Komplex Hadamard mátrixok konstrukciója és paraméterezése

Szöllősi Ferenc

Komplex Hadamard mátrixok konstrukciója és paraméterezése

Diplomamunka

Témavezető: Matolcsi Máté
Adjunktus, PhD

2008

Tartalomjegyzék

Elöszó **III**

Köszönetnyilvánítás **V**

English summary **VII**

1. Valós Hadamard mátrixok **1**

1.1. Bevezetés . . . 1

1.2. Alapfogalmak . . . 2

1.2.1. Ekvivalencia osztályok . . . 3

1.3. Klasszikus konstrukciók . . . 4

1.3.1. Sylvester Hadamard mátrixok . . . 5

1.3.2. Paley Hadamard mátrixok . . . 6

1.3.3. Blokkrendszerek és Hadamard-mátrixok . . . 7

1.3.4. Williamson Hadamard mátrixok . . . 12

1.4. Véges csoportokból származtatott konstrukciók . . . 13

1.4.1. Menon Hadamard mátrixok . . . 14

1.4.2. Ito Hadamard mátrixok . . . 15

1.4.3. A dupla ciklikus magú mátrixok . . . 16

1.4.4. T-mátrixok és a Goethals–Seidel tömb . . . 17

1.5. Összefoglalás . . . 17

2. Komplex Hadamard mátrixok **19**

2.1. Bevezetés . . . 19

2.2. Áttekintés . . . 21

2.3. Komplex Hadamard mátrixok konsrtukciója . . . 24

2.3.1. Butson Hadamard mátrixok . . . 24

2.3.2. A Dita-konstrukció . . . 26

2.3.3. Ciklikus komplex Hadamard mátrixok . . . 27

2.4. Komplex Hadamard- és konferencia mátrixok . . . 30

2.4.1. A diszkrét modell . . . 30

2.4.2. A folytonos mátrixcsaládok 33
2.4.3. Konstrukció általában – A konferencia mátrixok 35
2.4.4. Paraméterezés általában – Egy struktúratétel 36
2.4.5. A TZ-katalógus kiegészítése 39
2.5. Valós Hadamard mátrixok paraméterezése 42
2.5.1. Egy másik alkalmazás a Matolcsi–Réffy kritériumra 43
2.5.2. Paraméterezés általában 44
2.5.3. A TZ-katalógus kiegészítése 47
2.6. Egy nem várt alkalmazás 47

3. Új konstrukciók komplex Hadamard mátrixokra 51
3.1. Bevezetés 51
3.2. Komplex Hadamard mátrixok és blokkrendszerek 52
3.3. Egy szemtelen általánosítás 57
3.4. Újra konferencia mátrixok 65
3.5. Ad hoc konstrukciók 68
3.5.1. n=9 68
3.5.2. n=10 70
3.5.3. n=14 71

Előszó

A diplomamunkánkban egy nagyon izgalmas kombinatorikai struktúrával, az ún. Hadamard mátrixok vizsgálatával foglalkozunk. Hadamard 1893-as dolgozatában a később róla elnevezett mátrixok alatt eredetileg ± 1 elemű, páronként ortogonális sorokkal rendelkező mátrixot értett [38]. Mára már azonban ezen a klasszikus definíción túlmutatóan komplex elemű- [82], kvaterniókból álló- [14], vagy akár tetszőleges abc feletti olyan ortogonális mátrixokat kell érteni, amelyek elemeinek „nagyságára" bizonyos korlátozó feltételt szabunk. A komplex Hadamard mátrixok olyan ortogonális mátrixok, amelyek minden eleme egységnyi abszolút értékű. Néhány évtizede különösen nagy érdeklődés övezi őket, mert kiderült, hogy számos Fourier analízisbeli [84] valamint kvantum-információ elméleti problémában előkerülnek [87]. Munkánkat a W. Tadej és K. Życzkowski által 2006-ban megjelentetett *katalógus* motiválta, amelyben a szerzők minden általuk ismert kis dimenziós komplex Hadamard mátrixot felsoroltak [82]. A témakör két centrális kérdése közül az egyik az egzisztenciát firtató, még száz év elteltével is lényegében megoldatlan Hadamard-sejtés, a másik pedig az egy adott dimenzióban lévő mátrixok osztályozása. Ez utóbbi probléma a valós esetben 32, míg a komplexben 6 dimenziótól kezdve nyitott [4]. A katalógus megjelenése óta szoros nemzetközi együttműködés keretében vizsgáljuk a komplex Hadamard mátrixokat.

Dolgozatunk első fejeztében valós Hadamard mátrixokkal foglalkozunk. Ez a rész a dolgozatba csak a teljesség kedvéért került bele, nem tartalmaz saját eredményeket. A jól ismert klasszikus konstrukciók bemutatása mellett néhány mélyebb, főként csoportelméleti eredményt is röviden ismertetünk. A fejezet végén beszámolunk az Hadamard-sejtés jelenlegi állásáról valamint aszimptotikus eredményeket is tárgyalunk. Az ide kapcsolódó legfontosabb irodalom K. J. Horadam 2006-ban megjelent monográfiája [42], pontosabban annak a valós Hadamard mátrixokkal foglalkozó fejezetei.

A valós Hadamard mátrixok általánosításai közül mi kizárólag azt a típust vizsgáljuk, amelyben a mátrix elemei már tetszőleges, ám egységnyi abszolút értékű *komplex* számok lehetnek. A diszkrét Fourier transzformáció mátrixa – legalábbis konstans szorzó erejéig – egy közismert példa komplex Hadamard mátrixra. A dolgozat második fejezete ezek releváns tulajdonságait, valamint néhány általános konstrukciójukat tárgyalja. Beszélünk többek között Butson-, Diţă-szerű- illetve ciklikus komplex Hada-

mard mátrixokról is. Ezt követően rátérünk a 2006-os TDK dolgozatunk áttekintésére [80], amely Matolcsi Máté és Réffy Júlia egy eredményének illusztrálása mellett [56] a szerző további ezirányú, ám *teljesen önálló* eredményeit tartalmazó [81] folyóiratcikket foglalja össze. A szekció röviden egy eljárást körvonalaz, amely azt mutatja be, miként lehet egy diszkrét objektumból, egyetlen kiindulási Hadamard mátrixból bizonyos regularitási feltételek teljesülése esetén végtelen sok lényegesen különbözőt konstruálni. A fejezetben többek között új, az irodalomban nem szereplő paraméteres komplex Hadamard mátrixcsaládokat prezentálunk, és szerepel W. Tadej és K. Życzkowski egy nyitott problémájának a megválaszolása is. Az ide kapcsolódó legfontosabb irodalom az imént említett két szerző katalógusa [82], illetve annak naprakész, a legfrisebb eredményeket is tartalmazó on-line változata [83].

A harmadik fejezet *kizárólag új eredményeket* tartalmaz, amelyeket a későbbiek folyamán teljes egészében publikálni kívánunk. Három konstrukciót mutatunk arra, hogy valós Hadamard-rendszerek és konferencia mátrixok segítségével miként lehet komplex Hadamard mátrixokat származtatni. Nagyjából 20 évvel ezelőtt egy fontos nyitott kérdés volt, hogy prímdimenzióban létezik-e a Fourier-mátrixtól különböző komplex Hadamard mátrix, melyet teljes általánosságban elsőként Björck [8], majd nem sokkal később – ám tőle függetlenül – Munemasa és Watatani [58] illetve de la Harpe és Jones [23] válaszoltak meg. Az itt bizonyított tételeink ezeket az eredményeket *speciális esetként* tartalmazzák. Konstrukcióinkból *elméleti* magyarázatot adunk több, korábban számítógéppel talált mátrix létezésére, emellett egy új 9-, valamint legalább 10 új, páronként inekvivalnes 15 dimenziós komplex Hadamard mátrixot prezentálunk. Magát a diplomamunkát néhány további új, ad hoc jelleggel konstruált $9, 10$ illetve 14 dimenziós paraméteres mátrixcsalád bemutatásával, valamint egy sejtéssel zárjuk.

A diplomamunkánkat melegen ajánljuk mindazok számára, akik egy rövid bevezetőt szeretnének az ortogonális mátrixok elbűvölő világába. A dolgozat végén lévő igen bőséges irodalomjegyzékben szereplő cikkek böngészése minden bizonnyal kellemes időtöltést ígér a témakörben elmélyülni szándékozóknak. Sok sikert kívánunk nekik a Hadamard mátrixok konstrukciójához!

Köszönetnyilvánítás

Mindenek előtt szeretnék köszönetet mondani a témavezetőmnek, *Matolcsi Mátének*, amiért 2004-ben egy ELTE szemináriumon megemlítette az Hadamard-sejtést. Az ott elmondottak hatására kezdtem el a diszkrét matematika, pontosabban különféle kombinatorikus struktúrák és az Hadamard-mátrixok iránt érdeklődni. Azt gondolom, hogy Máté oktatói- és kutatói stílusa, a matematikához és általában az élethez való viszonyulása rendkívül nagy hatással volt rám. A vele való több éves konstruktív együttműködés, szüntelen és töretlen támogatása, bíztatása és persze kritikája nagyban elősegítette azt, hogy ez a diplomamunka határidőre elkészüljön, és ilyen releváns eredményeket tartalmazzon.

Hálás köszönet illeti *Recski András Tanár Urat*, amiért elsőévesen – számomra hatalmas meglepetést keltve – óraadónak hívot a SZIT Tanszékre, és ezáltal már nagyon korán bekapcsolódhattam az egyetemi oktatói légkörbe. Úgy gondolom, hogy ennek a páratlan lehetőségnek óriási szerepe volt abban, hogy ma a jövőmet nem programozóként, hanem kutatóként-, illetve egyetemi oktatóként képzelem el.

Köszönöm *Petz Dénesnek*, amiért elmesélte egy problémáját, amit aztán közösen sikerrel megoldottunk, és amely számos későbbi cikkének alapjául szolgált. Az első olyan tudományos dolgozat, amelyben én is részt vettem az ő irányírásával és szakértelmével jött létre [66].

Köszönöm továbbá *Illésnek*, hogy az egyetem első napjától kezdve bármiben fordulhattam hozzá, *Orsinak*, hogy javította az analízis házifeladataimat, *Briginek*, hogy levizsgáztatott geometriából és nem utolsó sorban *Julinak*, mert talán egyedül ő volt az, aki nem csak oktatni, hanem egy kicsit nevelni is próbált.

Szöllősi Ferenc
szoferi@math.bme.hu
Budapest, 2008. május 16.

English summary

In this monument work the author briefly introduces the reader to the theory of complex Hadamard matrices. Complex Hadamard matrices are special kind of orthogonal matrices, in particular all their entries have absolute value 1. During the past few decades they have received considerable attention due to their natural appearence in quantum information theory. Our work was motivated by the celebrated Cathaloge of Complex Hadamard Matrices, published by W. Tadej and K. Życzkowski very recently [82]. They have collected and exhibited all known complex Hadamards of small orders, and since then a fruitful international collaboration has begun in order to try understanding and fully classifying them.

The first chapter dealing with real Hadamard matrices is included only for completeness, in particular, it does not contain any new results. Besides listing some well-known properties, and introducing ancient constructions, we describe more advanced, mostly computer-aided methods, which could be useful when one is looking for real Hadamard matrices of higher orders.

In chapter 2 we turn our attention to complex Hadamard matrices. In the first few sections several basic properties and the most important general constructions are described. The rest of this chapter mostly deal with the author's recent article on complex Hadamard matrices [81], [80]. We illustrate step-by-step the rediscovery of the otherwise well-known "conference matrix construction" [19], [57], and by the aid of the obtained matrices we introduce a paramteric family of complex Hadamard matrices. Several connections between real Hadamard, complex Hadamard and real conference matrices are investigated. At the end of the chapter by proving that every real Hadamard matrix of order $n \geq 12$ admit an affine orbit, we settle a recent question of Tadej and Życzkowski [82].

In chapter 3 we reconsider the well-known $2-(4m-1, 2m-1, m-1)$ Hadamard-designs and conference matrices, and by the aid of them we rediscover Björck's "index-2" cyclic n-roots matrices of prime orders [8], which are precisely the same as the ones constructed independently but slightly later by Munemasa and Watatani for primes $n \equiv 3 \mod 4$ [58] and de la Harpe and Jones for $n \equiv 1 \mod 4$ [23] some 15 years ago. However, it turned out, that this construction in fact can be applied al-

so for non-prime orders. In particular, besides the rediscovery of the cyclic matrices $C_{7A}, C_{7B}, C_{11A}, C_{11B}, C_{13A}, C_{13B}$ of prime orders, we exhibit a new, previously unknown complex Hadamard matrix of order 9, which is from now on being called W_9, and at least five inequivalent complex Hadamard matrices of order 15. The entries of these matrices mostly belong to the field $\mathbb{Q}[\mathbf{i}\sqrt{n-1}]$. The principal theorem of this chapter, however, states that considering a *symmetric*, real Hadamard matrix of order $n \geq 8$, one can construct *another* family of complex Hadamard matrices of order $n-1$, all their entries belonging to the field $\mathbb{Q}[\mathbf{i}\sqrt{n-5}]$, instead of $\mathbb{Q}[\mathbf{i}\sqrt{n-1}]$. This is an essentially new construction, which subsequently leads to the rediscovery of Petrescu's P_7 matrix [64], Nicoara's $N_{11}^{(0)}$ matrix [82] – both of them found by means of computer earlier – and another five new, previously unknown complex Hadamard matrices of order 15. A formal paper from the results described in chapter 3 is in preparation.

We conclude our thesis by exhibiting several ad hoc constructions in dimensions $9, 10$ and 14. In particular we obtain a very exotic complex Hadamard matrix of order 9 possessing a circulant core. It is unknown, wether this matrix is an isolated one, or admits an affine orbit. Another construction leads to parametric families of complex Hadamard matrices of order 9. This orbit contains a matrix, whose entries are in the same field $\mathbb{Q}[\mathbf{i}\sqrt{15}]$, as N_{9A}'s and W_9's, however it is inequivalent to them. This observation implies, that we have at least three inequivalent matrices of order 9, all of their entries belonging to the field $\mathbb{Q}[\mathbf{i}\sqrt{15}]$. The last two matrices considered in this work are built of 6th roots of unity. We believe that they have already been known by design-theorists, however, based on the ideas described in chapter 2 we construct affine orbits to them, which leads to a new 5-parameter matrix of order 10, and a new 7-parameter matrix of order 14. At the end of the Thesis we propose a natural conjecture involving these matrices.

1. fejezet

Valós Hadamard mátrixok

1.1. Bevezetés

Történelmileg az első, Hadamard mátrixokkal kapcsolatos cikk még Sylvester nevéhez kötődik, aki 1867-ben egy rekurzív konstrukciót mutatott ± 1 elemű, 2^n dimenziós ortogonális mátrixokra [77]. Maga az elnevezés csak jóval később, egy tisztán lineáris algebrai probléma megválaszolását követően valósult meg: 1893-as dolgozatában Hadamard igazolta, hogy ha egy A $n \times n$-es mátrixban az elemek abszolút értéke korlátos, mégpedig egy M korláttal, akkor A determinánsa legfeljebb $M^n n^{\frac{n}{2}}$ lehet, és egyenlőség kizárólag Hadamard mátrixok esetén lehetséges [38]. Ezt követően 1933-ban Paley igazolta elsőként, hogy egy Hadamard mátrix csak $1, 2$, vagy 4-gyel osztható dimenzióban létezhet. Az általános vélekedés szerint itt a fordított állítás is igaz, nevezetesen: minden pozitív egész k esetén van $4k$ rendű valós Hadamard mátrix [63]. Magát a problémát Hadamard-sejtésnek nevezik, amely a mai napig teljes általánosságban még mindig megválaszolatlan.

Az Hadamard mátrixok a mindennapok során is többfelé előkerülnek: a Walsh–Hadamard transzformáció az egyik leggyakrabban használt diszkrét transzformáció. Hadamard mátrixokon alapul az ún. Reed-Muller hibajavító kód is, amelyet többek között az 1972-es Mariner Mars misszió alkalmával kommunikációs célokra használtak. Manapság modern, CDMA-t használó mobiltelefonokban modulációs célokra használják őket, ezáltal minimalizálva a rádiótorony irányába menő vonalak interferenciáját. Emellett még mintaillesztésre, optikai kommunikációra, titkosításra valamint különféle biológiai célokra használják [42].

Ebben a fejezetben elsőként röviden ismertetjük a valós Hadamard mátrixok legfontosabb tulajdonságait, majd bemutatjuk a négy jól ismert típusukat: a Sylvester-, Paley-, Williamson mátrixokat, valamint a blokkrendszerekkel való kapcsolatukat elemezzük. Ezt a Menon-rendszer bemutatása, majd 3 modern szemléletű, részben szá-

mítógépes apparátust igénylő konstrukció követi. Ezek közül kiemelnénk a „dupla ciklikus magú mátrix" konstrukciót, amely igen szellemes, bár egyáltalán nem közismert. A fejezet javarészt Horadam könyvének [42] első, bevezető részét dolgozza fel, és nem tartalmaz új, önálló eredményeket. Kutatásunk centrális objektuma ugyanis a következő fejezetekben tárgyalt komplex Hadamard mátrix lesz, így az elkövetkező szakaszok pusztán a problémakör érzékeltetése, valamint a jobb érthetőség kedvéért kerültek bele a dolgozatba.

1.2. Alapfogalmak

A következő definíció egy kényelmes, az előzővel természetesen ekvivalens karakterizációt ad.

1.2.1. Definíció. Egy H ± 1 elemű mátrixot Hadamard mátrixnak nevezünk, ha $HH^T = nI$ teljesül.

Az Hadamard-mátrixokra a továbbiakban tehát úgy gondolunk, mint ortogonális mátrixokra. A bevezetőben már említettük, hogy ők egy extremális lineáris algebrai probléma megoldásai. Érvényes ugyanis a következő

1.2.2. Lemma (Hadamard, [38]). *Egy $n \times n$-es, legfeljebb 1 abszolút értékű elemekből álló valós mátrix determinánsa legfeljebb $n^{\frac{n}{2}}$ lehet, és ezt a korlátot kizárólag az n-ed rendű, valós Hadamard mátrixok érik el.*

A maximális determinánsú ± 1 elemű mátrixok, vagy más néven „D-optimal" rendszerek irodalma rendkívül gazdag. Itt annyit említenénk meg, hogy ha n az $4k+3$ alakú, akkor még éles felső becslést sem ismerünk egy n-ed rendű, ± 1 elemű mátrix determinánsára. Speciálisan, már $n = 19$ esetén sem tudni, mekkora ez a maximum. A témakörrel kapcsolatban kiindulásként az Orrick és Solomon által fentartott honlap, valamint az ott fellelhető bőséges irodalom megtekintését javasoljuk [62].

A következőkben néhány példát mutatunk Hadamard mátrixokra, de előtte állapodjunk meg abban a sztenderd jelölésben, hogy a valós Hadamard mátrixokat egységesen H betűvel jelöljük, a dimenziójukat pedig H alsó indexeként tüntetjük fel.

1.2.3. Példa. Az alábbi három mátrix Hadamard:

$$H_1 = \begin{bmatrix} 1 \end{bmatrix}, H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, H_4 = \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix} \tag{1.1}$$

1.2.4. Definíció. Egy valós (vagy a későbbiekben komplex) Hadamard mátrixot normalizáltnak nevezünk, ha az első sorában és oszlopában kizárólag 1-esek állnak.

Teljesen világos, hogy tetszőleges valós (vagy később komplex) Hadamard mátrix ekvivalens egy ilyen normalizált Hadamard mátrixszal. Semmi más dolgunk nincs, mint a mátrix sorait (illetve oszlopait) megfelelő egységnyi abszolút értékű számmal beszorozni. Ezek szerint az érdemi információt egy Hadamard mátrix jobb alsó $n-1 \times n-1$-es részmátrixa tartalmazza. Ezt a mátrix *magjának* nevezzük. A továbbiakban ilyen normalizált mátrixokkal foglalkozunk. Mivel egy normalizált Hadamard mátrix sorai továbbrai is ortogonálisak, igaz a következő

1.2.5. Következmény. *Egy normalizált valós (komplex) Hadamard mátrix bármely (elsőtől különböző) sorában az elemek összege* 0*-t ad. Ez akkor is igaz, ha csak a mátrix első sora áll csupa* 1*-esből.*

1.2.1. Ekvivalencia osztályok

Az Hadamard-mátrixok körében fellép egy természetes ekvivalencia reláció, mégpedig a következőképpen: Ha H Hadamard, vagyis ortogonális mátrix, akkor természetesen a sorok- illetve oszlopok egy permutációját követően is az marad. Továbbá, bármely sort- vagy oszlopot szabad ± 1-gyel szorozni, ez sem sérti a Hadamard-tulajdonságot. Ezek az észrevételek motiválják a következőt:

1.2.6. Definíció. Ha H egy *valós* Hadamard-mátrix, akkor bármely D_1, D_2 *valós elemű* unitér diagonális illetve P_1, P_2 permutációs mátrixok esetén $H' = D_1 P_1 H P_2 D_2$ is Hadamard. Ekkor H'-t H-val ekvivalensnek mondjuk, és $H' \cong H$-ként jelöljük.

A legfeljebb 28 dimenziós Hadamard mátrixokat sikerült karakterizálni [16], a különböző ekvivalencia osztályok száma pedig rendre a következő: $n = 1, 2, 3, 4, 8$ és 12 dimenzióban mindössze egyetlen valós Hadamard mátrix van. Ismert még ezen kívül, hogy $n = 16$-ra 5, $n = 20$-ra 3, $n = 24$-re 60, végül $n = 28$-ra 487 páronként inekvivalens Hadamard mátrix van [39], [40], [52]. Ezek a dimenziók vannak teljesen leírva. Innentől azonban meglehetősen reménytelenné válik a helyzet: $n = 32$-re *legalább* 3.578.006, míg $n = 36$-ra *legalább* 18.292.717 ekvivalencia osztály létezik [61].

1. *Megjegyzés.* A fenti számok gyors növekedésének az egyik fő oka a következő jelenség, amelyre – többek között – Orrick hívta fel a figyelmet: Ha H_1 és H_2 két tetszőleges $m \times m$-es valós Hadamard mátrix, akkor bármely P általánosított permutációs mátrixra az alábbi két mátrix $2m \times 2m$-es Hadamard:

$$\begin{bmatrix} H_1 & PH_2 \\ H_1 & -PH_2 \end{bmatrix} \text{ és } \begin{bmatrix} H_1 & H_1 \\ H_2P & -H_2P \end{bmatrix} \tag{1.2}$$

Ezek a mátrixok azonban általában újabbnál újabb ekvivalencia osztályokat adhatnak $2m$ dimenzióban H_1, H_2, valamint P megválasztását követően. Az ilyenfajta jelenségek elkerülésére vezette be Orrick az ún. Q-ekvivalenciát, amelyek segítségével egy kezelhetőbb osztályozását adta a valós Hadamard mátrixoknak. Orrick [61]-ben igazolta, hogy $n = 4, 8, 12, 16, 20, 24$ és 28 dimenzióban rendre $1, 1, 1, 1, 1, 2$ és 2 Q-ekvivalencia osztály van, míg $n = 32$ és $n = 36$ dimenzióban a jelenleg ismert csillagászati számú inekvivalens valós Hadamard mátrixok mindössze 11 és 21 Q-ekvivalencia osztályba sorolhatók be.

2. *Megjegyzés.* Egyes irodalomban szokás az ún. általánosított ekvivalenciának a bevezetése, amelyben H^T is H-val ekvivalensnek tekintik. Ez nem magától értetődő, ugyanis előfordulhat, hogy H és H^T egymással szokásos értelemben nem ekvivalens. Az első ilyen jelenség $n = 16$ dimenzióban fordul elő.

Felmerül a kérdés, hogy két valós Hadamard mátrixról hogyan lehet eldönteni, hogy ekvivalensek-e? Ennek tárgyalásához van szükségünk a következőkre: egy permutációs mátrixot általánosítottnak nevezünk, ha minden sorában és minden oszlopában pontosan egy $+1$ vagy -1 áll. H önmagával való ekvivalenciáját H egy automorfizmusának nevezzük.

1.2.7. Definíció. Egy $n \times n$-es H Hadamard mátrix $\mathrm{Aut}(H)$ automorfizmuscsoportja a rendezett $n \times n$-es általánosított permutációs mátrix párok (U, V) halmaza, melyre $UHV^T = H$, a csoportművelet pedig a direktszorzat: $(U, V) \cdot (U', V') = (UU', VV')$.

Ebből azonnal adódik, hogy

1.2.8. Következmény. *Ha két mátrix automorfizmus csoportja különböző rendű, akkor a két mátrix nem lehet ekvivalens.*

3. *Megjegyzés.* Megjegyezzük azonban, hogy abból, hogy két mátrix automorfizmuscsoportja azonos elemszámú, sőt: izomorf, még nem következik, hogy a két mátrix ekvivalens lenne. Egy konkrét példa erre már említett két olyan inekvivalens, 16 dimenziós mátrix, melyben az egyik a másik transzponáltja.

1.3. Klasszikus konstrukciók

Ebben a fejezetben áttekintjük a legtermészetesebb, és a gyakorlati alkalmazások szempontjából legjelentősebb konstrukciókat. A jól ismert tenzorszorzat-módszer mellett bemutatjuk a Paley I és Paley II konstrukciót, továbbá beszélünk a Hadamard mátrixok és blokkrendszerek kapcsolatáról. Végül a Williamson-konstrukciót ismertetjük, amely az egyik legalapvetőbb iterációs eljárás, melynek építőkockái önmaguk nem Hadamard

mátrixok. Az ismertető előtt tisztázunk egy szükséges feltételt arra vonatkozóan, hogy milyen egészekre létezhet valós Hadamard mátrix.

1.3.1. Lemma. *Legyen H egy $n \times n$-es valós Hadamard mátrix. Ekkor $n = 1, 2$ vagy $n = 4k$ valamilyen k pozitív egész számra.*

Bizonyítás. $n = 1, 2$-re már láttunk konkrét példát. Ha H-nak legalább 3 sora van, akkor normalizáljuk le, és írjuk fel az ortogonalitási-egyenleteket az első három sorra. Az 1.2.5 következmény miatt H második sorában ugyanannyi $+1$, mint -1 szerepel, így n csak páros lehet, speciálisan: mind a $+1$, mind a -1 elemekből $n/2$-$n/2$ db van a második sorban. Természetesen ez a megállapítás H minden további sorára is érvényes. Felírva az ortogonalitási feltételt valamely két, az elsőtől különböző sorra adódik az állítás. □

Érdekes kérdés a fenti lemmának a megfordítása, mely szerint igaz-e, hogy minden 4-gyel osztható dimenzióban van Hadamard-mátrix? A kérdés több, mint 100 éve megoldatlan, és mindmáig a kombinatorikus mátrixanalízis talán egyik legizgalmasabb nyitott kérdése.

1.3.2. Sejtés (Hadamard)**.** *Minden 4-gyel osztható dimenzióban van valós Hadamard mátrix.*

A teljesség kedvéért mondjuk ki az alábbi lemmát.

1.3.3. Lemma. *Legyen H $n \times n$-es Hadamard mátrix. Legyen továbbá $\mathcal{S}_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. Ekkor*

1. *$-H$ is Hadamard mátrix;*
2. *H^T is Hadamard-mátrix;*
3. *ha H' is egy $n' \times n'$-s Hadamard-mátrix, akkor $H' \otimes H$ és $H \otimes H'$ is $n'n \times n'n$-es;*
4. *minden $t \geq 1$-re $(\otimes^t \mathcal{S}_1) \otimes H$ egy $2^t n$-edrendű Hadamard mátrix.*

1.3.1. Sylvester Hadamard mátrixok

A legősibb, és a gyakorlati alkalmazások szempontjából a leghasznosabb Hadamard-mátrix családot a Sylvester által konstruált $n = 2^t$ rendű mátrixok alkotják. Ezeket úgy kaphatjuk meg, hogy az előbb definiált $\mathcal{S}_1$ mátrixot t-szer tenzorszorozzuk önmagával, vagyis a fenti, 1.3.3 Lemmában $H = \begin{bmatrix} 1 \end{bmatrix}$-et veszünk. Az így kapott mátrixok mindegyike szimmetrikus.

1.3.4. Definíció. A Sylvester-Hadamard mátrixok az $\{\mathcal{S}_t = \otimes^t \mathcal{S}_1 : t \geq 1\}$ halmaz elemei.

1.3.5. Példa. $\mathcal{S}_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$,

$$\mathcal{S}_2 = \left[\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ \hline 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{array}\right], \mathcal{S}_3 = \left[\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ \hline 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{array}\right] \tag{1.3}$$

Egy, a tenzorszorzáshoz nagyban hasonlító konstrukció a 2.3.6 tétel alatt található.

1.3.2. Paley Hadamard mátrixok

A következő két Hadamard mátrix családot Paley konstruálta valamely páratlan rendű $GF(q)$ véges test kvadratikus maradékainak segítségével [63].

1.3.6. Definíció. Legyen $GF(q)^* = GF(q) \setminus \{0\}$ egy ciklikus csoport. Értelmezzünk ezen a csoporton egy χ karaktert a következőképpen. $\chi(g) = 1$, ha g kvadratikus maradék $GF(q)$-ban, és $\chi(g) = -1$, ha kvadratikus nemmaradék, majd terjesszük ki ezt a definíciót magára $GF(q)$-ra olymódon, hogy $\chi(0) = 0$ legyen. Ha $q = p$ prím, és $g \in \mathbb{Z}$, akkor χ a jól ismert $\left(\frac{g}{p}\right)$ Legendre-szimbólum.

Mi magának Paley-nek az eredeti konstrukcióját adjuk meg, egy elérhető bizonyítás [41]-ben található.

1.3.7. Lemma. *Legyen q prímhatvány, és legyen $\{g_0 = 0, g_1, g_2, \ldots, g_{q-1}\}$ $GF(q)$ egy felsorolása. Legyen továbbá $Q = \left[\ \chi(g_i - g_j)\ \right]_{0 \leq i,j < q}$, és így S az a $q+1 \times q+1$-es mátrix, amelyet úgy kapunk, hogy Q-hoz hozzáveszünk egy sor illetve egy oszlop $+1$-et, végül az első sor első elemét 0-nak definiáljuk. Ekkor*

1. *Ha $q \equiv 3 \mod 4$, akkor az ún Paley I Hadamard mátrix a következő $q+1$-ed rendű mátrix:*

$$P_q = \begin{bmatrix} 1 & (-1)^q \\ (1^q)^T & Q + I_q \end{bmatrix}. \tag{1.4}$$

2. *Ha* $q \equiv 1 \mod 4$, *akkor az ún Paley II Hadamard mátrix egy* $2(q+1)$ *rendű mátrix:*

$$P'_q = \begin{bmatrix} S + I_{q+1} & S - I_{q+1} \\ S - I_{q+1} & -S - I_{q+1} \end{bmatrix}. \tag{1.5}$$

1.3.8. Definíció. Legyenek $\{q_i, i \in I\}$ és $\{q'_j, j \in J\}$ véges sok prímhatványoknak a halmazai, melyek rendre 3-al illetve 1-gyel kongruensek, modulo 4. Ekkor Paley-mátrixnak nevezünk minden olyan mátrixot, amely ekvivalens egy $(\otimes_{i\in I} P_{q_i})\otimes(\otimes_{j\in J} P'_{q'_j})$ alakú mátrixszal.

A Paley-mátrixok automorfizmuscsoportja teljesen le van írva. Kantor a Paley I mátrixokét már 1969-ben karakterizálta [50], míg a Paley II mátrixok automorfizmuscsoportjára mintegy 40 évvel később derült fény: ezt csak 2007-ben tudta de Launey és Stafford meghatározni [25]. A két eredmény összevetéséből adódik az alábbi

1.3.9. Lemma (Kantor [50], de Launey–Stafford [25])**.** *Egy Paley I típusú* P_q *és egy Paley II típusú* $P'_{q'}$ *mátrix akkor és csak akkor ekvivalensek, ha* $q = 11$ *és* $q' = 5$.

1.3.10. Példa. $GF(11)$-ben a kvadratikus maradékok $1, 3, 4, 5, 9$, és az ebből kapható Paley I típusú P_{11} Hadamard mátrix a következő, 12×12-es mátrix:

$$H_{12} = P_{11} = \left[\begin{array}{c|cccccccccccc} 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ \hline 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \end{array}\right] \tag{1.6}$$

1.3.3. Blokkrendszerek és Hadamard-mátrixok

Három lényegesen különböző módon lehet blokkrendszerek segítségével Hadamard mátrixokat konstruálni. Ezek egyike, az előbb említett Paley I konstrukció. Most egy kis blokkrendszer-elmélet következik:

1.3.11. Definíció. Egy négyzetes $2-(v,k,\lambda)$-rendszer egy olyan $\mathcal{D}=(P,B)$ pár, ahol $P=\{p_1,p_2,\ldots,p_v\}$ a pontok halmaza, $B=\{B_1,B_2,\ldots B_v\}$ pedig ezen pontok valamely k elemű részhalmazai $(1<k<v)$, a blokkok, mégpedig úgy, hogy bármely két különböző pont pontosan λ blokkban szerepel.

A $\mathcal{D}$ teljes automorfizmus csoportja $\mathrm{Aut}(\mathcal{D})$, mely az összes olyan illeszkedés tartó $P\cup B$ bijekcióból áll, mely pontokat pontokba-, blokkokat blokkokba képez. $\mathcal{D}$ egy automorfizmus csoportján $\mathrm{Aut}(\mathcal{D})$ egy részcsoportját értjük. Ha G egy olyan automorfizmus csoportja $\mathcal{D}$-nek, hogy bármely p és p' pontok esetén egy és csak egy olyan $g\in G$ van, hogy $p^g=p'$, és ez hasonlóan a blokkokra is teljesül, akkor azt mondjuk, hogy $\mathcal{D}$ reguláris a pontokon, az ilyen tulajdonságú G pedig $\mathcal{D}$-nek egy reguláris- vagy Singer csoportja.

