

# Construction, classification and parametrization of complex Hadamard matrices



# Construction, classification and parametrization of complex Hadamard matrices

by

Ferenc Szöllősi

A THESIS

PRESENTED TO CENTRAL EUROPEAN UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

MATHEMATICS AND ITS APPLICATIONS

Supervisor: Professor Máté Matolcsi

Budapest, Hungary

2011





## **DEDICATION**

To my high school teachers  
Anna Pataki and Géza Magyar  
for revealing me the beauty of mathematics.



# Contents

<b>Introduction</b>	<b>ix</b>
<b>Acknowledgements</b>	<b>xv</b>
<b>1 Complex Hadamard matrices of composite orders</b>	<b>1</b>
1.1 Existence of complex Hadamard matrices . . . . .	1
1.2 Parametrizing complex Hadamard matrices . . . . .	6
1.3 Equivalence of complex Hadamard matrices . . . . .	15
1.4 Butson-type complex Hadamard matrices . . . . .	18
1.4.1 A course on $BH(n, 4)$ matrices . . . . .	20
1.4.2 A course on $BH(n, 6)$ matrices . . . . .	28
1.4.3 An application of Butson matrices: Tiles and spectral sets . . .	32
<b>2 Towards the classification of <math>6 \times 6</math> Hadamard matrices</b>	<b>39</b>
2.1 Classification up to order 5 . . . . .	39
2.2 The evolution of Hadamard matrices of order 6 . . . . .	41
2.2.1 Well-known matrices and their orbit . . . . .	41
2.2.2 The self-adjoint family . . . . .	43
2.2.3 A symmetric family . . . . .	45
2.2.4 Birculant matrices . . . . .	45
2.2.5 Karlsson's observation . . . . .	47
2.2.6 $H_2$ -reducible complex Hadamard matrices . . . . .	47
2.3 A four-parameter family . . . . .	49
2.3.1 The main ingredients . . . . .	49
2.3.2 Further preliminary results . . . . .	55
2.3.3 The construction: A high-level perspective . . . . .	62
2.3.4 A primer on Gröbner basis techniques . . . . .	63
2.3.5 The construction in details . . . . .	65
2.4 MUBs, MASAs and complex Hadamard matrices . . . . .	72
2.4.1 Connections to operator algebras . . . . .	72

2.4.2	The problem of Mutually Unbiased Bases in $\mathbb{C}^n$ . . . . .	73
2.4.3	Towards the solution of the MUB-6 problem . . . . .	76
2.4.4	MUBs and equiangular lines in $\mathbb{C}^n$ . . . . .	77
<b>3</b>	<b>Complex Hadamard matrices of prime orders</b>	<b>81</b>
3.1	Preliminaries . . . . .	82
3.2	Petrescu's construction revisited . . . . .	82
3.2.1	Constructing a $BH(19, 6)$ matrix . . . . .	85
3.2.2	Some non-existence results . . . . .	87
3.3	Circulant complex Hadamard matrices . . . . .	90
3.3.1	Cyclic $p$ -roots of simple index 2 . . . . .	94
3.3.2	Cyclic $p$ -roots of simple index 3 . . . . .	94
3.3.3	Cyclic $p$ -roots of simple index 4 . . . . .	96
3.4	Hadamard matrices with few different entries . . . . .	102
3.4.1	Two different entries . . . . .	103
3.4.2	Three different entries . . . . .	104
3.5	Application: Equiangular tight frames . . . . .	108
	<b>Bibliography</b>	<b>113</b>
	<b>Appendix A Petrescu-type Hadamard matrices</b>	<b>125</b>
A.1	Some small dimensional examples . . . . .	125
	<b>Appendix B All cyclic 17-roots of simple index 4</b>	<b>127</b>
B.1	The polynomial describing the solutions . . . . .	127
B.2	Analysing the solutions . . . . .	128
B.2.1	Solutions coming from $V_1(x)$ . . . . .	129
B.2.2	Solutions coming from $V_2(x)$ . . . . .	129
B.2.3	Solutions coming from $V_3(x)V_4(x)$ . . . . .	129
B.2.4	Solutions coming from $V_5(x)$ . . . . .	130
B.2.5	Solutions coming from $V_6(x)$ . . . . .	130
B.3	Concluding remarks . . . . .	132
	<b>Appendix C Hadamard matrices with circulant core</b>	<b>133</b>
C.1	The general theory . . . . .	133
C.1.1	Circulant core of index $k$ type . . . . .	135
C.2	Classification up to order 7 . . . . .	137



# Introduction

“Art is never finished, only abandoned.”

---

LEONARDO DA VINCI

This thesis is based on our recent research contributions to the theory of complex Hadamard matrices [129], [130], [131], [132], [134]. Some earlier results are also touched upon such as [71], [102], [103], as well as several new results which will be the subject of forthcoming publications.

Complex Hadamard matrices form an important family of orthogonal arrays with the additional unimodularity constraint imposed on their entries. These matrices obey the algebraic identity  $HH^* = nI_n$  where  $*$  stands for the Hermitian transpose, and  $I_n$  is the identity matrix of order  $n$ . It is easy to see that after proper scaling the Fourier matrices are well-known examples of complex Hadamard matrices.

Complex Hadamard matrices appear frequently in various branches of mathematics, including linear algebra [55], coding and operator theory [60], [115] and harmonic analysis [84], [140]. They play an important rôle in quantum optics, high-energy physics, and they are one of the key ingredients to quantum teleportation and dense coding schemes [144] and mutually unbiased bases (MUBs) [47].

The intended purpose of this work is to provide the reader with a comprehensive, state-of-the art presentation of the theory of complex Hadamard matrices, or at least report on the very recent advances. This manuscript consists of three chapters, each describing one of three distinct faces of this field whose treatment require various mathematical tools ranging from combinatorics, functional analysis to symbolic computation. Although we firmly believe that these beautiful objects are interesting on their own and worth investigating from a purely mathematical perspective we make considerable efforts to highlight some of their applications we aware of. Industrial applications can be found in the textbooks [1] and [67] which are warmly recommended to the interested reader.

This thesis has three main ingredients: known results from the existing literature; our contribution to the literature; and new results which are subject to a series of forthcoming publications. Each of these constitute about one third of this manuscript.

We are certain that this dissertation is just the starting point of a long-term journey and in order to keep us (and hopefully others) entertained along the way we pose over 30 research problems worth investigating in the future.

In the subsequent sections we outline, chapter by chapter, the contents of this thesis highlighting our main contributions.

## Complex Hadamard matrices of composite orders

In Chapter 1 we lay down the foundations of this work by recalling the relevant notions and results from the existing literature. Original interest was in real Hadamard matrices [61] whose existence is still a mystery. The Hadamard conjecture states that for every positive integer  $m$  there is a real Hadamard matrix of order  $4m$ . This century-old problem is currently far out of reach, despite continuous efforts. It is natural to investigate the problem in more generality and study complex Hadamard matrices of order  $n$  which are formed by some  $q$ th roots of unity. These matrices are called Butson-Hadamard matrices and are denoted by  $BH(n, q)$ . Researchers are interested in these more general objects because they can lead to real Hadamard matrices [28] and hopefully one day to the solution of the Hadamard Conjecture.

One of the fundamental differences between real and complex Hadamard matrices is that while studying and classifying real Hadamard matrices is a discrete problem which can be handled by deep algebraic methods and sophisticated computer programs, in the complex case various infinite, parametric families appear (i.e. matrices with certain degree of freedom). Therefore the complex case is not finite any longer and one cannot hope for a finite list of complex Hadamard matrices.

We investigate the parametrization properties of  $BH(n, q)$  matrices focusing on the cases  $q = 4$  and  $6$ . We give a comprehensive classification of  $BH(n, 4)$  matrices up to order  $n = 8$  and highlight some key facts regarding orders  $n = 10$  and  $12$  from a joint work with Pekka Lampio and Patric Östergård [92]. In particular, we mention the following two results.

**Theorem A.** *For  $4 \leq n \leq 12$  all  $BH(n, 4)$  matrices belong to some infinite, affine parametric family of complex Hadamard matrices.*

On the other hand, there are  $14 \times 14$  matrices which cannot be parametrized at all. This is a fundamental difference from the real case.

**Theorem B.** *There exist isolated  $BH(14, 4)$  matrices.*

The new result regarding  $BH(n, 6)$  matrices were obtained during a visit to Robert Craigen. We have obtained the following

**Theorem C.** *For every prime  $p$  there exists a  $BH(p^2, 6)$  matrix.*

To distinguish essentially different complex Hadamard matrices from each other we have introduced a powerful new invariant, the fingerprint [132].

As an application of Butson-Hadamard matrices we give a further look at Fuglede's conjecture [54] and obtain new, previously unknown counterexamples.

## Towards the classification of $6 \times 6$ Hadamard matrices

It is natural to ask what a “typical” complex Hadamard matrix of order  $n$  looks like, and a satisfying answer to this question can be given provided we have at our disposal a complete characterization of Hadamard matrices of order  $n$ . These types of problems, however, are notoriously difficult even for small  $n$ .

There is a complete classification of real Hadamard matrices up to order  $n = 28$ , and recent advances indicate that there is every reason to believe that at least an enumeration of the millions of matrices of order 32 and 36 is possible as well [81]. In contrast, a complete classification of complex Hadamard matrices is only available up to order  $n = 5$ . It is easy to see that the (rescaled) Fourier matrices are the unique examples in orders  $n \leq 3$ . The case  $n = 4$  is still elementary, and it was shown by Craigen that all complex Hadamard matrices of order 4 belong to an infinite, continuous one-parameter family [34]. In order 5 we have uniqueness again, a result which already is absolutely non-trivial. In particular, Lovász was the first who showed [101] that the Fourier matrix is the only circulant complex Hadamard matrix of order 5, and a decade later Haagerup managed to prove the uniqueness of the Fourier matrix by discovering an algebraic identity (see formula (2.16)) relating the matrix entries in a surprising way [60].

In order 6 various one [6], [44], [103] and [149]; two [77], [129]; and three-parameter families [76] have been constructed recently and it was conjectured that these are part of a more general, four-parameter family of complex Hadamard matrices [8]. This conjecture is supported by overwhelming numerical evidence [125], however so far only a fairly small subset of it was described by closed analytic formulae, including an isolated matrix  $S_6^{(0)}$  and a three-parameter family of matrices  $K_6^{(3)}$ . One of the main reasons why the complex case is so difficult is the presence of infinite parametric families and the lack of understanding of vanishing sums of order  $k$  for  $k \geq 5$ . In Chapter 2 we make substantial progress towards the classification of  $6 \times 6$  complex Hadamard matrices by giving a construction with four degrees of freedom. We believe that our construction captures the typical features of complex Hadamard matrices of order 6. The main result is essentially the following

**Theorem D.** *There is a four-parameter family of  $6 \times 6$  complex Hadamard matrices.*

The reason why the  $6 \times 6$  case received significant attention in the past couple of years is the fact that complex Hadamard matrices are closely related to mutually unbiased bases. Recall that two orthonormal bases of  $\mathbb{C}^n$ ,  $\mathcal{B}_1$  and  $\mathcal{B}_2$  are unbiased if for every  $e \in \mathcal{B}_1$ ,  $f \in \mathcal{B}_2$  we have  $|\langle e, f \rangle|^2 = 1/n$ . A family of orthonormal bases is said to be (pairwise) mutually unbiased if every two of them are unbiased. The famous MUB-6 problem asks for the maximal number of mutually unbiased bases in  $\mathbb{C}^6$ . On the one hand this number is at least 3, as there exists various infinite families of triplets of MUBs in this order [71], [129], [149]. In particular, by utilizing an elegant construction of Zauner [149] we obtain the following

**Theorem E.** *There is a two-parameter family of triplet of MUBs in  $\mathbb{C}^6$ .*

On the other hand it is well-known that the number of pairwise mutually unbiased bases cannot be larger than 7 (see the references of [8]) in  $\mathbb{C}^6$ . In fact, it is conjectured that a triplet is the best one can come up with in dimension 6 [149]. The connection between MUBs and Hadamard matrices of order 6 has been exploited in our joint work [71] very recently, where a discretization scheme was offered to attack the problem and it was proved by means of computers, however, in a mathematically rigorous way, that the members of the two-parameter Fourier family  $F_6^{(2)}(a, b)$  and its transpose cannot belong to a configuration of 7 MUBs containing the standard basis in dimension 6. One reasonable hope to finally settle the MUB-6 problem is to give a complete characterization of complex Hadamard matrices of order 6 and apply the same technique to them.

During Chapter 2 we propose a general framework towards the complete classification of complex Hadamard matrices of order 6. In particular, by characterizing the orthogonal triplets of rows in complex Hadamard matrices we generalize an observation of Haagerup [60] to obtain a new algebraic identity relating the matrix entries in an unexpected way. This is an essentially new tool to study complex Hadamard matrices of small orders, and one of the main achievements of this chapter. We apply this result to obtain complex Hadamard matrices, moreover we conjecture that the construction we present here reflects the true nature of complex Hadamard matrices of order 6. It has the following three features: Firstly, it is general in contrast with the earlier attempts where always some additional extra structure was imposed on the matrices including self-adjointness [6], symmetry [103], circulant block structure [129] or  $H_2$ -reducibility [75]. Secondly, it has 4 degrees of freedom and thirdly all the entries of the obtained matrices can be described by algebraic functions of roots of various sextic polynomials. This suggests on the one hand the existence of a four-parameter family of complex Hadamard matrices of order 6 and reminds us on the other hand

of the fact that the desired algebraical description where the entries are expressed by closed analytic formulae might not be possible at all. However, from the applicational point of view, and in particular, to utilize the computer-aided attack of [71] to the MUB-6 problem we anyway only need these matrices numerically.

Finally, to illustrate the applications of MUBs we exhibit equiangular lines in real spaces. Our results slightly improve on a recent construction of de Caen [39].

**Theorem F.** *For each  $n = 3 \cdot 2^{2t-1} + 1$ , with  $t$  any positive integer, there exists an equiangular set of  $\frac{2}{9}(n-1)(n+2)$  lines in  $\mathbb{R}^n$ .*

As a consequence we obtain a new general quadratic lower bound on the number of real equiangular lines (see Corollary 2.4.40).

## Complex Hadamard matrices of prime orders

The final chapter is devoted to the discussion of complex Hadamard matrices of prime orders. Constructing complex Hadamard matrices of prime orders requires considerable efforts. One of the reasons for this is that design theory fundamentally relies on “plug-in” methods and block constructions resulting in objects of composite orders. Furthermore it is known that the Fourier matrices of prime orders are isolated thus we do not have natural examples of parametric families of complex Hadamard matrices in the prime order case. Throughout Chapter 3 we recall Petrescu’s construction [113] and obtain new interesting examples of  $BH(n, q)$  matrices. On the one hand we settle the existence of  $BH(19, 6)$  matrices which is listed as unresolved in [27], on the other hand we obtain some non-existence results.

**Theorem G.** *There exists a  $BH(19, 6)$  matrix.*

We list several new examples of  $BH(n, q)$  matrices in Appendix A. Among these there is a  $BH(13, 30)$  matrix leading to a four-parameter family of complex Hadamard matrices of order 13.

In the subsequent sections we investigate circulant complex Hadamard matrices. Following the influential paper [11] we construct new examples of index 4 type circulant complex Hadamard matrices of prime orders. In particular, we prove the following

**Theorem H.** *For every prime  $p \equiv 1 \pmod{8}$  there is a new, previously unknown complex Hadamard matrix of simple index 4.*

These matrices come from an object which is the analogue of the well-known Paley matrix, but instead of describing the quadratic residues in  $\mathbb{Z}_p$  it encodes the quartic residues. In general the entries of these matrices are rather complicated. We believe

that some further improvements on our work will eventually lead to the full classification of all cyclic  $p$ -roots of simple index 4 when  $p \equiv 1 \pmod{8}$  is prime. The case  $p = 17$  is worked out in details in Appendix B.

Finally we investigate the problem of finding all complex Hadamard matrices with circulant core and solve it for  $n \leq 7$  yielding a new, previously unknown complex Hadamard matrix of order 7. To deal with this problem we utilize the full machinery of the theory of Gröbner bases [20] and we use it to investigate some special classes of higher order matrices as well. This computer experiment turned out to be fruitful as we have discovered two infinite classes of complex Hadamard matrices as follows:

**Theorem I.** *For every prime  $p \equiv 1 \pmod{8}$  there are two new, previously unknown examples of complex Hadamard matrices of order  $p + 1$ , having a circulant core.*

The underlying object behind both of these matrices are, again, the quartic residues in  $\mathbb{Z}_p$ . These results are rather technical and they are contained in Appendix C.

We conclude the thesis by investigating complex Hadamard matrices with few different entries, and we utilize them to construct new examples of equiangular tight frames [12].

# Acknowledgements

I am greatly indebted to Professor Máté Matolcsi for his continuous guidance and support since my freshman year. I am grateful for his permanent influence on my mathematical outlook and for his patience and wisdom allowing me to explore the mathematics I am fascinated with. I feel fortunate that during these years I had the opportunity of learning from him and doing research with him.

My warmest thanks go to Professor Robert Craigen who supervised my work during my visit as a guest student at the University of Manitoba. The training he provided me with substantially improved my knowledge on the subject of this thesis.

I acknowledge financial support by Central European University grant no. DRSG-131/2010-11; Hungarian Scientific Research Fund (OTKA) grant no. K-77748; and National Sciences and Engineering Research Council of Canada (NSERC) grant no. 155855-09.

Ferenc Szöllősi

szoferi@gmail.com

Budapest, October 25, 2011.





# Chapter 1

## Complex Hadamard matrices of composite orders

The purpose of this introductory chapter is to describe the basic terminology and the fundamental properties of complex Hadamard matrices. We shall give various examples of infinite, parametric families as well as examples of isolated complex Hadamard matrices in the sequel. Hadamard matrices, composed from roots of unity shall be investigated in details. Our intentions were to include relevant structural results from the existing very recent literature giving this chapter a survey flavour. The reader interested in classical results concerning real and generalized Hadamard matrices should consult Agaian's [1] or Horadam's book [67], or read the PhD thesis of Seberry [143] or Craigen [32]. Our contribution to this chapter is based on the papers [102], [132], [134] and the preprint [92]. Additionally, we briefly mention the important achievements from [133] and [135]. The new results in Sections 1.4.2 and 1.4.3 are subject to a possible forthcoming publication.

We begin our journey with investigating the existence of complex Hadamard matrices.

### 1.1 Existence of complex Hadamard matrices

Throughout this thesis we denote by  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$  and  $\mathbb{T}$  the natural, integral, rational, real, complex and complex unimodular numbers, respectively. We assume that  $0 \in \mathbb{N}$ . We denote the matrices by capital letters, e.g.  $I$  or  $I_n$  is the identity matrix of order  $n$ . We usually drop the subscript if it is irrelevant or clear from context. For a given matrix  $A$  we denote by  $\overline{A}$ ,  $A^T$  and  $A^*$  its entrywise conjugate, transpose and hermitean adjoint, respectively. The space of all  $n \times n$  complex matrices is denoted by  $\mathcal{M}_n(\mathbb{C})$ .

Our dissertation is entirely devoted to investigate the existence and the structure of the following concept.

**Definition 1.1.1.** A *complex Hadamard matrix*  $H$  is an  $n \times n$  matrix with complex entries of modulus 1 such that  $HH^* = nI$ .

Therefore a complex Hadamard matrix is essentially a unitary matrix with unimodular entries. Of course, we obtain a unitary matrix after proper normalization. As we shall see, it is easy to exhibit a complex Hadamard matrix in every order  $n$  but first let us fix some notations once and for all.

**Definition 1.1.2.** Throughout this thesis we denote by  $\Re[z]$  and  $\Im[z]$  the real and imaginary part of a complex number  $z$ , respectively. We denote by  $\mathbf{i}$  the principal fourth root of unity, that is  $\mathbf{i}^2 = -1$  with the convention that  $\Im[\mathbf{i}] = 1$ . Finally, let us denote by  $\omega$  the principal cubic root of unity, namely

$$\omega = \cos\left(\frac{2\pi}{3}\right) + \mathbf{i} \sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + \mathbf{i}\frac{\sqrt{3}}{2}.$$

With these notations at our hand, we can offer our very first

**Lemma 1.1.3.** *For every  $n \geq 1$  there exists a complex Hadamard matrix of order  $n$ .*

*Proof.* Indeed, as the Fourier matrix

$$[F_n]_{i,j} = \mathbf{e}^{2\pi\mathbf{i}(i-1)(j-1)/n}, \quad i, j = 1, \dots, n \quad (1.1)$$

is a well-known example of complex Hadamard matrices.  $\square$

Note that throughout this manuscript the term “Fourier matrix” is used to describe the complex Hadamard matrix  $F_n$  under (1.1), and not the unitary matrix  $\frac{1}{\sqrt{n}}F_n$ . We offer the following

**Example 1.1.4.** The following are complex Hadamard matrices of orders  $n = 1, 2$  and  $3$ , respectively:

$$F_1 = \begin{bmatrix} 1 \end{bmatrix}, \quad F_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad F_3 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix}.$$

One immediately observes that the matrices displayed in the preceding example all have a bordering row and column of numbers 1. This is a general feature of complex Hadamard matrices, up to the following equivalence.

**Definition 1.1.5.** The complex Hadamard matrices  $H$  and  $K$  are called (permutation-phasing) *equivalent*, if there are permutation matrices  $P_1$  and  $P_2$  and unitary diagonal matrices  $D_1$  and  $D_2$  such that  $P_1 D_1 H D_2 P_2 = K$ . This relation is denoted by  $H \sim K$ . If two Hadamard matrices are not equivalent then we say that they are inequivalent.

Definition 1.1.5 exploits the fact that the rearrangement of the rows and columns or the shift of the phase in any row or column of a complex Hadamard matrix maintains its fundamental properties: both the unitary and unimodular conditions still hold after these transformations. We recall the following

**Definition 1.1.6.** A complex Hadamard matrix  $H$  of order  $n$  is *dephased* if the first row and column of it consists of entirely of numbers 1. The lower right  $(n-1) \times (n-1)$  submatrix is called the *core* of  $H$ .

A dephased real Hadamard matrix is usually called normalized. It is immediate, that the following is true.

**Lemma 1.1.7.** *Every complex Hadamard matrix is equivalent to a dephased one.*

Henceforth it is enough to consider dephased complex Hadamard matrices. There are other “trivial” ways to obtain new complex Hadamard matrices from what is already at our hands. In particular, we have the following

**Lemma 1.1.8.** *If  $H$  is a complex Hadamard matrix, then so is  $H^*$ ,  $\overline{H}$  and  $H^T$ .*

*Proof.* Let  $H$  be a complex Hadamard matrix. Then conjugate the identity  $HH^* = nI$  in order to see that  $\overline{H}$  is a complex Hadamard matrix as well. It is also clear that  $H$  is invertible and  $H^{-1} = H^*/n$ . Hence, it follows that  $H^*H = nI$ , which shows that both  $H^*$  and, after conjugating again,  $H^T$  are complex Hadamard matrices.  $\square$

Another natural approach to construct new matrices from old is to lift given objects to higher orders via the Kronecker product. We use the following concept repeatedly in our manuscript.

**Definition 1.1.9.** Let  $H$  be an  $n \times n$ ,  $K$  be an  $m \times m$  matrix. Then their *Kronecker product*  $H \otimes K$  is an  $nm \times nm$  matrix with its  $(i, j)$ th block being given by  $[H]_{i,j}K$ ,  $i, j = 1, \dots, n$ .

The following is immediate.

**Lemma 1.1.10.** *If  $H$  and  $K$  are complex Hadamard matrices then so is  $H \otimes K$ .*

*Proof.* Clearly  $H \otimes K$  is unimodular, moreover

$$(H \otimes K)(H \otimes K)^* = HH^* \otimes KK^* = nI_n \otimes mI_m,$$

which can be identified with  $nmI_{nm}$ .  $\square$

In 1867 Sylvester constructed real Hadamard matrices of orders  $n = 2^k$  for every  $k \geq 1$  via Lemma 1.1.10, starting from the Fourier matrix  $F_2$  [127]. For comparison, we give an additional

**Example 1.1.11.**

$$H_4 = F_2 \otimes F_2 = \left[ \begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ \hline 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{array} \right], \quad F_4 = \left[ \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 1 & \mathbf{i} & -1 & -\mathbf{i} \\ 1 & -1 & 1 & -1 \\ 1 & -\mathbf{i} & -1 & \mathbf{i} \end{array} \right].$$

It is not immediately clear that the matrices  $H_4$  and  $F_4$  are inequivalent. Later we shall see several invariants easily detecting inequivalence in this, and various other cases. Here we offer the general treatment of the Kronecker product of Fourier matrices.

**Theorem 1.1.12** (Tadej, [137]). *Let  $F = F_{n_1} \otimes F_{n_2} \otimes \cdots \otimes F_{n_r}$  be a Kronecker product of Fourier matrices. Then  $F$  is equivalent to  $F_{m_1} \otimes F_{m_2} \otimes \cdots \otimes F_{m_s}$  if and only if the sequence  $(m_1, m_2, \dots, m_s)$  is obtained from the sequence  $(n_1, n_2, \dots, n_r)$  using a series of operations from the list below:*

1. *permuting a sequence;*
2. *replacing a subsequence  $n_a, n_b$  by  $n_c = n_a n_b$  if  $n_a$  and  $n_b$  are relatively prime;*
3. *replacing a sequence element  $n_c$  by a subsequence  $n_a, n_b$ , if  $n_c = n_a n_b$  and  $n_a, n_b$  are relatively prime.*

It follows from Theorem 1.1.12 that the matrices displayed in Example 1.1.11 are inequivalent. Therefore we already have a handful of examples of complex Hadamard matrices coming from purely the Fourier matrices at our disposal. Another source of examples are the real Hadamard matrices. It is natural to ask the following

**Problem 1.1.13.** Decide for which orders  $n$  exists a real Hadamard matrix.

It is immediate from Lemma 1.1.7 that the order of such a matrix must be 1 or even. However, a little more careful analysis reveals the following

**Lemma 1.1.14.** *If a real Hadamard matrix of order  $n$  exists, then  $n = 1, 2$  or  $n \equiv 0 \pmod{4}$ .*

It is widely believed that this is the only obstruction. In particular, we have the following long-standing

**Conjecture 1.1.15** (The Hadamard conjecture, [111]). *If  $n \equiv 0 \pmod{4}$  then there is a real Hadamard matrix.*

The truth of Conjecture 1.1.15 has been verified for orders  $n \leq 664$ ; order  $n = 428$  has been constructed only very recently in [80]. There are 13 open cases below  $n = 2000$

for which the existence is undecided [45], all of them are of the form  $n = 4p$  where  $p \equiv 3 \pmod{4}$  is prime.

From Lemma 1.1.14 it follows that there is no real Hadamard matrix of orders 5, 6 or 7. For order 8 we have a unique (up to equivalence) example given by  $F_2 \otimes F_2 \otimes F_2$ , while constructing a matrix of order 12 requires some additional terminology (see also the intriguing Example 1.4.40).

**Definition 1.1.16.** We say that an  $n \times n$  matrix  $C$  is *circulant*, induced by its first row  $x = (x_0, x_1, \dots, x_{n-1})$ , if  $C_{i,j} = x_{j-i}$  where the indices are taken modulo  $n$ . We usually denote such a matrix by  $C = \text{Circ}(x)$ . Similarly, we denote by  $D = \text{Diag}(x)$  a diagonal matrix of order  $n$  with main diagonal  $x$ .

Throughout this thesis we denote by  $\mathbb{Z}_p$  the ring of integers modulo  $p$ . Similarly,  $\mathbb{Z}_p^*$  stands for the multiplicative group of the nonzero elements of  $\mathbb{Z}_p$ . Now in order to construct a matrix of order 12, we recall the following fundamental

**Theorem 1.1.17** (Paley construction, [111]). *Let  $p$  be a prime number,  $p \equiv 3 \pmod{4}$ , and consider a vector  $x$  such that  $x_0 = 0$  and  $x_i = 1$  if  $i$  is a quadratic residue in  $\mathbb{Z}_p^*$ , otherwise  $x_i = -1$ . Let us define the Paley matrix  $P := \text{Circ}(x)$ . Then, the matrix  $C := P - I$ , bordered by a row and column of numbers 1 is a real Hadamard matrix of order  $p + 1$ .*

The Paley construction can be generalized to prime power orders as well using finite fields. In particular, for every prime  $p$  and  $k \geq 1$  there are real Hadamard matrices of order  $n = p^k + 1$  or  $n = 2(p^k + 1)$ , depending on whether we have  $p^k \equiv 3 \pmod{4}$  or  $p^k \equiv 1 \pmod{4}$ , respectively. It is worthwhile noting that Theorem 1.1.17 leads to real Hadamard matrices with circulant core. We will return to these objects later in Appendix C.

