau/2n & H_2^\tau/2n & \dots & H_m^\tau/2n \end{bmatrix}$$

Gramovu matricu skupa matrica  $\{I, \frac{1}{2n}H_1, \frac{1}{2n}H_2, \dots, \frac{1}{2n}H_m\}$ . Neka je  $B = 2n(M - I)$ . Onda je  $B$  simetrična  $(0, -1, 1)$  - matrica. Neka je

$$B = B_1 - B_2,$$

gdje su  $B_1$  i  $B_2$  disjunktne  $(0, 1)$  - matrice. Vrijedi sljedeće:

**Lema 5.1.** *Neka su  $I = I_{4n^2(m+1)}$ ,  $B_1, B_2$  i  $B_3 = I_{m+1} \otimes J_{4n^2} - I_{4n^2(m+1)}$  matrice. Te matrice tvore asocijacijsku shemu s 3 klase.*

*Dokaz.* Presječne brojeve možemo iščitati iz sljedećih jednažbi:

$$\begin{aligned} B_1^2 &= (2n^2 + n)mI + (n^2 + \frac{3}{2}n)(m-1)B_1 + (n^2 + \frac{1}{2}n)(m-1)B_2 + (n^2 + n)B_3, \\ B_2^2 &= (2n^2 - n)mI + (n^2 - \frac{1}{2}n)(m-1)B_1 + (n^2 - \frac{3}{2}n)(m-1)B_2 + (n^2 - n)B_3, \\ B_1B_2 &= (n^2 - \frac{1}{2}n)(m-1)B_1 + (n^2 + \frac{1}{2}n)(m-1)B_2 + n^2mB_3, \\ B_1B_3 &= (2n^2 + n - 1)B_1 + (2n^2 + n)B_2, \\ B_2B_3 &= (2n^2 - n)B_1 + (2n^2 - n - 1)B_2. \end{aligned}$$

□

U nastavku smatramo da su sve matrice  $H_i, i = 1, 2, \dots, m$ , Hadamardove matrice Bushovog tipa. Iz Leme 2.7 slijedi da možemo dodati još dvije klase pa imamo sljedeći rezultat:

**Teorem 5.2.** *Neka su  $B_1$  i  $B_2$  matrice definirane kao ranije. Neka vrijedi:*

- $A_0 = I_{4n^2(m+1)}$ ,
- $A_1 = I_{m+1} \otimes I_{2n} \otimes (J_{2n} - I_{2n})$ ,
- $A_2 = I_{m+1} \otimes (J_{2n} - I_{2n}) \otimes J_{2n}$ ,

- $A_3 = (J_{m+1} - I_{m+1}) \otimes I_{2n} \otimes J_{2n}$ ,
- $A_4 = B_1 - A_3$ ,
- $A_5 = B_2$ .

Tada  $A_0, A_1, A_2, A_3, A_4$  i  $A_5$  tvore asocijacijsku shemu s 5 klasa.

*Dokaz.* Odredit ćemo presječne brojeve koristeći neke od relacija iz Leme 5.1. Primjetimo da su  $A_0 + A_1$ ,  $A_3$  i  $A_0 + A_1 + A_2$  blok matrice s blokovima veličina  $2n$ ,  $2n$  i  $4n^2$  respektivno, gdje je svaki blok ili nul matrica ili matrica sa svim elementima jednakim 1. S druge strane,  $A_4$  i  $A_5$  su blok matrice s blokovima veličine  $2n$ , gdje je svaki blok ili nul matrica ili matrica za koju vrijedi da je suma svakog retka i suma svakog stupca jednaka  $n$ . Sada imamo sljedeće:

$$\begin{aligned}
A_1A_1 &= (2n-1)A_0 + (2n-2)A_1. \\
A_1A_2 &= (2n-1)A_2. \\
A_1A_3 &= (2n-1)A_3. \\
A_1A_4 &= (n-1)A_4 + nA_5. \\
A_1A_5 &= nA_4 + (n-1)A_5. \\
A_2A_2 &= 2n(2n-1)A_0 + 2n(2n-1)A_1 + 2n(2n-2)A_2. \\
A_2A_3 &= 2n(A_4 + A_5). \\
A_2A_4 &= (2n-1)nA_3 + (2n-2)n(A_4 + A_5). \\
A_2A_5 &= (2n-1)nA_3 + (2n-2)n(A_4 + A_5). \\
A_3A_3 &= 2mn(A_0 + A_1) + 2n(m-1)A_3. \\
A_3A_4 &= mnA_2 + (m-1)n(A_4 + A_5). \\
A_3A_5 &= mnA_2 + (m-1)n(A_4 + A_5).
\end{aligned}$$