$\mathcal{D}$ illeszkedési mátrixa az az $A=\left[\ a_{ij}\ \right]$ $v\times v$-es $\{0,1\}$-mátrix, melyben $a_{ij}=1$ akkor és csak akkor, ha $p_j\in B_i$.

Elemi leszámlálásból adódik a következő észrevétel:

1.3.12. Lemma. *Egy $2-(v,k,\lambda)$ blokkrendszer létezésének szükséges feltétele, hogy*

$$\lambda(v-1)=k(k-1) \tag{1.7}$$

fennálljon.

Ezekből következik, hogy egy $v\times v$-es $\{0,1\}$-mátrix akkor és csak akkor az illeszkedési mátrixa egy (v,k,λ) struktúrának, ha

$$AA^T=(k-\lambda)I+\lambda J, AJ=kJ \tag{1.8}$$

ahol szokás szerint I az identitás-, J pedig a csupaegy mátrixot jelöli.

1.3.13. Példa. Hogy illusztráljuk a konstrukciót, tekintsük a P_7 Paley I mátrixot, amelyet az $\{1,2,4\}$ kvadratikus maradékok (mod 7) definiálnak, majd normalizáljuk le, azaz szorozzuk be az összes, elsőtől különböző oszlopát -1-gyel, hogy a következőt kapjuk:

$$P_7\cong\begin{bmatrix}1 & 1^7\\ (1^7)^T & -(Q+I)\end{bmatrix}=\left[\begin{array}{c|cccccccc}1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\ \hline 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1\\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1\\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1\\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1\\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1\\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1\end{array}\right] \tag{1.9}$$

Látható, hogy a normalizált P_7 mátrix $-(Q+I)$ magja ciklikus. A magnak a $(0,1)$-verziója nem más, mint

$$A = \frac{1}{2}(J-(Q+I)) = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \tag{1.10}$$

Ekkor $AA^T = 2I + J, AJ = 3J$, A tehát az illeszkedési mátrixa valamely $(7,3,1)$-struktúrának, amely nem más, mint a jól ismert Fano-sík.

Általában véve az (1.8) formula segítségével lehet normalizált $n = 4m$ rendű Hadamard mátrixokat készíteni blokkrendszerekből, mégpedig oly módon, hogy a $(4m-1, 2m-1, m-1)$-rendszert azonosítjuk a Hadamard mátrix magjával, azaz ha $A' = 2A - J$ az illeszkedési mátrixból kapott ± 1 mátrix, akkor az alábbi

$$H = \begin{bmatrix} 1 & 1^{4m-1} \\ (1^{4m-1})^T & A' \end{bmatrix} \tag{1.11}$$

a megfelelő $n = 4m$-ed rendű Hadamard mátrix, és megfordítva. Érvényes tehát a következő

1.3.14. Lemma. *Akkor és csak akkor létezik $n = 4m$-ed rendű valós Hadamard mátrix, ha létezik egy négyzetes $(4m-1, 2m-1, m-1)$-rendszer.*

1.3.15. Definíció. Egy $(4m-1, 2m-1, m-1)$-rendszert Hadamard-rendszernek nevezünk.

Az egyik leghatékonyabb módja az Hadamard-rendszerek konstrukciójának, ha differencia halmazból származtatjuk őket.

1.3.16. Definíció. Legyen G egy additívan írt véges Abel-csoport. A $D \subset G$ részhalmazt (v,k,λ) differencia halmaznak nevezzük, ha $|G| = v$, $|D| = k$, továbbá minden $0 \neq g \in G$ esetén pontosan λ olyan $d_1 \neq d_2$ D-beli pár van, amelyre $d_1 - d_2 = g$. A differencia halmaz rendje $n = k - \lambda$. Egy differencia halmazt ciklikusnak, Abel-félének, stb. nevezünk, ha G ilyen tulajdonsággal rendelkezik.

A differencia halmazok és Hadamard rendszerek kapcsolatáról szól a következő

1.3.17. Tétel ([6]). *Legyen G egy v-ed rendű csoport, D pedig egy k elemű valódi részhalmaza. Jelölje* $\mathrm{dev}(D)$ *a* $(G, \{gD, g \in G\})$ *párt. Ekkor D egy (v, k, λ) differencia halmaz G-ben akkor és csak akkor, ha* $\mathrm{dev}(D)$ *egy négyzetes (v, k, λ)-rendszer, amelynek G egy reguláris csoportja. Minden reguláris G csoporttal rendelkező négyzetes blokkrendszer reprezentálható ilyen módon.*

1.3.18. Példa. Tekintsük (az additívan írt) $\mathbb{Z}_7$-ben a kvadratikus maradékok $D = \{1, 2, 4\}$ halmazát. Ekkor D egy $(7, 3, 1)$ differencia-halmaz $\mathbb{Z}_7$-ben, és a $\mathrm{dev}(D)$ illeszkedési mátrixa éppen a fenti (1.10) alatti A.

1.3.19. Definíció. Egy Hadamard (precízebben: Paley-Hadamard) differencia halmaz valamely G csoportban $(4m-1, 2m-1, m-1)$ paraméterekkel rendelkezik. A $GF(q)$-beli kvadratikus maradékoktól eltekintve, melyek segítségével a Paley I Hadamard mátrixok konstruálhatók, két további differencia halmaz konstrukció ismert, mégpedig a Singer- és az ikerprím differencia halmazok.

1.3.20. Példa. Az ismert három differencia halmaz család a következő:

1. Paley differencia halmazok, melyek paramétere $(q, (q-1)/2, (q-3)/4)$, ahol $q \equiv 3 \mod 4$, amelyek nem mások, mint a véges $GF(q)$ testnek a $(GF(q), +)$ additív csoportjában lévő kvadratikus maradékok halmaza:

$$D = \{g^2 : g \in GF(q)^*\} \tag{1.12}$$

2. Singer differencia halmazok, vagy más néven m-sorozatok, melyek paramétere $(2^t - 1, 2^{t-1} - 1, 2^{t-2} - 1)$. Ebben a differencia halmaz választható $\mod 2^t - 1$ azon egészeknek [47], amelyekre

$$D = \{i : 0 \le i \le 2^t - 1, \mathrm{tr}(\alpha^i) = 0\}, \tag{1.13}$$

ahol α egy generátora $GF(2^t)^*$-nak, és $\mathrm{tr} : GF(2^t) \to GF(2)$ nyomleképezés: $\mathrm{tr}(g) = \sum_{i=0}^{t-1} g^{2^i}$.

3. Az ikerprím differencia halmazok, melyek paramétere $(q(q+2), [q(q+2)-1]/2, [q(q+2)-3]/4)$, ahol q és $q+2$ mindketten prímhatványok. Itt a differencia halmaz választható $(GF(q), +) \times (GF(q+2), +)$ részeként, úgymint

$$D = \{(g, h) \in GF(q)^* \times GF(q+2)^* : \chi(g)\chi(h) = 1\} \cup \{(g, 0) : g \in GF(q)\}, \tag{1.14}$$

ahol χ a kvadratikus karaktere a megfelelő testnek [48].

És akkor most egy példa a példára:

1.3.21. Példa. Legyen $q = 3$, ekkor $q + 2 = 5$ prímhatványok. Ekkor $G = GF(3) \times GF(5)$, és a fenti 3-as konstrukció szerint kiválogathatjuk azokat a (g, h) párokat, amelyek vagy mindketten kvadratikus maradékok, $\mod 3$ és $\mod 5$, vagy egyikük sem. Az így nyert D halmaz a következő: $D = \{(0,0), (0,3), (0,4), (1,1), (1,2), (1,4), (2,4)\}$. Ebből pedig úgy kapunk mátrixot, hogy ezt a D halmazt $GF(3) \times GF(5)$ minden elemével eltoljuk. Ezt követően vesszük a csupanulla 15×15-ös mátrixot, amelynek a sorait illetve oszlopait G elemeivel indexeljük. Egy rögzített (g, h) indexű sorban a 0-kat $+1$-re pontosan a $(g, h) + D$ elemeivel indexelt oszlopokban cseréljük le. Így a következő $(15, 7, 3)$ Hadamard-rendszerhez jutunk, melynek A illeszkedési mátrixa:

$$\begin{array}{c|ccccc|ccccc|ccccc}
\{0,0\} & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\
\{0,1\} & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
\{0,2\} & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
\{0,3\} & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\
\{0,4\} & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
\hline
\{1,0\} & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
\{1,1\} & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
\{1,2\} & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
\{1,3\} & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
\{1,4\} & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
\hline
\{2,0\} & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
\{2,1\} & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
\{2,2\} & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
\{2,3\} & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
\{2,4\} & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1
\end{array} \tag{1.15}$$

Ezt követően A-t transzformáljuk át a szokásos módon ± 1 mátrixszá, majd egészítsük ki egy extra $+1$ sorral és oszloppal, hogy a következő 16×16-os Hadamard mátrixhoz jussunk:

$$H_{16} = \begin{array}{c|cccccccccccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\hline
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 \\
1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 \\
1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\
1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 \\
1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\
\hline
1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\
1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \\
1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\
1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\
1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\
\hline
1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\
1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & -1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1
\end{array} \tag{1.16}$$

1.3.4. Williamson Hadamard mátrixok

A Williamson Hadamard konstrukció az egyik legegyszerűbb helyettesítési technikát alkalmazó konstrukció, amely segítségével igen sokféle Hadamard mátrixot lehet konstruálni. Az alapgondolat az, hogy próbáljunk egy „nagy" Hadamard mátrix helyett több „kicsi" építőkockát keresni, amelyek bizonyos, az ortogonalitást helyettesítő tulajdonsággal bírnak. A Williamson Hadamard konstrukció pillére egy 4×4-es Hadamard mátrix, amely elemeit valamilyen nagyobb dimenziós blokkokra cseréljük a következő lemma szerint:

1.3.22. Lemma. *Ha léteznek olyan A, B, C, D $m \times m$-es ± 1 mátrixok, melyekre*

$$XY^T = YX^T \text{minden } X \neq Y \in \{A, B, C, D\}, \tag{1.17}$$

továbbá

$$AA^T + BB^T + CC^T + DD^T = 4mI_m, \tag{1.18}$$

akkor az alábbi

$$W = \begin{bmatrix} A & B & C & D \\ B & -A & D & -C \\ C & -D & -A & B \\ D & C & -B & -A \end{bmatrix} \tag{1.19}$$

tömb egy $n = 4m$ rendű Hadamard mátrix.

Williamson eredetileg szimmetrikus, ciklikus mátrixok formájában kereste az A, B, C és D komponenseket, ekkor ugyanis (1.17) automatikusan teljesül.

1.3.23. Definíció. A Williamson Hadamard mátrixok azok, amelyek a fenti 1.3.22 lemma segítségével kosntruálhatóak.

A Williamson Hadamard-mátrixok többségét masszív számítógépes kereséssel prezentálták. Đoković találta az első olyan páratlan $m = 35$ számot, amelyre nincs szimmetrikus, ciklikus komponensekből adódó Williamson-Hadamard mátrix [29]. Ez a legkisebb ilyen tulajdonságú szám. Valószínűsítik, hogy Williamson Hadamard mátrix minden $4k$ alakú n-re létezik, a legkisebb eldöntetlen eset a $w = 47$.

1.3.24. Sejtés. *Minden néggyel osztható n-re létezik $n \times n$-es Williamson Hadamard mátrix.*

A Williamson Hadamard mátrxiok kétféleképpen általánosíthatóak: egyrészt további szimmetriai feltételeket szabhatunk az A, B, C, D komponensekre, másfelől magát a 4×4-es alap-Hadamard mátrixot is variálhatjuk. Két speciális konstrukciót fogunk említeni a következő szakasz végén. Megjegyezzük, hogy az itt prezentált négy konstrukció nem feltétlenül ad egy adott dimenzióban inekvivalens mátrixokat. Ilyen egybeeséseket világít meg a fejezetet lezáró két lemma.

1.3.25. Lemma (Turyn, [85]). *Legyen $q \equiv 1 \mod 4$ egy prímszám, és legyen P'_q egy Paley II típusú Hadamard mátrix. Ekkor P'_q ekvivalens egy olyan Williamson Hadamard mátrixszal, amelynek komponensei szimmetrikus, ciklikus mátrixok.*

1.3.26. Lemma ([42]). *A Singer differencia halmazból konstruálható Hadamard mátrixok ekvivalensek az $\mathcal{S}_t$ Sylvester családdal.*

1.4. Véges csoportokból származtatott konstrukciók

Az előző fejezetet a Williamson-mátrixok tárgyalásával fejeztük be, és megemlítettük, hogy egy modern kutatási irány a komponens mátrixok belső struktúrájának a variálása. Egy jól bevált technika az, hogy a ciklikus mátrixokat „megfordítjuk", és anticiklikussá tesszük, ezáltal a mátrix belső struktúrája nagyban hasonlítani fog egy ciklikus csoport szorzástáblájára. Természetesen, ha egy Williamson mátrix komponenseit mind-mind szisztematikusan ciklikusból anticiklikussá változtatjuk, akkor az eredetivel ekvivalens mátrixot kapunk. Ez az észrevétel az, ami alapján véges csoportok elméletével próbálnak különféle speciális Williamson Hadamard mátrixokat konstruálni. A fő eszközök a véges csoportok karakterelmélete és különféle differencia-halmazok kombinatorikus tulajdonságainak az ismerete.

1.4.1. Definíció. Legyen G egy v-ed rendű multiplikatív csoport, melynek elemeinek egy rögzített felsorolása $\{g_1, g_2, \ldots, g_v\}$. Egy valamely S halmaz elemeiből készített mátrixról azt mondjuk, hogy a G csoportból származik, ha G elemeivel indexelve a mátrix sorait és oszlopait van egy olyan $\Phi : G \to S$ leképezés, hogy a mátrix (i,j)-dik eleme $\Phi(g_i g_j)$, minden $1 \leq i, j \leq v$-re. Az ilyen mátrixokat $\left[\ \Phi(g_i g_j) \ \right]_{1 \leq i,j \leq v}$ módon jelöljük.

Egy csoportból származó mátrixot csak egyetlen oszlopának, vagy sorának és persze a háttérben meghúzódó G csoportnak az ismerete alapján felépíthetünk. A g elemmel indexelt $\left[\ \Phi(gg_i) \ \right]_{1 \leq i \leq v}$ sort megkaphatjuk magából az $1 \in G$ elemmel indexelt $\left[\ \Phi(g_i) \ \right]_{1 \leq i \leq v}$ sorból egyetlen balszorzás segítségével.

Nyilvánvalóan a centrális kérdés az az, hogy mikor lesz egy csoportból származó mátrix Hadamard?

1.4.2. Példa. Az alábbi, negaciklikus Hadamard mátrix $\mathbb{Z}_4 = \{0,1,2,3\}$-ből származik, mégpedig úgy, hogy $\Phi(0) = \Phi(1) = \Phi(2) = -1$, és $\Phi(3) = 1$.

$$\begin{bmatrix} -1 & -1 & -1 & 1 \\ -1 & -1 & 1 & -1 \\ -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & -1 \end{bmatrix} \tag{1.20}$$

Az egyik centrális fogalom a regularitás:

1.4.3. Definíció. Azokat a mátrixokat, amelyekben egy adott sorban, vagy oszlopban lévő elemek összege állandó, regulárisnak nevezünk.

Természetesen egy olyan, csoportból származó mátrix, amelynek elemei ráadásul egy $(S,+)$ Abel-csoport elemei, mindig reguláris.

1.4.4. Lemma ([42]). *Legyen H egy $v\times v$-es ± 1 mátrix és legyen $A=\frac{1}{2}(H+J)$ a hozzá tartozó $\{0,1\}$ mátrix. Tegyük fel, hogy $v>2$. Ekkor egy H Hadamard mátrix pontosan akkor reguláris, ha $v=u^2$, és A az illeszkedési mátrixa egy négyzetes $(4u^2, 2u^2\pm u, u^2\pm u)$-rendszernek.*

1.4.1. Menon Hadamard mátrixok

Sejthető, hogy egy csoportból származó Hadamard mátrix – lévén reguláris – szoros kapcsolatban áll a négyzetes blokkrendszerekkel. Valójában kombinatorikai konstrukciókkal adódnak differencia halmazokból. Egy $(4u^2, 2u^2\pm u, u^2\pm u)$-differencia halmazt Menon-Hadamard differencia halmaznak nevezünk. A következő lemma összekapcsolja ezen differencia halmazokat és a csoportból származó Hadamard mátrixokat.

1.4.5. Lemma. *Legyen G egy $v=4u^2$ rendű csoport, és $\phi: G\to\{\pm 1\}$ egy leképezés. Egy G-ből származó mátrix akkor és csak akkor Hadamard, ha a $\{g\in G:\phi(g)=-1\}$ egy Menon-Hadamard differencia halmaz G-ben.*

1.4.6. Definíció. A Menon-Hadamard mátrixok azok az 1.4.5 lemma alapján létrejövő mátrixok.

Számos algebrista foglalkozott Menon-Hadamard differencia halmazok konstrukciójával, felvonultatva karakter elméleti-, véges geometriai- és algebrai számelméleti apparátusokat. A természetes, legegyszerűbb út az az lenne, hogy ciklikus $G=\mathbb{Z}_{4u^2}$ csoportból kiindulva próbálunk meg G-ből származó Menon-Hadamard mátrixot konstruálni. Meglepő módon azonban, az egyetlen 4×4-es negaciklikus mátrixtól eltekintve nem ismerünk ilyen mátrixokat, sőt, Schmidt aszimptotikus eredményének köszönhetően valószínűsíthető, hogy – valósban legalábbis – nincs is más ilyen mátrix.

1.4.7. Tétel (Schmidt, [49]). *Legyen Π páratlan prímek véges halmaza. Ekkor legfeljebb csak véges sok olyan ciklikus u^2 rendű Menon-Hadamard differencia halmaz lehet, amelyben u^2 minden prímosztója Π-beli.*

Speciálisan, mindössze 14 olyan páratlan $u\le 10.000$ van, amelyre még nem tisztázott, hogy van-e ciklikus valós Hadamard mátrix, a legkisebb ilyen az $u=165$.

1.4.8. Sejtés (Ryser, [60]). *Ha $n > 4$, akkor nincs ciklikus valós Hadamard mátrix.*

4. *Megjegyzés.* A valósakkal ellentétben komplex esetben *vannak* ciklikus komplex Hadamard mátrixok, melyek egy igen fontos általános családot alkotnak. Ezt bővebben a 2.3.3 szakaszban tárgyaljuk.

A szakaszt néhány csoportból származó Hadamard mátrix konstrukcióval zárjuk. Az első egy rendkívül mély eredmény, amely nemrégiben nyert bizonyítás. A tétel állítása az, hogy minden $4m^4$ dimenzióban van valós Hadamard mátrix.

1.4.9. Tétel (Xia [90], Wilson–Xiang [88], Chen [13]). *Bármely $a, b \geq 0$ és bármely páratlan m-re létezik $n = 4 \cdot 2^{2a} \cdot 3^{2b} \cdot m^4$ rendű, Abel-féle csoportból származó Menon-Hadamard mártix.*

A nem kommutatív csoportok esetén a diéder csoport lehetne az első, amelyből Hadamard mátrixokat próbálna konstruálni az ember, de sajnos egy ilyennek a felbukkanása ugyanúgy nem túl valószínű, mint a ciklikus Hadamard mátrixoké.

1.4.10. Tétel (Dillon, Fan et al. [22]). *Ha egy $4u^2$ rendű diéder csoport tartalmaz Menon-Hadamard differencia halmazt, akkor már maga $\mathbb{Z}_{4u^2}$ is.*

Ennek ellenére azért sikerült olyan Menon-Hadamard differencia halmazokat konstruálni nem kommutatív csoportok segítségével, ahol kommutatívokból egyébként nem lehet. Smith reprezentáció elméleti és számítógépes eszközöket felhasználva lelt rá egy olyan 100-ad rendű csoportra, amely se nem kommutatív, se nem a diéder csoport, de 5-Sylow részcsoportként tartalmazza a $\mathbb{Z}_5^2$-t. A tenzorszorzás segítségével ez az egyetlen példa egy végtelen családdá egészíthető ki.

1.4.11. Tétel (Smith, [76]). *Bármely olyan $a, b, c \geq 0$ számok esetén, amelyekre ha $b > 0$, akkor $a > 0$ teljesül, létezik $n = 4 \cdot 2^{2a} \cdot 3^{2b} \cdot 5^2 \cdot 10^{2c}$ rendű Menon-Hadamard mátrix.*

1.4.2. Ito Hadamard mátrixok

Ito 1981-ben vezette be az ún. Q-típusú Hadamard mátrixokat [43]. Ezek azon Hadamard mártixok, amelyek ekvivalensek egy, a következő alakban adott mátrixszal:

$$Q = \begin{bmatrix} A & B & C & D \\ B & -A & D & -C \\ C^T & -D^T & -A^T & B^T \\ D^T & C^T & -B^T & -A^T \end{bmatrix} \tag{1.21}$$

ahol az m-edrendű A, B, C, D mátrixok mindegyike ciklikus. Ito észrevette, hogy egy ilyen Q mátrix akkor és csak akkor lesz Hadamard, ha

$$AA^T + BB^T + CC^T + DD^T = 4mI_m \tag{1.22}$$

továbbá

$$AB^T + CD^T = BA^T + DC^T \tag{1.23}$$

Így speciálisan azok a Williamson Hadamard mátrixok, amelyek szimmetrikus, ciklikus komponensekből állnak egyúttal Q típusú Hadamard mátrixok. Ito megmutatta azt is, hogy a $4m$ rendű Paley I Hadamard mártixok minden olyan m-re Q típusúak, amelyekre $4m-1$ prímhatvány [44]. Nem sokkal később csoportelméleti eszközök segítségével olyan $4m$ dimenziós Hadamard mátrixokkal bővítette a palettát, amelyekre $2m-1 \equiv 1 \mod 4$ prímhatvány [45].

1.4.12. Definíció. Az Ito Hadamard mátrixok azok az olyan Hadamard mátrixok, amelyek ekvivalensek egy Q típusú mátrixszal úgy, hogy mind A, B, C, D ciklikusak.

1.4.13. Sejtés (Ito)**.** *Minden páratlan m-re létezik $4m$-ed rendű Ito Hadamard mátrix.*

1.4.3. A dupla ciklikus magú mátrixok

Most Fletcher, Gysin és Seberry konstrukcióját ismertetjük, melynek segítségével sikeresen mutattak Hadamard mátrixokat $4m = 2t+2$ dimenzióban, minden páratlan $3 \leq t \leq 75$-re, így az első hiányzó eset az $m = 39$-hez tartozik, és mindössze öt $t = 50$-nél kisebb hiányzó eset van [54]. A konstrukció a következő blokkmátrix-reprezentációt használja:

$$\begin{bmatrix} -1 & -1 & 1^t & 1^t \\ -1 & 1 & 1^t & (-1)^t \\ (1^t)^T & (1^t)^T & A & B \\ (1^t)^T & (-1^t)^T & B^T & A^T \end{bmatrix}, \tag{1.24}$$

ahol A és B olyan ciklikus mátrixok, amelyekre

$$AA^T + BB^T = (2t+2)I_t - 2J_t \tag{1.25}$$

teljesül.

1.4.14. Sejtés (Kotsireas–Koukouvinos–Seberry, [54])**.** *Minden $n = 4m$ dimenzióban van dupla ciklikus magú Hadamard mátrix.*

1.4.4. T-mátrixok és a Goethals–Seidel tömb

A fejezetet egy modern, ám rendkívül számításigényes konstrukcióval zárjuk. A módszer erősségét mutaja, hogy 2004-ben ennek a segítségével sikerült az akkori legkisebb nyitott dimenzióban, 428-ban Hadamard-mátrixot konstruálni, és vitathatatlanul legnagyobb esélyt a következő, 668-as dimenzió tisztázására is ez a módszer szolgáltat. A következő tétel tulajdonképpen kombinálja Williamson és Ito elképzeléseit.

1.4.15. Tétel (Goethals–Seidel). *Tegyük fel, hogy A, B, C, D olyan ciklikus $m \times m$-es mátrixok, amelyre szokás szerint*

$$AA^T + BB^T + CC^T + DD^T = 4mI_m \tag{1.26}$$

teljesül. Jelölje R az antidiagonális mátrixot. Ekkor a következő mátrix Hadamard:

$$GS = \begin{bmatrix} A & BR & CR & DR \\ BR & -A & RD & -RC \\ CR & -RD & -A & RB \\ DR & RC & -RB & -A \end{bmatrix} \tag{1.27}$$

A fenti A, B, C, D mátrixokat speciális ± 1 sorozatokból, ún. T- illetve Turyn-sorozatokból lehet konstruálni. Az érdeklődő olvasó mindezekről sokkal részletesebben a H_{428} felfedezéséről szóló [51] cikkben olvashat.

1.5. Összefoglalás

Ebben a fejezetben a mindannyiunk által jól ismert klasszikus konstrukciók mellett bemutattuk azokat az újabb fajta megközelítéseket is, amelyek segítségével valós Hadamard mátrixokat próbálnak konstruálni. Kiemelnénk ezek közül egyrészt a néhány éves, akkor nagy meglepetést keltett 1.4.9 tételt, illetve a mai számítógépes világban a legeredményesebbnek bizonyuló Goethals-Seidel tömb konstrukcióját.

Megjegyezzük, hogy a Sylvester- és a Paley I konsrtukció segítségével, valamint a tenzorszorzással csupán az $n = 92$, $n < 100$ eset az ami eldöntetlen, erre viszont egyszerű számítógépes kereséssel lehet Williamson-tömböt készíteni.

Habár számtalan módon lehet valós Hadamard mátrixokat konstruálni, maga az Hadamard-sejtés lényegében támadhatatlannak tűnik. A probléma centralitását többek között az is mutatja, hogy a *Mathworld*-ön (a Goldbach- és a Riemann-sejtést követően) a harmadik legfontosabb nyitott kérdésként szerepel [86]. A fejezetet néhány ezirányú aszimptotikus eredmény idézésével zárjuk.

1.5.1. Tétel (Agaian, [1]). *Ha van $4u$ és $4v$ rendű valós Hadamard mátrix, akkor $8uv$ rendű is van.*

Ennek egy bizonyos szempontból erősebb változata a következő.

1.5.2. Tétel (Craigen–Seberry–Zhang, [21]). *Tegyük fel, hogy létezik* $4u, 4v, 4p$ *és* $4q$ *rendű valós Hadamard mátrix. Ekkor létezik* $16uvpq$ *rendű is.*

1977-ig a legkisebb eldöntetlen dimenizó $n = 268 = 4 \cdot 67$ volt [69], azután 2004-ig $n = 428 = 4 \cdot 107$ [51]. A jelenlegi legkisebb ilyen az $n = 668 = 4 \cdot 167$. Az összes többi, legfeljebb 1000-es dimenzióra a 668-on kívül már csak a 716 és 892 esetek eldöntetlenek, legutóbb Đokovic konstruált 764 dimenzióban csoportelméleti megfontolásokat és számítógépes keresést kombinálva Hadamard mátrixot [30]. Azt gondoljuk, hogy a számítástechnika töretlen fejlődésének köszönhetően néhány éven belül sikerül a három szóban forgó, eddig még eldöntetlen dimenzióban is valós Hadamard mátrixot mutatni.

Az egyik lehetséges módszer az Hadamard-sejtés igazolására az, hogy megmutatjuk, hogy elég nagy n-től kezdve már létezik Hadamard-mátrix, a fennmaradó dimenziókban pedig valahogyan konstruálunk mátrixokat. Az első ilyen irányú eredmény 1976-ból Seberry nevéhez fűződik [73] (lásd még [46]). Ezt lényegesen megjavította Craigen, aki csoportelméleti eszközökkel, és speciális $\{0, \pm 1\}$ sorozatok segítségével érte el az alábbi eredményét:

1.5.3. Tétel (Craigen, [20]). *Ha* m *páratlan természetes szám, akkor van*

- $2^{2b}m$ *rendű Hadamard-mátrix, ahol* b *az* m *bináris alakjában lévő* 1*-esek száma.*
- $2^t m$, *ha* $t = 6\left\lfloor \frac{1}{16}\log_2\left((m-1)/2\right)\right\rfloor + 2$.

Egy másik, az eddigiektől eltérő út az Hadamard-sejtés megoldásához a következő kérdés minél pontosabb megválaszolása: Melyik az a legnagyobb $r := r(n)$ szám, amelyre van $r \times n$-es $\{\pm 1\}$ mátrix úgy, hogy $HH^T = rI$ teljesüljön? Másszóval, egy Hadamard mátrixnak hány sorát tudjuk mindenképpen garantálni? Ismert, hogy elég nagy n-re $r \geq \frac{1}{3}n$ mindig teljesül [24].

A fenti két irányt kombinálva igazolta nemrégiben de Launey és Gordon a következő, meglepő eredményt:

1.5.4. Tétel (de Launey–Gordon, [26]). *Legyen* $\varepsilon > 0$. *Ha az általánosított Riemann-sejtés igaz, akkor minden* $n = 4m$*-re* $r(n) \geq \frac{1}{2}n - n^{17/22+\varepsilon}$.

2. fejezet

Komplex Hadamard mátrixok

2.1. Bevezetés

A valós Hadamard mátrixok általánosításának egyik lehetősége az, hogy a valós, ± 1 elemek helyett már tetszőleges, egységnyi abszolút értékű komplex számokból építjük a mátrixainkat. A komplex Hadamard mátrixok iránti általánosabb érdeklődés tulajdonképpen Werner [87]-ben közölt eredményeinek köszönhető, ahol arra mutat rá, hogy különböző kvantum-információelméleti fogalmak – a páronként torzítatlan bázisok (MUB), az unitér operátorokból álló bázisok és bizonyos teleportáló illetve kvantum kódoló sémák – szoros kapcsolatban állnak a komplex Hadamard mátrixokkal. A komplex Hadamard mátrixok tehát inkább már analitikus, semmint algebrai struktúrának tekinthetőek, és az alkalmazások tekintetében is inkább kvantumfizikai problémákhoz köthetők.

A szituáció itt meglehetősen más, mint a valós esetben: egyrészt a jól ismert F_n Fourier mátrix az egy komplex Hadamard mátrix minden n dimenzióban, így nincs az Hadamard-sejtésnek komplex megfelelője, másfelől meglehetősen reménytelen vállalkozásnak tűnik átfogó, teljes képet adni róluk még kis dimenziókban is. Jelenleg teljes karakterizáció csak 5 dimenzióig van, Haagerup 1996-os eredményét [37] csak most sikerült Beauchampnak és Nicoaranák megjavítani: munkájuk teljesen leírja a 6×6-os *önadjungált* komplex Hadamard mátrixokat [4]. Két további figyelemre méltó, strukturális eredmény közül az egyik Moorhouse karakterizációja, aki a legnagyobb szimmetriákkal rendelkező, ún. 2-tranzitív komplex Hadamard mátrixokat írta le teljesen [57]. A másik cikk, amelyre felhívnánk a figyelmet, Björck és Haagerup munkássága, akik a komplex Hadamard mátrixoknak egy nagyon fontos osztályát, az ún. 3-indexű ciklikus komplex Hadamard mátrixokat klasszifikálták [10].

Egy másik alapvető eltérés abból fakad, hogy míg a valós Hadamard mátrixok keresése egy diszkrét, kombinatorikus probléma, addig a komplex Hadamard mátrixok

elemeit már a komplex egységkörön keressük, és előfordulhat hogy bizonyos mátrixok *paraméteres* családokat indukálnak. Diţă 2004-ben rámutatott arra [28], hogy összetett dimenzióban egy, a tenzorszorzáshoz hasonló eljárás segítségével kisebb dimenziójú Hadamard mátrixokból nagyobb dimenziójú, paraméteres családokat lehet létrehozni. Ezáltal ma már az ember a valós esettől eltérően nem egyszerűen izolált Hadamard mátrixok iránt érdeklődik, hanem arra kíváncsi, hogy egy adott mátrixból milyen paraméteres családok indulnak ki, és milyen kapcsolat van ezen családok között. 2006-ban két lengyel fizikus, W. Tadej és K. Życzkowski publikált egy katalógust [82], amelyben leírták a Fourier mátrixok egy paraméterezési lehetőségét, valamint felsorolták 16 dimenzióig az összes (általuk ismert) komplex Hadamard mátrixot. Ők vetették fel először azt a kérdést is, hogy vajon igaz-e hogy minden valós Hadamard mátrixból indul ki valamilyen paraméteres család. A katalógusuk azonban korántsem teljes, Matolcsi Máté, Réffy Júlia és a szerző egy közös munkában egy parkettázó konstrukció segítségével néhány új paraméteres Hadamard mátrix családot talált $8, 12$ illetve 16 dimenzióban [56]. Ez a fejezet azonban *nem* a közös munkát, hanem a szerző további ezirányú, *önálló* eredményeit mutatja be [81].

A fejezet felépítése a következő: először röviden ismertetjük a komplex Hadamard mátrixok alaptulajdonságait, valamint bemutatunk néhány korábbi olyan eredményt, amelyre a későbbiek folyamán hivatkozni fogunk. Ezt követően mutatunk egy, a [82] katalógusból kimaradt mátrix családot. Bemutatjuk, hogy miként leltünk rá először konkrét 10 és 14 dimenziós új mátrixokra, továbbá hogy ebből miként következtettünk magasabb dimenziós mátrixok létére, hogyan jöttünk rá a konferencia mátrixokkal való kapcsolatra. Legfontosabb eredményként megmutatjuk, hogy minden ilyen, konferencia mátrixokból konstruálható komplex Hadamard mátrix paraméterezhető. A fejezet második részében valós Hadamard mátrixok paraméterezésével foglalkozunk. Matolcsi Máté és Réffy Júlia korábbi eredményeit [56] felhasználva megmutatjuk, hogy nem minden valós Hadamard mátrix Diţă-szerű [28]. Speciálisan, ha p prím, akkor a $4p$ rendű valós Hadamard mátrix nem ilyen. Végezetül megadjuk a valós Hadamard mátrixok egy természetes paraméterezési lehetőségét: 12 dimenziótól kezdve minden valós Hadamard mátrixot ellátunk paraméterekkel. Eredményeink $10, 12$ és 14 dimenzióban új komplex Hadamard mátrixokkal egészítik ki a [82] katalógust, és megválaszolnak egy abban felvetett nyitott problémát.

