Szegedi Tudományegyetem
Természettudományi és Informatikai Kar
Bolyai Intézet

Egyszerű ortogonális tömbök paramétereinek becslései

DIPLOMAMUNKA

Készítette
KISS REBEKA
Matematikus MSc hallgató

Témavezető
DR. NAGY GÁBOR PÉTER
egyetemi tanár

Szeged
2022

Tartalomjegyzék

Bevezetés

Jelen diplomamunka tekinthető az alapszakos szakdolgozatom és a Nagy Gábor Péterrel írt közös cikkünk [6] folytatásának. Az utóbbi két év során mélyen beleástuk magunkat az ortogonális tömbök elméletébe, megismertük gyakorlati jelentőségüket és más matematikai struktúrákkal való összefonódásukat. Célul tűztük ki, hogy a terület vizsgálatát immáron haladó szinten végezve, a korábbiaknál meghatározóbb következtetéseket tudjunk levonni. A diplomamunka azon ortogonális tömbökre vonatkozó új eredményeket ismerteti, melyek a Claude Carlet-val és Nagy Gábor Péterrel végzett közös munkából erednek. A nyelvezet a [4] könyvben, a korábbi szakdolgozatban és a [6] cikkben szereplőeket követi, a negyedik és ötödik fejezetben olvasható eredmények az említett szerzők [3] munkájában megtalálhatók.

Mivel egy matematikus számára mindig szívmelengető látni, amikor az elmélet és a hús-vér valóság útja keresztezi egymást, ezért mindenekelőtt – motiválva az olvasót – leszögezzük, hogy bizonyos ortogonális tömbök vizsgálata kifejezetten fontos a gyakorlatban. Alkalmazásuk meghatározó a manapság széles körben kutatott kódoláselméletben, pontosabban bizonyos titkosító rendszerek létrehozásában. A munka első felében arra törekszünk, hogy átfogó képet adjunk az ortogonális tömbök tulajdonságairól, ismertessük a kódok és korreláció-immun függvények témáját, valamint azt, hogy utóbbiak az ortogonális tömbök elméletével kéz a kézben járnak. Felvértezve az így szerzett ismeretekkel, megcélozzuk a Claude–Guilley-sejtés megválaszolását. Szemünk előtt tartva ezt, a munka főtételeként megadunk egy elégséges feltételt ortogonális tömbök egyszerűségére. Ennek következményeként részleges eredményeket érünk el a fenti sejtés igazolásában.

1. fejezet

Ortogonális tömbök

Mielőtt az ortogonális tömbök vizsgálatának mélyére ásnánk, ismertetjük ezek definícióját, lényegesebb tulajdonságaikat és néhány alapvetően fontos rájuk vonatkozó, később gyakran említésre kerülő állítást. A diplomamunka során Hedayat, Sloane és Stufken szerzők [4] monográfiájának jelöléseit és nyelvezetét használjuk.

1.1. Alapfogalmak

Az ortogonális tömbök speciális tulajdonságokkal rendelkező számtáblázatok. Jellemzésük négy paraméterrel történik, ebből három a tömb megjelenéséről szolgáltat információt (sorok száma, oszlopok száma, lehetséges szimbólumok), míg a negyedik érték a bizonyos méretű résztáblázatok valamilyen értelemben vett teljességét követeli meg.

1.1. Definíció. *Az $N \times k$ méretű A mátrix ortogonális tömb s szinttel és t erősséggel ($0 \leq t \leq k$), ha elemei az $S = \{0, 1, ..., s-1\}$ halmazból kerülnek ki, és bármely t darab oszlopát kiválasztva az így kapott $N \times t$ méretű részmátrixban pontosan ugyanannyiszor szerepel az összes olyan t hosszú sorozat, amelynek elemei S-ből valók.*

- A fenti mátrix jelölése: $OA(N, k, s, t)$.
- A definícióban szereplő "pontosan ugyanannyiszor" érték egyértelműen meghatározott rögzített N, s és t értékek mellett. A $\lambda = \frac{N}{s^t}$ pozitív egész paramétert az ortogonális tömb indexének nevezzük. Rögtön következik, hogy rögzített s és t esetén a tömb sorainak számára s^t valamely többszöröse adódik. Így például az $s = 2, t = 2$ esetben az összes létező $OA(N, k, 2, 2)$ ortogonális tömb sorszáma 4-gyel osztható.
- Alkalmazhatósági okokból eredően a leggyakrabban az $s = 2$ esetet vizsgáljuk, ekkor a tömbök elemei 0, 1-esek.

- Szintén gyakorlati szempontból olyan ortogonális tömbökkel kívánatos dolgozni, amelyekben nincsenek többszörösen szereplő sorok. Ezeket egyszerű ortogonális tömböknek hívjuk.

1.2. Definíció. *Egy ortogonális tömb egyszerű, ha sorai között nincs ismétlődés.*

Amennyiben s prím, úgy $S = GF(s) = \{0, 1, \ldots, s-1\}$ egy s elemű véges testet alkot a modulo s szerinti összeadásra és szorzásra nézve. Abban az esetben, ha s nem prím, de prímhatvány, szintén létezik s elemű végest test, aminek elemeire most szintén $0, 1, \ldots, s-1$-ként hivatkozunk. Ezek után ha s prímhatvány, úgy $OA(N, k, s, t)$ minden sora felfogható úgy, mint s elemű test feletti k-dimenziós vektortér eleme. Itt két vektor összegén a komponensenkénti modulo s összeadást, valamint adott vektor $c \in GF(s)$ skalárszorosán a c skalárral való komponensenkénti modulo s szorzást értjük. Ezek után természetesen adódik a lineáris ortogonális tömbök fogalma.

1.3. Definíció. *Legyen s prímhatvány, $GF(s) = \{0, 1, \ldots, s-1\}$. Azt mondjuk, hogy $A = OA(N, k, s, t)$ ortogonális tömb lineáris, ha egyszerű, és a sorainak megfelelő vektorok alteret alkotnak $GF(s)^k$-ban. Másszóval, amennyiben R_1 és R_2 sorok A-ban, úgy bármely $c_1, c_2 \in GF(s)$ esetén $c_1R_2 + c_2R_2$ is az.*

A definícióból azonnal következik, hogy lineáris ortogonális tömbök esetén $N = s^n$ valamely $0 \leq n \leq k$ egészre. Ekkor n-et a lineáris ortogonális tömb dimenziójának hívjuk.

1.4. Példa. *Keressünk $OA(4, 3, 2, 2)$ tömböket. A többes szám nem véletlen, adott paraméterekre nem csak egyetlen ortogonális tömb létezik. Az alábbi két tömbre teljesül, hogy akárhogyan is hagyunk el belőlük egy-egy oszlopot, a visszamaradó részmátrixban a $00, 01, 10, 11$ kettősök ugyanannyiszor, $\lambda = 1$-szer jelennek meg. Az első ortogonális tömb lineáris és dimenziója 2, míg a második nemlineáris ortogonális tömb.*

$$\begin{array}{ccc} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{array} \qquad \begin{array}{ccc} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{array}$$

1.2. Tulajdonságok

Ebben az alfejezetben ismertetjük azokat a tulajdonságokat, amelyeket a későbbi eredmények bemutatásakor, igazolásakor felhasználunk.

1.5. Tulajdonság. *Ortogonális tömbből oszlopokat törölve ortogonális tömböt kapunk, nevezetesen $OA(N,k,s,t)$ bármely $N \times k'$-s részmátrixa $OA(N,k',s,t')$, ahol $t' = min\{k',t\}$.*

Megjegyezzük, hogy egyszerű ortogonális tömbből oszlopokat törölve sorismétlődés léphet fel. Következésképpen azt nem állíthatjuk, hogy egyszerű ortogonális tömbök oszlopait elhagyva továbbra is egyszerűeket kapunk.

Könnyen meggondolhatjuk, hogy ha A ortogonális tömb t erősséggel, akkor minden $t' < t$ esetén A tetszőleges $N \times t'$ méretű részmátrixában az összes t' hosszú sorozat pontosan ugyanannyiszor szerepel. Ebből következik a második tulajdonság.

1.6. Tulajdonság. *Minden s szintű, t erősségű ortogonális tömb t' erősségű is tetszőleges $0 \leq t' < t$-re. Ekkor a t' erősségű tömb indexe: $\lambda \cdot s^{t-t'}$, ahol λ a t erősséghez tartozó index.*

1.7. Tétel. *Legyen $A = OA(N,k,s,t)$ ortogonális tömb valamely s prímhatványra. Ekkor A bármely t darab oszlopa lineárisan független $GF(s)$ felett.*

Bizonyítás. Legyen $v_1,\ldots,v_t$ az $A = OA(N,k,s,t)$ ortogonális tömb tetszőleges t darab oszlopa, a hozzájuk tartozó részmátrixot jelöljük A_0-lal. Tegyük fel, hogy

$$c_1v_1 + \ldots + c_tv_t = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \in GF(s)^N, \quad c_1,\ldots,c_t \in GF(s).$$

Mivel A t erősségű ortogonális tömb, így a t-hosszú $10\ldots0$ szerepel sorként A_0-ban, amiből $c_1 = 0$. Hasonlóan $010\ldots0$-ra $c_2 = 0$, és így tovább, $0\ldots01$-re $c_t = 0$. Azt kapjuk, hogy a 0_N csupán a $v_1,\ldots,v_t$ oszlopvektorok triviális lineáris kombinációjaként jöhet létre, így a kiválasztott t oszlop valóban lineárisan független. □

1.8. Tétel. *Legyen A olyan $N \times k$ méretű mátrix $GF(s)$ felett, melynek sorai alteret alkotnak $GF(s)^k$-ban. Ha A tetszőleges t oszlopa lineárisan független $GF(s)$ felett, úgy A $OA(N,k,s,t)$ ortogonális tömb.*

Bizonyítás. Tegyük fel, hogy a tételben szereplő altér n dimenziós, azaz $N = s^n$. Legyen G az A mátrix egy $n \times k$ méretű generátormátrixa. Ez azt jelenti, hogy A sorai

pontosan azok a k hosszú vektorok, amelyek előállnak G sorainak $GF(s)$ feletti lineáris kombinációjaként, azaz $u = \xi G$ alakban, valamely $\xi = (\xi_1, \ldots, \xi_n) \in GF(s)^n$ vektorra. Válasszunk ki A-ból t darab oszlopot, és jelöljük ezt az $N \times t$ méretű részmátrixot A_1-gyel. Legyen G_1 az A_1 mátrixnak megfelelő $n \times t$ méretű részmátrix G-ből. Ha G_1 oszlopai lineárisan függőek lennének, úgy létezne $0 \neq \eta \in GF(s)^t$, amelyre $G_1\eta^T = 0_n$. Ekkor mivel A_1 minden sora előáll G_1 sorainak lineáris kombinációjaként, $A_1\eta^T = 0_n$ is teljesülne, ami ellentmondana a t darab oszlop megkövetelt függetlenségének. G_1 oszlopai tehát lineárisan függetlenek, az általuk alkotott vektorrendszer t rangú. Lineáris algebrából tudjuk, hogy ekkor a G_1 soraiból alkotott vektorrendszer is t rangú. Rögzítsünk egy $z \in GF(s)^t$ vektort. A_1-ben pontosan annyiszor szerepel z, ahány $\xi \in GF(s)^n$ esetén teljesül a $\xi G_1 = z$ egyenlőség. Válasszuk ki G_1 sorainak egy bázisát, és tekintsük az ettől diszjunkt $n - t$ darab sort G_1-ben. Legyen ξ_0 tetszőleges $GF(s)^{n-t}$-beli vektor. ξ_0-t az imént említett $n - t$ elemű sorrendszer együtthatóvektorának választva az adódó lineáris kombináció egy $v \in GF(s)^t$ vektor. Ugyanakkor a másik t darab, bázist alkotó vektor lineáris kombinációjaként egyértelműen megadható $z - v$, legyen a megfelelő együtthatóvektor $\xi_1 \in GF(s)^t$. Ekkor ha a G_1 sorainak együttes lineáris kombinációját vesszük a megfelelő, imént leírt együtthatókkal, úgy $v + (z - v) = z$-t kapjuk. Abból, hogy ξ_0 megválasztására s^{n-t} lehetőség van, következik, hogy pontosan $s^{n-t} = \frac{N}{s^t}$ darab ξ teljesíti a vizsgált $\xi G_1 = z$ egyenlőséget. Mivel z és A_1 választása tetszőleges volt, így pontosan a t erősségű ortogonális tömbök definíciójában szereplő feltételt láttuk be. □

1.9. Tétel. *A $\{0, 1, \ldots, s-1\}$ halmaz elemeiből álló $N \times k$ méretű mátrix pontosan akkor $OA(N, k, s, t)$, ha bármely olyan $v \in \{0, 1, \ldots, s-1\}^k$ esetén, amely w darab nemnulla elemet tartalmaz, $1 \leq w \leq t$,*

$$\sum_{u \text{ sor } A\text{-ban}} \zeta^{uv^T} = 0, \tag{1.1}$$

ahol $\zeta = e^{2\pi\mathrm{i}/s}$ s-edik egységgyök, és uv^T modulo s számolandó.

Mielőtt bebizonyítanánk a tételt, megjegyezzük, hogy $s = 2$ esetben ez éppen azt jelenti, hogy egy $N \times k$ méretű bináris A mátrix pontosan akkor $OA(N, k, 2, t)$, ha

$$\sum_{\text{u sor } A\text{-ban}} (-1)^{uv^T} = 0 \tag{1.2}$$

minden olyan k hosszú bináris v vektorra, ami pontosan w darab egyest tartalmaz, ahol $1 \leq w \leq t$.