A Hadamard matrix of order 20 was constructed by Hadamard in 1893 [61], and it took a century to have a complete classification of real Hadamard matrices of order at most 28 [126], while the enumeration of Hadamard matrices of order 32 begun just very recently, yielding over 13 million inequivalent matrices [81].

Let us try to understand how good we are doing in terms of Conjecture 1.1.15. In order to measure this, let us denote by  $S(x)$  the number of  $n \leq x$  for which a Hadamard matrix of order  $n$  exists. Now the Hadamard conjecture states that  $S(x)$  is about  $x/4$ , and hence the set of Hadamard orders has density  $1/4$ . As yet, it is not even known if this set has positive density, as taking into account all major known construction methods, one obtains only the following

**Theorem 1.1.18** (de Launey–Gordon, [42]). *For all  $\varepsilon > 0$  there is a natural number*

$x_\varepsilon$  such that for all  $x > x_\varepsilon$

$$S(x) \geq \frac{x}{\log x} \exp((C + \varepsilon)(\log \log \log x)^2),$$

for  $C = 0.8178\dots$

However, from another point of view we are doing quite well, as Seberry proved that for every odd  $m$  and for every large enough  $t = t(m)$ , there is a real Hadamard matrix of order  $n = 2^t m$  [123]. This was subsequently improved by Craigen [36]; currently the best known asymptotic result of this flavour is the following

**Theorem 1.1.19** (see [27]). *A Hadamard matrix of order  $2^t m$  for odd  $m$  exists for all*

$$t \geq 6 \left\lfloor \frac{\log_2 \frac{m-1}{2}}{16} \right\rfloor + 2.$$

In particular, for every odd  $m$  there are only finitely many numbers  $t$  such that the existence of a real Hadamard matrix of order  $2^t m$  is undecided.

A different approach is to try to guarantee a large number of pairwise orthogonal rows of  $\{\pm 1\}$  entries in a given order  $n$ . Let us denote by  $r(n)$  the largest number  $r$  such that there are  $r$  pairwise orthogonal  $\{\pm 1\}$  rows of length  $n$ . Then the following is true.

**Theorem 1.1.20** (de Launey–Gordon, [41]). *Let  $\varepsilon > 0$ . If the Extended Riemann Hypothesis is true, then for every sufficiently large  $n \equiv 0 \pmod{4}$*

$$r(n) \geq \frac{n}{2} - n^{\frac{17}{22} + \varepsilon}.$$

Thus, for  $n$  large enough we have about one half of a real Hadamard matrix of order  $n$ . It seems, however, that despite continuous efforts from researchers from a broad area, proving the truth of the Hadamard conjecture remains elusive, and fundamental new ideas are required for further progress.

## 1.2 Parametrizing complex Hadamard matrices

In this section we introduce the concept of parametrization, a powerful method obtaining new complex Hadamard matrices from old. The parametrization can be thought as a continuous analogue of the switching operation [110], a well-known technique in design-theory. These ideas were used by Craigen [34], Diță [44], Haagerup [60] and Nicoară [107] (among others), who exhibited various parametric families in the last decade. It should be noted that Hadamard himself, who investigated  $4 \times 4$  matrices with maximum determinant, exhibited essentially the following

**Example 1.2.1** (cf. [34], [61]). For every unimodular number  $a$  the matrix

$$F_4^{(1)}(a) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \mathbf{i}a & -1 & -\mathbf{i}a \\ 1 & -1 & 1 & -1 \\ 1 & -\mathbf{i}a & -1 & \mathbf{i}a \end{bmatrix}$$

is complex Hadamard, forming a one-parameter family of complex Hadamard matrices, stemming from the starting point matrix  $F_4 = F_4^{(1)}(1)$ .

The preceding example describes a family of complex Hadamard matrices as it incorporates various inequivalent matrices through the indeterminate  $a$ . In particular, for  $a = 1$  we have the Fourier matrix  $F_4 = F_4^{(1)}(1)$ , while for  $a = \mathbf{i}$  we get the real Hadamard matrix  $H_4 = F_2 \otimes F_2$ , which are inequivalent. We can look at this phenomenon from a different point of view. One might start with the single matrix  $F_4$ , and then try to find a way to introduce some degree of freedom into it, say, by introducing the parameter  $a$  as in Example 1.2.1 in order to exhibit new, previously unknown matrices, which are inequivalent from the starting point one. This approach, as we shall see in Section 1.4.3 where we discuss spectral sets and tiles in abelian groups, can lead to some very exciting discoveries.

Compare Example 1.2.1 with the following

**Example 1.2.2.** Consider the Fourier matrix  $F_3$  and multiply its second row by a unimodular number  $a$ , and multiply its third column by a unimodular number  $b$  to obtain the following

$$H_3^{(2)}(a, b) = \begin{bmatrix} 1 & 1 & b \\ a & \omega a & \omega^2 ab \\ 1 & \omega^2 & \omega b \end{bmatrix}.$$

We immediately see that for any unimodular choice of  $a$  and  $b$  the following equivalence holds

$$\text{Diag}(1, \bar{a}, 1)H_3^{(2)}(a, b)\text{Diag}(1, 1, \bar{b}) = F_3.$$

Therefore the seemingly two degrees of freedom does not give us even a single new matrix, being inequivalent from the starting-point matrix  $F_3$ .

The “trivial” parametrization coming from the multiplication by unitary diagonal matrices should be excluded, as it never leads to anything interesting. For this reason we will consider only families of dephased complex Hadamard matrices. Note here that for any complex Hadamard matrix  $H$  there is only a finite number of dephased complex Hadamard matrices  $K$  being equivalent to it (see Remark 1.3.3). This means, loosely speaking, that if we have a  $k$ -parameter family of dephased complex Hadamard matrices then it genuinely leads to a  $k$ -parameter family of inequivalent matrices. Before

formalizing these concepts mathematically rigorously, let us recall that  $\circ$  denotes the entry-wise (or Hadamard) product of matrices. Furthermore, let us denote by  $\text{EXP}(\cdot)$  the entry-wise exponential function acting on matrices. We recall the following

**Definition 1.2.3** (Tadej–Życzkowski, [138]). An *affine Hadamard family*  $H(V)$  stemming from a starting-point dephased  $n \times n$  complex Hadamard matrix  $H$ , associated with a subspace  $V$  of the space of all real  $n \times n$  matrices with zeros in the first row and column is the set of matrices  $\{H \circ \text{EXP}(\mathbf{i}R) : R \in V\}$ . We say that  $H(V)$  is a  $\dim(V)$ -parameter affine family.

Now let us see how to obtain interesting affine families in composite orders. We have the following fundamental

**Theorem 1.2.4** (Hosoya–Suzuki, [68]). Let  $M_1, M_2, \dots, M_v$  be  $k \times k$ ,  $N_1, N_2, \dots, N_k$  be  $v \times v$  complex Hadamard matrices. Then the generalized tensor product matrix, denoted by  $(M_1, M_2, \dots, M_v) \otimes (N_1, N_2, \dots, N_k)$ , whose  $(i, j)$ th block is given by the matrix  $\text{Diag}([M_1]_{i,j}, [M_2]_{i,j}, \dots, [M_v]_{i,j})N_j$  is a complex Hadamard matrix of order  $vk$ .

**Corollary 1.2.5** (Diță's construction, [44]). Let  $M$  be a  $k \times k$  and  $N_1, N_2, \dots, N_k$  be  $v \times v$  dephased complex Hadamard matrices with  $m$  and  $n_1, n_2, \dots, n_k$  free parameters, respectively. Then the block matrix  $M \otimes (N_1, N_2, \dots, N_k)$  with its  $(i, j)$ th block given by  $[M]_{i,j}N_j$  is a complex Hadamard matrix of order  $vk$  with  $m + \sum_{i=1}^k n_i + (k-1)(v-1)$  free parameters.

**Definition 1.2.6** (see [102]). We say that a complex Hadamard matrix is of *Diță-type*, if it is equivalent to a matrix arising with Corollary 1.2.5.

We offer the following

**Example 1.2.7.** Let  $k = 4, v = 2$ . Set the  $4 \times 4$  matrices to  $M_1 = F_4^{(1)}(a)$  and  $M_2 = F_4^{(1)}(b)$  while the  $2 \times 2$  matrices to  $N_1 = F_2, N_2 = \text{Diag}(1, c)F_2, N_3 = \text{Diag}(1, d)F_2$  and  $N_4 = \text{Diag}(1, e)F_2$ . Then the Hosoya–Suzuki construction leads to

$$H_8^{(5)}(a, b, c, d, e) = \left[ \begin{array}{cc|cc|cc|cc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & c & -c & d & -d & e & -e \\ \hline 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & c & -c & -d & d & -e & e \\ \hline 1 & 1 & -1 & -1 & a & a & -a & -a \\ 1 & -1 & -c & c & bd & -bd & -be & be \\ \hline 1 & 1 & -1 & -1 & -a & -a & a & a \\ 1 & -1 & -c & c & -bd & bd & be & -be \end{array} \right].$$



Note that we obtained a five-parameter family whereas Diță's construction with  $M_1 = M_2$  would give us a matrix with  $1 + \sum_{i=1}^4 0 + (2-1)(4-1) = 4$  parameters only. However, we can set  $k = 2$  and  $v = 4$  and  $M_1 = M_2 = M_3 = M_4 = F_2$  and  $N_1 = F_4^{(1)}(a)$ ,  $N_2 = \text{Diag}(1, b, c, d)F_4^{(1)}(e)$  to obtain a five-parameter family via Diță's method as well.

*Remark 1.2.8.* Diță-type complex Hadamard matrices can be recognized algorithmically [102]. See also [24] for some other useful concepts.  $\square$

Not every parametric family is affine, and the treatment of non-affine families is somewhat more technical. Fortunately, as long as they are given explicitly we can detect easily how many degrees of freedom they have.

**Definition 1.2.9.** Let  $H: \mathbb{R}^m \rightarrow \mathbb{C}^{n^2}$  be a smooth function such that the domain of  $H$  is an open neighbourhood of  $(0, 0, \dots, 0)$ . Assume that  $H(x_1, x_2, \dots, x_m)$  is a dephased complex Hadamard matrix for all choices of  $(x_1, x_2, \dots, x_m)$  in the domain of  $H$ . We say that  $H(x_1, x_2, \dots, x_m)$  is a *k-parameter family of complex Hadamard matrices*, stemming from  $H(0, 0, \dots, 0)$ , if the rank of the Jacobian matrix  $J_H(x_1, x_2, \dots, x_m)$  is constant  $k$  on the domain of  $H$ . Note that here we have identified  $\mathcal{M}_n(\mathbb{C})$  with  $\mathbb{C}^{n^2}$ .

It is clear that affine families are a special case of this more general concept. The reader might wish to jump ahead to Section 2.2.2 to see an example of a non-affine family.

If we are given a complex Hadamard matrix  $H$  we would like to know whether any smooth family is stemming from it. This is hard to decide in general, but we can give an upper bound on the dimension of any such potential family simply by differentiating the orthogonality relations between the rows. This leads to the following concept:

**Definition 1.2.10** (Tadej-Życzkowski, [138]). The *defect*  $d(H)$  of an  $n \times n$  complex Hadamard matrix  $H$  reads  $d(H) = m - 2n + 1$  where  $m$  is the dimension of the solution space of the real linear system with respect to the matrix variable  $R \in \mathbb{R}^{n \times n}$ :

$$\sum_{k=1}^n H_{i,k} \overline{H}_{j,k} (R_{i,k} - R_{j,k}) = 0, \quad 1 \leq i < j \leq n. \quad (1.2)$$

Let us note here that the defect is well-defined in the following sense.

**Lemma 1.2.11** (Tadej-Życzkowski, [139]). *The defect is invariant under the usual equivalence. Moreover  $d(H) = d(\overline{H}) = d(H^T) = d(H^*)$ .*

We have the following fundamental

**Proposition 1.2.12** (Tadej-Życzkowski, [138]). *Let  $H$  be a complex Hadamard matrix. Then  $d(H)$  gives an upper bound on the dimension of a smooth manifold of complex Hadamard matrices, stemming from  $H$ .*

It is easy to see that if a phasing matrix  $R$  satisfies (1.2) then the matrix  $K := H \circ \text{EXP}(\mathbf{i}R)$  is complex Hadamard to first order (i.e. we get a complex Hadamard matrix numerically if  $R$  is very close to the zero matrix), [47].

**Example 1.2.13.** For the real Hadamard matrix  $H_4 = F_2 \otimes F_2$  we have  $d(H_4) = 3$ . In contrast, Example 1.2.1 describes a one-parameter family only. Later we shall see that this cannot be improved (see Proposition 2.1.3), and hence the defect can be strictly larger than the dimension of any smooth manifold, stemming from  $H_4$ .

The defect of the Fourier matrices is known explicitly, and is given by the following

**Proposition 1.2.14** (Słomczyński's formula, [139]). *Let  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \geq 2$  be a natural number with the factorization into distinct prime numbers  $p_i, i = 1, \dots, r$ . Then*

$$d(F_n) = n \prod_{i=1}^r \left( 1 + \alpha_i - \frac{\alpha_i}{p_i} - 2 \right) + 1. \quad (1.3)$$

While Theorem 1.2.4 provides access to parametric families of complex Hadamard matrices, it does not reveal how to introduce parameters into a given matrix. This question was investigated for the Fourier matrices in [139], where an explicit construction was given to introduce  $p^{k-1} (k(p-1) - p) + 1$  affine parameters into  $F_{p^k}$  thus demonstrating that the absolute upper bound in (1.3) is sharp.

In what follows we describe various parametrization schemes.

There is a fairly general method, called “linear variation of phases” [138] allowing one to find affine parametric families stemming from complex Hadamard matrices with certain additional symmetries; however the method becomes computationally expensive for higher order matrices, or for those lacking the required symmetries. Nevertheless the maximal affine families, stemming from the Fourier matrices has been obtained this way [139], and the method can also be used to introduce additional degree of freedom into existing parametric families [102].

We investigated real Hadamard matrices in [135], where the following simple way to introduce free parameters into complex Hadamard matrices of even orders  $n \geq 4$  was mentioned.

**Lemma 1.2.15.** *Let  $H$  be a dephased complex Hadamard matrix of even order  $n \geq 4$  and suppose that there exists a pair of rows in  $H$ , say  $u$  and  $v$ , such that for every  $i = 1, 2, \dots, n$   $u_i^2 = v_i^2$ . Then for all such  $i$  for which  $u_i + v_i = 0$  replace  $u_i$  with  $\alpha u_i$  and  $v_i$  with  $\alpha v_i$  where  $\alpha$  is a unimodular complex number to obtain a one-parameter family of complex Hadamard matrices  $H(\alpha)$ .*

*Proof.* Indeed,  $H(\alpha)$  is unimodular and it is easy to see that the assumptions guarantee that the columns of it are pairwise orthogonal. Note that one might need to dephase

the matrix in order to obtain an affine family, but this operation does not remove the parameters from it as  $n \geq 4$ .  $\square$

Let us denote by  $\langle \cdot, \cdot \rangle$  the standard inner product in  $\mathbb{C}^n$  with the usual convention that it is linear in the first, and conjugate-linear in the second variable. Additionally, let us denote by  $1^n$  the all-1 vector of length  $n$ . The following is a more robust method obtaining parametric families.

**Theorem 1.2.16** (see [92]). *Let  $H$  be a dephased complex Hadamard matrix with the following block structure*

$$H = \begin{bmatrix} 1 & 1 & 1 & 1^p & 1^q \\ 1 & a & b & x & y \\ 1 & b & a & x & -y \\ (1^r)^T & z^T & z^T & A & B \\ (1^s)^T & w^T & -w^T & C & D \end{bmatrix},$$

where  $a$  and  $b$  are arbitrary unimodular numbers. Then, after replacing the vectors  $y$  with  $\alpha y$  and  $w$  with  $\bar{\alpha} w$  we obtain a one-parameter family of complex Hadamard matrices  $H(\alpha)$ . If, in addition,  $b = a$  then we can replace  $w$  one more time with  $\alpha \beta w$  to obtain a two-parameter family of complex Hadamard matrices  $H(\alpha, \beta)$ .

*Proof.* We need to show that the rows of  $H(\alpha, \beta)$  are pairwise orthogonal. It is immediate that

$$\langle y, 1^q \rangle = 0,$$

and hence the first three rows of  $H(\alpha, \beta)$  are pairwise orthogonal. Similarly, it is easily seen that the rest of the rows (beyond the first three) are pairwise orthogonal within themselves. Additionally, the first row is trivially orthogonal to all further rows, as  $w_i$  cancels out from the orthogonality equations for  $i = 1, \dots, s$ . Therefore it remains to be seen that the second and third rows of  $H(\alpha, \beta)$  are orthogonal to all additional one. We show first that they are orthogonal to rows which are type  $[1, z_i, z_i, A_i, B_i]$ ,  $i = 1, \dots, r$ . In the original matrix  $H$  (i.e. prior to parametrizing) we have

$$1 + z_i(\bar{a} + \bar{b}) + \langle A_i, x \rangle + \langle B_i, y \rangle = 0, \quad (1.4)$$

$$1 + z_i(\bar{a} + \bar{b}) + \langle A_i, x \rangle - \langle B_i, y \rangle = 0, \quad (1.5)$$

and hence  $\langle B_i, y \rangle = 0$  for every  $i = 1, \dots, r$ . It follows that after parametrization equations (1.4)-(1.5) remain valid. We proceed by proving that rows which are type  $[1, w_i, -w_i, C_i, D_i]$ ,  $i = 1, \dots, s$ , after parametrization, are orthogonal to the second and third row of  $H(\alpha, \beta)$ . Again, in the original matrix  $H$  we have

$$1 + w_i \bar{a} - w_i \bar{b} + \langle C_i, x \rangle + \langle D_i, y \rangle = 0, \quad (1.6)$$

$$1 - w_i \bar{a} + w_i \bar{b} + \langle C_i, x \rangle - \langle D_i, y \rangle = 0, \quad (1.7)$$

and hence  $\langle C_i, x \rangle = -1$  for every  $i = 1, \dots, s$ . It follows, that (1.6)-(1.7) are valid, provided that

$$w_i \bar{a} - w_i \bar{b} + \langle D_i, y \rangle = 0, \quad (1.8)$$

and therefore (1.6)-(1.7) remains true, after parametrization. If, in addition,  $b = a$ , then  $\langle D_i, y \rangle = 0$  for every  $i = 1, \dots, s$  and hence (1.8) holds, independently of the scalar factor in  $w$ .  $\square$

*Remark 1.2.17.* If  $a$  and  $b$  are as in Theorem 1.2.16, then it is easy to see that the expression  $2\Re[a\bar{b}]$  is an integral number and therefore  $b \in \pm a \cdot \{1, \omega, \omega^2, \mathbf{i}\}$ . It follows that the parametrizing scheme described is “natural” for complex Hadamard matrices with fourth and sixth roots of unity.  $\square$

*Remark 1.2.18.* Theorem 1.2.16 describes a local property of the complex Hadamard matrix  $H$ . Its conditions can be fairly easily checked, even by hand, and the method can be implemented as a computer program to construct infinite families automatically. This has been done in [92], where complex Hadamard matrices, composed of fourth roots of unity were investigated.  $\square$

Nicoară in a series of papers [107], [108] considered commuting squares of matrix algebras [115], and using operator theory obtained two interesting parametrization schemes. His results also offered a conceptual proof of the existence of certain sporadic examples of parametric families of complex Hadamard matrices. Before turning to his results let us introduce some notations first. We denote by  $\mathbb{C}I_n$  and  $\mathcal{D}_n$  the algebra of the scalar and diagonal matrices, respectively. Further we write  $\exp(A)$  for the matrix exponential of  $A$ . Note that this is different from the entrywise exponential function  $\text{EXP}(\cdot)$  we used earlier. Additionally, the symbol  $\setminus$  denotes the set-theoretical exclusion, while  $[A, B] := AB - BA$  denotes the commutator of the matrices  $A$  and  $B$ .

**Theorem 1.2.19** (Nicoară, [107]). *Let  $H$  be a complex Hadamard matrix of order  $n$ , and assume that  $A \in \mathcal{D}_n \setminus \mathbb{C}I_n$ ,  $B \in H^* \mathcal{D}_n H \setminus \mathbb{C}I_n$  are self-adjoint, commuting matrices (i.e.  $[A, B] = AB - BA = 0$ ). Then, for any  $t \in \mathbb{R}$ ,  $U(t) = \exp(\mathbf{i}tAB)$  is a one-parameter family of unitary matrices, such that  $K_n^{(1)}(t) = HU(t)$  is a one-parameter family of complex Hadamard matrices.*

**Example 1.2.20.** Let  $H = F_2 \otimes F_2$ ,  $A = \text{Diag}(0, 0, 1, 1)$ ,  $B = H^*AH/4$ . Then  $A$  and  $B$  are self-adjoint, commuting matrices. Therefore the conditions of Theorem 1.2.19

are met, and as a result

$$U(t) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1+e^{it}}{2} & \frac{1-e^{it}}{2} \\ 0 & 0 & \frac{1-e^{it}}{2} & \frac{1+e^{it}}{2} \end{bmatrix}, \text{ such that } K_4^{(1)}(t) = HU(t) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & e^{it} & -e^{it} \\ 1 & -1 & -e^{it} & e^{it} \end{bmatrix}$$

is a one-parameter family of complex Hadamard matrices.

**Theorem 1.2.21** (Nicoară, [107]). *Let  $H$  be a complex Hadamard matrix of order  $n$ , and assume that  $A_1, A_2 \in \mathcal{D}_n \setminus \mathbb{C}I_n$ ,  $B_1, B_2 \in H^*\mathcal{D}_nH \setminus \mathbb{C}I_n$  are orthogonal projections such that  $[A_1, B_1] = [A_2, B_2]$ . Then, for any  $a \in \mathbb{T}$ ,  $U(a) = I_n + (a - 1)A_1B_1 + (\bar{a} - 1)A_2B_2$  is a one-parameter family of unitary matrices, such that  $K_n^{(1)}(a) = HU^*(a)$  is a one-parameter family of complex Hadamard matrices.*

**Example 1.2.22.** Let  $H = F_2 \otimes F_2 \otimes F_2$ ,  $A_1 = \text{Diag}(0, 0, 1, 0, 1, 0, 0, 0)$ , while  $A_2 = \text{Diag}(0, 0, 0, 1, 0, 1, 0, 0)$ ,  $B_1 = H^*A_1H/8$ ,  $B_2 = H^*A_2H/8$ . It is clear that the matrices  $A_1, A_2, B_1, B_2$  are self-adjoint projections, moreover  $A_1A_2 = B_1B_2 = 0$ ,  $[A_1, B_1] = [A_2, B_2]$ , and hence the conditions of Theorem 1.2.21 are met resulting in the one-parameter family of complex Hadamard matrices:

$$K_8^{(1)}(a) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & \bar{a} & 1 & -\bar{a} & -1 & -1 & -1 \\ 1 & -1 & 1 & -a & -1 & a & -1 & 1 \\ 1 & 1 & -\bar{a} & -1 & \bar{a} & 1 & -1 & -1 \\ 1 & -1 & -1 & a & 1 & -a & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}.$$

Now we discuss some of the consequences of these results. From Lemma 1.2.15 it follows that every real Hadamard matrix of order  $n \geq 4$  admits an  $n/2 - 1$ -parameter affine orbit. Actually, we have shown a little more in [135]:

**Proposition 1.2.23** (see [135]). *Every real Hadamard matrix of order  $n \geq 12$  admits an  $n/2 + 1$ -parameter affine orbit.*

However, if there are real Hadamard matrices of orders  $n_1$  and  $n_2$ , then one can do way better in orders  $n_1n_2$  via Diță's construction, improving the coefficient from  $1/2$  to 1 as follows:

**Corollary 1.2.24.** *Let  $H$  and  $K$  be real Hadamard matrices of order  $n_1$  and  $n_2$ . Then there is a family of complex Hadamard matrices of order  $n_1n_2$ , with  $(n_1 - 1)(n_2 - 1)$  affine parameters, stemming from a real Diță-type Hadamard matrix.*

In light of this, it is natural to pose the following

**Problem 1.2.25.** Improve on Proposition 1.2.23.

*Remark 1.2.26.* The parametrization highlighted in Proposition 1.2.23 (essentially) introduces parameters into distinct pairs of rows of a real Hadamard matrix via Lemma 1.2.15. If one could introduce parameters into the rows and columns of the matrix simultaneously, then one might reach the desired improvement and obtain similar results as described in Corollary 1.2.24.  $\square$

Finally, it is natural to ask if real Hadamard matrices can be obtained from parametric families of complex Hadamard matrices. For example, one might wonder if a real Hadamard matrix of order 668 can be obtained from the Fourier matrix  $F_{668}$ , which is parametrized via Diță's construction. Unfortunately, real Hadamard matrices of order  $4p$  are not of Diță-type and therefore they cannot be obtained this way [135]. It is, however, unclear whether some clever parametrization scheme would yield such a matrix. We explicitly ask the following “baby case” of this

**Problem 1.2.27.** Investigate if the Fourier matrix  $F_{12}$  can be parametrized in a way such that its orbit contains the real Hadamard matrix  $H_{12}$ .

A positive, constructive resolution of Problem 1.2.27 might lead to the construction of new, previously intractable real Hadamard matrices of higher orders.

It would be nice to connect Theorem 1.2.16 to Theorems 1.2.19 and 1.2.21 and check if it is meaningful in the more general operator algebraic context. We have the following

**Problem 1.2.28.** Investigate if Lemma 1.2.15 and Theorem 1.2.16 can be reformulated in an operator algebraic fashion similarly to Theorems 1.2.19 and 1.2.21.

There are complex Hadamard matrices which cannot be parametrized at all. The relevant concept is what follows.

**Definition 1.2.29** (Tadej–Życzkowski, [139]). A complex Hadamard matrix  $H$  of order  $n$  is *isolated*, if around a small neighborhood of  $H$  all complex Hadamard matrices  $K$  are equivalent to it.

One might wonder why we allow other (yet equivalent) Hadamard matrices to exist around a neighborhood of  $H$ . The reason is quite simple: every complex Hadamard matrix can be transformed continuously to some other via multiplication by unitary diagonal matrices, which however is uninteresting as it never leads to new, inequivalent matrices (see Example 1.2.2). It turns out, that the defect provides a useful criterion detecting isolated matrices. In particular, from Proposition 1.2.12 it follows that no

smooth families can be obtained from a matrix whose defect is zero. This, however does not say anything about the existence of non-smooth families (e.g. a sequence of inequivalent matrices converging to  $H$ ). The following stronger result excludes this possibility.

**Proposition 1.2.30** (Tadej–Życzkowski, [139]). *Suppose that the defect of a complex Hadamard matrix  $H$  of order  $n$  is zero. Then  $H$  is isolated amongst all  $n \times n$  complex Hadamard matrices.*

Nicoară found an equivalent criterion (see [139]) what he calls the “span condition” [107]. Here we recall his result in a form relevant to us. We denote by  $[\mathcal{A}, \mathcal{B}]$  the linear span of the commutator of the matrix algebras  $\mathcal{A}, \mathcal{B} \subset \mathcal{M}_n(\mathbb{C})$ , namely

$$[\mathcal{A}, \mathcal{B}] = \text{span}\{AB - BA : A \in \mathcal{A}, B \in \mathcal{B}\}.$$

**Proposition 1.2.31** (Span condition, [107]). *If  $H$  is a complex Hadamard matrix of order  $n$  such that the dimension of the vector space  $[\mathcal{D}_n, H^* \mathcal{D}_n H]$  is  $n^2 - 2n + 1$  then  $H$  is isolated among all complex Hadamard matrices of order  $n$  (up to equivalence).*

It is easy to see that the matrices  $F_1$  and  $F_2$  satisfy the span condition (or equivalently, their defect is 0), thus from Proposition 1.2.23 it follows immediately that

**Corollary 1.2.32.** *A real Hadamard matrix is isolated if and only if it is equivalent to  $F_1$  or  $F_2$ .*

For results pertaining the defect of unitary matrices see e.g. [74], [136], [139].

## 1.3 Equivalence of complex Hadamard matrices

The existence of parametric families of complex Hadamard matrices in a given order  $n$  implies the existence of infinitely many inequivalent matrices [34]. This can be readily seen through the following invariant, introduced by Haagerup [60]:

**Definition 1.3.1.** The *Haagerup-set* of a complex Hadamard matrix  $H$  of order  $n$  is the set

$$\Lambda(H) := \{h_{ij}h_{kl}\bar{h}_{il}\bar{h}_{kj} : i, j, k, l = 1, \dots, n\}.$$

The following is immediate.