Koristeći to, činjenicu da vrijedi  $A_3 + A_4 = B_1$  i  $A_5(A_3 + A_4) = B_2B_1$ , te presječne brojeve iz Leme 5.1 dobivamo:

$$\begin{aligned}
A_4A_5 &= n^2mA_1 + m(n^2 - n)A_2 + (n^2 - \frac{n}{2})(m-1)A_3 + \\
&+ (n^2 - \frac{3n}{2})(m-1)A_4 + (n^2 - \frac{n}{2})(m-1)A_5.
\end{aligned}$$

Konačno, primjetimo da je  $A_4 - A_5$  blok matrica s blokovima veličine  $2n$ , gdje je svaki blok ili nul matrica ili matrica čije su sume redaka i stupaca jednake nuli. Odavdje slijedi da je

$$(A_4 + A_5)(A_4 - A_5) = 0,$$

pa imamo

$$\begin{aligned}
A_4A_4 &= A_5A_5 = (2n^2 - n)mA_0 + (n^2 - n)m(A_1 + A_2) + \\
&+ (n^2 - \frac{n}{2})(m-1)(A_3 + A_4) + (n^2 - \frac{3n}{2})(m-1)A_5.
\end{aligned}$$

□

**Napomena 5.3.** *Asocijacijska shema s 5 klasa je uniformna. Svaka dva vlakna definiraju koherentnu konfiguraciju. Svojstvene matrice i matrica  $B_5^\circ$  su:*

$$P = \begin{bmatrix} 1 & 2n-1 & 2n(2n-1) & 2nm & n(2n-1)m & n(2n-1)m \\ 1 & -1 & 0 & 0 & nm & -nm \\ 1 & 2n-1 & -2n & 2nm & -nm & -nm \\ 1 & 2n-1 & -2n & -2n & n & n \\ 1 & -1 & 0 & 0 & -n & n \\ 1 & 2n-1 & 2n(2n-1) & -2n & -n(2n-1) & -n(2n-1) \end{bmatrix},$$

$$Q = \begin{bmatrix} 1 & 2n(2n-1) & 2n-1 & (2n-1)m & 2n(2n-1)m & m \\ 1 & -2n & 2n-1 & (2n-1)m & -2nm & m \\ 1 & 0 & -1 & -m & 0 & m \\ 1 & 0 & 2n-1 & -2n+1 & 0 & -1 \\ 1 & 2n & -1 & 1 & -2n & -1 \\ 1 & -2n & -1 & 1 & 2n & -1 \end{bmatrix},$$

$$B_5^\circ = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & m & m-1 & 0 & 0 \\ 0 & m & 0 & 0 & m-1 & 0 \\ m & 0 & 0 & 0 & 0 & m-1 \end{bmatrix}.$$

**Napomena 5.4.** *Svojstvene matrice i matrica  $B_1^\circ$  asocijacijske sheme s tri klase su:*

$$P = \begin{bmatrix} 1 & n(2n+1)m & n(2n-1)m & 4n^2-1 \\ 1 & nm & -nm & -1 \\ 1 & -n & n & -1 \\ 1 & -n(2n+1) & -n(2n-1) & 4n^2-1 \end{bmatrix},$$

$$Q = \begin{bmatrix} 1 & 4n^2-1 & (4n^2-1)m & m \\ 1 & 2n-1 & -2n+1 & 1 \\ 1 & -2n-1 & 2n+1 & 1 \\ 1 & -1 & -m & m \end{bmatrix},$$

$$B_1^\circ = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 4n^2-1 & \frac{2(2n^2-m-1)}{m+1} & \frac{4n^2}{m+1} & 0 \\ 0 & \frac{4n^2m}{m+1} & \frac{(4n^2-2)m-2}{m+1} & 4n^2-1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