Bizonyítás. Legyen először $s = 2$, $A = OA(N, k, 2, t)$ és $v \in GF(2)^k$ ennek tetszőleges sora w darab ($1 \leq w \leq t$) egyessel. Jelöljük $i_1, \ldots, i_w$-vel ($1 \leq i_1 < \ldots < i_w \leq k$) azon indexeket, amelyeknek megfelelő komponensekben v egyest tartalmaz. Jelöljük A-nak ezen indexű oszlopaiból álló $N \times w$ méretű részmátrixát A'-vel. Tudván, hogy A t erősségű, az 1.6 Tulajdonság alapján w erősségű is, vagyis A' soraiban minden w hosszú bináris sorozat pontosan $\frac{N}{2^w}$-szer szerepel. Legyen u egy tetszőleges sor A-ból. Amennyiben u' és v' jelöli azokat a vektorokat, amelyek rendre u és v A'-re való megszorításai, úgy abból, hogy v' A'-n kívül mindenütt 0, adódik, hogy $uv^T = u'v'^T$. Ugyanakkor mivel v' minden eleme egyes, így $u'v'^T$ pontosan az u'-ben szereplő egyesek számával egyezik meg. Kihasználva A w erősségét, az utóbbi szerint számolva a tételben szereplő szummát, adódik, hogy

$$\begin{aligned}\sum_{\text{u sor } A\text{-ban}} (-1)^{uv^T} &= \sum_{\text{u' sor } A'\text{-ben}} (-1)^{u'v'^T} \\ &= \frac{N}{2^w}\left(\binom{w}{0} \cdot (-1)^0 + \binom{w}{1}(-1)^1 + \ldots + \binom{w}{w} \cdot (-1)^w\right) \\ &= \frac{N}{2^w}\left(\binom{w}{0} - \binom{w}{1} + \ldots + (-1)^w\binom{w}{w}\right) = 0,\end{aligned}$$

hiszen a Pascal háromszögben az egy sorban álló számokat váltakozó előjellel összeadva nullát kapunk. Az $s > 2$ eset belátása hasonlóan történik, ezt az olvasóra bízzuk.

A másik irány belátását ismét a bináris esettel kezdjük, mutatunk egy példát $s = 2, t = 2$ paraméterekre, ezzel vázolva az általános bizonyítás gondolatmenetét. Tegyük fel, hogy (1.2) teljesül a bináris $N \times k$ méretű A mátrixra. Megmutatjuk, hogy A első két oszlopa a $00, 01, 10, 11$ párok mindegyikét pontosan ugyanannyiszor tartalmazza. Jelölje rendre ezen előfordulások számát $n_{00}, n_{01}, n_{10}, n_{11}$. Ezek összege az A mátrix sorszámával egyenlő. Válasszuk v-nek sorra a $010\ldots0, \quad 100\ldots0, \quad 110\ldots0$ vektorokat. Ekkor v választásaiból és (1.2)-ből adódik a következő egyenletrendszer.

$$\begin{aligned} n_{00} + n_{01} + n_{10} + n_{11} &= N \\ n_{00} - n_{01} + n_{10} - n_{11} &= 0 \\ n_{00} + n_{01} - n_{10} - n_{11} &= 0 \end{aligned}$$

$$n_{00} - n_{01} - n_{10} + n_{11} = 0$$

Nyilvánvalóan az $n_{00} = n_{01} = n_{10} = n_{11} = N/4$ megoldása a fenti egyenletrendszernek. Mivel az

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

együttható mátrix invertálható, így a megoldás egyértelmű. Vegyük észre, hogy A bármely két oszlopára tárgyalhattuk volna a fentieket, amiből következik, hogy A $OA(N, k, 2, 2)$. Az általános eset bizonyítása éppígy adódik. Jelölje $n(i_1, \ldots, i_t)$ az $(i_1, \ldots, i_t)$ $(0 \leq i_r \leq s-1)$ vektor előfordulásainak számát az aktuálisan vizsgálandó t oszlopos részmátrixban. Legyen v sorra azon s^t darab különböző k hosszú vektor, amely a vizsgált indexű komponenseken tetszőleges értéket vehet fel $\{0, 1, \ldots, s-1\}$-ből, míg a többi komponensben 0. Ekkor s^t darab egyenlet adódik az s^t darab $n(i_1, \ldots, i_t)$ ismeretlenre. Ha v az azonosan 0 vektor, úgy az adott egyenlet jobb oldalán N áll, az összes többi esetben 0. Ekkor az összes $n(i_1, \ldots, i_t)$ ismeretlennek az N/s^t értéket adva az egyenletrendszer egy megoldását kapjuk. A fenti, speciális esethez hasonlóan az együtthatómátrix itt is invertálható, így ez a megoldás az egyetlen. Ezzel teljesül a t erősségű ortogonális tömb definíciójában szereplő feltétel. □

A következő tétel [4, Theorem 2.24.] a $2u$ és $2u+1$ erősségű ortogonális tömbök szoros összefüggését mutatja. A fennálló ekvivalencia nagyon hasznosnak bizonyult a vizsgálódásaink során, hisz így mindvégig elegendő volt csak a páros erősségű esetekkel foglalkoznunk.

1.10. Tétel. *Legyenek N, k és u rögzített pozitív egészek. $OA(N, k, 2, 2u)$ pontosan akkor létezik, ha $OA(2N, k+1, 2, 2u+1)$ létezik.*

Bizonyítás. Legyen A $OA(2N, k+1, 2, 2u+1)$. Az 1.6 Tulajdonság miatt A 1 erősségű is, így speciálisan a tömb első oszlopában ugyanannyi egyes van, mint nulla. Változtassuk meg a sorok sorrendjét úgy, hogy az első N darab 0-val, a második N darab 1-gyel kezdődjön. Az így kapott tömb első N sorát véve, és ennek első oszlopát törölve $OA(N, k, 2, 2u)$-t kapunk, ezzel adódik a tétel egyik irányú állítása.

Az ellentétes irányhoz vegyünk egy λ indexű $A = OA(N, k, 2, 2u)$-t. Adjuk meg A-ból az $\overline{A}$ ortogonális tömböt úgy, hogy nullák helyett egyeseket, egyesek helyett

nullákat írunk. Írjunk A után egy csupa 0-ból, $\overline{A}$ után pedig egy csupa 1-ből álló oszlopot, és jelöljük az így kapott mátrixokat A_1 és A_2-vel. Megmutatjuk, hogy ezeket egymás alá helyezve a kapott B mátrix λ indexű $OA(2N, k+1, 2, 2u+1)$. Nyilvánvalóan az első 3 paraméter egyből adódik a konstrukcióból, egyetlen dolgunk maradt hátra, belátni, hogy $t = 2u+1$ esetén B tetszőleges $2N \times t$ méretű részmátrixában minden bináris t hosszú sorozat λ sorban szerepel. Vizsgáljuk B-nek tetszőleges t darab oszlopát. Ha ezek közé beválasztottuk az utolsót, akkor az A ortogonális tömb $2u$ erősségéből adódik a bizonyítandó. Feltéve, hogy $k > 2u$, hátramaradt azon eset, amikor a kiválasztásban nem szerepel az utolsó oszlop. Az általánosság megszorítása nélkül feltehetjük, hogy a vizsgálandó részmátrix B első t oszlopából áll. Adott bináris t-hosszú $v = v_1 \dots v_t$ esetén jelöljük $n(v)$-vel azon A-beli sorok számát, amelyek v-vel kezdődnek. Ekkor B v-vel kezdődő sorainak száma $n(v) + n(\overline{v})$. Meg kell mutatnunk, hogy ez a szám minden lehetséges v esetén éppen λ-val egyenlő. Mivel A $t-1$ erősségű, így tudjuk, hogy ha v' pontosan egy helyen különbözik v-től, akkor $n(v) + n(v') = \lambda$. Adódik, hogy ha v és v'' pontosan két helyen különböznek, akkor

$$n(v) - n(v'') = n(v) + n(v') - (n(v') - n(v'')) = 0,$$

ahol v' olyan, hogy v-től és v''-től is pontosan 1 helyen tér el. Folytatva a leírtakat, következik, hogy amennyiben v és w páros sok helyen különböznek, akkor $n(v) = n(w)$. Mivel $\overline{v}$ és v' $2u$ helyen térnek el, így adódik, hogy $n(\overline{v}) = n(v')$ és ebből $n(v) + n(\overline{v}) = n(v) + n(v') = \lambda$, amit épp bizonyítani akartunk. □

1.11. Megjegyzés. *Figyeljük meg, hogy mi történik, ha az előző tétel bizonyításában mindkét irány tárgyalásakor egyszerű ortogonális tömbökből indulunk ki. Ha az első esetben leírt "felezés" eredményeképpen olyan tömb jön létre, melyben van ismétlődő sor, akkor tekintve az eredeti tömbben az ezeknek megfelelő sorokat, itt is egyezést találunk, ami ellentmond a kiinduló tömb egyszerűségének. Következésképpen, ha az eljárást egyszerű tömbökre alkalmazzuk, úgy csakis egyszerűeket kaphatunk. Ami a második esetet illeti, feltéve, hogy A egyszerű, következik, hogy A_1, és így $\overline{A}$ és A_2 is az. Ha A_1-et és A_2-t egymás alá helyezzük, semelyik két sor nem lehet azonos. Valóban, ha azok lennének, akkor az egyezés az említett egyszerűségek miatt csak úgy jöhetne létre, ha az egyik sor az A_1-ből, a másik pedig A_2-ből származna, amik utolsó koordinátájukban biztosan eltérőek.*

1.12. Következmény. *Legyenek N, k, u rögzített pozitív egészek. Pontosan akkor létezik egyszerű $OA(N, k, 2, 2u)$, ha egyszerű $OA(2N, k+1, 2, 2u+1)$ létezik.*

1.3. Nyitott problémák

Természetes módon merül fel a kérdés, hogy bizonyos paraméterek rögzítése mellett mik az extremális esetek. Nevezetesen, rögzítsünk le k, s, t értékeket, és vizsgáljuk meg, hogy mi a legkisebb N érték, amire létezik $OA(N, k, s, t)$ ortogonális tömb. Az így kapott értéket a későbbiekben $F(k, s, t)$-vel jelöljük. Ennél még nehezebb feladat, ha olyan minimális méretű tömböket keresünk, amelyek egyszerűek is, ekkor az $F^*(k, s, t)$ paramétert vizsgáljuk.

A diplomamunka legnagyobb motivációját ez a kérdéskör adta, így a fenti két paraméter nem meglepő módon kiemelt figyelmet kap a továbbiakban. Most megadjuk a rájuk vonatkozó formálisabb definíciókat is.

1.13. Definíció. *Legyenek k, s, t rögzített pozitív egész értékek, ahol, $t \leq k$. Ekkor*

$$F(k, s, t) = \min\{N \mid \exists\, OA(N, k, s, t)\},$$
$$F^*(k, s, t) = \min\{N \mid \exists\, \textit{egyszerű}\ OA(N, k, s, t)\}.$$

Használva, hogy egyszerű ortogonális tömb egyben általános ortogonális tömb is, természetesen adódik, hogy

$$F(k, s, t) \leq F^*(k, s, t). \tag{1.3}$$

Az elmúlt évben egy $F^*(k, 2, t)$ paramétert érintő sejtés megválaszolásán dolgoztunk, amely Claude Carlet és társszerzője, Sylvian Guilley [1, 2] nevéhez kapcsolódik. Az egyelőre megválaszolatlan kérdés korreláció-immun függvényekre vonatkozik, de a későbbi fejezetekben meglátjuk, hogy ekvivalensen megadható ortogonális tömbök nyelvezetén is.

1.14. Sejtés (Carlet–Guilley)**.** *Legyen t rögzített pozitív egész. Ekkor $F^*(k, 2, t)$ monoton nemcsökkenő sorozatot ad k függvényében.*

1.15. Megjegyzés. *A Carlet–Guilley-sejtés általános ortogonális tömböket tekintve egyértelműen teljesül. Valóban, ez éppen az 1.5 Tulajdonság közvetlen következménye, hisz $OA(F(k, s, t), k, s, t)$-ből oszlopokat elhagyva $OA(F(k, s, t), k', s, t)$ adódik, vagyis minden*

$t \leq k' \leq k$-ra

$$F(k', s, t) \leq F(k, s, t). \tag{1.4}$$

Speciálisan, minden k pozitív egészre

$$F(k, s, t) \leq F(k+1, s, t). \tag{1.5}$$

Egyszerű ortogonális tömbök esetén az okozza a nehézséget, hogy azokból oszlopokat elhagyva a visszamaradó tömbben előfordulhat sorismétlődés.

Látván, hogy az általános ortogonális tömbök értékes tulajdonságokkal bírnak, hasznos lehet megvizsgálni azon eseteket, amikor az F és F^* paraméterek egyenlőek.

1.16. Probléma. *Adjuk meg azon k, s, t hármasokat, melyekre $F(k, s, t) = F^*(k, s, t)$ teljesül.*

Ha adott k, s, t paraméterek ilyenek, úgy (1.3)-ből és az 1.15 Megjegyzésből adódik, hogy

$$F^*(k, s, t) = F(k, s, t) \leq F(k+1, s, t) \leq F^*(k+1, s, t).$$

1.4. Előzetes eredmények

Ismét csak azon előzményeket említjük [4]-ből, amelyek hozzájárultak a negyedik fejezetben ismertetett eredményeink igazolásához. Az első és legfontosabb ilyen eredmény a Rao–egyenlőtlenség, amely alsó korlátot ad $F(k, s, t)$-re, azaz a rögzített k, s, t paraméterekhez tartozó minimális sorszámra.

1.17. Tétel. *[4, Theorem 2.1.] Tetszőleges $OA(N, k, s, t)$ paraméterei kielégítik az alábbi egyenlőtlenségeket:*

$$N \geq \sum_{i=0}^{u} \binom{k}{i} \cdot (s-1)^i, \quad \text{ha } t = 2u,$$

$$N \geq \sum_{i=0}^{u} \binom{k}{i} \cdot (s-1)^i + \binom{k-1}{u} (s-1)^{u+1}, \quad \text{ha } t = 2u+1.$$

Megmutatjuk az 1.10 Tétel és az 1.12 Következmény alkalmazását az F és F^* paraméterekre vonatkozóan.

1.18. Tétel. *Legyenek k, u rögzített pozitív egészek. Ekkor*

$$2F(k,2,2u) = F(k+1,2,2u+1) \quad \textit{és} \quad 2F^*(k,2,2u) = F^*(k+1,2,2u+1). \tag{1.6}$$

2. fejezet

Kódok

Ebben a fejezetben számot adunk a hibajavító kódokról, valamint ortogonális tömbökkel való kapcsolatukról. Nevezetesen, egy kód kódszavait mátrix soraiba írva ortogonális tömböt kapunk, valamint fordítva, egy ortogonális tömb sorai kódot alkotnak. Felhasználva az összefüggést, bevezetjük és kimondjuk Delsarte lineáris programozási korlátjáról szóló tételét.

2.1. Bevezetés

A hibajavító kódok – nem meglepő módon – információk zajos csatornán keresztüli továbbítása során fellépő hibák javítására szolgálnak.

Rögzítsünk egy s méretű $S = \{0, \ldots, s-1\}$ szimbólumhalmazt, erre később ábécéként hivatkozunk. Jelölje S^k az S feletti k hosszú vektorok halmazát, vagyis $|S^k| = s^k$. Ennek tetszőleges C részhalmazát hibajavító kódnak vagy egyszerűen csak kódnak nevezzük, elemeit pedig kódszavaknak.