**Lemma 1.3.2.** *The Haagerup-set is invariant under the usual equivalence.*

*Remark 1.3.3.* Informally speaking, if two Hadamard matrices  $H$  and  $K$  have “essentially different” set of entries, they cannot be equivalent. In particular, it follows from the Haagerup invariant that for any complex Hadamard matrix  $H$  there is only a finite number of dephased complex Hadamard matrices  $K$  being equivalent to it. Indeed, any entry of  $K$  must be an element of  $\Lambda(H)$ .  $\square$

We illustrate an application of this invariant in the following

**Lemma 1.3.4.** *The matrices  $F_2 \otimes F_2$  and  $F_4$  are inequivalent (cf. Example 1.1.11).*

*Proof.* Indeed, as  $\Lambda(F_2 \otimes F_2) = \{\pm 1\}$ , and in particular, it does not contain the fourth root of unity  $\mathbf{i}$ , whereas  $\Lambda(F_4) = \{\pm 1, \pm \mathbf{i}\}$ .  $\square$

However, it is known that there are 5 inequivalent real Hadamard matrices of order 16 [62], all of which sharing the same Haagerup set, therefore they cannot be distinguished by this concept. There are a number of invariants introduced to detect the inequivalence of real Hadamard matrices, including the 4-profile [29] or the Smith Normal Form [104], however they cannot be translated directly to the complex case due to fundamental or practical reasons. We have introduced a new invariant in [132] to improve on this situation.

**Definition 1.3.5** (see [132]). The *fingerprint* of a complex Hadamard matrix  $H$  of order  $n$  is the following ordered set

$$\Phi(H) := \{ \{ (v_i(d), m_i(d)) : i \in I(d) \}_d : d = 2, \dots, \lfloor n/2 \rfloor \},$$

where for every  $2 \leq d \leq \lfloor n/2 \rfloor$   $I(d)$  is an index set, and  $v_i(d)$  and  $m_i(d)$  are the possible values of the moduli of the  $d \times d$  minors and its multiplicities, respectively.

We give here a quick

**Example 1.3.6.** The fingerprint of the  $8 \times 8$  real Hadamard matrix  $H := F_2 \otimes F_2 \otimes F_2$  reads

$$\Phi(H) = \{ \{ (0, 336), (2, 448) \}_2, \{ (0, 1344), (4, 1792) \}_3, \{ (0, 1428), (8, 3136), (16, 336) \}_4 \},$$

meaning that there are 336  $2 \times 2$  minors of value 0 and 448 minors of absolute value 2 in  $H$ , etc.

We remark here that the distribution of the absolute values of the minors of size greater than  $\lfloor n/2 \rfloor$  are not considered in the fingerprint because in unitary matrices any minor and its cofactor share the same absolute value [132]. This harmless observation lead to a surprising disproval of a natural conjecture of Koukovinos et al. on the distribution of minors of real Hadamard matrices [83].



Compared to the Haagerup-set which considers  $2 \times 2$  submatrices only, the fingerprint aims to capture some of the global properties of a complex Hadamard matrix. One of the limitations of the fingerprint is its computational complexity, however in practice one is free to use some subset of  $\Phi$ , say the distribution of minors up to order 3 or just the number of  $4 \times 4$  vanishing minors, etc., providing limited but hopefully enough information already. Another weak point of the concept is that it cannot distinguish a matrix from its transpose, conjugate or adjoint. Separating a matrix from its transpose, however, tends to be more important in the real case where the underlying design is studied. We point out a natural way to distinguish a complex Hadamard matrix from its transpose in the following

**Definition 1.3.7.** The *rectangular rank profile* of a complex Hadamard matrix  $H$  is the following ordered set

$$\mathcal{R}(H) = \{ \{ (r_i(j, k), m_i(j, k)) : i \in I(j, k) \}_{j \times k} : 2 \leq j, k \leq n - 2 \},$$

where for every  $2 \leq j, k \leq n - 2$   $I(j, k)$  is an index set, and  $r_i(j, k)$  and  $m_i(j, k)$  are the possible values of the rank of the  $j \times k$  submatrices of the matrix  $H$  and their multiplicities, respectively.

**Lemma 1.3.8.** *The rectangular rank profile is invariant, up to equivalence.*

*Proof.* The rank of a rectangular matrix can be calculated by considering the size of its largest nonsingular minor, which however is preserved during the equivalence operations.  $\square$

**Example 1.3.9.** The rectangular rank profile of the matrices  $F_2 \otimes F_2$  and  $F_4$  (see Example 1.1.11) read:

$$\mathcal{R}(F_2 \otimes F_2) = \{ \{ (1, 12), (2, 24) \}_{2 \times 2} \}, \quad \text{and} \quad \mathcal{R}(F_4) = \{ \{ (1, 4), (2, 32) \}_{2 \times 2} \},$$

respectively, meaning that in the matrix  $F_2 \otimes F_2$  the number of  $2 \times 2$  submatrices with rank 1 and 2 are 12 and 24, respectively, while in  $F_4$  the number of  $2 \times 2$  submatrices with rank 1 is 4 only.

We tend to believe that in a “typical” complex Hadamard matrix there are no vanishing minors at all, and as a result their rectangular rank profile is trivial. Nevertheless, when we consider highly structured matrices, such as real Hadamard matrices, it can be a valuable asset at our disposal. We shall see further applications of these invariants in the subsequent sections.

## 1.4 Butson-type complex Hadamard matrices

This section is dedicated to investigate the existence and structure of the following concept.

**Definition 1.4.1.** We say that a complex Hadamard matrix  $H$  of order  $n$  is of *Butson-type*, if  $H$  is composed from some  $q$ th roots of unity. We denote this class of matrices by  $BH(n, q)$ .

We advise the reader that the notation varies from author to author, some of them permuting the argument to  $BH(q, n)$ , or dropping the letter  $B$  resulting in the notations  $H(n, q)$  and  $H(q, n)$ , respectively.

We primarily focus on  $BH(n, 4)$  and  $BH(n, 6)$  matrices in this section, as the cases  $q = 4$  and  $q = 6$  are the two simplest generalization of the real Hadamard matrices, i.e. when  $q = 2$ , namely they correspond to the prime-power and composite case, respectively. Clearly, Lemma 1.1.7 applies to  $BH(n, q)$  matrices as well, resulting in the following concept.

**Definition 1.4.2.** We say that a  $k$ -term sum  $x_1 + x_2 + \dots + x_k$  is a *vanishing sum of order  $k$*  if its value is 0.

Now in order to find a pair of orthogonal rows of a  $BH(n, q)$  matrix one needs to exhibit a vanishing sum of order  $n$ , composed from  $q$ th root of unity. It is natural to ask when this is possible. The following resolution of this problem is a necessary condition on the existence of  $BH(n, q)$  matrices

**Theorem 1.4.3** (Lam–Leung, [91]). *For every  $q = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$  there is a vanishing sum of order  $n$ , composed from  $q$ th roots of unity if and only if  $n$  is a natural linear combination of the numbers  $p_i$ , i.e.  $n \in \mathbb{N}p_1 + \mathbb{N}p_2 + \dots + \mathbb{N}p_r$ .*

For a more general treatment of this question see [30].

Theorem 1.4.3 above, however, does not say anything about the existence of orthogonal triplets of rows in complex Hadamard matrices. For example, for numbers  $n \equiv 2 \pmod{4}$  one easily constructs a vanishing sum of order  $n$  composed from the numbers  $\pm 1$ , however, it follows from (the ideas behind) Lemma 1.1.14 that it is impossible to exhibit orthogonal triplets of real rows in this case.

Let us denote by  $\left(\frac{p}{q}\right)$  the Legendre symbol. We collect some well-known necessary conditions and the subsequent nonexistence results in the following

**Theorem 1.4.4** (see [21], [146]). *For a  $BH(n, q)$  matrix the following hold.*

1. *If  $p$  is prime and there is a  $BH(n, p^a)$ , then  $n = pt$  for some positive integer  $t$ .*

2. If  $p$  is prime, there exists a  $BH(2^j p^k, p)$  for all  $0 \leq j \leq k$ .
3. Suppose  $p \equiv 3 \pmod{4}$  is prime,  $n = p^b r^2 s$  is odd,  $s$  is square-free with  $(s, p) = 1$ , and there exists a prime  $q|s$  with quadratic character value  $\left(\frac{q}{p}\right) = -1$ . Then there is no  $BH(n, p^a)$  and no  $BH(n, 2p^a)$ .

Butson's basic construction yields a  $BH(2p, p)$  matrix for prime  $p$ ; it is known that there are  $BH(12, 3)$  [93] and  $BH(28, 7)$  matrices [105]. It is natural to ask the following

**Problem 1.4.5.** Decide for which primes  $p$  are there  $BH(4p, p)$  matrices.

Setting  $p = 3, n = q = s = 5$  in Part 3 above we arrive to the following

**Corollary 1.4.6.** *There is no  $BH(5, 6)$  matrix.*

Observe that we cannot apply Theorem 1.4.3 directly, as  $n = 2 + 3$ , and indeed, it is easy to exhibit a pair of orthogonal rows from sixth roots of unity. We shall recall a direct argument for Corollary 1.4.6, but first let us see the following

**Lemma 1.4.7.** *For a complex Hadamard matrix  $H$  of order  $n$  we have  $|\det(H)| = n^{n/2}$ .*

*Proof.* Indeed, as the determinant is multiplicative, we have

$$n^n = \det(nI_n) = \det(HH^*) = |\det(H)|^2. \quad \square$$

It is easy to see that complex Hadamard matrices have the largest determinant amongst all matrices whose entries are at most 1 in absolute value [1].

The following is attributed to de Launey (see [67]).

*Proof of Corollary 1.4.6.* We use Lemma 1.4.7 and try to reach a contradiction. Suppose to the contrary, that there is a  $BH(5, 6)$  matrix  $H$ . Then observe that its determinant is a sum of sixth roots of unity and hence there are integral numbers  $A$  and  $B$ , such that  $\det(H) = A + B\omega$ . Therefore we find that

$$5^5 = |\det(H)|^2 = |A + B\omega|^2 = A^2 + B^2 + AB(\omega + \omega^2) = A^2 + B^2 - AB,$$

the right hand side, however, cannot be 2 modulo 3, a contradiction.  $\square$

For a class of  $BH(n, q)$  matrices some further non-existence results shall be obtained in Section 3.2. Finally we emphasize that  $BH(n, q)$  matrices can be quickly recognized.

**Lemma 1.4.8.** *Suppose that a complex Hadamard matrix  $H$  is equivalent to a  $BH(n, q)$  matrix. Then the dephased form of  $H$  must be composed of purely complex  $q$ th roots of unity.*

*Proof.* Indeed, if the dephased form of  $H$  would contain an entry which is not a root of unity, then the Haagerup invariant set would contain this entry as well. However, the Haagerup set of  $BH(n, q)$  matrices can contain some subset of the  $q$ th roots of unity only.  $\square$

It follows that checking the number of inequivalent  $BH(n, q)$  matrices in dephased parametric families is a finite process. We shall repeatedly use this fact in the next subsection.

**Definition 1.4.9.** The *automorphism group* of a  $BH(n, q)$  matrix  $H$  is the group of pairs of monomial matrices  $(P, Q)$ , such that  $H = PHQ$ ; a monomial matrix is an  $n \times n$  matrix having a single nonzero entry in each row and column, these nonzero entries being complex  $q$ th roots of unity.

Note that the automorphism group depends on the choice of  $q$ , i.e. on the ambient space in which the  $BH(n, q)$  matrix is considered.

### 1.4.1 A course on $BH(n, 4)$ matrices

$BH(n, 4)$  matrices are probably the most natural examples of complex Hadamard matrices. In fact, in various earlier literature the term “complex Hadamard matrix” was used to refer to them exclusively, and the term “unit Hadamard” was proposed for the more general objects we are concerned with [34]. There are a vast number of papers available on  $BH(n, 4)$  matrices both in the mathematics and in the engineering literature, as they have many industrial applications, most notably in communications and coding theory [63] through complex Golay sequences [37]. For further applications we refer the reader to the manuals [1] and [67].

In this brief section we investigate  $BH(n, 4)$  matrices of small orders, and give a full classification of them up to order 8. We believe that this result is already known, but we were unable to find any relevant reference in this respect. Nevertheless, the presentation of these matrices in terms of infinite, affine families is indeed new, which is our contribution to this section.

The following is immediate from Theorem 1.4.3.

**Lemma 1.4.10.** *If a  $BH(n, 4)$  matrix exists then  $n = 1$  or  $n$  is even.*

Similarly to the real case, it seems that this trivial restriction is the only one, as we have the following long-standing

**Conjecture 1.4.11** (Seberry, cf. [27]). *For every even  $n$  there is a  $BH(n, 4)$  matrix.*

It turns out that Conjecture 1.4.11 implies the Hadamard conjecture thus the existence of  $BH(n, 4)$  matrices is deeply entwined with the existence of real Hadamard matrices (see [67]). We have the following folklore

**Lemma 1.4.12.** *If a  $BH(n, 4)$  matrix exists then so does a  $BH(2n, 2)$ , that is a real Hadamard matrix of twice the size.*

*Proof.* We can lift the starting point  $BH(n, 4)$  matrix via the function  $\varphi_B(\cdot)$  which assigns to the entries  $\pm 1$  and  $\pm \mathbf{i}$  the  $2 \times 2$  real Hadamard matrices

$$\varphi_B(\pm 1) = \pm \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \varphi_B(\pm \mathbf{i}) = \pm \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix},$$

where the  $\pm$  signs on the left and right hand side of the maps agree.  $\square$

**Example 1.4.13.** We can lift the  $BH(2, 4)$  matrix  $\text{Diag}(1, \mathbf{i})F_2\text{Diag}(1, \mathbf{i})$  as follows:

$$\begin{bmatrix} 1 & \mathbf{i} \\ \mathbf{i} & 1 \end{bmatrix} \rightsquigarrow \left[ \begin{array}{cc|cc} 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ \hline -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 \end{array} \right].$$

Let us stop for a moment and observe that both matrices featuring in the example above are equivalent to a circulant one. It is natural then to try to obtain circulant  $BH(n, 4)$  and  $BH(n, 2)$  matrices. However, we have the following discouraging

**Conjecture 1.4.14** (Ryser, [118]). *There is no circulant real Hadamard matrix for  $n > 4$ .*

The fact that Conjecture 1.4.14 is still open shows how little understanding we have about real Hadamard matrices. For the  $BH(n, 4)$  case we recall from [4] the following

**Example 1.4.15** (Arasu et al. [4]). The circulant matrices, induced by the first rows

$(1, \mathbf{i}); (1, -\mathbf{i}, 1, \mathbf{i}); (1, 1, \mathbf{i}, 1, 1, -1, \mathbf{i}, -1); (1, 1, \mathbf{i}, -\mathbf{i}, \mathbf{i}, 1, 1, \mathbf{i}, -1, 1, -\mathbf{i}, -\mathbf{i}, -\mathbf{i}, 1, -1, \mathbf{i})$

are  $BH(n, 4)$  matrices for order  $n = 2, 4, 8$  and  $16$ , respectively.

**Conjecture 1.4.16.** *There is no circulant  $BH(n, 4)$  matrix for  $n > 16$ .*

The following is a strong evidence, supporting the truth of Conjecture 1.4.16:

**Theorem 1.4.17** (Arasu et al. [4], cf. [121]). *Let  $P$  be any finite set of primes. Then there are only finitely many circulant  $BH(n, 4)$  matrices of order  $n$ , where all prime divisors of  $n$  are in  $P$ .*

So it seems that “nice” circulant complex Hadamard matrices are rare. This is not quite the case if one allows higher roots of unity or not necessarily root of unity entries to appear in the matrix. We will return to circulant matrices in Section 3.3.

It turns out, however, that  $BH(n, 4)$  matrices with circulant core exist for infinitely many orders  $n$ . The following is the complex counterpart of Theorem 1.1.17.

**Theorem 1.4.18** (see e.g. [67]). *Let  $p$  be a prime number,  $p \equiv 1 \pmod{4}$ , and consider a vector  $x$  such that  $x_0 = 0$  and  $x_i = 1$  if  $i$  is a quadratic residue in  $\mathbb{Z}_p^*$ , otherwise  $x_i = -1$ . Let us define the Paley matrix  $P := \text{Circ}(x)$ . Then, the matrix  $C := \mathbf{i}P - I$ , bordered by a row and column of numbers 1 is a  $BH(p + 1, 4)$  matrix.*

Now we turn to the parametrization of  $BH(n, 4)$  matrices, and investigate whether we have an analogue, more-or-less trivial way to introduce affine parameters into them similarly to the real case (see Lemma 1.2.15) for large enough  $n$ . It is immediate, that Lemma 1.2.15 applies as long as a  $BH(n, 4)$  matrix features two purely real rows or columns. Not every  $BH(n, 4)$  matrix has this type of structure though, as Theorem 1.4.18 clearly shows; nevertheless members of that particular class can be parametrized, as was shown in our Master’s thesis [133]. The following easily comes from Theorem 1.2.16.

**Corollary 1.4.19.** *Suppose that  $H$  is a dephased  $BH(n, 4)$  matrix such that its core has main diagonal  $-1$  and all other entries are  $\pm \mathbf{i}$ . Then  $H$  admits an at least one-parameter affine orbit.*

The reader might wish to jump ahead to Example 2.2.2 to see the one-parameter matrix  $D_6^{(1)}(c)$  as an illustration. So far we have accounted all  $BH(n, 4)$  matrices up to order 6. Indeed, it is rather easy to see that they are equivalent to  $F_1$ ,  $F_2$ , either  $F_2 \otimes F_2$  or  $F_4$ , and  $D_6^{(1)}(1)$ , respectively. The following is a short summary.

**Lemma 1.4.20.** *The number of inequivalent  $BH(n, 4)$  matrices reads 1, 1, 2, 1 for  $n = 1, 2, 4, 6$ . The matrices of orders 1 and 2 are isolated, whereas the matrices of orders 4 and 6 are part of an infinite, one-parameter affine family of complex Hadamard matrices.*

To further investigate the parametrizing capabilities of  $BH(n, 4)$  matrices, we have fully classified  $BH(8, 4)$  matrices. The results are quoted from [134] as follows.

**Theorem 1.4.21** (see [134]). *There are 15  $BH(8, 4)$  matrices, up to equivalence. All these matrices are members of 3, partially overlapping family of complex Hadamard matrices. All these matrices can be distinguished by the number of  $4 \times 4$  vanishing minors they contain up to transposition, conjugation and adjoint.*

*Proof.* The proof is a straightforward exhaustive computer search.  $\square$

We remark here that the proof is “straightforward” because the size of the problem is rather moderate. However, as the parameters  $n$  and  $q$  are increased, the classification problem of  $BH(n, q)$  matrices becomes computationally challenging. For some advanced techniques we refer the reader to [78] and [93].

It seems that all major features are shared by the matrices  $H$ ,  $H^*$ ,  $\overline{H}$  and  $H^T$ , therefore we have introduced the following

**Definition 1.4.22** (see [92]). The complex Hadamard matrices  $H$  and  $K$  are called *ACT-equivalent*, if  $H$  is equivalent to at least one of  $K$ ,  $K^*$ ,  $\overline{K}$  or  $K^T$ .

The acronym ACT stands for adjoint, conjugation and transpose in alphabetical order. To utilize this concept, we state the following

**Proposition 1.4.23.** *There are 10  $BH(8, 4)$  matrices, up to ACT-equivalence. All these matrices can be distinguished by the number of  $4 \times 4$  vanishing minors they contain.*

In what follows we describe the three parametric families mentioned in Theorem 1.4.21. Our first example is essentially the Fourier family  $F_8^{(5)}$ , reported first in [138].

$$F_8^{(5)}(a, b, c, d, e) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a & b & c & -1 & -a & -b & -c \\ 1 & d & -1 & -d & 1 & d & -1 & -d \\ 1 & e & -b & -\overline{a}ce & -1 & -e & b & \overline{a}ce \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -a & b & -c & -1 & a & -b & c \\ 1 & -d & -1 & d & 1 & -d & -1 & d \\ 1 & -e & -b & \overline{a}ce & -1 & e & b & -\overline{a}ce \end{bmatrix}.$$

As  $F_8^{(5)}(a, b, c, d, e)$  features two rows and columns with entries  $\pm 1$  it is an infinite family of jacket matrices (see [98]). Note that  $F_8^{(5)}(a\tau, b\tau^2, c\tau^3, d\tau^2, e\tau^3)$  where  $\tau = \mathbf{e}^{2\pi\mathbf{i}/8}$  is an eighth root of unity coincides with the matrix listed in [138], and hence is of Diță-type. The matrix corresponding to  $F_8^{(5)}(-1/t^2, \mathbf{i}, -\mathbf{i}/t^2, -\mathbf{i}, -\mathbf{i}/t^2)$  is equivalent to an infinite family of circulant matrices (see Theorem 3.3.4), containing in particular Horadam’s matrix  $K_4(\mathbf{i})$  (see [67, p. 88]).

After evaluating the matrix  $F_8^{(5)}(a, b, c, d, e)$  at the  $4^5 = 1024$  possible quintuples (see Lemma 1.4.8), we obtain the following

**Proposition 1.4.24.** *The family  $F_8^{(5)}(a, b, c, d, e)$  contains 8 inequivalent  $BH(8, 4)$  matrices: the symmetric matrices  $F_8^{(5)}(1, 1, 1, 1, 1)$ ,  $F_8^{(5)}(1, \mathbf{i}, \mathbf{i}, \mathbf{i}, \mathbf{i})$ ,  $F_8^{(5)}(\mathbf{i}, 1, \mathbf{i}, 1, \mathbf{i})$  and  $F_8^{(5)}(1, 1, \mathbf{i}, 1, \mathbf{i})$ ; and further the matrices  $F_8^{(5)}(1, 1, 1, 1, \mathbf{i})$ ,  $F_8^{(5)}(1, 1, \mathbf{i}, \mathbf{i}, \mathbf{i})$ , and their transpose.*

In [102] another family of  $8 \times 8$  complex Hadamard matrices were obtained from translational tiles in abelian groups (see Section 1.4.3):

$$S_8^{(4)}(a, b, c, d) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & d & -d & -d & -1 & cd & -cd & d \\ 1 & a\bar{d} & b\bar{d} & -b\bar{d} & 1 & -1 & -1 & -a\bar{d} \\ 1 & a & -b & b & -1 & -cd & cd & -a \\ 1 & -1 & -b\bar{d} & b\bar{d} & 1 & c & -c & -1 \\ 1 & -d & b & -b & -1 & d & d & -d \\ 1 & -a\bar{d} & -1 & -1 & 1 & -c & c & a\bar{d} \\ 1 & -a & d & d & -1 & -d & -d & a \end{bmatrix}. \quad (1.9)$$

It was shown that the matrix  $S_8^{(4)}(\mathbf{i}, \mathbf{i}, \mathbf{i}, 1)$  is not of Diță-type, and as the set of Diță-type matrices is closed it follows that a small neighborhood around it avoids the family  $F_8^{(5)}(a, b, c, d, e)$  completely. The matrix corresponding to  $S_8^{(4)}(1, 1, \mathbf{i}, \mathbf{i})$  is equivalent to the “jacket conference matrix”  $J_8$  [98]. By evaluating the matrix  $S_8^{(4)}(a, b, c, d)$  at the fourth roots of unity we find the following

**Proposition 1.4.25.** *The family  $S_8^{(4)}(a, b, c, d)$  and its transpose contain 8 inequivalent  $BH(8, 4)$  matrices: the real Hadamard matrix  $S_8^{(4)}(1, 1, 1, 1)$  and  $S_8^{(4)}(1, 1, \mathbf{i}, \mathbf{i})$ , which are equivalent to a symmetric matrix, and further the matrices  $S_8^{(4)}(1, 1, 1, \mathbf{i})$ ,  $S_8^{(4)}(1, \mathbf{i}, 1, \mathbf{i})$ ,  $S_8^{(4)}(1, 1, \mathbf{i}, 1)$ , and their transpose.*

By analyzing the fingerprint of the obtained matrices, one can see that the following equivalences hold:  $S_8^{(4)}(1, 1, 1, 1) \sim F_8^{(5)}(1, 1, 1, 1, 1)$  and  $\left(S_8^{(4)}(1, 1, \mathbf{i}, 1)\right)^T \sim F_8^{(5)}(1, 1, 1, 1, \mathbf{i})$ , and therefore a further family is required to describe all of the 15  $BH(8, 4)$  matrices.

*Remark 1.4.26.* The family  $S_8^{(4)}(a, b, c, d)$  is a maximal affine family (in the sense of [138]) and hence it cannot be part of larger, say, five-parameter affine family of complex Hadamard matrices.  $\square$

The following matrix was constructed from MUBs of order 4 (see Section 2.4) by Diță very recently in [43]:

$$D_{8B}^{(5)}(a, b, c, d, e) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a & -a & d & -d & -a & a & -1 \\ 1 & b & b\bar{c}e & -d & d & -b\bar{c}e & -b & -1 \\ 1 & c & -e & -1 & -1 & e & -c & 1 \\ 1 & -c & e & -1 & -1 & -e & c & 1 \\ 1 & -b & -b\bar{c}e & -d & d & b\bar{c}e & b & -1 \\ 1 & -a & a & d & -d & a & -a & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \end{bmatrix}.$$



We will see shortly that the family  $D_{8B}^{(5)}(a, b, c, d, e)$  is essentially different from the families  $F_8^{(5)}(a, b, c, d, e)$  and  $S_8^{(4)}(a, b, c, d)$ , as it accounts for most of the  $BH(8, 4)$  matrices. We remark here that the family  $\left(D_{8B}^{(5)}(a, b, c, 1, c)\right)^T$  is equivalent to the three-parameter family  $P_8$  reported in [14]. We have the following

**Proposition 1.4.27.** *The family  $D_{8B}^{(5)}(a, b, c, d, e)$  together with its transpose contain 11 inequivalent  $BH(8, 4)$  matrices, namely the real Hadamard matrix  $D_{8B}^{(5)}(1, 1, 1, 1, 1)$ ,  $D_{8B}^{(5)}(1, 1, \mathbf{i}, 1, 1)$  and the matrix  $D_{8B}^{(5)}(1, \mathbf{i}, \mathbf{i}, 1, \mathbf{i})$ , which are all equivalent to symmetric matrices, and further  $D_{8B}^{(5)}(1, 1, 1, 1, \mathbf{i})$ ,  $D_{8B}^{(5)}(1, 1, 1, \mathbf{i}, \mathbf{i})$ ,  $D_{8B}^{(5)}(1, 1, \mathbf{i}, \mathbf{i}, 1)$ ,  $D_{8B}^{(5)}(1, \mathbf{i}, \mathbf{i}, \mathbf{i}, \mathbf{i})$ , and their transpose.*

In particular, the matrix  $D_{8B}^{(5)}(1, 1, \mathbf{i}, \mathbf{i}, 1)$  is not a member of any of the families  $F_8^{(5)}(a, b, c, d, e)$ ,  $S_8^{(4)}(a, b, c, d)$  or  $\left(S_8^{(4)}(a, b, c, d)\right)^T$ .

*Remark 1.4.28.* It is possible to separate the matrices  $F_8^{(5)}(1, 1, 1, 1, \mathbf{i})$ ,  $F_8^{(5)}(1, 1, \mathbf{i}, \mathbf{i}, \mathbf{i})$ ,  $S_8^{(4)}(1, 1, 1, \mathbf{i})$ ,  $S_8^{(4)}(1, \mathbf{i}, 1, \mathbf{i})$  and  $D_{8B}^{(5)}(1, 1, \mathbf{i}, \mathbf{i}, 1)$  from their transpose by considering their rectangular rank profile.  $\square$

The summary concerning  $BH(8, 4)$  matrices is available in Table 1.1 for which the legend is as follows: column ACT describes if a matrix is equivalent to its adjoint,

Table 1.1: Summary of the  $BH(8, 4)$  matrices, up to ACT-equivalence

No.	Family	Coordinates	ACT	HBS	Auto	Defect	Orbit	$\mathbb{Z}_4$	Invariant
1	$F_8$	$(1, 1, 1, 1, 1)$	YYY	YYY	43008	21	5	3	1428
2	$F_8$	$(1, \mathbf{i}, \mathbf{i}, \mathbf{i}, \mathbf{i})$	YYY	YYY	1024	9	5	2	852
3	$F_8$	$(\mathbf{i}, 1, \mathbf{i}, 1, \mathbf{i})$	YYY	NYN	2048	13	5	2	1204
4	$F_8$	$(1, 1, 1, 1, \mathbf{i})$	NYN	NYN	1536	15	5	3	948
5	$F_8$	$(1, 1, \mathbf{i}, \mathbf{i}, \mathbf{i})$	NYN	NYN	512	7	5	2	836
6	$F_8$	$(1, 1, \mathbf{i}, 1, \mathbf{i})$	YYY	YYY	256	11	5	3	596
7	$S_8$	$(1, 1, \mathbf{i}, \mathbf{i})$	YYY	YYY	768	11	4	4	504
8	$S_8$	$(1, 1, 1, \mathbf{i})$	NYN	NYN	192	5	4	3	360
9	$S_8$	$(1, \mathbf{i}, 1, \mathbf{i})$	NYN	NYN	256	9	4	3	652
10	$D_{8B}$	$(1, 1, \mathbf{i}, \mathbf{i}, 1)$	NYN	NYN	256	9	5	3	348

conjugate or transpose; column HBS indicates if a matrix is equivalent to a Hermitian matrix, contains a  $4 \times 4$  subhadamard matrix (i.e. comes from a trivial doubling construction) or equivalent to a symmetric matrix; column “Auto” describes the order of the automorphism group; while column “Orbit” describes the number of degree of freedom of the family from which the matrix is obtained via the respective values of the “Coordinates” column; the final column describes the number of  $4 \times 4$  vanishing

minors in a matrix. The concept of the  $\mathbb{Z}_q$ -rank (which is the subject of column  $\mathbb{Z}_4$  in Table 1.1) is explained in the following

**Definition 1.4.29.** The  $\mathbb{Z}_q$ -rank of an integral matrix  $L$  of order  $n$  is the smallest positive integer  $r$ , such that there are integral matrices  $S$  and  $T$  of orders  $n \times r$  and  $r \times n$ , respectively, such that  $ST \equiv L \pmod{q}$ .