*Iz Teorema 5.8 u [4] slijedi da ova asocijacijska shema dolazi od SSSD-a.<sup>3</sup>*

Konačno, pokažimo da vrijedi obrat Teorema 5.2:

---

<sup>3</sup>Sustav spojenih simetričnih dizajna; Definicija 4.36 u [5]

**Teorem 5.5.** *Pretpostavimo da postoji asocijacijska shema sa svojstvenim matricama  $P$  i  $Q$  kao u Napomeni 5.3. Tada postoji skup MUBH  $\{H_1, \dots, H_m\}$  reda  $4n^2$ .*

*Dokaz.* Neka su  $A_0, A_1, \dots, A_5$  matrice susjedstva koje tvore asocijacijsku shemu čije su svojstvene matrice  $P$  i  $Q$ . Neka je  $B_0 = A_0$ ,  $B_1 = A_3 + A_4$ ,  $B_2 = A_5$  i  $B_3 = A_1 + A_2$ . Po Napomeni 5.4 matrice  $B_i$  tvore SSSD. Presložimo vrhove tako da je  $B_3 = I_{m+1} \otimes J_{4n^2} - I_{4n^2(m+1)}$ .

Prvo određujemo oblik matrice  $A_3$ . Kako je  $A_1$  matrica susjedstva imprimitivnog jako regularnog grafa sa svojstvenim vrijednostima  $2n - 1$  i  $-1$  čije su kratnosti  $2n(m+1)$  i  $2n(2n-1)(m+1)$ , onda  $A_1$  nakon preslagivanja vrhova postaje  $I_{2n(m+1)} \otimes (J_{2n} - I_{2n})$ . Kako je  $B_3 = I_{m+1} \otimes J_{4n^2} - I_{4n^2(m+1)} = A_1 + A_2$ , onda  $A_2$  ima željeni oblik. Nadalje, kako su  $B_3$  i  $A_3$  disjunktne i  $A_2 A_3 = 2n(A_4 + A_5)$ , dobivamo  $A_3 = (J_{m+1} - I_{m+1}) \otimes I_{2n} \otimes J_{2n}$ .

Neka je  $G = (m+1)(E_0 + E_1 + E_2)$ . Imamo

$$\begin{aligned} G &= (m+1)(E_0 + E_1 + E_2) \\ &= \frac{1}{4n^2} \sum_{i=0}^5 (Q_{0,i} + Q_{1,i} + Q_{2,i}) A_i \\ &= A_0 + \frac{1}{2n} A_3 + \frac{1}{2n} A_4 - \frac{1}{2n} A_5. \end{aligned}$$

Kako je  $A_3 + A_4 + A_5 = (J_{m+1} - I_{m+1}) \otimes J_{2n} \otimes I_{2n}$ ,  $G$  je oblika

$$G = \begin{bmatrix} I_{4n^2} & \frac{1}{2n} H_{1,2} & \cdots & \frac{1}{2n} H_{1,m+1} \\ \frac{1}{2n} H_{2,1} & I_{4n^2} & \cdots & \frac{1}{2n} H_{2,m+1} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{2n} H_{m+1,1} & \frac{1}{2n} H_{m+1,2} & \cdots & I_{4n^2} \end{bmatrix},$$

gdje je  $H_{i,j}$  ( $i \neq j$ )  $(1, -1)$ -matrica.

Tvrdimo da su  $H_k := H_{k+1,1}$  ( $1 \leq k \leq m$ ) MUBH. Označimo sa  $\bar{A}$  podmatricu od  $A$  čiji su elementi u retcima i stupcima prvog i  $(k+1)$  bloka. Promatramo glavnu podmatricu  $\bar{G}$ . Kako je asocijacijska shema uniformna, stavljajući  $m = 1$  i restrikcijom na indekse prvog i drugog bloka dobivamo asocijacijsku shemu sa svojstvenom matricom  $\bar{P} = (\bar{P}_{ij})_{i,j=0}^5$ .

