Szimmetrikus kombinatorikus struktúrák MSc hallgatók számára

Hadamard-mátrixok

Előadó: Hajnal Péter 2. hét

1. Hadamard-mátrixok

Ezen az előadáson látásra a blokkrendszerektől független kombinatorikus struktúrákat vizsgálunk. Vizsgálataink során azonban a blokkrendszerekkel való szoros kapcsolatra is rávilágítunk.

Definíció. Egy $n \times n$ méretű H mátrixot, amelynek minden eleme ± 1 és sorai páronként ortogonálisak, *Hadamard-mátrixnak* nevezünk.

Példa. Az

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{és} \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

mátrixok Hadamard-mátrixok.

Először a definíció néhány ekvivalensét tárgyaljuk.

1. Lemma. *Legyen H egy $n \times n$-es mátrix -1 és 1 elemekkel. Ekkor a következők ekvivalensek:*

(i) H *Hadamard-mátrix,*

(ii) $HH^T = nI$,

(iii) $|\det H| = n^{\frac{n}{2}}$.

Bizonyítás. $(i) \Rightarrow (ii)$: A mátrixazonosság annak a triviális átfogalmazása, hogy a sorok ortogonálisak és minden sorvektorának hossznégyzete n.

$(ii) \Rightarrow (iii)$: $(\det H)^2 = \det(HH^T) = \det nI = n^n$. Ebből $|\det H| = n^{n/2}$.

$(iii) \Rightarrow (i)$: $|\det K| \leq |k_1| \cdot |k_2| \cdot \ldots \cdot |k_n|$, ahol a k_i vektorok a K mátrix sorai. ($\det K$ a K sorai által adott vektorok által feszített paralellepipedon térfogata, $|k_1| \cdot |k_2| \cdot \ldots \cdot |k_n|$ a paralellepipedon élei hosszának szorzata.) Ezt H-ra alkalmazva kapjuk, hogy $|\det H| \leq (\sqrt{n})^n = n^{n/2}$. Egyenlőség akkor és csak akkor teljesül, ha a sorok ortogonálisak. ■

Megjegyzés. $HH^T = nI$ egyenlőségből adódik, hogy $H^T H = nI$, azaz H oszlopai is ortogonálisak.

Az alapkérdés a szokásos: Milyen n-re létezik $n \times n$-es Hadamard-mátrix? Az is a szokásos, hogy a látszólag ártatlan kérdes mind a mai napig nincs tisztázva. A következő lemma azt a egyetlen és szinte triviális feltételt írja le, ami ismereteink szerint szükséges Hadamard-mátrixok létezéséhez.

2. Lemma. *Legyen H egy $n \times n$-es Hadamard-mátrix. Ekkor $n = 1, 2$ vagy $4|n$.*

Bizonyítás. Tegyük fel, hogy $n \geq 3$. Egy Hadamard-mátrix tetszőleges oszlopát (vagy sorát) -1-gyel szorozva Hadamard-mátrixot kapunk. Így feltehető, hogy H első sora csupa 1-est tartalmaz. Ebből következik, hogy H tetszőleges másik sora ugyanannyi 1-est tartalmaz, mint -1-est. (Speciálisan n páros, $n = 2k$.) Az oszlopok átrendezésével elérhetjük, hogy a második sor első k eleme 1-es, a második k eleme -1-es. A harmadik sorban legyen α darab 1-es az első k pozíció között. Mivel a teljes sor $n/2 = k$ darab 1-est tartalmaz, ezért a második k pozícióban $k - \alpha$ darab 1-es van. Így a második és a harmadik sor skaláris szorzata $0 = \alpha - (k - \alpha) - (k - \alpha) + \alpha = 4\alpha - 2k = 4\alpha - n$. ■

Sejtés. Minden $4|n$ esetén létezik $n \times n$-es Hadamard-mátrix.

⋆

A következőkben Hadamard-mátrixok egy nagyon egyszerű konstrukcióját ismertetjük.