A következő két fejezetben $*$-gal jelöltük azokat a lemmákat illetve tételeket, amelyek a szerző önálló, eddig az irodalomban sehol nem szereplő eredményei.

2.2. Áttekintés

Legelőször tisztáznunk kell azokat a tulajdonságokat, amelyek a komplex Hadamard mátrixokat lényegesen megkülönböztetik a valósaktól. Az első lépés az 1.2.4 definíció kiterjesztése:

2.2.1. Definíció. Legyen H egységnyi abszolút értékekű elemekből álló $n\times n$-es mátrix. Ha $HH^* = nI$ teljesül, akkor H-t (komplex) Hadamard mátrixnak nevezzük.

A komplex Hadamard mátrixok tehát *tetszőleges* egységnyi abszolút értékű elemekből állhatnak. Innen azonnal adódik egy, a valósakkal szembeni releváns különbség. Míg egy fix n-re csak véges sok valós Hadamard mátrix lehetett, és mind a konstrukciókat, mind pedig az osztályozást is lényegében *diszkrét* eszközökkel lehetett kezelni, addig a komplex esetben már nem ez a helyzet. Egy komplex Hadamard mátrix bármely sorát egy tetszőleges, egységnyi abszolút értékű komplex számmal szorozva továbbra is komplex Hadamard mátrixot kapunk, íly módon máris *végtelen sok* mátrixot kapva. Annak érdekében, hogy az így egymásba transzformálható mátrixokat faktorizálhassuk, ki kell terjesztenünk az 1.2.6 definíciót a komplex esetre is:

2.2.2. Definíció. Két komplex Hadamard mátrixot, H_1-et és H_2-t ekvivalensnek nevezünk, ha vannak olyan D_1 és D_2 unitér diagonális mátrixok, illetve P_1 és P_2 permutációs mátrixok, hogy $H_2 = D_1P_1H_1P_2D_2$ teljesül. Erre a relációra szintén a $H_1 \cong H_2$-t jelölést használjuk.

Valójában az így nyert ekvivalencia relációt ki lehetne terjeszteni a transzponálásra illetve a komplex konjugálásra is, azonban három okból is a szokásos definíciónál maradnánk: egyrészt maga a transzponálás nem egy algebrailag kezelhető művelet, ezáltal elveszne (a valós Hadamard mátrixoknál nagyon lényeges) automorfizmus csoport (lásd az 1.2.7 definíciót) jelentősége. Másrészt a transzponálás, transzponálódás a gyakorlatban, fizikai rendszereknél sem fordul elő, mint jelenség. Harmadrészt a fellelhető irodalom elsöprő többsége ezt a szűkebb definíciót használja.

Meglepő módon a komplex esetben már nincs analógiája az Hadamard-sejtésnek.

2.2.3. Lemma. *Minden n dimenzióban van komplex Hadamard mátrix.*

Bizonyítás. A diszkrét Fourier transzformáció mátrixa, vagyis az $[F_n]_{i,j} = e^{\frac{2\pi \mathbf{i}}{n}ij}$ mátrix ilyen. Ezt a mátrixot röviden Fourier-mátrixnak nevezzük. □

Látszólag sokféle lehetőségünk van tehát komplex Hadamard mátrixokat konstruálni, azonban 5 dimenzióig már tisztázott a helyzet. Teljesen elemi úton ellenőrizhető, hogy a legfeljebb harmad rendű komplex Hadamard mátrixok azok ekvivalensek a megfelelő F_n Fourier-mátrixokkal. Némi megfontolás igényel ugyan, de hasonlóan könnyen

látható, hogy a négy dimenziós komplex Hadamard mátrixok az F_4-ből kiinduló egyparaméteres mátrixcsalád tagjaiként állnak elő. A jelölések ugyanazok, mint [82]-ben: a szabad paraméterek számát, ha ezt külön hangsúlyozni akarjuk, felső indexként jelöljük:

2.2.4. Példa. $F_1^{(0)} = H_1, F_2^{(0)} = H_2$, lásd az 1.1 példát.

$$F_3^{(0)} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix}, F_4^{(1)}(a) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \mathbf{i}e^{\mathbf{i}a} & -1 & -\mathbf{i}e^{\mathbf{i}a} \\ 1 & -1 & 1 & -1 \\ 1 & -\mathbf{i}e^{\mathbf{i}a} & -1 & \mathbf{i}e^{\mathbf{i}a} \end{bmatrix} \tag{2.1}$$

Itt $\omega = e^{\frac{2\pi\mathbf{i}}{3}}$, a komplex harmadik egységgyök.

A komplex Hadamard mátrixok osztályozásában fontos szerepet játszik az alábbi, a TZ-katalógusban [82]-ban bevezetett fogalom:

2.2.5. Definíció. Egy normalizált $n \times n$-es komplex Hadmard mátrix izolált, ha van olyan környezete amelyben rajta kívül nincs másik normalizált Hadamard mátrix.

2.2.6. Definíció. Legyen H egy paraméterezett komplex Hadamard mátrix. Ekkor H orbitján, vagy másként a H-ból kiinduló mátrixcsaládon azon mátrixok összességét értjük, amelyek a H-ban lévő szabad paraméterek értékadásait követően adódnak.

2.2.7. Definíció. Egy paraméterezett komplex Hadamard mátrix orbitja affin, ha az elemek fázisa a paramétereknek lineáris függvénye. Egy orbit maximálisan affin, ha további affin paraméterekkel nem bővíthető.

Az előző definíciók tükrében tehát $F_1^{(0)}, F_2^{(0)}$ és $F_3^{(0)}$ azok izolált Hadamard mátrixok, míg $F_4^{(1)}(a)$ nem izolált, orbitja pedig a $\{F_4^{(1)}(a) : \ a \in [0, 2\pi)\}$ halmaz, mely természetesen affin. A 3. fejezet végén a 3.5.3 példa illusztrálja a nem-affin paraméteres mátrixcsaládokat.

1996-ban sikerült Haagerupnak igazolnia, hogy ekvivalencia erejéig csak az F_5 Fourier mátrix az egyedüli komplex Hadamard mátrix 5 dimenzióban [37]. Magasabb dimenziókban azonban meglehetősen elbonyolódik a helyzet: 6 dimenzióban például több, lokálisan inekvivalens paraméteres család is található, lásd [82]. Beauchamp és Nicoara nemrégiben megjelent cikke [4] leírja az önadjungált 6×6-os komplex Hadamard mátrixokat, szintén egy érdekes, nem-affin orbitot prezentálva. Sajnos azonban még mindig nem tudni, hogy van-e további ismeretlen család ebben a dimenzióban.

Petrescu PhD dolgozatában igazolta az alábbi struktúratételt, példát mutatva ezáltal végtelen sok izolált komplex Hadamard mátrixra.

2.2.8. Tétel (Petrescu, [64]). *Ha p prím, akkor F_p izolált komplex Hadamard mátrix.*

5. *Megjegyzés.* Petrescu tétele korántsem jelenti azt, hogy prímdimenzióban ne lennének paraméteres családok, mint erre ő maga is rámutatott: $7, 13, 19, 31$ és 79 dimenziókban algebrai megfontolások és számítógép segítségével sikeresen konstruált legalább 1-paraméteres komplex Hadamard mátrix családokat. Állítása mindössze annyit jelent, hogy maguk az F_p mátrixok nem paraméterezhetők. Munkáját később Nicoara általánosította, aki elméleti úton adott magyarázatot a számítógéppel megtalált mátrixok létére [59].

6. *Megjegyzés.* Jelenleg nem ismert, hogy 11 dimenzióban van-e paraméteres Hadamard mátrixcsalád, vagy minden 11 dimenziós Hadamard mátrix izolált [82].

Látható, hogy még kis dimenziókban is rendkívül sokféle Hadamard mátrix lelhető fel, több közülük paraméteres családokat indukál. Az alábbi két példával szeretnénk azt megvilágítani hogy nem minden paraméter, ami annak látszik:

2.2.9. Példa.

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ e^{\mathbf{i}t} & e^{\mathbf{i}t} & -e^{\mathbf{i}t} & -e^{\mathbf{i}t} \\ 1 & -1 & -1 & 1 \end{bmatrix}, F_4^{(1)}(a) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \mathbf{i}e^{\mathbf{i}a} & -1 & -\mathbf{i}e^{\mathbf{i}a} \\ 1 & -1 & 1 & -1 \\ 1 & -\mathbf{i}e^{\mathbf{i}a} & 1 & \mathbf{i}e^{\mathbf{i}a} \end{bmatrix} \tag{2.2}$$

H_4 formálisan egyparaméteres 4×4-es Hadamard családnak tűnik, viszont látható, hogy a harmadik sorát $e^{-\mathbf{i}t}$-vel megszorozva a „mátrixcsalád" minden tagja ekvivalens azzal a mátrixszal, amelyet eleve $t = 0$ helyettesítéskor kapunk. Feltehető tehát, hogy egy paraméteres mátrixcsalád minden tagja normalizált. Sokkal érdekesebb a másik F_4 mátrix, amelyben a-t a $[0, \pi)$ intervallumon variálva egymással inekvivalens mátrixok jönnek ki. Hogy ez miért van így, arról szól a következő, igen fontos eredmény.

2.2.10. Lemma (Haagerup, [37])**.** *Legyen H tetszőleges komplex Hadamard mátrix. Tekintsük a hozzá tartozó $\Lambda_H := \{h_{ij}h_{kl}\overline{h}_{kj}\overline{h}_{il}\}$ halmazt. Ez a halmaz invariáns a $\cong$ ekvivalenciára nézve.*

2.2.11. Következmény ([37], Haagerup)**.** *Ha két komplex Hadamard mátrix különböző Λ-invariáns halmazzal rendelkezik, akkor nem lehetnek ekvivalensek.*

7. *Megjegyzés.* A fenti 2.2.10 lemma megfordítása nem érvényes. Minden valós H Hadamard mátrix esetén $\Lambda_H = \{-1, 1\}$, ugyanakkor vannak inekvivalens Hadamard mátrixok 16 dimenzióban.

A következőkben rátérünk a komplex Hadamard mátrixok konstrukciójára.

2.3. Komplex Hadamard mátrixok konsrtukciója

Az alábbiakban ismertetjük a komplex elemű Hadamard mátrixokra vonatkozó három legáltalánosabb konstrukciót. Az első lehetőség a valós Hadmard mátrixok egy természetes általánosításából adódik, nevezetesen egységgyökök segítségével próbálunk Hadamard mátrixokat konstruálni. A valós Hadamard mátrixok további általánosításaként lehet többdimenziós, $n \times n \times \ldots \times n$-es ortogonális mátrixokat is vizsgálni, erről további információkat az érdeklődő Olvasó Agaian monográfiájában talál [1], míg egy harmadik általánosításként a kvaternió elemű Hadamard mátrixokról Chterental és Đoković [14] cikkében lehet olvasni.

A teljesség kedvéért álljon itt az 1.3.3 lemma komplex változata.

2.3.1. Lemma. *Ha H egy komplex Hadamard mátrix, akkor $\overline{H}$ és H^* is komplex Hadamard.*

2.3.1. Butson Hadamard mátrixok

A talán legkézenfekvőbb dolog komplex Hadamard mátrixokat komplex egységgyökök segítségével konstruálni: Erre vonatkozóan Butson vezette be a $H(q,n)$ jelölést azon n-ed rendű Hadamard mátrixokra, amelyek minden eleme q-adik egységgyök. Ezzel az írásmóddal $H(2,n)$ az n-ed rendű valós, míg $H(4,n)$ az n-ed rendű $\{\pm 1, \pm \mathbf{i}\}$ elemkből álló komplex Hadamard mátrixokat jelöli [12]. A komplex Hadamard mátrixokra úgyis tekinthetünk tehát, mint a $H(\infty,n)$ halmazra.

Néhány szórványos negatív eredménytől eltekintve nem sokat tudni a Butson Hadamard mátrixok létezéséről. Butson maga bizonyított egy szükséges feltételt [12] a létezésre abban az esetben, ha $m = p^a$ prímhatvány. Később ezt Winterhof [89] általánosította, majd egy negatív feltételt prezentált. Ennek egy speciális esetét igazolta tőle függetlenül de Launey [15]. A főbb eredményeket összegzi az alábbi

2.3.2. Lemma. 1. *Ha p prím, és létezik egy $H(p^a,n)$, akkor $n = pt$ valamilyen pozitív egész t-re, [89].*

2. *Ha p prím, akkor létezik $H(p, 2^j p^k)$ minden $0 \leq j \leq k$ esetén [12].*

3. *Ha $p \equiv 3 \mod 4$ prím, $n = p^b r^2 s$ páratlan, s négyzetmentes, továbbá $(s,p) = 1$, és van olyan q prím, melyre $q \mid s$ és $\left(\frac{q}{p}\right) = -1$, akkor sem $H(p^a,n)$, sem pedig $H(2p^a,n)$ nem létezik [89].*

Az 1.2.5 lemma miatt világos, hogy egy Butson $H(q,n)$ típusú Hadamard mátrix létezésének egy szükséges feltétele az, hogy legyen n olyan komplex egységgyök, melyek összege 0. Lam és Leung [55], illetve sokkal általánosabban és más kontextusban

Coppersmith és Steinberger is éppen ezt a problémát vizsgálta [18], és tulajdonképpen az alábbi eredményre jutott:

2.3.3. Tétel (Lam–Leung, [55]). *Minden $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ esetén akkor és csak akkor van n olyan komplex m-edik egységgyök, melyek összege 0, ha $n \in \mathbb{N}p_1 + \mathbb{N}p_2 + \ldots + \mathbb{N}p_r$.*

Most lássuk a pragmatikus Agaian–Moorhouse–Tao mátrixot [1], [57], [84].

2.3.4. Példa. Az alábbi $S_6^{(0)}$ mátrix egy szimmetrikus Butson $H(3,6)$ típusú mátrix, mely az egyetlen ma ismert 6×6-os izolált komplex Hadamard mátrix. $S_6^{(0)}$ központi szerepet játszott a Fields medálos Terrence Tao egy eredményében is, melyben a Fuglede sejtés [34] egyik irányát cáfolta. A másik irányt Kolountzakis és Matolcsi támadták sikerrel [53]. A probléma érdekessége, hogy a Fuglede sejtés egy tisztán analízisbeli probléma, Tao mégis egy látványos diszkretizáció, majd H_{12} illetve $S_6^{(0)}$ felhasználásával ért el sikereket.

$$S_6^{(0)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & \omega & \omega & \omega^2 & \omega^2 \\ 1 & \omega & 1 & \omega^2 & \omega^2 & \omega \\ 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^2 & \omega & 1 & \omega \\ 1 & \omega^2 & \omega & \omega^2 & \omega & 1 \end{bmatrix} \tag{2.3}$$

Butson-típusú mátrixok különféle spektrálhalmaz- illetve parkettázó konstrukciókból is származhatnak, mint erre Matolcsi Máté és Réffy Júlia egy eredménye rámutat. Ők új, nem-Diţă-szerű mátrixokat mutattak egy [53]-ból illetve [78]-ból vett konstrukció segítségével $8, 12$ és 16 dimenziókban, ezáltal kiegészítve a TZ-katalógust. Az alábbi S_8 mátrix egy 4-paraméteres folytonos mátrixcsaládot indukál, amelyet egymástól függetlenül W. Tadej és a szerző is felfedezett. Mindezekről bővebben [56]-ban lehet olvasni.

2.3.5. Példa. Az alábbi $H(4,8)$ mátrixot Matolcsi Máté és Réffy Júlia konstruálta parkettázó- és spektrálhalmazok vizsgálatakor.

$$S_8 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & \mathbf{i} & -\mathbf{i} & 1 & -1 & \mathbf{i} & -\mathbf{i} \\ 1 & -1 & -\mathbf{i} & \mathbf{i} & 1 & -1 & -\mathbf{i} & \mathbf{i} \\ 1 & 1 & -1 & -1 & \mathbf{i} & \mathbf{i} & -\mathbf{i} & -\mathbf{i} \\ 1 & \mathbf{i} & 1 & \mathbf{i} & -1 & -\mathbf{i} & -1 & -\mathbf{i} \\ 1 & -\mathbf{i} & 1 & -\mathbf{i} & -1 & \mathbf{i} & -1 & \mathbf{i} \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & -1 & -1 & -\mathbf{i} & -\mathbf{i} & \mathbf{i} & \mathbf{i} \end{bmatrix} \tag{2.4}$$

A negyedik egységgyökökből álló Butson típusú mátrixokkal kapcsolatosan egy fontos sejtést említünk a 2.4 szakaszban. További példák Butson Hadamard mátrixokra a 3.5 fejezetben találhatók.

2.3.2. A Diţă konstrukció

Diţă most következő, valósakból átvett [42] konstrukciója azt mutatja, hogy összetett dimenzióban mindig vannak paraméteres Hadamard mátrix családok:

2.3.6. Tétel (Diţă, [28]). *Ha az M és $N_i, i = 1, 2, \ldots, k$ $k \times k$-as illetve $n \times n$-es mátrixok mindannyian Hadamard mátrixok, akkor a következő kn dimenziós Q mátrix is az:*

$$Q = \begin{bmatrix} m_{11}N_1 & . & . & m_{1k}N_k \\ . & . & . & . \\ . & . & . & . \\ m_{k1}N_1 & . & . & m_{kk}N_k \end{bmatrix} \tag{2.5}$$

2.3.7. Definíció. Egy komplex Hadamard mátrixot Diţă-szerűnek nevezünk, ha ekvivalens egy olyan mátrixszal, amely a (2.5) formulából származik.

A Diţă-konstrukció segítségével tehát kisebb dimenziójú Hadamard mátrixokból magasabb dimenziójú mátrixokat lehet készíteni. A konstrukció igazi erejét azonban az adja, hogy így lehetőség van paraméteres Hadamard mátrixoknak a megépítésére. Az eljárás nagyon egyszerű: ha az előző tételben szereplő $N_i, i > 1$ mátrixok $j > 1$-dik sorait végigszorozzuk egy tetszőleges egységnyi abszolút értékű számmal, akkor az így adódó N_i' mátrixok változatlanul komplex Hadamard mátrixok maradnak, tehát az alábbi Q_8 egy paraméteres komplex Hadamard mátrix családot indukál.

2.3.8. Példa. Jelölje $D(.)$ a diagonális mátrixot, és legyen

$$M = F_2, N_1 = F_4(a), N_2 = D(1, e^{\mathrm{i}b}, e^{\mathrm{i}c}, e^{\mathrm{i}d})F_4(e) \tag{2.6}$$

Ekkor

$$Q_8^{(5)}(a,b,c,d,e) = \left[\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \mathbf{ie}^{\mathrm{i}a} & -1 & -\mathbf{ie}^{\mathrm{i}a} & \mathbf{e}^{\mathrm{i}b} & \mathbf{ie}^{\mathrm{i}(e+b)} & -\mathbf{e}^{\mathrm{i}b} & -\mathbf{ie}^{\mathrm{i}(e+b)} \\ 1 & -1 & 1 & -1 & \mathbf{e}^{\mathrm{i}c} & -\mathbf{e}^{\mathrm{i}c} & \mathbf{e}^{\mathrm{i}c} & -\mathbf{e}^{\mathrm{i}c} \\ 1 & -\mathbf{ie}^{\mathrm{i}a} & -1 & \mathbf{ie}^{\mathrm{i}a} & \mathbf{e}^{\mathrm{i}d} & -\mathbf{ie}^{\mathrm{i}(e+d)} & -\mathbf{e}^{\mathrm{i}d} & \mathbf{ie}^{\mathrm{i}(e+d)} \\ \hline 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & \mathbf{ie}^{\mathrm{i}a} & -1 & -\mathbf{ie}^{\mathrm{i}a} & -\mathbf{e}^{\mathrm{i}b} & -\mathbf{ie}^{\mathrm{i}(e+b)} & \mathbf{e}^{\mathrm{i}b} & \mathbf{ie}^{\mathrm{i}(e+b)} \\ 1 & -1 & 1 & -1 & -\mathbf{e}^{\mathrm{i}c} & \mathbf{e}^{\mathrm{i}c} & -\mathbf{e}^{\mathrm{i}c} & \mathbf{e}^{\mathrm{i}c} \\ 1 & -\mathbf{ie}^{\mathrm{i}a} & -1 & \mathbf{ie}^{\mathrm{i}a} & -\mathbf{e}^{\mathrm{i}d} & \mathbf{ie}^{\mathrm{i}(e+d)} & \mathbf{e}^{\mathrm{i}d} & -\mathbf{ie}^{\mathrm{i}(e+d)} \end{array}\right] \tag{2.7}$$

egy 5 paraméteres komplex Hadamard mátrix.

Ez alapján kimondható a következő

2.3.9. Lemma (Diţă, [28]). *Ha M illetve $N_i, i = 1, \ldots, k$ rendre $k \times k$ illetve $n \times n$-es komplex Hadamard mátrixok, amelyek rendre m_1 illetve $n_i, i = 1, \ldots, k$ paramétertől függenek akkor a (2.5) formula segítségével definiált nk rendű Q mátrix az*

$$m_1 + (n-1)(k-1) + \sum_{i=1}^{k} n_i \tag{2.8}$$

paraméteres családot indukál.

Összetett dimenziókban tehát garantáltan vannak paraméteres Hadamard mátrix családok, sőt a Diţă konstrukció mutatja, hogy szemben a 2.2.8 tétellel összetett n-re az F_n Fourier mátrix mindig paraméteres családokat indukál.

2.3.3. Ciklikus komplex Hadamard mátrixok

Most egy másik általános módszert ismertetünk komplex Hadamard mátrixok konstrukciójára. Az elképzelés az, hogy speciális alakú, ciklikus formában megadott komplex Hadamard mátrixokat próbálunk keresni. A szekcióban a Haagerup dolgozatában leírtakat közöljük [37].

Legyen $n \geq 2$, és jelölje $\mathbb{Z}_n^*$ az egész számok $\mathbb{Z}_n$ gyűrűjének invertálható elemeit. Egy $(\alpha, \beta) \in \mathbb{Z}_n^* \times \mathbb{Z}_n$ párra tekintsük a következő $\mathbb{Z}_n$-en értelmezett $x^{(\alpha,\beta)}$ függvényt, melynek j helyen felvett $x_j^{(\alpha,\beta)}$ értéke a következő:

$$x_j^{(\alpha,\beta)} = \begin{cases} \exp\left(\frac{2\pi \mathbf{i}}{n}\left(\frac{\alpha j^2}{2} + \beta j\right)\right) & \text{ha } j \in \mathbb{Z}_n,\ n \text{ páros} \\ \exp\left(\frac{2\pi \mathbf{i}}{n}\left(\frac{\alpha j(j-1)}{2} + \beta j\right)\right) & \text{ha } j \in \mathbb{Z}_n,\ n \text{ páratlan} \end{cases} \tag{2.9}$$

Ekkor természetesen $|x_j| = 1, j \in \mathbb{Z}_n$, és könnyű ellenőrizni, hogy

2.3.10. Lemma. *Az $U = \left(\frac{1}{\sqrt{n}} x_{i-j}\right)_{i,j \in \mathbb{Z}_n}$ ciklikus mátrix unitér.*

$$\sum_{j \in \mathbb{Z}_n} x_j \overline{x}_{j+k} = \begin{cases} n & \text{ha } k = 0 \pmod{n} \\ 0 & \text{ha } k \neq 0 \pmod{n} \end{cases} \tag{2.10}$$

Más szóval az x olyan egységnyi abszolút értékű elemekből álló vektor, melynek $\hat{x}$ Fourier transzformáltját is egységnyi abszolút értékű elemek alkotják: $|x_j| = |\hat{x}_j| = 1, j \in \mathbb{Z}_n$. Az U mátrixot sztenderd biunitér mátrixnak nevezzük.

1983-ban Enflo azt a kérdést vetette fel, hogy valamely p prím esetén a

$$cx^{(\alpha,\beta)}, (c, \alpha, \beta) \in \mathbb{T} \times \mathbb{Z}_p^* \times \mathbb{Z}_p \tag{2.11}$$

alakú $x : \mathbb{Z}_p \to \mathbb{C}$ függvények az egyetlenek, amelyekre mind x-nek, mind $\hat{x}$-nak egységnyi abszolút értékűek az elemei? Enflo azt sejtette, hogy a kérdésre a válasz igenlő. Björck átfogalmazta a (2.10) egyenletet, és a $z_j = \frac{x_{j+1}}{x_j}$ változótranszformációval az alábbi n egyenlethez jutott [7]:

$$\begin{cases} z_0 + z_1 + z_2 + \ldots + z_{n-1} = 0 \\ z_0z_1 + z_1z_2 + \ldots + z_{n-1}z_0 = 0 \\ \vdots \\ z_0z_1 \ldots z_{n-2} + z_1z_2 \ldots z_{n-1} + \ldots + z_{n-1}z_1 \ldots z_{n-3} = 0 \\ z_0z_1 \ldots z_{n-1} = 1 \end{cases} \tag{2.12}$$

Megjegyezzük, hogy a fenti egyenletrendszer általános tagja csak egy n tagú ciklikus összeg, amely általában *nem* elemi szimmetrikus polinom.

2.3.11. Definíció. A (2.12) egyenletrendszer valamely $z = (z_0, z_1, \ldots, z_{n-1})$ megoldását ciklikus n-dik gyöknek (cyclic n-root) nevezzük.

2.3.12. Definíció. A (2.9) által definiált (transzformálandó) megoldások a klasszikus cyclic n-rootok.

Világos, hogy az egységnyi abszolút értékű cyclic n-rootok egyúttal Enflo unitér problémájára is megoldást szolgáltatnak. $n = 2, 3$-ra az egyenleteket triviális megoldani. $n = 4$-re végtelen sok megoldás, valójában a teljes $F_4^{(1)}(a)$ család adódik. Sőt, mint arra Backelin rámutat: nem négyzetmentes n-re mindig van végtelen sok megoldás [2].

2.3.13. Lemma (Backelin, [2])**.** *Ha m^2 osztja n-t, akkor a cyclic n-root megoldáshalmaz legalább $m-1$ dimenziós.*

Az egyenleteket $n = 5$-re Lovász, majd később Björck és Fröberg [9], végül Haagerup [37] oldotta meg, és így igazolta, hogy annak az egységnyi abszolút értékű megoldásai kizárólag a klasszikus cyclic 5-rootok. $n = 6$-ra a klasszikus megoldás mellett van egy attól lényegesen különböző is, amely a C_6 mátrixot generálja [82]. Björck egy általános megoldása alapján $p \geq 7$ prímre a klasszikus cyclic n-root megoldásokon kívül további egységnyi abszolút értékűek konstruálhatók [8], így Enflo sejtése általánosságban nem igaz. Björck eredeti konstrukcióját később egymástól függetlenül Munemasa és Watatani [58], valamint de la Harpe és Jones [23] is felfedezte. Valójában mindhárom cikkben az $x : \mathbb{Z}_p \to \mathbb{T}$ az alábbi alakot ölti:

$$x_j = \begin{cases} 1 & j = 0 \pmod p \\ \alpha & j \neq 0,\ j \ \text{ kvadratikus maradék } \pmod p \\ \beta & j \neq 0,\ j \ \text{ kvadratikus nemmaradék } \pmod p, \end{cases} \tag{2.13}$$

ahol α és β értéke úgy van megválasztva, hogy mind x, mind pedig $\hat{x}$ egységnyi abszolút értékű elemekből álljon, másszóval a $\frac{1}{\sqrt{p}}\left[x_{j-k}\right]_{j,k,\in\mathbb{Z}_p}$ mátrix unitér legyen. A következő definíció bemutatja a cyclic-n-root mátrixok egy fontos osztályát.

2.3.14. Definíció. A fenti, (2.13) összefüggéssel definiált ciklikus komplex Hadamard mátrixokat 2-indexű cyclic n-root mátrixoknak nevezzük.

A 2-indexű cyclic n-roots mátrixokat egy kicsit bővebben a 3. fejezetben tárgyaljuk.

8. *Megjegyzés.* A „2-indexű" elnevezés onnan származik, hogy p prím esetén a kvadratikus maradékok egy 2-indexű részcsoportját alkotják $\mathbb{Z}_p^*$-nak, és α és β úgy van definiálva, hogy az x vektor x_j koordinátái ezen részcsoport mellékosztályain konstans értéket vegyenek fel. Ha $p \equiv 1 \pmod 6$ prím, akkor a köbös maradékok egy 3-indexű részcsoportot fognak alkotni, és a (2.13) összefüggés értelemszerű módosításával ilyenkor is komplex Hadamard mátrixokat lehet konstruálni. A 3-indexű cyclic n-rootok teljes klasszifikációját 12 év munkát követően Björck és Haagerup 2008 áprilisában publikálta [10].

2.3.15. Példa. Ha $n = 7$, akkor a fenti egyenleteket Gröbner-bázisok [11] segítségével meg lehet oldani, és a klasszikus megoldások mellett nemklasszikus, 2-indexű illetve 3-indexű megoldások is vannak. Mi a 2-indexű megoldásokból származó Hadamard-mátrixokat, a C_{7A} és a konjugáltját, C_{7B}-t prezentáljuk. Az $n = 7$ eset részletes tárgyalása és a további megoldások [3]-ban találhatóak.

$$C_{7A}, C_{7B} = \begin{bmatrix} 1 & c & c & 1 & c & 1 & 1 \\ 1 & 1 & c & c & 1 & c & 1 \\ 1 & 1 & 1 & c & c & 1 & c \\ c & 1 & 1 & 1 & c & c & 1 \\ 1 & c & 1 & 1 & 1 & c & c \\ c & 1 & c & 1 & 1 & 1 & c \\ c & c & 1 & c & 1 & 1 & 1 \end{bmatrix}, c = -\frac{3}{4} \pm \mathbf{i}\frac{\sqrt{7}}{4} \tag{2.14}$$

Backelin már ismertetett eredménye alapján $n = 8$-ra és $n = 9$-re végtelen sok cyclic n-root van. Előbbit még Björck és Fröberg osztályozta 1992-ben, míg utóbbit Faugère egy teljesen új komputer algebrai csomag megírásával nagyjából tíz évvel később, 2001-ben karakterizálta [32]. A cyclic 10-rootok karakterizálásához nélkülözhetetlen Gröbner bázisoknak első ízben történő előállítása is az ő nevéhez fűződik [33]. $n \geq 11$-től csak részeredmények ismertek [70].

A szekciót egy Haageruptól származó végességi eredménnyel zárjuk.

2.3.16. Tétel (Haagerup, [36])**.** *Ha p prím, akkor multiplicitással együtt $\binom{2p-2}{p-1}$ cyclic p-root van. Speciálisan: a p prímszámrendű, 1 fődiagonálisú ciklikus komplex Hadamard mátrixok száma legfeljebb $\binom{2p-2}{p-1}$.*

2.4. Komplex Hadamard- és konferencia mátrixok

2006 elején jelent meg egy monumentális – több mint 50 oldalas – cikk, amelyben két lengyel fizikus, W. Tadej és K. Życzkowski próbált meg átfogó képet adni a komplex Hadamard mátrixokról, és sok érdekes eredmény mellett felsorolták az általuk ismert *összes* komplex Hadamard mátrixot 16 dimenzióig bezárólag. Erre a katalógusra a továbbiakban [82] helyett TZ-katalógusként fogunk hivatkozni. A katalógusban bemutatott mátrixok egyrészt igen sokfélék, hiszen szerzői paraméteres családokat mutatnak be, másfelől bizony hiányos, mint ahogyan arra Matolcsi Máté és Réffy Júlia munkája rámutat: egy, az [53]-ban szereplőhöz hasonló spektrálhalmaz-konstrukció segítségével új, a katalógusban nem szereplő mátrixokat készítettek $8, 12$ és 16 dimenzióban, mely mátrixok paraméterezését a szerző végezte el [56]. A közös munka rendkívül gyümölcsöző volt: számos itt felsorolt új eredmény alapgondolata ekkor született meg. Hangsúlyozni szeretnénk azonban, hogy ez a dolgozat pusztán *felhasználja* az [56]-ban közölt közös eredményeket, és valójában az egyénileg készített, [81]-ben szereplő új, teljesen önálló eredményeket tartalmazza. Az önálló kutatás megkezdéséhez szükségünk volt egy ötletre, amely a következő sejtést látva fogant meg:

2.4.1. Sejtés ([71], Seberry)**.** *Minden páros dimenzióban van Butson-típusú $H(4, N)$, azaz $\{\pm 1, \pm \boldsymbol{i}\}$ elemekből álló komplex Hadamard mátrix.*

9. *Megjegyzés.* Világos, hogy ilyen mátrixokat nem remélhetünk páratlan dimenziókban a 1.2.5 következmény miatt, és az is érvényes, hogy amennyiben ez a sejtés igaz, akkor az Hadamard-sejtés is az [71].

A kutatás megkezdését az motiválta, hogy a TZ-katalógusban nem szerepelt explicite a fenti 2.4.1 sejtésnek megfelelő $H(4, N)$ mátrix 10 és 14 dimenzióban. Persze nem zárhattuk ki azt a lehetőséget, hogy esetleg valamelyik ottani paraméteres családban ezek már szerepelnek, viszont ez már 6 dimenzióban sem igaz, ahol az $F_6^{(2)}$ és $D_6^{(1)}$ mátrixcsaládok eltérőek, lévén nem egyforma számú affin paraméterük van [82]. A tény, hogy ezen mátrixcsaládok már 6 dimenzióban is különbözőek mindenképpen azt sugallta, hogy érdemes magasabb dimenziókban is körülnézni, és megpróbálni a 2.4.1 sejtésnek megfelelő Hadamard mátrixokat konstruálni. A kiindulási cél tehát az volt, hogy valahogyan mutassunk 10 és 14 dimenziós $H(4, N)$ mátrixokat.