Egy $u = (u_1, \ldots, u_k) \in S^k$ kódszó Hamming súlyán u nemnulla komponenseinek számát értjük, és $w(u)$-val jelöljük. Továbbá, $u, v \in S^k$ Hamming távolsága $\mathrm{dist}(u, v) = w(u - v)$, azaz azon pozíciók száma, ahol u és v különbözik. A C kód minimália távolsága $d = \min_{u,v \in C, u \neq v} dist(u, v)$, vagyis a minimális távolság C két különböző kódszava között. Amennyiben egy kód üres, akkor a minimális távolságát nem definiáljuk, továbbá ha csak egyetlen kódszót tartalmaz, úgy megállapodás szerint $d = k + 1$. Ezen választás oka világossá válik a későbbi 2.11 Példa során.

Habár a kódoláselméletben jellemzően nem engedjük meg kódszavak ismétlődését, a mostani tárgyalásban ezt mégis megtesszük, hiszen az ortogonális tömbök akár többszörös multiplicitással is tartalmazhatnak sorokat.

Ha a $C \subseteq S^k$ kód N darab kódszóból áll, akkor azt mondjuk, hogy k hosszú, N méretű és d minimális távolságú az s elemű ábécé felett, vagy formálisan egy $(k, N, d)_s$ kód.

Gyakorlati alkalmazást tekintve csupán azon kódok vizsgálandók, melyekben

nem lép fel ismétlődés, ezeket egyszerű kódoknak nevezzük. Könnyen meggondolható, hogy egy egyszerű kód d minimális távolsággal legfeljebb $e = \lfloor (d-1)/2 \rfloor$ hiba javítására képes, ezért e-hibajavító kódnak nevezzük.

2.1. Példa. *$C = \{00000, 11111\}$ egy $(5,2,5)_2$ kód, ami legfeljebb $e = \lfloor (5-1)/2 \rfloor = 2$ hiba javítására képes, vagyis dupla hibajavító kód. Valóban, tegyük fel, hogy az elküldött kódszó a* 00000*, míg a zajos csatornán való továbbítás eredményeképp a címzett a* 10100 *üzenetet kapja. Ekkor a fogadó fél megkeresi azt a kódszót, ami a kapotthoz legközelebb áll, s így a kapott üzenetet* 00000*-ként dekódolja, vagyis a kommunikáció sikeresen lezajlik. Ugyanakkor, ha a hibák száma* 3 *lett volna, és az* 10110 *üzenet érkezik meg hozzá, akkor a dekódoló hibásan azt gondolná, hogy valószínűleg az* 11111 *üzenetet akarták elküldeni neki.*

A kódoláselmélet egyik központi problémája megtalálni rögzített k, s, d értékek esetén N maximális értékét úgy, hogy létezzen $(k, N, d)_s$ egyszerű kód. A gyakorlatban ugyanakkor olyan kódokkal szeretnénk dolgozni, amelyekkel kódolni és dekódolni is könnyű, ilyenek lehetnek a lineáris kódok.

2.2. Lineáris kódok

A kódokat tekintve a linearitás igazán hasznos tulajdonságnak bizonyul.

2.2. Definíció. *Egy k hosszú C kód lineáris, ha a kódszavai különböznek és C altér S^k-ban. Ekkor C méretére $N = s^n$ adódik valamely $0 \leq n \leq k$ nemnegatív egészre, ahol n-et a kód dimenziójának hívjuk.*

Tetszőleges lineáris kód tartalmazza a hosszának megfelelő csupa 0 vektort. Ebből adódik, hogy lineáris kódok minimális távolsága megegyezik a nemnulla kódszavak súlyának minimumával, azaz $d = \min_{u \in C, u \neq 0} w(u)$.

2.3. Megjegyzés. *Egy n-dimenziós lineáris kód egyértelműen meghatározható egy $n \times k$ méretű G generátormátrixszal úgy, hogy G sorai a kód – azaz az S^k-beli altér – bázisát adják. Ekkor a kódszavak azon u vektorok lesznek, amelyekre $u = xG$ valamely $x \in S^n$-re. Mindig kiválasztható olyan generátormátrix, amely $G = [I_n A]$ alakú, ahol A $n \times (k-n)$ méretű mátrix S felett.*

2.4. Megjegyzés. *Egy másik, alternatív mód n-dimenziós lineáris C kód meghatározására az úgynevezett P ellenőrző mátrix megadása. Itt P olyan $(k-n) \times k$ méretű mátrix S felett, melynek sorai kifeszítik a C lineáris kód által meghatározott lineáris altér ortogonális terét. Másszóval C elemei azok az $u \in S^k$ vektorok, melyekre $Pu^T = 0_{k-n}$.*

Ha a generátormátrix $G = [I_n A]$ alakú, akkor a megfelelő ellenőrző mátrix $P = [-A^T I_{k-n}]$.

2.5. Példa. *A 2.1 Példa-beli* $C = \{00000, 11111\}$ 1*-dimenziós lineáris kód* $\{0, 1\}$ *felett. A hozzá tartozó generátormátrix* $G = [11111]$*, míg ellenőrző mátrixa*

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

Minden C lineáris kódhoz megadható annak duálisa, ez szintén egy lineáris kód. Számunkra nagy jelentőséggel bír a dualitás, erről a következő alfejezetben részletesen beszélünk.

2.6. Definíció. *Azt mondjuk, hogy a* $C^\perp$ *kód duálisa a* k*-hosszú* C *lineáris kódnak, ha kódszavai pontosan azok a* $v \in S^k$ *vektorok, melyekre*

$$uv^T = 0 \quad \textit{minden} \quad u \in C \quad \textit{esetén}.$$

Tetszőleges k-hosszú lineáris kód duálisa nemüres, hisz tartalmazza a $(0 \dots 0)$ k-hosszú nullvektort.

A következő tétel a lineáris kódok és duálisaik paraméterei, generátormátrixai és ellenőrző mátrixai között ad kapcsolatot.

2.7. Tétel. *Legyen* C $(k, s^n, d)_s$ *lineáris kód. Ekkor*

(a) $C^\perp$ *egy* $(k, s^{k-n}, d^\perp)_s$ *duális kód valamely* $d^\perp$ *pozitív egészre.*

(b) C *tetszőleges generátormátrixa ellenőrző mátrixa* $C^\perp$*-nak, és fordítva,* C *bármely ellenőrző mátrixa* $C^\perp$ *egy generátormátrixát adja.*

(c) $(C^\perp)^\perp = C$.

A tételben szereplő $d^\perp$ értéket a C lineáris kód duális távolságának nevezzük. Megjegyezzük, hogy a tétel nem mond semmit d és $d^\perp$ kapcsolatáról.

2.3. Ortogonális tömbök és kódok kapcsolata

Ebben az alfejezetben bemutatjuk a lineáris ortogonális tömbök és lineáris kódok közötti fontos összefüggést.

Elöljáróban leszögezzük, hogy bármely – akár lineáris, akár nem – $OA(N,k,s,t)$ ortogonális tömbbel azonosítható egy $(k,N,d)_s$ kód valamely d pozitív egészre úgy, hogy a kódszavakat a tömb sorai adják. Ez fordítva is igaz, bármely $(k,N,d)_s$ kód kódszavait egy mátrix soraiba írva $OA(N,k,s,t)$ ortogonális tömböt kapunk valamely t nemnegatív egészre. Megjegyezzük, hogy nincsen összefüggés az ortogonális tömb erőssége és a kód minimális távolsága között, a későbbiekben viszont látni fogjuk, hogy a kód duális távolsága annál inkább meghatározó a megfeleltetés során.

A következő tétel rögtön következik a lineáris ortogonális tömbök és lineáris kódok definíciójából.

2.8. Tétel. *Adott kódhoz a fenti értelemben tartozó ortogonális tömb pontosan akkor lineáris, ha a kód is az.*

Ezek után értelemszerűen adódik, hogy mit hívunk egy lineáris ortogonális tömb ellenőrző mátrixának és duálisának. Előbbi a tömbnek megfelelő lineáris kód tetszőleges ellenőrző mátrixa, utóbbi a szóbanforgó kód duálisával azonosítható ortogonális tömb. Az A ortogonális tömb duális ortogonális tömbjének sorai között tehát pontosan akkor szerepel a v vektor, ha minden A-beli u sor esetén $uv^T = 0$.

Az alábbi tétel Bose 1961-es eredménye, mely megadja, hogy lineáris ortogonális tömb erőssége milyen módon határozható meg a kapcsolódó lineáris kód paramétereiből. Felhívjuk a figyelmet arra, hogy a tömb t erőssége és a kód d minimálisa távolsága direkt módon nem függ egymástól, az eredmény jelentőségét ez az észrevétel adja. Tulajdonképpen a tétel első fele Kempthorne-nak tulajdonítható (1947), míg az általánosítását Delsarte adta meg 1973-ban (lásd később, 2.19 Tétel).

2.9. Tétel. *Ha C egy $GF(s)$ feletti $(k,N,d)_s$ lineáris kód $d^\perp$ duális távolsággal, úgy kódszavai egy lineáris $OA(N,k,s,d^\perp-1)$ ortogonális tömb sorait adják. Fordítva, lineáris $OA(N,k,s,t)$ sorai, mint kódszavak, egy $(k,N,d)_s$ lineáris kódot alkotnak $d^\perp \geq t+1$ duális távolsággal. Ha az ortogonális tömb t, de nem $t+1$ erősségű, akkor $d^\perp = t+1$.*

Bizonyítás. Tegyük fel, hogy C a tétel első felében megjelenő lineáris kód az ott leírt tulajdonságokkal, A azon $N \times k$ méretű mátrix, melynek sorait C kódszavai adják. Ekkor A tetszőleges $d^\perp - 1$ oszlopa lineárisan független S felett. Valóban, ha valamely $1 \leq i_1 < i_2 < \ldots < i_{d^\perp-1} \leq k$ egészekre az A mátrix $i_1, i_2, \ldots, i_{d^\perp-1}$ indexű oszlopai lineárisan függőek lennének, úgy léteznének olyan $c_{i_1}, c_{i_2}, \ldots, c_{i_{d^\perp-1}} \in S$ számok, melyek nem mindegyike 0, és a szóbanforgó oszlopok ezen együtthatókkal vett lineáris kombinációja az N hosszú nullvektort adná ki. Ez ugyanakkor azt

is jelentené, hogy az A duálisának megfelelő $C^\perp$ lineáris kódban szerepel az a vektor, melynek i_j-edik koordinátája c_{i_j}, míg a többi 0. Ezen vektor Hamming távolsága 0-nál nagyobb, de legfeljebb $d^\perp - 1$, vagyis C duális távolsága $d^\perp - 1$ vagy annál kisebb, amivel ellentmondásra jutnánk. Az igazolt függetlenségből és az 1.8 Tételből rögtön következik a tétel ezen iránya.

A másik irányhoz legyen C az $A = OA(N, k, s, t)$ lineáris ortogonális tömbhöz tartozó lineáris kód. Az 1.7 Tétel szerint a tömb bármely t darab oszlopa lineárisan független, így az A duálisában szereplő nemnulla sorok mindegyike – a duális definíciójából adódóan – legalább $t+1$ nemnulla elemet tartalmaz. Ebből $C^\perp$ minimális súlya, így minimális távolsága is legalább $t+1$. Ugyanakkor ha A már nem $t+1$ erősségű, akkor valamely $t+1$ darab oszlopa lineárisan függő, jelöljük az ezek által alkotott részmátrixot A_0-lal. Ekkor létezik $0 \neq \xi \in GF(s)^{t+1}$, hogy $A_0\xi = 0$. Ezzel azt kaptuk, hogy $A^\perp$-ban benne van az a k hosszú vektor, amely az említett $t+1$ komponensben a megfelelő ξ_i elemeket tartalmazza, a többi helyen 0-át. Ez alapján van olyan $C^\perp$-beli kódszó, amelynek Hamming súlya $t+1$, vagyis $d^\perp = t+1$. □

2.10. Példa. *A 2.1 Példában szereplő* $C = \{00000, 11111\}$ *olyan* $(5, 2, 5)_2$ *lineáris kód, amelynek duális távolsága* $d^\perp = 2$. *Ekkor* $C^\perp$ *a 2.7 Tétel alapján egy lineáris* $(5, 16, 2)_2$. *Felhasználva a 2.9 Tételt adódik, hogy C kódszavai egy* $OA(2, 5, 2, 1)$ *ortogonális tömb sorait adják (nem túl érdekes eset), míg* $C^\perp$ *ekvivalens egy* $OA(16, 5, 2, 4)$ *tömbbel.*

2.11. Példa. *Vegyük azt a* $C = (5, 32, 1)_2$ *lineáris kódot, ami az összes* $GF(2)$ *feletti* 5 *hosszú vektort tartalmazza. Gondoljuk meg, hogy C kódszavait sorokba írva* $OA(32, 5, 2, 5)$ *tömböt kapunk* $\lambda = 1$ *indexszel. Ugyanakkor a kód duálisában csak a* 00000 *kódszó szerepel, így* $C^\perp$ *minimális távolsága megállapodás szerint* $k + 1 = 6$. *Erre alkalmazva a 2.9 Tételt, a kapott eredmény valóban egybecseng* $OA(32, 5, 2, 5)$*-tel.*

2.4. Lineáris Programozási korlát

Az alfejezetben bemutatjuk a 2.9 Tétel általánosítását, amely alkalmazható nemlineáris kódok, ortogonális tömbök esetén is. Erre az eredményre épül a Lineáris Programozási tétel, ami a Rao-korlátnál élesebb alsó becslést ad $F(k, s, t)$-re.

Ahhoz, hogy az LP-tételt kimondhassuk, szükségünk van nemlineáris kódok duális távolságának definiálására. Ehhez először bevezetjük a kódokhoz tartozó súlyeloszlásokat és súlypolinomokat.

