Eötvös Loránd Tudományegyetem
Természettudományi Kar

Sulan Ádám

Hadamard-mátrixok és kapcsolódó struktúrák

Szakdolgozat
Matematika BSc
Matematikus szakirány

Témavezető: Blázsik Zoltán
Tudományos munkatárs, Ph.D.

Budapest, 2022.

Tartalomjegyzék

1. Bevezetés **1**

2. Illeszkedési struktúrák **3**

2.1. Alapvető definíciók 3

2.2. Blokkrendszerek 7

2.3. t-rendszerek 9

2.4. Négyzetes blokkrendszerek 10

3. Hadamard-mátrixok és blokkrendszerek **13**

3.1. Alapvető tulajdonságok 13

3.2. Hadamard-mátrixok konstrukciói 16

4. Kódelmélet **23**

4.1. Lineáris kódok 23

4.2. Hadamard-kódok 27

Irodalomjegyzék **31**

Köszönetnyilvánítás

Szeretném megköszönni témavezetőmnek Blázsik Zoltánnak, hogy elvállalta a témavezetést, az izgalmas témajavaslatot, és a témához kapcsolódó érdekes cikkek és források bemutatását, az egész éves konzultációkat és gyors válaszait.

Köszönöm továbbá a családomnak, barátnőmnek és matektanáraimnak a folyamatos támogatásukat tanulmányaim során.

1. fejezet

Bevezetés

Szakdolgozatomban bemutatjuk az Hadamard-blokkrendszerek, az Hadamard-mátrixok és az Hadamard-kódok közti kapcsolatokat. Egy Hadamard-mátrix egy olyan négyzetes $-1, 1$ mátrix, ahol bármely két oszlopot vagy sort egymás mellé rakva pontosan a mezők fele egyezik meg.

Először bemutatunk néhány alapvető illeszkedési struktúrát és tulajdonságaikat.

A 3. fejezetben ismertetjük az Hadamard-mátrixok definícióját, az Hadamard által bizonyított determináns-egyenlőtlenséget, amely pontosan az Hadamard-mátrixokra teljesül egyenlőséggel. Megvizsgáljuk, hogy milyen rendű Hadamard-mátrixok léteznek, majd mutatunk néhány példát rájuk. Feltárjuk a kapcsolatot az Hadamard-blokkrendszerek és mátrixok között. Ezután a 3.2. részben az Hadamard-mátrixok különböző előállítási módszerei közül ismertetünk néhányat. Bemutatjuk Sylvester, Scarpis, Paley és Williamson konstrukcióit, és szót ejtünk arról, hogy jelenleg hol tart a tudomány az Hadamard-sejtéssel kapcsolatosan.

A 4. fejezetben bemutatjuk a kódelmélet alapvető definícióit, majd az Hadamard-kódokat is definiáljuk. Ha A-ból B-be el szeretnénk juttatni egy üzenetet egy nagyon zajos csatornán keresztül, akkor fennáll a veszélye annak, hogy nagyon sok helyen meghibásodik az üzenetünk, ezért egy olyan kódolást szeretnénk választani, aminek magas a hibajavító képessége. Az Hadamard-kódok ilyenek, a NASA Mariner 9 űrhajója Marsról készült fényképek kódolására használta.

2. fejezet

Illeszkedési struktúrák

Az alapvető fogalmak bevezetésénél Szőnyi Tamás: Szimmetrikus struktúrák [1] jegyzetére támaszkodunk.

2.1. Alapvető definíciók

2.1.1. Definíció. *Egy* $(\boldsymbol{P}, \boldsymbol{B}, I)$ *hármast* illeszkedési struktúrának *nevezünk, ahol* $\boldsymbol{P}$ *és* $\boldsymbol{B}$ *két diszjunkt halmaz és* $I \subset \boldsymbol{P} \times \boldsymbol{B}$ *pedig a köztük lévő illeszkedési relációt jelöli.*

Geometriai megfontolásból $\mathbf{P}$ elemeit pontoknak, $\mathbf{B}$ elemeit blokkoknak nevezzük és az illeszkedést $(p, B) \in I$ helyett pIB-ként fogom jelölni.

Az Illeszkedési struktúrákat azonosíthatjuk hipergráfokkal is, ha a hipergráf csúcsait azonosítjuk a $\mathbf{P}$ pontokkal, és a $\mathbf{B}$ blokkokat pedig a hipergráf hiperéleivel.

2.1.2. Definíció. *Legyen* $\boldsymbol{D} = (\boldsymbol{P}, \boldsymbol{B}, I)$ *és* $\boldsymbol{D'} = (\boldsymbol{P'}, \boldsymbol{B'}, I')$ *két illeszkedési struktúra. Azt mondjuk, hogy* $\boldsymbol{D}$ *és* $\boldsymbol{D'}$ *izomorf, ha létezik* $\alpha : \boldsymbol{P} \cup \boldsymbol{B} \Rightarrow \boldsymbol{P'} \cup \boldsymbol{B'}$ *illeszkedéstartó bijektív leképezés, amire* $\boldsymbol{P}^\alpha = \boldsymbol{P'}$, $\boldsymbol{B}^\alpha = \boldsymbol{B'}$,. *Ha* $\boldsymbol{D} = \boldsymbol{D'}$, *akkor* α*-t automorfizmusnak nevezzük.*

2.1.3. Definíció. *A* $\boldsymbol{D} = (\boldsymbol{P}, \boldsymbol{B}, I)$ *illeszkedési struktúra* duálisa $\boldsymbol{D}^* = (\boldsymbol{P}^*, \boldsymbol{B}^*, I^*)$, *ahol* $\boldsymbol{P}^* = \boldsymbol{B}$, $\boldsymbol{B}^* = \boldsymbol{P}$ *és* I^* *az* I *inverze.*

2.1.4. Definíció. *Egy* $p \in \boldsymbol{P}$ *pont fokának a rá illeszkedő blokkok számát nevezzük, azaz* $deg(p) = |\{B \in \boldsymbol{B} : pIB\}|$. *Hasonlóan egy* $B \in \boldsymbol{B}$ *blokk fokának a rá illeszkedő pontok számát hívjuk, azaz* $deg(B) = |\{p \in \boldsymbol{P} : pIB\}|$.

Ha egy illeszkedési struktúrában minden pont foka r, akkor azt r-regulárisnak nevezzük. Hasonlóan, ha minden blokk foka k, akkor a struktúrát k-uniformnak hívjuk.

2.1.5. Definíció. *Egy illeszkedési struktúrát* egyszerűnek *hívunk, ha nincs két olyan blokkja, melyek pontosan ugyanazokat a pontokat tartalmazzák.*

2.1.6. Definíció. *Egy* $\mathcal{H} = (V(\mathcal{H}), E(\mathcal{H}))$ *párt halmazrendszernek hívunk, ha* $E(\mathcal{H})$ *elemei* $V(\mathcal{H})$ *bizonyos részhalmazai.*

Egyszerű illeszkedési struktúrákat azonosíthatóak a rájuk illeszkedő pontokkal: $(\mathbf{P}, \mathbf{B}, I)$ izomorf a $(\mathbf{P}, \mathbf{B}^*, \in)$ struktúrával, ahol $\mathbf{B}^* = \{\{p : pIB\} : B \in \mathbf{B}\}$. Ebből az izomorfiából látszik, hogy az egyszerű illeszkedési struktúrák azonosíthatók halmazrendszerekkel.

Egy halmazrendszert r-regulárisnak nevezünk, ha minden elemet pontosan r halmaz tartalmaz, és k-uniform, ha minden halmaz elemszáma k.

Lássunk néhány nevezetes példát illeszkedési struktúrákra!

2.1.7. Definíció. *A* (Π, Λ) *párt* projektív síknak *nevezzük, ha* Π *nemüres halmaz, és elemeit "pontoknak" hívunk,* Λ *pedig* Π *néhány részhalmazának halmaza, amelyek elemeit "egyeneseknek" nevezünk, ha eleget tesznek az első* 3 *axiómának. Ha a* 4. *axiómát is teljesítik, akkor véges vagy* q-ad rendű *projektív síknak nevezzük:*

1. *Bármely két* Π*-beli ponthoz pontosan egy egyenes van* Λ*-ban, amely mindkettőt tartalmazza.*
2. *Bármely két* Λ*-beli egyeneshez pontosan egy* Π*-beli pont van, melyet mindkét egyenes tartalmaz.*
3. *Létezik* 4 *olyan* Π*-beli pont, melyen közül bárhogy választunk ki* 3*-at, nem létezik ezekre egyszerre illeszkedő egyenes.*
4. *Van olyan* Λ*-beli egyenes, ami* $q + 1$ *pontot tartalmaz.*

2.1.8. Példa. *Legyen* $\Pi = \{0, ..., 6\}$,

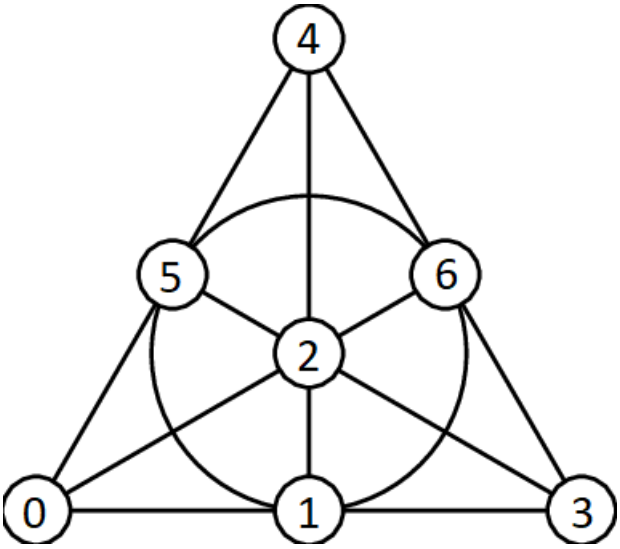
$$\Lambda = \{\{0, 1, 3\}, \{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 0\}, \{5, 6, 1\}, \{6, 0, 2\}\}$$

Ezt a projektív síkot Fano-síknak *nevezzük.*

A q-adrendű véges projektív síkokra jellemző alábbi tulajdonságok levezethetőek a fenti axiómákból.