**Definition 1.4.30.** The  $\mathbb{Z}_q$ -rank of a  $BH(n, q)$  matrix  $H$  is the  $\mathbb{Z}_q$ -rank of the corresponding  $(0, \dots, q-1)$ -matrix  $L$  which can be obtained from  $H$  by exchanging the  $q$ th roots of unity  $e^{2\pi it/q}$  with  $t$  in it for every  $t = 0, \dots, q-1$ .

We shall convince the reader later in Section 1.4.3 that some  $BH(n, q)$  matrices with small  $\mathbb{Z}_q$ -rank has some interesting applications in harmonic analysis [140].

It does not seem obvious how to calculate the  $\mathbb{Z}_4$ -rank of a matrix efficiently, as  $\mathbb{Z}_4$  is not a field (cf. [27] for the prime case). A modular Gaussian elimination gives an upper bound to the  $\mathbb{Z}_q$ -rank, but it is unclear if and when this bound is sharp. Therefore to be on the safe side we have conducted a brute-force search by utilizing the following easy

**Lemma 1.4.31.** Suppose that the  $\mathbb{Z}_4$ -rank of an integral matrix  $L$  is  $r$ . Then there are  $r$  rows of  $L$  forming an  $r \times n$  matrix  $T$  for which there is an integral matrix  $S$  such that  $ST \equiv L \pmod{4}$ .

*Proof.* By Definition 1.4.29 there are integral matrices  $S$  and  $T$  of orders  $n \times r$  and  $r \times n$  such that  $ST \equiv L \pmod{4}$ . Our goal is to modify the decomposition  $S$  and  $T$  by eventually showing that  $T$ , after proper modifications, consists of some of the rows of  $L$ . First observe that one can suppose that there is a number 1 in every column of  $S$ . Indeed: if there is no number 1 present in a column, but there is a number 3, then one can multiply that column and the corresponding row of  $T$  by 3 to leave the product matrix  $ST$  unchanged. If there are neither numbers 1 nor 3 in a column, then one can change every 2 to 1 and then multiply the corresponding row of  $T$  by 2 to leave the product matrix  $ST$  unchanged. Let us denote the  $i$ th row of  $S$  and  $T$  by  $\alpha_i$ ,  $i = 1, \dots, n$  and  $v_i$ ,  $i = 1, \dots, r$ , respectively.

Now consider a row of  $S$ , say  $\alpha_j$ , of which the first coordinate is 1. It follows that the  $j$ th row of  $L$ ,  $L_j$ , can be written in the form  $\alpha_j T \equiv L_j \pmod{4}$ , and as the coefficient of the vector  $v_1$  is 1, one can express  $v_1$  in terms of  $L_j$  and  $v_2, \dots, v_r$ . Now it follows trivially that we can use the row  $L_j$  instead of  $v_1$  in  $T$  by appropriately changing  $S$ . In particular, the  $j$ th row of  $S$  can be set to  $[1, 0, \dots, 0]$ . Now the whole argument can be repeated, *mutatis mutandis* until  $r$  rows of  $L$  are featured in  $T$ .  $\square$

So it seemed that all  $BH(n, 4)$  matrices admit an affine orbit for  $4 \leq n \leq 8$ , yet a general parametrization scheme remained to be found. In order to find more examples

of  $BH(n, 4)$  matrices the author jointly with Pekka Lampio and Patric Östergård proved the following result in [92]:

**Theorem 1.4.32** (see [92]). *Every  $BH(n, 4)$  matrix for  $n = 10, 12$  admit an affine orbit.*

This further supports the idea that all  $BH(n, 4)$  matrices can be parametrized in some “magical” way, perhaps through Theorem 1.2.16. As it is an ongoing work we do not give any further details regarding Theorem 1.4.32, its sole purpose is to give contrast to the following rather surprising

**Theorem 1.4.33** (see [92]). *There are isolated  $BH(14, 4)$  matrices.*

**Example 1.4.34** (Lampio). The following is an isolated  $BH(14, 4)$  matrix:

$$L_{14A}^{(0)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 & 1 & -i & -1 & -1 & i & -i & -1 & i & 1 \\ 1 & 1 & i & i & i & -i & 1 & -i & -1 & -i & -1 & 1 & -1 & -1 \\ 1 & 1 & i & -i & -i & -i & -1 & i & i & -1 & 1 & i & -i & -1 \\ 1 & 1 & -i & 1 & -1 & i & -1 & -i & 1 & 1 & i & -1 & -1 & -1 \\ 1 & i & -1 & -i & -1 & -1 & -i & i & 1 & -i & -1 & 1 & i & 1 \\ 1 & i & -i & i & 1 & -1 & -1 & -i & -i & -1 & -i & i & 1 & i \\ 1 & -1 & 1 & 1 & -1 & i & i & i & -1 & -i & -i & -i & 1 & -1 \\ 1 & -1 & 1 & -i & i & -1 & 1 & -1 & -i & i & i & i & -i & -i \\ 1 & -1 & i & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -i & -i & i \\ 1 & -1 & -1 & 1 & i & -i & -1 & 1 & -1 & i & 1 & -i & -1 & 1 \\ 1 & -1 & -i & -1 & -i & 1 & i & -i & i & -1 & i & 1 & i & -i \\ 1 & -i & -1 & i & 1 & i & 1 & i & 1 & -1 & -i & -1 & -1 & -i \\ 1 & -i & -1 & -1 & -i & -1 & 1 & 1 & -1 & 1 & i & -1 & 1 & i \end{bmatrix}.$$

*Proof of Theorem 1.4.33.* The matrix  $L_{14A}^{(0)}$ , described in Example 1.4.34 above, has defect 0 and hence the statement follows from Proposition 1.2.30.  $\square$

Therefore Lemma 1.2.15 does not have a complex analogue working for all  $BH(n, 4)$  matrices. It is natural though to ask the following

**Problem 1.4.35.** Identify some large class of  $BH(n, 4)$  matrices admitting an infinite, affine orbit.

Once it is realized that there are isolated  $BH(n, 4)$  matrices one would like to understand how common they are. Isolated matrices are unique objects which cannot be obtained from parametric families due to their rigid structure. Therefore we pose the following

**Problem 1.4.36.** Find additional isolated  $BH(n, q)$  matrices for  $n \leq 14$ .

A related, equally important problem besides the classification of  $BH(n, 4)$  matrices is finding new construction methods yielding  $BH(n, 4)$  matrices in those orders where the existence of these objects is unresolved. It seems (see [67]) that the smallest outstanding order is  $n = 70$ ; we pose this here as a relevant

**Problem 1.4.37.** Construct a  $BH(70, 4)$  matrix.

### 1.4.2 A course on $BH(n, 6)$ matrices

In this section we briefly describe the simplest case of  $BH(n, q)$  matrices when  $q$  is composite, i.e. when  $q = 6$ . There is a renewed interest in the existence of  $BH(n, 6)$  matrices, in part because of the following seminal result due to Compton, Craigen and de Launey. Recall that we have denoted by  $\omega$  the principal cubic root of unity (see Definition 1.1.2).

**Theorem 1.4.38** (see [28]). *Let  $H$  be a  $BH(n, 6)$  matrix with no  $\pm 1$  entries. Then  $\varphi(H)$  is a real Hadamard matrix of order  $4n$ , where the map  $\varphi: \mathbb{Q}(\omega) \rightarrow \mathcal{M}_4(\mathbb{Q})$ , given by*

$$\varphi(a + b\omega + c\omega^2) := \begin{bmatrix} 2a - b - c & b - c & b - c & b - c \\ c - b & 2a - b - c & b - c & c - b \\ c - b & c - b & 2a - b - c & b - c \\ c - b & b - c & c - b & 2a - b - c \end{bmatrix},$$

*acts entrywise on the matrix  $H$ .*

We recall the following

**Definition 1.4.39** (see [28]). A  $BH(n, 6)$  matrix with no  $\pm 1$  entries is called an *unreal*  $BH(n, 6)$  matrix.

**Example 1.4.40.** The  $3 \times 3$  unreal circulant complex Hadamard matrix, equivalent

to  $F_3$ , induces the (unique) real Hadamard matrix of order 12 as follows

$$\begin{bmatrix} \omega & \omega^2 & \omega^2 \\ \omega^2 & \omega & \omega^2 \\ \omega^2 & \omega^2 & \omega \end{bmatrix} \rightsquigarrow \left[ \begin{array}{cccc|cccc|cccc} -1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ -1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ \hline -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 \\ \hline -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 \end{array} \right].$$

Theorem 1.4.38 establishes a strong connection between the existence of real and a class of  $BH(n, 6)$  matrices. However, by Corollary 1.4.6 there is no  $BH(5, 6)$  matrix and therefore it is impossible to obtain a real Hadamard matrix of order 20 with this method. Another implication of Corollary 1.4.6 is that one does not have direct access to  $BH(25, 6)$  matrices via the Kronecker product. In what follows we use a related approach to construct such a matrix.

We plug some unknown, unimodular matrices  $X$ ,  $Y$  and  $Z$  of order 5 into the  $5 \times 5$  Paley matrix in place of its entries  $\{0, 1, -1\}$  to obtain

$$W_{25} := \begin{bmatrix} X & Y & Z & Z & Y \\ Y & X & Y & Z & Z \\ Z & Y & X & Y & Z \\ Z & Z & Y & X & Y \\ Y & Z & Z & Y & X \end{bmatrix}, \quad (1.10)$$

and try to solve the arising orthogonality equations. As the underlying matrix is circulant, we have only three equations to deal with, namely

$$XX^* + 2YY^* + ZZ^* = 25I_5, \quad (1.11)$$

$$XY^* + YX^* + ZY^* + YZ^* + ZZ^* = 0, \quad (1.12)$$

$$XZ^* + ZX^* + YZ^* + ZY^* + YY^* = 0. \quad (1.13)$$

It remains to find some feasible matrices  $X$ ,  $Y$  and  $Z$ , composed from sixth roots of unity. It is straightforward to attack the problem with a computer search, however, to shrink the size of the search space considerably we impose the simplifying assumption

that all  $X, Y$  and  $Z$  are circulant. In this way we have found the following solution to the system of equations (1.11)-(1.13):

$$X = \begin{bmatrix} 1 & -\omega^2 & -\omega^2 & -\omega^2 & -\omega^2 \\ -\omega^2 & 1 & -\omega^2 & -\omega^2 & -\omega^2 \\ -\omega^2 & -\omega^2 & 1 & -\omega^2 & -\omega^2 \\ -\omega^2 & -\omega^2 & -\omega^2 & 1 & -\omega^2 \\ -\omega^2 & -\omega^2 & -\omega^2 & -\omega^2 & 1 \end{bmatrix}, \quad Y = \begin{bmatrix} -\omega & -\omega & \omega & \omega & -\omega \\ -\omega & -\omega & -\omega & \omega & \omega \\ \omega & -\omega & -\omega & -\omega & \omega \\ \omega & \omega & -\omega & -\omega & -\omega \\ -\omega & \omega & \omega & -\omega & -\omega \end{bmatrix},$$

$$Z = \begin{bmatrix} -\omega & \omega & -\omega & -\omega & \omega \\ \omega & -\omega & \omega & -\omega & -\omega \\ -\omega & \omega & -\omega & \omega & -\omega \\ -\omega & -\omega & \omega & -\omega & \omega \\ \omega & -\omega & -\omega & \omega & -\omega \end{bmatrix}.$$

Next we describe our construction method in a more sophisticated way by using the Kronecker product. Let  $P$  be the Paley matrix of order  $p$  and decompose it into  $(0, 1)$ -matrices  $S$  and  $N$  such that  $P = S - N$ . The matrices  $S$  and  $N$  are circulant, hence they commute and their first rows are the indicator vector of the squares and nonsquares modulo  $p$ . Based on the example we have found of order 25 we expect that

$$H = I \otimes (I - \omega^2(J - I)) - \omega S \otimes (P + I) + \omega N \otimes (P - I)$$

is a  $BH(p^2, 6)$  matrix. Note that it is unimodular, as required. Let us simplify  $H$  as follows

$$\begin{aligned} H &= I \otimes I - \omega^2 I \otimes J + \omega^2 I \otimes I - \omega(S - N) \otimes P - \omega(S + N) \otimes I \\ &= -\omega P \otimes P - \omega(J - I) \otimes I - \omega^2 I \otimes J - \omega I \otimes I \\ &= -\omega P \otimes P - \omega J \otimes I - \omega^2 I \otimes J. \end{aligned}$$

Now multiply  $H$  by  $-\omega^2$  to obtain

$$K = P \otimes P + J \otimes I + \omega I \otimes J$$

and check if  $K$  is complex Hadamard. We have

$$\begin{aligned} KK^* &= PP^T \otimes PP^T + pJ \otimes I + \omega^2 J \otimes J + \omega J \otimes J + pI \otimes J \\ &= (pI - J) \otimes (pI - J) + pJ \otimes I + pI \otimes J - J \otimes J = p^2 I \otimes I. \end{aligned}$$

This construction is a joint work with Professor Robert Craigen and will be included in a forthcoming publication in the near future. We summarize it in the following

**Theorem 1.4.41.** *Let  $p$  be a prime number and  $P$  be the Paley-matrix of order  $p$ . Then the matrix  $H = P \otimes P + J \otimes I + \omega I \otimes J$  is a  $BH(p^2, 6)$  matrix.*

A construction, similar in spirit, can be found in the early literature (cf. [7], [142]) resulting in various real orthogonal matrices.

**Corollary 1.4.42.** *For every natural numbers  $n$  and  $k$  there is a  $BH(n^{2k}, 6)$  matrix.*

*Proof.* Use the binary expansion of  $2k$  and the Kronecker product of square matrices from Theorem 1.4.41.  $\square$

Now we construct some sporadic examples of bicirculant  $BH(n, 6)$  matrices.

**Example 1.4.43.** Let

$$A = \omega^2 I + \omega P,$$

$$B = \omega I - \omega^2 N - \omega S,$$

where  $P = S - N$  is the Paley-matrix of order 11, such that  $S$  and  $N$  are the  $(0, 1)$ -characteristic matrices of the squares and nonsquares modulo 11. Then, we find that

$$AA^* = 12I - J - \mathbf{i}\sqrt{3}P, \quad (1.14)$$

$$BB^* = 10I + J + \mathbf{i}\sqrt{3}P, \quad (1.15)$$

and it follows that  $AA^* + BB^* = 22I$ . In particular the bicirculant matrix

$$W_{22} := \begin{bmatrix} A & B \\ B^* & -A^* \end{bmatrix}$$

is an unreal  $BH(22, 6)$  matrix.

*Remark 1.4.44.* It is intriguing that the blocks  $A$  and  $B$  have already a nice structure as described by (1.14)-(1.15) and one begins to wonder if a similar construction might work in higher orders as well. However, experiments show that a similar phenomenon, where the product matrices  $AA^*$  and  $BB^*$  are already a linear combination of  $I$ ,  $J$  and  $P$  only occurs in dimension 7 and 11.  $\square$

In the next two examples we utilize quartic residues.

**Example 1.4.45.** Let  $J = I + Q + S + N$ , where  $Q$ ,  $S$  and  $N$  are the  $(0, 1)$ -characteristic matrices of the quartic residues; quadratic, but not quartic residues; and the quadratic nonresidues modulo 17, respectively. Then set

$$A = I + Q - \omega^2 S + \omega N,$$

$$B = I - Q - \omega S - \omega^2 N.$$

One readily checks (by computer, if one wishes) that  $AA^* + BB^* = 34I$ . Therefore the bicirculant matrix

$$W_{34} := \begin{bmatrix} A & B \\ B^* & -A^* \end{bmatrix}$$

is a  $BH(34, 6)$  matrix.

Similarly, one has

**Example 1.4.46.** Consider the generator  $g = 2$  of  $\mathbb{Z}_{29}^*$  and let  $J = I + Q + S + N_1 + N_2$ , where  $Q, S$ , and  $N_1 + N_2 = N$  are the  $(0, 1)$ -characteristic matrices of quartic residues; quadratic, but not quartic residues; and the quadratic nonresidues modulo 29, respectively. Additionally, let the first row of  $N_1$  be the characteristic vector of those elements  $x \in \mathbb{Z}_{29}^*$  such that  $x = g^{4i+1}$  for some  $i$ . Then set

$$\begin{aligned} A &= \omega I + \omega Q + \omega^2 S + \omega^2 N_1 - \omega^2 N_2, \\ B &= \omega^2 I - \omega Q + \omega S - \omega N_1 + \omega N_2. \end{aligned}$$

One readily checks (by computer, if one wishes) that  $AA^* + BB^* = 58I$ . Therefore the bicirculant matrix

$$W_{58} := \begin{bmatrix} A & B \\ B^* & -A^* \end{bmatrix}$$

is an unreal  $BH(58, 6)$  matrix.

Table 1.2 summarizes the existence of  $BH(n, 6)$  matrices of small even orders (consult Table 3.1 for odd orders). These ad-hoc constructions of bicirculant  $BH(n, 6)$

Table 1.2: Existence of  $BH(n, 6)$  matrices for  $n \leq 62$ ,  $n \equiv 2 \pmod{4}$

$n$	Existence	Remark	$n$	Existence	Remark
2	$F_2$		34	$W_{34}$	Example 1.4.45
6	$S_6$	Example 2.2.1	38	$F_2 \otimes W_{19}$	Example 3.2.10
10	$W'$	See [28]	42	$F_2 \otimes F_3 \otimes P_7$	Example 3.2.2
14	$F_2 \otimes P_7$	Example 3.2.2	46	?	$46 = 2 \cdot 23$
18	$F_2 \otimes F_3 \otimes F_3$		50	$F_2 \otimes W_{25}$	Theorem 1.4.41
22	$W_{22}$	Example 1.4.43	54	$F_2 \otimes F_3 \otimes F_3 \otimes F_3$	
26	$F_2 \otimes X_{13}$	See [28]	58	$W_{58}$	Example 1.4.46
30	$F_3 \otimes W'$	See [28]	62	?	$62 = 2 \cdot 31$

matrices support a conjecture we formulated in our Master's thesis (see [133, p. 74]):

**Conjecture 1.4.47.** *For every prime  $p$  there is a  $BH(2p, 6)$  matrix.*

We shall revisit Butson-type complex Hadamard matrices once again in Section 3.2.

### 1.4.3 An application of Butson matrices: Tiles and spectral sets

A rather surprising application of complex Hadamard matrices has been found recently by Tao [140]. To understand his achievement we need to introduce the concept of



translational tiling and spectral sets. We remark that everything what is stated here has far reaching generalizations in harmonic analysis, and there are analogous statements available in locally compact abelian groups, but highlighting those connections are beyond the scope of this thesis. Instead, we recall only the most elementary concepts relevant to us, and to the theory of  $BH(n, q)$  matrices. We refer the interested reader to the survey article [86] and to the recent literature, including the papers [50], [69] and [94].

**Definition 1.4.48.** We say that a subset  $T$  of  $\mathbb{Z}_q^d$  tiles  $\mathbb{Z}_q^d$  by translation when there exists a subset  $\Lambda \subset \mathbb{Z}_q^d$  such that every  $g \in \mathbb{Z}_q^d$  has a unique representation

$$g = t + \lambda, \quad t \in T, \lambda \in \Lambda. \quad (1.16)$$

The sets  $T$  and  $\Lambda$  are called tiling complements of each other.

**Example 1.4.49.** Let  $q = 3, d = 2$ , and  $T = \{(0, 0), (1, 1), (2, 1)\} \subset \mathbb{Z}_3^2$ . Then  $T$  tiles  $\mathbb{Z}_3^2$  with the tiling complement  $\Lambda = \{(0, 0), (0, 1), (0, 2)\}$ .

There is an elegant characterization of the tiling property by means of harmonic analysis, but instead of recalling it we offer the following obvious condition which is enough for our purposes. We denote by  $|S|$  the cardinality of the set  $S$ .

**Lemma 1.4.50.** If  $T$  tiles  $\mathbb{Z}_q^d$  by translation then  $|T|$  divides  $|\mathbb{Z}_q^d| = q^d$ .

*Proof.* Indeed, as by the tiling property (1.16) we have trivially  $|\mathbb{Z}_q^d| = |T| \cdot |\Lambda|$ .  $\square$

To introduce spectral sets we need some notation first. Let us identify the elements of  $\mathbb{Z}_q^d$  with column vectors, each coordinate being in the range  $\{0, 1, \dots, q-1\}$ . Thus, a set  $S \subset \mathbb{Z}_q^d$  with  $n$  elements can be identified with a  $d \times n$  matrix, the columns of which are the elements of  $S$ . We denote this matrix also by  $S$ . The dual group  $\widehat{\mathbb{Z}_q^d}$  can be identified with row vectors, whose coordinates are, again, in  $\{0, 1, \dots, q-1\}$ . Recall that we have denoted by  $\text{EXP}(L)$  the entrywise exponential of the matrix  $L$ .

**Definition 1.4.51.** We say that an  $n$ -element subset  $S \subset \mathbb{Z}_q^d$  is a *spectral set* when there is an  $n$ -element subset  $Q \subset \widehat{\mathbb{Z}_q^d}$  such that the matrix

$$\text{EXP}\left(\frac{2\pi\mathbf{i}}{q}QS\right)$$

is a complex Hadamard, i.e. a  $BH(n, q)$  matrix. We say that  $Q$  is the spectrum of  $S$  and that the two sets form a spectral pair.

**Example 1.4.52.** The whole group  $\mathbb{Z}_q$  is spectral, and its spectrum is the whole dual group  $\widehat{\mathbb{Z}_q}$  (i.e. we have  $n = q$ ), giving rise to the Fourier matrix  $F_n = \text{EXP}\left(\frac{2\pi\mathbf{i}}{q}\widehat{\mathbb{Z}_q}\mathbb{Z}_q\right)$ .

While tiling seems to be a rather intuitive, geometric concept, spectral sets are more difficult to understand. The following connection between them, which is natural if one sees the underlying harmonic analytic concepts, was proposed (originally in  $\mathbb{R}^d$ ) in 1974:

**Conjecture 1.4.53** (Fuglede, [54]). *A subset  $S \subset \mathbb{Z}_q^d$  is spectral, if and only if it tiles  $\mathbb{Z}_q^d$ .*

It turns out that via the tiling-spectral correspondence “trivial” tiling constructions indeed have a spectral analogue leading to families of Diță-type complex Hadamard matrices [102]. However, a non-standard tiling construction of Szabó [128] was used in [102] to produce previously unknown families of complex Hadamard matrices in dimensions 8, 12 and 16 (see the matrix  $S_8^{(4)}(a, b, c, d)$  in (1.9)).

Several positive partial results were obtained regarding some special cases of Fuglede’s conjecture (see [69], [94]), before Tao exhibited a non-tiling spectral set in  $\mathbb{Z}_3^6$ , which then he slightly modified to obtain a counterexample in  $\mathbb{Z}_3^5$  as well.

**Example 1.4.54** (Tao, [140]). Let  $d = 6$ ,  $n = 6$ ,  $q = 3$ ,  $S = I_6$ , and

$$Q = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 2 & 1 \\ 0 & 1 & 0 & 1 & 2 & 2 \\ 0 & 2 & 1 & 0 & 1 & 2 \\ 0 & 2 & 2 & 1 & 0 & 1 \\ 0 & 1 & 2 & 2 & 1 & 0 \end{bmatrix}.$$

Then the matrix  $\text{EXP}\left(\frac{2\pi i}{3}QS\right)$  is a  $BH(6, 3)$  matrix, and hence  $S$  is spectral in  $\mathbb{Z}_3^6$  with spectrum  $Q$ . However,  $S$  cannot tile  $\mathbb{Z}_3^6$  by Lemma 1.4.50.

Tao’s arguments also implied that Fuglede’s conjecture fails in  $\mathbb{R}^d$  in any dimension higher than 5 and subsequent counterexamples were found refuting both directions for  $d \geq 3$ , see [49] and [84]. In fact, much of the technical difficulties arise in transferring the counterexamples from the finite group setting to  $\mathbb{R}^d$ . However, for the purposes of this thesis we simply stay in the finite setting, where the complex Hadamard matrices play their essential rôle.

We recall the following improvement over Tao’s result.

**Example 1.4.55** (Kolountzakis–Matolcsi, [84]). Let  $d = 3$ ,  $n = 6$ ,  $q = 8$  and

$$S = \begin{bmatrix} 0 & 2 & 4 & 1 & 5 & 6 \\ 0 & 6 & 3 & 4 & 2 & 7 \\ 0 & 6 & 7 & 2 & 4 & 3 \end{bmatrix}, \text{ and } Q^T = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 7 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}, \quad (1.17)$$

where we have given  $Q^T$  instead of  $Q$  for typographical reasons. We have

$$QS \equiv \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 2 & 6 & 6 & 2 \\ 0 & 2 & 4 & 1 & 5 & 6 \\ 0 & 6 & 3 & 4 & 2 & 7 \\ 0 & 6 & 7 & 2 & 4 & 3 \\ 0 & 2 & 6 & 5 & 1 & 4 \end{bmatrix} \pmod{8}, \quad (1.18)$$

and it is easy to see that  $\text{EXP}\left(\frac{2\pi i}{8}QS\right)$  is a  $BH(6, 8)$  matrix. It follows that the set  $S \subset \mathbb{Z}_8^3$  is spectral, but does not tile  $\mathbb{Z}_8^3$  by Lemma 1.4.50, as 6 does not divide  $8^3$ .

It seemed that these small dimensional counterexamples (i.e.  $d = 6, 3$ ) surfaced because one has access to “sporadic”, small dimensional  $BH(n, q)$  matrices with small  $\mathbb{Z}_q$ -rank for  $q = 3$ , or  $q = 8$ . Of course, by considering larger sets, and hence, larger Butson Hadamard matrices it seems more and more difficult to control the  $\mathbb{Z}_q$ -rank, and therefore one does not really expect to find further  $BH(n, q)$  matrices satisfying the divisibility conditions required to the failure of Lemma 1.4.50. Rather surprisingly, however, we have discovered an infinite sequence of counterexamples with  $\mathbb{Z}_q$ -rank 3, which is our contribution to this section. We have the following

**Theorem 1.4.56.** *If  $H$  is a  $BH(n, q)$  matrix with  $\mathbb{Z}_q$ -rank  $r$ , then for every integral number  $m \geq 1$  there is a Diță-type  $BH(mn, mq)$  matrix with  $\mathbb{Z}_{mq}$ -rank at most  $r$ .*

Let us denote by  $C_1$  the matrix in which the first column is pure 1 and all other entries are 0. Similarly, let us denote by  $R_1$  the matrix in which the first row is pure 1 and all other entries are 0. The size of the matrices shall be clear from context.

*Proof.* Let  $Q$  and  $S$  be  $n \times r$  and  $r \times n$   $(0, \dots, q-1)$ -matrices, respectively, such that  $\text{EXP}\left(\frac{2\pi i}{q}QS\right) = H$ . Then define the block matrix

$$L = \begin{bmatrix} Q \\ Q + qC_1 \\ \vdots \\ Q + (m-1)qC_1 \end{bmatrix} \cdot \begin{bmatrix} mS & mS + R_1 & \dots & mS + (m-1)R_1 \end{bmatrix}.$$

Hence, the  $(i, j)$ th block of  $L$  reads

$$(Q + (i-1)qC_1)(mS + (j-1)R_1) \equiv mQS + (j-1)QR_1 + (i-1)(j-1)qJ$$

modulo  $mq$ . Now it is clear that the matrix  $K = \text{EXP}\left(\frac{2\pi i}{mq}L\right)$  is exactly the Diță-type matrix

$$K = F_m \otimes (H, \dots, \text{Diag}(Q_{1,1}^{j-1}, \dots, Q_{n,1}^{j-1})H, \dots, \text{Diag}(Q_{1,1}^{m-1}, \dots, Q_{n,1}^{m-1})H)$$

coming from Corollary 1.2.5, where  $F_m$  is the Fourier matrix of order  $m$ .  $\square$

*Remark 1.4.57.* Note that Theorem 1.4.56 does not describe the Kronecker product construction.  $\square$

We offer a simple

**Example 1.4.58.** Let  $n = m = q = 2$ ,  $H = F_2$ . Then

$$S = \begin{bmatrix} 0 & 1 \end{bmatrix}, Q = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

We have

$$L = \begin{bmatrix} 0 \\ \frac{1}{2} \\ 2 \\ 3 \end{bmatrix} \cdot \begin{bmatrix} 0 & 2 & 1 & 3 \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 3 \\ 0 & 0 & 2 & 2 \\ 0 & 2 & 3 & 1 \end{bmatrix} \pmod{4},$$

giving rise to  $F_4 = \text{EXP}\left(\frac{2\pi i}{4}L\right)$ , which is not equivalent to  $F_2 \otimes F_2$ .