Definíció. Legyen A egy $n \times n$-es és B egy $m \times m$-es mátrix. Soraik legyenek azonosítva az A_s és B_s halmazzal, oszlopaik pedig legyenek azonosítva az A_o és B_o halmazzal. $\sigma \in A_s$ es $\omega \in A_o$ esetén az A mátrix megfelelő pozíciójában álló elemet $A_{\sigma,\omega}$-val jelöljük. A két mátrix *tenzor vagy Kronecker-szorzata* $A \otimes B$ a következő mátrix: $A \otimes B$ mérete $mn \times mn$. Sorai az $A_s \times B_s$ és oszlopai az $A_o \times B_o$ halmazzal vannak azonosítva. $(\sigma, \sigma') \in A_s \times B_s$ és $(\omega, \omega') \in A_o \times B_o$ párok által leírt sor és oszlop találkozásában álló elem $A_{\sigma,\omega} B_{\sigma',\omega'}$.

Megjegyzés. Legyen A egy $n \times n$ méretű és B egy $m \times m$ méretű -1-1 mátrix. Ekkor $A \otimes B$-t úgy kapjuk, hogy a B mátrix 1 értékű elemeit A egy példányával, míg a -1 elemeket $-A$ egy példányával helyettesítjük.

3. Lemma. *Legyen A és B két Hadamard-mátrix. Ekkor $A \otimes B$ is Hadamard-mátrix.*

4. Lemma. *Válasszunk ki két különböző sort $A \otimes B$-ből: (σ, σ')-t és (τ, τ')-t ($\sigma \neq \tau$ vagy $\sigma' \neq \tau'$). A két sor belső szorzata*

$$\sum_{(\omega,\omega') \in A_o \times B_o} (A_{\sigma,\omega} B_{\sigma',\omega'}) (A_{\tau,\omega} B_{\tau',\omega'}) = \left(\sum_{\omega \in A_o} A_{\sigma,\omega} A_{\tau,\omega} \right) \left(\sum_{\omega' \in B_o} B_{\sigma',\omega'} B_{\tau',\omega'} \right).$$

A két sor különbözősége, továbbá A és B Hadamard-mátrix volta miatt legalább az egyik tényező értéke 0 lesz. Így a szorzat is 0.

5. Következmény. *Létezik $2^k \times 2^k$ méretű Hadamard-mátrix.*

Bizonyítás. $H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ egy 2×2-es Hadamard-mátrix. Az előző lemmát alkalmazva $H_2 = H_1 \otimes H_1, \ldots, H_i = H_1 \otimes H_{i-1}, \ldots$ sorozat mindegyik tagja is Hadamard-mátix. H_i mérete $2^i \times 2^i$. ■

Megjegyzés. A H_n mátrix nemcsak rekurzívan, hanem közvetlenül is definiálható: H_n mátrixnak 2^n sora és 2^n oszlopa van. Sorai és oszlopai azonosíthatók az n-elemű halmaz összes részhalmazával. Egy S halmaz sorának és egy T halmaz oszlopának metszetében álló elem $(-1)^{|S \cap T|}$. Ezen definíció alapján közvetlen is igazolható, hogy H_n egy Hadamard-mátrix.

$\star$

Az alábbiakban Hadamard-mátrixok egy számelméleti konstrukcióját ismertetjük. Először azonban összefoglaljuk a kvadratikus maradékok elméletének legalapvetőbb tudnivalóit.