2.4.1. A diszkrét modell: Butson $H(4, N)$ Hadamard mátrixok keresése

Az $N = 8, 12$ és $N = 16$ dimenziós mátrixokkal első körben nem foglalkoztunk, mert egyrészt az [56]-ban szereplő S_8 mátrix az pont egy $H(4, 8)$ típusú Hadamard mátrix

volt, másrészt ezek azok a dimenziók, ahol még valós Hadamard családok is vannak, és előfordulhat, hogy egy általunk újnak vélt $H(4,N)$ mátrix az valójában benne van valamely N-ed rendű valós Hadamard mátrix orbitjában. Az első érdekes dimenzió az $N = 10$ volt. Egyrészt nincs 10-ed rendű valós Hadamard mátrix, másrészt a TZ-katalógusban kizárólag az F_{10} paraméterezett Fourier-mátrix szerepelt, amiről heurisztikusan azt gondolja az ember, hogy - lévén az tele van 10-ik gyökökkel - nem lehet beforgatni egy $H(4,10)$ mátrixba.

A keresés a következőképpen zajlott: mivel a mátrix első sora választható a csupaegy vektornak, a normalizálás miatt pedig feltehető, hogy az összes többi sorok 1-gyel kezdődnek, azt kaptuk, hogy a mátrix második sora - ekvivalencia erejéig - már csak az alábbi 5-féle sorvektor valamelyike lehet. Ellenkező esetben ugyanis bármilyen, az 1.2.5 következmény miatti zérus elemösszegű sorvektort oszloppermutáció révén az alábbi 5 alak valamelyikére hozhatjuk:

$$s_1 = [1,1,1,1,1,-1,-1,-1,-1,-1]\,, s_2 = [1,1,1,1,\mathbf{i},-\mathbf{i},-1,-1,-1,-1] \tag{2.15}$$

$$s_3 = [1,1,1,\mathbf{i},\mathbf{i},-\mathbf{i},-\mathbf{i},-1,-1,-1]\,, s_4 = [1,1,\mathbf{i},\mathbf{i},\mathbf{i},-\mathbf{i},-\mathbf{i},-\mathbf{i},-1,-1] \tag{2.16}$$

$$s_5 = [1,\mathbf{i},\mathbf{i},\mathbf{i},\mathbf{i},-\mathbf{i},-\mathbf{i},-\mathbf{i},-\mathbf{i},-1] \tag{2.17}$$

Nyilván az ember úgy folytatná a keresést, hogy legenerálja a fenti sorvektorok összes olyan 1-essel kezdődő permutációját, amely merőleges a fenti 5 sorvektor valamelyikére, ezáltal elkészítvén olyan sorpárokat, amelyek merőlegesek egymásra. Ezt követően teljesen hasonlóan páronként merőleges sorhármasokat csinálna, stb. Ez a módszer azonban már 10 dimenzióban is kivitelezhetetlen. Könnyen látszik ugyan, hogy az s_1 sorvektorra semmilyen másik $\{\pm 1, \pm\mathbf{i}\}$ sorvektor nem lesz merőleges, azonban ezt elhagyván a megmaradó négy $s_i, i = 2,\ldots,5$ sorvektoroknak 15750 különböző 1-gyel kezdődő permutációja létezik, ezek közül 6912 olyan, amely az $s_i, i = 2,\ldots,5$ sorvektorok valamelyikével merőleges sorpárt alkot. Az ezekre merőleges 3-asok pedig már kezelhetetlenül sokan vannak.

Megpróbáltuk ezt a dolgot megkerülni, és egyedül azt néztük, hogy valamely rögzített i-re a fenti s_i sorvektornak hány olyan 1-gyel kezdődő permutációja van, amelyek páronként merőlegesek egymásra. Heurisztikusan úgy gondoltuk, hogy érdemes a legkevesebb permutációval rendelkező sorvektort nézegetni, hiszen ez lesz az, amely még számítógéppel követhető esetszámot generál: ez a sorvektor az s_5. Meglepő eredmény született. Gyakorlatilag kimerítő kereséssel sikerült 9 páronként ortogonális sorvektort csinálni, ami a csupaegy sorral együtt egy 10 dimenziós komplex Hadamard mátrixot eredményez. Így készült el az alábbi, D_{10}-zel jelölt mátrix [81].

$$D_{10} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -\mathbf{i} & -\mathbf{i} & -\mathbf{i} & -\mathbf{i} & \mathbf{i} & \mathbf{i} & \mathbf{i} & \mathbf{i} \\ 1 & -\mathbf{i} & -1 & -\mathbf{i} & \mathbf{i} & \mathbf{i} & -\mathbf{i} & -\mathbf{i} & \mathbf{i} & \mathbf{i} \\ 1 & -\mathbf{i} & -\mathbf{i} & -1 & \mathbf{i} & \mathbf{i} & \mathbf{i} & \mathbf{i} & -\mathbf{i} & -\mathbf{i} \\ 1 & -\mathbf{i} & \mathbf{i} & \mathbf{i} & -1 & -\mathbf{i} & -\mathbf{i} & \mathbf{i} & -\mathbf{i} & \mathbf{i} \\ 1 & -\mathbf{i} & \mathbf{i} & \mathbf{i} & -\mathbf{i} & -1 & \mathbf{i} & -\mathbf{i} & \mathbf{i} & -\mathbf{i} \\ 1 & \mathbf{i} & -\mathbf{i} & \mathbf{i} & -\mathbf{i} & \mathbf{i} & -1 & -\mathbf{i} & -\mathbf{i} & \mathbf{i} \\ 1 & \mathbf{i} & -\mathbf{i} & \mathbf{i} & \mathbf{i} & -\mathbf{i} & -\mathbf{i} & -1 & \mathbf{i} & -\mathbf{i} \\ 1 & \mathbf{i} & \mathbf{i} & -\mathbf{i} & -\mathbf{i} & \mathbf{i} & -\mathbf{i} & \mathbf{i} & -1 & -\mathbf{i} \\ 1 & \mathbf{i} & \mathbf{i} & -\mathbf{i} & \mathbf{i} & -\mathbf{i} & \mathbf{i} & -\mathbf{i} & -\mathbf{i} & -1 \end{bmatrix} \tag{2.18}$$

Nagyon vázlatosan a program, amelyet a *Mathematica* programcsomagban implementáltunk a következőképpen nézett ki: sorra definiáltunk olyan A_k ($k \geq 2$) tömböket, amelyek minden eleme $k-1$ páronként ortogonális sorvektor. Kezdetben minden A_k üres, $A[i]$ az A halmaz i-edik elemét, míg $\#A$ az A halmaz elemszámát jelöli.

A program egy pszeudo-kódja:

Legyen $A_1 = \{s_5\}$
Legyen $\Omega = \{s_5$ 1-gyel kezdődő permutációi$\}$
For i from 1 to $\#\Omega$
    Ha $\Omega[i]$ merőleges s_5-re, akkor $A_2 = A_2 \cup \Omega[i]$
$i++$
For k from 2 to 9
    For i from 1 to $\#A_2$
        For j from 1 to $\#A_k$
            Ha $A_2[i]$ merőleges $A_k[j]$-nek mind a $k-1$ elemére, akkor
             $A_{k+1} = A_{k+1} \cup \{A_k[j], A_2[i]\}$
        $j++$
    $i++$
    Ha A_k-nak van két olyan x és y eleme, hogy az $A_k[x]$ illetve $A_k[y]$
     elemekhez tartozó $k-1$ sorvektor csupán sorrendben különbözik
     egymástól, akkor A_k-ból $A_k[x]$-et dobjuk ki.
    Ha $\#A_k$ még így is nagy, akkor dobjunk el belőle annyit,
     hogy kezelhető méretű maradjon.
$k++$
Ha A_9 üres, akkor kezdjük elölről az egészet, egyébként KÉSZ.

10. *Megjegyzés.* A fenti program egyetlen nemvilágos részt tartalmaz, mégpedig azt, hogy miért lehet ad hoc módon az A_k elemszámát csökkenteni, ha már az nagyon fel-

fújódna. A háttérben az áll, hogy amennyiben van egyetlen Hadamard mátrix, amit a fenti eljárás megtalál, akkor nagyon sok ilyen is van: a sorok és oszlopok permutálgatását követően számtalan egymással ekvivalens Hadamard mátrixot lehet csinálni. Amikor A_k-ból kidobálunk elemeket, akkor valójában csak annyi történik, hogy feltesszük, hogy a keresendő mátrix első $k+1$ sora éppen olyan alakra van permutálva, amilyen elemek az A_k-ban végül megmaradtak.

A fentihez teljesen hasonló eljárással sikerült még ilyen Hadamard mátrixokat 14 és 18 dimenzióban is konstruálni. Mivel a TZ-katalógus szempontjából csak a legfeljebb 16 dimenziósak az érdekesek, ezért itt csak D_{14}-et adjuk meg:

$$D_{14} = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & \mathrm{i} & -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} & \mathrm{i} \\
1 & \mathrm{i} & -1 & \mathrm{i} & -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} \\
1 & -\mathrm{i} & \mathrm{i} & -1 & \mathrm{i} & -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} & \mathrm{i} & \mathrm{i} \\
1 & \mathrm{i} & -\mathrm{i} & \mathrm{i} & -1 & \mathrm{i} & -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} & \mathrm{i} \\
1 & \mathrm{i} & \mathrm{i} & -\mathrm{i} & \mathrm{i} & -1 & \mathrm{i} & -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} \\
1 & -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} & \mathrm{i} & -1 & \mathrm{i} & -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} \\
1 & -\mathrm{i} & -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} & \mathrm{i} & -1 & \mathrm{i} & -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} & -\mathrm{i} \\
1 & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} & \mathrm{i} & -1 & \mathrm{i} & -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} \\
1 & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} & \mathrm{i} & -1 & \mathrm{i} & -\mathrm{i} & \mathrm{i} & \mathrm{i} \\
1 & \mathrm{i} & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} & \mathrm{i} & -1 & \mathrm{i} & -\mathrm{i} & \mathrm{i} \\
1 & \mathrm{i} & \mathrm{i} & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} & \mathrm{i} & -1 & \mathrm{i} & -\mathrm{i} \\
1 & -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} & \mathrm{i} & -1 & \mathrm{i} \\
1 & \mathrm{i} & -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} & -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} & \mathrm{i} & -1
\end{bmatrix} \tag{2.19}$$

2.4.2. A folyonos mátrixcsaládok: Paraméterezés 10 és 14 dimenzióban

Az előzőekben megtalált D_{10} és D_{14} mátrixokról azt sejtjük tehát, hogy nem szerepelnek a TZ-katalógusban. Nem állítjuk azonban azt, hogy ezek a mátrixok újak: egyáltalán nincs kizárva, hogy már valamelyik múlt századi kombinatorikus lapban leközölték őket, mint akkori új eredményt (valójában, mint azt később látni fogjuk, ez a helyzet). Az viszont garantált, hogy senki nem vizsgálta még meg, hogy miféle orbittal rendelkeznek, vagyis hogy indulnak-e ki paraméteres családok ezen $H(4,10)$ illetve $H(4,14)$ típusú mátrixokból. Ebben a fejezetben azt írjuk le, hogy miként konstruáltunk orbitot a D_{10} illetve a D_{14} mátrixoknak.

Egyáltalán nem világos az, hogy egy mátrixba hova, mely elemek helyére rakjunk be szabad paramétereket. Semmiféle általános eljárás, módszer nincs ilyenkor. A mi ötletünk a következő volt: tegyük fel, hogy egy mátrix az valamilyen módon paraméterezhető, esetleg több paramétere is van. Ekkor ha egyetlenegy szabad paraméter

mentén módosítjuk a kiindulási mátrixot de úgy, hogy az eredményül kapott mátrix még mindig ugyanolyan, $H(4,10)$ típusú, akkor van remény arra, hogy megtaláljuk a módosítandó elemeket. Hogyan? A korábban prezentált példákból, és a TZ-katalógus alapos áttanulmányozását követően az ember azt gondolja, hogy egy paraméter esetén a mátrix méretéhez képest viszonylag kevés elem változik meg. Ezért azt csináltuk, hogy rögzítettük a D_{10} első négy sorát, majd legeneráltuk az *összes* olyan normalizált $H(4,10)$ mátrixot, amelyik ezen 4 sor kiegészítésével volt kapható. Jelölje az így kapott mátrixok halmazát $\mathcal{H}$. Ebben a $\mathcal{H}$ halmazban nem túl sok, mindösszesen 11520 mátrix volt, ennyiféleképpen lehetett D_{10} első 4 sorát Hadamard mátrixszá kiegészíteni. Ezt követően sorra vettük az összes $H \in \mathcal{H}$ mátrixokra a $D_{10} - H$ különbség mátrixokat, és olyat kerestünk ezek között, amelyekben nagyon sok 0 szerepelt. Ez nyilván azt mutatta, hogy a két mátrix egymástól eltér ugyan, de csak viszonylag kevés helyen. Ezekre a helyekre pedig ad hoc megpróbáltunk paramétereket illeszteni. Az alábbiakban mutatunk egy konkrét $H \in \mathcal{H}$-ra vonatkozó $D_{10} - H$ mátrixot, továbbá megadjuk azt az R-rel jelölt perturbáló mátrixot, amely ez alapján D_{10}-et sejtésünknek megfelelően paraméterekkel látja el. Itt és a továbbiakban mindenütt $\bullet$-tal helyettesítettük a 0-kat R-ben:

$D_{10} - H =$

$$\begin{bmatrix}
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & -2\mathbf{i} & 2\mathbf{i} & -2\mathbf{i} & 2\mathbf{i} \\
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & 2\mathbf{i} & -2\mathbf{i} & 2\mathbf{i} & -2\mathbf{i} \\
\bullet & \bullet & \bullet & \bullet & -2\mathbf{i} & 2\mathbf{i} & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet & 2\mathbf{i} & -2\mathbf{i} & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet & -2\mathbf{i} & 2\mathbf{i} & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet & 2\mathbf{i} & -2\mathbf{i} & \bullet & \bullet & \bullet & \bullet
\end{bmatrix}, R_{D_{10}^{(1)}(t)} = \begin{bmatrix}
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & t & t & t & t \\
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & t & t & t & t \\
\bullet & \bullet & \bullet & \bullet & -t & -t & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet & -t & -t & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet & -t & -t & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet & -t & -t & \bullet & \bullet & \bullet & \bullet
\end{bmatrix} \tag{2.20}$$

2.4.2. Definíció. Az A és B $N \times N$-es mátrixok Hadamard-szorzatán azt az $A \circ B$-vel jelölt $N \times N$-es mátrixot értjük, amelyre $[A \circ B]_{i,j} = [A]_{i,j} \cdot [B]_{i,j}$ teljesül.

2.4.3. Definíció. Jelölje $\mathbf{EXP}(H)$ azt a mátrixot, amelyet H-ból úgy kapunk, hogy H minden elemét e-re emeljük: $[\mathbf{EXP}(H)]_{i,j} = e^{[H]_{i,j}}$. Hasonló módon legyen $\log(H)$ az a $\mod 1$ vett mátrix, amelyre $\mathbf{EXP}(2\pi\mathbf{i}\log(H)) = H$ teljesül.

Számítógéppel ellenőriztük, hogy érvényes a következő

2.4.4. Lemma $(*)$**.** *A* $D_{10}^{(1)}(t) = D_{10} \circ \boldsymbol{EXP}\left(\boldsymbol{i} \cdot R_{D_{10}^{(1)}}(t)\right)$ *egy egyparaméteres komplex Hadamard mátrix család.*

Az előzőekben tehát azt illusztráltuk hogyan paramétereztük be sikerrel a korábban megtalált D_{10} mátrixot. Megjegyezzük, hogy az itt mutatott egyparaméteres orbit további vizsgálatok segítségével 3-má bővíthető; mind ezt a $D_{10}^{(3)}$-at, mind a D_{14}-ből konstruált 6-paraméteres $D_{14}^{(6)}$ családot a fejezet végén prezentáljuk.

2.4.3. Konstrukció általában – A konferencia mátrixok

Mindenképpen figyelemre méltó az a tény, hogy mind D_{10} mind pedig a D_{14} mátrixok olyan speciális alakú komplex Hadamard mátrixok voltak, amelyeknek a magja az úgy nézett ki, hogy a főátló az csupa -1 volt, az összes többi elem pedig $\pm\mathbf{i}$. Ez motivált bennünket abban, hogy megpróbáljuk a D_N mátrixok struktúráját egy kicsivel jobban megismerni.

Ha elhagyjuk D_N első sorát és oszlopát, és csakis a magra koncentrálunk, akkor a következőt kapjuk: olyan Q, $\{-1,0,1\}$ elemekből álló $N-1\times N-1$-es mátrixot keresünk, amelyik a következő mátrixegyenletet elégíti ki:

$$(\mathbf{i}Q-I)(\mathbf{i}Q-I)^*=NI-J \tag{2.21}$$

ahol J a szokásos módon a csupaegy mátrixot jelöli. Ezt átalakítva

$$QQ^T-\mathbf{i}Q+\mathbf{i}Q^T=(N-1)I-J \tag{2.22}$$

Mivel mind Q, QQ^T, valamint az egyenlet jobb oldala valós, ezért $Q=Q^T$ adódik.

2.4.5. Következmény. *A D_N mátrixok szimmetrikusak.*

Így tehát olyan Q, $\{-1,0,1\}$ elemekből álló $N-1\times N-1$-es szimmetrikus mátrixokat keresünk, amelyekre

$$QQ^T=(N-1)I-J. \tag{2.23}$$

Egyáltalán nem világos, hogy általában ki lehet-e ezt az egyenletet elégíteni. Az viszont, hogy ilyen mátrixok vannak $6, 10, 14$ és 18 dimenzióban mindenképpen biztató jel. A megoldást egy jól ismert fogalom, mégpedig a konferencia-mátrixok szolgáltatták.

2.4.6. Definíció. Egy N-edrendű konferencia mátrix az egy olyan C $N\times N$-es mátrix, amelyre $CC^T=C^TC=(N-1)I$ teljesül, továbbá $C_{ii}=0, i=1,2\ldots,N$ és $C_{ij}\in\{-1,1\}$ ha $i\neq j$.

A konferencia mátrixok egy nagyon fontos és érdekes struktúrát alkotnak, régóta és rendkívül széles körben vizsgálják őket. Mi itt csak annyit említenénk meg, hogy kizárólag páros rendű konferencia mátrixok léteznek [27], azonban Raghavarao [68]-ban rámutatott arra, hogy ez csak egy szükséges, de nem elégséges feltétel. Hasonlóan az Hadamard mátrixok tulajdonságaihoz egy konferencia mátrix sorait illetve oszlopait is szabad ±1-gyel szorozni, és számos konstrukció van arra, hogy bizonyos dimenziókban hogyan lehet ilyen mátrixokat létrehozni. A további velük kapcsolatos eredményeket illetően lásd [31], [74]. Azt, hogy Q milyen kapcsolatban van a konferencia mátrixokkal a következő lemma tisztázza:

2.4.7. Lemma. *Legyen C egy olyan N-ed rendű szimmetrikus konferencia mátrix, amelynek sem az első sora, sem az első oszlopa nem tartalmaz -1-et, továbbá legyen Q az az $N-1 \times N-1$-es mátrix, amelyet úgy kapunk, hogy C első sorát és oszlopát elhagyjuk. Ekkor $QQ^T = (N-1)I - J$ teljesül, és így $H = \mathbf{i}C - I$ egy N-ed rendű komplex Hadamard mátrixot definiál.*

Bizonyítás. Könnyű meggondolni, hogy mivel az első sorban és oszlopban nem szerepelnek -1-ek, ezért elhagyván az első sort és oszlopot olyan Q mátrixhoz jutunk, amelyet ha megszorzunk a transzponáltjával, akkor a szorzatmátrix minden eleme pontosan 1-gyel kisebb, mintha magát C-t szoroztuk volna meg a transzponáltjával. Ez éppen azt jelenti, hogy $QQ^T = (N-1)I - J$, ezzel az állítás első részét beláttuk. Ha C konferencia mátrix volt, akkor H minden eleme egységnyi abszolút értékű, továbbá $C = C^T$ miatt

$$HH^* = (\mathbf{i}C - I)(\mathbf{i}C - I)^* = CC^T + \mathbf{i}C^T - \mathbf{i}C + I = (N-1)I + I = NI. \qquad (2.24)$$

teljesül. Ezzel az állítást igazoltuk. □

Azt látjuk tehát, hogy konferencia mátrixok segítségével Butson típusú $H(4, N)$ komplex Hadamard mátrixokat lehet konstruálni. Sajnos mint kiderült, ez nem új eredmény: ezt a fajta konferencia mátrixokból adódó konstrukciót többek között [57] és [19] is említi. Ezen mátrixok általános paraméterezési lehetőségeit azonban eddig még senki nem vizsgálta meg; mi ezt fogjuk tenni a következőkben.

2.4.4. Paraméterezés általában – Egy struktúratétel

A 10 és 14 dimenzióban számítógép segítségével végrehajtott paraméterezéseket követően felmerült a kérdés, hogy vajon tudunk-e általában is valamit mondani a D_N mátrixok orbitjáról. Jelenleg úgy tűnik hogy maximális (tehát tovább már nem bővíthető) orbit felállítása teljesen reménytelen, annyit azonban sikerült tisztázni, hogy minden D_N mátrixból indul valamilyen paraméteres család. Érvényes tehát a következő

2.4.8. Tétel $(*)$**.** *A D_N mátrixok legalább 1-paraméteres affin családot indukálnak minden olyan dimenzióban, amelyben léteznek.*

Bizonyítás. A bizonyítás teljesen elemi, de számos esetet kell megvizsgálni. Legyen $N \geq 10$ és legyen D_N egy tetszőleges, a konferencia mátrix konstrukcióból adódó N-ed rendű komplex Hadamard mátrix. Feltehető, hogy D_N szimmetrikus és normalizált. A következőkben eljárást adunk 1 paraméter bevezetésére. Tekintsük most D_N második ($\mathbf{u}$) és harmadik ($\mathbf{v}$) sorát. Mivel D_N Hadamard mátrix, pontosan $\frac{N-2}{2}$ koordinátánál fognak az $\mathbf{u}$ és $\mathbf{v}$ sorvektorok csak egy előjelben különbözni. Szorozzuk meg ezeket az

elemeket $e^{\mathbf{i}t}$-vel. Most tekintsük D_N második és harmadik *oszlopát*, és szorozzuk meg $e^{-\mathbf{i}t}$-vel azokat az elemeket, amelyek soronként csak előjelben különböznek. Megmutatjuk, hogy az így adódó 1-paraméteres $D_N^{(1)}(t)$ mátrix t-től függetlenül Hadamard mátrix; egészen pontosan azt fogjuk igazolni, hogy az így kapott mátrix sorai t értékétől függetlenül páronként ortogonálisak. Számos triviális eset mellett kettő olyan van, amely némi meggondolást igényel:

ELSŐ ESET: Most azt fogjuk megmutatni, hogy mind **u** mind pedig **v** merőleges lesz minden változatlanul hagyott sorra. Teljesen világos, hogy D_N első sorára ortogonálisak. $D_N^{(1)}(t)$ sorainak és oszlopainak esetleges permutációit követően feltehető, hogy a mátrix a lenti (szimmetrikus) formát ölti; világos továbbá, hogy szükség esetén a mátrix konjugáltját véve, a bal fölső 3×3-as részmátrixban lévő elemek **i**-k. Most tekintsük bármely, az elsőtől különböző, ám módosítatlan sort. Egy ilyen sor első három eleme értelemszerűen vagy $(1, \mathbf{i}, \mathbf{i})$ vagy $(1, -\mathbf{i}, -\mathbf{i})$. Az első esetet vizsgáljuk, a második teljesen hasonlóan kezelhető.

$$
\begin{array}{c|ccc|c|ccc|ccc|ccc|ccc|}
 & 1 & 1 & 1 & 1 & 1 & \dots & 1 & 1 & \dots & 1 & 1 & \dots & 1 & 1 & \dots & 1 \\
\hline
(\mathbf{u}) & 1 & -1 & \mathbf{i} & \mathbf{i} & \mathbf{i} & \dots & \mathbf{i} & \mathbf{i}e^{\mathbf{i}t} & \dots & \mathbf{i}e^{\mathbf{i}t} & -\mathbf{i}e^{\mathbf{i}t} & \dots & -\mathbf{i}e^{\mathbf{i}t} & -\mathbf{i} & \dots & -\mathbf{i} \\
(\mathbf{v}) & 1 & \mathbf{i} & -1 & \mathbf{i} & \mathbf{i} & \dots & \mathbf{i} & -\mathbf{i}e^{\mathbf{i}t} & \dots & -\mathbf{i}e^{\mathbf{i}t} & \mathbf{i}e^{\mathbf{i}t} & \dots & \mathbf{i}e^{\mathbf{i}t} & -\mathbf{i} & \dots & -\mathbf{i} \\
\hline
 & 1 & \mathbf{i} & \mathbf{i} & -1 & \mathrm{a} & & \mathrm{b} & \mathrm{c} & & \mathrm{d} & \mathrm{e} & & \mathrm{f} & \mathrm{g} & & \mathrm{h} \\
\hline
 & 1 & \mathbf{i} & \mathbf{i} & & -1 & & & & & & & & & & & \\
 & \vdots & \vdots & \vdots & & & \ddots & & & & & & & & & & \\
 & 1 & \mathbf{i} & \mathbf{i} & & & & -1 & & & & & & & & & \\
\hline
 & 1 & \mathbf{i}e^{-\mathbf{i}t} & -\mathbf{i}e^{-\mathbf{i}t} & & & & & -1 & & & & & & & & \\
 & \vdots & \vdots & \vdots & & & & & & \ddots & & & & & & & \\
 & 1 & \mathbf{i}e^{-\mathbf{i}t} & -\mathbf{i}e^{-\mathbf{i}t} & & & & & & & -1 & & & & & & \\
\hline
 & 1 & -\mathbf{i}e^{-\mathbf{i}t} & \mathbf{i}e^{-\mathbf{i}t} & & & & & & & & -1 & & & & & \\
 & \vdots & \vdots & \vdots & & & & & & & & & \ddots & & & & \\
 & 1 & -\mathbf{i}e^{-\mathbf{i}t} & \mathbf{i}e^{-\mathbf{i}t} & & & & & & & & & & -1 & & & \\
\hline
 & 1 & -\mathbf{i} & -\mathbf{i} & & & & & & & & & & & -1 & & \\
 & \vdots & \vdots & \vdots & & & & & & & & & & & & \ddots & \\
 & 1 & -\mathbf{i} & -\mathbf{i} & & & & & & & & & & & & & -1 \\
\hline
\end{array}
\tag{2.25}
$$

A fenti ábrán a negyedik sor az, amellyel foglalkozunk. Ebben az $(1, \mathbf{i}, \mathbf{i})$-vel kezdődő sor megfelelő cellájában jelölje a, c, e és g az **i**-k, még b, d, f és h a $-\mathbf{i}$-k számát. D_N első három sorának a skalárszorzatát tekintve kiszámolható, hogy összesen hány $(\mathbf{i}, \mathbf{i}), (\mathbf{i}, -\mathbf{i}), (-\mathbf{i}, \mathbf{i})$ illetve $(-\mathbf{i}, -\mathbf{i})$ alakú, függőleges pár van az $(\mathbf{u}, \mathbf{v})$ sorokban, mely a következő összefüggéseket adja:

$$b = \frac{N-2}{4} - 2 - a \tag{2.26}$$

$$d = \frac{N-2}{4} - c \tag{2.27}$$

$$f = \frac{N-2}{4} - e \tag{2.28}$$

$$h = \frac{N-2}{4} - g \tag{2.29}$$

Az $\mathbf{i}$-k száma soronként $\frac{N-2}{2}$, így

$$a+c+e+g=\frac{N-2}{2}-2 \tag{2.30}$$

Mivel $D_N^{(1)}(0)$ Hadamard, ezért a negyedik sor ortogonális a módosítást megelőzően $\mathbf{u}$-ra, így

$$2+a-b+c-d-e+f-g+h=0 \tag{2.31}$$

Most helyettesítsük be a (2.26)-(2.29) egyenleteket (2.31)-be, hogy

$$a+c=e+g-2 \tag{2.32}$$

adódjon. Hasonlóan, $D_N^{(1)}(0)$ negyedik sora merőleges a módosítást megelőzően $\mathbf{v}$-re, amiből

$$2+a-b-c+d+e-f-g+h=0 \tag{2.33}$$

folyik. Visszahelyettesítve (2.26)-(2.29)-et (2.33)-ba kapjuk, hogy

$$a+e=c+g-2. \tag{2.34}$$

Végezetül használjuk (2.30)-at (2.32) és (2.34)-ben, hogy

$$a+c=a+e\left(=\frac{N-10}{4}\right) \tag{2.35}$$

adódjon. Kapjuk, hogy $c=e$, és így (2.27) és (2.28)-ból már $d=f$. Innentől egyszerű számolás mutatja, hogy $\mathbf{u}$ és $\mathbf{v}$ t-től függetlenül merőleges $D_N^{(1)}(t)$ negyedik sorára.

MÁSODIK ESET: Már csak azt kell megmutatni, hogy az $e^{-\mathbf{i}t}$ alakú paramétereket tartalmazó sorok merőlegesek mind $\mathbf{u}$-ra mind pedig $\mathbf{v}$-re. Ismét feltehető (a mátrix sorainak illetve oszlopainak permutációját követően), hogy $D_N^{(1)}(t)$ az alábbi alakot ölti. A jelölések megegyeznek az előzőekkel, azonban felhívjuk rá a figyelmet, hogy a cellák mérete ezúttal megváltozott:

$$\begin{array}{r} \\ (\mathbf{u}) \\ (\mathbf{v}) \\ \\ \end{array}\left[\begin{array}{c|cc|c|ccc|ccc|ccc|ccc} 1 & 1 & 1 & 1 & 1 & \dots & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & -1 & \mathbf{i} & \mathbf{i}e^{\mathbf{i}t} & \mathbf{i} & \dots & \mathbf{i} & \mathbf{i}e^{\mathbf{i}t} & \dots & \mathbf{i}e^{\mathbf{i}t} & -\mathbf{i}e^{\mathbf{i}t} & \dots & -\mathbf{i}e^{\mathbf{i}t} & -\mathbf{i} & \dots & -\mathbf{i} \\ 1 & \mathbf{i} & -1 & -\mathbf{i}e^{\mathbf{i}t} & \mathbf{i} & \dots & \mathbf{i} & -\mathbf{i}e^{\mathbf{i}t} & \dots & -\mathbf{i}e^{\mathbf{i}t} & \mathbf{i}e^{\mathbf{i}t} & \dots & \mathbf{i}e^{\mathbf{i}t} & -\mathbf{i} & \dots & -\mathbf{i} \\ \hline 1 & \mathbf{i}e^{-\mathbf{i}t} & -\mathbf{i}e^{-\mathbf{i}t} & -1 & \mathrm{a} & & \mathrm{b} & \mathrm{c} & & \mathrm{d} & \mathrm{e} & & \mathrm{f} & \mathrm{g} & & \mathrm{h} \end{array}\right] \tag{2.36}$$

A fenti ábrában tehát tekintsük most a negyedik sort. Ebben a,b,c,d,e,f,g és h ugyanazzal a jelentéssel bír, mint az első esetben. $D_N^{(1)}(t)$ első három sorára ismét felírva az ortogonalitási egyenleteket kapjuk, hogy

$$b=\frac{N-2}{4}-1-a \tag{2.37}$$

$$d=\frac{N-2}{4}-1-c \tag{2.38}$$

$$f = \frac{N-2}{4} - e \tag{2.39}$$

$$h = \frac{N-2}{4} - g. \tag{2.40}$$

És az **i**-k száma miatt

$$a + c + e + g = \frac{N-2}{2} - 1. \tag{2.41}$$

Mivel **u** és **v** merőleges a paraméterezett sorra, ha $t = 0$, kapjuk, hogy

$$a - b + c - d - e + f - g + h = 0, \tag{2.42}$$

valamint

$$2 + a - b - c + d + e - f - g + h = 0. \tag{2.43}$$

Behelyettesítve (2.37)-(2.40)-et (2.42) és (2.43)-ba

$$a + c = e + g - 1 \tag{2.44}$$

és

$$a + e = c + g - 1 \tag{2.45}$$

adódik. Végül ugyanúgy, mint az első esetben a (2.41)-et (2.44) és (2.45)-be behelyettesítve

$$a + c = a + e \left(= \frac{N-6}{4} \right) \tag{2.46}$$

nyerhető. Innen $c = e$, és (2.38) és (2.39)-ből $d = f - 1$ adódik. Ezen utolsó két egyenlet felhasználásával könnyen látszik, hogy mind **u** mind **v** t-től függetlenül ortogonális $D_N^{(1)}(t)$ negyedik sorára. Teljesen triviális, hogy bármely másik két sorvektor merőleges egymásra. Ezzel a bizonyítás kész. □

2.4.5. A TZ-katalógus kiegészítése

Egyetlen egy dolog várt már csak tisztázásra, mégpedig az, hogy az általunk talált $D_{10}^{(3)}$ illetve $D_{14}^{(6)}$ mátrixok azok szerepelnek-e vagy sem a TZ-katalógusban. Mint mondtuk: heurisztikusan azt sejtjük, hogy nem lehet beforgatni illetve átszorozgatni a 10 illetve 14-ik gyököket tartalmazó, a TZ-katalógusban szereplő mátrixokat $H(4, N)$ alakúra. Ennek tisztázására elevenítsük fel hogy Matolcsi Máté és Réffy Júlia hogyan válaszolt meg [56]-ban egy hasonló típusú kérdést. A parkettázó konstrukciójukkal adódó Hadamard mátrixaikkal úgy sikerült kiegészíteniük a TZ-katalógust, hogy megmutatták, hogy az általuk talált mátrixok nem Diţă-szerűek. Mivel a TZ-katalógusban csupán Diţă-szerű mátrixok szerpeltek 8 és 16 dimenziókban, nyilvánvaló, hogy azok, amiket találtak új Hadamard mátrixok. Pontosan ezt fogjuk a következőkben mi is csinálni. A Diţă-mátrixok általános struktúrájáról szól a következő két, [56]-ból vett eredmény:

2.4.9. Definíció. Legyen L egy $N \times N$ valós mátrix. Egy $I = \{i_1, i_2, \ldots, i_n\} \subset \{1, 2, \ldots, N\}$ indexhalmazra nézve két sort (vagy oszlopot), **s**-t és **q**-t, I-ekvivalensnek nevezünk és $\mathbf{s} \sim_I \mathbf{q}$-val jelölünk, ha a koordinátánként értelmezett $s_i - q_i$ különbségek törtrészei megegyeznek minden $i \in I$ esetén. Két sort (vagy oszlopot), **s**-t és **q**-t, (d)-n-ekvivalensnek nevezünk, ha vannak olyan n-elemű diszjunkt $I_1, \ldots, I_d$ indexhalmazok hogy $\mathbf{s} \sim_{I_j} \mathbf{q}$ teljesül minden $j = 1, \ldots, d$ esetén.