If one has some additional structure on the initial matrix  $H$ , one can prove a somewhat stronger result. We state the case  $m = 2$  relevant to us.

**Corollary 1.4.59.** *Let  $q$  be even. Suppose that  $H = \text{EXP}\left(\frac{2\pi i}{q}L\right)$  is a  $BH(n, q)$  matrix with  $\mathbb{Z}_q$ -rank  $r$  such that there is a decomposition  $QS \equiv L \pmod{q}$  where every entry in the first row of  $S$  is even. Then there is a  $BH(2n, q)$  matrix with  $\mathbb{Z}_q$ -rank  $r$ .*

*Proof.* Indeed, the matrix

$$\begin{bmatrix} Q \\ Q + (q/2)C_1 \end{bmatrix} \cdot \begin{bmatrix} S & S + R_1 \end{bmatrix} =$$

$$\begin{bmatrix} QS & QS + QR_1 \\ QS + q/2C_1S & QS + QR_1 + (q/2)C_1S + q/2J \end{bmatrix} \equiv \begin{bmatrix} QS & QS + QR_1 \\ QS & QS + QR_1 + q/2J \end{bmatrix}$$

$\pmod{q}$  will do the job. Note that resulting matrix contains  $L$  as a submatrix and therefore its  $\mathbb{Z}_q$ -rank cannot fall below  $r$ .  $\square$

**Corollary 1.4.60.** *There is a  $BH(12, 8)$  matrix with  $\mathbb{Z}_8$ -rank 3.*

*Proof.* Observe that in the second row of the matrix  $QS$  in (1.18) all coordinates are even, therefore it is natural to check if  $S$  in (1.17) can be replaced with some  $S'$  featuring the second row of  $L$ . This is exactly the case. We have

$$S' = \begin{bmatrix} 0 & 4 & 2 & 6 & 6 & 2 \\ 0 & 2 & 4 & 1 & 5 & 6 \\ 0 & 6 & 3 & 4 & 2 & 7 \end{bmatrix}, (Q')^T = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 7 \\ 0 & 0 & 0 & 1 & 7 & 0 \end{bmatrix},$$

so an application of Corollary 1.4.59 yields the result.  $\square$

Once we have established the existence of a  $BH(12, 8)$  matrix with  $\mathbb{Z}_8$ -rank 3 it was natural to look for a matrix possessing the special structure required by Corollary 1.4.59. We found the following by investigating various Diță-type complex Hadamard matrices of order 12.

**Example 1.4.61.** The matrix  $\text{EXP}\left(\frac{2\pi i}{8}QS\right)$  is a  $BH(12, 8)$  matrix with  $\mathbb{Z}_8$ -rank 3, where

$$S = \begin{bmatrix} 0 & 2 & 4 & 2 & 6 & 6 & 0 & 2 & 4 & 2 & 6 & 6 \\ 0 & 4 & 2 & 6 & 7 & 3 & 1 & 5 & 3 & 7 & 0 & 4 \\ 0 & 5 & 6 & 1 & 4 & 2 & 0 & 5 & 6 & 1 & 4 & 2 \end{bmatrix},$$

$$Q^T = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 2 & 2 & 3 & 3 & 2 & 3 \\ 0 & 1 & 0 & 3 & 0 & 0 & 4 & 5 & 4 & 7 & 4 & 4 \\ 0 & 0 & 0 & 0 & 1 & 3 & 4 & 4 & 4 & 4 & 5 & 7 \end{bmatrix}.$$

Note that the first row of  $S$  consists of even numbers.

Combining Corollary 1.4.59 and Example 1.4.61 we arrive at the following

**Corollary 1.4.62.** *There is a  $BH(24, 8)$  matrix with  $\mathbb{Z}_8$ -rank 3.*

The other direction of Fuglede's conjecture could not be treated directly by Tao's ideas, but using a tricky duality argument Kolountzakis and Matolcsi exhibited a non-spectral tile in  $\mathbb{Z}_3^6$  thus disproving this part of Conjecture 1.4.53 too [85]. It would be very interesting to find additional  $BH(n, q)$  matrices with small  $\mathbb{Z}_q$ -rank hopefully leading to the disproval of Fuglede's conjecture in dimension 2 as well. We formulate this as a

**Problem 1.4.63.** Find a  $BH(n, q)$  matrix with  $\mathbb{Z}_q$ -rank 2, such that  $n$  does not divide  $q^2$ , or prove that no such a matrix exists.

Despite the negative results in dimensions  $d \geq 3$ , Fuglede's conjecture might be true for  $d = 1$ . For some interesting number-theoretic consequences consult the paper [31] and its references.

**Problem 1.4.64.** Settle both directions of Fuglede's conjecture in  $d \leq 2$  dimensions.



# Chapter 2

## Towards the classification of $6 \times 6$ complex Hadamard matrices

This chapter is devoted to the classification of complex Hadamard matrices of small orders. During the 1990s the classification up to order 5 has been completed [34], [60] and recently various constructions of  $6 \times 6$  complex Hadamard matrices appeared in the literature [6], [10], [44]. However, the full classification of complex Hadamard matrices of order 5 required non-trivial ideas already, and the  $6 \times 6$  case seemed, despite various efforts from the mathematics and physics community, far out of reach.

Complex Hadamard matrices of order  $n$  are related to Mutually Unbiased Bases (MUBs), a geometric configuration of vectors in  $\mathbb{C}^n$ ; an object which has wide range of applications in quantum information theory due to a celebrated result of Werner [144]. Informally speaking, the basic step towards understanding MUBs requires understanding complex Hadamard matrices and once a full classification of complex Hadamard matrices is available (in a given order) significant advances are expected on the theory of MUBs as well (see [17]). We shall investigate them in details in Section 2.4.

This chapter is based on the papers [71], [103], [129] and [131]. The main result is a construction, capturing the structure of a “typical” complex Hadamard matrix of order 6. Moreover, we conjecture that the construction in fact describes all, previously unknown matrices of this order. This method, however, is by no means a comprehensive and irredundant classification of complex Hadamard matrices of order 6 and further and deeper understanding of these objects is needed in order to achieve this.

### 2.1 Classification up to order 5

In this section we go through the description of all complex Hadamard matrices up to order 5. Recall from Lemma 1.1.7 that every complex Hadamard matrix is equivalent to a dephased one, and hence we can suppose that the first row and column of the

matrices we describe here is composed of numbers 1. Therefore one is interested in finding those unimodular row vectors whose coordinates add up to 0. We begin with a characterization of vanishing sums of order  $k$  for  $k \leq 4$ .

**Lemma 2.1.1.** *Suppose that  $x, y, u$  and  $v$  are complex unimodular numbers. Then*

- (a)  $x + y = 0$  implies  $y = -x$ ;
- (b)  $x + y + u = 0$  implies  $y = \varepsilon x$ ,  $u = \varepsilon^2 x$  such that  $1 + \varepsilon + \varepsilon^2 = 0$ .
- (c)  $x + y + u + v = 0$  implies  $x \in \{-y, -u, -v\}$ .

*Proof.* Indeed, this is easily seen through geometry. □

Lemmata 1.1.7 and 2.1.1 allow us to give a full classification of complex Hadamard matrices up to orders 4.

**Lemma 2.1.2.** *For orders  $n = 1, 2, 3$  all complex Hadamard matrices are equivalent to the Fourier matrix  $F_n$ .*

However, at order 4 we have already seen a non-trivial, one-parameter family (see Example 1.2.1). That particular construction is the only possibility we have.

**Proposition 2.1.3** (Craigen, [34]). *All complex Hadamard matrices of order 4 are members of the one-parameter Fourier family, described in Example 1.2.1, such that  $a = \mathbf{e}^{it}$ ,  $t \in [0, \pi/2)$ .*

All these results are elementary, and we invite the reader to verify the statements. However, classification of  $5 \times 5$  complex Hadamard matrices turned out to be extremely difficult. One of the main reasons of this difficulty is the lack of understanding vanishing sums of order 5. Also it might be possible that we have a vanishing sum of order 5 which cannot be extended with a further one being orthogonal to it. By Corollary 1.4.6 we know that there are no  $BH(5, 6)$  matrices, and it is fairly easy to see that there are no triplets of pairwise orthogonal rows of length 5, composed from 6th roots of unity. Yet, we have the following intriguing

**Example 2.1.4.** The following is a triplet of orthogonal rows in order 5, composed from 12th roots of unity:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \mathbf{i} & -\mathbf{i} \\ 1 & -\mathbf{i}\omega^2 & -\mathbf{i}\omega & -\mathbf{i} & -1 \end{bmatrix}.$$



In light of the example above, one cannot but wonder if, by utilizing  $q$ th roots of unity for some large  $q$ , nontrivial complex Hadamard matrices of order 5 can be obtained. The next result gives a necessary condition on the structure of orthogonal triplets of rows in complex Hadamard matrices.

**Lemma 2.1.5** (Haagerup's trick, [60]). *Let  $(1, 1, 1, 1, 1)$ ,  $(1, a, b, s_1, s_2)$  and  $(1, c, d, s_3, s_4)$  be pairwise orthogonal rows of a complex Hadamard matrix of order 5. Then*

$$(1 + a + b)(1 + \bar{c} + \bar{d})(1 + c\bar{a} + d\bar{b}) \in \mathbb{R}.$$

This identity establishes a non-trivial algebraic relation in-between four entries of the  $5 \times 5$  matrix, or, in other words, eliminates 4 out of the 8 unknown variables. This leads, after further non-trivial arguments, to the following

**Theorem 2.1.6** (Haagerup, [60]). *All complex Hadamard matrices of order 5 are equivalent to the Fourier matrix  $F_5$ .*

We remark here that Lemma 2.1.5 applies for other orders as well (cf. Corollary 2.3.7). Haagerup's trick turned out to be powerful enough to deal with the full classification of the inverse-orthogonal matrices of order 5 as well [109]; it also has been successfully utilized in higher orders resulting in new examples of complex Hadamard matrices of order 6 [6], [103].

## 2.2 The evolution of Hadamard matrices of order 6

To fully appreciate our achievements described in this chapter we first recall all previous attempts which contributed towards the deeper understanding of the structure of complex Hadamard matrices of order 6.

### 2.2.1 Well-known matrices and their orbit

The most natural source of complex Hadamard matrices is the class of  $BH(n, q)$  matrices (see Definition 1.4.1). The case  $q = 2$  is well-known to be vacuous for  $n = 6$  but the next possible value already gives us the following

**Example 2.2.1** (Butson, [21]).

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

The  $BH(6, 3)$  matrix  $S_6^{(0)}$  is isolated amongst all complex Hadamard matrices of order 6 (see Definition 1.2.29). It can be obtained from Butson's doubling construction [21] and was utilized by Tao [140] to disprove Fuglede's conjecture (see Section 1.4.3). It is also a sporadic example of 2-transitive complex Hadamard matrices [105].

The next example comes from the conference matrix construction, described in Theorem 1.4.18. However, it was only realized very recently that this particular matrix admits an affine orbit.

**Example 2.2.2** (Diță, [44]).

$$D_6^{(1)}(c) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & \mathbf{i} & -c\mathbf{i} & -\mathbf{i} & c\mathbf{i} \\ 1 & \mathbf{i} & -1 & c\mathbf{i} & -\mathbf{i} & -c\mathbf{i} \\ 1 & -c\mathbf{i} & c\mathbf{i} & -1 & \mathbf{i} & -\mathbf{i} \\ 1 & -\mathbf{i} & -\mathbf{i} & \mathbf{i} & -1 & \mathbf{i} \\ 1 & c\mathbf{i} & -c\mathbf{i} & -\mathbf{i} & \mathbf{i} & -1 \end{bmatrix}.$$

The matrix  $D_6 = D_6^{(1)}(1)$  plays a central rôle in various constructions. We highlight some key facts as follows.

*Remark 2.2.3.* The free parameter  $c$  can be introduced into the matrix  $D_6$  through Theorem 1.2.16.  $\square$

*Remark 2.2.4.* The matrices  $S_6^{(0)}$  and  $D_6^{(1)}(1)$  are deeply entwined, as they both come from a general construction of complex Hadamard matrices with circulant core (see Lemma C.1.6). Also, they are the only  $6 \times 6$  dephased symmetric complex Hadamard matrices with real diagonal, [103].  $\square$

*Remark 2.2.5.* The  $BH(6, 8)$  matrix  $D_6^{(1)}(\mathbf{e}^{2\pi\mathbf{i}/8})$  is equivalent to the matrix found by Kolountzakis and Matolcsi, described in Example 1.4.55.  $\square$

Next we introduce the two-parameter Fourier families known already by Hadamard [61] as noted in [33] and rediscovered independently by Haagerup [60]. Their existence also follows from Diță's general construction (see [138]).

**Example 2.2.6.**

$$F_6^{(2)}(a, b) = \left[ \begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & a & a\omega & a\omega^2 \\ 1 & \omega^2 & \omega & b & b\omega^2 & b\omega \\ \hline 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & \omega & \omega^2 & -a & -a\omega & -a\omega^2 \\ 1 & \omega^2 & \omega & -b & -b\omega^2 & -b\omega \end{array} \right].$$

Note that the families  $F_6^{(2)}(a, b)$  and  $F_6^{(2)}(a, b)^T$  are inequivalent.

It is easy to see (for example, via Haagerup's invariant) that for generic values of the parameters  $a, b$  and  $c$  the families  $F_6^{(2)}(a, b)$ ,  $F_6^{(2)}(a, b)^T$  and  $D_6^{(1)}(c)$  are inequivalent matrices.

Our next example is the Björck–Fröberg cyclic 6-root matrix [10].

**Example 2.2.7** (Björck–Fröberg, [10]).

$$C_6 = \begin{bmatrix} 1 & \mathbf{i}d & -d & -\mathbf{i} & -\bar{d} & \mathbf{i}\bar{d} \\ \mathbf{i}\bar{d} & 1 & \mathbf{i}d & -d & -\mathbf{i} & -\bar{d} \\ -\bar{d} & \mathbf{i}\bar{d} & 1 & \mathbf{i}d & -d & -\mathbf{i} \\ -\mathbf{i} & -\bar{d} & \mathbf{i}\bar{d} & 1 & \mathbf{i}d & -d \\ -d & -\mathbf{i} & -\bar{d} & \mathbf{i}\bar{d} & 1 & \mathbf{i}d \\ \mathbf{i}d & -d & -\mathbf{i} & -\bar{d} & \mathbf{i}\bar{d} & 1 \end{bmatrix},$$

where  $d$  is Björck's “magical” number:<sup>1</sup>

$$d = \frac{1 - \sqrt{3}}{2} + \mathbf{i} \frac{\sqrt{2\sqrt{3}}}{2}.$$

We will return to the problem of the classification of circulant complex Hadamard matrices in Section 3.3.

It is natural to ask how well are we doing in terms of the classification of  $6 \times 6$  complex Hadamard matrices. It turns out that randomly chosen members of the families above, as well as the matrix  $C_6$  has defect 4 and hence all these matrices might be part of a larger, four-parameter family of complex Hadamard matrices, except for the single isolated point  $S_6^{(0)}$ . This observation led to the following

**Conjecture 2.2.8** (Bengtsson et al., [8]). *There is a four-parameter family of complex Hadamard matrices of order 6.*

Numerical experiments confirm the truth of this conjecture in a neighborhood around the Fourier matrix  $F_6$  [125]. In the next couple of subsections we shall recall further families with one, two and three parameters from the existing literature.

### 2.2.2 The self-adjoint family

So far we have listed “trivial” examples of complex Hadamard matrices. They are trivial for two reasons: first, the starting point matrices  $F_6^{(2)}(1, 1)$ ,  $D_6^{(1)}(1)$  and the matrices  $S_6^{(0)}$  and  $C_6$  can be found by a straightforward computer search. One simply knows in advance (or at least have an intelligent guess) what to look for. On the other hand, they are trivial because their orbit is affine. The first non-trivial, that is: non-affine

<sup>1</sup>As Bengtsson et al. refer to it in [8].

family of complex Hadamard matrices of order 6 was discovered by Beauchamp and Nicoară in 2006 [6], whose efforts were motivated by various operator algebraic reasons (see e.g. [56] and [72]). Their result amounts to a full classification of all self-adjoint complex Hadamard matrices of order 6.

**Example 2.2.9** (Beauchamp–Nicoară, [6]).

$$B_6^{(1)}(\theta) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -\bar{x} & -y & y & \bar{x} \\ 1 & -x & 1 & y & \bar{z} & -\overline{xyz} \\ 1 & -\bar{y} & \bar{y} & -1 & -\overline{xyz} & \overline{xyz} \\ 1 & \bar{y} & z & -xyz & 1 & -\bar{x} \\ 1 & x & -xyz & xyz & -x & -1 \end{bmatrix},$$

where

$$x = \frac{1 + 2y + y^2 \pm \sqrt{2}\sqrt{1 + 2y + 2y^3 + y^4}}{1 + 2y - y^2}, \quad z = \frac{1 + 2y - y^2}{y(-1 + 2y + y^2)},$$

and  $y = e^{i\theta}$  such that

$$\theta \in \left[-\pi, -\arccos\left(\left(\sqrt{3} - 1\right)/2\right)\right] \cup \left[\arccos\left(\left(\sqrt{3} - 1\right)/2\right), \pi\right]. \quad (2.1)$$

Note that this family is non-affine, and it is a priori unclear whether its entries are unimodular. In particular, the unimodularity of  $x$  forces the restriction (2.1) on the phase of  $y$ .

The main reason why this particular family can be described by relatively simple algebraic formulae is the fact that the entry  $-1$  appears in its core multiple times. Indeed, the presence of these entries imply that many of the vanishing sums of order 6 within this matrix trivially simplify to 6-term sums composed of a vanishing sum of order 4 and a vanishing sum of order 2, which we understand through Lemma 2.1.1.

We remark here that self-adjoint matrices are relatively rare, as the following folklore spectral analysis shows.

**Lemma 2.2.10.** *Let  $H$  be a self-adjoint complex Hadamard matrix of order  $n$ . Then either  $n$  is square or  $n$  is even and  $\text{Tr}(H) = 0$ .*

*Proof.* Consider a self-adjoint complex Hadamard matrix  $H$  of order  $n$  and suppose that the number 1 appears exactly  $k$  times in its main diagonal. Clearly, as  $H$  is self-adjoint its eigenvalues are  $\pm\sqrt{n}$  with multiplicities  $s$  and  $n - s$ , respectively. Then, we have

$$\text{Tr}(H) = s\sqrt{n} - (n - s)\sqrt{n} = k - (n - k),$$

from which the assertion follows.  $\square$

### 2.2.3 A symmetric family

Once it was realized that some preliminary assumptions on the structure of the matrix gives such a huge reduction in complexity Máté Matolcsi and the author managed to exhibit a new, previously unknown family of symmetric matrices [103].

**Example 2.2.11** (see [103]).

$$M_6^{(1)}(x) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & x & x & -x & -x \\ 1 & x & a & b & c & d \\ 1 & x & b & a & d & c \\ 1 & -x & c & d & e & f \\ 1 & -x & d & c & f & e \end{bmatrix},$$

where

$$\begin{aligned} a &= \frac{x^2 - 2x - 1}{4} + \mathbf{i} \frac{(x^2 - 2x - 1)\sqrt{16 - |x^2 - 2x - 1|^2}}{4|x^2 - 2x - 1|}, \\ b &= \frac{x^2 - 2x - 1}{4} - \mathbf{i} \frac{(x^2 - 2x - 1)\sqrt{16 - |x^2 - 2x - 1|^2}}{4|x^2 - 2x - 1|}, \\ c &= -\frac{x^2 + 1}{4} + \mathbf{i} \frac{(x^2 + 1)\sqrt{16 - |x^2 + 1|^2}}{4|x^2 + 1|}, \\ d &= -\frac{x^2 + 1}{4} - \mathbf{i} \frac{(x^2 + 1)\sqrt{16 - |x^2 + 1|^2}}{4|x^2 + 1|}, \\ e &= \frac{x^2 + 2x - 1}{4} + \mathbf{i} \frac{(x^2 + 2x - 1)\sqrt{16 - |x^2 + 2x - 1|^2}}{4|x^2 + 2x - 1|}, \\ f &= \frac{x^2 + 2x - 1}{4} - \mathbf{i} \frac{(x^2 + 2x - 1)\sqrt{16 - |x^2 + 2x - 1|^2}}{4|x^2 + 2x - 1|}, \end{aligned}$$

and  $x \neq \pm \mathbf{i}$  is any unimodular complex number.

The family  $M_6^{(1)}(x)$  was discovered by a careful analysis of dephased symmetric complex Hadamard matrices with real diagonal. We note that it connects the Fourier families  $F_6^{(2)}(a, b)$  with the family  $D_6^{(1)}(c)$ . Clearly the family  $M_6^{(1)}(x)$  does not describe all symmetric complex Hadamard matrices of order 6 as it misses the isolated matrix  $S_6^{(0)}$ . It is rather disappointing that a comprehensive characterization of all  $6 \times 6$  symmetric complex Hadamard matrices is still unavailable. We pose this as a

**Problem 2.2.12.** Classify all symmetric  $6 \times 6$  complex Hadamard matrices.

### 2.2.4 Bicirculant matrices

The first non-trivial two-dimensional family was constructed by the author during summer 2008 [129]. It was found by assuming that the matrix has a bicirculant structure, as follows.

**Example 2.2.13** (see [129]). Let

$$H = \begin{bmatrix} A & B \\ B^* & -A^* \end{bmatrix},$$

where  $A$  and  $B$  are  $3 \times 3$  circulant matrices:

$$A = \begin{bmatrix} 1 & a & b \\ b & 1 & a \\ a & b & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & c & d \\ d & 1 & c \\ c & d & 1 \end{bmatrix},$$

where the assumption that  $A$  and  $B$  have real diagonal 1 can be made due to equivalence. After dephasing the matrix  $H$  and change of variables we get

$$X_6^{(2)}(\alpha) \equiv X_6^{(2)}(x, y, u, v) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x^2y & xy^2 & \frac{xy}{uv} & uxy & vxy \\ 1 & \frac{x}{y} & x^2y & \frac{x}{u} & \frac{x}{v} & uvx \\ 1 & uvx & uxy & -1 & -uxy & -uvx \\ 1 & \frac{x}{u} & vxy & -\frac{x}{u} & -1 & -vxy \\ 1 & \frac{x}{v} & \frac{xy}{uv} & -\frac{xy}{uv} & -\frac{x}{v} & -1 \end{bmatrix},$$

where  $\alpha := x + y + \overline{xy}$ . It turns out, that in order to fill the matrix  $X_6^{(2)}(\alpha)$  in with unimodular entries one should restrict  $\alpha$  to come from the fundamental domain  $\mathbb{D}$  characterized by the property  $D(\alpha) \leq 0$  and  $D(-\alpha) \leq 0$  where the function  $D$  reads

$$D(\alpha) := |\alpha|^4 + 18|\alpha|^2 - 8\Re[\alpha^3] - 27.$$

We remark here that  $\mathbb{D}$  is an umbrella-shaped region coming from the intersection of two hypocycloids. For such numbers  $\alpha$  one can solve the cubic equation

$$f_\alpha(x) := x^3 - \alpha x^2 + \overline{\alpha}x - 1 \quad (2.2)$$

to obtain its roots  $r_1, r_2$  and  $r_3$  and set  $x = r_1, y = r_2$ . One should solve the equation  $f_{-\alpha}(u)$  as well to obtain its roots  $q_1, q_2$  and  $q_3$ , and similarly, set  $u = q_1, v = q_2$ . For  $\alpha \in \text{int}\mathbb{D}$  the roots of (2.2) are distinct and of modulus 1. In general for  $\alpha \in \text{int}\mathbb{D}$  one has  $6 \cdot 6 = 36$  choices for the ordered quadruple  $(x, y, u, v)$ . However, an easy automated calculation shows that all these matrices will be equivalent to either  $X_6^{(2)}(r_1, r_2, q_1, q_2)$  or its transpose.

We remark here that the family  $X_6^{(2)}(\alpha)$  unified and extended some of the eariler families introduced. In particular, for  $|\alpha| = 1$  we get the family  $D_6^{(1)}(c)$ , while on the boundary of  $\mathbb{D}$  we find the self-adjoint family  $B_6^{(1)}(\theta)$ . The reader should consult [129] for the details. We shall utilize the family  $X_6^{(2)}(\alpha)$  once again in Section 2.4.

### 2.2.5 Karlsson's observation

The next two-parameter family was discovered by Karlsson [77], who extended the family  $M_6^{(1)}(x)$  (see Example 2.2.11) with an additional degree of freedom as follows.

**Example 2.2.14** (Karlsson, [77]).

$$K_6^{(2)}(x_1, x_2) = \left[ \begin{array}{cc|cc|cc} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & z_1 & -z_1 & z_1 & -z_1 \\ \hline 1 & z_2 & -f_1 & -z_2 f_2 & -\bar{f}_3 & -z_2 \bar{f}_4 \\ 1 & -z_2 & -z_1 \bar{f}_2 & z_1 z_2 \bar{f}_1 & -z_1 f_4 & z_1 z_2 f_3 \\ \hline 1 & z_2 & -\bar{f}_3 & -z_2 \bar{f}_4 & -f_1 & -z_2 f_2 \\ 1 & -z_2 & -z_1 f_4 & z_1 z_2 f_3 & -z_1 \bar{f}_2 & z_1 z_2 \bar{f}_1 \end{array} \right],$$

where  $z_1 = \mathbf{e}^{\mathbf{i}x_1}$ ,  $z_2 = \mathbf{e}^{\mathbf{i}x_2}$ ,  $f_1 = f(x_1, x_2)$ ,  $f_2 = f(x_1, -x_2)$ ,  $f_3 = f(-x_1, -x_2)$  and  $f_4 = f(-x_1, x_2)$ , where

$$f(x_1, x_2) = \mathbf{e}^{\mathbf{i}(x_1+x_2)/2} \times \left( \cos\left(\frac{x_1-x_2}{2}\right) - \mathbf{i} \sin\left(\frac{x_1+x_2}{2}\right) \right) \left( \frac{1}{2} + \mathbf{i} \sqrt{\frac{1}{1+\sin(x_1)\sin(x_2)} - \frac{1}{4}} \right).$$

Karlsson also pointed out that all 9  $2 \times 2$  blocks are complex Hadamard. This discovery of his later lead to breakthrough results, which we shall discuss in more details soon.

Karlsson's matrix contains the Diță-family at the four limit points  $(x_1, x_2) \rightarrow (\pm\pi/2, \pm\pi/2)$  (the one-parameter comes from the direction of approach);  $K_6^{(2)}(x_1, 0)$  coincides with a one-parameter subfamily of the Fourier family  $F_6^{(2)}(a, b)$ , similarly, the family  $K_6^{(2)}(0, x_2)$  coincides with a one-parameter subfamily of the transposed Fourier family  $F_6^{(2)}(a, b)^T$ , and additionally for  $x_1 = x_2 =: x$  it coincides with the family  $M_6^{(1)}(x)$ , up to equivalence. Therefore Karlsson's matrix provides a bridge in-between previously known families.

### 2.2.6 $H_2$ -reducible complex Hadamard matrices

In a subsequent paper [75] Karlsson fully described the following important class of  $6 \times 6$  complex Hadamard matrices.

**Definition 2.2.15** (Karlsson, [75]). We say that a  $6 \times 6$  complex Hadamard matrix is  $H_2$ -reducible, if it is equivalent to a matrix in which all 9  $2 \times 2$  submatrices are complex Hadamard.

It turns out, that the  $H_2$ -reducible matrices can be described by a single, three-parameter family  $K_6^{(3)}(\theta, \varphi, z_1)$  in a very elegant way. Let us mention here the following breakthrough

**Theorem 2.2.16** (Karlsson, [75], [76]). *Let  $H$  be a dephased complex Hadamard matrix of order 6. Then the following are equivalent:*

- (a)  $H$  belongs to the three-parameter family  $K_6^{(3)}(\theta, \varphi, z_1)$ ;
- (b)  $H$  is  $H_2$ -reducible;
- (c) The core of  $H$  contains a  $-1$ ;
- (d) Some row or column of  $H$  contains a vanishing sum of order 2;
- (e) Some row or column of  $H$  contains a vanishing sum of order 4.