2.12. Definíció. *A C $(k, N, d)_s$ kód súlyeloszlása az $u \in C$ kódszóra nézve az a $k+1$ hosszú, nemnegatív egészeket tartalmazó $(A_0(u), \ldots, A_k(u))$ vektor, amelyben $A_i(u)$ megadja az u kódszótól pontosan i Hamming távolságra fekvő C-beli kódszavak számát.*

2.13. Definíció. *A C $(k, N, d)_s$ kód súlyeloszlása az a $k+1$ hosszú, nemnegatív racionális számokat tartalmazó $(A_0, \ldots, A_k)$ vektor, amelyben*

$$A_i = \frac{1}{N} \sum_{u \in C} A_i(u), \quad 0 \leq i \leq k.$$

Adott kód minimális távolsága az a d legnagyobb pozitív egész, amelyre

$$A_1 = \cdots = A_{d-1} = 0.$$

Valóban, ha a kód minimális távolsága d, úgy bármely két különböző kódszó legalább ennyi pozícióban tér el egymástól, vagyis tetszőleges $u \in C$-re $A_i(u) = 0$ minden $i = 1, \ldots, d-1$ esetén. Definíciójából következik, hogy ezen i indexekre A_i is 0. Ugyanakkor léteznie kell C-ben két kódszónak, u-nak és v-nek, hogy $w(u-v) = d$. Ekkor $A_d(u)$ és $A_d(v)$ is pozitív egészek, amiből $A_d > 0$ következik.

Fordítva, ha $A_1 = \cdots = A_{d-1} = 0$ igaz, úgy a tagok nemnegativitása miatt $A_1(u) = \cdots = A_{d-1}(u) = 0$ minden $u \in C$-re, ami épp azt jelenti, hogy a minimális távolság d vagy annál nagyobb. Ugyanakkor mivel $A_d = 0$ már nem teljesül, így valamely $u \in C$-re $A_d(u) \geq 1$, vagyis van olyan v kódszó, amelyre $w(u-v) = d$, így C minimális távolsága éppen d.

2.14. Definíció. *A C kód súlypolinomján a*

$$W_C(x, y) = \sum_{i=0}^{k} A_i x^{k-i} y^i$$

homogén polinomot értjük. Ennek foka megegyezik a kód hosszával.

Tetszőleges $(k, N, d)_s$ kód esetén

$$\sum_{i=0}^{k} A_i = \frac{1}{N} \sum_{u \in C} \sum_{i=0}^{k} A_i(u) = \frac{1}{N} N^2 = N. \tag{2.1}$$

Teljesül továbbá, hogy

$$\begin{aligned} &A_0 \geq 1, \\ &A_1 = A_2 = \ldots = A_{d-1} = 0, \\ &A_i \geq 0, \quad \text{minden } 0 \leq i \leq k \text{ esetén.} \end{aligned} \tag{2.2}$$

Egy kód akkor és csak akkor egyszerű, ha $A_0 = 1$.

Amennyiben egy kód lineáris, úgy súlypolinomjából explicit módon megadható a duális kódjának súlypolinomja. Ez az eredmény F. J. MacWilliams nevéhez fűződik. Erre a tételre úgy tekintünk, mint motiváció nemlineáris kódok duális távolságának definiálására.

2.15. Tétel. *A C $(k, s^n, d)_s$ lineáris kód esetén*

$$W_{C^\perp}(x, y) = \frac{1}{N} W_C(x + (s-1)y, x - y). \tag{2.3}$$

A tétel bizonyítását most nem közöljük, azonban jelentését az alábbi példával illusztráljuk.

2.16. Példa. *A 2.1 Példa-beli $C = \{00000, 11111\}$ lineáris kód esetén $A_0 = 1, A_1 = A_2 = A_3 = A_4 = 0, A_5 = 1$. Ebből*

$$W_C(x, y) = x^5 + y^5.$$

A 2.15 Tételt alkalmazva

$$\begin{aligned} W_{C^\perp}(x, y) &= \frac{1}{2} W_C(x + y, x - y) \\ &= \frac{1}{2} \left((x+y)^5 + (x-y)^5 \right) = x^5 + 10x^3y^2 + 5xy^4. \end{aligned}$$

Valóban, $C^\perp$-ban 16 darab 5 hosszú kódszó szerepel, pontosan azok, amelyek páros sok darab 1-est tartalmaznak, hisz csak ezeknek lesz 0 az (11111) vektorral vett skaláris szorzatuk. Összesen $\binom{5}{2} = 10$ darab olyan vektor van, amelyben 2 darab egyes és $\binom{5}{4} = 5$ olyan, amelyben 4 darab egyes van. A 16. kódszó a 00000. Ekkor $A_0^\perp = 1, A_2^\perp = 10, A_4^\perp = 5, A_1^\perp = A_3^\perp = A_5^\perp = 0$.

Továbbra is lineáris kódokat vizsgálunk, legyen a C $(k, s^n, d)_s$ lineáris kód duálisának, $C^\perp$-nak a súlyeloszlása $(A_0^\perp, \ldots, A_k^\perp)$. Ekkor a 2.15 Tétel egyenlősége azt

állítja, hogy

$$\sum_{i=0}^{k} A_i^{\perp} x^{k-i} y^i = \frac{1}{N} \sum_{j=0}^{k} A_j (x + (s-1)y)^{k-j} (x-y)^j.$$

Kifejtve a jobb oldalt azt kapjuk, hogy

$$A_i^{\perp} = \frac{1}{N} \sum_{j=0}^{k} A_j P_i(j), \quad 0 \le i \le k, \tag{2.4}$$

ahol

$$P_i(z) = \sum_{r=0}^{i} (-1)^r (s-1)^{i-r} \binom{z}{r} \binom{k-z}{i-r}, \quad 0 \le i \le k, \tag{2.5}$$

és

$$\binom{z}{r} = \frac{z(z-1)\dots(z-r+1)}{r!}.$$

A (2.5)-beli P_i-t Krawtchouk-polinomnak nevezzük.

Mivel $(A_0^{\perp}, \dots, A_k^{\perp})$ az s^{k-n} méretű, $d^{\perp}$ minimális súlyú lineáris duális kód súlyeloszlása, így $\sum_{i=0}^{k} A_i^{\perp} = s^k/N$, továbbá

$$\begin{aligned} &A_0^{\perp} = 1, \\ &A_1^{\perp} = A_2^{\perp} = \dots = A_{d^{\perp}-1}^{\perp} = 0, \\ &A_i^{\perp} \ge 0, \quad \text{minden } 0 \le i \le k \text{ esetén.} \end{aligned} \tag{2.6}$$

Mint már említettük, a 2.15 Tétel és annak (2.4) következménye motiválja a nemlineáris kódok duális távolságának definícióját. Nevezetesen, nemlineáris esetben is megadhatjuk a (2.3)-beli duális súlypolinomot és (2.4)-beli duális súlyeloszlást. Ekkor $(A_0^{\perp}, \dots, A_k^{\perp})$-t a súlyeloszlás MacWilliams transzformáltjának nevezzük.

A 2.18 Tételben megmutatjuk, hogy nemlineáris kódok esetén is igaz, hogy $A_i^{\perp} \ge 0$ minden i-re. A következő fontos lépés, hogy nemlineáris kód duális távolságának – a lineáris esethez hasonlóan – azt a $d^{\perp}$ legnagyobb pozitív egészet definiáljuk, amelyre

$$A_1^{\perp} = \dots = A_{d^{\perp}-1}^{\perp} = 0.$$

Amennyiben $A_1^{\perp} = \dots = A_k^{\perp} = 0$, akkor $d^{\perp}$-t megállapodás szerint $k+1$-nek választjuk. Mivel $P_0(j) = 1$ minden $0 \le j \le k$ esetén, így (2.1)-ből és (2.4)-ből $A_0^{\perp} = \frac{1}{N} \sum_{j=0}^{k} A_j = 1$ adódik. Vegyük észre, hogy a leírtak alapján a (2.6)-beli egyen-

lőségek és egyenlőtlenségek nemlineáris kódok esetén is teljesülnek.

Mielőtt bebizonyítanánk a duális súlyok nemnegativitását, megadjuk $s = 2$ esetben a Krawtchouk polinomok egy egyszerű tulajdonságát.

2.17. Tétel. *Legyen $v \in GF(2)^k$ olyan, hogy $w(v) = j$ valamely $0 \leq j \leq k$-ra. Ekkor*

$$\sum_{w(u)=i} (-1)^{uv^T} = P_i(j), \tag{2.7}$$

ahol a szummázás az összes i súlyú, $GF(2)^k$-beli vektorra történik.

Bizonyítás. Könnyű meggondolni, hogy $\binom{j}{r}\binom{k-j}{i-r}$ olyan i súlyú $u \in GF(2)^k$ létezik, mely pontosan r darab ($0 \leq r \leq i$) pozícióban tartalmaz úgy egyest, hogy ezeken a helyeken v is egyest tartalmaz. Ekkor $uv^T = r$, így a (2.7) bal oldalán szereplő kifejezés

$$\sum_{r=0}^{i} (-1)^r \binom{j}{r}\binom{k-j}{i-r},$$

ami éppen $P_i(j)$ az $s = 2$ esetben. □

2.18. Tétel. *Tetszőleges $GF(s)$ feletti $(k, N, d)_s$ kód duális súlyeloszlására*

$$A_i^{\perp} \geq 0, \quad 0 \leq i \leq k.$$

A tétel bizonyítást csak az $s = 2$ esetben írjuk le.

Bizonyítás. Legyen $s = 2$. Definíció szerint

$$A_j = \frac{1}{N} \sum_{u \in C} A_j(u) = \frac{1}{N} \sum_{\substack{x,y \in C \\ \mathrm{dist}(x,y)=j}} 1.$$

Ekkor (2.7) alapján

$$\begin{aligned} A_i^{\perp} = \frac{1}{N} \sum_{j=0}^{k} A_j P_i(j) &= \frac{1}{N^2} \sum_{j=0}^{k} \sum_{\substack{x,y \in C \\ \mathrm{dist}(x,y)=j}} \sum_{w(v)=i} (-1)^{(x-y)v^T} \\ &= \frac{1}{N^2} \sum_{w(v)=i} \sum_{x,y \in C} (-1)^{xv^T} (-1)^{yv^T} \qquad (2.8) \\ &= \sum_{w(v)=i} \left(\frac{1}{N} \sum_{x \in C} (-1)^{xv^T} \right)^2 \geq 0. \end{aligned}$$

□

Most már kimondhatjuk a régóta áhított, Delsarte nevéhez kapcsolódó tételt, amely immáron tetszőleges ortogonális tömbök és kódok kapcsolatát hivatott kifejezni. Delsarte tételét csak az $s = 2$ esetben bizonyítjuk.

2.19. Tétel. *Amennyiben C $(k, N, d)_s$ kód $d^\perp$ duális távolsággal, úgy kódszavai egy $OA(N, k, s, d^\perp - 1)$ ortogonális tömb sorait adják. Fordítva, $OA(N, k, s, t)$ sorai, mint kódszavak egy $(k, N, d)_s$ kódot alkotnak $d^\perp \geq t + 1$ duális távolsággal. Ha az ortogonális tömb t, de nem $t + 1$ erősségű, akkor $d^\perp = t + 1$.*

Bizonyítás. Feltesszük, hogy $s = 2$. Ha C duális távolsága $d^\perp$, akkor $A_1^\perp = \cdots = A_{d^\perp - 1}^\perp = 0$. A (2.8)-beli egyenlőségekből következik, hogy minden v esetén, melyre $1 \leq w(v) \leq d^\perp - 1$,

$$\sum_{x \in C} (-1)^{xv^T} = 0.$$

Használva az 1.9 Tétel $s = 2$-re vonatkozó (1.2) állítását, adódik, hogy C kódszavai ortogonális tömböt alkotnak $d^\perp - 1$ erősséggel. Fordítva, ha az ortogonális tömb t erősségű, akkor (1.2)-ból és (2.8)-ből következik, hogy $A_1^\perp = \cdots = A_t^\perp = 0$ és így $d^\perp \geq t + 1$. Végül, ha a tömb t, de nem $t + 1$ erősségű, akkor $A_1^\perp = \cdots = A_t^\perp = 0$ és $A_{t+1}^\perp > 0$, s így $d^\perp = t + 1$. □

2.20. Példa. *Vegyük a $C = \{000, 000, 011, 011, 101, 101, 110, 110\}$ nem egyszerű és nemlineáris kódot $GF(2)$ felett. Ennek súlyeloszlása*

$$W_C(x, y) = 2x^3 + 6xy^2.$$

Ekkor a 2.15 Tételből

$$W_{C^\perp}(x, y) = \frac{1}{8}\left(2(x + y)^3 + 6(x + y)(x - y)^2\right) = x^3 + y^3,$$

vagyis $d^\perp = 3$. Valóban teljesül, hogy C kódszavait sorokba írva az adódó ortogonális tömb $OA(8, 3, 2, 2)$.

Megjegyezzük, hogy a 2.18 Tétel nem olyan "ártatlan", mint amilyennek tűnik. Az $A_i^\perp \geq 0$ egyenlőtlenségek erős lineáris feltételeket adnak adott kód súlyeloszlására.

Ahogyan azt már az 1.3. Fejezetben leírtuk, egyik célunk $F(k, s, t)$ meghatározása rögzített k, s, t paraméterek esetén. Vizsgáljuk a problémát kódok oldaláról.

Tegyük fel, hogy adott k, s, d értékekre C egy $(k, N, d)_s$ kód $d^\perp$ duális távolsággal. Nehéz megmondani, hogy milyen lehetőségek adódnak ekkor N értékére, viszont alsó becslést minden esetben tudunk adni. Tudjuk, hogy bármely létező kód $(A_0, \ldots, A_k)$ súlyeloszlása és $(A_0^\perp, \ldots, A_k^\perp)$ duális súlyeloszlása kielégíti (2.2) és (2.6) egyenlőségeit és egyenlőtlenségeit. Ezentúl a kódszavak száma éppen

$$N = A_0 + A_1 + \ldots + A_k.$$

A későbbiekben a (2.2) második sorában szereplő $A_1 = A_2 = \ldots = A_{d-1} = 0$ feltételeket figyelmen kívül hagyjuk, hiszen ahogyan a 2.19 Tételben láttuk, ortogonális tömb paraméterei nem függnek az ekvivalens kód minimális távolságától.

Amennyiben megtaláljuk azt a legkisebb – nem feltétlenül egész – értéket $A_0 + A_1 + \ldots + A_k$-ra, amely nem sérti meg a szükséges lineáris feltételeket, úgy biztosan alsó korlátot kapunk az N paraméter értékére. Az $N_{LP}(k, d^\perp)$ minimális értéket Delsarte Lineáris Programozási korlátjának hívjuk.