2.4.10. Lemma (Matolcsi–Réffy, [56])**.** *Legyen H egy komplex Hadamard mátrix. Ekkor $\log(H)$ sorainak illetve oszlopainak a permutációja, továbbá egyes sorok (vagy oszlopok) elemeinek egy konstanssal való módosítása nem befolyásolja a H-ban lévő (d)-n-ekvivalens sorok vagy (oszlopok) meglétét vagy hiányát.*

Ezen két észrevétel valamint a (2.5) formula segítségével azt látja az ember tehát, hogy az $N \times N$-es ($N = nk$) D-vel jelölt Diţă-szerű mátrixok szerkezetéből adódóan a $\log(D)$ mátrixban vannak olyan n elemű diszjunkt indexhalmazok, $I_1 = \{1, 2, \ldots, n\}, \ldots, I_k = \{(k-1)n + 1, \ldots, kn\}$ és $R_j = \{\mathbf{r}_j, \mathbf{r}_{j+n}, \ldots, \mathbf{r}_{j+(k-1)n}\}$ ($j = 1, \ldots, n$) sorvektor k-asok, hogy egy rögzített k-asban lévő bármely két sor ekvivalens az I_m-ekre nézve, azaz $\mathbf{r}_{j+(i-1)n} \sim_{I_m} \mathbf{r}_{j+(s-1)n}$ minden $j = 1, \ldots, n$ illetve $i, s, m = 1, \ldots, k$ esetén. Másszóval bármely R_j-vel jelölt sorvektor k-as bármely két sora (k)-n-ekvivalens az I_m halmazokra nézve. Ezek alapján elmondható a következő

2.4.11. Lemma $(*)$**.** *Ha egy normalizált komplex Hadamard mátrix magjában nem szerepel 1-es, akkor a mátrix nem Diţă-szerű.*

Bizonyítás. Legyen H egy normalizált komplex Hadamard mátrix, és tegyük fel indirekt módon, hogy mégis Diţă-szerű. Ekkor az előzőek miatt feltehető, hogy $\{1\} \subseteq I_1$, majd H oszlopainak esetleges permutálását követően az, hogy $\{1, 2\} \subseteq I_1$. A feltevésünk miatt $\log(H)$-nak kizárólag az első sorában van egynél több 0. Most vegyük észre, hogy ha valamelyik sor I_1-ekvivalens $\log(H)$ első sorával, akkor abban az első két koordináta meg kell, hogy egyezzen. Mivel az első koordináta minden sorvektorban 0, ezért a másodiknak is annak kellene lennie, de ez ellentmondás, hiszen nincs ilyen sor $\log(H)$-ban. □

Ebből viszont már azonnal adódik, hogy

2.4.12. Következmény $(*)$**.** *A D_N mátrixok nem Diţă-szerűek.*

Végezetül megemlítünk egy a 2.4.8 tételnél általánosabbnak tűnő paraméterezési konstrukciót, amely segítségével egy N dimenziós konferencia mátrixból képzett Hadamard mátrixba $\frac{N}{2} - 2$ paramétert lehet beilleszteni. Ez a konstrukció működik 6, 10 és 14 dimenzióban, de nem sikerült általánosságban is igazolni:

2.4.13. Konstrukció. *Legyen D egy normalizált szimmetrikus, a konferencia mátrix konstrukcióból adódó N-ed rendű komplex Hadamard mátrix. Használjuk a 2.4.8 tételben látott módszert, és D egy sor- illetve a hozzá tartozó oszloppárjába vezessünk be egy új, szabad paramétert. Ezt követően tekintsünk egy további „megfelelő" sorpárt (és a hozzá tartozó oszloppárt), ha ez lehetséges, hogy újra a 2.4.8 tételt használva egy további paramétert vezessünk be. Egy sorpár „megfelelő", ha az alábbi két feltételt teljesíti:*

i) az összes függőleges elempárja (a már bevezetett paramétereket is figyelembe véve) vagy ugyanazon elemekből, vagy pedig ellentétes előjelű elemekből áll (kivéve az elkerülhetetlen $(-1,*)$ és $(*,-1)$ párokat);

ii) van még olyan függőleges $(\boldsymbol{i},-\boldsymbol{i})$ vagy $(-\boldsymbol{i},\boldsymbol{i})$ elempárja, amely nem függ paraméterektől.

Ha egy megfelelő sorpárt találtunk, akkor vezessünk be (a hozzá tartozó oszlopokat is figyelembe véve) egy új paramétert a 2.4.8 tételnek megfelelően, azaz szorozzuk be az ellentétes előjelű elemeket $e^{\pm \boldsymbol{i}t}$-vel. Ismételjük az eljárást egészen addig, amíg ilyen megfelelő sorpárok vannak.

A fenti két feltétel a paraméterezhetőség *szükséges* feltétele az alábbi értelemben. Az i) feltétel azt biztosítja, hogy D első sora és az újonnan paraméterezett sorok páronként merőlegesek maradjanak. A ii) feltétel azért szükséges, hogy garantáljuk, hogy az új lépésben a már meglévőektől független paramétert vezetünk be. Nem világos azonban, hogy ez a két feltétel elégséges-e, azaz jelenleg nem tudjuk formálisan bizonyítani, hogy a konstrukció alapján paraméterezett mátrixok ortogonálisok maradnak. Emellett, előfordulhat hogy egy adott állapotban többféle megfelelő sorpár is adódik, és nem tudni, melyiket érdemes paraméterezni. Mindenesetre ezzel a módszerrel legfeljebb $\frac{N}{2}-1$ paraméteret lehet bevezetni. Ezen konstrukció segítségével készítettük el a D_{10} és D_{14} mátrixok orbitjait, majd számítógéppel ellenőriztük az eredmények helyességét.

2.4.14. Példa.

$$D_{10}^{(3)}(a,b,c) = D_{10} \circ \mathbf{EXP}\left(\mathbf{i} \cdot R_{D_{10}^{(3)}}(a,b,c)\right) \tag{2.47}$$

ahol

$$R_{D_{10}^{(3)}}(a,b,c) = \begin{bmatrix}
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & a-b & a & -c & \bullet & -c & a & a-b & \bullet \\
\bullet & -a+b & \bullet & b & -c & \bullet & -c & b & \bullet & -a+b \\
\bullet & -a & -b & \bullet & \bullet & \bullet & \bullet & \bullet & -b & -a \\
\bullet & c & c & \bullet & \bullet & \bullet & \bullet & \bullet & c & c \\
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
\bullet & c & c & \bullet & \bullet & \bullet & \bullet & \bullet & c & c \\
\bullet & -a & -b & \bullet & \bullet & \bullet & \bullet & \bullet & -b & -a \\
\bullet & -a+b & \bullet & b & -c & \bullet & -c & b & \bullet & -a+b \\
\bullet & \bullet & a-b & a & -c & \bullet & -c & a & a-b & \bullet
\end{bmatrix} \tag{2.48}$$

$$D_{14}^{(6)}(a,b,c,d,e,f) = D_{14} \circ \mathbf{EXP}\left(\mathbf{i} \cdot R_{D_{14}^{(6)}}(a,b,c,d,e,f)\right) \tag{2.49}$$

ahol

$$R_{D_{14}^{(6)}}(a,b,c,d,e,f) =$$

$$\begin{bmatrix}
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & a-b & a-b & -c & a & -e & -c & \bullet & a & -e & a & a \\
\bullet & \bullet & \bullet & a-b & a-b & -c & a & -e & -c & \bullet & a & -e & a & a \\
\bullet & b-a & b-a & \bullet & \bullet & b & b & -e & b & \bullet & -f & -e & b & -f \\
\bullet & b-a & b-a & \bullet & \bullet & b & b & -e & b & \bullet & -f & -e & b & -f \\
\bullet & c & c & -b & -b & \bullet & c-d & c & \bullet & \bullet & \bullet & c & c-d & \bullet \\
\bullet & -a & -a & -b & -b & d-c & \bullet & d-e & d-c & \bullet & d-f & d-e & \bullet & d-f \\
\bullet & e & e & e & e & -c & e-d & \bullet & -c & \bullet & -f & \bullet & e-d & -f \\
\bullet & c & c & -b & -b & \bullet & c-d & c & \bullet & \bullet & \bullet & c & c-d & \bullet \\
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
\bullet & -a & -a & f & f & \bullet & f-d & f & \bullet & \bullet & \bullet & f & f-d & \bullet \\
\bullet & e & e & e & e & -c & e-d & \bullet & -c & \bullet & -f & \bullet & e-d & -f \\
\bullet & -a & -a & -b & -b & d-c & \bullet & d-e & d-c & \bullet & d-f & d-e & \bullet & d-f \\
\bullet & -a & -a & f & f & \bullet & f-d & f & \bullet & \bullet & \bullet & f & f-d & \bullet
\end{bmatrix} \tag{2.50}$$

2.4.15. Lemma $(*)$. *A $D_{10}^{(3)}$ illetve $D_{14}^{(6)}$ mátrixok lokálisan inekvivalensek a TZ-katalógusban felsorolt mátrixok mindegyikével.*

Bizonyítás. A 2.4.11 lemma miatt D_{10} és D_{14} nem Diţă-szerű mátrix. Mivel a Diţă-szerű mátrixok halmaza zárt [56], ezért a paraméterezett D_{10} illetve D_{14} mátrixok orbitja lokálisan nem Diţă-szerű. Végül vegyük észre, hogy 10 és 14 dimenzióban kizárólag Diţă-mátrixok szerpelnek a TZ-katalógusban. □

11. *Megjegyzés.* Nem tudunk többet állítani a lokális inekvivalenciánál, előfordulhat ugyanis az, hogy a D_{10}-ből és az F_{10}-ből kiinduló mátrixcsaládok valahol metszik egymást hasonlóan ahhoz, ahogyan 8 dimenzióban az F_8 és az S_8 mátrixok orbitjai is a valós H_8 mátrixban találkoznak [82], [56].

12. *Megjegyzés.* Előfordulhat, hogy egy adott N dimenzióban több, páronként inekvivalens konferencia mátrix is létezik [31], amelyekből lokálisan inekvivalens D_N komplex Hadmard mátrix családokat lehet készíteni.

Összegzésként elmondhatjuk tehát, hogy sikeresen konstruáltunk két olyan paraméteres komplex Hadamard mátrix családot 10 és 14 dimenzióban, amely elkerülte a TZ-katalógus készítőinek a figyelmét. A mátrixok által indukált orbit új, sehol az irodalomban fel nem lelhető eredmény.

2.5. Valós Hadamard mátrixok paraméterezése

Ebben a fejezetben egy más jellegű eredményünket fogjuk ismertetni. A már többször is említett [56]-ben szereplő S_8, S_{12} és S_{16} mátrixok paraméterezését a szerző végezte el. Ezen munkálatok közben sikerült rájönni arra, hogy általában hogyan lehet paramétereket elhelyezni egy akármilyen komplex Hadamard mátrixba, a legfontosabb eredményünk pedig az, hogy

tisztáztuk a TZ-katalógus szerzőinek, W. Tadej és K. Życzkowski egy kérdését, mely szerint minden valós Hadamard mátrix paraméterezhető. Mellékeredményként megmutatjuk, hogy a $\cong$ ekvivalencia erejéig egyértelmű valós H_{12} mátrix sem szerepelt a TZ-katalógusban, és megadjuk neki egy 7 paraméteres orbitját. Mindezek előtt azonban nézzük meg közelebbről a $4p$ rendű valós Hadamard mátrixokat.

2.5.1. Egy másik alkalmazás a Matolcsi–Réffy kritériumra: H_{4p} nem Diţă-szerű

Legelőszöris egy önmagában is érdekes, a valós Hadamard mátrixok általános struktúrájára jellemző tételt prezentálunk, amely arról szól, hogy a Diţă-konstrukció segítségével általában véve nem állítható elő minden valós Hadamard mátrix. Speciálisan, ha p prím, akkor a $4p$ rendű valós Hadamard mátrix nem Diţă-szerű. Mielőtt igazolnánk a fenti állítást, szükségünk van egy közismert lemmára.

2.5.1. Lemma. *Legyen $p \geq 3$ tetszőleges páratlan szám. Tegyük fel, hogy egy valós, $\{-1,1\}$ elemű, $4p$ rendű mátrixnak az első 4 sora a következő alakú: (minden valós Hadamard mátrix ekvivalens egy olyannal, amelynek az első 3 sora ugyanolyan, mint az alábbi mátrixnak):*

$$\begin{bmatrix} 1^p & 1^p & 1^p & 1^p \\ 1^p & 1^p & (-1)^p & (-1)^p \\ 1^p & (-1)^p & 1^p & (-1)^p \\ 1^p & (-1)^p & (-1)^p & 1^p \end{bmatrix} \tag{2.51}$$

ahol 1^p a p db 1-est tartalmazó sorvektort jelenti. Ekkor ezen sorvektorok nem egészíthetőek ki egy olyan további, $\{-1,1\}$-ből álló sorvektorral, amely mind a 4-re merőleges volna.

A lemma a 2.4.8 tételhez hasonló eszközökkel látható be, ezért bizonyítását mellőzzük. Most pedig rátérünk a korábbiakban már felvezetett struktúratételnek az igazolására:

2.5.2. Tétel $(*)$. *Ha p egy páratlan prím, akkor semelyik $4p$ rendű H_{4p} valós Hadamard mátrix nem Diţă-szerű.*

Bizonyítás. Az [56]-ban szereplő eredményeket (vagyis lényegében a 2.4.10 lemmát) fogjuk felhasználni. Megjegyezzük azonban, hogy lévén H_{4p} valós Hadamard mátrix, természetes módon tudjuk $\log H_{4p}$-vel azonosítani. Technikai okokból mi most a $\log(H_{4p})$ mátrix helyett magára H_{4p}-re fogjuk alkalmazni a 2.4.10 lemma értelemszerű módosítását.

Tegyük fel indirekt, hogy H_{4p} mégis Diţă-szerű. Ebben az esetben (lásd megint [56]-ot) n lehetséges értékei $2, 4, p$ valamint $2p$ (és így k rendre $2p, p, 4$ valamint 2). Feltehető hogy H_{4p} normalizált, és jelölje (2.51) sorait rendre $\mathbf{s}, \mathbf{t}, \mathbf{u}$ és $\mathbf{v}$. Az n és k értékeitől függően tehát 4 különböző esetet kell vizsgálnunk:

ELSŐ ESET: Tegyük fel hogy $n = 2p, k = 2$. Ekkor ha H_{4p} Diţă-szerű lenne, akkor lenne két diszjunkt $2p$ elemű I_1 és I_2 indexhalmaz úgy, hogy H_{4p}-ben $2p$ sorpár ekvivalens

I_1-re és I_2-re. Most tekintsük **s**-t, és tegyük fel hogy van egy I_1-re és I_2-re vonatkozó párja. A sorok és oszlopok permutálását követően feltehető, hogy H_{4p} első 3 sora rendre $\mathbf{s}, \mathbf{t}$ és $\mathbf{u}$, azaz **s** párja **t**, és $I_1 = \{1, 2, \ldots, 2p\}$ valamint $I_2 = \{2p+1, 2p+2, \ldots, 4p\}$. Most tekintsük **u**-t. Ha lenne neki is egy párja, akkor az első $2p$ elemük meg kellene hogy egyezzen. Ekkor viszont mivel H_{4p} Hadamard mátrix, a további $2p$ eleme **u**-nak és a párjának szükségképpen különbözik. Azt kaptuk tehát, hogy **u** párja **v**, de ez ellentmondás, hiszen a 2.5.1 lemma miatt nincs ilyen sor H_{4p}-ben.

MÁSODIK ESET: Tegyük fel most, hogy $n = p, k = 4$. Ebben az esetben van 4 olyan p-elemű I_1, I_2, I_3 valamint I_4 indexhalmaz, hogy H_{4p}-ben p darab diszjunkt sorvektor 4-es található úgy, hogy bármely két sor egy rögzített sor 4-esen belül ekvivalens ezekre az indexhalmazokra nézve. Feltehető, hogy $I_1 = \{1, 2, \ldots, p\}, I_2 = \{p+1, p+2, \ldots, 2p\}, I_3 = \{2p+1, 2p+2, \ldots, 3p\}$ és $I_4 = \{3p+1, 3p+2, \ldots, 4p\}$. Most vegyük észre, hogy mivel **s**-ben csak 1-esek vannak, bármely sor, amely ekvivalens vele az I_1, I_2, I_3 valemint I_4 halmazokra nézve szükségképpen $\mathbf{t}, \mathbf{u}$ vagy **v** lesz. Ebben az esetben viszont mindhárom megnevezett sorra szükségünk van ahhoz, hogy egy sor 4-est hozzunk létre, de ez ismét ellentmond a 2.5.1 lemmának.

HARMADIK ESET: Most az $n = 4, k = p$ esetet vizsgáljuk. Ebben az esetben vannak olyan $I_1, I_2, \ldots, I_p$ 4 elemű indexhalmazok, hogy H_{4p}-ben van 4 diszkjunt sorvektor p-s úgy, hogy bármely két sor egy rögzített p-esben ekvivalens ezekre az indexhalmazokra nézve. Az előzőekhez hasonló módon keresünk egy párt **s**-hez. Most vegyük észre, hogy mivel minden **s**-től különböző sor $2p$ darab 1-est és $2p$ db -1-est tartalmaz, lehetetlen az elemeiket páratlan darab diszjunkt halmazzá bontani úgy, hogy a halmazok pontosan ugyanazokat az elemeket tartalmazzák. Így nincs olyan sorvektor H_{4p}-ben, amely **s**-sel ekvivalens lenne ezen indexhalmazokra nézve.

NEGYEDIK ESET: Végül tegyük fel, hogy $n = 2, k = 2p$. Ismét feltehető (H_{4p} oszlopainak a permutációit követően), hogy $I_1 = \{1, 2\}$ valamint $I_2 = \{3, 4\}$ teljesül. Mivel H_{4p} valós Hadamard mátrix az is feltehető továbbá, hogy (néhány sor permutálását követően) H_{4p} első három *oszlopa* pontosan ugyanaz, mint (2.51) első három sorának a transzponáltja. Most vegyük észre, hogy az első $2p$ sor és a második $2p$ sor alkotja szükségképpen a 2 db sorvektor $2p$-eseket. Ekkor viszont ahhoz, hogy az I_2-re való ekvivalenciát is megőrizzük, könnyen látszik hogy H_{4p} negyedik oszlopa éppen (2.51) negyedik sorának a transzponáltja kell, hogy legyen. Ez ismét ellentmondás. □

Ebből azonnal adódik, hogy

2.5.3. Következmény $(*)$. *H_{12} nem Diţă-szerű.*

2.5.2. Paraméterezés általában: W. Tadej és K. Życzkowski kérdésének a megválaszolása

Már korábban is említettük, hogy a komplex Hadamard mátrixok paraméterezése egyáltalán nemtriviális feladat. Mindössze 3 általános módszer ismert paraméterek bevezetésére. Egy-

részt van a Diţă-konstrukció, ami egy direkt módszer arra, hogy hogyan készítsünk összetett dimenzióban paraméteres mátrixcsaládokat, azonban ez semmit nem mond arról, hogy egy általános mátrixba hova helyezzünk el paramétereket. Egy másik lehetőség M. Petrescu konstrukciója, akinek bizonyos prím dimenziókban is sikerült paraméteres családokat konstruálnia [64] (és ezzel cáfolni Popa azon sejtését, miszerint prímdimenziókban csak izolált komplex Hadamard mátrixok vannak [67]). Végül van egy harmadik, ezektől eltérő, kombinatorikai eljárás, az ún. „linear variaton of phases method", amelyek segítségével *affin* családokat lehet bevezetni [82]. Az algoritmus hátránya, hogy rendkívül számolásigényes, és úgy tűnik, hogy csupán kis dimenziókban, és csak speciális struktúrájú (Fourier) mátrixokra működik hatékonyan. A következőkben egy teljesen természetes paraméterezési lehetőséget mutatunk, tulajdonképpen az alábbi lemma segítségével sikerült az [56]-ban szereplő $S_8^{(4)}, S_{12}^{(5)}$ illetve $S_{16}^{(11)}$ mátrixokat felparaméterezni.

2.5.4. Lemma $(*)$. *Legyen H egy tetszőleges, normalizált N-ed rendű komplex Hadamard mátrix, és tegyük fel, hogy H-ban van két olyan oszlop, mondjuk $\mathbf{u}$ és $\mathbf{v}$, hogy $u_i + v_i = 0$ vagy $u_i = v_i$ teljesül minden $i = 1, 2, \ldots, N$-re. Ekkor H affin paraméteres családot indukál.*

Bizonyítás. Legyen H a fenti lemma feltételeit kielégítő mátrix, és minden olyan (u_i, v_i) koordinátákat, amelyekre $u_i + v_i = 0$ teljesül szorozzunk meg $e^{\mathbf{i}t}$-vel (másszóval az (u_i, v_i) koordinátapárt cseréljük ki $(u_i e^{\mathbf{i}t}, v_i e^{\mathbf{i}t})$-re. Ekkor az így kapott új mátrix Hadamard lesz, hiszen minden eleme továbbra is egységnyi abszolút értékű, továbbá könnyen látszik, hogy bármely két sorának véve a skaláris szorzatát a t paraméter kiesik a szorzatokból, és ha H Hadamard volt akkor a módosított mátrix is Hadamard marad. □

A következőkben azt mutatjuk meg, hogy a triviális $(N = 1, 2)$ esetektől eltekintve nincs izolált valós Hadamard mátrix. Régóta ismert tény, hogy H_4 egy egyparaméteres családot indukál, míg H_8-ra két lényegesen különböző orbitot sikerült nemrégiben konstruálni [82], [56]. Az ennél nagyobb dimenziójú mátrixok esetét a következő tétel tisztázza:

2.5.5. Tétel $(*)$. *Legyen H_N valamely $N \geq 12$-re egy valós Hadamard mátrix. Ekkor H_N-ből legalább egy $\frac{N}{2} + 1$ független paramétert tartalmazó család indul ki.*

Bizonyítás. Legyen $N \geq 12$, és legyen H egy normalizált, N dimenziós valós Hadmard mátrix. Világos, hogy H bármely két oszlopát is tekintjük, pontosan $\frac{N}{2}$ olyan sor lesz, amelyben az oszlopokban lévő elemek eltérnek, és ugyanúgy $\frac{N}{2}$ olyan sor, ahol megegyeznek. A 2.5.4 lemma feltételei tehát teljesülnek. A következőkben ennek a lemmának a bizonyításában látott konstrukciót fogjuk egy kicsit általánosabban alkalmazni.

Feltehetjük, hogy H a következő „kanonikus" alakra van permutálva: $H_{2,1} = H_{2,2} = \ldots = H_{2,N/2} = 1$ és így $H_{2,N/2+1} = H_{2,N/2+2} = \ldots = H_{2,N} = -1$, továbbá $H_{3,3} = H_{3,4} = 1$ és $H_{3,2} = H_{3,N-1} = H_{3,N} = -1$. Tekintsük most a következő, indexpárokból álló halmazt: $T = \{(2i-1, 2i), i = 1, 2, \ldots, \frac{N}{2}\}$. Minden T-beli elem megfelel H egy oszloppárjának. A paraméterezési eljárás legyen a következő: minden $i = 1, 2, \ldots, \frac{N}{2}$ esetén vegyük T i-dik elemét, majd tekintsük a megfelelő oszlopok *sorait*. Ha egy adott sorban az elemek különbözőek, akkor

szorozzuk meg őket $e^{\mathbf{i}x_i}$-vel (hangsúlyozzuk, hogy pontosan $\frac{N}{2}$ ilyen sor van). Ez az eljárás a 2.5.4 lemmához hasonlóan egy $\frac{N}{2}$ paraméteres, H-ból kiinduló családot indukál. Vegyük észre azonban hogy az így kapott mátrix nem normalizált, ezért normalizálnunk kell azt: szorozzuk be néhány sorát $e^{-\mathbf{i}x_1}$-vel. Lévén $H_{3,3} = H_{3,4}$ azt látjuk, hogy a normalizálást követően ezek az elemek csak x_1-től függenek, vagyis $x_1, x_2, \ldots, x_{N/2}$ függetlenek maradnak a normalizálás után is. Kényelmi szempontokból helyettesíthetjük x_1-et $-x_1$-gyel. Most tekintsük H első két *sorát*, és vegyül észre hogy ezek még mind függetlenek az x_i paraméterektől. Szorozzuk be most ezen két sor utolsó $\frac{N}{2}$ elemét $e^{-\mathbf{i}x_{N/2+1}}$-vel. Világos, hogy az így kapott mátrix is még mindig Hadamard, azonban hasonlóan az előzőekhez nincs normalizálva. Vegyük észre azonban, hogy normalizálást követően a $H_{3,N-1} = H_{3,N}$ feltétel miatt ezek az elemek csakis x_1-től és $x_{N/2+1}$-től függenek. Mivel a legutolsó paraméter bevezetése nem változtatta meg sem $H_{3,3}$-at sem $H_{3,4}$-et ezért az állítást beláttuk. □

A fenti tétel tehát megválaszolja W. Tadej és K. Życzkowski kérdését. Most adunk egy példát.

2.5.6. Példa.

$$H_{12} = \left[\begin{array}{cccccccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\
1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\
1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 \\
1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 \\
1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 \\
1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\
1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 \\
1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1
\end{array}\right] \tag{2.52}$$

$$H_{12}^{(7)}(a,b,c,d,e,f,g) = H_{12} \circ \mathbf{EXP}\left(\mathbf{i} \cdot R_{H_{12}^{(7)}}(a,b,c,d,e,f,g)\right) \tag{2.53}$$

ahol

$$R_{H_{12}^{(7)}}(a,b,c,d,e,f,g) = \tag{2.54}$$

$$\left[\begin{array}{cccccccccccc}
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & a & a & a & a & a+g & a+g & a+e+g & a+e+g & a+g & a+g \\
\bullet & \bullet & a+b & a+b & a+c & a+c & a+d+g & a+d+g & a+e+g & a+e+g & a+f+g & a+f+g \\
\bullet & \bullet & a+b & a+b & a+c & a+c & a+d+g & a+d+g & a+e+g & a+e+g & a+f+g & a+f+g \\
\bullet & \bullet & b & b & \bullet & \bullet & d+g & d+g & e+g & e+g & f+g & f+g \\
\bullet & \bullet & \bullet & \bullet & c & c & d+g & d+g & e+g & e+g & f+g & f+g \\
\bullet & \bullet & b & b & \bullet & \bullet & g & g & g & g & f+g & f+g \\
\bullet & \bullet & a+b & a+b & a+c & a+c & a+g & a+g & a+e+g & a+e+g & a+g & a+g \\
\bullet & \bullet & \bullet & \bullet & c & c & g & g & g & g & f+g & f+g \\
\bullet & \bullet & a & a & a & a & a+d+g & a+d+g & a+g & a+g & a+g & a+g \\
\bullet & \bullet & a+b & a+b & a+c & a+c & a+d+g & a+d+g & a+g & a+g & a+g & a+g
\end{array}\right] \tag{2.55}$$

2.5.3. A TZ-katalógus kiegészítése H_{12}-vel

Ismét csak az volt hátra, hogy a 16 dimenziónál kisebb esetekről eldöntsük, vajon szerepelnek-e a TZ-katalógusban, vagy sem. A 8 dimenziós mátrixszal nem foglalkoztunk, arról ugyanis nem mond semmit a 2.5.5 tétel. A következő szóba jöhető rend, a 12, rendkívül ígéretesnek mutatkozott. Nem lehetett azonban itt ugyanúgy érvelni, mint a D_N mátrixok esetében, ugyanis 12 dimenzióban nem csupán Diţă-szerű mátrixok voltak felsorolva a TZ-katalógusban. Heurisztikusan azonban itt is azt gondoltuk, hogy 12-ik gyököket tartalmazó mátrixot nem fog tudni az ember átforgatni, átpermutálni valósba. A megoldást Matolcsi Máté szolgáltatta, aki rámutatott arra, hogy a Haagerup-feltétel (lásd a 2.2.11 lemmát) alkalmas arra, hogy belássuk: H_{12} nem szerepel a TZ-katalógusban.

2.5.7. Lemma (Matolcsi[1]). *H_{12} inekvivalens a [82]-ben illetve az [56]-ban felsorolt mátrixok mindegyikétől.*

Bizonyítás. A Haagerup kritériumot fogjuk alkalmazni. Világos, hogy a H_{12}-höz tartozó invariáns halmaz csupán a ± 1 számokat tartalmazza, vagyis $\Lambda_{H_{12}} = \{-1, 1\}$. Most vegyük sorra először a TZ-katalógusban szereplő különféle orbitjait az F_{12} mátrixnak, és vegyük észre, hogy paraméterválasztástól függetlenül $e^{2\pi \mathbf{i}/8} \in \Lambda_{F_{12}}$. Tekintsük most az [56]-ból származó S_{12} mátrixot, és vegyük észre, hogy – megint, paraméterezéstől függetlenül – $e^{2\pi \mathbf{i}/3} \in \Lambda_{S_{12}}$. Mivel a mátrixok Λ-invariáns halmazai különböznek, ezért a 2.2.11 lemma értelmében nem lehetnek ekvivalensek. □

2.5.8. Következmény (∗). *$H_{12}(a, b, c, d, e, f, g)$ lokálisan inekvivalens a TZ-katalógusban szereplő mátrixok mindegyikével.*

13. *Megjegyzés.* A fenti konstrukció természetesen 16 dimenzióban is működik, ám itt már 5, egymással inekvivalens valós Hadamard mátrix van, amiket nem tudunk összehasonlítani a TZ-katalógusban szereplő F_{16} mátrixból induló paraméteres családokkal.

Sikerült tehát ismét egy új, paraméteres Hadamard mátrix családot kosntruálnunk. Maga H_{12} természetesen egy jól ismert mátrix volt, az orbitja azonban új eredmény.

A fejezetet a komplex Hadamard mátrixok egy nem várt alkalmazásával zárjuk.

2.6. Egy meglepő alkalmazás Hadamard mátrixokra

A BME Analízis Tanszékének munkatársai évek óta behatóan vizsgálnak különféle kvantumfizikai rendszereket. Ezen vizsgálatok közben merült fel egy érdekes probléma, amelynek megoldásában (többekkel együtt) jelen diplomamunka szerzője is részt

[1] Magánbeszélgetés

vett. Mivel ez a témakör nem kapcsolódik szervesen a dolgozathoz, ezért csak röviden vázolnánk magát a problémát, illetve a rá adott megoldást.

Egy két qubitből álló kvantumrendszer leírása 4×4-es mátrixok segítségével történik. Ha a rendszert olyan összetett rendszerként fogjuk fel, ami két feles spinből áll, akkor ez matematikailag azt jelenti, hogy a 4×4-es mátrixok $M_4(\mathbb{C})$ algebráját azonosítjuk az $M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$ algebrával. Petz Dénes azt a kérdést vetette fel, hogy legkevesebb hány olyan $\mathcal{A}_k$ részalgebrát kell venni $M_4(\mathbb{C})$-ből, melyek egyrészt izomorfak $M_2(\mathbb{C})$-vel, másrészt a valós lineáris kombinációjuk kifeszíti az egész $M_4(\mathbb{C})$ teret. Mivel $M_4(\mathbb{C})$ nyomnélküli altere a valósak felett 15 dimenziós, minden $\mathcal{A}_k$ pedig 3 dimenziós, ezért világos, hogy legalább 5 ilyen részalgebrát kell mutatni. Ismert, hogy $M_2(\mathbb{C})$-t kifeszítik a $\sigma_k, k = 0, \ldots, 3$ Pauli-mátrixok, és könnyen adódik, hogy annak a feltétele, hogy valamely $\mathcal{A}_k$ részalgebra algebrailag izomorf legyen $M_2(\mathbb{C})$-vel az alábbi két feltétellel ekvivalens: Létezik egy olyan (S_1, S_2, S_3) operátorhármas, amelyre i) $S_k, k = 1, 2, 3$ önadjungált unitér, és ii) $S_3 = -\mathbf{i}S_1S_2$, $S_1S_2 + S_2S_1 = 0$ teljesül. Ekkor az I, S_1, S_2, S_3 operátorok természetes módon azonosíthatóak a Pauli mátrixokkal, és így egy $M_2(\mathbb{C})$-vel izomorf részalgebrát generálnak.