2.1.9. Állítás. *Egy* q*-adrendű véges projektív síkra teljesülnek az alábbiak:*

1. *Minden egyenes pontosan* $q + 1$ *pontból áll.*
2. *Minden pontra pontosan* $q + 1$ *egyenes illeszkedik.*
3. *A* Π *és a* Λ *elemszáma is pontosan* $q^2 + q + 1$.



2.1. ábra. Fano-sík

Egy másik jól ismert példa az affin sík fogalma. Erre az illeszkedési struktúrára gondolhatunk úgy is, mint ha a projektív sík egy egyenesét és az arra illeszkedő pontokat töröltük volna. A következőkben az axiomatikus bevezetésüket is megadjuk, az ezekből levezethető tulajdonságaikkal együtt.

2.1.10. Definíció. *A* (Π, Λ) *illeszkedési struktúrát* affin síknak *nevezzük, ha az alábbi axiómákat teljesítik:*

1. *Bármely két* Π*-beli ponthoz pontosan egy egyenes van* Λ*-ban, amely mindkettőt tartalmazza.*
2. *Egy* Λ*-beli egyeneshez, és egy erre nem illeszkedő* Π*-beli ponthoz pontosan egy olyan* Λ*-beli egyenes van, amely illeszkedik a pontra, de nem metszi a másik egyenest.*
3. *Létezik 3 pontja* Π*-nek, amik nem esnek egy egyenesre.*

2.1.11. Állítás. *Ha a* (Π, Λ) *affin síknak van olyan egyenese, amelyre* q *pont illeszkedik, akkor:*

1. *Minden egyenesre pontosan* q *pont illeszkedik.*
2. *Egy ponton pontosan* $q + 1$ *egyenes halad át.*
3. *Összesen* q^2 *pontja és* $q^2 + q$ *egyenese van.*

Ekkor a q *számot az affin sík* rendjének *nevezzük.*

A továbbiakban a véges illeszkedési struktúrákat mátrixokkal fogjuk reprezentálni, amelyek a pontok és a blokkok közötti illeszkedéseket fogják megadni. A véges illeszkedési struktúrákat többféleképpen is leírhatjuk mátrixokkal.

2.1.12. Definíció. *A* $(\boldsymbol{P}, \boldsymbol{B}, I)$ *illeszkedési struktúrát jellemezhetjük* illeszkedési mátrixal*, ha* $\boldsymbol{P} = \{p_1, p_2, ..., p_v\}$ *és* $\boldsymbol{B} = \{B_1, B_2, ..., B_b\}$*, és tekintjük azt az* M *mátrixot, amely* $v \times b$ *méretű* $0, 1$ *elemű, és* $\forall i \in \{1, 2, ..., v\}, j \in \{1, 2, ..., b\}$: $m_{ij} = 1$*, ha* $p_i I B_j$*, különben* $m_{ij} = 0$*.*

2.1.13. Példa. *A Fano-sík illeszkedési mátrixa:*

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Jellemezhetjük a véges illeszkedési struktúrákat szomszédsági mátrixokkal is.

2.1.14. Definíció. *A* $(\boldsymbol{P}, \boldsymbol{B}, I)$ *véges illeszkedési struktúra* A szomszédsági mátrixát *megkaphatjuk az* M *illeszkedési mátrixából. Méghozzá* $A = MM^T$*.*

Tehát az $A = (a_{ij})$ *szomszédsági mátrix* $v \times v$ *méretű és szimmetrikus. Továbbá* $a_{i,j}$ *azt jelöli, hogy a hány olyan blokkja van az illeszkedési struktúrának, ami a* p_i *és a* p_j *pontokra egyszerre illeszkedik. Könnyen látható, hogy a szomszédsági mátrix főátlójában épp a pontok fokszámai szerepelnek.*

2.1.15. Tétel. *Tetszőleges* $\boldsymbol{D} = (\boldsymbol{P}, \boldsymbol{B}, I)$ *illeszkedési struktúrában*

$$\sum_{p \in \boldsymbol{P}} deg(p) = \sum_{B \in \boldsymbol{B}} deg(B)$$

ahol $deg(B) = |B|$ *és* $deg(p)$ *a* p *pontot tartalmazó blokkok száma.*

Bizonyítás. Vegyük $\boldsymbol{D}$ illeszkedési mátrixát, ezt jelölje M. Ekkor a mátrix oszlopai a blokkokat jelölik, a sorok pedig a pontokat. Egy oszlopban a hozzá tartozó blokk elemeinél 1-es van, mindenhol máshol 0. Egy sorban a hozzá tartozó pontnál azoknál a blokkoknál van 1-es, melyekben benne van, mindenhol máshol 0. Ekkor látszik, hogy mindkét szumma az M-ben lévő 1-esek számát számolja meg, tehát megegyeznek. Az első a sorok (pontok) szerint, a második pedig az oszlopok (blokkok) szerint. □

2.1.16. Következmény. *Ha* $\mathcal{H}$ *egy* k*-uniform* r*-reguláris hipergráf, melynek* v *pontja és* b *blokkja van, akkor* $vr = bk$*.*

2.1.17. Definíció. *Egy illeszkedési struktúra* komplementerének *azt az illeszkedési struktúrát nevezzük, ahol a pontok és a blokkok változatlanok, de az illeszkedési reláció komplementer reláció, azaz az új struktúrában egy pont akkor és csak akkor illeszkedik egy blokkra, ha a régiben nem illeszkedett rá.*

Ha az eredeti illeszkedési struktúra illeszkedési mátrixa M, akkor a komplementeréé is egyszerűen elkészíthető, csak ki kell cserélni a 0-kat és az 1-eket, mivel az illeszkedés a komplementeréje változott.

2.1.18. Példa. *A Fano-sík komplementerének illeszkedési mátrixa:*

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

2.2. Blokkrendszerek

2.2.1. Definíció. $2-(v,k,\lambda)$-blokkrendszernek *nevezünk egy olyan* $\boldsymbol{D}=(\boldsymbol{P},\boldsymbol{B},I)$ *illeszkedési struktúrát, ami k-uniform (vagyis $\forall B \in \boldsymbol{B} : |B| = k$) és $|\boldsymbol{P}| = v$, valamint bármely két különböző pont pontosan λ blokkban van benne.*

2.2.2. Állítás. *Egy $2-(v,k,\lambda)$-blokkrendszerben minden pont fokszáma r (azaz r-reguláris), ahol $r=\lambda(v-1)/(k-1)$, és a blokkok száma pedig $b=\lambda v(v-1)/(k(k-1))$.*

Bizonyítás. Rögzítsünk egy p pontot. Kettős leszámlálással meg fogjuk számolni azokat a (q,B) egymásra illeszkedő pont-egyenes párokat, melyekre $q \neq p$ és $p \in B$. Ezek száma egyrészt $deg(p)(k-1)$, mivel minden p-t tartalmazó blokkban még $k-1$ másik pont van. Másrészt viszont ezek száma $(v-1)\lambda$, mivel minden rajta kívüli ponttal pontosan λ darab blokkban vannak közösen. Tehát $deg(p)(k-1)=(v-1)\lambda$, tehát $r = deg(p) = \lambda(v-1)/(k-1)$. A 2.1.16 következmény miatt $vr = bk$, tehát $b = vr/k = \lambda v(v-1)/(k(k-1))$. □

Ebből az eredményből a blokkrendszerek létezésére kaphatunk szükséges oszthatósági feltételeket.

2.2.3. Következmény. *$2-(v,k,\lambda)$-blokkrendszer csak akkor létezhet, ha az alábbi feltételek egyaránt teljesülnek:*

$$\lambda(v-1) \equiv 0 \ (mod\ k-1) \text{ és } \lambda v(v-1) \equiv 0 \ (mod\ k(k-1)).$$

Fontos megjegyeznünk, hogy ezek az oszthatósági feltételek általában nem elégségesek, azonban például a Steiner rendszerek (amik éppen a $2-(v,k,1)$-blokkrendszerek) esetén elégségesek is. Az elégségességet Kirkman [2] és Skolem [3] konstrukcióiból vezethetjük le, azonban mi ettől most eltekintünk. Általánosságban a $2-(v,k,\lambda)$-blokkrendszerek létezéséhez szükséges oszthatósági feltételek elégségességéről szól Wilson alábbi híres tétele. Ennek a bizonyítása megtalálható Beth, Jungnickel, Lenz [4] könyvében.

2.2.4. Tétel (Wilson)**.** *Ha k és λ rögzített, akkor található olyan v_0, hogy tetszőleges $v > v_0$ értékre, amire a 2.2.2 állításbeli oszthatósági feltételek teljesülnek létezik is $2-(v,k,\lambda)$-blokkrendszer.*

Most pedig lássunk pár példát blokkrendszerekre.

2.2.5. Példa. *A korábban említett véges projektív és affin síkok is blokkrendszerek:*

1. *Az n-ed rendű projektív sík egy $2-(n^2+n+1, n+1, 1)$ rendszer.*
2. *Az n-ed rendű affin sík pedig egy $2-(n^2, n, 1)$ rendszer.*

2.2.6. Példa. *Egy $2-(v,k,\lambda)$ blokkrendszer komplementere egy $2-(v, v-k, b-2r+\lambda)$ blokkrendszer.*

Ez könnyen látszik, mivel a blokkok pont a komplementerek lesznek, és az eredeti blokkrendszerben két ponton át nem menő blokkok száma $b-2r+\lambda$.

Most pedig következzen egy neves tétel, ami kapcsolatot teremt a blokkrendszer bizonyos paraméterei között:

2.2.7. Tétel (Fisher egyenlőtlenség)**.** *Egy $2-(v,k,\lambda)$-blokkrendszerben, ha $k < v$, akkor $b \geq v$.*

Bizonyítás. Jelölje M a blokkrendszer illeszkedési mátrixát, $A = MM^T$ pedig a szomszédsági mátrixát. A szomszédsági mátrix főátlójában mindenhol r van, a többi helyen pedig λ. A 2.2.2 állítás miatt mivel $k \neq v$, így $r \neq \lambda$. Ekkor $A = MM^T$ rangja v és $rang(MM^T) \leq rang(M) = b$, tehát $b \geq v$. □

2.2.8. Következmény. *Ha egy* $\boldsymbol{D}$ *blokkrendszerben* $k < v$*, akkor a következő állítások ekvivalensek:*

1. $b = v$.
2. $r = k$.
3. *bármely két blokk pontosan* λ *pontban metszi egymást.*
4. *bármely két blokk metszete ugyanakkora.*

Bizonyítás. Az első két állítás ekvivalenciája 2.1.16-ból következik.