2.21. Tétel. *Legyen $N_{LP}(k, d^\perp)$ a következő lineáris programozási feladat megoldása:*

$$\textit{Minimalizáljuk } A_0 + \ldots + A_k\textit{-t}$$

feltéve, hogy

$$A_0 \geq 1, \quad A_i \geq 0, \quad 1 \leq i \leq k, \tag{2.9}$$

$$B_0 \geq 1, \quad B_i \geq 0, \quad 1 \leq i \leq k, \tag{2.10}$$

$$B_1 = \ldots = B_t = 0, \tag{2.11}$$

ahol

$$B_i = \sum_{j=0}^{k} A_j P_i(j), \quad 0 \leq i \leq k,$$

$t = d^\perp - 1$ és P_i a (2.5)*-beli Krawtchouk-polinom. Ekkor tetszőleges $OA(N, k, s, t)$ ortogonális tömbre*

$$N \geq N_{LP}(k, d^\perp).$$

2.22. Következmény. *Adott k, s, t értékekre*

$$F(k, s, t) \geq N_{LP}(k, t + 1).$$

3. fejezet

Korreláció-immun függvények

A korreláció-immun Boole-függvényeket – röviden CI-függvényeket – speciális tulajdonságaik miatt előszeretettel használják titkosítási eljárásokban. Alkalmazásukkal a kriptorendszerek képesek bizonyos támadások kivédésére, ezzel növelve saját biztonságukat. A 20. század végéig a CI-függvényeket a Siegenthaler-féle korrelációs támadással szembeni ellenállásra használták kombináló függvényekként a folyamatos rejtjelezőkben (*stream cipher*). Az új évszázad beköszöntével azonban olyan támadások jöttek létre, amelyek a titkosító függvények alacsony fokszámában rejlő gyengeségeket különösen hatékonyan használták ki. Az úgynevezett Siegenthaler-korlát miatt a korreláció-immun függvények sajnálatos módon éppen ilyenek.

Az utóbbi időben ezen függvények vizsgálata mégis virágkorát éli, ami annak köszönhető, hogy hatékony védelmet nyújtanak a gyakorlatban különösen veszélyes oldalcsatornás támadások ellen is. Az említettekről a második alfejezetben részletesebben is beszélünk.

3.1. Korreláció-immun Boole-függvények

A Boole-függvények tárgyalását egy olyan példával kezdjük, amely Thor Martinsen [7] munkájának 3. Fejezetében szerepel.

3.1. Definíció. *Ha f egy $\mathbb{F}_2^k$-ból $\mathbb{F}_2$-be képező függvény, akkor k-változós Boole-függvénynek nevezzük. Támasza vagy tartója $supp(f) = \{x \in \mathbb{F}_2^k \colon f(x) = 1\}$, azaz azon input vektorok halmaza, amelyekhez tartozó függvényérték nem nulla.*

3.2. Definíció. *Az f Boole-függvény Hamming súlyán támaszának méretét értjük.*

Tekintsük a következő 3-változós Boole-függvényt:

$$f(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3. \tag{3.1}$$

Ezentúl $\oplus$ a modulo 2 összeadást jelöli, és a szorzáson a modulo 2 szorzást értjük. Ekkor az f-hez tartozó igazságtáblázat:

Input	000	001	010	011	100	101	110	111
Output	0	0	0	1	0	1	1	1

A függvény támasza a $\{011, 101, 110, 111\}$ halmaz, így f Hamming súlya 4. A függvényértékek ismeretében megadjuk annak a valószínűségét, hogy az input vektor adott indexű komponense 0 vagy 1.

$f(\mathbf{x}) = 0$	$f(\mathbf{x}) = 1$
$P(x_1 = 0 \mid f(\mathbf{x}) = 0) = 3/4$	$P(x_1 = 0 \mid f(\mathbf{x}) = 1) = 1/4$
$P(x_1 = 1 \mid f(\mathbf{x}) = 0) = 1/4$	$P(x_1 = 1 \mid f(\mathbf{x}) = 1) = 3/4$
$P(x_2 = 0 \mid f(\mathbf{x}) = 0) = 3/4$	$P(x_2 = 0 \mid f(\mathbf{x}) = 1) = 1/4$
$P(x_2 = 1 \mid f(\mathbf{x}) = 0) = 1/4$	$P(x_2 = 1 \mid f(\mathbf{x}) = 1) = 3/4$
$P(x_3 = 0 \mid f(\mathbf{x}) = 0) = 3/4$	$P(x_3 = 0 \mid f(\mathbf{x}) = 1) = 1/4$
$P(x_3 = 1 \mid f(\mathbf{x}) = 0) = 1/4$	$P(x_3 = 1 \mid f(\mathbf{x}) = 1) = 3/4$

Látjuk, hogy például amennyiben az f függvény outputja 1, úgy 0.75 annak a valószínűsége, hogy az input vektor első koordinátája 1. Ha a függvényt titkosítás létrehozására használnánk, úgy a támadók – ismerve a fenti tulajdonságot – többletinformációkhoz juthatnának a kriptorendszer működését illetően. Erre konkrét példát mutatunk a következő, korreláció-immun függvények alkalmazásáról szóló alfejezetben.

Ezek után világossá válik, hogy nehezen sebezhető kriptorendszerek megalkotásához körültekintően kell megválasztanunk a Boole-függvényeket. Egy ilyen választást adhatnak a korreláció-immun függvények, hisz ezekkel elkerülhetők az input és output értékek közötti összefüggésekből eredő problémák.

3.3. Definíció. *Az $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ Boole-függvényt t-edrendű ($1 \leq t \leq k$) korreláció-immunnak nevezzük, és **CI(t)**-vel jelöljük, ha tetszőleges rögzített $(a_1, a_2, \ldots, a_t) \in \mathbb{F}_2^t$ vektor és bármely t darab $i_1, i_2, \ldots, i_t$, $(1 \leq i_1 < \ldots < i_t \leq k)$ index esetén*

$$\mathbb{P}\left((x_{i_1}, x_{i_2}, \ldots, x_{i_t}) = (a_1, a_2, \ldots, a_t) \mid f(x) = 1\right) = \frac{1}{2^t}$$

$$\mathbb{P}\left((x_{i_1}, x_{i_2}, \ldots, x_{i_t}) = (a_1, a_2, \ldots, a_t) \mid f(x) = 0\right) = \frac{1}{2^t}.$$

3.2. Alkalmazás

Siegenthaler 1984-ben írt először a korrelációs veszélyről, ami bizonyos Boole-függények esetén az input bitsorozatok és output bitek között fennálló korrelációt használja fel a kriptorendszer megtámadására. Példát adunk olyan folyamatos rejtjelezőre, amelyben ha az alkalmazni kívánt Boole-függvényt nem választjuk legalább elsőrendű korreláció-immunnak, úgy ezzel egy kívülálló olyan információk birtokába juthat, ami elősegítheti a kriptorendszer feltörését.

A nyilvános kulcsú titkosítások egy csoportját adják a folyamatos rejtjelezők (angolul *stream cipher*), amelyek a kódolni kívánt nyílt szöveget elemi szinten, karakterekként dolgozzák fel. Ezek az eljárás során a nyílt szöveg minden bitjét úgy titkosítják, hogy ahhoz modulo 2 hozzáadnak egy másik bitet, nevezetesen a rendszer titkos kulcssorozatának egy megfelelő bitjét. Ez utóbbi pszeudo-random vagy véletlenszerű kulcssorozat, ami statisztikailag véletlennek tűnő – így egy idegennek tulajdonképpen megsejthetetlen –, de mégis előállítható egy teljesen determinisztikus, megismételhető folyamat eredményeként.

A folyamatos rejtjelezőkben gyakran használnak LFSR-eket (Linear Feedback Shift Register – Lineáris visszacsatolásos léptetőszámláló) a rendszer kissé bonyolultabbá tételéhez, törekedvén ezzel a biztonság fokozására. Az LFSR olyan léptetőszámláló, amelynek az i-edik állapotbeli inputja kizárólag az $i-1$-edik állapot output bitjeitől függ, méghozzá lineáris függvényen keresztül. A kezdeti bitsorozatot az LFSR magjának nevezzük.

Vegyük azt a folyamatos rejtjelező titkosítást, amelyben a kulcssorozat megadása a Geffe pszeudo-random generátorral történik. Ekkor a kriptorendszer három darab LFSR-ből, és egy háromváltozós F Boole-függvényből áll.

Jelöljük a regisztereket LFSR-1, LFSR-2 és LFSR-3-mal, valamint ezek i-edik állapotbeli outputjait rendre x_{1i}, x_{2i}, x_{3i}-vel. A regisztereket kombináló Boole-függvény

$$F\colon \mathbb{F}_2^3 \to \mathbb{F}_2, \quad F(x_1, x_2, x_3) = (x_1 x_2) \oplus ((1 - x_1) x_3),$$

ahol a szorzás és összeadás modulo 2 értendő. A Geffe generátor által megadott kulcssorozat i-edik tagja $F(x_{1i}, x_{2i}, x_{3i})$.

F alábbi igazságtáblázatában láthatjuk, hogy az $F(x_1, x_2, x_3)$ bitek az esetek háromnegyedében megegyeznek az x_3 bittel.

x_1	x_2	x_3	$F(x_1, x_2, x_3)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

Nézzük meg, hogy egy támadó hogyan boldogul a fenti rendszer feltörésével. A Kerckhoff-elv szerint egy jó kriptorendszer olyan, hogy biztonsága egyedül a kulcsnak, és nem magának az eljárásnak a titkosságán alapul. Éppen ezért feltesszük, hogy az algoritmus nyilvános, vagyis minden kívülálló a titkos kulcsoktól eltekintve ismeri a rendszert. Esetünkben ez azt jelenti, hogy a támadó egyedül azt nem tudja, hogy mi az egyes LFSR-ek magja. Ekkor természetesen nem ismeri azok outputjait, valamint így F függvény inputjait és outputjait sem. Feltehető, hogy birtokában van a – nyílt szöveg $p_1, p_2, \ldots$ bitjeihez tartozó – kódolt szöveg egészének, jelöljük ezeket a biteket $c_1, c_2, \ldots$-vel. A kódolás a $c_i = p_i \oplus F(x_{1i}, x_{2i}, x_{3i})$ módon történik.

Tegyük fel, hogy a támadó tudomására jut a nyílt szöveg első 32 darab bitje, $p_1, p_2, \ldots p_{32}$ (ez a feltétel szigorúnak tűnik, de a gyakorlatban mégis gyakran előfordulhat). Ezen ismeretekkel bárki könnyen kitalálhatja $F(x_{1i}, x_{2i}, x_{3i})$-t minden $i = 1, 2, \ldots, 32$-re, modulo 2 összeadván p_i-t és c_i-t . A feltörőnek az a célja, hogy a kulcssorozat egészének, azaz tetszőleges sorszámú bitjének előállítására képes legyen. Ehhez először arra törekszik, hogy megtalálja a harmadik regiszter magját. Brute force támadást indít, és az összes lehetséges kezdeti bitsorozatra legyártatja LFSR-3 első 32 darab output bitjét, majd ezeket rendre összehasonlítja az ismert $F(x_{1i}, x_{2i}, x_{3i})$ bitekkel. Tudván, hogy LFSR-3 és F outputja között a korreláció mértéke 0.75, a támadó megsejtheti, ha éppen a maggal azonos sorozatot adta meg LFSR-3 kezdeti bitsorozatának, hisz ekkor a rendszer által számolt LFSR-3 outputok és a meglévő F értékek nagyjából 24 alkalommal egyeznek meg és 8-szor különböznek. Egyértelműen látszik, hogy a teljes kipróbálás módszerével viszonylag rövid időn belül lehetővé válik a harmadik regiszter magjának megsejtése. Folytatva a leírtakat a második regiszterre, adódik, hogy a Geffe generátor feltörése 3, egymástól független LFSR feltörésére redukálódik, ami a titkosító rendszer nagymértékű sebezhető-

ségére utal. Látván ezt a gyengeséget, valóban jogos követelésnek tűnik, hogy F-et magasabb rendű korreláció-immunnak válasszuk. Az $m+1$-ed rendű korrelációs támadás olyan rendszerekre jelent fenyegetést, amelyekben a használt Boole-függvény $m+1$-nél alacsonyabb rendű korreláció-immun. A fenti példából azonban látszik, hogy nagyobb m esetén ahhoz, hogy a támadó érdemben következtetni tudjon a – kombináló függvény inputjának m változója és outputja között – fennálló m-edrendű korrelációból az egyes LFSR-ek inizializációjára, a nyílt szöveg jóval nagyobb részét ismernie kell.

Habár a korreláció-immun függvények valóban hasznosak a Siegenthaler-támadás kivédésére, az úgynevezett Siegenthaler-korlát felső határt ad ezen függvények fokszámára. A 2000-es évek elején megjelenő új támadások éppen az alacsony fokszámú függvények bizonyos szempontból vett gyengeségeit támadták meg, így a CI-függvények ezekkel szemben nem adódtak ellenállónak. Kutatásuk és jelentőségük azonban továbbra sem hanyatlik, köszönhetően annak, hogy egy új területen, méghozzá a gyakorlatban különösen hatékony oldalcsatornás támadások kivédésében játszanak központi szerepet. Utóbbiak nem a rendszer matematikai gyengeségeit, hanem az implementáció során létrejövő fizikai hatásokat (elektromágneses hullámok, energiaszükséglet, időszükséglet) megfigyelve vonnak le következtetéseket a rendszer működéséről, paramétereiről. Ahhoz, hogy egy titkosítás védve legyen az oldalcsatornás támadásokkal szemben, az implementációjában nyilvánvalóan erre irányuló ellenintézkedésekre van szükség. Ez sajnálatos módon lelassítja a kriptorendszer működését, és további memóriatár-igényt jelent. Az arany középutat az oldalcsatornás támadásokkal szembeni ellenállóság és a nem kívánatos idő- és tárigénytöbblet között a kis Hamming súlyú, azaz kis méretű támasszal rendelkező korreláció-immun függvények jelentik.

3.3. Ortogonális tömbök és korreláció-immun függvények kapcsolata

Hamarosan egyértelművé válik az olvasó számára a korreláció-immun függvényekről szóló fejezet jelenléte a munkában, hiszen megmutatjuk, hogy ezek és az ortogonális tömbök között nagyon szoros összefüggés van.

Vegyük egy t-edrendű korreláció-immun Boole-függvény támaszát, és írjuk be ennek elemeit egy mátrix soraiba. A t-korreláció-immunitás definíciójából követke-

zik, hogy ezen táblázat tetszőleges t darab oszlopát kiválasztva a kapott részmátrixban minden t hosszú bináris sorozat pontosan ugyanannyiszor, $N/2^t$-szer szerepel.