Legyen q egy prímhatvány. $\mathbb{F}_q$ egy nem 0 elemét, m-et kvadratikus maradéknak nevezzük, ha az $x^2 = m$ egyenlet megoldható $\mathbb{F}_q$ felett. Legyen Q_q a kvadratikus maradékok halmaza. $\mathbb{F}_q$ azon nem 0 elemei, amelyek nem kvadratikus maradékok alkossák a $\overline{Q}_q$ halmazt. Így $\mathbb{F}_q$ elemeit három csoportba osztottuk: $\mathbb{F}_q = \{0\} \dot\cup Q_q \dot\cup \overline{Q}_q$. Kvadratikus maradékok szorzata is kvadratikus maradék, továbbá egy kvadratikus maradék és egy nem kvadratikus maradék szorzata nem kvadratikus maradék. Ha $\overline{Q}_q$ nem üres, akkor elemszáma azonos Q_q elemszámával. Ezt úgy lehet könnyen belátni, hogy $n \in \overline{Q}_q$ elemre az $x \mapsto nx$ leképezés Q_q elemeihez $\overline{Q}_q$-beli elemeket rendel, ami a két halmaz elemeit párbaállítja. Ha $\overline{Q}_q$ nem üres, akkor két nem kvadratikus maradék szorzata kvadratikus maradék.

A továbbiakban q-ról tegyük fel, hogy egy páratlan szám. Ekkor $\overline{Q}_q$ nem üres, és így Q_q és $\overline{Q}_q$ elemszáma azonos, azaz $(q-1)/2$.

A továbbiakban feltesszük, hogy $q \equiv -1 \pmod 4$. Ekkor $-1 \in \overline{Q}_q$. Ekkor $x \mapsto -x$ a Q_q elemeihez bijektív módon $\overline{Q}_q$ egy-egy elemét rendeli.

Az alapismeretek felelevenítése után lássuk a konstrukciót.

6. Tétel. *Legyen $q = 4\ell - 1$ egy prímhatvány, amelyre $q \equiv -1 \pmod 4$ (azaz ℓ egész). Ekkor létezik $(q+1) \times (q+1)$ méterű Hadamard-mátrix.*

Bizonyítás. Először egy H_0 $q \times q$ méretű mátrixot definiálunk. A mártix sorai és oszlopai is $\mathbb{F}_q$ elemeivel vannak azonosítva. Az $a \in \mathbb{F}_q$ sor és $b \in \mathbb{F}_q$ oszlop találkozásában álljon 1, ha $a - b$ kvadratikus maradék modulo q. Más esetekben a megfelelő pozícióban álljon -1. Összefoglaljuk a H_0 mátrixunk néhány tulajdonságát:

(1) Mátrixunk főátlójában -1-esek állnak. (0 nem kvadratikus maradék.)

(2) A főátlón kívül álló, a főátlóra nézve szimmetrikus pozíciópárokban két ellentett szám áll. ($a \neq 0$ esetén a és $-a$ közül az egyik kvadratikus maradék, a másik kvadratikus nem-maradék.)

(3) Mátrixunk minden sorát úgy kapjuk az előző sorból (az $i+1$ elemnek megfelelő sort az i elemnek megfelelő sorból), hogy azt ciklikusan eggyel elforgatjuk.

(4) Minden sorban $\frac{q-1}{2}$ darab 1-es és $\frac{q+1}{2}$ darab -1-es szerepel. (A kvadratikus maradékok száma $\frac{q-1}{2}$.)

(5) Két különböző sor skaláris szorzata -1. Ezen tulajdonság belátása már komolyabb munkát igényel. Az alábbiakban ezt írjuk le.

Az i és j különböző $\mathbb{F}_q$ beli elemeknek megfelelő sorok skaláris szorzata 1-ek ($1 = 1 \cdot 1 = (-1) \cdot (-1)$) és -1-ek ($-1 = (-1) \cdot 1 = 1 \cdot (-1)$) összege. Egy $\mathbb{F}_q$-beli k elemnek megfelelő pozíció akkor és csak akkor járul a skaláris szorzathoz egy 1 taggal, ha $i - k$ és $j - k$ viszonya a Q_q halmazhoz ugyanaz (mindkettő kvadratikus maradék vagy egyik sem az). Az $(x, y) \in Q_q \times Q_q$ ($x \neq y$) különböző kvadratikus maradékokból álló párok $|Q_q \times Q_q| - |Q_q|$-elemű U halmazának azon (x, y) elemei,