$2 \Rightarrow 3$: Mivel $r = k$, így a pontok és a blokkok fokszáma megegyezik, tehát $MJ = JM$, ahol J a csupa 1-ből álló mátrix, és M felcserélhető MM^T-val is, így $M^2M^T = MM^TM$. Mivel MM^T nemszinguláris, így M sem, azaz $MM^T = M^TM$. Ez pedig azt fejezi ki, hogy a duális illeszkedési struktúra is blokkrendszer, mivel a duális illeszkedési struktúra illeszkedési mátrixa az eredeti illeszkedési mátrixának transzponáltja. Tehát az eredetiben két blokk λ pontban metszi egymást.

A $3 \Rightarrow 4$ irány triviális.

$4 \Rightarrow 1$: 4 miatt a duális is blokkrendszer, és a Fisher egyenlőtlenséget alkalmazva az eredeti blokkrendszerre azt kapjuk, hogy $b \geq v$, a duálisra alkalmazva pedig hogy $b \leq v$, tehát $b = v$. □

2.3. t-rendszerek

2.3.1. Definíció. *Egy* $\boldsymbol{D} = (\boldsymbol{P}, \boldsymbol{B}, I)$ *egyszerű illeszkedési struktúrát* $t - (v, k, \lambda)$ *rendszernek hívunk, ha* $|\boldsymbol{P}| = v$*, k-uniform (minden blokkra pontosan k pont illeszkedik), és bármely t különböző pont pontosan* λ *blokkban van benne.* $(v > k > 1, k \geq t \geq 1)$

A $t = 1$ esetben a reguláris, uniform hipergráfokat kapjuk vissza, $t = 2$ esetben pedig a blokkrendszereket.

2.3.2. Állítás. *Egy* $\boldsymbol{D}$ $t - (v, k, \lambda)$ *rendszerben a*

$$\lambda_i = \lambda \frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}}$$

az i különböző ponton átmenő blokkok számát adja meg minden $i \in \{0, 1, ..., t\}$*-re, azaz a* λ_i *számok egészek.*

Bizonyítás. Vegyünk egy tetszőleges i elemű $X \subset \mathbf{P}$ részhalmazt és számoljuk meg az X-en átmenő blokkokat. Egészítsük ki az I-t t elemű halmazzá, és tekintsük

az ezen átmenő blokkokat. Ekkor $\lambda\binom{v-i}{t-i}$-t kapunk, de minden blokkot $\binom{k-i}{t-i}$-szer számoltunk. □

2.3.3. Példa. *Ha egy* $(\boldsymbol{P}, \boldsymbol{B}, I)$ *illeszkedési struktúra blokkjai megegyeznek az* $\boldsymbol{P}$ *összes* k*-elemű részhalmazával, akkor* teljes k-uniform hipergráfról *beszélhetünk. Ez minden* $t \leq k$ *értékre egy* $t-(v,k,\lambda)$*-rendszer, ahol* $\lambda = \binom{v-t}{k-t}$.

2.4. Négyzetes blokkrendszerek

Ebben a részben a blokkrendszerek egy speciális típusával a *négyzetes blokkrendszerekkel* fogunk megismerkedni, majd bemutatunk két nevezetes tételt is ezekkel kapcsolatban.

2.4.1. Definíció. *Egy* $2-(v,k,\lambda)$*-blokkrendszert akkor hívunk* négyzetesnek*, ha a pontjainak a száma és a blokkjainak a száma megegyezik, azaz, ha* $v = b$.

Ekkor a 2.2.8 következményből könnyen látszik, hogy $r = k$ és bármely két blokk metszete λ elemű.

2.4.2. Definíció. *Négyzetes* $2-(v,k,\lambda)$*-blokkrendszerekre a* $n = k - \lambda$ *mennyiséget a blokkrendszer* rendjének *nevezzük.*

2.4.3. Állítás. *Egy négyzetes* $2-(v,k,\lambda)$*-rendszerben ahol* $1 < k < v-1$ *fennáll, hogy:*

$$4n - 1 \leq v \leq n^2 + n + 1.$$

Bizonyítás. A 2.2.2 miatt tudjuk, hogy $r = \lambda(v-1)/(k-1)$. Tehát mivel négyzetes blokkrendszerről van szó, ezért $r = k$ és így : $v = 1+k(k-1)/\lambda = n(n-1)/\lambda+2n+\lambda$. Ekkor λ-val szorozva: $\lambda^2 - (v-2n)\lambda + n(n-1) = 0$ egyenletet kapjuk, ezt λ-ra megoldva: $\lambda_{1,2} = 1/2((v-2n) \pm \sqrt{(v-2n)^2 - 4n(n-1)})$. Mivel $\lambda_{1,2} \geq 1$, így $v - 2n - 2 \geq \sqrt{(v-2n)^2 - 4n(n-1)}$, amiből $v \leq n^2 + n + 1$.
Mivel bármely két blokk metszete λ elemű, így $v \geq 2k - \lambda \geq 2n$. Az egyenlet diszkriminánsa is nemnegatív, tehát $(v-2n)^2 \geq 4n(n-1) = (2n-1)^2 - 1$, és mivel $v \geq 2n$, így $v - 2n \geq 2n - 1$, tehát a bal oldali egyenlőtlenség is igaz. □

Ezek az egyenlőtlenségek végtelen sok n-re élesek. A felső korlátot a projektív síkok, az alsó korlátot pedig az Hadamard-blokkrendszerek (lásd 3.1.5) teljesítik egyenlőséggel.

Bizonyítás nélkül megemlítjük az egyetlen ismert általános szükséges feltételt négyzetes blokkrendszerek létezéséről. A Bruck-Chowla-Ryser tétel (lásd [5, 7]) bizonyítása megtalálható például a [1] jegyzetben. A bizonyítása egy elemi számelméleti azonosságon és az alábbi híres számelméleti lemmán alapul.

2.4.4. Lemma (Lagrange)**.** *Minden pozitív egész szám előáll négy négyzetszám összegeként.*

2.4.5. Tétel (Bruck–Chowla–Ryser-tétel)**.** *Tegyük fel, hogy v páratlan, és létezik négyzetes $2-(v,k,\lambda)$ rendszer. Ekkor a*

$$z^2 = (k-\lambda)x^2 + (-1)^{(v-1)/2}\lambda y^2$$

diofantoszi egyenletnek van nemtriviális egész megoldása.

3. fejezet

Hadamard-mátrixok és blokkrendszerek

Most következik a szakdolgozat központi fogalmának bemutatása, amire már 2.4.3 állítás után is hivatkoztunk. A fejezet elején megmagyarázzuk, hogy miért nevezték el ezeket az objektumokat Hadamardról. A későbbiekben az Hadamard-mátrixok és Hadamard-blokkrendszerek kapcsolatát mutatjuk be. Az itteni rész tárgyalásánál a [9], [10], [18] könyveket követjük.

3.1. Alapvető tulajdonságok

3.1.1. Definíció. *Egy olyan $n \times n$-es H mátrixot, aminek minden eleme ± 1, és teljesül rá hogy $HH^T = nI$,* Hadamard-mátrixnak *nevezünk. (I az $n \times n$-es egységmátrix.)*

Vegyük észre, hogy $HH^T = nI$-ből $H^TH = nI$ is következik. Az ilyen tulajdonságú mátrixok elnevezését az alábbi Hadamard-által bizonyított determináns-egyenlőtlenség ihlette. Ezt a [6] cikk segítségével tárgyaljuk.

3.1.2. Tétel (Hadamard-egyenlőtlenség)**.** *Ha N egy $n \times n$-es mátrix, ahol $\forall i, j \in \{1, 2, \ldots, n\} : |N_{ij}| \leq B$, akkor $|det(N)| \leq B^n n^{n/2}$. Sőt $B = 1$ mellett egyenlőség akkor és csak akkor teljesül, ha N egy Hadamard-mátrix.*

Bizonyítás. Ha N szinguláris, akkor az állítás triviálisan igaz, úgyhogy tekintsük azt az esetet, amikor nem az. Jelöljük $(\underline{v_i})_{i=1}^n$-vel a mátrix oszlopvektorait. Ekkor ha minden oszlopvektort leosztunk a hosszával, akkor a feladat ekvivalens azzal a speciális esettel, hogy az oszlopvektorok egységvektorok. Az így kapott vektorokat jelöljük $\underline{e_i}$-vel, és tekintsük a belőlük alkotott M mátrixot. Ekkor az állítás:

$|det(M)| \leq 1$. Tekintsük a $P = M^*M$ mátrixot, ahol M^* az adjungált mátrix, és jelöljük P sajátértékeit λ_i-vel. Mivel M minden oszlopvektorának hossza 1, így P főátlójában minden elem 1, így $trP = n$. A számtani és mértani közép közti egyenlőtlenség miatt:

$$detP = \prod_{i=1}^{n} \lambda_i \leq \left(\frac{1}{n}\sum_{i=1}^{n}\lambda_i\right)^n = \left(\frac{1}{n}trP\right)^n = 1^n = 1.$$

Tehát $|detM| = \sqrt{detM^*M} = \sqrt{detP} \leq 1$ adódik, azaz:

$$|detN| = \left(\prod_{i=1}^{n}||v_i||\right)|detM| \leq \prod_{i=1}^{n}||v_i|| \leq \prod_{i=1}^{n}\sqrt{nB^2} = B^n n^{n/2}.$$

Egyenlőség akkor és csak akkor áll fenn, ha az oszlopvektorok hosszánál is egyenlőség áll fenn, vagyis $||v_i|| = \sqrt{nB^2}$, és $|N_{ij}| = B$, valamint a számtani-mértani közepek közti egyenlőtlenségben is mindenhol egyenlőség teljesül, azaz $\lambda_1 = ... = \lambda_n = 1$, mivel $\sum_{i=1}^{n}\lambda_i = trP = n$. Továbbá $P = P^*$, így diagonalizálható, ezért ez az egységmátrix, tehát M oszlopai páronként ortogonálisak, ahonnan következik, hogy N oszlopai páronként ortogonálisak. □

Tehát a fenti egyenlőtlenséget pontosan az Hadamard-mátrixok teljesítik. Szimmetriai okokból ugyanez igaz a sorokra is, tehát tetszőleges Hadamard-mátrixban a sorok és az oszlopok is páronként ortogonálisak, azaz bármely két sor vagy bármely két oszlop skaláris szorzata 0.