Ezzel a problémával korábban Szántó András is foglalkozott, aki a Pauli-mátrixok segítségével sikeresen konstruált 6 ilyen algebrát [79]. Az ő megoldása az alábbi volt:

2.6.1. Példa.

$$\begin{aligned}
&\{\sigma_1 \otimes \sigma_1, \sigma_1 \otimes \sigma_2, \sigma_0 \otimes \sigma_3\},\\
&\{\sigma_2 \otimes \sigma_2, \sigma_2 \otimes \sigma_3, \sigma_0 \otimes \sigma_1\},\\
&\{\sigma_3 \otimes \sigma_3, \sigma_3 \otimes \sigma_1, \sigma_0 \otimes \sigma_2\},\\
&\{\sigma_2 \otimes \sigma_2, \sigma_3 \otimes \sigma_2, \sigma_1 \otimes \sigma_0\},\\
&\{\sigma_3 \otimes \sigma_3, \sigma_1 \otimes \sigma_3, \sigma_2 \otimes \sigma_0\},\\
&\{\sigma_1 \otimes \sigma_1, \sigma_2 \otimes \sigma_1, \sigma_3 \otimes \sigma_0\}.
\end{aligned} \tag{2.56}$$

Az I identitás operátorral együtt a fenti hármasok egy-egy $\mathcal{A}_j, 1 \leq j \leq 6$ részalgebrát generálnak, és a 6 részalgebra együtt az egész $M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$ teret kifeszíti.

A fenti konstrukció elegáns, mert jól ismert mátrixok segítségével konstruálja meg ezeket az algebrákat, és könnyű elenőrizni, hogy ez a hat részalgebra elégséges az $M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$ tér kifeszítéséhez. A konstrukció „hátránya” azonban az, hogy nagyfokú redundanciával is bír, hiszen a $\sigma_i \otimes \sigma_i, i = 1, 2, 3$ elemeket két-két algebra is tartalmazza. De vajon meg lehet szabadulni az itt fellépő redundanciától?

A kérdésre a válasz igenlő, ugyanis a fenti konstrukciót sikerült a szerzőnek megjavítania, és a minimális 5 részalgebrát prezentálnia. Meglepő módon egy olyan algebra került elő, és játszott központi szerepet a megoldásban, amelynek az elemei (konstans szorzótól eltekintve) komplex Hadamard mátrixok. Az alapgondolat az volt, hogy a Pauli-mátrixok segítségével próbáljuk meg a lehető legbővebb, ám redundáns elemek

fellépése nélküli részalgebrákat megkonstruálni, a maradék, $M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$ kifeszítéséhez hiányzóakat pedig valamilyen nagyfokú szimmetriamegkötések mellett keresni. Így találtunk rá az alábbi négy, illetve az azt kiegészítő ötödik részalgebrára:

2.6.2. Példa. Az alábbi négy, Pauli mátrixokból álló halmaz az I identitásoperátorral együtt egy-egy $\mathcal{A}_k$, $M_2(\mathbb{C})$-vel izomorf részalgebrát alkot.

$$\{\sigma_0 \otimes \sigma_1, -\sigma_1 \otimes \sigma_3, \sigma_1 \otimes \sigma_2\} \tag{2.57}$$

$$\{\sigma_3 \otimes \sigma_1,\ \sigma_1 \otimes \sigma_1,\ \sigma_2 \otimes \sigma_0\} \tag{2.58}$$

$$\{\sigma_1 \otimes \sigma_0,\ \sigma_2 \otimes \sigma_2,\ \sigma_3 \otimes \sigma_2\} \tag{2.59}$$

$$\{\sigma_0 \otimes \sigma_2,\ \sigma_2 \otimes \sigma_3,\ \sigma_2 \otimes \sigma_1\} \tag{2.60}$$

Fontos észrevenni, hogy az itt felsorolt mátrixok páronként ortogonálisak, továbbá mindegyiküknek azonosan 0 a fődiagonálisa. Pauli mátrixokból nem várhatunk kiegészítő részalgebrát, hiszen az itt felsorolt négy részalgebrának az ortokomplementuma már kommutatív, de ha találunk egy további olyan algebrát, amelyben szereplő mátrixok diagonálisa lineárisan független, akkor ez a már felsorolt négy algebrával együtt kifeszíti az egész $M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$ teret. A kérdés már csak az, hogyan konstruáljunk „természetes” módon unitér mátrixokat? Megdöbbentő módon a problémára van „szép”, mégpedig (átskálázott) komplex Hadamard mátrixokból álló megoldás:

$$\left\{ \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix}, \quad \frac{1}{2}\begin{bmatrix} 1 & \mathbf{i} & \mathbf{i} & -1 \\ -\mathbf{i} & -1 & -1 & \mathbf{i} \\ -\mathbf{i} & -1 & 1 & -\mathbf{i} \\ -1 & -\mathbf{i} & \mathbf{i} & -1 \end{bmatrix}, \quad \frac{1}{2}\begin{bmatrix} -1 & \mathbf{i} & 1 & \mathbf{i} \\ -\mathbf{i} & 1 & \mathbf{i} & 1 \\ 1 & -\mathbf{i} & 1 & \mathbf{i} \\ -\mathbf{i} & 1 & -\mathbf{i} & -1 \end{bmatrix} \right\}. \tag{2.61}$$

A további részleteket, illetve a kvantum-információelméleti hátteret illetően lásd [79], [66] és [65].

3. fejezet

Új konstrukciók komplex Hadamard mátrixokra

3.1. Bevezetés

1983-ban Popa az $M_n(\mathbb{C})$ mátixalgebra ortogonális rész $*$-algebrái vizsgálata következtében mutatott rá arra, hogy egy ortogonális részalgebra-pár létezése lényegében egy komplex Hadamard mátrix megadásával jellemezhető. Popa azt sejtette, hogy ha n prím, akkor az egyetlen ilyen komplex Hadamard mátrix (természetesen ekvivalencia erejéig) csak a Fourier mátrix lehet. Ezt azonban rövidesen cáfolta Björck [8] majd tőle függetlenül Pierre de la Harpe és a Fields-medálos Vaughan F. R. Jones, akik [23]-ban $n \geq 13$-tól kezdve minden $n \equiv 1 \mod 4$ prímre mutattak egy ettől inekvivalens mátrixot. Konstrukciójukban jól ismert diszkrét matematikai objektumokat, az ún. Paley gráfokat használták. Ezt a konstrukciót némileg módosította néhány évvel később Munemasa és Watatani, akik $n \equiv 3 \mod 4$ prím esetén asszociációs sémák segítségével gyártottak a Fouriertől inekvivalens komplex Hadamard mátrixokat [58].

Mi ebben a fejezetben valós Hadamard mátrixok segítségével egy teljesen elemi bizonyítást adunk Munemasa és Watatani eredményeire, amelyből nem feltétlen prím n-ekre is új komplex Hadamard mátrixok adódnak. Az első ilyen, eddig ismeretlen példa $n = 15$ dimenzióban konstruálható. A legfontosabb, fejezetbeli eredményünk az, hogy ha feltesszük még azt is, hogy a szóbanforgó valós Hadamard mátrix még szimmetrikus is, akkor egy további, mind az előzőtől, mind pedig a Fourier mátrixtól is inekvivalens komplex Hadamard mátrixot lehet gyártani. Végezetül újra elővesszük a konferencia mátrixokat, és ezek segítségével de la Harpe és Jones eredményét fedezzük fel ismét, de egy olyan általánosabb formában, amely a nem feltétlen prím dimenziókban is működik, feltéve hogy egy valós, szimmetrikus konferencia mátrix létezése garantálva van.

A konstrukcióink legfontosabb gondolata az, hogy egy blokkrendszer olyan gazdag szimmetriákkal rendelkezik, hogy két sor ortogonalitása tulajdonképpen független azok választásától. Ha egy „kicsit" módosítjuk a blokkrendszerünket, akkor még kezelhető mennyiségű ortogonalitási feltételt kapunk, amelyeket jó eséllyel ki lehet majd elégíteni. A fejezetben prezentált három konstrukció olyannyira erősnek bizonyult, hogy a legtöbb ma ismert kis dimenziós ($n \leq 16$) komplex Hadamard mátrix származtatható belőle.

3.2. Komplex Hadamard mátrixok és blokkrendszerek

Ebben a fejezetben visszatérünk az 1.3.3 szekcióban ismertetett blokkrendszerek vizsgálatára. Adunk egy elégséges feltételt arra, hogy egy valós $2-(v,k,\lambda)$ blokkrendszerből mikor lehet egy $v \times v$-es komplex Hadamard mátrixot nyerni. Az alapgondolat az, hogy míg a valós esetben a $(4m-1, 2m-1, m-1)$ blokkrendszert még *kiegészítettük* egy további sorral és oszloppal, addig a komplex esetben ez nem feltétlenül szükséges, léteznek ugyanis $4m-1$ dimenziós komplex Hadamard mátrixok. A szakaszban feltesszük, hogy $\lambda < k < v$, hogy kizárjuk az elfajuló eseteket.

3.2.1. Definíció $(*)$**.** Azt mondjuk, hogy egy $v \times v$-es komplex Hadamard mátrix egy négyzetes $2-(v,k,\lambda)$ blokkrendszerből származik, ha ki lehet cserélni a blokkrendszerben lévő 0-k mindegyikét egy egységnyi abszolút értékű x komplex számra úgy, hogy egy komplex Hadamard mátrixhoz jussunk.

Némi előkészület következik.

3.2.2. Lemma. *Legyen H egy $v \times v$-es reguláris komplex Hadamard mátrix. Ekkor H valamely sor- illetve oszlopában lévő elemek összege abszolút értékben $\sqrt{v}$.*

Bizonyítás. Jelöljük σ-val H valamely sorában lévő elemek összegét. Ekkor H regularitása miatt $HJ = \sigma J$. Ezt megszorozva balról H^*-gal $H^*HJ = \sigma H^*J$ adódik, ahonnan kapjuk, hogy $vJ = |\sigma|^2 J$. Speciálisan: $|\sigma| = \sqrt{v}$. □

3.2.3. Tétel $(*)$**.** *Akkor és csak akkor létezik $2-(v,k,\lambda)$ blokkrendszerből származó komplex Hadamard mátrix, ha teljesül a*

$$\frac{v-\sqrt{v}}{2} \leq k \leq \frac{v+\sqrt{v}}{2} \tag{3.1}$$

egyenlőtlenség.

Bizonyítás. Tegyük fel, hogy van egy $2-(v,k,\lambda)$ négyzetes blokkrendszerünk, és tekintsük neki az A illeszkedési mátrixát. A blokkrendszer definíciója alapján nézhetjük, hogy valamely két sort tekintve hányszor fordul elő, hogy oszloponként két $+1$, vagy egy $+1$ és egy 0, végül két azonos 0 elem szerepel. Nyilván két $+1$ pontosan

λ koordinátán, egy $+1$ és egy 0 (a sorrend miatt) $2(k-\lambda)$ koordinátán, végül két 0 $v-2(k-\lambda)-\lambda = v+\lambda-2k$ koordinátán találkozik. Most cseréljük le a 0-kat egy ismeretlen x komplex számra, és válasszuk meg x értékét úgy, hogy teljesüljön az ortogonalitás. Speciálisan

$$\lambda + 2(k-\lambda)\Re[x] + v + \lambda - 2k = 0, \tag{3.2}$$

adódik, ahonnan rendezés, majd $k-\lambda \neq 0$-val való osztás, és a $\lambda = \frac{k(k-1)}{v-1}$ értékadás után kapjuk, hogy

$$\Re[x] = \frac{2k^2 - 2vk + v^2 - v}{2k(k-v)} = 1 - \frac{v(v-1)}{2k(v-k)}. \tag{3.3}$$

Világos, hogy innen x valós része nem lehet nagyobb, mint $+1$, kell még, hogy ne legyen kisebb, mint -1, vagyis

$$1 - \frac{v(v-1)}{2k(v-k)} \geq -1 \tag{3.4}$$

ahonnan már a kívánt (3.1) egyenlőtlenség adódik. A megfordítás nyilvánvaló, ekkor ugyanis $\Re[x] < -1$ volna, ami ellentmond a Hadamard-tulajdonságnak. □

A fenti tétel bizonyos értelemben vett megfordítása következik.

3.2.4. Tétel $(*)$**.** *Ha létezik egy olyan H $v\times v$-s komplex Hadamard mátrix, amely reguláris, és pontosan két különböző komplex szám szerepel benne, akkor ebből egy négyzetes $2-(v,k,\lambda)$ blokkrendszer származtatható.*

Bizonyítás. Ha H valós, akkor készen vagyunk, a származtatott renszer a jól ismert Menon-rendszer. Ha H komplex Hadamard mátrix, akkor feltehető, hogy benne kizárólag $+1$ és valamilyen, egységnyi abszolút értékű x szám szerepel. Célunk megmutatni, hogy ha x-et nullával helyettesítjük, akkor egy $2-(v,k,\lambda)$ blokkrendszert kapunk. Elsőként megmutatjuk, hogy a regularitásból az adódik, hogy a mátrixban minden sorban és minden oszlopban ugyanannyi $+1$ szerepel. Tegyük fel indirekt, hogy ez mégsem igaz, vagyis van egy olyan sor, amiben s db $+1$ és $(v-s)$ db x szerepel, továbbá van egy tőle különböző, amelyben t db $+1$ és $(v-t)$ db x szerepel. Felhasználva, hogy a mátrix reguláris, kapjuk, hogy

$$v = s^2 + (v-s)^2 + 2(v-s)\Re[x] \tag{3.5}$$

és

$$v = t^2 + (v-t)^2 + 2(v-t)\Re[x] \tag{3.6}$$

adódnak. A két egyenletet kivonva egymásból kapjuk, hogy

$$2(s-t)(s+t) - 2v(s-t) - 2\Re[x](s-t) = 0 \tag{3.7}$$

Innen végigosztva $2(s-t) \neq 0$-val kapjuk, hogy

$$\Re[x] = s + t - v \tag{3.8}$$

Speciálisan, $\Re[x]$ egész szám. Így $\Re[x] = 0$, vagyis (konjugálás erejéig) $x = \mathbf{i}$ adódik. Ez viszont megint nem lehet, ugyanis könnyen látszik, hogy két olyan sorvektor, amelyben kizárólag $+1$ és $\mathbf{i}$ szerepel nem tartalmazhat azonos koordinátán lévő $+1$-et illetve $\mathbf{i}$-t. Ebből kifolyólag az egyik vektor minden olyan koordinátán, ahol $+1$ van a másik vektorban $\mathbf{i}$-nek kell lennie, és fordítva. Mivel ilyen tulajdonságú ortogonális sorokból is összesen csak legfeljebb 2 lehet, kapjuk, hogy csupán 2×2-es Hadamard mátrix lehet az, amelyben $\Re[x] = \mathbf{i}$. Ilyenkor viszont $s = t$ adódik, ami ellentmondás. Kaptuk, hogy a regularitás maga után vonja azt, hogy H-ban minden sorban és minden oszlopban pontosan ugyannanyiszor fordul elő $+1$, a H-hoz hozzárendelt A illeszkedési mátrix tehát a szokásos értelemben reguláris, legyen a regularitás száma k.

A szokásos módon tekintsük H két sorát, és állapítsuk meg, hogy abban pontosan λ koordinátában találkoznak $+1$-ek, $2(k-\lambda)$ koordinátában az $1, x$ végül $v-2(k-\lambda)-\lambda$ koordinátán találkozik az x, x pár. Megmutatjuk, hogy ez a λ szám független a sorok választásától. Az ortogonalitás miatt

$$\lambda + 2(k-\lambda)\Re[x] + v - 2(k-\lambda) - \lambda = 0 \tag{3.9}$$

teljesül, ahonnan a $\Re[x] \neq 1$ természetes feltétel miatt

$$\lambda = k + \frac{v}{2(\Re[x]-1)} \tag{3.10}$$

Ezzel a bizonyítást befejeztük. □

14. *Megjegyzés.* Megjegyezzük, hogy az előbbi bizonyításból az is kijön, hogy

$$\Re[x] = \frac{v - 2k^2 - v^2 + 2kv}{2k(v-k)} = 1 - \frac{v(v-1)}{2k(v-k)}. \tag{3.11}$$

valamint, hogy tulajdonképpen nem meglepő módon

$$\lambda = \frac{k(k-1)}{v-1} \tag{3.12}$$

Ehhez semmi mást nem kell tenni, mint (3.5)-ben $s = k$ helyettesítést követően kifejezni $\Re[x]$-et, majd azt (3.10)-be behelyettesíteni.

Most a 3.2.3 tételt használva bebizonyítjuk a szakasz egyik fő eredményét.

3.2.5. Tétel $(*)$**.** *Ha van $4m$-ed rendű valós Hadamard mátrix, akkor ebből konstruálható egy $4m-1$-ed rendű komplex Hadamard mátrix.*

Bizonyítás. Legyen H egy valós Hadamard mátrix, és tekintsük a belőle származtatható $(4m-1, 2m-1, m-1)$ blokkrendszert. Ekkor azt kell igazolni, hogy a (3.1) egyenlőtlenség fennál, azaz

$$\frac{4m-1-\sqrt{4m-1}}{2} \leq 2m-1 \leq \frac{4m-1+\sqrt{4m-1}}{2} \tag{3.13}$$

fennáll, ami viszont triviális. Speciálisan, (3.11)-ből azt kapjuk, hogy

$$\Re[x] = 1 - \frac{(4m-1)(4m-2)}{2(2m-1)(4m-1-2m+1)} = 1 - \frac{4m-1}{2m} = -1 + \frac{1}{2m}. \tag{3.14}$$

és így

$$x = -1 + \frac{1}{2m} \pm \mathbf{i}\frac{\sqrt{4m-1}}{2m} \tag{3.15}$$

□

3.2.6. Definíció. A 3.2.5 tételből származó $n = 4m-1$-ed rendű komplex Hadamard mátrixokat U_n-nel jelöljük.

Fentebb igazoltuk tehát, hogy végtelen sok olyan struktúra van, amelyekből komplex Hadamard mátrix konstruálható. Felmerül azonban a kérdés, hogy van-e más, nem a Hadamard-rendszerből származó blokkrendszer, amely teljesíti a 3.2.3 tétel feltételeit? Másszóval: ismerünk-e további olyan struktúrát, amelyben $k \approx \frac{v}{2}$? A kérdésre nem könnyű felelni. A sztenderd referenciának számító *Handbook of Combinatorial Designs* könyv 21 szimmetrikus struktúra családot sorol fel, ezen kívül további 50 egyedi konstrukciót, amelyekből egy-egy konkrét struktúra kapható [16]. Áttanulmányozva ezeknek a struktúráknak a listáját azt láthatjuk, hogy az esetek zömében $k \approx \frac{v}{4}$, az egyedüli eset a Hadamard-rendszer mellett a Menon-rendszer, amely természetesen a valós Hadamard mátrixokat adná vissza. Ez a bizonytalanság motiválja a következő megválaszolatlan kérdéspárt:

3.2.7. Kérdés $(*)$**.** *Tudunk-e olyan, a Hadamard- és a Menon-rendszertől különböző kombinatorikus struktúrát mutatni, amelyből a 3.2.1 definíció értelmében komplex Hadamard mátrix származtatható? Lehet-e a 3.2.3 tétel állítását élesíteni?*

3.2.8. Példa. A fenti 3.2.5 tétel segítségével számos kis dimenziós komplex Hadamard mátrix meglétére adhatunk elméleti magyarázatot. Speciálisan, $n = 4$-re F_3, $n = 8$-ra a Fano-síkból C_{7A}, illetve a konjugáltja, C_{7B} adódik, $n = 12$-re a Paley-mátrixból C_{11A} és a konjugáltja, C_{11B} [82], végül $n = 16$-ra, valós ekvivalencia osztályonként legalább 1-1, azaz összesen legalább öt (!) új, eddig ismeretlen komplex Hadamard mátrixot konstruálhatunk. Illusztrációként álljon itt az $\mathcal{S}_4$ Sylvester-féle mátrixból

kapható mátrix:

$$U_{15} = \begin{bmatrix} 1 & x & x & 1 & 1 & x & x & 1 & 1 & x & x & 1 & 1 & x & x \\ x & 1 & x & 1 & x & 1 & x & 1 & x & 1 & x & 1 & x & 1 & x \\ x & x & 1 & 1 & x & x & 1 & 1 & x & x & 1 & 1 & x & x & 1 \\ 1 & 1 & 1 & x & x & x & x & 1 & 1 & 1 & 1 & x & x & x & x \\ 1 & x & x & x & x & 1 & 1 & 1 & 1 & x & x & x & x & 1 & 1 \\ x & 1 & x & x & 1 & x & 1 & 1 & x & 1 & x & x & 1 & x & 1 \\ x & x & 1 & x & 1 & 1 & x & 1 & x & x & 1 & x & 1 & 1 & x \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & x & x & x & x & x & x & x & x \\ 1 & x & x & 1 & 1 & x & x & x & x & 1 & 1 & x & x & 1 & 1 \\ x & 1 & x & 1 & x & 1 & x & x & 1 & x & 1 & x & 1 & x & 1 \\ x & x & 1 & 1 & x & x & 1 & x & 1 & 1 & x & x & 1 & 1 & x \\ 1 & 1 & 1 & x & x & x & x & x & x & x & x & 1 & 1 & 1 & 1 \\ 1 & x & x & x & x & 1 & 1 & x & x & 1 & 1 & 1 & 1 & x & x \\ x & 1 & x & x & 1 & x & 1 & x & 1 & x & 1 & 1 & x & 1 & x \\ x & x & 1 & x & 1 & 1 & x & x & 1 & 1 & x & 1 & x & x & 1 \end{bmatrix}, x = -\frac{7}{8} + \mathbf{i}\frac{\sqrt{15}}{8} \tag{3.16}$$

Sztenderd érvelés mutatja, hogy az U_{15} mátrix nem szerepel a Tadej–Życzkowski katalógusban:

3.2.9. Lemma $(*)$**.** *U_{15} inekvivalens mátrix minden eddig ismert 15×15-ös komplex Hadamard mátrixtól.*

Bizonyítás. Jelenleg egyetlen 15×15-ös komplex Hadamard mátrixcsalád található a TZ-katalógusban, ez pedig $F_{15}^{(8)}$. Könnyen látszik, hogy a nyolcparaméteres család minden egyes mátrixának a Haagerup-féle Λ halmazában megtalálható pl. a $w = \mathbf{e}^{\frac{2\pi\mathbf{i}}{5}}$ komplex 5-ik egységgyök. Ez viszont világos, hogy nincs benne U_{15} invariáns halmazában, hiszen az nem más, mint $\Lambda_{U_{15}} = \{1, x, x^2, \overline{x}, \overline{x}^2\}$. □

15. *Megjegyzés.* Nem tudni, hogy a U_{15} mátrix ekvivalens-e a konjugáltjával, a Haagerup invariáns halmazuk ugyanis azonos.

A fenti 3.2.5 tételből nagyon fontos, ciklikus komplex Hadamard mátrixok adódnak.

3.2.10. Következmény. *Tegyük fel, hogy létezik egy $n = 4m$ rendű, ciklikus maggal rendelkező valós Hadamard mátrix. Ekkor van $4m - 1$ dimenziós ciklikus komplex Hadamard mátrix is.*

Mivel abban az esetben, ha $n = 4m - 1$ prím, akkor a Paley-konstrukció szolgáltat ilyen mátrixot, kapjuk Munemasa és Watatani eredményét:

3.2.11. Következmény (Munemasa–Watatani, [58])**.** *Ha $n = 4m - 1$ prím, akkor létezik a Fourier mátrixtól inekvivalens n-edrendű ciklikus komplex Hadamard mátrix.*

3.3. Egy szemtelen általánosítás

Ebben a fejezetben a 3.2.5 tételnek egy igen jelentős általánosítása következik. Az alapgondolat az volt, hogy ha bizonyos extra szimmetria tulajdonságokat teszünk fel egy Hadamard-rendszerre, akkor két különböző elem segítsége helyett *három* különböző elem felhasználásával komplex Hadamard mátrixot tudunk gyártani. Az első gondolat természetesen a szimmetrikus, konstans diagonálisú mátrixok vizsgálata. Ezek az extra feltételek azt biztosítják, hogy még így is viszonylag kevés ortogonalitási feltételelünk lesz. Sajnos azonban viszonylag ritkák a szimmetrikus, konstans diagonálisú valós Hadamard mátrixok. Éppen ezért gondolunk egy nagyot, és egyszerűen eldobjuk azt a feltételt, hogy a diagonális konstans legyen, és csak a szimmetriát tartjuk meg, vállalva a négy különböző elem fellépésével adódó nehézségeket. Ezzel a konstrukcióval bővítjük az újra felfedezett kis dimenziós komplex Hadamard mátrixok listáját, többek között Petrescu híres, 7 dimenziós mátrixa is megjelnik, ezen felül további öt új 15 dimenziós mátrixszal egészítjük ki Życzkowskiék listáját. A szakasz fő eredménye a következő:

3.3.1. Tétel $(*)$**.** *Tegyük fel, hogy létezik egy szimmetrikus, $n = 4m \geq 8$ dimenziós valós Hadamard mátrix. Ekkor ebből egy olyan $4m-1$ dimenziós komplex Hadamard mátrix nyerhető, amelynek négy különböző eleme van, s amelyek mindegyike benne van a $\mathbb{Q}[i\sqrt{4m-5}]$ testben.*

A bizonyítás előtt tisztáznunk kell két nagyon fontos dolgot:

3.3.2. Lemma. *Akkor és csak akkor van valós, szimmetrikus Hadamard mátrix, ha normalizált is van.*

Bizonyítás. Legyen H egy valós, szimmetrikus Hadamard mátrix. Ha H első sorának első eleme -1, akkor tekintsük $-H$-t, amely az 1.3.3 lemma miatt szintén Hadamard, továbbá szintén szimmetrikus mátrix. Ezt követően tekintsük H vagy $-H$ közül azt, amelyikben az első sor első eleme már $+1$, és azon sorait és oszlopait, amelyek első eleme -1, szorozzuk be -1-gyel. Így egy normalizált Hadamard mátrixot nyerünk. Az állítás megfordítása világos. □

3.3.3. Sejtés (Lin–Wallis, [16])**.** *Ha létezik n-edrendű valós Hadamard mátrix, akkor olyan is van, amely ekvivalens egy szimmetrikus Hadamard mátrixszal.*

16. *Megjegyzés.* A fenti 3.3.3 sejtést $n = 88$-ig igazolták, a legkisebb eldöntetlen dimenzió tehát a 92 [16].

A 3.3.1 tétel bizonyítása. A bizonyítás egy hosszú számolás. Tegyük fel tehát, hogy van egy $n = 4m$ dimenziós, valós szimmetrikus Hadamard mátrixunk. A mátrix normalizálását követően a 3.3.2 lemma miatt még mindig szimmetrikus mátrixot kapunk.

Hagyjuk most el a mátrix első sorát és oszlopát, majd végezzük el a következő helyettesítést: A főátlóban a -1-eket cseréljük le x-re, a mátrix főátlón kívüli $+1$-eit y-nal, még a -1-eit z-re cseréljük le, a főátlóban a $+1$-eket pedig ne változtassuk meg. Ezen transzformációt követően egy $\{1, x, y, z\}$ mátrixot kapunk. A következőkben feltérképezzük, hogy milyen ortogonalitási feltételeknek kell teljesülniük annak érdekében, hogy egy komplex Hadamard mártixot kapjunk.

Mielőtt hozzákezdenénk az esetszétválasztáshoz, előre bocsájtanánk a következőt. Ha tekintjük H bármely két sorát, akkor a sorok és oszlopok permutációját követően feltehetjük, hogy a két sor a következő alakot ölti:

$$\left[\begin{array}{cc|cccc} 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 & 1 & -1 \\ \hline & & c & 2k-3-c & 2k-3-c & c+3 \end{array}\right], \quad \left[\begin{array}{cc|cccc} x & 1 & 1 & 1 & z & z \\ 1 & x & 1 & z & 1 & z \end{array}\right] \tag{3.17}$$

Itt a két blokkmátrix közül a bal oldali az *eredeti*, valós Hadamard-rendszer két sorát reprezentálja, még a jobb oldalon a konvenciónknak megfelelő módon transzformált, már komplex elemekkel feltöltött képe látható. A bal oldali mátrix harmadik sorában a jobb áttekinthetőség kedvéért a felette lévő, tisztán $+1$ vagy -1-ekből álló blokkok méretét jeleztük. A bal felső 2×2-es részmátrix természetesen négy, egyenként 1-1 elemből álló blokkot tartalmaz.

Az esetszétválasztás aszerint megy, hogy egyrészt milyen elemek vannak a két általunk választott sor diagonálisában, illetve, hogy milyen (azonos!) elempár van a bal fölső részmátrix off-diagonális helyein. Ezek alapján összesen legfeljebb 8 ortogonalitási egyenletünk lesz: 4 féleképpen választhatjuk a diagonál elemeket, és mindegyik választáshoz még $2-2$ választás a diagonál elemek sarkaira. Azonban jogunk van a mátrix valamely két sorát permutálni, ezáltal két esetet megúszni. Összességében tehát 6 db ortogonalitási egyenletet kell kapnunk.

ELSŐ ESET: $(+1, +1, +1)$

Tegyük fel, hogy az általunk kiválasztott két sor a következő alakú. A diagonálisban mindkét sorban, valamint az off-diagonál helyeken is $+1$ áll. Jelöljük c_1-gyel azt, hogy a két sor mindegyikében összesen hány oszlopban található mindkét koordinátán $+1$. Ennek segítségével már megkapható, hogy hány olyan koordináta van, amelyben az első sorban $+1$, a másodikban pedig -1 áll, mégpedig a következőképpen: eredetileg összesen $2m-1$ db $+1$ szerepelt a mátrix bármely sorában, ebből kettő már az első két koordinátán áll, c_1 az első blokkban, így aztán a második blokkba $2m-1-2-c_1$ db van összesen. Teljesen hasonló okfejtéssel, csak most a második sort nézve, ugyanígy adódik, hogy a harmadik blokkban $2m-1-2-c_1$ db egyes szerepelhet. Végül a negyedik blokk kitöltéséhez használjuk fel, hogy egy sorban $2m$ db -1 szerepel, amelyekből már (mindkét sorban) $2m-3-c_1$-t felhasználtunk, így tehát ebből c_1+3 kell legyen.

Ezeket a számokat tüntettük fel a jobb áttekinthetőség kedvéért a bal oldali mátrix harmadik sorában. A jobb oldali mátrix – mint azt már írtuk – azt mutatja, hogy milyen transzformációt hajtottunk végre az eredeti Hadamard-rendszer elemein.

$$\left[\begin{array}{cc|cccc} 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 & 1 & -1 \\ \hline & & c_1 & 2m-3-c_1 & 2m-3-c_1 & c_1+3 \end{array}\right], \quad \left[\begin{array}{cc|cccc} x & 1 & 1 & 1 & z & z \\ 1 & x & 1 & z & 1 & z \end{array}\right] \tag{3.18}$$

Az első feladat c_1 meghatározása, ezt onnan tudjuk kiszámolni, hogy felírjuk a bal oldali mátrixra a kvázi-ortogonalitási egyenletet; a kvázi előtag amiatt van, hogy mivel elhagytuk az első $+1$ koordinátákat a Hadamard-mátrixunkból, a megmaradó Hadamard-rendszerben természetesen bármely két sor skalárszorzata -1 lesz.

$$2 + c_1 - 2(2m - 3 - c_1) + c_1 + 3 = -1 \tag{3.19}$$

Innen $c_1 = m - 3$ adódik. Itt rögtön megjegyezzük, hogy ennek az esetnek csak akkor van jelentősége, ha $m \geq 3$. Most, hogy c_1 értékét már meghatároztuk, felírhatjuk a transzformált mátrixban lévő, itt már valódi ortogonalitási egyenletet:

$$2\Re[x] + c_1 + 2(2m - 3 - c_1)\Re[z] + c_1 + 3 = 0 \tag{3.20}$$

ahonnan

$$2m\Re[z] + 2\Re[x] + 2m - 3 = 0 \tag{3.21}$$

adódik. Ez az első esethez tartozó ortogonalitási egyenlet.

MÁSODIK ESET: $(+1, +1, -1)$

Most is, mint az első esetben, a célunk, hogy feltérképezzük, hogy hány közös koordinátán vannak $+1$-ek a két mátrixban. Ezt a számot ezúttal c_2-vel jelöltük. Az eset diagramja az alábbi:

$$\left[\begin{array}{cc|cccc} 1 & -1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 & 1 & -1 \\ \hline & & c_2 & 2m-2-c_2 & 2m-2-c_2 & c_2+1 \end{array}\right], \quad \left[\begin{array}{cc|cccc} x & z & 1 & 1 & z & z \\ z & x & 1 & z & 1 & z \end{array}\right] \tag{3.22}$$

A kvázi-ortogonalitási egyenlet most a következő.

$$-2 + c_2 - 2(2m - 2 - c_2) + c_2 + 1 = -1 \tag{3.23}$$

Innen $c_2 = m - 1$ adódik. A transzformált mátrixban lévő ortogonalitási egyenlet:

$$2\Re[x\overline{z}] + c_2 + 2(2m - 2 - c_2)\Re[z] + c_2 + 1 = 0 \tag{3.24}$$

ahonnan

$$2(m-1)\Re[z] + 2\Re[x\overline{z}] + 2m - 1 = 0 \tag{3.25}$$

adódik. Ez a második ortogonalitási egyenlet.

HARMADIK ESET: $(+1,-1,+1)$

Most is, mint az első esetben, a célunk, hogy feltérképezzük, hogy hány közös koordinátán vannak $+1$-ek a két mátrixban. Ezt a számot ezúttal c_3-vel jelöltük. Az eset diagramja az alábbi:

$$\left[\begin{array}{cc|cccc} 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 \\ \hline & & c_3 & 2m-3-c_3 & 2m-2-c_3 & c_3+2 \end{array}\right], \quad \left[\begin{array}{cc|cccc} x & 1 & 1 & 1 & z & z \\ 1 & y & 1 & z & 1 & z \end{array}\right] \tag{3.26}$$

A kvázi-ortogonalitási egyenlet most a következő.

$$c_3 - (2m-3-c_3) - (2m-2-c_3) + c_3 + 2 = -1 \tag{3.27}$$

Innen $c_3 = m-2$ adódik. A transzformált mátrixban lévő ortogonalitási egyenlet:

$$x + \overline{y} + c_3 + (2m-3-c_3)\overline{z} + (2m-2-c_3)z + c_3 + 2 = 0 \tag{3.28}$$

ahonnan

$$2m\Re[z] + x + \overline{y} - \overline{z} + 2m - 2 = 0 \tag{3.29}$$

adódik. Ez a harmadik ortogonalitási egyenlet.