amelyekre $x - y = d$ alkossák az U_d halmazt. Ekkor azon $k \in \mathbb{F}_q$ elemek száma, amelyekre $i - k$ és $j - k$ is kvadratikus maradék megegyezik az U_{i-j} halmaz α_{i-j} elemszámával. Ezzel a jelöléssel H_0 i-vel és j-vel azonosított sorának skaláris szorzata

$$\alpha_{i-j}(1 \cdot 1) + \left(\tfrac{q-1}{2} - \alpha_{i-j}\right)(1 \cdot (-1)) + \left(\tfrac{q-1}{2} - \alpha_{i-j}\right)((-1) \cdot 1)$$
$$+ \left(\tfrac{q+1}{2} - \left(\tfrac{q-1}{2} - \alpha_{i-j}\right)\right)((-1) \cdot (-1)) = 4\alpha_{i-j} - q + 2.$$

Először belátjuk,hogy az α_d számok értékei megegyeznek. Legyen d és d' két különböző $\mathbb{F}_q \setminus \{0\}$-beli szám. α_d az U_d halmaz elemszáma. Először tegyük fel, hogy $d' = md$, ahol m kvadratikus maradék ($m = d'/d$). Ekkor $\alpha_{d'}$ az U_{md} halmaz elemszáma. Az U_d halmaz elemeinek m-szeresei pontosan az U_{md} halmazt alkotják. Így a két halmaz elemszáma azonos, $\alpha_d = \alpha_{d'}$. Másodszor belátjuk, hogy $\alpha_1 = \alpha_{-1}$. α_1 az U_1 halmaz elemszáma, míg α_{-1} az U_{-1} halmaz elemszáma. Az (x, y) pár akkor és csak akkor eleme az U_1 halmaznak, ha (y, x) eleme az U_{-1} halmaznak. Így egy bijekciót létesítettünk az U_1 és U_{-1} halmazok között, speciálisan elemszámuk is megegyezik. A két tulajdonságból adódik, hogy az α_d értékek ugyanazok. Speciálisan H_0 tetszőleges két sorának skaláris szorzata megegyezik. Végül igazoljuk, hogy az α_d számok értéke $\frac{q+1}{4}$.

Az U-beli $|Q_q \times Q_q| - |Q_q| = (q-1)/q \cdot (q-1)/2 - (q-1)/2 = (q-1)(q-3)/4$ számpárt az első és második koordinátájuk különbsége alapján az $U_1, U_2, U_3, \ldots, U_{q-1}$ azonos elemszámú halmazokba osztályoztuk. Így ezen osztályok mindegyike $\alpha = (q-3)/4$ elemszámú. Ez az egyenlőség az (5) tulajdonságot bizonyítja.

Ezzel a H_0 mátrix öt tulajdonságát igazoltuk. Ezek az Hadamard-mátrixoktól megkövetelt tulajdonságoktól (tetszőleges két különböző sor skaláris szorzata 0) „nem nagyon" térnek el. A hibát könnyen korrigálhatjuk: Legyen H az a mátrix, amelyet H_0-ból úgy kapunk, hogy egy új sort és oszlopot adunk hozzá, amelyeknek összes pozíciója az 1 elemet tartalmazza. Az olvasóra bízzuk annak belátását, hogy a H mátrix egy $(q+1) \times (q+1)$ méretű Hadamard-mátrix lesz. ■

Példa. Legyen $q = 11$. Ekkor

$$\mathbb{F}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\},$$

és

$$Q_q = \{1, 4, 9, 5, 3\}, \qquad \overline{Q}_q = \{2, 6, 7, 8, 10\}.$$

A megfelelő 12×12 méretű H_{12} Hadamard-mátrix:

$$H_{12} = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\
1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\
1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 \\
1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\
1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \\
1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 \\
1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1
\end{pmatrix}.$$

$\star$

Az Hadamard-mátrixok lehetséges méreteire vonatkozó sejtés kapcsolatos adott paraméterű blokkrendszerek létezésének problémájával. Ennek a kapcsolatnak a kidolgozása előtt egy definícióra lesz szükségünk.