3.1.3. Példa. *Például a következő mátrixok Hadamard-mátrixok:*

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

Felmerülhet az olvasóban a kérdés, hogy milyen pozitív egész n értékek esetén létezhetnek egyáltalán Hadamard-mátrixok. A következő elemi észrevétel egy szükséges feltételt ad az Hadamard-mátrix rendjére nézve.

3.1.4. Tétel. *Egy Hadamard-mátrix rendje csak* $1, 2$ *vagy* 4*-el osztható lehet.*

Bizonyítás. A 3.1.3 példában látott 1, illetve 2 rendű mátrix létezik.
Tegyük fel a továbbiakban, hogy az Hadamard-mátrix rendje legalább 3. Vegyük észre, hogy egy H Hadamard-mátrix esetén a $HH^T = nI$ összefüggés akkor is teljesülni fog, ha bármelyik sorát vagy oszlopát -1-gyel végigszorozzuk, vagy ha felcseréljük

bármelyik két sorát vagy oszlopát. Tehát feltehetjük, hogy egy Hadamard-mátrix első sora és oszlopa csupa +1-ből áll (ezt *normalizált állapotnak* is hívjuk), illetve a második sor elején csak +1-ek állnak, utánuk pedig csak −1-ek. Ekkor mivel az első két sor ortogonális, így a mátrix rendje páros ($n = 2m$, ahol $m \in \mathbb{Z}$).

Tekintsük az Hadamard-mátrix harmadik sorát. Legyen az első m helyen lévő +1-esek száma x, a második m helyen lévők száma pedig y. Ekkor mivel az első és a harmadik sor is ortogonális, így a két sor skaláris szorzata 0, ezért $x - (m - x) + y - (m - y) = 0$, tehát $x + y = m$. A második és a harmadik sor ortogonalitásából következik, hogy $x - (m - x) - y + (m - y) = 0$, ahonnan $x = y$. Tehát beláttuk, hogy a mátrix rendje 4-el osztható ($n = 2m = 4x$, ahol $x \in \mathbb{Z}$). □

3.1.5. Definíció. *Egy négyzetes* $2 - (4\lambda + 3, 2\lambda + 1, \lambda)$*-blokkrendszert* Hadamard-féle blokkrendszernek *hívunk.*

3.1.6. Példa. *A* $PG_{n-1}(n, 2)$ *projektív tér Hadamard-féle blokkrendszer.*

Most pedig nézzük meg, hogy mi a kapcsolat a négyzetes blokkrendszerek és az Hadamard-mátrixok között.

3.1.7. Tétel. *Pontosan akkor létezik* 4ℓ *rendű Hadamard-mátrix, ha létezik négyzetes* $2 - (4(\ell - 1) + 3, 2(\ell - 1) + 1, \ell - 1)$*-blokkrendszer.*

Bizonyítás. Tegyük fel, hogy a mátrix normalizált állapotú. Ekkor hagyjuk el az első sort és oszlopot, és a maradék részen a (-1)-eket cseréljük ki 0-kra. Ekkor a megmaradt mátrix a fenti négyzetes blokkrendszer illeszkedési mátrixa. Az ortogonalitási feltételekből következik, hogy minden sorban $4\ell/2 - 1 = 2\ell - 1$ darab 1-es van, tehát $r = 2\ell - 1$. Szimmetriai okok miatt tetszőleges két sornak pontosan $4\ell/4 - 1 = \ell - 1$ darab 1-es van (az előző 3.1.4 tétel bizonyításából látszik), tehát $\lambda = \ell - 1$. Mivel a mátrix négyzetes, így $k = r$, tehát a megfelelő paraméterű blokkrendszert kapjuk. Ezeket a lépéseket visszafele elvégezve a másik irány bizonyítását kapjuk meg. □

Észrevehetjük, hogy ekvivalens mátrixokból izomorf Hadamard-féle blokkrendszereket kapunk, de visszafele ezt nem tudjuk elmondani.

3.1.8. Sejtés (Hadamard-sejtés)**.** *Minden* ℓ *pozitív egészre létezik* 4ℓ *rendű Hadamard-mátrix.*

Ez a sejtés jelenleg nem megoldott, rengeteg konstrukció van, amelyek közül néhányat a következő fejezetrészben be is mutatunk. A legkisebb rend, amelyre az Hadamard-mátrix létezése nem ismert az a 668 [8].

3.2. Hadamard-mátrixok konstrukciói

A most következő részben bemutatunk több olyan módszert, amelyek segítségével Hadamard-mátrixokat állíthatunk elő. Elsőként Sylvester észrevételét vizsgáljuk meg, ami mátrixok Kronecker szorzatán alapul.

3.2.1. Definíció. *Ha $A = (a_{ij})$ egy $m \times n$ méretű mátrix, és $B = (b_{ij})$ egy $p \times q$ méretű mátrix, akkor a Kronecker szorzatuk $A \otimes B$ egy $mp \times nq$ méretű mátrix, melyre:* $A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{bmatrix}$

Először felelevenítjük a mátrixok Kronecker szorzásának alapvető tulajdonságait. Ennek a lemmának a bizonyítása megtalálható a [16] cikkben.

3.2.2. Lemma. *Legyen $A = (a_{ij})$ egy $m \times n$ méretű mátrix, és $B = (b_{ij})$ egy $p \times q$ méretű mátrix. Ekkor $(A \otimes B)^T = A^T \otimes B^T$ és $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$.*

Most ezeket a tulajdonságokat használva igazolhatjuk Sylvester tételét, amivel egy jól alkalmazható módszert kapunk arra, hogy ismert Hadamard-mátrixokból újabb, nagyobb Hadamard-mátrixot állítsunk elő.

3.2.3. Tétel (Sylvester tétel)**.** *Ha H_n egy $n \times n$-es Hadamard-mátrix, H_m pedig egy $m \times m$-es, akkor $H_n \otimes H_m$ is egy $nm \times nm$-es Hadamard-mátrix.*

Bizonyítás. A 3.2.2 miatt $(H_n \otimes H_m)(H_n \otimes H_m)^T = (H_n \otimes H_m)(H_n^T \otimes H_m^T) = (H_n H_n^T) \otimes (H_m H_m^T) = (nI_n) \otimes (mI_m) = nmI_{nm}$. □

3.2.4. Következmény (Sylvester)**.** *Minden pozitív egész k-ra létezik $n = 2^k$ rendű Hadamard-mátrix.*

Bizonyítás. Tudjuk, hogy létezik 2 rendű Hadamard-mátrix: $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Ezt k-szor Kronecker szorozva önmagával egy $2^k \times 2^k$ Hadamard-mátrixot kapunk a 3.2.3 tétel miatt. □

Az így kapott mátrixok Hadamard-mátrixok: $H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$$H \otimes H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$H \otimes H \otimes H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

Így most már minden $n = 2^k$ $(k \geq 1, k \in \mathbb{Z})$ rendre tudunk konstruálni n rendű Hadamard-mátrixot, és ha adott egy $n \times n$-es és egy $m \times m$-es Hadamard-mátrix, akkor tudunk konstruálni $nm \times nm$-es Hadamard-mátrixot is.

Most egy újabb módszer jön, ami Paley nevéhez fűződik (lásd [13]), ám speciális esetét Scarpis [15] igazolta. Ennek a bizonyításához a [9] és a [18], a jelölésekhez és fogalmakhoz pedig a [12] cikkeket vettük alapul.

3.2.5. Tétel (Umberto Scarpis)**.** *Legyen p egy prímszám. Ekkor a következő igaz:*

1. *Ha $p \equiv 3 \ (mod\ 4)$, akkor létezik $p+1$ rendű Hadamard-mátrix.*
2. *Ha $p \equiv 1 \ (mod\ 4)$, akkor létezik $2(p+1)$ rendű Hadamard-mátrix.*

Ezt a tételt Paley általánosította, és most ezt fogom bebizonyítani.

3.2.6. Tétel (Paley)**.** *Legyen p egy prím, és $\alpha > 1, \alpha \in \mathbb{Z}$. Ekkor*

1. *Ha $p^\alpha \equiv 3 \ (mod\ 4)$, akkor létezik $p^\alpha + 1$ rendű Hadamard-mátrix.*
2. *Ha $p^\alpha \equiv 1 \ (mod\ 4)$, akkor létezik $2(p^\alpha + 1)$ rendű Hadamard-mátrix.*

Észrevehetjük, hogy $\alpha = 1$ esetén a 3.2.5 tételt kapjuk.

A következő részben a 3.2.6 második részének bizonyítását készítjük elő.

3.2.7. Lemma. *Tegyük fel, hogy q egy páratlan prímhatvány, $\mathbb{F}_q$ pedig jelölje a q elemű véges testet. Ekkor definiáljuk $\chi_q : \mathbb{F}_q \to \{-1, 0, 1\}$-et, a $\mathbb{F}_q$ kvadratikus karakterét a következőképpen:*

$$\chi_q(x) = \begin{cases} 0, & \text{ha } x = 0 \\ 1, & \text{ha } x \text{ nemnulla négyzetelem } \mathbb{F}_q\text{-ban} \\ -1, & \text{ha } x \text{ nem négyzetelem } \mathbb{F}_q\text{-ban} \end{cases}$$

Ekkor fennáll a következő két egyenlőség:

1. $\sum_{x \in \mathbb{F}_q} \chi_q(x) = 0$
2. $\sum_{x \in \mathbb{F}_q} \chi_q(x)\chi_q(x+y) = -1 \ \forall \ y \in \mathbb{Z}_q \setminus \{0\}$

Bizonyítás. 1. : mivel a |nemnulla négyzetelemek| = |nem négyzetlemek|, és q = |nemnulla négyzetelemek| + |nem négyzetelemek| + |0| így |nemnulla négyzetelemek| $= (q-1)/2$, tehát az állítást bebizonyítottuk.