NEGYEDIK ESET: $(+1,-1,-1)$

Most is, mint az első esetben, a célunk, hogy feltérképezzük, hogy hány közös koordinátán vannak $+1$-ek a két mátrixban. Ezt a számot ezúttal c_4-gyel jelöltük. Az eset diagramja az alábbi:

$$\left[\begin{array}{cc|cccc} 1 & -1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 & 1 & -1 \\ \hline & & c_4 & 2m-2-c_4 & 2m-1-c_4 & c_4 \end{array}\right], \quad \left[\begin{array}{cc|cccc} x & z & 1 & 1 & z & z \\ z & y & 1 & z & 1 & z \end{array}\right] \tag{3.30}$$

A kvázi-ortogonalitási egyenlet most a következő.

$$c_4 - (2m-2-c_4) - (2m-1-c_4) + c_4 = -1 \tag{3.31}$$

Innen $c_4 = m-1$ adódik. A transzformált mátrixban lévő ortogonalitási egyenlet:

$$x\overline{z} + z\overline{y} + c_4 + (2m-2-c_4)\overline{z} + (2m-1-c_4)z + c_4 = 0 \tag{3.32}$$

ahonnan

$$2m\Re[z] + x\overline{z} + z\overline{y} - \overline{z} + 2m - 2 = 0 \tag{3.33}$$

adódik. Ez a negyedik ortogonalitási egyenlet.

ÖTÖDIK ESET: $(-1,-1,+1)$

Most is, mint az első esetben, a célunk, hogy feltérképezzük, hogy hány közös koordinátán vannak $+1$-ek a két mátrixban. Ezt a számot ezúttal c_5-gyel jelöltük. Az eset diagramja az alábbi:

$$\left[\begin{array}{cc|cccc} -1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 \\ \hline & & c_5 & 2m-2-c_5 & 2m-2-c_5 & c_5+1 \end{array}\right], \quad \left[\begin{array}{cc|cccc} y & 1 & 1 & 1 & z & z \\ 1 & y & 1 & z & 1 & z \end{array}\right] \tag{3.34}$$

A kvázi-ortogonalitási egyenlet most ugyanaz, mint a második esetben.

$$-2+c_5-2(2m-2-c_5)+c_5+1=-1 \tag{3.35}$$

Innen $c_5=m-1$ adódik. A transzformált mátrixban lévő ortogonalitási egyenlet:

$$2\Re[y]+c_5+2(2m-2-c_5)\Re[z]+c_5+1=0 \tag{3.36}$$

ahonnan

$$2(m-1)\Re[z]+2\Re[y]+2m-1=0 \tag{3.37}$$

adódik. Ez az ötödik ortogonalitási egyenlet.

HATODIK ESET: $(-1,-1,-1)$

Most is, mint az első esetben, a célunk, hogy feltérképezzük, hogy hány közös koordinátán vannak $+1$-ek a két mátrixban. Ezt a számot ezúttal c_6-tal jelöltük. Az eset diagramja az alábbi:

$$\left[\begin{array}{cc|cccc} -1 & -1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 & 1 & -1 \\ \hline & & c_6 & 2m-1-c_6 & 2m-1-c_6 & c_6-1 \end{array}\right], \quad \left[\begin{array}{cc|cccc} y & z & 1 & 1 & z & z \\ z & y & 1 & z & 1 & z \end{array}\right] \tag{3.38}$$

A kvázi-ortogonalitási egyenlet most ugyanaz, mint a második esetben.

$$2+c_6-2(2m-1-c_6)+c_6-1=-1 \tag{3.39}$$

Innen $c_6=m-1$ adódik. A transzformált mátrixban lévő ortogonalitási egyenlet:

$$2\Re[y\overline{z}]+c_6+2(2m-1-c_6)\Re[z]+c_6-1=0 \tag{3.40}$$

ahonnan

$$2m\Re[z]+2\Re[y\overline{z}]+2m-3=0 \tag{3.41}$$

adódik. Ez a hatodik ortogonalitási egyenlet.

A hátralévő két eset, nevezetesen a $(-1,+1,+1)$ és $(-1,+1,-1)$ a harmadik és negyedik esettel lényegében azonos. A számolás során a megfelelő ortogonalitási egyenletek *konjugáltjai* jönnek be. Most rátérünk a fenti (3.21)-(3.41) egyenletek megoldására.

A (3.37) egyenletből egyrészt

$$\Re[y] = -\left((m-1)\Re[z] + \frac{2m-1}{2}\right) \tag{3.42}$$

másrészt (3.41) szerint, felhasználva, hogy $\Re[ab] = \Re[a]\Re[b] - \Im[a]\Im[b]$, kapjuk, hogy

$$2m\Re[z] + 2\Re[y]\Re[z] + 2\Im[y]\Im[z] + 2m - 3 = 0 \tag{3.43}$$

Most felhasználva, hogy y és z egységnyi abszolút értékű, továbbá, hogy konjugálás erejéig feltehető, hogy $\Im[z] \geq 0$ kapjuk, hogy

$$(2m-2)\Re[z]^2 - \Re[z] - 2m + 3 = \pm 2\sqrt{1 - \left((m-1)\Re[z] + \frac{2m-1}{2}\right)^2}\sqrt{1-\Re[z]^2} \tag{3.44}$$

ahonnan négyzetre emelést követően a

$$\left(8m^2-8m\right)\Re[z]^3 + \left(8m^2-16m+4\right)\Re[z]^2 + \left(-8m^2+8m+2\right)\Re[z] - 8m^2 + 16m - 6 = 0 \tag{3.45}$$

harmadfokú egyenlet adódik. A 3.2.5 tételből tudjuk, hogy ennek *garantáltan* megoldása a $\Re[z_1] = -1 + \frac{1}{2m}$, és innen a többi megoldás is egyszerű számolással adódik: $\Re[z_2] = 1$, $\Re[z_3] = -1 + \frac{1}{2m-2}$. Ha $z_2 = 1$, akkor (3.42) miatt könnyen látszik, hogy csakis $m = 1$ lehet, ezt viszont kizártuk. Marad tehát a két további, releváns eset:

Tegyük fel, hogy $z = z_1 = -1 + \frac{1}{2m} + \mathbf{i}\frac{\sqrt{4m-1}}{2m}$. Ekkor (3.42) miatt $y = -1 + \frac{1}{2m} \pm \mathbf{i}\frac{\sqrt{4m-1}}{2m}$. El kell döntenünk, hogy y milyen előjelet kap valójában, ebben a (3.43)-ba való visszahelyettesítés segít, ahonnan

$$2m\left(-1+\frac{1}{2m}\right) + 2\left(-1+\frac{1}{2m}\right)^2 + 2\frac{\sqrt{4m-1}}{2m}\Im[z] + 2m - 3 = 0, \tag{3.46}$$

és így $\Im[z] = \frac{\sqrt{4m-1}}{2m}$ adódik, azaz valójában $z = y$. Hátra van x értékének a meghatározása. Ehhez a negyedik esethez tartozó (3.33) egyenletbe kell behelyettesíteni:

$$2m\left(-1+\frac{1}{2m}\right) + x\overline{z} + 1 - \overline{z} + 2m - 2 = 0, \tag{3.47}$$

ahonnan $x = 1$ adódik. Tehát ebben az esetben teljes egészében visszakaptuk a 3.2.5 tétel által nyújtott konstrukciót.

Végül tegyük fel, hogy $z = z_2 = -1 + \frac{1}{2m-2} + \mathbf{i}\frac{\sqrt{4m-5}}{2m-2}$. Ekkor (3.42) miatt $y = -1$. Végül x értékét újfent a (3.33)-ba való behelyettesítéssel határozzuk meg:

$$2m\left(-1+\frac{1}{2m-2}\right) + x\overline{z} + z - \overline{z} + 2m - 2 = 0, \tag{3.48}$$

ahonnan rövid számolás után $x = -z$ adódik.

Hátra van még annak az ellenőrzése, hogy az így kapott $\{1, z, -1, -z\}$ elemekből álló mátrix valóban teljesíti az összes ortogonalitási feltételt. Ezt a számolást az olvasóra bízzuk. □

Összefoglalva a fenti konstrukciót, elmondhatjuk a következőt.

3.3.4. Következmény. *Tegyük fel, hogy van egy valós szimmetrikus $n = 4m \geq 8$-ad rendű valós Hadamard mátrixunk. Ekkor normalizáljuk le, majd hagyjuk el az első sorát és oszlopát. Ezt követően a 3.3.1 tételnek megfelelően a mátrix minden $+1$ fődiagonális elemét cseréljük le az $x = 1 - \frac{1}{2m-2} \pm \boldsymbol{i}\frac{\sqrt{4m-5}}{2m-2}$ számra, végül a mátrix nemfődiagonál -1 elemeit $-x$-re. Ekkor egy $4m-1$-ed rendű komplex Hadamard mártixot kapunk.*

3.3.5. Definíció. A 3.3.1 tételből származó $n = 4m - 1$ dimenziós, a $\mathbb{Q}[\mathbf{i}\sqrt{4m-5}]$ test elemeiből álló komplex Hadamard mátrixokat V_n-nel jelöljük.

3.3.6. Példa. $n = 8$-ra vehetjük az $\mathcal{S}_3$ Sylvester-féle mátrixot, amely nyilvánvalóan szimmetrikus. Ha végrehajtjuk rajta a 3.3.4 következmény által adott konstrukciót, akkor Petrescu 7×7-es P_7 [82], [64], [5], a 3.2.5 tétel által adott konstrukcióval pedig a már megismert C_{7A} és C_{7B} mátrixokat (lásd 29. oldal) kapjuk. Legyen tehát $\{x, y, z\} = \{\frac{1}{2} + \mathbf{i}\frac{\sqrt{3}}{2}, -1, -\frac{1}{2} - \mathbf{i}\frac{\sqrt{3}}{2}\}$. Ekkor az alábbi $V_7 \cong P_7$ mátrix Hadamard.

$$H_8 = \left[\begin{array}{c|cccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{array}\right], V_7 = \left[\begin{array}{ccccccc} x & z & z & 1 & 1 & z & z \\ z & x & z & 1 & z & 1 & z \\ z & z & x & 1 & z & z & 1 \\ 1 & 1 & 1 & y & z & z & z \\ 1 & z & z & z & y & 1 & 1 \\ z & 1 & z & z & 1 & y & 1 \\ z & z & 1 & z & 1 & 1 & y \end{array}\right] \tag{3.49}$$

A következőkben igazoljuk, hogy a TZ-katalógusban szereplő $N_{11A}^{(0)}$ mátrix megkapható a 3.3.4 konstrukció segítségével.

3.3.7. Példa. A 16. megjegyzés miatt létezik $n = 12$-re valós szimmetrikus Hadamard márix. Természetes konstrukció nem lévén, számítógéppel generáltuk egy ilyen mátri-

xot, majd a 3.3.4 konstrukció végrehajtását követően az alábbi mátrixhoz jutottunk.

$$V_{11} = \begin{bmatrix} a & -a & -a & -a & -a & -a & -a & 1 & 1 & 1 & 1 \\ -a & -1 & 1 & 1 & 1 & -a & -a & -a & -a & 1 & 1 \\ -a & 1 & -1 & 1 & 1 & -a & -a & 1 & 1 & -a & -a \\ -a & 1 & 1 & -1 & -a & -a & 1 & 1 & -a & -a & 1 \\ -a & 1 & 1 & -a & -1 & 1 & -a & -a & 1 & 1 & -a \\ -a & -a & -a & -a & 1 & a & 1 & -a & 1 & -a & 1 \\ -a & -a & -a & 1 & -a & 1 & a & 1 & -a & 1 & -a \\ 1 & -a & 1 & 1 & -a & -a & 1 & -1 & 1 & -a & -a \\ 1 & -a & 1 & -a & 1 & 1 & -a & 1 & -1 & -a & -a \\ 1 & 1 & -a & -a & 1 & -a & 1 & -a & -a & a & -a \\ 1 & 1 & -a & 1 & -a & 1 & -a & -a & -a & -a & a \end{bmatrix}, a = \frac{3}{4} + \mathbf{i}\frac{\sqrt{7}}{4} \quad (3.50)$$

Legyenek most

$$P_1 = [e_1, e_2, e_3, e_4, e_5, e_7, e_6, e_8, e_9, e_{11}, e_{10}] \quad (3.51)$$

valamint

$$P_2 = [e_1, e_2, e_3, e_5, e_4, e_6, e_7, e_9, e_8, e_{10}, e_{11}] \quad (3.52)$$

permutációs-, továbbá

$$D = \mathrm{Diag}\,(-1, 1, 1, 1, 1, 1, 1, -\overline{a}, -\overline{a}, -\overline{a}, -\overline{a}) \quad (3.53)$$

unitér diagonális mátrixok. Ekkor

$$N_{11A}^{(0)} = aDP_1\overline{V}_{11}P_2D \quad (3.54)$$

Végezetül adunk egy példát egy 15×15-ös mátrixra.

3.3.8. Példa. $V_{15} =$

$$\begin{bmatrix} -1 & 1 & -x & 1 & -x & 1 & -x & 1 & -x & 1 & -x & 1 & -x & 1 & -x \\ 1 & -1 & -x & 1 & 1 & -x & -x & 1 & 1 & -x & -x & 1 & 1 & -x & -x \\ -x & -x & x & 1 & -x & -x & 1 & 1 & -x & -x & 1 & 1 & -x & -x & 1 \\ 1 & 1 & 1 & -1 & -x & -x & -x & 1 & 1 & 1 & 1 & -x & -x & -x & -x \\ -x & 1 & -x & -x & x & -x & 1 & 1 & -x & 1 & -x & -x & 1 & -x & 1 \\ 1 & -x & -x & -x & -x & x & 1 & 1 & 1 & -x & -x & -x & -x & 1 & 1 \\ -x & -x & 1 & -x & 1 & 1 & -1 & 1 & -x & -x & 1 & -x & 1 & 1 & -x \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -x & -x & -x & -x & -x & -x & -x \\ -x & 1 & -x & 1 & -x & 1 & -x & -x & x & -x & 1 & -x & 1 & -x & 1 \\ 1 & -x & -x & 1 & 1 & -x & -x & -x & -x & x & 1 & -x & -x & 1 & 1 \\ -x & -x & 1 & 1 & -x & -x & 1 & -x & 1 & 1 & -1 & -x & 1 & 1 & -x \\ 1 & 1 & 1 & -x & -x & -x & -x & -x & -x & -x & -x & x & 1 & 1 & 1 \\ -x & 1 & -x & -x & 1 & -x & 1 & -x & 1 & -x & 1 & 1 & -1 & 1 & -x \\ 1 & -x & -x & -x & -x & 1 & 1 & -x & -x & 1 & 1 & 1 & 1 & -1 & -x \\ -x & -x & 1 & -x & 1 & 1 & -x & -x & 1 & 1 & -x & 1 & -x & -x & x \end{bmatrix}, x = \frac{5}{6} + \mathbf{i}\frac{\sqrt{11}}{6} \quad (3.55)$$

3.3.9. Lemma. *V_{15} nem szerepel a TZ-katalógusban.*

Bizonyítás. A TZ-katalógusban csakis az $F_{15}^{(8)}$ Fourier mátrix szerepel 15 dimenzióban. Ezen mátrixok mindegyikének Λ invariáns halmaza tartalmazza az ω komplex harmadik egységgyököt, V_{15} invariáns halmaza viszont nem. Az, hogy V_{15} inkekvivalens a korábbi, U_{15} mátrixtól onnan következik, hogy elemeik a racionális számtest különböző másodfokú algebrai bővítésében szerepelnek. □

17. *Megjegyzés.* Természetesnek hat az ötlet, hogy a szimmetrikus mátrixok helyett inkább a ferdén szimmetrikusakat tekintsük, ekkor ugyanis további két ortogonalitási egyenlettel kevesebb lesz, és reménykedhetünk benne, hogy hátha szabad paraméterek maradnak a kezünkben, amelyek segítségével végtelen sok mátrixot konstruálhatnánk egy adott n-re. Sajnos azonban – mint azt ellenőriztük – ez a vizsgálati irány nem vezet el további új mátrixokhoz.

3.4. Újra konferencia mátrixok

Az előző két fejezetben eljárást mutattunk arra, hogy ha $n \equiv 3 \mod 4$, akkor miként lehet az Hadamard-struktúrából $n = 4m - 1$-ed rendű komplex Hadamard mátrixokat konstruálni. A szerző [81]-ben szimmetrikus konferencia mátrixokat vizsgált, és segítségükkel paraméteres komplex Hadamard mátrixokat konstruált. Ebben a fejezetben még egyszer elővesszük a szimmetrikus konferencia mátrixokat, amelyek belső strukturális szimmetriáit kihasználva új, $n = 4m+1$ dimenziós komplex Hadamard mátrixokat gyártunk.

A szakaszban új 9 dimenziós komplex Hadamard mátrixot konstruálunk a következő tétel segítségével.

3.4.1. Tétel $(*)$**.** *Tegyük fel, hogy létezik egy $n = 4m + 2 \geq 6$-od rendű szimmetrikus konferencia mátrix. Ekkor konstruálható olyan $4m + 1$-ed rendű komplex Hadamard mátrix, amelyben összesen 3 különböző elem van, melyek mindegyike benne van a racionális test egy legfeljebb negyedfokú algebrai bővítésében.*

Bizonyítás. A bizonyítás hasonló a 3.2.5 tételéhez: első lépésként lenormalizáljuk a konferencia mátrixunkat, majd eldobjuk az első sorát és oszlopát. Ezt követően a megmaradt, $4m + 1 \times 4m + 1$ mátrixban a fődiagonálisban a 0-kat lecseréljük $+1$-gyé (ezt mindig megtehetjük, hiszen az utólag kapott komplex Hadamard mátrix minden sorát végigszorozhatjuk majd úgy, hogy a fődiagonálisba $+1$-et kapjunk). Ezt követően a fődiagonálison kívül lévő $+1$ és -1 elemeket cseréljük le a most még ismeretlen x és y változókra. A célunk feltérképezni, hogy milyen ortogonalitási feltételeknek kell teljesülniük ahhoz, hogy íly módon egy komplex Hadamard mátrixot kapjunk.

Vegyük észre, hogy bármely két sort is vesszük, permutálgatás után azok a következő két kanonikus alak valamelyikére hozhatóak:

ELSŐ ESET: $(0,0,1)$

A 3.3.1 tétel bizonyításához hasonlóan először a célunk feltérképezni, hogy hány közös koordinátán vannak $+1$-ek a két mátrixban. Ezt a számot ezúttal d_1-tal jelöltük. Az eset diagramja az alábbi:

$$\left[\begin{array}{cc|cccc} 0 & 1 & 1 & 1 & -1 & -1 \\ 1 & 0 & 1 & -1 & 1 & -1 \\ \hline & & d_1 & 2m-1-d_1 & 2m-1-d_1 & d_1+1 \end{array}\right], \quad \left[\begin{array}{cc|cccc} 1 & x & x & x & y & y \\ x & 1 & x & y & x & y \end{array}\right] \tag{3.56}$$

A kvázi-ortogonalitási egyenlet a következő:

$$d_1 - 2(2m-1-d_1) + d_1 + 1 = -1 \tag{3.57}$$

Innen $d_1 = m-1$ adódik. A transzformált mátrixban lévő ortogonalitási egyenlet:

$$2\Re[x] + d_1 + 2(2m-1-d_1)\Re[x\overline{y}] + d_1 + 1 = 0 \tag{3.58}$$

ahonnan

$$2\Re[x] + 2m\Re[x\overline{y}] + 2m - 1 = 0. \tag{3.59}$$

Ez az első ortogonalitási egyenlet.

MÁSODIK ESET: $(0,0,-1)$

A másik lényegi rész az, amikor a diagonálelemekkel párban -1-ek állnak. Hasonlóan, mint az előbb, először d_2 meghatározása a cél. Az eset diagramja az alábbi:

$$\left[\begin{array}{cc|cccc} 0 & -1 & 1 & 1 & -1 & -1 \\ -1 & 0 & 1 & -1 & 1 & -1 \\ \hline & & d_2 & 2m-d_2 & 2m-d_2 & d_2-1 \end{array}\right], \quad \left[\begin{array}{cc|cccc} 1 & y & x & x & y & y \\ y & 1 & x & y & x & y \end{array}\right] \tag{3.60}$$

A kvázi-ortogonalitási egyenlet a következő:

$$d_2 - 2(2m-d_2) + d_2 - 1 = -1 \tag{3.61}$$

Innen $d_2 = m$ adódik. A transzformált mátrixban lévő ortogonalitási egyenlet:

$$2\Re[y] + d_2 + 2(2m-d_2)\Re[x\overline{y}] + d_2 - 1 = 0 \tag{3.62}$$

ahonnan

$$2\Re[y] + 2m\Re[x\overline{y}] + 2m - 1 = 0. \tag{3.63}$$

Ez a második ortogonalitási egyenlet.

Most megoldjuk ezeket az egyenleteket. Azonnal adódik (3.59) és (3.62)-ből, hogy $\Re[x] = \Re[y]$, és innen – nyilvánvaló okokból – $y = \overline{x}$ adódik. $x = y$ nem lehet, mert

akkor túl sok egyforma eleme lenne a mátrixnak, ezáltal nem teljesülhetne az ortogonalitás. Ezt, valamint az $|x| = 1$ miatti $\Re[x^2] = 2\Re[x]^2 - 1$ összefüggést felhasználva kapjuk, hogy

$$2\Re[x] + 2m\left(2\Re[x]^2 - 1\right) + 2m - 1 = 0 \tag{3.64}$$

$$4m\Re[x]^2 + 2\Re[x] - 1 = 0 \tag{3.65}$$

ahonnan

$$\Re[x]_{1,2} = \frac{-1 \pm \sqrt{4m+1}}{4m} = -\frac{1}{4m} \pm \frac{\sqrt{4m+1}}{4m} \tag{3.66}$$

Könnyen ellenőrizhető, hogy x egységnyi abszolút értékű komplex számmá tehető. □

3.4.2. Definíció. A 3.4.1 tételből származó $n = 4m + 1$-ed rendű komplex Hadamard mátrixokat W_n-nel jelöljük.

18. *Megjegyzés.* Ha $p \equiv 1 \mod 4$ prím, akkor létezik $p + 1$-ed rendű szimmetrikus, ciklikus konferencia mátrix. A mátrix a szokásos módon $\mathbb{Z}_p$ kvadratikus karakterének segítségével konstruálható meg (lásd a Paley II konstrukciót a 6. oldalon).

3.4.3. Következmény. *Tegyük fel, hogy van $n = 4m + 2$ dimenziós, ciklikus magú konferencia mátrix. Ekkor létezik $4m + 1$-ed rendű ciklikus komplex Hadamard mátrix.*

3.4.4. Következmény (de la Harpe–Jones, [23])**.** *Ha $n \equiv 1 \mod 4$ prímszám, akkor létezik n-edrendű, a Fourier-mátrixtól inekvivalens komplex Hadamar mátrix.*

3.4.5. Példa. A D_{10} mátrixból (lásd a 31. oldalt) az alábbi 9×9-es komplex Hadamard mátrix származtatható:

$$W_9 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x^2 & x & x^3 & x^3 & x^{-1} & x^{-1} & x & x \\ 1 & x & x^2 & x^3 & x^3 & x & x & x^{-1} & x^{-1} \\ 1 & x^3 & x^3 & x^2 & x & x^{-1} & x & x^{-1} & x \\ 1 & x^3 & x^3 & x & x^2 & x & x^{-1} & x & x^{-1} \\ 1 & x^{-1} & x & x^{-1} & x & x^{-2} & x^{-3} & x^{-3} & x^{-1} \\ 1 & x^{-1} & x & x & x^{-1} & x^{-3} & x^{-2} & x^{-1} & x^{-3} \\ 1 & x & x^{-1} & x^{-1} & x & x^{-3} & x^{-1} & x^{-2} & x^{-3} \\ 1 & x & x^{-1} & x & x^{-1} & x^{-1} & x^{-3} & x^{-3} & x^{-2} \end{bmatrix}, x = \frac{1}{4} + \mathbf{i}\frac{\sqrt{15}}{4} \tag{3.67}$$

A TZ-katalógust, illetve annak online verzióját böngészve [83], igazolható az alábbi

3.4.6. Lemma $(*)$**.** *W_9 nem szerepel a TZ-katalógusban.*

Bizonyítás. W_9 Λ_{W_9} invariáns halmazát vizsgálva adódik, hogy maga a mátrix nem szerepel az $F_9^{(4)}$ család orbitjában, hiszen az utóbbi mátrixok Λ_{F_9}-halmaza a paraméterválasztástól függetlenül tartalmazza az ω komplex harmadik egységgyököt, ellenben

$\omega \notin \Lambda_{W_9}$. Hasonló érveléssel látható be, hogy W_9 inekvivalens a 10-ik komplex egységgyökökből álló B_9 mátrixtól is. Végül W_9 inekvivalens N_9-től, mert $-1 \in \Lambda_{N_9}$ ugyanakkor $-1 \notin \Lambda_{W_9}$. □

19. *Megjegyzés.* A fenti konstrukció D_6-ból [82] a jól ismert F_5 Fourier mátrixot adja vissza, D_{14}-ből – lévén ciklikus maggal rendelkezik – pedig a C_{13A} és C_{13B} 2-indexű ciklikus komplex Hadamard mátrixok adódnak [8].

3.5. Ad hoc konstrukciók

Diplomamunkánk utolsó szakaszában további új, eddig ismeretlen komplex Hadamard mátrixokat mutatnánk be, amelyek konstrukciója nem követ semmiféle általános módszert, hanem mindig az adott dimenzióra szabva adta magát. Egy egzotikus valamint egy, a $\mathbb{Q}(\mathbf{i}\sqrt{15})$ testbeli elemekkel rendelkező komplex Hadamard mátrix mellett két további, hatodik egységgyökökből álló $H(6,10)$ és $H(6,14)$ típusú Butson Hadamard mátrixot ismertetünk.

3.5.1. n=9

Az alábbi példát TDK dolgozatunk végén prezentáltuk [80]. A mátrix rendkívül nagy szimmetriával rendelkezik: magja kváziciklikus, melynek első sora radásul speciális, $\{x_1, x_2, x_3, x_4, \overline{x}_1, \overline{x}_2, \overline{x}_3, \overline{x}_4\}$ alakú. A mátrixot úgy találtuk, hogy az x_i ismeretlenekre direktben megoldottuk a felmerülő ortogonalitási egyenleteket.

3.5.1. Példa. Legyen

$$t_1 = \arccos\left(-\frac{1}{2} + \frac{\sqrt{2 - 2\sqrt{13}\cos\left(\frac{\pi}{3} + \frac{1}{3}\arctan\left(\frac{3\sqrt{771}}{43}\right)\right)}}{2}\right) \approx 1.607289, \tag{3.68}$$

$$t_2 = \arccos\left(\frac{1}{4} + \frac{\sqrt{1 + 8\sqrt{13}\cos\left(\frac{\pi}{3} + \frac{1}{3}\arctan\left(\frac{3\sqrt{771}}{43}\right)\right)}}{4}\right) \approx 0.574210, \tag{3.69}$$

$$t_3 = \arccos\left(-\frac{1}{2} - \frac{\sqrt{2 - 2\sqrt{13}\cos\left(\frac{\pi}{3} + \frac{1}{3}\arctan\left(\frac{3\sqrt{771}}{43}\right)\right)}}{2}\right) \approx 2.870637, \tag{3.70}$$

$$t_4 = \arccos\left(\frac{1}{4} - \frac{\sqrt{1 + 8\sqrt{13}\cos\left(\frac{\pi}{3} + \frac{1}{3}\arctan\left(\frac{3\sqrt{771}}{43}\right)\right)}}{4}\right) \approx 1.917311. \tag{3.71}$$

Ekkor az alábbi

$$Q_9 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \mathbf{e}^{\mathbf{i}t_1} & \mathbf{e}^{\mathbf{i}t_2} & \mathbf{e}^{\mathbf{i}t_3} & \mathbf{e}^{\mathbf{i}t_4} & \mathbf{e}^{-\mathbf{i}t_1} & \mathbf{e}^{-\mathbf{i}t_2} & \mathbf{e}^{-\mathbf{i}t_3} & \mathbf{e}^{-\mathbf{i}t_4} \\ 1 & \mathbf{e}^{-\mathbf{i}t_4} & \mathbf{e}^{\mathbf{i}t_1} & \mathbf{e}^{\mathbf{i}t_2} & \mathbf{e}^{\mathbf{i}t_3} & \mathbf{e}^{\mathbf{i}t_4} & \mathbf{e}^{-\mathbf{i}t_1} & \mathbf{e}^{-\mathbf{i}t_2} & \mathbf{e}^{-\mathbf{i}t_3} \\ 1 & \mathbf{e}^{-\mathbf{i}t_3} & \mathbf{e}^{-\mathbf{i}t_4} & \mathbf{e}^{\mathbf{i}t_1} & \mathbf{e}^{\mathbf{i}t_2} & \mathbf{e}^{\mathbf{i}t_3} & \mathbf{e}^{\mathbf{i}t_4} & \mathbf{e}^{-\mathbf{i}t_1} & \mathbf{e}^{-\mathbf{i}t_2} \\ 1 & \mathbf{e}^{-\mathbf{i}t_2} & \mathbf{e}^{-\mathbf{i}t_3} & \mathbf{e}^{-\mathbf{i}t_4} & \mathbf{e}^{\mathbf{i}t_1} & \mathbf{e}^{\mathbf{i}t_2} & \mathbf{e}^{\mathbf{i}t_3} & \mathbf{e}^{\mathbf{i}t_4} & \mathbf{e}^{-\mathbf{i}t_1} \\ 1 & \mathbf{e}^{-\mathbf{i}t_1} & \mathbf{e}^{-\mathbf{i}t_2} & \mathbf{e}^{-\mathbf{i}t_3} & \mathbf{e}^{-\mathbf{i}t_4} & \mathbf{e}^{\mathbf{i}t_1} & \mathbf{e}^{\mathbf{i}t_2} & \mathbf{e}^{\mathbf{i}t_3} & \mathbf{e}^{\mathbf{i}t_4} \\ 1 & \mathbf{e}^{\mathbf{i}t_4} & \mathbf{e}^{-\mathbf{i}t_1} & \mathbf{e}^{-\mathbf{i}t_2} & \mathbf{e}^{-\mathbf{i}t_3} & \mathbf{e}^{-\mathbf{i}t_4} & \mathbf{e}^{\mathbf{i}t_1} & \mathbf{e}^{\mathbf{i}t_2} & \mathbf{e}^{\mathbf{i}t_3} \\ 1 & \mathbf{e}^{\mathbf{i}t_3} & \mathbf{e}^{\mathbf{i}t_4} & \mathbf{e}^{-\mathbf{i}t_1} & \mathbf{e}^{-\mathbf{i}t_2} & \mathbf{e}^{-\mathbf{i}t_3} & \mathbf{e}^{-\mathbf{i}t_4} & \mathbf{e}^{\mathbf{i}t_1} & \mathbf{e}^{\mathbf{i}t_2} \\ 1 & \mathbf{e}^{\mathbf{i}t_2} & \mathbf{e}^{\mathbf{i}t_3} & \mathbf{e}^{\mathbf{i}t_4} & \mathbf{e}^{-\mathbf{i}t_1} & \mathbf{e}^{-\mathbf{i}t_2} & \mathbf{e}^{-\mathbf{i}t_3} & \mathbf{e}^{-\mathbf{i}t_4} & \mathbf{e}^{\mathbf{i}t_1} \end{bmatrix} \tag{3.72}$$

mátrix Hadamard.

3.5.2. Lemma $(*)$**.** *Q_9 nem szerepel a TZ-katalógusban.*

Bizonyítás. Numerikusan könnyen ellenőrizhető, hogy Q_9 Λ-invariáns halmaza nem tartalmazza az $\omega = \mathbf{e}^{\frac{2\pi\mathbf{i}}{3}}$-at, így nem része az $F_9^{(4)}$ családnak. Továbbá sem 10-ik gyököket, sem pedig a $-\frac{1}{4} \pm \mathbf{i}\frac{\sqrt{15}}{4}$ számokat nem tartalmazza, így speciálisan, a B_9, az N_9, illetve az előbb bemutatott W_9 mátrixokkal sem ekvivalens [82]. □

3.5.3. Példa. A következőkben egy nem-affin paraméteres mátrix családot mutatunk 9 dimenzióban, amely újfent nagyfokú szimmetriákkal rendelkezik. A Z_9 mátrix építőblokkjai $\alpha I + (\beta - \alpha)J$ alakúak. Az ilyen blokkmátrixok alkalmazása általában csak kevés ortogonalitási egyenlethez vezet.

$$Z_9^{(1)}(x) = \left[\begin{array}{ccc|ccc|ccc} 1 & x & x & a & b & b & a & b & b \\ x & 1 & x & b & a & b & b & a & b \\ x & x & 1 & b & b & a & b & b & a \\ \hline a & b & b & 1 & x & x & a & b & b \\ b & a & b & x & 1 & x & b & a & b \\ b & b & a & x & x & 1 & b & b & a \\ \hline a & b & b & a & b & b & 1 & x & x \\ b & a & b & b & a & b & x & 1 & x \\ b & b & a & b & b & a & x & x & 1 \end{array}\right] \tag{3.73}$$

Legyen továbbá $x = \mathbf{e}^{\mathbf{i}t}$, ahol $t \in [\frac{1}{3}\pi, \frac{5}{3}\pi]$, és így

$$a = a(x) = \frac{-x^2 - x - 1 + \sqrt{x^4 + 6x^3 - 5x^2 + 6x + 1}}{2(x-1)} \tag{3.74}$$

$$b = b(x) = \frac{-x^2 + 5x - 1 - \sqrt{x^4 + 6x^3 - 5x^2 + 6x + 1}}{4(x-1)} \tag{3.75}$$

egységnyi abszolút értékű számok (ez nemtriviális, hogy miért van így. Lásd [4]). Érdekességképpen megjegyezzük, hogy $x = -1$ esetén egyúttal speciálisan $b = -a^2$ adódik. Ekkor az így kapható mátrix egy permutált verziója az alábbi

$$Z_9^{(1)}(-1) \cong \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a^{-2} & -a^{-1} & 1 & a^{-2} & -a^{-1} & a^{-1} & a^{-1} & -a^{-1} \\ 1 & -a^{-1} & a^{-2} & 1 & -a^{-1} & a^{-2} & a^{-1} & -a^{-1} & a^{-1} \\ 1 & 1 & 1 & a^{-1} & a^{-2} & a^{-2} & a & a^2 & a^2 \\ 1 & a^{-2} & -a^{-1} & a^{-2} & a^{-3} & -a^{-3} & a & 1 & -a \\ 1 & -a^{-1} & a^{-2} & a^{-2} & -a^{-3} & a^{-3} & a & -a & 1 \\ 1 & a^{-1} & a^{-1} & a & a & a & a^2 & a^3 & a^3 \\ 1 & a^{-1} & -a^{-1} & a^2 & 1 & -a & a^3 & a^2 & -a^3 \\ 1 & -a^{-1} & a^{-1} & a^2 & -a & 1 & a^3 & -a^3 & a^2 \end{bmatrix}, \; a = \frac{1}{4} - \mathbf{i}\frac{\sqrt{15}}{4} \tag{3.76}$$

A fenti $Z_9^{(1)}(-1)$ mátrix sok hasonlóságot mutat a [4]-ben talált $N_9^{(0)}$ mátrixszal. Bár ugyanazon kvadratikus irracionális szám segítségével lehet mindkét mátrixot megkonstruálni, Λ-invariáns halmazuk különbözik, így nem lehetnek ekvivalensek.