This is a very powerful theorem as Part (c) and (d) allow us to quickly recognize if a matrix belongs to the family  $K_6^{(3)}$ , and we shall heavily use these conditions later. As the family  $K_6^{(3)}$  forms a three-parameter subset, the matrices it contains are atypical, hence we often use the adjective “degenerate” in connection with it (see Conjecture 2.3.33).

As we can see from Part (c) of Theorem 2.2.16 Karlsson’s family contains all previously discovered matrices, except from the isolated matrix  $S_6^{(0)}$ , giving them an elegant and comprehensive presentation.

Let us recall Karlsson’s three-parameter family as follows.

**Example 2.2.17** (Karlsson, [76]).

$$K_6^{(3)}(\theta, \varphi, z_1) = \begin{bmatrix} F_2 & Z_1 & Z_2 \\ Z_3 & \frac{1}{2}Z_3AZ_1 & \frac{1}{2}Z_3BZ_2 \\ Z_4 & \frac{1}{2}Z_4BZ_1 & \frac{1}{2}Z_4AZ_2 \end{bmatrix}, \quad A = \begin{bmatrix} A_{11} & A_{12} \\ \overline{A}_{12} & -\overline{A}_{11} \end{bmatrix},$$

where

$$A_{11} = -\frac{1}{2} + \mathbf{i}\frac{\sqrt{3}}{2}(\cos \theta + \mathbf{e}^{-\mathbf{i}\varphi} \sin \theta), \quad A_{12} = -\frac{1}{2} + \mathbf{i}\frac{\sqrt{3}}{2}(-\cos \theta + \mathbf{e}^{\mathbf{i}\varphi} \sin \theta)$$

and  $B = -F_2 - A$  for any  $\theta \in [0, \pi)$  and  $\varphi \in [0, \pi)$ . In the matrices

$$Z_i = \begin{bmatrix} 1 & 1 \\ z_i & -z_i \end{bmatrix}$$

for  $i = 1, 2$  and their transpose (for  $i = 3, 4$ ) the elements  $z_i$  are related through the Möbius transformations as follows:

$$z_3^2 = \mathcal{M}_A(z_1^2), \quad z_3^2 = \mathcal{M}_B(z_2^2), \quad z_4^2 = \mathcal{M}_A(z_2^2), \quad z_4^2 = \mathcal{M}_B(z_1^2),$$

where

$$\mathcal{M}(z) = \frac{\alpha z - \beta}{\overline{\beta} z - \overline{\alpha}},$$



such that  $\alpha_A = A_{12}^2, \beta_A = A_{11}^2$  and  $\alpha_B = B_{12}^2, \beta_B = B_{11}^2$ . In general, any of the parameters  $z_i$  can be chosen freely, say  $z_1$  in which case

$$z_2^2 = \mathcal{M}_A^{-1}(\mathcal{M}_B(z_1^2)) = \mathcal{M}_B^{-1}(\mathcal{M}_A(z_1^2)), \quad z_3^2 = \mathcal{M}_A(z_1^2), \quad z_4^2 = \mathcal{M}_B(z_1^2)^2.$$

Any sign combination of the entries  $z_i$  will lead to equivalent matrices.

*Remark 2.2.18.* A similar structure theorem was suggested by Craigen, who asked if every real Hadamard matrix of order  $n > 1$  can be partitioned into a canonical form in which all of the  $n^2/4$   $2 \times 2$  matrices are of rank 2. Robert Lecnik confirmed this up to order 28 by a computer search.<sup>2</sup>  $\square$

## 2.3 A four-parameter family

Karlsson's results are very impressive, however they do not shed any light on the existence of a four-parameter family, as the introduction of any additional parameter into the matrix  $K_6^{(3)}(\theta, \varphi, z_1)$  would immediately destroy its underlying  $H_2$ -reducible property. Hence it is absolutely unclear how to generalize further Karlsson's construction, and it seems that one should come up with essentially new ideas to achieve this. In what follows we are going to describe one reasonable way to attack Conjecture 2.2.8. In the next subsection we collect a handful of ideas leading to a construction with four degrees of freedom, which is one of the main contributions of this manuscript. The results are to appear in [131].

### 2.3.1 The main ingredients

After seeing Karlsson's results we became extremely motivated to construct a four-parameter family, but in order to achieve this, some essentially new tools were needed. The breakthrough came when we managed to improve on Haagerup's result (cf. Lemma 2.1.5). Let us introduce the following crucial

**Definition 2.3.1** (Haagerup polynomial, [131]). The *Haagerup polynomial*  $\mathcal{H}$  associated with the rows  $(1, 1, 1, 1, 1, 1)$ ,  $(1, a, b, e, *, *)$  and  $(1, c, d, f, *, *)$  of a complex Hadamard matrix of order 6 reads

$$\mathcal{H}(a, b, c, d, e, f) := (1 + a + b + e)(1 + \bar{c} + \bar{d} + \bar{f})(1 + c\bar{a} + d\bar{b} + f\bar{e}).$$

The next result is our improvement upon Lemma 2.1.5.

---

<sup>2</sup>Private communication from R. Craigen; consult [35] for further details.

**Theorem 2.3.2** (see [131]). *Suppose that we have the partial rows  $(1, a, b, e, *, *)$  and  $(1, c, d, f, *, *)$ , composed from unimodular entries. Then one can specify some unimodular numbers  $s_1, s_2, s_3$  and  $s_4$  in place of the unknown numbers  $*$  to make these rows together with  $(1, 1, 1, 1, 1, 1)$  mutually orthogonal if and only if*

$$\mathcal{H}(a, b, c, d, e, f) = 4 - |1 + a + b + e|^2 - |1 + c + d + f|^2 - |1 + c\bar{a} + d\bar{b} + f\bar{e}|^2 \quad (2.3)$$

and

$$|1 + a + b + e| \leq 2. \quad (2.4)$$

Before proceeding to the Proof of Theorem 2.3.2 we shall need two easy results first.

**Lemma 2.3.3.** *Suppose that we have a partial row  $(1, a, b, e, *, *)$  composed from unimodular entries. Then one can specify some unimodular numbers  $s_1$  and  $s_2$  in place of the unknown numbers  $*$  to make this row orthogonal to  $(1, 1, 1, 1, 1, 1)$  if and only if  $|1 + a + b + e| \leq 2$ .*

*Proof.* We need to have  $1 + a + b + e + s_1 + s_2 = 0$  to ensure orthogonality, from which it follows that  $|1 + a + b + e| = |s_1 + s_2| \leq 2$ . It is easily seen through geometry that in this case we can define the unimodular numbers required.  $\square$

The missing coordinates featuring in Lemma 2.3.3,  $s_1$  and  $s_2$ , can be obtained algebraically through the well-known

**Lemma 2.3.4** (Decomposition formula, [103]). *Suppose that the rows  $(1, 1, 1, 1, 1, 1)$  and  $(1, a, b, e, s_1, s_2)$  containing unimodular entries are orthogonal. Let us denote by  $\Sigma := 1 + a + b + e$ , and suppose that  $0 < |\Sigma| \leq 2$ . Then*

$$s_{1,2} = -\frac{\Sigma}{2} \pm \mathbf{i} \frac{\Sigma}{|\Sigma|} \sqrt{1 - \frac{|\Sigma|^2}{4}}; \quad (2.5)$$

otherwise, if  $\Sigma = 0$ , then  $s_1$  is independent from  $a, b, e$  but  $s_2 = -s_1$ .

*Proof.* If  $\Sigma = 0$  then the result is trivial. Otherwise  $s_1$  and  $s_2$  are the (unique) unimodular numbers with  $s_1 + s_2 = -\Sigma$ , required by orthogonality.  $\square$

Observe that in (2.5) we would divide by zero in case  $\Sigma = 0$ . This, however, can never happen when we investigate complex Hadamard matrices which are not  $H_2$ -reducible, as seen by Part (e) of Theorem 2.2.16. Therefore it follows that once we have four entries in a row or column of a matrix which lies outside the family  $K_6^{(3)}$  the Decomposition formula readily derives the unique remaining two values through (2.5). Now we can turn to the

*Proof of Theorem 2.3.2.* First we start by proving that (2.3) holds. To do this, we utilize Haagerup's idea [60] as follows: by pairwise orthogonality, we find that

$$\begin{aligned} 1 + a + b + e &= -s_1 - s_2, \\ 1 + \bar{c} + \bar{d} + \bar{f} &= -\bar{s}_3 - \bar{s}_4, \\ 1 + c\bar{a} + d\bar{b} + f\bar{e} &= -s_3\bar{s}_1 - s_4\bar{s}_2. \end{aligned}$$

The first equation above ensures that (2.4) holds. Further, the product of these equations read

$$\begin{aligned} \mathcal{H} &= -(s_1 + s_2)(\bar{s}_3 + \bar{s}_4)(s_3\bar{s}_1 + s_4\bar{s}_2) = -(s_1\bar{s}_3 + s_2\bar{s}_4 + s_1\bar{s}_4 + s_2\bar{s}_3)(s_3\bar{s}_1 + s_4\bar{s}_2) \\ &= -|s_1\bar{s}_3 + s_2\bar{s}_4|^2 - (s_1\bar{s}_4 + s_2\bar{s}_3)(s_3\bar{s}_1 + s_4\bar{s}_2) = -|s_1\bar{s}_3 + s_2\bar{s}_4|^2 - 2\Re(s_1\bar{s}_2 + s_3\bar{s}_4). \end{aligned}$$

To conclude the proof, we need to show that

$$2\Re(s_1\bar{s}_2 + s_3\bar{s}_4) = |1 + a + b + e|^2 + |1 + c + d + f|^2 - 4$$

holds, however this follows directly from the Decomposition formula.

To see the converse direction, we need to show that (2.3) essentially encodes orthogonality. Let us use the notations  $\Sigma := 1 + a + b + e$ ,  $\Delta := 1 + c + d + f$ ,  $\Psi := 1 + c\bar{a} + d\bar{b} + f\bar{e}$ . With this notation we have  $|\Sigma| \leq 2$  from (2.4) while condition (2.3) boils down to

$$\mathcal{H} = \Sigma\bar{\Delta}\Psi = 4 - |\Sigma|^2 - |\Delta|^2 - |\Psi|^2. \quad (2.6)$$

If, in addition,  $|\Delta| \leq 2$  holds, then by the Decomposition formula we can find  $s_1, s_2, s_3$  and  $s_4$  to ensure orthogonality to row  $(1, 1, 1, 1, 1, 1)$ . Now observe, that the mutual orthogonality of rows  $(1, a, b, e, s_1, s_2)$  and  $(1, c, d, f, s_3, s_4)$  reads

$$\Psi + s_3\bar{s}_1 + s_4\bar{s}_2 = 0. \quad (2.7)$$

Suppose first that we have the trivial case  $\Sigma = \Delta = 0$ . Then, by the Decomposition formula we have  $s_2 = -s_1$  and  $s_4 = -s_3$ , and (2.6) implies that  $|\Psi| = 2$ . Therefore, if we set the unimodular number  $s_3 := -\Psi s_1/2$  the orthogonality equation (2.7) is fulfilled.

Suppose secondly, that we have  $\Delta = 0$ , but  $\Sigma \neq 0$ . Then we have  $s_4 = -s_3$ , and from (2.6) it follows that

$$|\Psi| = \sqrt{4 - |\Sigma|^2}. \quad (2.8)$$

Now we use the Decomposition formula to find the values of  $s_1$  and  $s_2$  and the orthogonality equation (2.7) becomes

$$\Psi + s_3 \left( -2i \frac{\bar{\Sigma}}{|\Sigma|} \sqrt{1 - \frac{|\Sigma|^2}{4}} \right) = 0. \quad (2.9)$$

This holds, independently of  $s_3$ , if  $|\Sigma| = 2$ , as by (2.8)  $\Psi = 0$  follows. Otherwise, set the unimodular number

$$s_3 := -\mathbf{i} \frac{\Sigma\Psi}{|\Sigma||\Psi|}$$

to ensure the orthogonality through (2.9). The case  $\Sigma = 0$ ,  $\Delta \neq 0$  can be treated similarly by noting that  $|\Delta| \leq 2$  follows from (2.6).

Finally, let us suppose that  $\Sigma \neq 0$  and  $\Delta \neq 0$ . Now observe that in this case the value of  $\Psi$  needed for formula (2.7) can be calculated through (2.6). The other ingredient, namely the value of  $s_3\bar{s}_1 + s_4\bar{s}_2$  can be established through the Decomposition formula, once we derive the required bound  $|\Delta| \leq 2$ . Depending on the value of  $\mathcal{H}$ , we treat several cases differently.

CASE 1: Suppose that  $-|\Psi|^2 \leq \mathcal{H}$ . This implies, via (2.6), that  $|\Sigma|^2 + |\Delta|^2 \leq 4$ , and in particular  $|\Delta| \leq 2$  follows. Next we calculate  $|\Psi|$  from (2.6).

Suppose first that  $\mathcal{H} \geq 0$ . Hence, after taking absolute values, (2.6) becomes

$$|\Psi|^2 + |\Sigma||\Delta||\Psi| + |\Sigma|^2 + |\Delta|^2 - 4 = 0,$$

and the only non-negative root is

$$|\Psi| = \frac{-|\Sigma||\Delta| + \sqrt{(4 - |\Sigma|^2)(4 - |\Delta|^2)}}{2}. \quad (2.10)$$

Now suppose that  $-|\Psi|^2 \leq \mathcal{H} < 0$ . Hence, after taking absolute values, (2.6) becomes

$$|\Psi|^2 - |\Sigma||\Delta||\Psi| + |\Sigma|^2 + |\Delta|^2 - 4 = 0, \quad (2.11)$$

and we find that its only non-negative root under the assumption  $|\Sigma|^2 + |\Delta|^2 \leq 4$  reads

$$|\Psi| = \frac{|\Sigma||\Delta| + \sqrt{(4 - |\Sigma|^2)(4 - |\Delta|^2)}}{2}. \quad (2.12)$$

CASE 2: Suppose now that  $\mathcal{H} < -|\Psi|^2$ . This implies that  $|\Sigma|^2 + |\Delta|^2 > 4$ , and we do not have a priori the bound  $|\Delta| \leq 2$ . Nevertheless, we derive equation (2.11) again, and we find that the values of  $|\Psi|$  can be any of

$$|\Psi|_{1,2} = \frac{|\Sigma||\Delta| \pm \sqrt{(4 - |\Sigma|^2)(4 - |\Delta|^2)}}{2}, \quad (2.13)$$

provided that the roots are real, namely we have either  $|\Sigma| > 2$  and  $|\Delta| > 2$  or  $|\Sigma| \leq 2$  and  $|\Delta| \leq 2$ . The first case, however, contradicts the crucial condition (2.4).

Once we have established the bound  $|\Delta| \leq 2$  and the value(s) of  $|\Psi|$  has been found, we are free to use the Decomposition formula to obtain the values of  $s_1$ ,  $s_2$ ,  $s_3$  and  $s_4$ . Clearly, we can set  $s_1$  with the  $+$  sign, while  $s_2$  with the  $-$  sign as in formula (2.5), up

to equivalence. However, we do not know a priori how to distribute the signs amongst  $s_3$  and  $s_4$ , and to simplify the notations we define

$$s_3 = -\frac{\Delta}{2} \pm \mathbf{i} \frac{\Delta}{|\Delta|} \sqrt{1 - \frac{|\Delta|^2}{4}}, \quad s_4 = -\frac{\Delta}{2} \mp \mathbf{i} \frac{\Delta}{|\Delta|} \sqrt{1 - \frac{|\Delta|^2}{4}}. \quad (2.14)$$

In particular, by using (2.6) and (2.14) we find that the orthogonality equation (2.7) becomes

$$\frac{4 - |\Sigma|^2 - |\Delta|^2 - |\Psi|^2}{\Sigma\Delta} + \frac{\bar{\Sigma}\Delta}{2} \pm 2 \frac{\bar{\Sigma}\Delta}{|\Sigma||\Delta|} \sqrt{1 - \frac{|\Sigma|^2}{4}} \sqrt{1 - \frac{|\Delta|^2}{4}} = 0, \quad (2.15)$$

where the  $\pm$  sign agrees with the definition of  $s_3$ . To conclude the theorem plug in all of the possible values of  $|\Psi|$  as described in (2.10), (2.12), (2.13) into (2.15) to verify that for some sign choice it holds identically.  $\square$

*Remark 2.3.5.* Both of the two possible signs described by formula (2.13) can be realized, as the following two examples demonstrate:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -\omega^2 & \omega & -1 & \omega^2 & -\omega \\ 1 & -\omega & \omega^2 & -1 & \omega & -\omega^2 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -\omega^2 & \omega & -1 & \omega^2 & -\omega \\ 1 & -\omega^2 & \omega^2 & -\omega & \omega & -1 \end{bmatrix}.$$

In particular, there are two different orthogonal triplet of rows of order 6, composed from sixth roots of unity, such that  $|\Sigma| = |\Delta| = \sqrt{3}$  in both cases, however, in one of the cases  $|\Psi| = 1$  while  $|\Psi| = 2$  in the other.  $\square$

It is natural to ask if condition (2.3) implies the inequality (2.4) automatically. While we tend to believe that this is so, proving such a statement would require a more sophisticated understanding of the geometry of orthogonal vectors of modulus 1. We pose this as a relevant

**Problem 2.3.6.** Investigate if condition (2.3) implies the inequality (2.4) automatically in Theorem 2.3.2.

We have already seen the following statement formulated for  $5 \times 5$  matrices (cf. Lemma 2.1.5). We state it again tailored especially for the  $6 \times 6$  case.

**Corollary 2.3.7** (Haagerup's trick, [60]). *Suppose that  $(1, 1, 1, 1, 1, 1)$ ,  $(1, a, b, e, s_1, s_2)$  and  $(1, c, d, f, s_3, s_4)$  are three pairwise orthogonal rows of a complex Hadamard matrix of order 6. Then*

$$\mathcal{H}(a, b, c, d, e, f) \in \mathbb{R}. \quad (2.16)$$

As we have pointed out earlier, Haagerup used the property (2.16) to give a complete characterization of complex Hadamard matrices of order 5, or equivalently, describe

the orthogonal maximal abelian  $*$ -subalgebras of the  $5 \times 5$  matrices [60]. Since then it was used in [6] and [103] to construct new, previously unknown complex Hadamard matrices of order 6 as well. However, to guarantee the mutual orthogonality of three rows the necessary condition (2.16) should be replaced by the more informative identity (2.3). Nevertheless, (2.16) will play an essential rôle in our construction too. These type of identities are extremely useful as they feature less variables than the standard orthogonality equations considerably simplifying the calculations required.

Thus, we have given an algebraic characterization of the orthogonality of triplets of rows in complex Hadamard matrices of order 6. This, however, still give us six degrees of freedom instead of the desired 4, and it is not entirely trivial how to get rid of two of the six parameters.

The other essential tool of our construction is motivated by the following well-known theorem in functional analysis (see [112]). We recall that an operator  $A$  is said to be a contraction, if its operator norm satisfies  $\|A\| \leq 1$ .

**Theorem 2.3.8** (Unitary dilation). *Every contraction  $A$  has a unitary dilation.*

*Proof.* Indeed, let us define the so-called defect operator

$$D_A := (I - A^*A)^{\frac{1}{2}},$$

which is positive where the square root is defined via the continuous functional calculus. Then, the desired unitary matrix reads

$$U = \begin{bmatrix} A & D_{A^*} \\ D_A & -A^* \end{bmatrix}. \quad \square$$

Now we combine the previous two ideas as follows. We start with a submatrix

$$E(a, b, c, d) := \begin{bmatrix} 1 & 1 & 1 \\ 1 & a & b \\ 1 & c & d \end{bmatrix} \quad (2.17)$$

and attempt to embed it into a complex Hadamard matrix of order 6

$$G_6^{(4)}(a, b, c, d) := \left[ \begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a & b & e & s_1 & s_2 \\ 1 & c & d & f & s_3 & s_4 \\ \hline 1 & g & h & * & * & * \\ 1 & t_1 & t_3 & * & * & * \\ 1 & t_2 & t_4 & * & * & * \end{array} \right] \equiv \begin{bmatrix} E & B \\ C & D \end{bmatrix} \quad (2.18)$$

with  $3 \times 3$  blocks  $E, B, C$  and  $D$  in two steps, as follows. First we construct the submatrices  $B$  and  $C$  featuring unimodular entries to obtain three orthogonal rows

and columns of  $G_6$ . Secondly we find the unique lower right submatrix  $D$  to get a unitary matrix. Should the entries of this matrix become unimodular, we have found a complex Hadamard matrix. We conjecture that the submatrix  $E$  can be chosen, up to equivalence, in a way that there will be only finitely many candidates for the blocks  $B$  and  $C$  and therefore we can ultimately decide throughout a finite, case-by-case analysis whether the submatrix  $E$  can be embedded into a complex Hadamard matrix. The resulting matrix  $G_6$  can be thought as the “Hadamard dilation” of the operator  $E$ .

Now we turn to the details of our construction.

### 2.3.2 Further preliminary results

In this section we present various other results necessary to the construction of the family  $G_6^{(4)}$ , outlined previously.

Solving the system of equations (2.3)–(2.16) is the key step to obtain the submatrices  $B$  and  $C$  of  $G_6$ , and once we have three orthogonal rows and columns we readily fill out the remaining lower right submatrix  $D$ . This is explained by the following two lemmata, the first of which being a special case of a more general matrix inversion

**Lemma 2.3.9.** *If  $U$  and  $V$  are  $n \times n$  matrices then*

$$(I_n + UV)^{-1} = I_n - U(I_n + VU)^{-1}V$$

*provided that one of the matrices  $I_n + UV$  or  $I_n + VU$  is nonsingular.*

*Proof.* By symmetry, we can suppose that the matrix  $I_n + VU$  is nonsingular. Then, we have

$$(I_n + UV)(I_n - U(I_n + VU)^{-1}V) = I_n + UV - U(I_n + VU)(I_n + VU)^{-1}V = I_n. \quad \square$$

**Lemma 2.3.10.** *Suppose that we have a  $6 \times 6$  partial complex Hadamard matrix consisting of three orthogonal rows and columns, containing no vanishing  $3 \times 3$  minor. Then there is a unique way to construct a  $6 \times 6$  unitary matrix containing these rows and columns as a submatrix.*

*Proof.* Let  $U$  be a  $6 \times 6$  matrix with  $3 \times 3$  blocks  $A, B, C$  and  $D$ , as the following:

$$U = \begin{bmatrix} A & B \\ C & D \end{bmatrix}.$$

By the orthogonality of the first three rows and columns and using the fact that the entries are unimodular, we have

$$AA^* + BB^* = 6I_3 \tag{2.19}$$

$$A^*A + C^*C = 6I_3 \quad (2.20)$$

To ensure orthogonality in-between the first three and the last three rows we need to have  $AC^* + BD^* = 0$ . As  $B$  is nonsingular by our assumptions we can define

$$D := -CA^*(B^{-1})^*. \quad (2.21)$$

Now we need to show that the last three rows are mutually orthogonal as well. Indeed, by using (2.21) and (2.19) we have

$$CC^* + DD^* = C(I_3 + A^*(BB^*)^{-1}A)C^* = C(I_3 + A^*(6I_3 - AA^*)^{-1}A)C^*,$$

which, by Lemma 2.3.9 and (2.20) equals to

$$C\left(I_3 + \frac{1}{6}A^*\left(I_3 - \frac{1}{6}AA^*\right)^{-1}A\right)C^* = C\left(I_3 - \frac{1}{6}A^*A\right)^{-1}C^* = 6C(C^*C)^{-1}C^* = 6I_3.$$

□

We do not state that the obtained unitary matrix  $U$  is Hadamard, which is not true in general. Recall that our goal is to embed the submatrix  $E$  into the matrix  $G_6$  (see (2.17)-(2.18)). We have the following trivial

**Lemma 2.3.11.** *Suppose that a submatrix  $E$  can be embedded into a complex Hadamard matrix  $G_6$  of order 6 in which the upper right submatrix  $B$  is invertible. Then for some unimodular submatrix  $C$  for which the first three columns of  $G_6$  are orthogonal the lower right submatrix  $D = -CE^*(B^{-1})^*$  is unimodular.*

*Proof.* Indeed, this is exactly what embedding means. □

In particular, if the submatrices  $B$  and  $C$  are chosen carefully, the unimodular property of  $D$  follows for free.

**Corollary 2.3.12.** *Start from a submatrix  $E$  and suppose that there are only finitely many invertible candidate matrices  $B \in SOL_B$  and  $C \in SOL_C$  such that the first three rows and columns of the matrix  $G_6$  are orthogonal. Then  $E$  can be embedded into a complex Hadamard matrix of order 6 if and only if there is some  $B \in SOL_B$  and  $C \in SOL_C$  such that the matrix  $D = -CE^*(B^{-1})^*$  is unimodular.*

Note that due to the finiteness condition in Corollary 2.3.12 once we have all (and only finitely many) candidate matrices  $B$  and  $C$  we can decide algorithmically whether the submatrix  $E$  can be embedded into a complex Hadamard matrix.

The next step is to characterize  $6 \times 6$  complex Hadamard matrices with vanishing  $3 \times 3$  minors. To do this we need two auxiliary results first.



**Lemma 2.3.13.** *Suppose that in a dephased  $6 \times 6$  complex Hadamard matrix there exists a noninitial row (or column) containing three identical entries  $x$ . Then  $x = \pm 1$  and this row (or column) reads  $(1, 1, 1, -1, -1, -1)$ , up to permutations.*

*Proof.* Suppose to the contrary, that there are three nonreal numbers  $x$  in a row (column). Then the sum of these numbers  $x$  together with the leading 1 read  $|1 + 3x|^2 = 10 + 6\Re[x] > 4$ , and hence, by Lemma 2.3.3 this row (column) cannot be orthogonal to the first row (column), a contradiction. To ensure orthogonality to the first row (column) we should specify the remaining three entries to  $-x$  and hence the last part of the statement follows.  $\square$

Now by combining Lemma 2.3.13 with Theorem 2.2.16 we arrive at the following

**Corollary 2.3.14.** *Suppose that in a dephased  $6 \times 6$  complex Hadamard matrix  $H$  there exists a noninitial row (or column) containing three identical entries. Then  $H$  belongs to the family  $K_6^{(3)}$ .*

Now we can state the desired structural result.

**Proposition 2.3.15.** *Suppose that a  $6 \times 6$  complex Hadamard matrix  $H$  has a vanishing  $3 \times 3$  minor. Then  $H$  belongs to the family  $K_6^{(3)}$ .*

*Proof.* Suppose that  $H$  has a vanishing  $3 \times 3$  minor, say the upper left submatrix  $E(a, b, c, d)$ , as in formula (2.17). Such an assumption can be made, up to equivalence. As  $\det(E) = b + c - a - d + ad - bc = 0$ , we find that if any of the indeterminates  $a, b, c, d$  is equal to 1 then  $E$  contains a noninitial row (or column) containing three 1s, and therefore by Corollary 2.3.14 we conclude that this matrix belongs to the family  $K_6^{(3)}$ . Otherwise, we can suppose that none of  $a, b, c, d$  is equal to 1 and hence we find that  $d = (a + bc - b - c)/(a - 1)$ , which should be of modulus one. To ensure this, solve the equation  $d\bar{d} - 1 = 0$  to find that either  $b = a$  or  $c = a$  should hold, but then we have either  $d = c$  or  $d = b$  as well. In particular, we find that  $E$  has two identical columns (or rows). Therefore  $E$  can be transformed, by appropriate multiplication of the rows (or columns) by unimodular numbers, into a matrix  $E'$  which has two column (or row) of entries 1, and a reference to Corollary 2.3.14 concludes the lemma.  $\square$

Therefore to investigate those matrices which lie outside the family  $K_6^{(3)}$  we can safely use Lemma 2.3.10 and in particular the inversion formula (2.21).

It turns out, that the isolated matrix  $S_6^{(0)}$  (see Example 2.2.1) requires a special treatment as well. It is featured in the following

**Lemma 2.3.16.** *Suppose that in a  $6 \times 6$  dephased complex Hadamard matrix  $H$  there is a noninitial row or column composed of cubic roots of unity. Then  $H$  is either equivalent to  $S_6^{(0)}$  or belongs to the family  $K_6^{(3)}$ .*

Recall that we have denoted by  $\omega$  the principal cubic root of unity.