Definíció. Egy H Hadamard-mátrix *normális*, ha az első sora és oszlopa csak 1-eseket tartalmaz.

Tudjuk, ha egy Hadamard-mátrix sorait és oszlopait -1-gyel szorozzuk, akkor Hadamard-mátrixhoz jutunk. Így a következő egyszerű állítást mondhatjuk ki.

7. Lemma. *Akkor és csak akkor létezik $n \times n$-es Hadamard-mátrix, ha $n \times n$ méretű normális Hadamard-mátrix létezik.*

Definíció. Legyen H egy normális Hadamard-mátrix, azaz

$$H = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & \mathcal{A}(H) & \\ 1 & & & \end{pmatrix}.$$

Azaz $\mathcal{A}(H)$-t H-ból az első sor és első oszlop elhagyásával kapjuk.

A fordított operációt is leírjuk.

Definíció. Legyen A egy ± 1 mátrix. Legyen $\mathcal{H}(A)$ az a mátrix, amelyet A sorai és oszlopai elé egy-egy csupa 1-est tartalmazó sor és oszlop rakásával kapunk.

Megjegyzés. $\mathcal{H}(\mathcal{A}(H)) = H$.

Definíció. Legyen A egy ± 1 mátrix. Legyen $\widetilde{A}$ az a mátrix, amit az A-ból nyerünk, a -1-esek 0-vá változtatásával.

A fordított operációt is leírjuk.

Definíció. Legyen A egy 0-1 mátrix. Legyen $\widehat{A}$ az a mátrix, amit A 0 elemeinek -1-re való cserélésével kapunk.

Megjegyzés. $\widetilde{\widehat{A}} = A$ és $\widehat{\widetilde{A}} = A$.

A következő lemma normális Hadamard-mátixok és blokkrendszerek fogalmát köti össze.

8. Lemma. *(i) Legyen H egy normális Hadamard-mátrix. Ekkor $\widetilde{\mathcal{A}(H)}$ egy $(4t-1, 2t-1, t-1)$ paraméterű $\mathcal{B}$ blokkrendszer illeszkedési mátrixa.*

(ii) Ha A egy $(4t-1, 2t-1, t-1)$ paraméterű $\mathcal{B}$ blokkrendszer illeszkedési mátrixa, akkor $\mathcal{H}(\widehat{A})$ egy $4t \times 4t$ méretű normális Hadamard-mátrix.

Bizonyítás. Egyszerű. ■

Megjegyzés. A $(4t-1, 2t-1, t-1)$ paraméterű blokkrendszer további paraméterei könnyen kiszámolhatók: $b = v = 4t-1$ és $r = k = 2t-1$.

9. Következmény. *Akkor és csak akkor létezik $4t \times 4t$ méretű Hadamard-mátrix, ha létezik $(4t-1, 2t-1, t-1)$ paraméterű blokkrendszer.*

A Wilson-tétel sajnos nem segít. k és λ rögzítésével az alaphalmaz méretét is rögzítjük a keresett típusú blokkrendszereknél. A Wilson-tétel megköveteli az alaphalmaz méretének változtathatóságát, és csak nagy alaphalmazok esetén garantálja a létezést.

10. Feladat. *Legyen R egy $a \times b$-s részmátrixa (tetszőleges a sor és b oszlop metszéseiben álló számok mátrixa) egy $n \times n$-es Hadamard-mátrixnak. Bizonyítsuk be, hogy az R-beli elemek összege legfeljebb $\sqrt{abn}$.*

11. Feladat. *Egy $n \times n$-es táblázat minden mezőjében vagy 1, vagy -1, vagy 0 áll. Bármelyik két sort választjuk is ki, és a két sor azonos oszlopaiban álló elemeit összeszorozzuk, a kapott szorzatok összege 0. Bizonyítsuk be, hogy a táblázatban található számok összege nem nagyobb mint $n\sqrt{n}$.*