Hasonlóan látható be, mint az előbb, hogy $Z_9^{(1)}(-1)$ nem szerepel a katalógusban.

3.5.4. Lemma $(*)$**.** *$Z_9^{(1)}(-1)$, és annak egy környezete nem szerepel a TZ-katalógusban.*

Bizonyítás. $Z_9^{(1)}(-1)$ Λ_{Z_9} invariáns halmazát vizsgálva adódik, hogy maga a mátrix nem szerepel az $F_9^{(4)}$ család orbitjában, hiszen az utóbbi mátrixok Λ_{F_9}-halmaza a paraméterválasztástól függetlenül tartalmazza az ω komplex harmadik egységgyököt, ellenben $\omega \notin \Lambda_{Z_9}$. Hasonló érveléssel látható be, hogy $Z_9^{(1)}(-1)$ inekvivalens a 10-ik komplex egységgyökökből álló B_9 mátrixtól is. Az $N_9^{(0)}$ mátrixtól való inekvivalenciája abból következik, hogy az $N_9^{(0)}$ mátrix izolált, így speciálisan nem indukál folytonos paraméteres családokat. Végül $Z_9^{(1)}(-1)$ inekvivalens a korábban talált Q_9 és W_9 mátrixoktól is, mert a Λ invariáns halmazuk különbözik. Ezzel a bizonyítás kész. □

3.5.2. n=10

Agaian monográfiájában [1] található egy 10×10-es komplex Hadamard mátrix, mely 6-ik gyökökből áll. Az ott prezentált mátrix eléggé szabálytalan szerkezettel bír, ám átpermutálva, majd a paraméterezést követően az elemeit elforgatva az alábbi, nagyfokú szimmetriákkal rendelkező mátrix adódik.

$$A_{10} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & \mathbf{e}^{-\frac{i\pi}{3}} & \mathbf{e}^{\frac{i\pi}{3}} & 1 & -1 & 1 & \mathbf{e}^{-\frac{2i\pi}{3}} & \mathbf{e}^{\frac{2i\pi}{3}} \\ 1 & 1 & -1 & -\mathbf{e}^{-\frac{i\pi}{3}} & -\mathbf{e}^{\frac{i\pi}{3}} & -1 & 1 & 1 & \mathbf{e}^{-\frac{2i\pi}{3}} & \mathbf{e}^{\frac{2i\pi}{3}} \\ 1 & -1 & -1 & \mathbf{e}^{\frac{i\pi}{3}} & \mathbf{e}^{-\frac{i\pi}{3}} & 1 & 1 & -1 & \mathbf{e}^{\frac{2i\pi}{3}} & \mathbf{e}^{-\frac{2i\pi}{3}} \\ 1 & -1 & 1 & -\mathbf{e}^{\frac{i\pi}{3}} & -\mathbf{e}^{-\frac{i\pi}{3}} & -1 & 1 & 1 & \mathbf{e}^{\frac{2i\pi}{3}} & \mathbf{e}^{-\frac{2i\pi}{3}} \\ 1 & \mathbf{e}^{-\frac{i\pi}{3}} & \mathbf{e}^{\frac{i\pi}{3}} & -1 & -1 & 1 & \mathbf{e}^{\frac{2i\pi}{3}} & \mathbf{e}^{-\frac{2i\pi}{3}} & 1 & -1 \\ 1 & -\mathbf{e}^{-\frac{i\pi}{3}} & -\mathbf{e}^{\frac{i\pi}{3}} & 1 & -1 & -1 & \mathbf{e}^{\frac{2i\pi}{3}} & \mathbf{e}^{-\frac{2i\pi}{3}} & 1 & 1 \\ 1 & \mathbf{e}^{\frac{i\pi}{3}} & \mathbf{e}^{-\frac{i\pi}{3}} & -1 & -1 & 1 & \mathbf{e}^{-\frac{2i\pi}{3}} & \mathbf{e}^{\frac{2i\pi}{3}} & -1 & 1 \\ 1 & -\mathbf{e}^{\frac{i\pi}{3}} & -\mathbf{e}^{-\frac{i\pi}{3}} & -1 & 1 & -1 & \mathbf{e}^{-\frac{2i\pi}{3}} & \mathbf{e}^{\frac{2i\pi}{3}} & 1 & 1 \end{bmatrix} \tag{3.77}$$

A_{10} paraméteres családokat indukál, mégpedig a következő séma szerint:

$$A_{10}^{(5)}(a,b,c,d,e) = A_{10} \circ \mathbf{EXP}\left(\mathbf{i} \cdot R_{A_{10}^{(5)}}(a,b,c,d,e)\right), \tag{3.78}$$

ahol

$$R_{A_{10}}^{(5)}(a,b,c,d,e) = \begin{bmatrix} \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & a & \bullet & a & a & a+e & a+e & e & e & e \\ \bullet & a & \bullet & a & a & a+e & a+e & e & e & e \\ \bullet & \bullet & b & b & b & b+e & e & b+e & e & e \\ \bullet & \bullet & b & b & b & b+e & e & b+e & e & e \\ \bullet & c & c & c & \bullet & c+e & e & e & e & c+e \\ \bullet & c & c & c & \bullet & c+e & e & e & e & c+e \\ \bullet & d & d & \bullet & d & d+e & e & e & d+e & e \\ \bullet & d & d & \bullet & d & d+e & e & e & d+e & e \end{bmatrix} \tag{3.79}$$

3.5.5. Lemma $(*)$**.** *$A_{10}(a,b,c,d,e)$ nem szerepel a TZ-katalógusban.*

Bizonyítás. A katalógus 10 dimenzióban csak legfeljebb 4 paraméteres mátrixcsaládokat tartalmaz. □

3.5.3. n=14

A 10×10-es példa szerkezetét megértve megpróbáltunk magasabb dimenziókban is hatodik egységgyökökből álló komplex Hadamard mártixokat keresni. A kereséskor eleve nem sorokat, hanem egyből olyan sorpárokat kerestünk, amelyre a 2.5.4 lemma alkalmazható, s így rögtön paraméteres családok is nyerhetők. Ez az elgondolás nemcsak a keresés idejét csökkentette le, hanem a mátrix paraméterezését is megkönnyítette.

$A_{14} =$

$$\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & -1 & -1 & -1 & 1 & \mathbf{e}^{-\frac{i\pi}{3}} & \mathbf{e}^{\frac{i\pi}{3}} & 1 & -1 & -1 & -1 & 1 & \mathbf{e}^{-\frac{i\pi}{3}} & \mathbf{e}^{\frac{i\pi}{3}} \\
1 & 1 & -1 & -1 & -1 & \mathbf{e}^{-\frac{i\pi}{3}} & \mathbf{e}^{\frac{i\pi}{3}} & -1 & 1 & -1 & 1 & 1 & -\mathbf{e}^{-\frac{i\pi}{3}} & -\mathbf{e}^{\frac{i\pi}{3}} \\
1 & -1 & -1 & 1 & -1 & \mathbf{e}^{\frac{i\pi}{3}} & \mathbf{e}^{-\frac{i\pi}{3}} & 1 & -1 & -1 & 1 & -1 & \mathbf{e}^{\frac{i\pi}{3}} & \mathbf{e}^{-\frac{i\pi}{3}} \\
1 & -1 & 1 & -1 & -1 & \mathbf{e}^{\frac{i\pi}{3}} & \mathbf{e}^{-\frac{i\pi}{3}} & -1 & -1 & 1 & 1 & 1 & -\mathbf{e}^{\frac{i\pi}{3}} & -\mathbf{e}^{-\frac{i\pi}{3}} \\
1 & -1 & 1 & \mathbf{e}^{-\frac{i\pi}{3}} & \mathbf{e}^{\frac{i\pi}{3}} & -1 & -1 & 1 & 1 & -1 & \mathbf{e}^{\frac{i\pi}{3}} & \mathbf{e}^{-\frac{i\pi}{3}} & -1 & -1 \\
1 & -1 & -1 & \mathbf{e}^{-\frac{i\pi}{3}} & \mathbf{e}^{\frac{i\pi}{3}} & -1 & 1 & -1 & 1 & 1 & -\mathbf{e}^{\frac{i\pi}{3}} & -\mathbf{e}^{-\frac{i\pi}{3}} & -1 & 1 \\
1 & 1 & -1 & \mathbf{e}^{\frac{i\pi}{3}} & \mathbf{e}^{-\frac{i\pi}{3}} & -1 & -1 & 1 & -1 & 1 & \mathbf{e}^{-\frac{i\pi}{3}} & \mathbf{e}^{\frac{i\pi}{3}} & -1 & -1 \\
1 & -1 & -1 & \mathbf{e}^{\frac{i\pi}{3}} & \mathbf{e}^{-\frac{i\pi}{3}} & 1 & -1 & -1 & 1 & 1 & -\mathbf{e}^{-\frac{i\pi}{3}} & -\mathbf{e}^{\frac{i\pi}{3}} & 1 & -1 \\
1 & \mathbf{e}^{-\frac{i\pi}{3}} & \mathbf{e}^{\frac{i\pi}{3}} & -1 & -1 & 1 & -1 & 1 & \mathbf{e}^{-\frac{i\pi}{3}} & \mathbf{e}^{\frac{i\pi}{3}} & -1 & -1 & -1 & 1 \\
1 & \mathbf{e}^{-\frac{i\pi}{3}} & \mathbf{e}^{\frac{i\pi}{3}} & -1 & 1 & -1 & -1 & -1 & -\mathbf{e}^{-\frac{i\pi}{3}} & -\mathbf{e}^{\frac{i\pi}{3}} & 1 & -1 & 1 & 1 \\
1 & \mathbf{e}^{\frac{i\pi}{3}} & \mathbf{e}^{-\frac{i\pi}{3}} & -1 & -1 & -1 & 1 & 1 & \mathbf{e}^{\frac{i\pi}{3}} & \mathbf{e}^{-\frac{i\pi}{3}} & -1 & -1 & 1 & -1 \\
1 & \mathbf{e}^{\frac{i\pi}{3}} & \mathbf{e}^{-\frac{i\pi}{3}} & 1 & -1 & -1 & -1 & -1 & -\mathbf{e}^{\frac{i\pi}{3}} & -\mathbf{e}^{-\frac{i\pi}{3}} & -1 & 1 & 1 & 1
\end{bmatrix} \tag{3.80}$$

A_{14} paraméteres családokat indukál, mégpedig a következő séma szerint:

$$A_{14}^{(7)}(a,b,c,d,e,f,g) = A_{14} \circ \mathbf{EXP}\left(\mathbf{i} \cdot R_{A_{14}^{(7)}}(a,b,c,d,e,f,g)\right), \tag{3.81}$$

ahol

$$R_{A_{14}}^{(7)} = \begin{bmatrix}
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
\bullet & a & \bullet & \bullet & a & \bullet & \bullet & a+g & a+g & g & a+g & g & a+g & a+g \\
\bullet & a & \bullet & \bullet & a & \bullet & \bullet & a+g & a+g & g & a+g & g & a+g & a+g \\
\bullet & \bullet & b & b & \bullet & \bullet & \bullet & b+g & g & b+g & g & b+g & b+g & b+g \\
\bullet & \bullet & b & b & \bullet & \bullet & \bullet & b+g & g & b+g & g & b+g & b+g & b+g \\
\bullet & \bullet & c & \bullet & \bullet & \bullet & c & c+g & g & c+g & c+g & c+g & g & c+g \\
\bullet & \bullet & c & \bullet & \bullet & \bullet & c & c+g & g & c+g & c+g & c+g & g & c+g \\
\bullet & d & \bullet & \bullet & \bullet & d & \bullet & d+g & d+g & g & d+g & d+g & d+g & g \\
\bullet & d & \bullet & \bullet & \bullet & d & \bullet & d+g & d+g & g & d+g & d+g & d+g & g \\
\bullet & \bullet & \bullet & \bullet & e & e & \bullet & e+g & e+g & e+g & e+g & g & e+g & g \\
\bullet & \bullet & \bullet & \bullet & e & e & \bullet & e+g & e+g & e+g & e+g & g & e+g & g \\
\bullet & \bullet & \bullet & f & \bullet & \bullet & f & f+g & f+g & f+g & g & f+g & g & f+g \\
\bullet & \bullet & \bullet & f & \bullet & \bullet & f & f+g & f+g & f+g & g & f+g & g & f+g
\end{bmatrix} \tag{3.82}$$

Fent tehát egy 14 dimenziós, hatodik egységgyökökből álló mátrix látható. Felmerül a kérdés, hogy vajon ez a mátrix nem kapható-e meg a Diţă-konstrukció segítségével a P_7 illetve az F_2 mátrixokból. Az alábbiakban a 2.5.2 tétel bizonyításához hasonlóan igazoljuk az alábbit:

3.5.6. Lemma $(*)$**.** *A_{14} és A_{14}^T nem Diţă-szerű.*

Bizonyítás. Ismét az [56]-ban szereplő eredményeket fogjuk használni. Tegyük fel indirekt, hogy A_{14} mégis Diţă-szerű. Ezért most $N = kn = 14$, és így két eset adódik aszerint, hogy $n = 2$ vagy $n = 7$.

ELSŐ ESET: Tegyük fel, hogy $n = 2$, és így $k = 7$. Ekkor az indirekt feltevés miatt A_{14}-ben két sor 7-es van, amelyek ekvivalensek valamely $I_1, I_2, \ldots, I_7$ halmazokra nézve. Mivel a mátrix normalizált, ezért azonnal adódik, hogy egy olyan sor, amely az első sorral azonos sor 7-esben van, garantáltan minden elemét páros sokszor tartalmazza. Más szóval egy sorvektor nem lehet az elsővel azonos sor 7-esben, ha tartalmaz olyan elemeket, amelyek csak páratlan sokszor szerepelnek. Ránézve A_{14}-re világos, hogy az ilyen tulajdonságú sorok kizárólag a $\{3, 5, 7, 9, 11\}$ sorok, vagyis az elsővel együtt ők kell hogy alkossák az egyik sor 7-est. A harmadik sort megvizsgálva azonnal adódik, hogy $\{7, 14\}$ oszlopok egy I_k indexhalmazt kell hogy alkossanak, legyen ez az I_1. Ekkor az I_1-re való ekvivalencia miatt az kellene, hogy a $\{3, 5, 7, 9, 11\}$ sorok mindegyike azonos elemeket tartalmazzon a 7-ik és 14-ik oszlopban, de ez a 11-ik sorra nem teljesül. Ez ellentmondás, vagyis A_{14} nem Diţă-szerű mátrix.

MÁSODIK ESET: Most tegyük fel, hogy $n = 7$, és így $k = 2$. Ekkor hasonlóan, mint az első esetben hét sorpár van, amelyek ekvivalensek valamely I_1 és I_2 indexhalmazokra nézve. Az első sor párja tehát csak olyan lehet, amelyben hét $+1$ mellett hét további azonos elem van. Mivel ez kizárólag a második sorra teljesül adódik, hogy $I_1 = \{1, 2, \ldots, 7\}, I_2 = \{8, 9, \ldots, 14\}$. Ha most lenne egy további olyan sorpár, amely ekvivalens az I_1-re, akkor mivel minden sor $+1$-gyel kezdődik, kapjuk, hogy egy ilyen sorpár első hét koordinátáján azonos elemek állnak, ilyen további sorpár viszont nincs A_{14}-ben. Az ellentmondás garantálja, hogy A_{14} nem Diţă-szerű.

Hasonlóan mutatható meg, hogy A_{14}^T nem Diţă-szerű. □

3.5.7. Következmény. *$A_{14}^{(7)}(a, b, c, d, e, f, g)$ lokálisan inekvivalens a TZ-katalógusban található mátrixok mindegyikétől.*

Bizonyítás. A 14 dimenziós ismert komplex Hadamard mátrixok a $D_{14}^{(6)}$-tól eltekintve mind a Diţă-konstrukcióval kaphatóak meg, azok halmaza pedig zárt halmaz [81]. Így speciálisan, A_{14} egy környezetében nem Diţă-szerű mátrixokat generál. Az, hogy ezek a mátrixok nincsenek benne a $D_{14}^{(6)}$ családban a következőből folyik: a $D_{14}^{(6)}$-ban szereplő minden mátrix Λ invariáns halmaza tartalmazza a $\mathbf{i}$ komplex számot, amely sem az A_{14}, sem pedig annak egy környezetében lévő mátrixok Λ halmaza nem tartalmaz. Így ezek a mátrixok nem lehetnek ekvivalensek. □

Érdekes kérdés, hogy általánosságban milyen n-re létezik Butson típusú $H(6, n)$ mátrix. Az világos, hogy a valós Hadamard mátrixok speciálisan ilyenek. Emellett a tenzorszorzás segítségével az F_3 Fourier mátrixból minden $n = 2^a \cdot 3^b$ dimenzióban konstruálhatók még ilyenek. Ellenben Haagerup 5×5-ös klasszifikációja [37] révén tudjuk, hogy $n = 5$-re nincs $H(6, 5)$ mátrix. Van viszont $n = 7$-re, mint azt a P_7 mátrix mutatja [64], és van $n = 13$-ra, amely [16]-ban található. A most megkonstruált A_{10} és A_{14} mátrixokkal együtt így összességében azt mondhatjuk, hogy

$$\exists H(6,n), \text{ ha } n \in \{1,2,3,4,6,7,8,9,10,12,13,14,16,18,20\}. \tag{3.83}$$

A negatív eredmények tekintetében szintén [16] irányadó. Itt Compton, de Launey és Seberry eredménye szerepel, mely szerint $\nexists H(6,n)$, ha $n \in \{5,11,15,17\}$. A legkisebb eldöntetlen dimenzió tehát az $n = 19$. Mindezekről részletesebben a most előkészületben lévő [17] cikkben lehet majd olvasni.

A diplomamunkát az S_6, A_{10} és A_{14} mátrixok létezéséből adódóan a következő természetes sejtéssel zárjuk.

3.5.8. Sejtés $(*)$**.** *Ha p prím, akkor létezik Butson $H(6,2p)$ komplex Hadamard mátrix.*

Irodalomjegyzék

[1] S. S. Agaian: Hadamard Matrices and Their Applications, *Springer-Verlag: Lecture Notes in Mathematics* (1985)

[2] J. Backelin: Square multiples n gives infinite many cyclic n-roots. *Reports, Matematiska Institutionen*, Stockholms Universitet, **8**., (1989)

[3] J. Backelin, R. Fröberg: How we proved that there are exactly 924 cyclic 7-roots. *Proc. ISAAC '91* (S. M. Watts szerk.), ACM 103–111. (1991)

[4] K. Beauchamp, R. Nicoara: Orthogonal maximal abelian $*$-subalgebras of the 6×6 matrices, *arXiv:math/0609076v1 [math.OA]* (2006)

[5] B. W. Brock: Hermitian congruence and the existence and completion of generalised Hadamard matrices *J. Combin. Th. A* **49**., 233–261. (1988)

[6] T. Beth, D. Jungnickel, H. Lenz: Design Theory, 2nd ed., CUP, Cambridge (1999)

[7] G. Björck: Functions of modulus one on $\mathbb{Z}_p$, whose Fourier transforms have constant modulus. Proceedings of A. Haar Memorial Conference, Budapest Colloq. Math. Soc. János Boyai **49**., 193–197. (1985)

[8] G. Björck: Functions of modulus 1 on $\mathbb{Z}_n$, whose Fourier transforms have constant modulus, and „cyclic n-roots". Recent Advances in Fourier Analysis and its applications. NATO *Adv. Sci. Inst. Ser. C: Math. Phys. Sci.*, Kluwer **315**., 131–140. (1990)

[9] G. Björck, R. Fröberg: A faster way to count the solutions of inhomogeneous systems of Algebraic Equations, with Applications to Cyclic n-roots, *J. Symbolic Computation* **12**., 329-336 (1991)

[10] G. Björck, U. Haagerup: All cyclic p-roots of index 3, found by symmetry-preserving calculations, *arXiv:0803.2506v1 [math.AC]* (2008)

[11] B. Buchberger: An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal, *Journal of Symbolic Computation* **41(3–4)**., 475–511 (2006)

[12] A. T. Butson: Generalized Hadamard matrices, *Proc. Am. Math. Soc.* **13**., 894–898. (1962)

[13] Y. Q. Chen: On the existence of abelian Hadamard difference sets and new family of difference sets, *Finite Fields Appl.* **3**., 234–256. (1997)

[14] O. Chterental, D. Ž. Đoković, On Orthostochastic, Unistochastic And Qustochastic Matrices, *arXiv:0708.4051v1 [math-ph]* (2007)

[15] C. J. Colbourn and W. de Launey: Difference matrices, Chapter IV.11, *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, 1996.

[16] C. Colbourn, J. Dinitz (szerk.), Handbook of Combinatorial Designs, second edition, *CRC Publishing Company* (2006)

[17] R. Compton, W. de Launey, J. R. Seberry: Generalized Hadamard matrices over sixth roots of unity *előkészületben* (2006)

[18] D. Coppersmith, J. Steinberger: On the entry sum of cyclotomic arrays, *Electronic Journal of Combinatorial and Additive Number Theory, megjelenés alatt* (2007)

[19] R. Craigen: Regular conference matrices and complex Hadamard matrices, *Util. Math.* **45**., 65–69. (1994)

[20] R. Craigen: Signed groups, sequences, and the asymptotic existence of Hadamard matrices, *J. Comb. Theory, Ser. A* **71**(2): 241–254 (1995)

[21] R. Craigen, Jennifer Seberry, Xian-Mo Zhang: The Product of Four Hadamard Matrices, *J. Combinatorial Th. (Ser A)*, **59**., 318–320. (1992)

[22] J. A. Davis and J. Jedwab: A survey on Hadamard difference sets, *Groups, Difference Sets and the Monster*, K. T. Arasu et al. (szerk.), de Gruyter, Berlin 145–156. (1996)

[23] P. de la Harpe, V. F. R. Jones: Paires de sous-algèbres semi-simples et graphes fortement réguliers, *C. R. Acad. Sci. Paris*, **311**., Serie I. 147–150. (1990)

[24] W. de Launey: On the asymptotic existence of partial complex Hadamard matrices and releated combinatorial objects, *Discr. Appl. Math.* **102**., 37–45. (2000)

[25] W. de Launey, R. M. Stafford: On the automorphisms of Paley's Type II Hadamard matrix, *Discr. Math.*, megjelenés alatt (2007)

[26] W. de Launey, D. M. Gordon: A comment on the Hadamard conjecture, *J. Combin. Theory A* **95**., 180–184. (2001)

[27] P. Delsarte, J. M. Goethals, J. J. Seidel: Orthogonal Matrices with Zero Diagonal, *Canad. J. Math* **23**., 816–832. (1971)

[28] P. Diţă: Some results on the parametrization of complex Hadamard matrices, *J. Phys. A*, **37**. no. 20, 5355–5374. (2004)

[29] D. Ž. Đoković: Hadamard matrices of order 764 exists, *arXiv:math/0703312v1 [math.CO]* (2007)

[30] D. Ž. Đoković: Williamson matrices of orders $4n$ for $n = 33, 35, 39$, *Discr. Math.* **115**., 267–271. (1993)

[31] C. Elster, A. Neumaier: Screening by Conference Designs, *Biometrika* **82**., 589–602. (1995)

[32] J.-C. Faugère: Finding all the solutions of cyclic 9 using Gröbner Basis techniques, *Computer Mathematics* (Matsuyama, 2001), Lecture Notes Ser. Comput. **9**., World Sci. Publ. 1–12. (2001)

[33] J.-C. Faugère: A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5), *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation ISSAC*, 75–83. ACM Press (2002)

[34] B. Fuglede: Commuting Self-Adjoint Partial Differential Operators and a Group Theoretic Problem. *J. Func. Anal.* **16**., 101–121. (1974)

[35] A. V. Geramita, J. Seberry: *Orthogonal Designs: Quadratic Forms and Hadamard matrices*, Marcel Dekker, Inc., New York, NY (1979)

[36] U. Haagerup: Cyclic p-roots of prime length p and releated complex Hadamard matrices, *arXiv:0803.2629v1 [math.AC]* (2008)

[37] U. Haagerup: Orthogonal maximal abelian $*$-subalgebras of the $n \times n$ matrices and cyclic n-roots, *Operator Algebras and Quantum Field Theory* (Rome), Cambridge, MA International Press, 296–322. (1996)

[38] J. Hadamard: Resolution d'une question relative aux determinants, *Bull. Sci. Math.* **17**., 240–6 (1893)

[39] M. Hall, Jr.: *Research Summary* No. 36–10, Volume I, chapter Hadamard matrices of order 16, pages 21–26. Jet Propulsion Laboratory, Pasadena, (1961)

[40] M. Hall, Jr.: Hadamard matrices of order 20. *Technical Report* 32–761., Jet Propulsion Laboratory, Pasadena, (1965)

[41] A. S. Hedayat, N. J. A. Sloane, J. Stufken: Orthogonal Arrays, Theory and Applications, *Springer*, New York (1999)

[42] K. J. Horadam: Hadamard Matrices and Their Applications *Princeton University Press* (2007)

[43] N. Ito: Note on Hadamard matrices of type Q, *Studia Sci. Math. Hungar.* **16**., 389–393. (1981)

[44] N. Ito: On Hadamard groups I, *J. Algebra* **168**., 981–987. (1994)

[45] N. Ito: On Hadamard groups II, *J. Algebra* **169**., 936–942. (1994)

[46] J. L. Jensen: Correction of paper published in J. Combinatorial Theory 21, 1976: On the Existence of Hadamard Matrices, *arXiv:0706.1720v1 [math.CO]* (2007)

[47] D. Jungnickel, A. Pott: Difference sets: Abelian, *The CRC Handbook of Combinatorial Designs*, C. J. Colburn and J. H. Dinitz (szerk.), CRC Press, Boca Raton (1996)

[48] D. Jungnickel, A. Pott: Difference sets: an introduction, *Difference Sets, Sequences and Their Correlation Properties*, A. Pott et al. (szerk.), NATO Science Series C, 542, Kluwer, Dordrecht, 259–295. (1999)

[49] D. Jungnickel, B. Schmidt: Difference sets: a second update, *Rend. Circ. Mat. Palermo* (2) Suppl. **53**., 89–118. (1998)

[50] W. M. Kantor, Automorphism groups of Hadamard matrices, *J. Combin. Theory A* **6**., 279–281. (1969)

[51] H. Kharaghani, B. Tayfeh-Rezaie: A Hadamard matrix of order 428, *J. Combin. Designs*, **13**., 435-440. (2005)

[52] H. Kimura: Classification of Hadamard matrices of order 28, *Discrete Math.*, **133(1–3)**., 171–180, (1994)

[53] M. Kolountzakis, M. Matolcsi: Tiles with no spectra, *Forum Math.*, **18**., 519–528. (2006)

[54] I. S. Kotsireas, C. Koukouvinos, J. Seberry: Hadamard ideals and Hadamard matrices with two circulant cores, *European J. Combin.* **27**., 658–668 (2006)

[55] T. Y. Lam and K. H. Leung: On vanishing sums of roots of unity, *J. of Algebra* **224**., 91–109. (2000)

[56] M. Matolcsi, J. Réffy, F. Szöllősi: Constructions of complex Hadamard matrices via tiling Abelian groups, *Open Sys. & Inf. Dyn.* **14:3**, 247–263 (2007)

[57] G. E. Moorhouse: The 2-Transitive Complex Hadamard Matrices, *Designs, Codes and Cryptography* (2001)

[58] A. Munemasa, Y. Watatani: Orthogonal Pairs of $*$-Subalgebras and Association Schemes, *C. R. Acad. Sci. Paris*, **314**., 329–331. (1992)

[59] R. Nicoara: A finiteness result for commuting squares of matrix algebras, *arXiv:math/0404301v1 [math.OA]* (2004)

[60] H. J. Ryser: *Combinatorial Mathematics.* Buffalo, NY: Math. Assoc. Amer., 104–122. (1963)

[61] W. P. Orrick: Switching Operations for Hadamard Matrices: math/0507515

[62] W. P. Orrick és B. Solomon által szerkesztett honlap:
`http://www.indiana.edu/~maxdet/`

[63] R.E.A.C Paley: On Orthogonal Matrices, *J. Math and Phys.* **12**., 311–320. (1933)

[64] M. Petrescu: Existence of continuous families of complex Hadamard matrices of certain prime dimensions, *Ph.D thesis*, UCLA (1997)

[65] D. Petz, J. Kahn: Complementary reductions for two qubits, *arXiv:quant-ph/0608227v2* (2006)

[66] D. Petz, K. M. Hangos, A. Szántó, F. Szöllősi: State tomography for two qubits using reduced densities, *J. Phys. A: Math. Gen.* **39**., 10901–10907. (2006)

[67] S. Popa: Orthogonal pairs of $*$-subalgebras in finite von Neumann algebras, *J. Operator Theory* **9**., 253–268. (1983)

[68] D. Raghavarao: Constructions and combinatorial problems in designs of experiments, *New York: Dover* (1988)

[69] K. Sawade: A Hadamard Matrix of Order 268. *Graphs Combinatorics* **1**., 185–187. (1985)

[70] A. Sommese, J. Verschelde, C. W. Wampler: Using Monodromy to Decompose Solution Sets of Polynomial Systems into Irreducible Components, *Application of Algebraic Geometry to Coding Theory, Physics and Computation*, C. Ciliberto, F. Hirzebruch, R. Miranda, and M. Teicher szerk. 297–315 (2001)

[71] J. Seberry: Life's Work on Hadamard Matrices, Statistical Designs, http://www.uow.edu.au/~jennie/lifework.html

[72] J. Seberry online katalógusa: http://www.uow.edu.au/~jennie/

[73] J. Seberry Wallis: On the Existence of Hadamard Matrices, *J. Comb. Theory (A)* **21**., 188–195. (1976)

[74] J. Seberry, X. Zhang: Some orthogonal matrices constructed by strong kronecker multiplication, *Australian Journal of Combinatorics* **7**., 213–224. (1993)

[75] N. J. A. Sloane online katalógusa: http://www.research.att.com/~njas/hadamard/

[76] K. W. Smith: Nonabelian Hadamard difference sets, *J. Combin Theory A* **70**., 144–156. (1995)

[77] J. J. Sylvester: Thoughts on inverse orthogonal matrices, simultaneous sign-successions, and tessellated pavements in two or more colors, with applications to Newton's rule, ornamental tile-work, and the theory of numbers, *Phil. Mag.* **34**., 461. (1867)

[78] S. Szabó. A type of factorization of finite abelian groups, *Discrete Math.* **54**., no. 1, 121–124. (1985)

[79] A. Szántó: Két feles spin állapotának rekonstrukciója (in Hungarian), *Student Research Report, BUTE* (2005)

[80] F. Szöllősi: Komplex Hadamard mátrixok konstrukciója és paraméterezése (in Hungarian), *Student Research Report, BUTE* (2006)

[81] F. Szöllősi: Parametrization of Complex Hadamard matrices, *European Journal of Combinatorics* **29**., 1219–1234. (2008)

[82] W. Tadej, K. Życzkowski: A concise guide to complex Hadamard matrices *Open Systems & Infor. Dyn.* **13**., 133-177. (2006)

[83] W. Tadej és K. Życzkowski online katalógusa: http://chaos.if.uj.edu.pl/~karol/hadamard/index.html

[84] T. Tao: Fuglede's Conjecture Is False in 5 and Higher Dimensions. *Math. Res. Letters*, **11**., 251–258. (2004)

[85] R. J. Turyn: An infinite class of Williamson matrices, *J. Combin. Theory A* **12**., 319–321. (1972)

[86] E. W. Weisstein: Unsolved Problems. From *MathWorld* – A Wolfram Web Resource. `http://mathworld.wolfram.com/UnsolvedProblems.html`

[87] R. F. Werner: All teleportation and dense coding schemes, *J. Phys. A: Math. Gen.* **34**., 7081–94 (2001)

[88] R. M. Wilson and Q. Xiang: Constructions of Hadamard difference sets, J. Combin. Theory A **77**., 148–160. (1997)

[89] A. Winterhof, On the non-existence of generalised Hadamard matrices, *J. Statist. Plann. Inference* **84**., 337–342. (2000)

[90] M.-Y. Xia: Some infinite classes of special Williamson matrices and difference sets, *J. Combin. Theory A* **61**., 230–242. (1992)