Kako je  $\bar{G} = (m+1)(\bar{E}_0 + \bar{E}_1 + \bar{E}_2)$  i  $\frac{m+1}{2} \bar{E}_i$  ( $i = 0, 1, 2$ ) su primitivne idempotentne dobivene podsheme, imamo  $\bar{G}^2 = 2\bar{G}$ . Iz  $\bar{G} = \begin{bmatrix} I_{4n^2} & \frac{1}{2n} H_k^\tau \\ \frac{1}{2n} H_k & I_{4n^2} \end{bmatrix}$  slijedi

$$\begin{bmatrix} I_{4n^2} + \frac{1}{4n^2} H_k^\tau H_k & \frac{1}{n} H_k^\tau \\ \frac{1}{n} H_k & I_{4n^2} + \frac{1}{4n^2} H_k H_k^\tau \end{bmatrix} = \begin{bmatrix} 2I_{4n^2} & \frac{1}{n} H_k^\tau \\ \frac{1}{n} H_k & 2I_{4n^2} \end{bmatrix}.$$

Oдавдје slijedi da je  $H_k$  Hadamardova matrica reda  $4n^2$ .

Pokažimo sada da je  $H_k$  Bushovog tipa. Imamo

$$\begin{aligned}
\overline{A_3}\overline{G} &= (m+1)\overline{A_3}(\overline{E_0} + \overline{E_1} + \overline{E_2}) \\
&= (m+1)\left(\sum_{i=0}^5 \overline{P_{i3}}\overline{E_i}\right)(\overline{E_0} + \overline{E_1} + \overline{E_2}) \\
&= (m+1)\left(\sum_{i=0}^2 \overline{P_{i3}}\overline{E_i}\right) \\
&= 2n(m+1)(\overline{E_0} + \overline{E_2}) \\
&= 2n(m+1)\left(\frac{1}{4n^2(m+1)}\sum_{i=0}^5(\overline{Q_{i,0}} + \overline{Q_{i,2}})\overline{A_i}\right) \\
&= (A_0 + A_1 + A_3) \\
&= \begin{bmatrix} I_{2n} \otimes J_{2n} & I_{2n} \otimes J_{2n} \\ I_{2n} \otimes J_{2n} & I_{2n} \otimes J_{2n} \end{bmatrix}.
\end{aligned} \tag{1}$$

S druge strane,

$$\begin{aligned}
\overline{A_3}\overline{G} &= \begin{bmatrix} 0 & I_{2n} \otimes J_{2n} \\ I_{2n} \otimes J_{2n} & 0 \end{bmatrix} \begin{bmatrix} I_{4n^2} & \frac{1}{2n}H_k^\tau \\ \frac{1}{2n}H_k & I_{4n^2} \end{bmatrix} \\
&= \begin{bmatrix} \frac{1}{2n}(I_{2n} \otimes J_{2n})H_k & I_{2n} \otimes J_{2n} \\ I_{2n} \otimes J_{2n} & \frac{1}{2n}(I_{2n} \otimes J_{2n})H_k^\tau \end{bmatrix}.
\end{aligned} \tag{2}$$

Uspoređujući (1) i (2) dobijemo

$$(I_{2n} \otimes J_{2n})H_k = (I_{2n} \otimes J_{2n})H_k^\tau = 2n(I_{2n} \otimes J_{2n}).$$

Iz Leme 2.7 slijedi da je  $H_k$  Hadamardova matrica Bushovog tipa.