2. : Vegyük észre, hogy ha $x \neq 0$, akkor

$$\chi_q(x)\chi_q(x+y) = \chi_q(x)\chi_q(x)\chi_q(1+yx^{-1}) = \chi_q(1+yx^{-1}).$$

Mivel x minden nemnulla értéket felvesz $\mathbb{F}_q$-ból és $y \neq 0$, így $1+yx^{-1}$ is minden F_q-beli értéket felvesz az 1-en kívül (mivel $x \neq 0$, így ezt csak az $y = 0$ helyen tudná felvenni). Tehát $\sum_{x\in\mathbb{F}_q} \chi_q(x)\chi_q(x+y) = \sum_{x\in\mathbb{F}_q, x\neq 0} \chi_q(1+yx^{-1}) = \sum_{x\in\mathbb{F}_q, x\neq 1} \chi_q(x) = \sum_{x\in\mathbb{F}_q} \chi_q(x) - \chi(1) = 0 - 1 = -1$. □

3.2.8. Definíció. *Egy $C = (c_{ij})$: $n \times n$ mátrixot* konferenciamátrixnak *hívunk, ha minden eleme $\{1, 0, -1\}$, $c_{ii} = 0\ \forall\ i \in \{1, 2, \ldots, n\}$, és $CC^T = (n-1)I_n$. Ha $c_{ij} = c_{ji}\ \forall\ i, j \in \{1, 2, \ldots, n\}$, akkor szimmetrikus konferenciamátrixnak hívjuk.*

3.2.9. Tétel. *Legyen $q \equiv 1\ (mod\ 4)$, prímhatvány, és $W = (w_{ij})$, ahol a sorok és az oszlopok indexei: $\mathbb{F}_q \cup \{\infty\}$, és* $w_{ij} = \begin{cases} 0, & ha\ i = j = \infty \\ 1, & ha\ i = \infty, j \neq \infty \\ 1, & ha\ j = \infty, i \neq \infty \\ \chi_q(i-j), & ha\ i, j \in \mathbb{F}_q \end{cases}$.
Ekkor W egy $q+1$ rendű szimmetrikus konferenciamátrix.

Bizonyítás. W főátlójában mindenhol 0 van, és mindenhol máshol ± 1 van.

Ekkor WW^T (i,i)-edik eleme q $(\forall\ i \in \mathbb{F}_q \cup \{\infty\})$.

$\chi(-1) = 1$, mivel $q \equiv 1\ (mod\ 4)$, tehát $w_{ji} = \chi(j-i) = \chi((-1)(i-j)) = \chi(-1)\chi(i-j) = (1)(\chi(i-j)) = w_{ij}$ Ezzel beláttuk, hogy W szimmetrikus.

Be kellene látnunk, hogy WW^T mindenhol máshol 0 értéket vesz fel. i, j szerinti esetszétválasztással mutatjuk ezt meg.

Legyen $i, j \in \mathbb{F}_q, i \neq j$. Ekkor a 3.2.7 lemma 2. része miatt miatt WW^T (i,j)-edik eleme: $1 + \sum_{h\in\mathbb{F}_q} \chi(i-h)\chi(j-h) = 1 + \sum_{x\in\mathbb{F}_q} \chi(x)\chi(x+y) = 1 + (-1) = 0$ $x = i-h$, $y = j-i$ helyettesítéssel. Tehát $i \neq j$ esetben pedig WW^T (i,j)-edik eleme 0.

A kimaradt esetek az (i, ∞), és (∞, j)-edik eleme WW^T-nek. Ekkor $0 \cdot 1 + \sum_{x\in\mathbb{F}_q} \chi(x) = 0$ a 3.2.7 lemma 1. része miatt, tehát WW^T ezen elemein is 0-t vesz fel.

Ezzel bebizonyítottuk, hogy W egy szimmetrikus konferenciamátrix. □

3.2.10. Példa. *Legyen $q = 5$. Ekkor a nemnulla négyzetelemek a $\{1, 4\}$, a nemnégyzetelemek a $\{2, 3\}$. Tehát $\chi(1) = \chi(4) = 1$, $\chi(2) = \chi(3) = -1$ és $\chi(0) = 0$.*

$$W = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 & -1 & -1 \\ 1 & 1 & 0 & 1 & -1 & -1 \\ 1 & -1 & 1 & 0 & 1 & -1 \\ 1 & -1 & -1 & 1 & 0 & 1 \\ 1 & 1 & -1 & -1 & 1 & 0 \end{pmatrix}$$ *mátrix szimmetrikus konferenciamátrix.*

Szimmetrikus konferenciamátrixok segítségével is tudunk Hadamard-mátrixokat konstruálni.

Most következik Paley 3.2.6 tételének második részének bizonyítása.

3.2.11. Tétel. *Legyen C egy ilyen 3.2.9 típusú $m \times m$ szimmetrikus konferenciamátrix, ahol $(m-1) \equiv 1 \pmod 4$. Ekkor $H = \begin{bmatrix} C + I_m & C - I_m \\ C - I_m & -C - I_m \end{bmatrix}$ mátrix egy $2m$ rendű Hadamard-mátrix.*

Bizonyítás. Mivel C szimmetrikus, így $H = H^T$, és H minden eleme ± 1.

$$HH^T = \begin{bmatrix} C + I_m & C - I_m \\ C - I_m & -C - I_m \end{bmatrix} \begin{bmatrix} C + I_m & C - I_m \\ C - I_m & -C - I_m \end{bmatrix} =$$
$$\begin{bmatrix} (C + I_m)^2 + (C - I_m)^2 & (C + I_m)(C - I_m) + (C - I_m)(-C - I_m) \\ (C - I_m)(C + I_m) + (-C - I_m)(C - I_m) & (C - I_m)^2(-C - I_m)^2 \end{bmatrix}$$

Ennek a blokkmátrixnak a blokkjait pedig külön kiszámolhatjuk.

$$(C + I_m)^2 + (C - I_m)^2 = 2C^2 + 2I_m^2 = 2(m-1)I_m + 2I_m = 2mI_m$$

$$(C + I_m)(C - I_m) + (C - I_m)(-C - I_m) = 0$$

$$(C - I_m)(C + I_m) + (-C - I_m)(C - I_m) = 0$$

$$(C - I_m)^2(-C - I_m)^2 = 2C^2 + 2I_m^2 = 2mI_m$$

Tehát $HH^T = \begin{bmatrix} 2mI_m & 0 \\ 0 & 2mI_m \end{bmatrix}$. □

3.2.12. Példa. *A 3.2.10 szimmetrikus konferenciamátrixból megkapjuk a következő*

12×12 *Hadamard-mátrixot.*

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 \\
1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\
1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 \\
-1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\
1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 \\
1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 \\
1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 \\
1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & -1
\end{pmatrix}$$

Most pedig Paley 3.2.6 tételének első részének bizonyítását készítjük elő.

3.2.13. Definíció. *Legyen $C = (c_{ij})$ egy $n \times n$ konferenciamátrix. Ezt antiszimmetrikusnak hívjuk, ha $\forall\, i \neq j \in \{1, 2, \ldots, n\}$-re $c_{ij} = -c_{ji}$*

3.2.14. Tétel. *Legyen q prímhatvány, amire $q \equiv 3\ (mod\ 4)$ és legyen $W = (w_{ij})$, ahol a sorok és az oszlopok indexei: $\mathbb{F}_q \cup \{\infty\}$, és*

$$w_{ij} = \begin{cases} 0, & ha\ i = j = \infty \\ 1, & ha\ i = \infty, j \neq \infty \\ -1, & ha\ j = \infty, i \neq \infty \\ \chi_q(i-j), & ha\ i, j \in \mathbb{F}_q \end{cases}.$$

Ekkor W egy $q+1$ rendű antiszimmetrikus konferenciamátrix.

Bizonyítás. W főátlójában mindenhol 0 van, és mindenhol máshol ± 1 van.

Ekkor WW^T (i,i)-edik eleme q ($\forall\, i \in \mathbb{F}_q \cup \{\infty\}$).

$\chi(-1) = -1$, mivel $q \equiv 3\ (mod\ 4)$, tehát $w_{ji} = \chi(j-i) = \chi((-1)(i-j)) = \chi(-1)\chi(i-j) = (-1)(\chi(i-j)) = -w_{ij}$ Ezzel beláttuk, hogy W antiszimmetrikus.

Be kellene látnunk, hogy WW^T mindenhol máshol 0 értéket vesz fel. i, j szerinti esetszétválasztással mutatjuk ezt meg.

Legyen $i, j \in \mathbb{F}_q, i \neq j$. Ekkor a 3.2.7 lemma 2. része miatt miatt WW^T (i,j)-edik eleme: $(-1)^2 + \sum_{h \in \mathbb{F}_q} \chi(i-h)\chi(j-h) = 1 + \sum_{x \in \mathbb{F}_q} \chi(x)\chi(x+y) = 1 + (-1) = 0$ $x = i - h,\ y = j - i$ helyettesítéssel. Tehát $i \neq j$ esetben pedig WW^T (i,j)-edik eleme 0.

A kimaradt esetek az (i, ∞), és (∞, j)-edik eleme WW^T-nek. Ekkor $0 \cdot (\pm 1) + \sum_{x \in \mathbb{F}_q} \chi(x) = 0$ a 3.2.7 lemma 1. része miatt.

Ezzel bebizonyítottuk, hogy W egy antiszimmetrikus konferenciamátrix. □

Most következik Paley 3.2.6 tételének első részének bizonyítása.

3.2.15. Tétel. *Legyen C egy ilyen 3.2.14 típusú $m \times m$ antiszimmetrikus konferenciamátrix, ahol $(m-1) \equiv 3 \pmod 4$. Ekkor $H = C + I_m$ mátrix egy m rendű Hadamard-mátrix.*

Bizonyítás. $I_m I_m = I_m$, $CI_m = 0$ és $I_m C^T = 0$, mivel C és C^T főátlójában csupa 0 van. Tehát a mátrixszorzás tulajdonságai miatt: $HH^T = (C + I_m)(C + I_m)^T = (C + I_m)(C^T + I_m^T) = CC^T + CI_m^T + I_m C^T + I_m I_m^T = (m-1)I_m + I_m = mI_m$. □

Most jön egy következő módszer, ami Williamson [14] nevéhez fűződik. Williamson észrevette, hogy ha adott néhány $n \times n$-es ± 1 elemű mátrix, amik bizonyos feltételeknek eleget tesznek, akkor ezekből előállíthatunk egy $4n \times 4n$-es Hadamard-mátrixot.