*Proof.* We can assume that the core of  $H$  does not contain a  $-1$ , otherwise, by Theorem 2.2.16, we are done. Let us suppose that  $H$  contains a full row of cubic entries, and its second and third row reads  $(1, 1, \omega, \omega, \omega^2, \omega^2)$  and  $(1, a, b, c, d, e)$ , respectively. Then, by considering the orthogonality equations in-between the first three rows of  $H$ , we easily obtain that  $1 + a - b\omega - c\omega = 0$  implying (as  $a \neq -1$ ) that  $b = \omega^2$  or  $c = \omega^2$ . Now notice that this means that in any further row of  $H$  one of the third or fourth entries must be  $\omega^2$ . However, this implies that both the third and fourth column of  $H$  is composed of purely cubic entries. Similarly, one can deduce the equation  $1 + a - d\omega^2 - e\omega^2 = 0$  and apply the same argument *mutatis mutandis* to the fifth and sixth columns of  $H$  as well. To conclude observe that from the aforementioned it follows that the matrix  $H$  is composed entirely of cubic roots of unity and hence it is equivalent to  $S_6^{(0)}$  as desired. The case when  $H$  contains a full column of cubic entries is analogous.  $\square$

Now we turn to the presetting of the submatrix  $E(a, b, c, d)$  (see (2.17)). In order to avoid the case when the system of equations (2.3)–(2.16) is linearly dependent we need to exclude various input quadruples  $(a, b, c, d)$ . However, it shall turn out that we are free to do such restrictions, up to equivalence. To simplify the forthcoming terminology let us define the following two-variable function mapping  $\mathbb{T}^2$  to  $\mathbb{C}$  as follows:

$$\mathcal{E}(x, y) := x + y + x^2 + y^2 + xy^2 + x^2y.$$

We say that  $y$  is an elliptical pair of  $x$ , if  $\mathcal{E}(x, y) = 0$ . Observe that for a given  $x \neq -1$  the sum of its elliptical pairs read  $y_1 + y_2 = -(1 + x^2)/(1 + x)$ . The following is a strictly technical

**Proposition 2.3.17** (Canonical transformation). *Suppose that we have a complex Hadamard matrix  $H$  inequivalent from  $S_6^{(0)}$  and any of the members of the family  $K_6^{(3)}$ . Then  $H$  has a  $3 \times 3$  submatrix  $E(a, b, c, d)$  as in formula (2.17), up to equivalence, satisfying*

$$(b - 1)(c - 1)(b - d^2)(c - d^2)(b - c)(bc - d)\mathcal{E}(b, d)\mathcal{E}(c, d) \neq 0. \quad (2.22)$$

*Proof.* The strategy of the proof is the following: first we pick a “central element”  $d$  from the core of the matrix and then we show that  $b$  and  $c$  can be set satisfying (2.22). Recall, that by Lemma 2.3.16 there is no noninitial row or column composed from cubic roots of unity in the matrix.

First let us assume that there is a number 1 in the core somewhere; set  $d = 1$ , and choose a non-cubic  $c$  from its row. Note that there cannot be a further noninitial 1 in the row or column of  $d$  by Corollary 2.3.14. Now observe that as the elliptical pairs

of 1 are  $\omega$  and  $\omega^2$ , we can choose a suitable  $b$  from the column of  $d$  unless all entries there are members of the set  $\{\omega, \omega^2, c, \bar{c}\}$ . Note that  $\omega$  together with  $\omega^2$  cannot be in the column of  $d$  at the same time, and from this it is easily seen that we can define the value of  $b$  to satisfy (2.22) unless the column of  $d$  is one of the following four cases, up to permutations:  $(1, 1, \omega, c, c, \bar{c})$ ,  $(1, 1, \omega, c, \bar{c}, \bar{c})$ ,  $(1, 1, \omega^2, c, c, \bar{c})$ ,  $(1, 1, \omega^2, c, \bar{c}, \bar{c})$ . However, by normalization and by orthogonality, the sum of the entries in this column should add up to 0, and we find in all cases that the unimodular solution to  $c$  is a cubic root of unity, contradicting the choice of  $c$ . Therefore one of the entries in the column of  $d$  is different from  $\omega, \omega^2, c, \bar{c}$  which will be chosen as  $b$ .

Secondly, let us suppose, that the number 1 is not present in the core. In particular, all entries in the core are different rowwise and columnwise.

Pick an arbitrary number  $d$  from the core of the matrix, and let us denote by  $c_1$  and  $c_2$  its the elliptical pairs (maybe  $c_1 = c_2$ , or they are undefined). Now we have several cases depending on the appearance of these values in the row and column containing  $d$ .

CASE 1:  $c_1$  and  $c_2$  present in both the row and column containing  $d$ . Hence, in this row and column there are the entries 1,  $d$ ,  $c_1$  and  $c_2$  already and the remaining two,  $\alpha$  and  $\beta$ , are uniquely determined by the Decomposition formula. Note that  $\alpha \neq d^2$ , as otherwise we would have  $\beta = -(2d + d^2 + d^3)/(1 + d)$  (as the sum of all entries in a noninitial row add up to 0, and the sum of the elliptical pairs is known), which is unimodular if and only if  $d = \pm \mathbf{i}$  or  $d = \omega$  or  $d = \omega^2$ . In the first case we have  $\beta = \mp \mathbf{i}$  and we are dealing with a member of the family  $K_6^{(3)}$ . The second and third case imply that we have a full row and a full column of cubics, a contradiction. If  $\beta \neq d/\alpha$  then by picking  $c = \alpha$  from the row we can set  $b = \beta$  in the column. Otherwise, in case we have  $\beta = d/\alpha$ , then reset the central element  $d$  to the number  $\alpha$  which is in the same row as  $d$ . Now observe that after this exchange we should meet the requirements of Case 1 again (otherwise we are done here), and hence the elliptical pairs of  $\alpha$ ,  $\alpha_1$  and  $\alpha_2$ , should present in the row and column of  $\alpha$ , which therefore contain exactly the same entries. However  $\alpha_{1,2} \neq d$ , as otherwise orthogonality, together with the condition  $\mathcal{E}(\alpha, d) = 0$  would imply  $d = \pm 1$ , a contradiction;  $\alpha_{1,2} \neq d/\alpha$ , as otherwise  $d = \omega$  or  $d = \omega^2$  would follow from the same argument implying that the row containing  $\alpha$  has a noninitial 1, a contradiction. Therefore, the only option left is that  $\alpha_{1,2} = c_{1,2}$ . But then we can set  $c = d \neq \alpha^2$  and  $b = d/\alpha \neq \alpha^2$ , and we are done.

CASE 2:  $c_1$  and  $c_2$  present in (to say) the row containing  $d$ , but only one of these values (say  $c_1$ ) is present in the column of  $d$ . Let us denote by  $\alpha$  and  $\beta$  the two further entries in this row which, again, are different from  $d^2$ . In the column of  $d$  there are already the numbers 1,  $d$  and  $c_1$ , and observe that the remaining triplet of entries cannot be  $(d^2, \alpha, \beta)$  as this would imply  $d^2 = c_2$ , contradicting our case-assumption.

Therefore one of the three unspecified entries  $\gamma$  is different from  $d^2$ ,  $\alpha$  and  $\beta$ . Now if  $\gamma \neq d/\alpha$  then set  $c = \alpha$ ,  $b = \gamma$  otherwise set  $c = \beta$ ,  $b = \gamma$ . We are done.

CASE 3: Only the value  $c_1$  is in (to say) the row containing  $d$  and in the column of  $d$  as well. This is a tricky case, as it might happen that the undetermined triplet in both the  $d$ th row and column is precisely  $(d^2, \alpha, d/\alpha)$ , and therefore we cannot ensure condition (2.22). However, from the orthogonality equation  $1 + d + d^2 + c_1 + \alpha + d/\alpha = 0$  and from its conjugate we can eliminate the variable  $c_1$  in order to obtain the equation  $(1 + \alpha)(d + \alpha)(c_1 - \bar{d}) = 0$  leading us either to the family  $K_6^{(3)}$  or to  $c_1 = \bar{d}$ . In the latter case, however, we can calculate the values of  $d$  and  $\alpha$  explicitly by invoking the elliptical condition  $\mathcal{E}(c_1, d) = 0$ . In particular, we find that the values of  $d$  and  $\alpha$  are given by some of the unimodular roots of the following polynomials  $1 + 2d + 2d^3 + d^4 = 0$  and  $1 + 4\alpha - 2\alpha^2 - 8\alpha^3 - 8\alpha^4 - 8\alpha^5 - 2\alpha^6 + 4\alpha^7 + \alpha^8 = 0$ . Now reset the “central” entry  $d$  to  $\alpha$ , and observe that the elliptical pairs of  $\alpha$  are not present in its row, and therefore the conditions of this subcase are no longer met. Otherwise we can suppose that the undetermined triplet in the column of  $d$  is not  $(d^2, \alpha, d/\alpha)$ . Set  $c = \alpha \neq d^2$ . Pick  $\gamma$  from the column which is different from  $d^2$ ,  $\alpha$ ,  $d/\alpha$ , set  $b = \gamma$  and we are done.

CASE 4: Only the value  $c_1$  is in (to say) the row containing  $d$  and in the column of  $d$  there is the other elliptical value  $c_2 \neq c_1$ . We can suppose that two of the undetermined entries in the row of  $d$  satisfy  $\alpha \neq d^2$  and  $\beta \neq d^2$  and set  $c = \alpha$ . Now if in the column the undefined triplet is precisely  $(\alpha, d/\alpha, d^2)$ , then observe that the same triplet cannot appear in the row, as otherwise  $c_1 = c_2$  would follow. Therefore we can reset  $c$  to a value different from  $\alpha, d/\alpha, d^2$ , and set  $b = \alpha$ . Otherwise there is an entry in the column which can be set to  $b$ , we are done.

CASE 5: In the column of  $d$  there are no elliptical values at all. Pick any  $c = \alpha \neq d^2$  from the row of  $d$  which is different from both  $c_1$  and  $c_2$ . As in the column of  $d$  there are four unspecified entries, one of them, say  $\gamma$  will be different from  $d^2$ ,  $\alpha$  and  $d/\alpha$ . Set  $b = \gamma$ . We are done.  $\square$

However, not every submatrix  $E$  can be embedded into a complex Hadamard matrix of order 6 as we shall see shortly. Let us denote by  $\|\cdot\|_2$  both the Euclidean norm on  $\mathbb{C}^6$  and the induced operator norm on the space of  $6 \times 6$  matrices. We have the following necessary condition.

**Lemma 2.3.18.** *Suppose that  $A$  is a  $3 \times 3$  submatrix of a complex Hadamard matrix  $H$  of order 6. Then  $A/\sqrt{6}$  is a contraction.*

*Proof.* Clearly, we can assume that this submatrix  $A$  is the upper left of the matrix  $H$ , which we will write in block form, as follows:

$$H = \begin{bmatrix} A & B \\ C & D \end{bmatrix}.$$

Now suppose, to the contrary that there is some vector  $s$ , such that  $\|As\|_2 > \sqrt{6} \|s\|_2$  and consider the block vector  $s' := (s, 0)^T \in \mathbb{C}^6$ . We have

$$\|Hs'\|_2 = \|(As, Cs)^T\|_2 \geq \|(As, 0)^T\|_2 = \|As\|_2 > \sqrt{6} \|s\|_2 = \sqrt{6} \|s'\|_2 = \|Hs'\|_2,$$

where in the last step we used that the matrix  $H/\sqrt{6}$  is unitary.  $\square$

**Corollary 2.3.19.** *Suppose that the submatrix  $E$  can be embedded into a complex Hadamard matrix of order 6. Then every eigenvalue  $\lambda$  of the matrix  $E^*E$  satisfies  $\lambda \leq 6$ .*

Corollary 2.3.19 is a useful criterion to show that a given matrix  $E$  cannot be embedded into a complex Hadamard matrix, however, it is unclear how to utilize it for our purposes. In particular, we do not know how to characterize those  $3 \times 3$  matrices which satisfy its conditions. Also it is natural to ask whether the presence of a large eigenvalue is the only obstruction forbidding the submatrix  $E$  to be embedded. The answer to this question might depend on the dimension, as it is easily seen that while every  $2 \times 2$  matrix can be embedded into a complex Hadamard matrix of order 4, only a handful of very special  $2 \times 2$  matrices can be embedded into a complex Hadamard matrix of order 5 due to the finiteness result of Haagerup [60]; compare Example 1.2.1 with Theorem 2.1.6.

A related, yet seemingly weaker restriction is offered by Lindsey's

**Lemma 2.3.20** (Lindsey, [48]). *Suppose that an  $s \times t$  matrix  $A$  appears as a submatrix within an  $n \times n$  complex Hadamard matrix  $H$ . Then*

$$\left| \sum_{i=1}^s \sum_{j=1}^t A_{ij} \right| \leq \sqrt{stn}.$$

*Proof.* We can suppose, up to equivalence, that  $A$  is in the first  $s$  rows and first  $t$  columns of  $H$ . Let us denote by  $u$  and  $v$  the vectors  $(1^s, 0^{n-s})$  and  $(1^t, 0^{n-t})^T$ , respectively. Then we find, after an application of the Cauchy–Schwarz inequality, that

$$\left| \sum_{i=1}^s \sum_{j=1}^t A_{ij} \right| = |\langle u, Hv \rangle| \leq \|u\|_2 \|Hv\|_2 \leq \|u\|_2 \|v\|_2 \|H\|_2 = \sqrt{stn},$$

where we have used that the norm of  $H$  reads  $\|H\|_2 = \sqrt{\lambda_{\max}(H^*H)} = \sqrt{\lambda_{\max}(nI_n)}$ , where  $\lambda_{\max}(\cdot)$  denotes the largest eigenvalue.  $\square$

Now we are ready to present a new family of complex Hadamard matrices. The next section gives an overview of the results.

### 2.3.3 The construction: A high-level perspective

Here we describe the generic family  $G_6^{(4)}$  from a high-level perspective. In particular, we outline the main steps only, and do not discuss some degenerate cases which might come up during the construction. We shall investigate the process in details later in Section 2.3.5. The main result of this chapter is the following

**Construction 2.3.21** (The Dilation Algorithm). *Do the following step by step to obtain complex Hadamard matrices of order 6.*

#1: INPUT: the quadruple  $(a, b, c, d)$ , forming the upper left  $3 \times 3$  submatrix  $E(a, b, c, d)$  as in formula (2.17).

#2: Use Haagerup's trick to the first three rows of  $G_6^{(4)}$  (see (2.18)) to obtain a quadratic equation to  $f$ :

$$\mathcal{F}_1 + \mathcal{F}_2 f + \mathcal{F}_3 f^2 = 0, \quad (2.23)$$

where the coefficients  $\mathcal{F}_1$ ,  $\mathcal{F}_2$  and  $\mathcal{F}_3$  depend on the parameters  $a, b, c, d$  and the indeterminate  $e$ , and derive the following linearization formula from it:

$$f^2 = -\frac{\mathcal{F}_1}{\mathcal{F}_3} - \frac{\mathcal{F}_2}{\mathcal{F}_3} f. \quad (2.24)$$

#3: Use Theorem 2.3.2 to obtain another quadratic equation to  $f$ :

$$\mathcal{G}_1 + \mathcal{G}_2 f + \mathcal{G}_3 f^2 = 0, \quad (2.25)$$

where, again, the coefficients  $\mathcal{G}_1$ ,  $\mathcal{G}_2$  and  $\mathcal{G}_3$  depend on the parameters  $a, b, c, d$  and the indeterminate  $e$ . Plug the linearization formula (2.24) into (2.25) and rearrange to obtain the companion value of  $e$ ,  $f = F(e)$ , where

$$F(e) := -\frac{\mathcal{F}_3 \mathcal{G}_1 - \mathcal{F}_1 \mathcal{G}_3}{\mathcal{F}_3 \mathcal{G}_2 - \mathcal{F}_2 \mathcal{G}_3}. \quad (2.26)$$

#4: As  $|f| = 1$  should hold, calculate the sextic polynomial  $\mathcal{P}_{a,b,c,d}(e)$  coming from the equation  $F(e)\overline{F(e)} - 1 = 0$  and solve it for  $e$ .

#5: Amongst the roots of  $\mathcal{P}_{a,b,c,d}(e)$  find all unimodular triplets  $(e, s_1, s_2)$  satisfying  $e + s_1 + s_2 = -1 - a - b$ , calculate the companion values  $f = F(e)$ ,  $s_3 = F(s_1)$  and  $s_4 = F(s_2)$  through formula (2.26) and store all sextuples  $(e, s_1, s_2, f, s_3, s_4)$  in a solution set called  $SOL_B$ .

#6: Repeat Steps #2-#5 to the transposed matrix (i.e. to the first three columns), *mutatis mutandis* to obtain the solution set  $SOL_C$ .

#7: For every pair of sextuples from  $SOL_B$  and  $SOL_C$  construct the submatrices  $B$  and  $C$ , check if the first three rows and columns of  $G_6^{(4)}$  are mutually orthogonal and finally use Lemma 2.3.10 to compute the lower right submatrix  $D$  through formula (2.21).

#8: **OUTPUT:** all unimodular matrices found in Step #7.

Construction 2.3.21 gives the essence of the new family discovered, and in Section 2.3.5 we shall give it a mathematically rigorous, low-level look. Before doing so, we invite the reader to join us to a rapid course in symbolic computation.

### 2.3.4 A primer on Gröbner basis techniques

Solving polynomial systems is of fundamental interest in mathematics. However, unless we are facing with very simple academic problems in two or three variables, we cannot solve these systems by hand in a reasonable time, and therefore in real-life situations we heavily rely on computers. In 1965 Buchberger in his PhD thesis introduced the concept of Gröbner basis, and proposed an algorithm for deciding ideal membership, which is widely used today [20].

Here we give an informal introduction to Gröbner basis and illustrate some of the standard tricks of symbolic computation which shall come handy during the subsequent sections. The interested reader is referred to Lazard's bulletin which we consider as the perfect starting point to the subject [96].

During this thesis we shall encounter polynomial systems  $F = \{f_1, f_2, \dots, f_n\}$  in  $m$  variables  $x_1, x_2, \dots, x_m$  and our goal is to find all common solutions, i.e. all  $m$ -tuples  $y = (y_1, y_2, \dots, y_m)$  for which  $f_1(y) = f_2(y) = \dots = f_n(y) = 0$ . If there are infinitely many solutions, then some of the solution vectors  $y$  shall depend on some free parameters. By computing a Gröbner basis for  $F$  we essentially create a new system  $G = \{g_1, g_2, \dots, g_k\}$  such that the polynomial ideals, generated by  $F$  and  $G$  are the same, yet  $G$  has some further useful properties. The resulting Gröbner basis and its "complexity" greatly depends on the monomial ordering used. We shall simply use the most informative, yet the most computational expensive pure lexicographic ordering. For example, if  $F$  generates a zero dimensional ideal, i.e. the system  $F$  has finitely many solutions only, then a pure lexicographic Gröbner basis  $G$  will be (essentially) a triangular system where  $g_i = g_i(x_1, x_2, \dots, x_i)$ ,  $i = 1, 2, \dots, m$ . As a result, all solutions  $y = (y_1, y_2, \dots, y_m)$  can be extracted by solving the univariate polynomial  $g_1(x_1)$  first, and then iteratively  $g_2(y_1, x_2)$ , etc. up to  $g_m(y_1, y_2, \dots, y_{m-1}, x_m)$ , where  $g_1(y_1) = g_2(y_1, y_2) = \dots = g_m(y_1, y_2, \dots, y_m) = 0$ .

Our primary goal is to construct new examples of complex Hadamard matrices by

means of computer algebra, and hence we are interested in the unimodular solutions of  $F$  only. Unfortunately, due to the lack of the notion of complex conjugation one cannot formalize the unimodular conditions  $|x_i|^2 - 1 = 0$ ,  $i = 1, \dots, m$  as polynomials and include them into  $F$ . This means that in general we need to separate the unimodular solutions from the large number of complex solutions by hand. It is possible to slightly improve on this situation by observing that the conjugate of unimodular numbers is their reciprocal, and hence the conjugate of a multivariate polynomial  $f$  with real coefficients, depending on the unimodular indeterminates  $x_1, x_2, \dots, x_m$  is just the rational function  $h = f(1/x_1, 1/x_2, \dots, 1/x_m)$ , where both the numerator and the denominator of  $h$ , denoted by  $s$  and  $t$ , are polynomials. As we are interested in the common solutions of these systems we can include  $s$  into  $F$ , but should exclude those solutions by hand which would result in  $t = 0$ . One can circumvent this inconvenience by introducing a new, “dummy” variable  $u$ , and include  $ut - 1$  to  $F$  as well. Clearly in this way we could encode that  $t$  is nonvanishing.

In summary, instead of solving  $F = \{f_1, f_2, \dots, f_n\}$  in the variables  $x_1, x_2, \dots, x_m$  we rather consider  $F' = \{f_1, s_1, f_2, s_2, \dots, f_n, s_n, ut_1 t_2 \cdots t_n - 1\}$  in the variables  $u, x_1, x_2, \dots, x_m$ , where  $f_i(1/x_1, 1/x_2, \dots, 1/x_m) = s_i(x_1, x_2, \dots, x_m)/t_i(x_1, x_2, \dots, x_m)$ ,  $i = 1, 2, \dots, n$ . Experiments confirm that the solution set of  $F'$  is considerably smaller than the solution set of  $F$ .

The reader might have some doubts why is it useful to include the conjugate of the polynomials as well into the systems we consider. To illustrate these ideas more transparently, we offer him or her the opportunity to study the following

**Example 2.3.22.** Here we solve the polynomial system  $F_1 = \{f_1\}$ , containing a single polynomial  $f_1 = x + y + y^2$ , where  $x, y \in \mathbb{T}$  by means of Gröbner basis. Of course, as we are dealing with a single polynomial calculating a Gröbner basis results in the trivial system  $G_1 = \{x + y + y^2\}$ , as expected. However, we can improve on this by including the conjugate of  $f_1$  (or rather, the numerator of its conjugate) as well, by considering

$$h_1(x, y) = f_1(1/x, 1/y) = \frac{1}{x} + \frac{1}{y} + \frac{1}{y^2} = \frac{x + xy + y^2}{xy^2} =: \frac{s_1(x, y)}{t_1(x, y)}$$

and the corresponding system  $F_2 = \{f_1, f_2\}$ , where  $f_2 = s_1$ . Calculating a Gröbner basis for  $F_2$  shall result in  $G_2 = \{g_1, g_2\} = \{y + y^2 + y^3, x + y + y^2\}$  which is a triangular system. By considering  $g_1$  we find that  $y_1 = 0, y_2 = \omega, y_3 = \omega^2$ , and then, by considering  $g_2$  we find that  $(x_1, y_1) = (0, 0)$ ,  $(x_2, y_2) = (1, \omega)$  and  $(x_3, y_3) = (1, \omega^2)$ , where  $\omega$  is the complex cubic root of unity. As we would like to avoid the solutions where either of the variables is 0, we include  $f_3 = uxy - 1$  into  $F_2$  (strictly speaking,  $f_3 = ut_1 - 1 = uxy^2 - 1$  should have been included, but it is always a good idea to keep the degree of the polynomials to the absolute minimum, and hence we just ignore



the extra power of  $y$ ) and consider  $F_3 = \{f_1, f_2, f_3\}$  in the variables  $u, x, y \in \mathbb{T}$ . We find that  $G_3 = \{1 + y + y^2, x - 1, 1 + u + y\}$  and by solving this triangular system we find that  $(x_1, y_1, u_1) = (1, \omega, \omega^2)$  and  $(x_2, y_2, u_2) = (1, \omega^2, \omega)$ .

After realizing that considering the conjugate equations as well is certainly a rewarding idea, the reader is ready to advance to the next section where the Dilation Algorithm is discussed in details. During our construction we have used various Gröbner bases techniques [20] similar in spirit to [10], [52] and [58], and performed the required calculations with the aid of MAPLE and *Mathematica*. The reader is advised to use a computer algebra system of his or her choice for bookkeeping purposes.

### 2.3.5 The construction in details

Here we investigate the steps of Construction 2.3.21 in details. During the construction we shall reject all those matrices which turn out to be equivalent to  $S_6^{(0)}$  or belong to the family  $K_6^{(3)}$ .

STEP #1: Choose a quadruple  $(a, b, c, d)$  in compliance with the Canonical Transformation described by Proposition 2.3.17 as the INPUT, and form the submatrix  $E$ . Check if it meets the requirements of Corollary 2.3.19; if so, then proceed, otherwise conclude that it cannot be embedded into a complex Hadamard matrix of order 6. Experimental results show that the four parameters can be chosen independently of each other and lead to a complex Hadamard matrix with positive probability. This means, heuristically, that we indeed get a four-parameter family. Proving such a statement rigorously would require explicit formulas for the matrix entries, which is out of reach due to the appearance of sextic polynomials (see (2.32)).

STEP #2: Consider the equation

$$abcdef(\mathcal{H}(a, b, c, d, e, f) - \mathcal{H}(1/a, 1/b, 1/c, 1/d, 1/e, 1/f)) = 0,$$

and collect the variable  $f$  in order to obtain the polynomial (2.23) whose coefficients read

$$\begin{aligned}\mathcal{F}_1 &= cd(a^2b + ab^2 + bc + b^2c + ad + a^2d)e - cd(a + b + ac + abc + bd + abd)e^2; \\ \mathcal{F}_2 &= -ab(bc + bc^2 + ad + c^2d + ad^2 + cd^2) + (abc + bc^2 + abd + bc^2d + ad^2 + acd^2)e^2 + \\ &\quad (a^2bc - b^2c + bc^2 - ab^2c^2 - a^2d + ab^2d - ac^2d + b^2c^2d + ad^2 - a^2bd^2 + a^2cd^2 - bcd^2)e;\end{aligned}$$

and  $\mathcal{F}_3 = -(abcde)^2\overline{\mathcal{F}_1}$ . To obtain formula (2.24) we need to see that  $\mathcal{F}_3 \neq 0$ . First we show that  $\mathcal{F}_3$ , as a polynomial of  $e$ , is not identically 0. Indeed, suppose otherwise, which means that the following system of equations (where the first two are the coefficients of  $e$  and  $e^2$  in  $\mathcal{F}_1$ , and the last two are the conjugates of the first two, up to

some irrelevant constant factors)

$$\begin{cases} a^2b + ab^2 + bc + b^2c + ad + a^2d & \equiv 0, \\ a + b + ac + abc + bd + abd & \equiv 0, \\ b^2c + ab^2c + a^2d + a^2bd + acd + bcd & \equiv 0, \\ abc + a^2bc + abd + ab^2d + a^2bcd + ab^2cd & \equiv 0, \end{cases} \quad (2.27)$$

are fulfilled. We compute a Gröbner basis and find that the polynomial

$$bcd(1 + c^2)(c - d)(1 + d^2)(c^2 + d^2)(1 + d + d^2) \quad (2.28)$$

is a member of the ideal, generated by (2.27). One can consider each of the factors of (2.28) one by one, and substitute them back into the original equations (2.27) to find that there is either a vanishing sum of order 2 in  $E$  or  $a = b = 1$  and therefore the whole family is a member of  $K_6^{(3)}$ , or we have  $E = F_3$  or  $E = F_3^*$  (the Fourier matrix or its adjoint) but these matrices have  $b = c$  which however is not allowed by the Canonical transformation. Thus we have shown that if  $\mathcal{F}_3 \equiv 0$  then we are dealing with the family  $K_6^{(3)}$  and therefore we do not proceed any further with our algorithm.

It might happen that  $\mathcal{F}_3 \neq 0$  but there is a unimodular  $e$  making it vanish, which cannot be anything else, but

$$e_0 := \frac{a^2b + a^2d + ab^2 + ad + b^2c + bc}{abc + abd + ac + a + bd + b} = \frac{ab(c + ac + d + bd + acd + bcd)}{a^2bd + a^2d + ab^2c + acd + b^2c + bcd}. \quad (2.29)$$

Nevertheless, in one of the pairs  $(e, f)$ ,  $(s_1, s_3)$  and  $(s_2, s_4)$  the first coordinate must be different from  $e_0$  above, otherwise we would have  $e = s_1 = s_2$ , and therefore by Lemma 2.3.13  $e = s_1 = s_2 = -1$ , resulting in some member of the family  $K_6^{(3)}$  by Corollary 2.3.14. We may therefore suppose, up to equivalence, that  $e \neq e_0$  and conclude that  $\mathcal{F}_3 \neq 0$ .