3.4. Állítás. *Ha $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ t-edrendű korreláció-immun függvény, úgy a támaszában szereplő vektorokat egy táblázat soraiba írva egyszerű $OA(N,k,2,t)$ ortogonális tömböt kapunk. Ekkor N a függvény Hamming súlyával, azaz támaszának méretével egyenlő.*

3.4. Carlet–Guilley-sejtés

Ahogyan említettük, a tárgyalt terület kutatása a mai napig aktív, nagyon bőséges a korreláció-immun függvényekről szóló irodalomtár. Az ezen témában kutató matematikusok közül kiemelnénk Claude Carlet-t és munkatársait. Az irodalomjegyzékben most csupán néhány tőlük származó munkát említünk meg, számunkra ezek lesznek relevánsak.

Mivel az oldalcsatornás támadások kivédésére olyan CI-függvények beépítése a legkedvezőbb, amelyeknek támasza a lehető legkisebb méretű, így erre az értékre nagy figyelmet fordítunk. Legyen $\omega_{k,t}$ az a legkisebb érték, amire létezik ilyen Hamming súlyú, nemnulla, k-változós, t-edrendű korreláció-immun Boole-függvény.

Claude Carlet és társszerzőinek [1, 2] munkájában szerepel az alábbi táblázat. Ez az $\omega_{k,t}$ értékeket tartalmazza kis k és t paraméterek esetén. Megjegyezzük, hogy a szerzők a Boole-függvények változóinak számára az n, a korreláció-immunitás rendjére a d paramétereket használják. Mi, már az ortogonális tömbökkel való kapcsolatukra utalván, rendre a k és t paraméterekkel dolgozunk. A táblázatban láthatunk hiányzó elemeket. Ez bizonyítja igazán, hogy az $\omega_{k,t}$ értékek meghatározása még kis k,t paraméterek esetén sem egyszerű feladat.

Kihasználva az ortogonális tömbök és korreláció-immun Boole-függvények közötti összefüggést, az utóbbiakat érintő problémákat ortogonális tömbök oldaláról is vizsgálhatjuk.

3.5. Megjegyzés. *Rögzített k,t értékek esetén $\omega_{k,t} = F^*(k,2,t)$.*

Ha lerögzítünk egy t értéket, azaz csupán a táblázat t-edik oszlopát tekintjük, úgy észrevehetjük, hogy $\omega_{k,t}$ értékek monoton növekvőek.

Claude Carlet és Sylvian Guilley nevéhez kötődik az előbbi megfigyelésből eredő sejtés.

3.6. Sejtés (Carlet-Guilley)**.** *Rögzített t érték esetén az $\omega_{k,t}$ függvény monoton nemcsökkenő sorozatot ad k függvényében.*

Table 2. Values $\min_{f:\mathbb{F}_2^n \to \mathbb{F}_2/d\text{-CI.}} card\,(supp(f))$

n \ d	1	2	3	4	5	6	7	8	9	10	11	12	13
1	**2**												
2	**2**	**4**											
3	**2**	**4**	**8**										
4	**2**	**8**	**8**	**16**									
5	**2**	**8**	**16**	**16**	**32**								
6	**2**	**8**	**16**	**32**	**32**	**64**							
7	**2**	**8**	**16**	**64**	**64**	**64**	**128**						
8	**2**	**12**	**16**	**64**	**128**	**128**	**128**	**256**					
9	**2**	**12**	**24**	**128**	**128**	**256**	**256**	**256**	**512**				
10	**2**	**12**	**24**	**128**	**256**	*512*	*512*	*512*	*512*	*1024*			
11	**2**	**12**	**24**	?	?	*512*	*1024*	*1024*	*1024*	*1024*	*2048*		
12	**2**	**16**	**24**	?	?	?	*1024*	*2048*	*2048*	*2048*	*2048*	*4096*	
13	**2**	**16**	*32*	?	?	?	?	*4096*	*4096*	*4096*	*4096*	*4096*	*8192*

Az említett $\omega_{k,t}$ és $F^*(k,2,t)$ közötti egyenlőségből fakadóan az előbbi sejtés ekvivalens az első fejezetben közölt, ortogonális tömbökre vonatkozó 1.14 Sejtéssel.

4. fejezet

Eredmények

Az olvasó mostanra láthatta az ortogonális tömbök definícióját, tulajdonságait, a kódokkal és korreláció-immun Boole-függvényekkel való kapcsolatukat, valamint a minimális sorszámukra vonatkozó Rao és LP-korlátot.

Ebben a fejezetben az 1.3. Alfejezet nyitott problémáira vonatkozó, [3]-ban szereplő részleges eredményeinket közöljük és igazoljuk.

4.1. Előzmények

A korábban már szereplő (1.3), (1.5) és (1.6) relációkat újból kiemeljük, a fejezetben sokszor fogjuk használni őket.

$$F(k,s,t) \leq F^*(k,s,t), \tag{4.1}$$

$$F(k,s,t) \leq F(k+1,s,t), \tag{4.2}$$

$$2\,F(k,2,2u) = F(k+1,2,2u+1), \tag{4.3}$$

$$2\,F^*(k,2,2u) = F^*(k+1,2,2u+1). \tag{4.4}$$

Mivel a tételeink bizonyításában komplex vektorokkal is dolgozunk, most néhány sorban összefoglaljuk a legfontosabb tudnivalókat róluk.

Továbbra is $w(u)$-val jelöjük az $u \in \{0,\ldots,s-1\}^k$ vektor Hamming súlyát, továbbá az $u,v \in \{0,\ldots,s-1\}^k$ vektorok $u \cdot v$ vagy $\langle u,v\rangle$ skaláris szorzatán az alábbi szummát értjük:

$$uv^T = \sum_{i=0}^{k} u_i v_i.$$

Tegyük fel, hogy a H mátrix elemei komplex számok. Ekkor H konjugált transzponáltját H^*-gal jelöljük.

Komplex $u, v \in \mathbb{C}^n$ vektorokra

$$uv^* = \sum_{i=0}^{k} u_i \overline{v}_i.$$

Az $u \in \mathbb{C}^n$ vektor 2-normája

$$\|u\| = \sqrt{uu^*}.$$

Komplex vektorok esetén a Cauchy-Schwarz egyenőtlenség:

$$|uv^*| \leq \|u\|\|v\|.$$

Legyen s pozitív egész és ζ s-edik egységgyök, vagyis olyan komplex szám, amelynek s-edik hatványa 1. Vegyünk egy $N \times k$ méretű A mátrixot, amelynek elemei $\{0, \ldots, s-1\}$-ből kerülnek ki. Az A mátrix i-edik sorára a_i-ként hivatkozunk ($1 \leq i \leq N$), valamint rögzített $1 \leq i \leq N$ és $v \in \{0, \ldots, s-1\}^k$ vektor esetén bevezetjük az alábbi jelölést:

$$\alpha_{i,v} = \zeta^{a_i v^T}.$$

Amennyiben $v = 0$, úgy $\alpha_{i,0} = \zeta^{a_i 0^T} = 1$, továbbá tetszőleges $v, v' \in \{0, \ldots, s-1\}^k$ vektorokra

$$\alpha_{i,v}\alpha_{i,v'} = (\zeta^{a_i v^T})(\zeta^{a_i (v')^T}) = \zeta^{a_i (v+v')^T} = \alpha_{i,v+v'},$$

valamint

$$\overline{a}_{i,v} = \overline{\zeta^{a_i v^T}} = \zeta^{-a_i v^T} = \zeta^{a_i (-v)^T} = \alpha_{i,-v}.$$

Az $\alpha_{i,v}$ komplex számok hasznosnak bizonyulnak ortogonális tömbök jellemzése során.

4.1. Lemma. *A következő állítások ekvivalensek:*

(i) Az A mátrix $OA(N, k, s, t)$ ortogonális tömb.

(ii) $\sum_{i=1}^{N} \alpha_{i,v} = 0$ minden olyan $v \in \{0, \ldots, s-1\}^k$ esetén, amelyre $w(v) \leq t$.

(iii) $\sum_{i=1}^{N} \alpha_{i,v}\bar{\alpha}_{i,v'} = 0$ minden olyan $v, v' \in \{0, \ldots, s-1\}^k$ esetén, amelyekre $w(v) + w(v') \leq t$.

Bizonyítás. Az (i) és (ii) állítások ekvivalenciája pontosan az 1.9 Tétel.

(iii) $\rightarrow$ (ii): Legyen $v' = 0$. Ekkor $\bar{\alpha}_{i,v'} = 1$ és $w(v') = 0$, amiből azonnal következik (ii).

(ii) $\rightarrow$ (iii): Adott v, v' vektorok esetén $\alpha_{i,v}\bar{\alpha}_{i,v'} = \alpha_{i,v-v'}$, továbbá $w(v-v') \leq w(v) + w(v')$, hiszen $v - v'$ adott komponensében csak akkor lehet nemnulla elem, ha ezen a helyen v vagy v' valamelyike is nemnulla. Amennyiben $w(v) + w(v') \leq t$, úgy $w(v-v') \leq t$, és ekkor (ii) alapján

$$\sum_{i=1}^{N} \alpha_{i,v}\bar{\alpha}_{i,v'} = \sum_{i=1}^{N} \alpha_{i,v-v'} = 0,$$

ami épp a harmadik állítás. □

Fő eredményünkben [3, Theorem 1.] elegendő feltételt adunk ortogonális tömbök egyszerűségére, valamint jellemezzük azon eseteket, amelyekben az ortogonális tömbök sorszáma éppen a Rao-korlát kétszeresével egyenlő. Mivel a $2u$ és $2u+1$ erősségek között fennálló ekvivalenciát már megmutattuk az 1.10 Tételben, így ezentúl csak a $t = 2u$ esettel foglalkozunk.

4.2. Főtétel

4.2. Tétel. *[3, Theorem 1.] Legyen A egy $OA(N, k, s, 2u)$ ortogonális tömb, és $M(k, s, 2u)$ a rögzített k, s és $t = 2u$ paraméterekhez tartozó Rao-korlát*

$$M(k, s, 2u) = \sum_{j=0}^{u} \binom{k}{j} (s-1)^j.$$

(i) Ha $N < 2M(k, s, 2u)$, akkor A egyszerű.

(ii) Ha $N = 2M(k, s, 2u)$, akkor A minden sorának multiplicitása legfeljebb 2.

(iii) Ha $k \geq 5$, $s = 2$ és $u = 2$, valamint $N = 2M(k, 2, 4) = k^2 + k + 2$, akkor A vagy egyszerű, vagy $k = 5$ és A az egyértelmű $OA(16, 5, 2, 4)$ ortogonális tömb kétszer egymás alá helyezésével kapható meg.

Bizonyítás. A Rao-tétel [4, Theorem 2.1.] igazolása egy speciális H mátrix bevezetésével kezdődik. A mi bizonyításunkat is ez a mátrix motiválta.

Legyen adott A $OA(N, k, s, 2u)$ ortogonális tömb. Minden $0 \leq j \leq u$ esetén definiálunk egy $N \times \binom{k}{j}(s-1)^j$ méretű H_j mátrixot. H_j oszlopait azokkal a $v \in \{0, \ldots, s-1\}^k$ vektorokkal indexeljük, amelyekre $w(v) = j$, azaz pontosan j darab

nemnulla elemet tartalmaznak. Rögzített $1 \leq i \leq N$ és v vektor esetén a H_j mátrix (i, v) pozíciójában álljon az $\alpha_{i,v} = \zeta^{a_i v^T}$ komplex szám.

Ekkor a

$$H = [H_0\, H_1\, \cdots\, H_u],$$

mátrixnak N darab sora és

$$M = \sum_{j=0}^{u} \binom{k}{j} (s-1)^j = M(k, s, 2u)$$

darab oszlopa van. Vegyük H két oszlopát, legyenek ezek a v-vel és v'-vel indexelt h_v és $h_{v'}$ vektorok ($w(v) \leq u$ és $w(v') \leq u$) . Mivel $w(v) + w(v') \leq 2u = t$, így a 4.1 Lemma (iii) pontja alapján

$$h_v h_{v'}^* = \sum_{i=1}^{N} \alpha_{i,v} \bar{\alpha}_{i,v'} = 0,$$

amiből következik, hogy H bármely két oszlopa ortogonális. Amennyiben $h = h_v$ az a vektor, amely a H mátrix v-vel indexelt oszlopát adja, úgy

$$hh^* = \sum_{i=1}^{N} \alpha_{i,v} \bar{\alpha}_{i,v} = \sum_{i=1}^{N} \alpha_{i,v} \alpha_{i,-v} = \sum_{i=1}^{N} \alpha_{i,v-v} = N.$$

Ebből $H^* H = NI$, és így teljesül, hogy $\frac{1}{\sqrt{N}} H$ oszlopai ortonormált vektorrendszert adnak $\mathbb{C}^N$-ben. Lineáris algebrából tudjuk, hogy ez a rendszer kibővíthető N elemű ortonormált bázissá. A kibővítést adó vektorokat fűzzük hozzá oszlopvektorokként $\frac{1}{\sqrt{N}} H$-hoz, és jelöljük az így keletkező mátrixot Q-val. Ez egy $N \times N$ méretű mátrix, amelyre $Q^* Q = I$. Oszlopai, és így sorai is ortonormált bázist alkotnak, erre a tulajdonságra a későbbiekben még nagy szükségünk lesz. Q tetszőleges i-edik sorára $[u\, u']$ alakban hivatkozunk, ahol u a H mátrix i-edik sorának $\frac{1}{\sqrt{N}}$-szerese, u' a bázissá bővítésből adódó $N - M$ hosszú vektor. Ekkor

$$\|u\| = \sqrt{M/N}, \quad \|u'\| = \sqrt{1 - M/N}. \tag{4.5}$$

Megmutatjuk, hogy ha A nem egyszerű, akkor $N \geq 2M$. Tegyük fel, hogy A két sora, a_i és a_j megegyezik. Ekkor H i és j-edik sora is azonos, jelöljük ezt az M hosszú vektort u-val. Q i-edik és j-edik sora rendre $[u\, u']$ és $[u\, u'']$ alakú, továbbá Q sorainak

ortonormalitásából

$$uu^* + u'(u'')^* = 0. \tag{4.6}$$

A (4.5), (4.6) és a Cauchy-Schwarz egyenlőtlenség implikálja, hogy

$$M/N = \|u\|^2 = |uu^*| = |u'(u'')^*| \leq \|u'\| \, \|u''\| = 1 - M/N. \tag{4.7}$$

Ebből $2M \leq N$, így adódik az (i) állías.