3.2.16. Tétel (Williamson)**.** *Legyenek A_1, A_2, A_3 és A_4 négyzetes n rendű ± 1 elemű mátrixok, melyekre teljesülnek az alábbi összefüggések:*

1. $A_1 A_1^T + A_2 A_2^T + A_3 A_3^T + A_4 A_4^T = 4nI_n$
2. $XY^T = YX^T \quad \forall X, Y \in \{A_1, A_2, A_3, A_4\}$

Akkor $H = \begin{bmatrix} A_1 & A_2 & A_3 & A_4 \\ -A_2 & A_1 & -A_4 & A_3 \\ -A_3 & A_4 & A_1 & -A_2 \\ -A_4 & -A_3 & A_2 & A_1 \end{bmatrix}$ *egy $4n$ rendű Hadamard-mátrix.*

Bizonyítás. Tekintsük az $M = HH^T$ mátrixot, mint egy blokkmátrixot $n \times n$-es blokkokkal. Ekkor:

$$M_{i,i} = A_1 A_1^T + A_2 A_2^T + A_3 A_3^T + A_4 A_4^T = 4nI_n \quad \forall i \in \{1, 2, 3, 4\}$$

$$M_{1,2} = -A_1 A_2^T + A_2 A_1^T - A_3 A_4^T + A_3 A_4^T = 0.$$

Hasonlóan ellenőrizhető, hogy bármely $i \neq j$-re, ha $i, j \in \{1, 2, 3, 4\}$, *akkor* $M_{i,j} = 0$. Ebből az következik, hogy:

$$M = HH^T = \begin{bmatrix} 4nI_n & 0 & 0 & 0 \\ 0 & 4nI_n & 0 & 0 \\ 0 & 0 & 4nI_n & 0 \\ 0 & 0 & 0 & 4nI_n \end{bmatrix} = 4nI_{4n}.$$

□

Ekkor a Sylvester konstrukcióval minden $n = 2^k,\ \forall k \in \mathbb{Z}, k \geq 1$-re létezik $n \times n$-es Hadamard-mátrix. Paley 1. konstrukciójával $n = p^\alpha + 1,\ ahol\ p^\alpha \equiv 3\ (mod\ 4)$ rendű Hadamard-mátrixot is létre tudunk hozni. Ekkor már $n = 11 + 1 = 12;\quad 19 + 1 = 20;\quad 23 + 1 = 24;\quad 3^3 + 1 = 28;\quad 43 + 1 = 44;\quad 47 + 1 = 48;\quad 59 + 1 = 60;\quad 67 + 1 = 68;\quad 71 + 1 = 72;\quad 79 + 1 = 80;\quad 83 + 1 = 84$-re is van konstrukciónk. Paley 2. konstrukciójával $n = 2(p^\alpha + 1),\ ahol\ p \equiv 1\ (mod\ 4)$ rendű Hadamard-mátrixot tudunk létrehozni. Így $n = 2(17 + 1) = 36;\quad 2(5^2 + 1) = 52;\quad 2(37 + 1) = 76;\quad 2(7^2 + 1) = 100$-ra ismerünk konstrukciókat. Ekkor $n = 40;\ 56;\ 88;\ 96$-ra Kronecker szorzás és Paley 1. konstrukciója segítségével tudunk Hadamard-mátrixot konstruálni. $40 = 20 \cdot 2;\quad 56 = 28 \cdot 2;\quad 88 = 44 \cdot 1;\quad 96 = 48 \cdot 2 = 24 \cdot 4 = 12 \cdot 8$. Williamson a módszerével $148 = 4 \cdot 34;\quad 172 = 4 \cdot 43$ rendű Hadamard-mátrixokra talált konstrukciót.

2005-ben Hadi Kharaghani és Behruz Tayfeh-Rezaie-nak sikerült konstruálniuk 428 rendű Hadamard-mátrixot, így jelenleg a legkisebb rend, amire nem tudjuk, hogy létezik-e Hadamard-mátrix az a 668.

4. fejezet

Kódelmélet

Először bevezetjük az alapvető kódelméleti fogalmakat, majd bemutatjuk a kapcsolatot bizonyos javító kódok és az Hadamard-mátrixok között. Ebben a fejezetben az [1], [11], [18], [19] könyveket vettük alapul.

A fejezet elején szeretnénk egy az emberi életben számos helyen előforduló gyakorlati problémán keresztül bemutatni a kódelméleti alapfogalmakat. Tegyük fel, hogy Alice egy *üzenetet* szeretne eljuttatni Bobhoz, de az üzenetet közvetítő *csatorna* zajos, azaz elképzelhető, hogy útközben az üzenet megváltozik és Bobhoz nem feltétlenül ugyanaz az üzenetet érkezik meg, amit Alice eredetileg el szeretett volna küldeni. Ennek kiküszöbülésére Alice és Bob megegyeznek egy *kódolási eljárásban*, amivel a küldeni kívánt üzeneteket átalakítják azzal a céllal, hogy a csatornában előforduló hibákat, sérüléseket utólag minél könnyebb legyen kiszűrni. Mivel Bob tisztában van azokkal a kódokkal, amik értelmes üzenetből származhatnak, ezért az általa kapott információ alapján megkeresi valamilyen módszerrel az ahhoz „legközelebbi" értelmes üzenetből kapható *kódszót* és az ennek megfelelő értelmes üzenetet tekinti az elküldeni kívánt eredeti üzenetnek. Ezt a lépést nevezzük *dekódolásnak*. Tipikusan az a cél, hogy Bob az esetleges módosulások ellenére is vissza tudja fejteni az Alice által küldeni kívánt üzenetet. Most pedig térjünk rá a fenti általános gyakorlati probléma matematikai modellezésére, a szükséges alapfogalmak definiálására.

4.1. Lineáris kódok

4.1.1. Definíció. *Legyen F_q egy q elemű ábécé, és F_q^n jelölje az összes n hosszú sorozatot, amit az F_q ábécé elemeiből képezhetünk. Ezeket a sorozatokat n hosszú* szavaknak *nevezzük. F_q^n részhalmazait n hosszú* kód*nak nevezzük.*

Az egyszerűség kedvéért általában az F_q^n-re tekinthetünk úgy is, mint egy n dimenziós vektortér elemeire az $\mathbb{F}_q$ q elemű véges test fölött. A dekódoláskor fontos szerepet játszik a kapott üzenetnek a kódszavainktól való távolsága, ezért bevezetünk egy távolságfogalmat.

Vezessünk be egy fogalmat két kódszó közötti távolságról.

4.1.2. Definíció (Hamming-távolság)**.** *Legyen $\underline{x}, \underline{y} \in \mathbb{F}_q^n$. Ekkor $\underline{x}$ és $\underline{y}$* Hamming távolsága *a $d(\underline{x}, \underline{y})$ érték, melyre $d(\underline{x}, \underline{y}) = |\{i : 1 \leq i \leq n;\ x_i \neq y_i\}|$*

A következő állítások ehhez a távolságfogalomhoz fognak kapcsolódni.

4.1.3. Definíció. *Egy C kód* minimális d távolsága *alatt a benne lévő különböző kódszavak Hamming-távolságainak minimumát értjük. Azaz $d = \min_{\underline{x},\underline{y} \in C} d(\underline{x}, \underline{y})$.*

4.1.4. Definíció. *Legyen $\underline{x} \in \mathbb{F}_q^n$. Ekkor $\underline{x}$ súlyán a $w(\underline{x}) = d(\underline{x}, \underline{0})$ értéket értjük, ahol $\underline{0}$ a 0-vektor $\mathbb{F}_q^n$-ben.*

4.1.5. Definíció. *Egy C kód* minimális súlya *alatt a benne lévő nemnulla kódszavak súlyainak minimumát értjük.*

4.1.6. Definíció. *$\varrho > 0$ és $\underline{x} \in \mathbb{F}_q^n$-re a ϱ* sugarú gömb *$\underline{x}$ körül: $B(\underline{x}, \varrho) = \{\underline{y} \in \mathbb{F}_q^n : d(\underline{x}, \underline{y}) \leq \varrho\}$.*

Most pedig bevezetjük egy speciális kódcsoport, a lineáris kódok fogalmát.

4.1.7. Definíció (Lineáris kód)**.** *Az $\mathbb{F}_q^n$ lineáris altereit $\mathbb{F}_q$ feletti* lineáris kódnak *nevezzük.*

Lineáris kódok esetén a minimális távolság és minimális súly fogalmak között a következő állítás teremt kapcsolatot.

4.1.8. Állítás. *A minimális távolság egy lineáris C kódban egyenlő a nemnulla kódszavak minimális súlyával.*

Bizonyítás. Legyen $\underline{x}, \underline{y} \in C$. Ekkor mivel C egy lineáris altér, így $\underline{x} - \underline{y} \in C$, és $d(\underline{x}, \underline{y}) = d(\underline{x} - \underline{y}, 0) = w(\underline{x} - \underline{y})$, és mivel $\underline{x} - \underline{y} \in C$, így az állítást bebizonyítottuk. □

Vezessünk be egy általános jelölést a véges testre épített kódokra.

4.1.9. Definíció. *Ha $C \subset \mathbb{F}_q^n$ egy k-dimenziós altér, azaz lineáris, és C minimális súlya d, akkor C-t egy $[n, k, d]_q$ kódnak nevezzük.*

Ha C nem lineáris, akkor a dimenzió helyett $M = |C|$, a kódszavak számát és minimális súly helyett pedig a minimális távolságot tüntetjük fel, tehát ekkor C-t egy $(n, M, d)_q$ kódnak nevezzük.

Vegyük észre, hogy lineáris kódra $M = q^k$ lenne.

4.1.10. Definíció. *Két lineáris kódot* ekvivalensnek*, nevezzük, ha egyik a másikból a koordináták permutációjával megkapható.*

Legyen $C \subset \mathbb{F}_q^n$ egy olyan kód, hogy bármely két $\underline{x}, \underline{y} \in C$-re $d(\underline{x}, \underline{y}) \geq 2e+1$, más szóval a kód minimális távolsága szigorúan nagyobb, mint $2e$. Vegyünk egy $\underline{x} \in C$ szót, és tegyük fel, hogy megváltoztatjuk $t \leq e$ koordinátáját. Ekkor az így kapott szó és a C-beli kódszavak Hamming-távolsága $\underline{x}$-re veszi fel a minimumát, tehát ha $t \leq e$ hibás koordináta van egy szóban, akkor az eredeti üzenet még dekódolható, a hibák kijavíthatóak.