Konačno, pokažimo da su matrice  $H_1, \dots, H_m$  međusobno nepristrane. Neka su  $k, k' \in \mathbb{N}$  takvi da je  $1 \leq k < k' \leq m$ . Označimo sa  $\tilde{A}$  podmatricu vrhova koji leže u retcima i stupcima prvog,  $(k+1)$  i  $(k'+1)$  bloka. Onda je  $\tilde{G}^2 = 3\tilde{G}$ . Uspoređujući (2, 3) - blok, dobivamo

$$\frac{1}{4n^2}H_kH_{k'}^\tau + \frac{1}{2n}I_{4n^2}H_{k+1,k'+1} + \frac{1}{2n}H_{k+1,k'+1}I_{4n^2} = \frac{3}{2n}H_{k+1,k'+1},$$

odnosno  $\frac{1}{4n^2}H_kH_{k'}^\tau = \frac{1}{2n}H_{k+1,k'+1}$ . Kako je  $H_{k+1,k'+1}$   $(1, -1)$  - matrica, slijedi da su  $H_k$  i  $H_{k'}$  nepristrane.  $\square$

**Primjer 5.6.** *Konstruirajmo asocijacijsku shemu s 3 klase koristeći Lemu 5.1. U [6] na stranici 164 dani su prvi retci 5 MOLS-a:*

$$\begin{aligned}
L_1 &: 00 01 02 03 04 05 10 11 12 13 14 15 \\
L_2 &: 00 03 10 01 13 15 02 12 05 04 11 14 \\
L_3 &: 00 12 01 15 05 13 03 14 02 11 10 04 \\
L_4 &: 00 04 15 14 02 11 12 10 13 01 03 05 \\
L_5 &: 00 10 12 02 11 01 13 15 04 14 05 03
\end{aligned}$$

*Svaki se latinski kvadrat dobije razvijanjem prvog retka nad  $\mathbb{Z}_2 \times \mathbb{Z}_6$ . Element grupe  $(x, y)$  zapisujemo kao  $xy$ .*

U Prilogu 1 nalazi se kod za računalni program GAP za konstrukciju asocijacijske sheme s 3 klase iz 5 MOLS-a.

**Primjer 5.7.** *Koristeći MSLS-e  $L_1, L_2$  i  $L_3$  iz Primjera 3.7 i Hadamardovu matricu  $H$  iz Primjera 2.6 konstruirajmo asocijacijsku shemu s 5 klasa.*

Koristimo Propoziciju 3.8 i Teorem 5.2. U Prilogu 2 nalazi se kod za računalni program GAP za konstrukciju asocijacijske sheme s 5 klasa iz 3 MSLS-a.

## Literatura

- [1] H. Kharaghani, S. Sasani, S. Suda, Mutually unbiased bush-type Hadamard matrices and association schemes. *Electron. J. Comb.* 22, No. 3, Research Paper P3.10, 11 p. (2015).
- [2] W. H. Holzmann, H. Kharaghani, W. Orrick, On the real unbiased Hadamard matrices. *Combinatorics and Graphs*, 243-250, *Contemp. Math.*, 531, Amer. Math. Soc., Providence, RI, 2010.
- [3] E. Bannai, T. Ito, *Algebraic Combinatorics I: Association Schemes*, Benjamin/Cummings, Menro Park, CA, 1984.
- [4] E. van. Dam, Three-class association schemes, *J. Algebraic. Combin.* 10(1) (1999), 69-107
- [5] V. Krčadinac, *Asocijacijske sheme*, Sveučilište u Zagrebu, 2024.
- [6] C. J. Colbourn, J. H. Dinitz, (Eds.). (2006). *Handbook of Combinatorial Designs* (2nd ed.). Chapman and Hall/CRC.