Ha $2M = N$, akkor (4.7)-ben végig egyenlőség teljesül, ami a Cauchy-Schwarz egyenlőtlenség szerint csak úgy lehetséges, ha u' és u'' lineárisan függőek, azaz $u'' = \beta u'$ valamely $\beta \in \mathbb{C}$-re. Mivel u' és u'' normája megegyezik – hisz (4.5) alapján mindkettő $\sqrt{1 - M/N}$ – , így $|\beta| = 1$. Másfelől (4.6)-ból adódik, hogy

$$-uu^* = \overline{\beta} u' u'^*,$$

amiből

$$\beta = \overline{\beta} = -\|u\|^2 / \|u'\|^2,$$

vagyis β negatív valós szám. Összességében azt kapjuk, hogy $u'' = -u'$. Tegyük fel, hogy A-ban szerepel egy $a_i = a_j$-vel megegyező harmadik sor, jelöljük az ennek megfelelő Q-beli sort $[u\, u''']$-vel. A leírtakat u'''-re alkalmazva megint csak azt kapjuk, hogy $u''' = -u'$. Ekkor Q-ban $[u\, u''] = [u\, u''']$, ami ellentmond annak, hogy sorai ortonormált bázist alkotnak. Ezzel beláttuk, hogy $2M = N$ esetén legfeljebb két ismétlődő sor lehet A-ban.

A (iii) állítás bizonyításához vegyünk egy nem egyszerű $OA(k^2 + k + 2, k, 2, 4)$, $k \geq 5$ ortogonális tömböt, legyen ez A. Azzal, hogy A minden sorához modulo 2 hozzáadjuk ugyanazt a rögzített k hosszú bináris sorozatot, és a tömb sorainak sorrendjét megcserélgetjük, érdembeli változtatást nem teszünk, s így feltehetjük, hogy A első két sora a csupa 0 vektor. Vegyük az (i) bizonyításában szereplő konstrukcióval megalkotott H_i ($i = 0, 1, 2$), H és Q mátrixokat. Ekkor H-nak $N = k^2 + k + 2$ sora és a feltétel szerint $M = N/2$ oszlopa van. Második egységgyöknek $\zeta = -1$-et választva H elemei ± 1-ek.

A következő állítás kulcsfontosságú lesz (iii) igazolásában.

4.3. Lemma. *Ha $i = 3, \dots, N$, úgy A i-edik sorában az egyesek száma ℓ_1 vagy ℓ_2, ahol*

$$\ell_{1,2} = \frac{k+1 \pm \sqrt{k-1}}{2}. \tag{4.8}$$

Lemma bizonyítása. Mivel A első két sora a csupa 0 vektor, így minden v vektorra

$$\alpha_{1,v} = \alpha_{2,v} = (-1)^{0v^T} = 1.$$

Ebből adódik, hogy Q első valamint második sora $[u\, u']$ és $[u\, u'']$ alakú, ahol

$$u = \left[\frac{1}{\sqrt{N}} \cdots \frac{1}{\sqrt{N}}\right].$$

Mivel $N = 2M(k, 2, 4)$, így a (ii) bizonyításában szereplő gondolatmenetből kapjuk, hogy $u'' = -u'$. Legyen $[v\, v']$ Q i-edik sora, ahol $i \geq 3$. Mivel $[v\, v']$ ortogonális az első két sorra, így

$$\begin{aligned} 0 &= uv^T + u'(v')^T, \\ 0 &= uv^T + u''(v')^T = uv^T - u'(v')^T. \end{aligned}$$

Kapjuk, hogy $uv^T = 0$, ami u specialitása miatt akkor és csak akkor teljesülhet, ha v-ben az $\frac{1}{\sqrt{N}}$ és $-\frac{1}{\sqrt{N}}$ elemek pontosan ugyanannyiszor, $M/2$-ször szerepelnek, s így H i-edik sorában pontosan $M/2 = N/4$ darab 1-es van.
Jelölje ℓ A i-edik sorában lévő egyeseinek számát. Most egy másik módon számoljuk meg, hogy hány egyes szerepel H i-edik sorában. H_0-nak egyetlen oszlopa van, és ebben minden elem 1, H_1 i-edik sorában az elemek $(-1)^{a_{ij}}$ alakúak – ahol a_{ij} az A (i, j) pozíciójában szereplő elem – , így itt $k - \ell$ darab egyes van. H_2 i-edik sorában az egyesek száma az a_i sorban megjelenő 11 és 00 párok száma, ami éppen

$$\binom{\ell}{2} + \binom{k-\ell}{2}.$$

Összességében a H mátrix i-edik sorában

$$1 + k - \ell + \binom{\ell}{2} + \binom{k-\ell}{2}$$

darab egyes szerepel. A két leszámolással kapott értékeknek meg kell egyeznie,

$$1 + k - \ell + \binom{\ell}{2} + \binom{k-\ell}{2} = \frac{k^2+k+2}{4},$$

ekvivalensen

$$\ell^2 - (k+1)\ell + (k^2+k+2)/4 = 0.$$

A másodfokú egyenletet megoldva azonnal következik a (4.8) formula ℓ_1 és ℓ_2-re. □

A 4.3 Lemma egyszerű következményei, hogy $\ell_1 - \ell_2 = \kappa = \sqrt{k-1}$ egész, $N = \kappa^4 + 3\kappa^2 + 4$ és $\ell_{1,2} = (\kappa^2 \pm \kappa + 2)/2$.

Térjünk vissza (iii) bizonyításához. Adjuk meg azt az A' mátrixot, amelyet A-ból azon sorok kiválasztásával kapunk, amelyek 3 darab 0-val kezdődnek. Ekkor

$$A' = \begin{bmatrix} 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & & & \\ 0 & 0 & 0 & & B & \\ 0 & 0 & 0 & & & \end{bmatrix},$$

ahol B-nek $k-3$ oszlopa és $N/8-2$ darab sora van, hiszen A 4, és így speciálisan 3 erősségű is. Szintén a 4-es erősségből következik, hogy A' bármely 3-nál nagyobb indexű oszlopában az egyesek száma $N/16$, hisz csak így teljesülhet, hogy A első 4 oszlopában a 0000 és 0001 négyesek pontosan ugyanannyiszor, $N/16$-szor szerepelnek. A 4.3 Lemma alapján az A, így speciálisan az A' nemnulla soraiban, sőt ez utóbbi megválasztása miatt B soraiban is az egyesek száma csak ℓ_1 vagy ℓ_2 lehet. Jelöljük a-val a B mátrix ℓ_1 súlyú sorait. A B-ben szereplő egyesek számára egyrészt $N/16 \cdot (k-3)$, másrészt $a\ell_1 + (N/8-2-a)\ell_2$ adódik. Átrendezve az

$$a\ell_1 + (N/8-2-a)\ell_2 = N/16 \cdot (k-3).$$

egyenletet, teljesülnie kell, hogy

$$a(\ell_1 - \ell_2) = N(k-3)/16 - (N-16)\ell_2/8.$$

Mindkét oldalt κ függvényében megadva a következő egyenlőségek adódnak.

$$\begin{aligned} 16\,a\,\kappa &= (\kappa^4+3\kappa^2+4)(\kappa^2-2)-(\kappa^4+3\kappa^2-12)(\kappa^2-\kappa+2) \\ &= \kappa^5-4\kappa^4+3\kappa^3+4\kappa^2-12\kappa+16. \end{aligned}$$

Ebből kapjuk, hogy $16 \equiv 0 \pmod{\kappa}$, s így $\kappa \in \{2,4,8,16\}$, hisz a $k \geq 5$ feltétel alapján $\kappa \geq 2$.
Ha $\kappa \in \{4,8,16\}$ lenne, akkor $-12\kappa+16 \equiv 0 \pmod{64}$, vagyis $3\kappa \equiv 4 \pmod{16}$. Ebből $\kappa \equiv 12 \pmod{16}$ adódna, ami ellentmondás.
Egyetlen megoldásként $\kappa = 2$ adódik. Ekkor $k = 5$, $N = 32$, $\ell_1 = 4$ és $\ell_2 = 2$. Ebben az esetben A-nak 30 nemnulla sora van, és ezek mindegyike 2 vagy 4 darab egyest tartalmaz. Ilyen 5 hosszú vektorból pontosan $\binom{5}{2}+\binom{5}{4} = 15$ darab különböző van. Ebből, és (ii)-ből, miszerint minden sor legfeljebb kétszer jelenhet meg az ortogonális tömbben, következik, hogy A-ban minden páros sok egyest tartalmazó sor duplán szerepel, és így az egyértelmű $OA(16,5,2,4)$ megkétszerezésével adódik. □

A tétel következményeként rögzített k,s,t értékek esetén elegendő feltételt adtunk F és F^* paraméterek egyenlőségére.

4.4. Következmény. *Ha t páros és $F(k,s,t) < 2\,M(k,s,t)$, akkor*

$$F^*(k,s,t) = F(k,s,t).$$

Bizonyítás. Legyen A olyan $OA(N,k,s,t)$, amelyre $N = F(k,s,t)$, vagyis A a rögzített k,s,t értékekre létező ortogonális tömbök közül egy minimális sorszámú. Ekkor a feltételből $N < 2M(k,s,t)$, s így a 4.2 Tételből A egyszerű. Ez azt jelenti, hogy $F^*(k,s,t) \leq F(k,s,t)$, de mivel a másik irányú egyenlőtlenség mindig triviálisan teljesül, a két paraméter között valóban egyenlőség áll fenn. □

Megjegyezzük, hogy a munkánk során leggyakrabban nem a főtételt, hanem az imént közölt következményt használtuk. Ennek oka, hogy leginkább az F, F^* értékekre koncentráltunk.

5. fejezet

A 2-es és 4-es erősség esete

Ebben a fejezetben kivesézzük az 4.2 Tétel $t = 2$ és $t = 4$ esetekre vonatkozó következményeit. Ismertetjük az Hadamard mátrixok és a 2-es erősségű ortogonális tömbök ekvivalenciáját, valamint ezen speciális esetben megerősítő választ adunk a Carlet–Guilley-sejtésre.

5.1. Hadamard mátrixok

Az Hadamard mátrixok olyan $+1$ és -1 elemeket tartalmazó négyzetes mátrixok, amelyeknek sorai páronként ortogonálisak. Nevüket Jacques Hadamard (1865-1963) francia matematikus után kapták. A 2-szintű, 2 és 3 erősségű ortogonális tömbök és az Hadamard mátrixok elmélete egybevág. Ebben az alfejezetben megadjuk utóbbiak alapvető tulajdonságait és egy számunkra különösen hasznos ekvivalenciát.

5.1. Definíció. *H_n n-edrenű Hadamard mátrix, ha $n \times n$ méretű, elemei ± 1-ek és sorai ortogonálisak, azaz*

$$H_n H_n^T = n I_n. \tag{5.1}$$

5.2. Példa.

$$H_1 = \begin{bmatrix} +1 \end{bmatrix} \qquad H_2 = \begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix} \qquad H_4 = \begin{bmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 \end{bmatrix}$$

Vajon milyen n-ek esetén létezik Hadamard mátrix? A kérdés olyannyira nehéz, hogy a mai napig sem sikerült megválaszolni. Látni fogjuk, hogy amennyiben H_n létezik, úgy n értékére $1, 2$ vagy 4 valamely többszöröse adódik. A fordított irányú állítás jóval érdekesebb, ez a diszkrét matematika egyik alapvető nyitott kérdése.

Tegyük fel, hogy H_n n-edrendű Hadamard mátrix. Ekkor $H_n^{-1} = n^{-1}H_n^T$, amiből

$$H_n^T H_n = nI_n, \tag{5.2}$$

vagyis H_n oszlopai is ortogonálisak.

Amennyiben H_n teljesíti az (5.1) és (5.2) egyenlőségeket, úgy teljesíti az a mátrix is, amit H_n-ből a sorok, oszlopok permutálásával vagy bármely sor, oszlop (-1)-gyel való szorzásával kapunk. Az összes ily módon megkapható mátrixot H_n-nel izomorfnak vagy ekvivalensnek mondjuk. Ezen észrevétel után megállapodhatunk abban, hogy H_n első sorában és első oszlopában az összes elem $+1$. Az ilyen Hadamard mátrixokat normalizáltaknak nevezzük.

5.3. Lemma. *Legyen H_n n-edrenű normalizált Hadamard mátrix, $n \geq 2$. Legyen $u = (u_1, \ldots, u_n)$ és $v = (v_1, \ldots, v_n)$ két, az első sortól különböző diszjunkt sor H_n-ben. Ekkor*

(i) a koordináták felére $u_i = +1$, másik felére $u_i = -1$.

(ii) a következő esetek mindegyike a koordináták negyedében, $n/4$ darab i-re teljesül:

$$u_i = v_i = +1, \quad u_i = +1, v_i = -1, \quad u_i = -1, v_i = +1, \quad u_i = v_i = -1.$$

(iii) az előző eredmények igazak H_n oszlopaira is.

Bizonyítás. A H_n Hadamard mátrix első sorát 1_n-nel jelölve az $1_n u^T = 0$ egyenlőségből azonnal következik az (i) állítás. Legyen u és v két diszjunkt, 1_n-től különböző sor H_n-ben. Ekkor mivel $uv^T = 0$ és u, v elemei ± 1-ek – úgy, hogy (i) szerint az elemek fele $(+1)$, a másik fele (-1) –, u és v szükségszerűen $n/2$ helyen megegyezik és ugyanennyi helyen eltér egymástól. Ez a feltételek alapján csak úgy történhet, ahogyan azt a (ii) állítás mondja. A (iii) helyessége azonnal következik (5.2)-ből. □

Ezen lemma után rögtön adódik az alábbi.

5.4. Következmény. *Ha létezik H_n n-edrendű Hadamard mátrix, úgy n 1, 2 vagy 4 valamely többszöröse.*

5.2. Hadamard-sejtés, Carlet–Chen-sejtés

A 5.4 Következmény fordított irányának megválaszolása nem ilyen egyszerű. Sőt, olyannyira nehéz, hogy hosszú idők óta nem született megoldás a problémá-

ra.

5.5. Sejtés (Hadamard)**.** *Amennyiben n 1, 2 vagy 4 többszöröse, úgy létezik n-edrendű H_n Hadamard mátrix.*

Amennyiben $n = 2^m$ valamely m-re, úgy megadható H_n Hadamard mátrix. Ennek megmutatásához először definiáljuk bináris mátrixok tenzorszorzatát.

5.6. Definíció. *Legyen $A = (a_{ij})$ és $B = (b_{ij})$ rendre $m \times n$ és $u \times v$ méretű bináris mátrixok. A és B tenzor- vagy Kronecker szorzatán azt az $mu \times nv$ méretű $A \otimes B$ mátrixot értjük, amelyre*

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

úgy, hogy $a_{ij} * B$ azt az $u \times v$ méretű mátrixot jelöli, amelyet úgy kapunk, hogy B minden elemét megszorozzuk a_{ij}-vel.