4.1.11. Definíció. *Egy $C \subset \mathbb{F}_q^n$ kódot* e-hibajavítónak *hívunk, ha*
$\forall \underline{x}, \underline{y} \in C \; \underline{x} \neq \underline{y} \Longrightarrow d(\underline{x}, \underline{y}) \geq 2e + 1$.

Vegyük észre, hogy ekkor a C kódbeli szavak körüli e sugarú gömbök diszjunktak.

4.1.12. Definíció. *Egy $C \subset \mathbb{F}_q^n$ kódot* perfektnek *hívunk, ha a e-hibajavító, és $\cup_{\underline{x} \in C} B(\underline{x}, e) = \mathbb{F}_q^n$, azaz az e-sugarú gömbök egyrétűen lefedik $\mathbb{F}_q^n$-et.*

4.1.13. Tétel (Hamming-korlát)**.** *Ha egy $\mathbb{F}_q$ feletti $(n, M, d)_q$ kód e hibát javít, akkor*

$$M \sum_{i=0}^{e} \binom{n}{i} (q-1)^i \leq q^n.$$

Bizonyítás. A bal oldalon lévő összeg az e sugarú gömbben lévő vektorok számát adja meg minden kódszó körül, a jobb oldal pedig az összes lehetséges vektorok számát $\mathbb{F}_q^n$-ben. □

A 4.1.12 definíció értelmében pontosan a perfekt kódokra teljesül egyenlőség az előbbi tételben.

4.1.14. Állítás. *Ha létezik n hosszú, perfekt e-hibajavító kód q elemű ábécé felett, akkor $\sum_{i=0}^{e} \binom{n}{i}(q-1)^i$ osztója q^n-nek.*

Bizonyítás. Mivel a kód perfekt, így $M \sum_{i=0}^{e} \binom{n}{i}(q-1)^i = q^n$, tehát az állítást beláttuk. □

Ha a kód lineáris is, akkor $M = q^k$, tehát $\sum_{i=0}^{e} \binom{n}{i}(q-1)^i = q^{n-k}$.

A következőkben n hosszú lineáris kódok megadását fogjuk bemutatni generátormátrix segítségével.

4.1.15. Definíció. *Legyen $C \subset \mathbb{F}_q^n$ egy $[n,k,d]_q$ lineáris kód. Ekkor C* generátormátrixának *azt a G mátrixot hívjuk, aminek a soraiban C egy bázisa található. Ekkor a sorok lineáris kombinációjaként megkapjuk a kódszavakat, azaz úgy tudunk egy generátormátrixal kódolni, hogy megszorozzuk vele az üzenetet.*

Ha szeretnénk eldönteni hogy egy $w \in \mathbb{F}_q^n$ szó benne van-e C lineáris kódban, a $w = xG$ egyenletet kellene megoldanunk. Ezt egyszerűbben tudjuk megtenni C ortogonális kiegészítő mátrixának segítségével.

4.1.16. Definíció. *Egy $C \subset \mathbb{F}_q^n$ $[n,k,d]_q$ lineáris kód* duálisa $C^\perp = \{\underline{w} \in \mathbb{F}_q^n : \langle \underline{w}, \underline{x} \rangle = 0,\ \forall \underline{x} \in C\}$, *ahol $\langle \underline{x}, \underline{y} \rangle = \sum_{i=1}^n x_i y_i$ a skaláris szorzás $\underline{x} = (x_1, \ldots, x_n)$ és $\underline{y} = (y_1, \ldots, y_n)$ között $\mathbb{F}_q^n$ felett. Ekkor, ha H a $C^\perp$ duális kód generátormátrixa, akkor H-t a C kód* ellenőrző mátrixának *nevezzük.*

Ekkor H sorai ortogonálisak a kódszavakra, tehát $\underline{x} \in C$, ha $\underline{x}H^T = 0$.

Lineáris $[n,k,d]_q$ kód duálisa egy lineáris $[n, n-k, d']_q$ kód alkalmas d'-re.

4.1.17. Állítás. *Egy C $[n,k,d]_q$ lineáris kód minimális távolsága pontosan akkor d, ha az ellenőrző mátrix bármely $d-1$ oszlopa független, de van d oszlopa, melyek lineárisan összefüggők.*

Bizonyítás. A kód egy d súlyú vektora épp d oszlopra ad meg lineáris összefüggést, tehát van d oszlop, ami összefügg, de ha kevesebb is lenne, akkor lenne olyan vektor, aminek a súlya kevesebb, mint d lenne. □

4.1.18. Tétel (Singleton-korlát)**.** *Ha C lineáris $[n,k,d]_q$ kód, akkor $d \leq n-k+1$.*

Bizonyítás. Tekintsük C ellenőrzőmátrixát. Ennek a mérete $(n-k) \times n$, tehát a rangja legfeljebb $(n-k)$, tehát az oszloprangja is, így nem lehet $(n-k)$-nál több független oszlopa. □

4.1.19. Definíció (Reed-Muller-kód)**.** *Legyen $V : \mathbb{F}_2[x_1, \ldots, x_m] \to \mathbb{F}_2^H$, amely egy polinomhoz a $H = \{0,1\}^m$ m-dimenziós hiperkockán felvett értékét rendeli hozzá. Ekkor Reed-Muller-kódnak a $RM_{m,k} = \{V(f) :\ deg(f) \leq k,\ deg_{x_i}(f) \leq 1\}$kódot nevezzük.*

Megmutatható, hogy ezek a kódok lineárisak, és dimenziójuk $\sum_{i=0}^k \binom{m}{i}$.

4.1.20. Állítás. *$RM_{m,k}$ minimális távolsága 2^{m-k}.*

Bizonyítás. A tételt azon részét, hogy ennél kisebb súlyú kódszó nem lehet k és m szerinti teljes indukcióval bizonyítjuk be.

$k = 0$-ra teljesül, hogy a minimális távolság 2^m.

Tekintsük a k-adfokú $f = x_m g(x_1, \ldots, x_{m-1}) - h(x_1, \ldots, x_{m-1})$ multilineáris polinomot, ahol $deg(g) \leq k-1$ és $deg(h) \leq k$. Mivel k-nál kisebb fokú, vagy m-nél kevesebb változós polinomra igaz az állítást, így ennek a polinomnak a segítségével szeretnénk visszavezetni a feladatot.

Ha g vagy $g+h$ azonosan 0, akkor az indukciós feltevés miatt $2^{m-1-(k-1)} = 2^{m-k}$ olyan $m-1$ hosszú vektor van, amelyre f értéke nem 0. Ezeket $g \equiv 0$ esetben $x_m = 1$-el, a $g + h \equiv 0$ esetben $x_m = 0$-val kiegészítve 2^{m-k} olyan vektort kapunk, ahol f nem 0.

Ha sem g, sem $g + h$ nem azonosan 0, akkor $x_m = 0$-t helyettesítve a h, míg $x_m = 1$-et helyettesítve a $g - h$ polinomokhoz keresünk olyan vektort, ahol ők nem 0-k. Mivel mindkét polinom $(m-1)$ változós, ezért az indukciós feltevés miatt összesen $2^{m-1-k} + 2^{m-1-k} = 2^{m-k}$ olyan helyet jelent, ahol f nem 0.

Már csak az kell, hogy létezik 2^{m-k} súlyú kódszó, például $V(x_1 x_2 \ldots x_k)$, tehát a becslés éles.

Ezzel a teljes indukcióval beláttuk a feladatot. □

4.2. Hadamard-kódok

Ebben a részben megmutatjuk a kapcsolatot az Hadamard-mátrixok, és az Hadamard-kódok között.

Az Hadamard-kódok olyan hibajavító kódok, melyeket nagyon zajos csatornákon használnak. 1971-ben a NASA Mariner 9 űrhajója Marsról készült fényképek kódolására használta, melyeket a Földre küldött. A Mars 85%-át sikerült feltérképezni, több mint 7000 kép segítségével, például Naprendszerünk legnagyobb ismert hegyét az Olympos Mons-t, a Naprendszerünk legnagyobb ismert kanyonját a Valles Marinerist, és a két kis holdját a Phobos-t és a Deimos-t.

A képek elkódolására az $A = \begin{bmatrix} H_{32} \\ -H_{32} \end{bmatrix}$ mátrixot használták, ahol H_{32} a 32 rendű $H_{32} = H_2 \otimes H_2 \otimes H_2 \otimes H_2 \otimes H_2$ Hadamard-mátrix. Ekkor ez egy 64 sorú mátrix, és a kamera minden pixelre egy $0, \ldots, 63$ skálán megmondta hogy mennyire sötét egy képkocka, és ezeket kódolta el az A mátrix sorai szerint. Később belátjuk, hogy ez egy 7 hibajavító kódolás.

Azért volt szükség erre a kódolásra, mivel egy bit-hiba valószínűsége 10% volt, és javító kódolás nélkül az üzeneteknek körülbelül 47%-a hibás lett volna. Az Hadamard-kódok segítségével annak a valószínűsége, hogy hibás üzenetet kapunk

$0,01\%$-ra csökkent.

Kétféleképpen szokták definiálni az Hadamard-kódokat, most először a generátormátrixos változatot mutatjuk be.

4.2.1. Definíció (Hadamard-kód)**.** *Legyen H_n egy $n = 2^k$ rendű Hadamard-mátrix, ahol $H_n = \underbrace{H_2 \otimes \cdots \otimes H_2}_{k}$, Sylvester típusú. Cserélük ki a H_n mátrixban a -1-es elemeket 1-re, az 1-es elemeket meg 0-ra. Ekkor az így kapott $0-1$ mátrix 2^k sora alkotja az Hadamard-kód kódszavait. Ezeket a 2^k kódszavakból álló kódokat hívjuk Hadamard-kódoknak.*

A H_n Hadamard-mátrixban a sorok páronkénti ortogonalitásából következett, hogy minden nemnulla kódszó Hamming súlya pontosan 2^{k-1}, így a kód minimális távolsága is éppen 2^{k-1}.

Továbbá a Sylvester típusú Hadamard-mátrixból származó Hadamard-kód lineáris lesz, és így paraméterei: $[2^k, k, 2^{k-1}]_2$. Azonban ha egy tetszőleges Hadamard-mátrixból származó Hadamard-kódot tekintünk, akkor a linearitás nem feltétlenül teljesül, tehát akkor egy $(n, 2n, n/2)_2$ kódot kapunk.