# Prilozi

Prilog 1. Kod za konstrukciju asocijacijske sheme s 3 klase za računalni program GAP (Primjer 5.6)

```
LoadPackage("AssociationSchemes");
LoadPackage("PAG");

L1:=[00, 01, 02, 03, 04, 05, 10, 11, 12, 13, 14, 15];;
L2:=[00, 03, 10, 01, 13, 15, 02, 12, 05, 04, 11, 14];;
L3:=[00, 12, 01, 15, 05, 13, 03, 14, 02, 11, 10, 04];;
L4:=[00, 04, 15, 14, 02, 11, 12, 10, 13, 01, 03, 05];;
L5:=[00, 10, 12, 02, 11, 01, 13, 15, 04, 14, 05, 03];;

bb:=List([L1,L2,L3,L4,L5],y->List(y,x->[Int(x/10),x mod 10]));
g:=Cartesian([0,1],[0..5]);
tols:=l->List(List(g,x->x+1),x->List(x,y->(y[1] mod 2)*6+(y[2] mod 6)+1));
mols12:=List(bb,tols);

AreMOLS(mols12);
ToMSLS:=l->OrthogonalArrayToMOLS(List(MOLSToOrthogonalArray([1]),x->x{[3,2,1]}))[1];
msls12:=List(mols12,ToMSLS);

h:=Paley1Mat(11);
d1:=DiagonalMat([-1,1,1,1,1,1,1,1,1,1,1]);
hn:=(-d1)*h*d1;
ToC:=h->List(h,x->TransposedMat([x])*[x]);
c:=ToC(hn);

lstrans:=l->MatrixByBlockMatrix(BlockMatrix(Concatenation(List(
[1..12],i->List([1..12],j->[i,j,c[l[i,j]]]))),12,12));
mubh:=List(mols12,lstrans);

mc:=Concatenation(Concatenation([IdentityMat(144)],mubh/12));;
M:=mc*TransposedMat(mc);;
B:=12*(M-IdentityMat(864));;
B1:=List(B,x->List(x,y->IversonBracket(y=1)));;
B2:=List(B,x->List(x,y->IversonBracket(y=-1)));;
I:=IdentityMat(864);;
B3:=KroneckerProduct(IdentityMat(6),AllOnesMat(144))-I;
c:=B1+2*B2+3*B3;
a:=AssociationScheme(c);
```

Prilog 2. Kod za konstrukciju asocijacijske sheme s 5 klasa za računalni program GAP (Primjer 5.7)

```

LoadPackage("AssociationSchemes");
LoadPackage("PAG");

L1:=[0,2,3,1],[2,0,1,3],[3,1,0,2],[1,3,2,0];;
L2:=[0,3,1,2],[3,0,2,1],[1,2,0,3],[2,1,3,0];;
L3:=[0,1,2,3],[1,0,3,2],[2,3,0,1],[3,2,1,0];;

L:=[L1,L2,L3];;

m:=3;; # koliko MSLS-a imamo
n:=2;; # red MSLS je 2n = 4 --> n = 2

H:=[[1,1,1,1],[1,1,-1,-1],[1,-1,1,-1],[1,-1,-1,1]];;

ToC:=h->List(h,x->TransposedMat([x])*[x]);
C:=ToC(H);

lstrans:=l->MatrixByBlockMatrix(BlockMatrix(Concatenation(List([1..4],i->List([1..4],j
MUBHs:=List(L,lstrans);

H1:=MUBHs[1];;
H2:=MUBHs[2];;
H3:=MUBHs[3];;

I:=IdentityMat(16);;
mc:=Concatenation(Concatenation([IdentityMat(16)],MUBHs/4));;
M:=mc*TransposedMat(mc);;
B:=4*(M-IdentityMat(64));;
B1:=List(B,x->List(x,y->IversonBracket(y=1)));;
B2:=List(B,x->List(x,y->IversonBracket(y=-1)));;

A0:=IdentityMat(4*n^2*(m+1));;
A1:=KroneckerProduct(KroneckerProduct(
IdentityMat(m+1),IdentityMat(2*n)),
AllOnesMat(2*n)-IdentityMat(2*n));;
A2:=KroneckerProduct(KroneckerProduct(
IdentityMat(m+1),AllOnesMat(2*n)-IdentityMat(2*n)),
AllOnesMat(2*n));;
A3:=KroneckerProduct(KroneckerProduct(
AllOnesMat(m+1)-IdentityMat(m+1),

```

```
IdentityMat(2*n)),  
AllOnesMat(2*n));;  
A4:=B1-A3;;  
A5:=B2;;  
  
AS:=[A0,A1,A2,A3,A4,A5];;  
  
mat:=Sum([0..5],i->i*AS[i+1]);;  
  
shema:=AssociationScheme(mat);  
  
P:=CharacterTableOfHomogeneousCoherentConfiguration(shema);;
```