Legyen $H_1 = \begin{bmatrix} 1 \end{bmatrix}$ és $H_2 = \begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix}$ első- és másodrendű Hadamard mátrixok. Ekkor H_2 önmagával vett m-tényezős tenzorszorzata 2^m-edrendű H_{2^m} Hadamard mátrix.

Az Hadamard mátrixok ismerete hasznosnak bizonyul a 2-es erősségű ortogonális tömbök vizsgálatában, ezt jól mutatja a következő tétel.

5.7. Tétel. *$OA(4\lambda, 4\lambda - 1, 2, 2)$ és $OA(8\lambda, 4\lambda, 2, 3)$ ortogonális tömbök pontosan akkor léteznek, ha létezik 4λ rendű Hadamard mátrix.*

Bizonyítás. Mivel $OA(4\lambda, 4\lambda - 1, 2, 2)$ és $OA(8\lambda, 4\lambda, 2, 3)$ létezése egymással ekvivalens az 1.10 Tétel szerint, így elegendő az állítást csak az egyik esetben belátnunk. Tegyük fel, hogy $H_{4\lambda}$ normalizált Hadamard mátrix. Elhagyva ennek első oszlopát, a 5.3 Lemma alapján rögtön adódik, hogy a visszamaradó mátrix összes oszlopában az elemek fele $+1$, a másik fele -1, valamint bármely 2 oszlopban az összes bináris páros pontosan ugyanannyiszor, λ-szor szerepel. Ez pontosan a másodrendű, $S = \{-1, +1\}$ feletti ortogonális tömb definíciója.

Fordítva, legyen $A = OA(4\lambda, 4\lambda - 1, 2, 2)$, amiben az elemek ± 1-ek. Ekkor az ortogonális tömbök definíciójából adódik, hogy A bármely két oszlopa ortogonális. Egy csupa egyest tartalmazó oszlopot A elé fűzve 4λ rendű Hadamard mátrixot kapunk. □

Az 5.7 Tételből és abból, hogy tetszőleges nemnegatív egész m esetén létezik H_{2^m} Hadamard mátrix, következik, hogy

$$F(2^m - 1, 2, 2) \leq 2^m. \tag{5.3}$$

5.3. Elméleti eredmények

5.8. Állítás. *Minden $k \geq 2$ esetén $F^*(k, 2, 2) = F(k, 2, 2)$. Speciálisan, $F^*(k, 2, 2)$ monoton nemcsökkenő sorozat k függvényében.*

Bizonyítás. Ahogyan azt az előző alfejezetben láttuk, tetszőleges h pozitív egész esetén

$$F(2^h - 1, 2, 2) \leq 2^h.$$

Ugyanakkor a Rao-korlát $M(2^h - 1, 2, 2) = 1 + (2^h - 1) = 2^h$, vagyis

$$F(2^h - 1, 2, 2) = 2^h. \tag{5.4}$$

Legyen adott k és hozzá h az a pozitív egész, amelyre $2^{h-1} \leq k \leq 2^h - 1$ teljesül. Az $F(k, s, t)$ paraméter (1.4)-beli monotonitása és (5.4) miatt

$$F(k, 2, 2) \leq F(2^h - 1, 2, 2) = 2^h \leq 2k.$$

Mivel $M(k, 2, 2) = k + 1$, így azt kapjuk, hogy

$$F(k, 2, 2) < 2M(k, 2, 2),$$

és ekkor a 4.4 Következményből adódik, hogy $F^*(k, 2, 2) = F(k, 2, 2)$. Tudjuk, hogy $F(k, 2, 2)$ monoton növekvő, így speciálisan $F^*(k, 2, 2)$ is az, ami épp a Carlet–Guilley sejtés $t = 2$ esete. □

Használva az előző állítást, (4.3)-at és (4.4)-et, azt kapjuk, hogy $k \geq 2$-re

$$F^*(k + 1, 2, 3) = 2F^*(k, 2, 2) = 2F(k, 2, 2) = F(k + 1, 2, 3),$$

amiből következik, hogy $F^*(k, 2, 3)$ is monoton nemcsökkenő sorozat k függvényében, és így $t = 3$-ra is igaz a Carlet–Guilley-sejtés.

Claude Carlet és Xi Chen [1] munkájában szerepel egy másik sejtés a $t = 3$ esetre vonatkozóan.

5.9. Sejtés (Carlet-Chen)**.**

$$F^*(k, 2, 3) = 8 \left\lceil \frac{k}{4} \right\rceil . \tag{5.5}$$

Habár Wang igazolta [9, Theorem 3.7.], hogy az Hadamard és Carlet–Chen-sejtés egymással ekvivalensek, most mi is adunk egy teljes bizonyítást az ortogonális tömbök nyelvén.

5.10. Állítás. *A Hadamard és Carlet–Chen-sejtés egymással ekvivalenek.*

Bizonyítás. Az 5.7 Tételből következik, hogy az Hadamard-sejtés ekvivalens azzal, hogy minden $\lambda \geq 1$ esetén létezik $OA(4\lambda, 4\lambda - 1, 2, 2)$. Ugyanakkor a Rao-korlátból $F(4\lambda - 1, 2, 2) \geq M(4\lambda - 1, 2, 2) = 4\lambda$, így a sejtés azzal ekvivalens, hogy

$$F(4\lambda - 1, 2, 2) = 4\lambda \quad \text{minden } \lambda \text{ pozitív egészre.} \tag{5.6}$$

Vegyük észre, hogy (4.4) alapján (5.5) éppen azt mondja, hogy

$$F^*(k - 1, 2, 2) = 4 \left\lceil \frac{k}{4} \right\rceil ,$$

ami az 5.8 Állítás eredményeképp az

$$F(k - 1, 2, 2) = 4 \left\lceil \frac{k}{4} \right\rceil \tag{5.7}$$

egyenlőséggel ekvivalens.

Ezentúl az a dolgunk, hogy igazoljuk (5.6) és (5.7) ekvivalenciáját.

Amennyiben $k = 4\lambda$, úgy az ekvivalencia nyilvánvaló. Tegyük fel, hogy (5.6) igaz, és nézzük meg, mi történik, ha $k = 4\lambda + \varepsilon$ alakú, ahol $1 \leq \varepsilon \leq 3$. A Rao-korlát alapján azt kapjuk, hogy

$$4\lambda < k \leq F(k - 1, 2, 2).$$

Mivelhogy $F(k - 1, 2, 2)$ 4-gyel osztható és k-ban monoton nemcsökkenő, így

$$4\lambda + 4 \leq F(k - 1, 2, 2) \leq F(4\lambda + 3, 2, 2) = 4 \left\lceil \frac{4\lambda + 4}{4} \right\rceil , \tag{5.8}$$

vagyis

$$F(k-1,2,2) = 4\lambda + 4 = 4\left\lceil \frac{k}{4} \right\rceil,$$

ami épp a bizonyítani kívánt Carlet–Chen-sejtés. □

5.4. Főtétel alkalmazásai

A főtétel nem csak elméleti eredmények belátására szolgál. Alkalmazva az 4.2 Tétel (i) és (iii) pontját, meg tudtuk határozni a Carlet–Guilley-táblázat $t = 4$ és $t = 5$ oszlopaiból hiányzó értékeket.

5.11. Állítás.

$$F^*(k,2,4) = 128 \qquad 11 \le k \le 15,$$
$$F^*(k,2,5) = 256 \qquad 11 \le k \le 16,$$

Bizonyítás. Csak az első egyenlőséget bizonyítjuk, hisz ebből (4.4) alapján rögtön következik a második egyenlőség is. Ismert, hogy létezik $OA(256,16,2,5)$ ortogonális tömb: találhatunk egy ilyet a Sloane honlapján [8] szereplő OA könyvtárban, de használva a tömbök és kódok közötti kapcsolatot, a Kerdock kód is definiál egy $OA(256,16,2,5)$-öt [5]. Ebből oszlopokat elhagyva (1.5) miatt adódik, hogy $F(k+1,2,5) \le 256$ minden $11 \le k \le 15$ esetén. Ugyanakkor (4.3) és $2M(k,2,4) = k^2+k+2$ miatt az is igaz, hogy

$$F(k,2,4) \le 128 \le 2M(k,2,4), \qquad 11 \le k \le 15.$$

Ekkor az 4.4 Következményből $F^*(k,2,4) = F(k,2,4) \le 128$, $11 \le k \le 15$ adódik. Figyeljük meg, hogy a Carlet–Guilley-táblázat $(10,4)$ pozíciójában az $F^*(10,2,4) = 128$ érték áll. Tegyük fel, hogy $F(10,2,4) < 128$, jelöljön A egy olyan $OA(N,10,2,4)$ ortogonális tömböt, amire $N < 128$. Mivel N szükségképpen 16 többszöröse, így $N \le 112 = 2M(10,2,4)$. Alkalmazva a 4.2 Tétel (i) és (iii) állítását, azt kapjuk, hogy A egyszerű. Ezzel $F^*(10,2,4) \le 112$ adódik, ami ellentmond a táblázatban szereplő értékkel. Összefoglalva,

$$F^*(k,2,4) = F(k,2,4) \qquad \text{minden } 10 \le k \le 15 \text{ esetén.}$$

Felhasználva, hogy F monoton és $F(10,2,4) = 128$, adódik, hogy

$$F(k,2,4) \geq 128 \qquad 11 \leq k \leq 15,$$

és így $11 \leq k \leq 15$ esetén

$$F^*(k,2,4) = F(k,2,4) = 128. \qquad \square$$

Megjegyezzük, hogy a táblázat $(13,6)$ pozíciójában lévő ismeretlen érték

$$F^*(13,2,6) = 1024.$$

Ennek oka, hogy a

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

generátormátrix egy olyan $(13, 2^3, 7)_2$ lineáris kódot határoz meg, aminek duálisa egy $(13, 2^{10}, 7)_2$ lineáris kód. Ekkor a 2.9 Tétel alapján következik, hogy létezik egyszerű $OA(1024, 13, 2, 6)$ ortogonális tömb, azaz $F^*(13,2,6) \leq 1024$. Ugyanakkor az LP-korlát $N_{LP}(13,7) = 1024$, így

$$1024 \leq F(13,2,6) \leq F^*(13,2,6) \leq 1024,$$

amiből adódik, hogy $F^*(13,2,6) = 1024$.

A táblázat maradék két hiányzó elemére is megadtuk az F^* értékeket, azonban ezen eredmény javarészt számítógéppel végzett vizsgálatoknak köszönhető. Az ortogonális tömbökre vonatkozó kérdések gyakran egészértékű lineáris programozási feladattal ekvivalensek, lásd [6]. A fent részletezett eredmények megadási módszerében az a szép, hogy ezek a tiszta matematikát használják. Habár a munka megírásának időpontjáig a Carlet–Guilley-sejtés teljes helyessége nem került megválaszolásra, a leírt eredmények mindenképp hasznosnak bizonyultak a részleges válaszadásban.

Irodalom

[1] Claude Carlet és Xi Chen. „Constructing low-weight dth-order correlation-immune Boolean functions through the Fourier-Hadamard transform”. *IEEE Trans. Inform. Theory* 64.4, part 2 (2018), 2969–2978. old. ISSN: 0018-9448. DOI: 10.1109/TIT.2017.2785775. URL: https://doi.org/10.1109/TIT.2017.2785775.

[2] Claude Carlet és Sylvain Guilley. „Correlation-immune Boolean functions for easing counter measures to side-channel attacks”. *Algebraic curves and finite fields*. 16. köt. Radon Ser. Comput. Appl. Math. De Gruyter, Berlin, 2014, 41–70. old.

[3] Claude Carlet, Rebeka Kiss és Gábor P. Nagy. *Simplicity conditions for binary orthogonal arrays*. 2022. DOI: 10.48550/ARXIV.2204.00835. URL: https://arxiv.org/abs/2204.00835.

[4] A. S. Hedayat, N. J. A. Sloane és John Stufken. *Orthogonal arrays*. Springer Series in Statistics. Theory and applications, With a foreword by C. R. Rao. Springer-Verlag, New York, 1999, xxiv+416. old. ISBN: 0-387-98766-5. DOI: 10.1007/978-1-4612-1478-6. URL: https://doi.org/10.1007/978-1-4612-1478-6.

[5] A.M. Kerdock. „A class of low-rate nonlinear binary codes”. *Information and Control* 20.2 (1972), 182–187. old. ISSN: 0019-9958. DOI: https://doi.org/10.1016/S0019-9958(72)90376-2. URL: https://www.sciencedirect.com/science/article/pii/S0019995872903762.

[6] R. Kiss és G. P. Nagy. „On the nonexistence of certain orthogonal arrays of strength four”. *Prikl. Diskretn. Mat.* 52 (2021), 65–68. old. ISSN: 2071-0410. DOI: 10.17223/20710410/51/3. URL: https://doi.org/10.17223/20710410/51/3.

[7] Thor Martinsen. *Correlation immunity, avalanche features, and other cryptographic properties of generalized Boolean functions*. 2017-09. URL: http://hdl.handle.net/10945/56155.

[8] Sloane, N. J. A. *A Library of Orthogonal Arrays*. http://neilsloane.com/oadir/, Last accessed on 2022-01-13. 2007.

[9] Qichun Wang. „Hadamard matrices, d-linearly independent sets and correlation-immune Boolean functions with minimum Hamming weights”. *Des. Codes Cryptogr.* 87.10 (2019), 2321–2333. old. ISSN: 0925-1022. DOI: 10.1007/s10623-019-00620-1. URL: https://doi.org/10.1007/s10623-019-00620-1.

Nyilatkozat

Alulírott Kiss Rebeka kijelentem, hogy a diplomamunkában foglaltak saját munkám eredményei, és csak a hivatkozott forrásokat (szakirodalom, eszközök, stb.) használtam fel. A diplomamunka a 2018-1.2.1-NKP-2018-00004 számú "IoT rendszerek biztonságát növelõ technológiák (SETIT)" projekt keretében, a Nemzeti Kutatási és Innovációs Alapból biztosított támogatással, a "Nemzeti Kiválósági Program: 2018-1.2.1-NKP" pályázati program finanszírozásában valósult meg. Tudomásul veszem, hogy diplomamunkámat a Szegedi Tudományegyetem könyvtárában a kölcsönözhető könyvek között helyezik el, és az interneten is nyilvánosságra hozhatják.

Szeged, 2022. május 13.

.....

aláírás