A továbbiakban a (Sylvester típusú) lineáris Hadamard-kódokkal foglalkozunk, és megvizsgáljuk a kód egyéb módszerekkel való előállításait.

Tehát mivel H_{2^k}-hoz tartozó Hadamard-kód egy lineáris kód, így generátormátrixal is meglehet adni.

Egy tetszőleges $\underline{x} \in \{0,1\}^k$ üzenethez tartozó $Had(\underline{x})$-el jelölt kódszót definiálhatunk mod 2 skaláris szorzás segítségével is. Tekintsük a $\langle \underline{x}, \underline{y} \rangle = \sum_{i=1}^{k} x_i y_i \pmod 2$ értéket az összes $\underline{y} \in \{0,1\}^k$ vektorra. Az ezen értékekből álló 2^k hosszú sorozat lesz $Had(\underline{x})$, azaz $Had(\underline{x}) = \Big(\langle \underline{x}, \underline{y} \rangle\Big)_{\underline{y} \in \{0,1\}^k}$.

Ebből adódik a generátormátrixos megadás is. Vegyük ugyanis a $G = \begin{pmatrix} \underline{y}_1 & \underline{y}_2 & \dots & \underline{y}_{2^k} \end{pmatrix}$ mátrixot, ahol $\underline{y}_i \in \{0,1\}^k$ oszlopvektorok mátrixaként az $i.$ oszlop az $i.$ bináris vektor lexikografikus sorrendben. Ekkor könnyen látható, hogy $Had(\underline{x}) = \underline{x}G$ teljesülni fog tetszőleges $\underline{x} \in \{0,1\}^k$ üzenetre, tehát G a $[2^k, k, 2^{k-1}]_2$ lineáris Hadamard-kód generátormátrixa.

Ezzel beláttuk, hogy G egy $(k \times 2^k)$ méretű generátormátrixa a kódnak.

4.2.2. Példa. *$k = 3$-ra a generátormátrix:* $G = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$. *$k = 4$-re*

$$\textit{pedig } G = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Most pedig rátérünk a kiterjesztett Hadamard-kódokra, amiket az előzőekhez hasonló módon kaphatunk.

4.2.3. Definíció (kiterjesztett Hadamard-kód)**.** *Legyen H_n egy $n = 2^k$ rendű Hadamard-mátrix, ahol $H_n = \otimes_{i=1}^{k} H_2$, Sylvester típusú. Ekkor az $A = \begin{bmatrix} H_n \\ -H_n \end{bmatrix}$ mátrixban a (-1)-es elemeket kicseréljük 0-ra. Ekkor ez a 2^{k+1} sor 2^{k+1} darab 2^k hosszú kódszót ad. Ezeket a 2^{k+1} darab kódszavakból álló kódokat hívjuk kiterjesztett Hadamard-kódoknak.*

H_n és $-H_n$ sorainak páronkénti ortogonalitásából következik, hogy minden nem csupa nulla és nem csupa 1 kószó súlya pontosan 2^{k-1}, tehát az így kapott kód minimális távolsága is $2^k - 1$.

A Sylvester típusú Hadamard-mátrixból származó kiterjesztett Hadamard-kód is lineáris lesz $[2^k, k+1, 2^{k-1}]_2$ paraméterekkel.

Tehát ezeket a kiterjesztett Hadamard-kódokat is fel lehet írni generátormátrixszal.

Egy tetszőleges $\underline{x} \in \{0,1\}^k$ üzenethez tartozó $pHad(\underline{x})$-el jelölt kódszót definiáljunk az előzőekhez hasonló módon $pHad(\underline{x}) = \left(\langle \underline{x}, \underline{y} \rangle\right)_{\underline{y} \in \{1\} \times \{0,1\}^{k-1}}$-el.

Ebből adódik a generátormátrixos megadás is. Vegyük ugyanis a $G' = \begin{pmatrix} \underline{y}_1 & \underline{y}_2 & \dots & \underline{y}_{2^{k-1}} \end{pmatrix}$ mátrixot, ahol $\underline{y}_i \in \{0,1\}^k$, és $\underline{y}_{i_1} = 1$ oszlopvektorok. Ekkor könnyen látható, hogy $pHad(\underline{x}) = \underline{x}G$ teljesülni fog tetszőleges $\underline{x} \in \{0,1\}^k$ üzenetre, tehát G' a $[2^k, k+1, 2^{k-1}]_2$ lineáris Hadamard-kód generátormátrixa.

Ezzel beláttuk, hogy G' egy $(k \times 2^{k-1})$ méretű generátormátrixa a kódnak.

Ekkor az üzenet hossza egy Sylvester típusú H_n $(n = 2^k)$ Hadamard-kódnál $log_2(2n) = k + 1$ lehet.

Egy $C : [2^k, k+1, 2^{k-1}]_q$ kiterjesztett Hadamard-kód a 4.1.11 definíció miatt $2^{k-2} - 1$-hibajavító kód.

4.2.4. Definíció. *Egy C egy $(n,k,d)_q$ kódban tekintsük a $R = \frac{k}{n}$ információs rátát vagy más néven* kódsebességet.

Ez az információs ráta $R = \frac{k}{2^k}$ az első definícióban (4.2.1), és $R' = \frac{k+1}{2^k}$ a második definícióban (4.2.3), tehát a kiterjesztett Hadamard-kód kicsivel jobb, mint az Hadamard-kód, ugyanis ugyanakkora a minimális távolsága, és a hibajavító képessége, de az információs rátája egy kicsivel jobb.

A Mariner 9 egy $(32, 6, 16)_2$ lineáris kiterjesztett Hadamard-kódot használt, aminek információs rátája $\frac{6}{32}$-ed, ami azt jelenti, hogy egy 6 bit hosszú üzenetet egy 32 bit hosszú kódszó reprezentál.

Megjegyezzük, hogy a kiterjesztett Hadamard-kódok a Reed-Muller kódok speciális esetei a kételemű test fölött. Ráadásul csak akkor kapunk Reed-Muller kódot, ha $n = 2^k$ és az Hadamard-mátrix Sylvester típusú. Bose és Shrikhande 1959-ben [17] már készítettek nem Sylvester típusú Hadamard-mátrixból hasonló módon $(n, 2n, n/2)_2$ kódokat, amik viszont nem feltétlenül lineárisak.

4.2.5. Definíció. *Egy C egy $(n, k, d)_q$ kód optimális, ha R a lehető legnagyobb adott n, d és q értékekre.*

Általános Hadamard-mátrixok segítségével is tudunk létrehozni Hadamard-kódokat. Legyen H egy $n \times n$ méretű Hadamard-mátrix. Ekkor $A = \begin{bmatrix} H \\ -H \end{bmatrix}$-ban a (-1)-eket írjuk át 0-kra. Ekkor $2n$ darab kódszóból állnak A sorai és bármely kettő távolsága legalább $n/2$, mivel eredetileg ortogonálisak voltak H sorai, és a (-1)-el szorzás nem változtat az ortogonalitáson, csak a H i. sora és a hozzá tartozó $-H$ i. sorának a távolsága $n > n/2$.

Vegyük észre, hogy ez a kód nem feltétlenül lineáris, tehát nincs mindig generátormátrixa.

Tetszőleges k-ra a kiterjesztett Hadamard-kód generátormátrixa megegyezik a 2^{k-1} hosszú, $2^{k-1} - k$ dimenziójú kibővített Hamming-kód ellenőrző mátrixával. Ezt úgy is megfogalmazhatjuk, hogy a kiterjesztett Hadamard-kód a megfelelő kibővített Hamming-kód duálisa kódja.

Irodalomjegyzék

[1] T. Szőnyi, Szimmetrikus struktúrák. *Typotex*, (2014)

[2] T. P. Kirkman, On a Problem in Combinations. *The Cambridge and Dublin Mathematical Journal*, **II**:, (1847), 191–204.

[3] T. Skolem, Some Remarks on the Triple Systems of Steiner. *MATHEMATICA SCANDINAVICA*, **6**:, (1958), 273–280.

[4] Th. Beth, D. Jungnickel, H. Lenz, Design Theory, I–II, *Cambridge University Press*, (1999).

[5] R.H. Bruck, H.J. Ryser, The nonexistence of certain finite projective planes. *Canadian Journal of Mathematics*, **1**, (1949), 88-93.

[6] J. Hadamard R´esolution d'une question relative aux d´eterminants. *Bulletin des sciences math* **2**, 17 (1893), 240–248.

[7] S. Chowla, H.J. Ryser, Combinatorial problems. *Canadian Journal of Mathematics*, **2**, (1950), 93-99.

[8] H. Kharaghani, B. Tayfeh-Rezaie, A Hadamard matrix of order 428. *Journal of Combinatorial Designs*, **13**(6), (2005), 435-440.

[9] Douglas R. Stinson, Combinatorial Designs: Constructions and Analysis. *Springer*, (2004)

[10] Jacob Steepleton, Constructions of Hadamard-Matrices *Chancellor's Honors Program Projects*, (2019)

[11] P.J.Cameron, J.H. van Lint, Designs, Graphs, Codes and their Links *Cambridge University Press*, (1991)

[12] JORGE CASTINEIRA MOREIRA AND PATRICK GUY FARRELL, Appendix B: Galois Fields GF(q): Essentials of Error-Control Coding *John Wiley & Sons* (2006)

[13] PALEY, R.E.A.C., On orthogonal matrices *Journal of Mathematics and Physics* **12** (1993) 311-320.

[14] WILLIAMSON, JOHN, Hadamard's determinant theorem and the sum of four squares. *Duke Mathematical Journal* **11** (1944) 65-81.

[15] SCARPIS, UMBERTO, Sui determinanti di valore massimo, Rendiconti della R. *Istituto Lombardo di Scienze e Lettere* (1898) **31** 1441-1446.

[16] TAGOBA, MARCO, Properties of the Kronecker product *Lectures on matrix algebra* (2021)

[17] R.C. BOSE, S.S. SHRIKHANDE, A note on a result in the theory of code construction. *Information and Control*, **2** (2):, (1959), 183–194.

[18] RAYMOND NGUYEN, Hadamard-Matrices: Truth & Consequences *The University of Missouri Math 8190 (Master's Project)*

[19] MALEK, MASSOUD, Coding Theory: Hadarmark Codes *California State University, East Bay* (2006)