STEP #3: Multiply (2.3) by  $abcdef$  in order to get (2.25) whose coefficients read

$$\begin{aligned} \mathcal{G}_1 &= cd(2ab + a^2b + ab^2 + bc + 2abc + b^2c + ad + a^2d + 2abd)e + 2cd(ab + bc + ad)e^2; \\ \mathcal{G}_2 &= 2abcd(1 + a + b) + (abc + bc^2 + abd + 2acd + 2bcd + 2abcd + bc^2d + ad^2 + acd^2)e^2 \\ &\quad + (2abc + a^2bc + 2ab^2c + bc^2 + 2abc^2 + 2b^2c^2 + 2abd + 2a^2bd + ab^2d \\ &\quad + 2acd + 2a^2cd + 2bcd + 12abcd + 2a^2bcd + 2b^2cd + 2ab^2cd + 2bc^2d \\ &\quad + 2abc^2d + b^2c^2d + ad^2 + 2a^2d^2 + 2abd^2 + 2acd^2 + a^2cd^2 + 2abcd^2)e; \\ \mathcal{G}_3 &= ab(c + ac + 2bc + d + 2ad + bd + 2cd + acd + bcd) + 2ab(c + d + cd)e. \end{aligned}$$

Clearly, one cannot expect to recover a unique  $f$  from  $e$  in general, as formula (2.26) might suggest. Indeed, there are complex Hadamard matrices in which  $s_1 = e$ , but  $s_3 \neq f$ . The reason for this phenomenon is that formulas (2.23) and (2.25) might be linearly dependent. After plugging (2.24) into (2.25) we obtain the expression

$$\mathcal{F}_3\mathcal{G}_1 - \mathcal{F}_1\mathcal{G}_3 + (\mathcal{F}_3\mathcal{G}_2 - \mathcal{F}_2\mathcal{G}_3)f = 0,$$

where we claim that the left hand side is not identically 0. To see this, assume that

$$\mathcal{F}_3\mathcal{G}_1 - \mathcal{F}_1\mathcal{G}_3 \equiv \mathcal{F}_3\mathcal{G}_2 - \mathcal{F}_2\mathcal{G}_3 \equiv 0. \quad (2.30)$$

Then, we consider the equations (2.30) and their conjugate as polynomials of  $e$ , and using computer algebra we eliminate the variable  $a$  from their coefficients to find that

$$b^2c(b-1)(b-c)(bc-d)(1+c+d)(b-d^2)\mathcal{E}(c,d) = 0$$

must hold, if (2.30) holds. Therefore we have either  $c+d = -1$  or one of the degenerate cases described in the Canonical transformation. The case  $c+d = -1$  implies that the set  $\{c,d\}$  consists of nontrivial cubic roots only. By directly solving the corresponding equations, we find that the quadruples  $(1,1,\omega,\omega^2)$ ,  $(\omega^2,\omega,\omega,\omega^2)$  and  $(1,1,\omega^2,\omega)$ ,  $(\omega,\omega^2,\omega^2,\omega)$  can make both polynomials vanish, but these cases were excluded by the Canonical transformation.

We have thus shown that  $\mathcal{F}_3\mathcal{G}_1 - \mathcal{F}_1\mathcal{G}_3$  and  $\mathcal{F}_3\mathcal{G}_2 - \mathcal{F}_2\mathcal{G}_3$  are not identically zero at the same time. It is, however, possible that

$$\mathcal{F}_3\mathcal{G}_1 - \mathcal{F}_1\mathcal{G}_3 = \mathcal{F}_3\mathcal{G}_2 - \mathcal{F}_2\mathcal{G}_3 = 0 \quad (2.31)$$

for some numbers  $|e_1| = 1$ ,  $e_1 \neq e_0$ , meaning that we do not have another condition on  $f$  and therefore formula (2.26) does not hold. However, having these numbers  $e_1$  at our disposal we can check if they meet (2.4) and then we can recover the two possible values of  $f$  from (2.24). Note that condition (2.31) together with our assumption that  $\mathcal{F}_3 \neq 0$  imply that (2.25) holds as well. We check if the numbers  $f$  are unimodular and once we have the candidate pairs  $(e_1, f_1)$  and  $(e_1, f_2)$  for a given  $e_1$ , we readily calculate the remaining pairs  $(s_1, s_3)$  and  $(s_2, s_4)$  through the Decomposition formula. We disregard those cases in which  $s_1 + s_2 = 0$  or  $s_3 + s_4 = 0$  hold as they would lead to matrices belonging to  $K_6^{(3)}$ , and store all the remaining sextuples  $(e, s_1, s_2, f, s_3, s_4)$  in the solution set  $SOL_B$ .

Next we suppose that  $e \neq e_1$ ,  $e \neq e_0$ , derive formula (2.26) for  $F(e)$  and proceed to Step #4.

STEP #4: Now we need to ensure that  $f$  is of modulus one. To do this, we calculate the fundamental polynomial

$$\mathcal{P}_{a,b,c,d}(e) \equiv a^4b^4c^3d^3e^3 (|\mathcal{F}_3\mathcal{G}_1 - \mathcal{F}_1\mathcal{G}_3|^2 - |\mathcal{F}_3\mathcal{G}_2 - \mathcal{F}_2\mathcal{G}_3|^2). \quad (2.32)$$

After some calculations, it will be apparent that  $\mathcal{P}$  has the following remarkable structure:

$$\mathcal{P} \equiv a^8b^8c^6d^6\bar{P} + 2a^8b^8c^6d^6\bar{P}(1+\bar{a}+\bar{b})e + a^8b^8c^6d^6\bar{Q}e^2 + Re^3 + Qe^4 + 2P(1+a+b)e^5 + Pe^6$$

where the coefficients  $P, Q$  and  $R$  depend on the quadruple  $(a, b, c, d)$  only. If  $\mathcal{P} \equiv 0$  then the construction fails. Otherwise we find all unimodular roots of  $\mathcal{P}(e)$  satisfying  $e \neq e_0$  and  $e \neq e_1$ . Note that the unimodular numbers  $e_1$  (defined after (2.31)) are roots automatically. We shall discuss the issue of unimodularity later in Theorem 2.3.30.

STEP #5: If the number  $e_0$  defined in (2.29) is not of modulus one, then the rôle of the pairs  $(e, f)$ ,  $(s_1, s_3)$  and  $(s_2, s_4)$  is symmetric, and from all of the roots of  $\mathcal{P}$  of modulus one (which are different from the numbers  $e_1$ ) we select all possible triplets  $(e, s_1, s_2)$  satisfying  $e + s_1 + s_2 = -1 - a - b$ , which is needed to ensure orthogonality of the first two rows. Note that this fulfills the second requirement (2.4) of Theorem 2.3.2. From (2.26) we compute the unique companion values  $f = F(e)$ ,  $s_3 = F(s_1)$  and  $s_4 = F(s_2)$ .

Otherwise, should the number on the right hand side of (2.29) be of modulus one, then for every root  $e$  ( $\neq e_0, e_1$ ) of  $\mathcal{P}$  we check if condition (2.4) holds, calculate the unique companion value  $f = F(e)$ , and finally we use the Decomposition formula to determine the pairs  $(s_1, s_3)$  and  $(s_2, s_4)$ . Again, we disregard the cases when  $s_1 + s_2 = 0$  or  $s_3 + s_4 = 0$ .

At the end of this step we add all obtained sextuples  $(e, s_1, s_2, f, s_3, s_4)$  to the solution set  $SOL_B$ . Typically two distinct sextuples are found.

STEP #6: In this step one constructs the first three columns along the lines of Steps #2-#5 described above and obtain the set  $SOL_C$  in a similar way.

STEP #7: For every solution from  $SOL_B$  and  $SOL_C$  we build up the candidate matrices  $B$  and  $C$  and disregard those cases in which the block  $B$  is singular. Note that as we have fulfilled both requirements of Theorem 2.3.2 the first three rows and columns of  $G_6^{(4)}$  are orthogonal. Therefore we can use Lemma 2.3.10 to obtain the missing lower right submatrix  $D$  and check if it is composed of unimodular entries. Recall that by Proposition 2.3.15 we have disregarded members of the family  $K_6^{(3)}$  only.

STEP #8: Finally, we OUTPUT all unimodular matrices found during the process. We remark here that by Corollary 2.3.12 if no unimodular matrices were found then the submatrix  $E$  cannot be embedded into any complex Hadamard matrix of order 6 which is different from  $S_6^{(0)}$  and lies outside the degenerate family  $K_6^{(3)}$ . If unimodular matrices are found, then typically we find two matrices, as the solution set  $SOL_B$  and  $SOL_C$  contains two suitable sextuples each, however, experimental results show that for each sextuple in  $SOL_B$  there is a unique one in  $SOL_C$  making  $D$  unimodular as required.

We have finished the discussion of Construction 2.3.21. The results are summarized in the following

**Theorem 2.3.23** (see [131]). *Start from a submatrix  $E$  as in (2.17) and suppose that there are only finitely many invertible candidate submatrices  $B$  and  $C$  such that the first three rows and columns of the matrix  $G_6$  (see (2.18)) are orthogonal. Then all*

complex Hadamard matrices containing  $E$  as a submatrix, which are inequivalent from  $S_6^{(0)}$  and do not belong to the family  $K_6^{(3)}$ , can be obtained, up to equivalence, through Construction 2.3.21.

The interested reader might want to see an example of generic Hadamard matrices which can be described by closed analytic formulae, that is for which the fundamental polynomials  $\mathcal{P}_{a,b,c,d}$  and  $\mathcal{P}_{a,c,b,d}$  are both solvable. We sketch how to obtain such a matrix in the following

**Example 2.3.24.** Let  $a$  be a unimodular complex number such that its real part is the unique real solution of  $4\Re[a]^3 - 2\Re[a] + 1 = 0$ , and its imaginary part is positive. Further set  $c = (-a^3 + a^2 + a + 1)/(a^4 + a^3 + a^2 - a)$  and consider the input submatrix  $E(a, \bar{a}, c, a)$ . These initial settings imply that one of the roots of  $\mathcal{P}_{a,\bar{a},c,a}$  will be  $a$  and then two additional one can be obtained through the Decomposition formula, while the remaining cubic polynomial can be solved by radicals. From this, and from the delicate structure of this specially tailored matrix it follows that  $F(a) = \bar{a}$  (see (2.26)) will be a root of  $\mathcal{P}_{a,c,\bar{a},a}$  and, again, two additional roots can be found easily. Clearly, the complex Hadamard matrices we obtain are inequivalent from  $S_6^{(0)}$  and do not belong to the family  $K_6^{(3)}$ . This latter fact can be checked through Part (c) of Theorem 2.2.16. We spare the reader the details.

**Problem 2.3.25.** Find a textbook example of generic complex Hadamard matrices, i.e. one with as “simple” entries as just possible.

Now we briefly discuss the results.

*Remark 2.3.26.* One might simplify some of the lengthy case by case analyses of Steps #2-#3 of the construction above by including the equation

$$uabcd(a+1)(b+1)(c+1)(d+1)(a+b)(a+c)(b+d)(c+d) - 1 = 0,$$

featuring a “dummy” variable  $u$  into the system of equations (2.27) and (2.30), respectively. This would ensure that  $abcd \neq 0$  and a vanishing sum of order 2 does not appear in the submatrix  $E$  (cf. Example 2.3.22). The presence of this extra variable, however, significantly increases the complexity of the problems and consequently prolongs the time and memory consumption of the required calculations.  $\square$

*Remark 2.3.27.* When  $\mathcal{P} \equiv 0$  then the main difficulty we are facing is that we have infinitely many candidate submatrices  $B$ . In this case we have the trivial restriction (2.4) on  $e$ , while the companion value  $f$  coming from (2.26) is unimodular unconditionally. Although in principle we can find three orthogonal rows through the Decomposition formula for every suitable  $e$ , we do not know which one to favor in order to obtain a

unimodular submatrix  $D$  via formula (2.21). Also, it might happen that the polynomial  $\mathcal{P}_{a,c,b,d}$ , coming from considering the first three columns of  $G_6^{(4)}$  during Step #6, shall vanish as well, bringing another free parameter into the game and making things even more complicated. In contrast, if both  $\mathcal{P}_{a,b,c,d} \neq 0$  and  $\mathcal{P}_{a,c,b,d} \neq 0$ , then we have finitely many choices for the submatrices  $B$  and  $C$  and we can use Corollary 2.3.12 to conclude the construction.  $\square$

*Remark 2.3.28.* The polynomial  $\mathcal{P}$  formally can vanish when we have  $\mathcal{F}_3\mathcal{G}_1 - \mathcal{F}_1\mathcal{G}_3 \equiv \mathcal{F}_3\mathcal{G}_2 - \mathcal{F}_2\mathcal{G}_3 \equiv 0$ , however this is excluded by the Canonical Transformation and is explained in details in Step #3. It might vanish for some other, non-trivial quadruples as well making the whole construction process fail. In theory, the common roots of the coefficients of  $\mathcal{P}$  can be calculated by means of Gröbner bases, but as these coefficients are rather complicated obtaining such a basis turned out to be a task beyond our capabilities. Nevertheless, we conjecture that the case  $\mathcal{P} \equiv 0$  can be excluded completely in a similar fashion as we disregarded various quadruples during the Canonical Transformation. This would mean that all complex Hadamard matrices of order 6, except for  $S_6^{(0)}$  and  $K_6^{(3)}$ , can be recovered from Construction 2.3.21.  $\square$

So far we have completely avoided the issue of unimodularity. It turns out that there are tools available guaranteeing that all six roots of the fundamental polynomial are unimodular. We recall the following

**Definition 2.3.29.** A complex polynomial  $f(x) = a_0 + a_1x + \dots + a_mx^m$  of degree  $m$  is called *self-inversive* if  $a_{m-k} = \varepsilon \bar{a}_k$  for every  $k = 0, \dots, m$ , where  $|\varepsilon| = 1$ .

We observe that the polynomial  $\mathcal{P}_{a,b,c,d}(e)/(a^4b^4c^3d^3)$  is self-inversive (with  $\varepsilon = 1$ ). In particular, its middle coefficient  $R/(a^4b^4c^3d^3)$  is real. A classical theorem of Cohn [26] gives a characterization of polynomials having exclusively unimodular roots (see also [90] for an elegant sufficient condition).

**Theorem 2.3.30** (Cohn, [26]). *All roots of the polynomial  $f(x) = a_0 + a_1x + \dots + a_mx^m$  of degree  $m$  are unimodular if and only if*

- (a)  *$f$  is self-inversive; and*
- (b) *all roots  $r$  of the derivative  $f'$  satisfy  $|r| \leq 1$ .*

Therefore self-inversive polynomials are the relevant objects to study. Cohn's theorem is powerful enough to guarantee that the fundamental polynomials  $\mathcal{P}$  has exclusively unimodular roots around a small neighborhood of a fixed quadruple  $(a, b, c, d)$ . In particular, from Example 2.3.24 we have the following

**Corollary 2.3.31.** *There is a four-parameter family of unitary matrices of order 6, such that the first three rows and columns of the matrices are unimodular.*

Yet, it is unclear how to ensure the unimodularity of the lower right submatrix  $D$  of the matrix  $G_6^{(4)}$  automatically, i.e. without checking it by hand in a particular example.

*Remark 2.3.32.* We outline an alternate way to obtain the lower right submatrix  $D$ , instead of using formula (2.21). Once the first three rows and columns of the matrix  $G_6^{(4)}$  has been obtained, we have several new  $3 \times 3$  submatrices, from which the Dilation algorithm can be “restarted” again in order to obtain some of the missing entries of  $G_6^{(4)}$ . The advantage of this method is that by Cohn’s theorem the unimodularity of the entries can be guaranteed, the pitfall is that by this method we cannot control the mutual orthogonality of more than three rows at the same time.  $\square$

It is reasonable to think that every complex Hadamard matrix of order 6 has some  $3 \times 3$  submatrix  $E$  leading to nonvanishing fundamental polynomials. In particular, we do not expect any complex Hadamard matrices of order 6 (except maybe  $S_6^{(0)}$  and  $K_6^{(3)}$ ) which cannot be recovered from Construction 2.3.21. Therefore we formulate the following

**Conjecture 2.3.33.** *The list of complex Hadamard matrices of order 6 is as follows: the isolated matrix  $S_6^{(0)}$ , the three-parameter degenerate family  $K_6^{(3)}$  and the four-parameter generic family  $G_6^{(4)}$  as described above.*

It would be nice to understand the structure of  $G_6^{(4)}$  more thoroughly and express the entries of these matrices by some well-chosen trigonometric functions in a similar fashion as  $K_6^{(3)}$  is described, however, as we have encountered rather delicate sextic polynomials already the appearance of compact and elegant formulas is somewhat unexpected. Also, it is natural to ask which matrices satisfy the conditions of Corollary 2.3.19. An algebraic characterization of these matrices might lead to a deeper understanding of the generic family  $G_6^{(4)}$  and hopefully to the desired full classification of complex Hadamard matrices of order 6.

**Problem 2.3.34.** Classify all embeddable matrices  $E$ .

The results presented here might be further improved in the future, when faster computation of Gröbner basis shall be available; either by utilizing a large-scale computing cluster to handle the equations, or by using improved algorithms.

**Problem 2.3.35.** Characterize the cases when the fundamental polynomial  $\mathcal{P}_{a,b,c,d}(e)$  (2.32) vanishes (e.g. by means of computing a Gröbner basis with respect to the pure lexicographic monomial order).

**Problem 2.3.36.** Give a full characterization of  $6 \times 6$  complex Hadamard matrices.

## 2.4 MUBs, MASAs and complex Hadamard matrices

In this section we give some applications of complex Hadamard matrices.

### 2.4.1 Connections to operator algebras

The following is a fundamental concept in the theory of operator algebras, see e.g. [6], [60] and [114].

**Definition 2.4.1.** We say that an algebra  $\mathcal{A} \subset \mathcal{M}_n(\mathbb{C})$  is a *maximal abelian \*-subalgebra* (or MASA) if it is commutative, closed under the adjoint operation and maximal with respect to the inclusion.

**Example 2.4.2.** For every  $n$  the algebra of diagonal matrices  $\mathcal{D}_n$  is a MASA in  $\mathcal{M}_n(\mathbb{C})$ .

In fact, it is easy to see that essentially this is the only example.

**Lemma 2.4.3.** *Let  $\mathcal{A}$  be a MASA in  $\mathcal{M}_n(\mathbb{C})$ . Then there exists a unitary matrix  $U$  such that  $U^* \mathcal{A} U = \mathcal{D}_n$ .*

*Proof.* All elements of  $\mathcal{A}$  are pairwise commuting normal operators and hence they can be simultaneously diagonalized.  $\square$

**Definition 2.4.4.** The MASAs  $\mathcal{A}$  and  $\mathcal{B}$  are called *orthogonal* if the orthogonal complements  $\mathcal{A} \ominus \mathbb{C}I$  and  $\mathcal{B} \ominus \mathbb{C}I$  are orthogonal with respect to the Hilbert–Schmidt inner product in  $\mathcal{M}_n(\mathbb{C})$ .

We denote the Hilbert–Schmidt inner product of the matrices  $A, B \in \mathcal{M}_n(\mathbb{C})$  by  $\langle A, B \rangle_{\text{HS}} = \text{Tr}(A^* B)$ . The following question arises naturally

**Problem 2.4.5.** Decide the largest number of pairwise orthogonal MASAs in  $\mathcal{M}_n(\mathbb{C})$ .

We recall the following upper bound as follows.

**Lemma 2.4.6.** *There are at most  $n + 1$  pairwise orthogonal MASAs in  $\mathcal{M}_n(\mathbb{C})$ .*

*Proof.* Let  $\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_m$  be pairwise orthogonal MASAs in  $\mathcal{M}_n(\mathbb{C})$ . Each of the subspaces  $\mathcal{A}_i \ominus \mathbb{C}I$  are of dimension  $n - 1$ , and hence, by orthogonality,  $m(n - 1) + 1 \leq n^2$  from which the result follows.  $\square$

We have the following characterization of orthogonal MASAs.

**Lemma 2.4.7.** *Suppose that  $\mathcal{D}_n$  and  $U^* \mathcal{D}_n U$  is a pair of orthogonal MASAs in  $\mathcal{M}_n(\mathbb{C})$ . Then  $\sqrt{n}U$  is a complex Hadamard matrix.*



*Proof.* Let us fix some  $1 \leq i, j \leq n$  and consider the matrices  $D_j \in \mathcal{D}_n$  and  $U^* D_i U \in U^* \mathcal{D}_n U$ , where  $D_i$  is the diagonal matrix with its  $(i, i)$ th entry being 1 and all other entries being 0. Then, by orthogonality, we have

$$\left\langle D_j - \frac{1}{n}I, U^* D_i U - \frac{1}{n}I \right\rangle_{\text{HS}} = \text{Tr} \left[ \left( D_j - \frac{1}{n}I \right)^* \left( U^* D_i U - \frac{1}{n}I \right) \right] = 0,$$

from which  $\text{Tr}(D_j U^* D_i U) = |U_{i,j}|^2 = 1/n$  follows.  $\square$

**Corollary 2.4.8.** *Let  $\mathcal{D}_n, \frac{1}{n}H_2^* \mathcal{D}_n H_2, \dots, \frac{1}{n}H_m^* \mathcal{D}_n H_m$  be a collection of  $m$  pairwise orthogonal MASAs in  $\mathcal{M}_n(\mathbb{C})$ . Then  $H_i$ , as well as  $\frac{1}{\sqrt{n}}H_i H_j^*$  are complex Hadamard matrices for every  $2 \leq i < j \leq m$ .*

**Example 2.4.9.** Let  $n = 2$  and consider in  $\mathcal{M}_2(\mathbb{C})$  the following MASAs:

$$\mathcal{D}_2 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\}, \quad \mathcal{C}_2 = U^* \mathcal{D}_2 U = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}, \quad \text{and} \\ \mathcal{B}_2 = V^* \mathcal{D}_2 V = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & \mathbf{i} \\ -\mathbf{i} & 0 \end{bmatrix} \right\}, \quad U = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad V = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & \mathbf{i} \\ 1 & -\mathbf{i} \end{bmatrix}.$$

Here  $\mathcal{D}_2$  and  $\mathcal{C}_2$  are the algebra of the diagonal and circulant matrices, respectively and  $U$  is the matrix describing the usual discrete Fourier transform.

Finally, we mention the following neat result highlighting a gap in the maximum number of pairwise orthogonal MASAs.

**Theorem 2.4.10** (Weiner, [145]). *The maximal number of pairwise orthogonal MASAs in  $\mathcal{M}_n(\mathbb{C})$  is either  $n + 1$  or at most  $n - 1$ .*

In other words, if  $n$  pairwise orthogonal MASAs are constructed in  $\mathcal{M}_n(\mathbb{C})$ , an additional one can be obtained as well. We shall use these results coming from operator theory in the subsequent sections.

### 2.4.2 The problem of Mutually Unbiased Bases in $\mathbb{C}^n$

We begin with recalling the following concept arising in quantum information theory naturally.

**Definition 2.4.11.** Two orthonormal bases of  $\mathbb{C}^n$ ,  $\mathcal{B}_1$  and  $\mathcal{B}_2$  are called *mutually unbiased* if for every  $e \in \mathcal{B}_1$  and  $f \in \mathcal{B}_2$  we have  $|\langle e, f \rangle| = 1/\sqrt{n}$ . A collection of orthonormal bases  $\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_m$  are called (pairwise) mutually unbiased if every two of them are mutually unbiased.

We refer to mutually unbiased bases as MUBs, and identify them with unitary matrices  $B_1, B_2, \dots, B_m$  of order  $n$ , whose row vectors amount to the basis vectors. It is immediate that if we fix  $B_1 = I$ , which we can do without loss of generality, then all further matrices  $B_i$ ,  $i = 2, \dots, m$  are complex Hadamard, up to a scaling factor of  $1/\sqrt{n}$ . Thus understanding MUBs requires understanding complex Hadamard matrices. Conversely, any construction of MUBs gives a construction of complex Hadamard matrices. The standard reference to the subject is [47].

Observe that MUBs has the following remarkable property (cf. Corollary 2.4.8).

**Lemma 2.4.12.** *Let  $\{I, \frac{1}{\sqrt{n}}H_2, \dots, \frac{1}{\sqrt{n}}H_m\}$  be a collection of  $m$  MUBs in  $\mathbb{C}^n$ . Then  $H_i$ , as well as  $\frac{1}{\sqrt{n}}H_iH_j^*$  are complex Hadamard matrices for every  $2 \leq i < j \leq m$ .*

Therefore MASAs and MUBs are exactly the same concept, coming from different areas of mathematics.

**Example 2.4.13.** Let  $n = 2$ , and consider the following unitary matrices:

$$B_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, B_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, B_3 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & \mathbf{i} \\ 1 & -\mathbf{i} \end{bmatrix}.$$

It is easy to see that  $\{B_1, B_2, B_3\}$  form a triplet of MUBs in  $\mathbb{C}^2$ . In particular, the product matrix

$$\sqrt{2}B_2B_3^* = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 - \mathbf{i} & 1 + \mathbf{i} \\ 1 + \mathbf{i} & 1 - \mathbf{i} \end{bmatrix}$$

is a complex Hadamard matrix.

The following question arises naturally.

**Problem 2.4.14.** Decide the maximal number of MUBs in  $\mathbb{C}^n$ .

In what follows we collect some well-known facts on MUBs. The first result easily comes from Lemma 2.4.6.

**Corollary 2.4.15.** *There are at most  $n + 1$  MUBs in  $\mathbb{C}^n$  and at most  $n/2 + 1$  real MUBs in  $\mathbb{R}^n$ , respectively.*

**Theorem 2.4.16** (see e.g. [70], [148]). *For every prime power  $p^k$  there is a complete set of MUBs consisting of  $p^k + 1$  bases in  $\mathbb{C}^{p^k}$ .*

For a discussion of the equivalence of various MUB constructions see [55] and [73].

The non prime power case remains elusive, nevertheless it is easy to obtain a lower bound on the number of MUBs here as follows.

**Lemma 2.4.17.** *Let us suppose that there is  $k_1$  and  $k_2$  MUBs in  $\mathbb{C}^{n_1}$  and  $\mathbb{C}^{n_2}$ , respectively. Then there is at least  $\min\{k_1, k_2\}$  MUBs in  $\mathbb{C}^{n_1n_2}$ .*

*Proof.* Let  $m := \min\{k_1, k_2\}$  and consider  $m$  MUBs in  $\mathbb{C}^{n_1}$ :  $\{I_{n_1}, \frac{1}{\sqrt{n_1}}H_2, \dots, \frac{1}{\sqrt{n_1}}H_m\}$ ; and similarly,  $m$  MUBs in  $\mathbb{C}^{n_2}$ :  $\{I_{n_2}, \frac{1}{\sqrt{n_2}}K_2, \dots, \frac{1}{\sqrt{n_2}}K_m\}$ . Then the following set  $\{I_{n_1} \otimes I_{n_2}, \frac{1}{\sqrt{n_1 n_2}}H_2 \otimes K_2, \dots, \frac{1}{\sqrt{n_1 n_2}}H_m \otimes K_m\}$  is a collection of  $m$  MUBs in  $\mathbb{C}^{n_1 n_2}$ .  $\square$

As the smallest prime-power factor of a composite number is at least 2, it follows that

**Corollary 2.4.18.** *For every  $n > 1$  there is a triplet of MUBs in  $\mathbb{C}^n$ .*

Currently this is the best known general lower bound.

Finally, we mention here the following result connecting MUBs to latin squares.

**Theorem 2.4.19** (Wocjan–Beth, [147]). *For square orders  $n = s^2$  there are at least  $N(s) + 2$  MUBs, where  $N(s)$  is the number of mutually orthogonal latin squares of order  $s$ .*

Theorem 2.4.19 results in 6 MUBs in dimension  $n = 26^2$  whereas from Lemma 2.4.17 only 5 MUBs can be obtained.

In what follows we briefly mention an elegant construction of Zauner, yielding infinite families of triplets of MUBs, coming from bicirculant complex Hadamard matrices.

**Theorem 2.4.20** (Zauner’s construction, [149]). *If  $T$  is a complex Hadamard matrix of order  $2m$  with  $m \times m$  circulant blocks, then there exist complex Hadamard matrices  $Z_1$  and  $Z_2$  of order  $2m$  such that  $T = \frac{1}{\sqrt{2m}}Z_1Z_2^*$ . In particular,  $\{I_{2m}, \frac{1}{\sqrt{2m}}Z_1, \frac{1}{\sqrt{2m}}Z_2\}$  forms a triplet of MUBs in  $\mathbb{C}^{2m}$ .*

Zauner’s construction is based on the following remarkable representation of  $2 \times 2$  unitary matrices, as well on a clever use of the Fourier matrices which are well-known to diagonalize circulant matrices. The details can be found in [149] (or in [71] in English).

**Lemma 2.4.21** (Zauner, [149]). *Suppose that  $M$  is a  $2 \times 2$  unitary matrix. Then there are complex unimodular numbers  $u, v, x$  and  $y$ , such that*

$$M = \frac{1}{2} \begin{bmatrix} u+v & y(u-v) \\ (u-v)/x & y(u+v)/x \end{bmatrix}.$$

Zauner applied his result to the following one-parameter family of bicirculant matrices which is equivalent to the family  $D_6^{(1)}(c)$  (cf. Example 2.2.2):

$$\left[ \begin{array}{ccc|ccc} 1 & i\bar{c} & ic & 1 & \bar{c} & -c \\ ic & 1 & i\bar{c} & -c & 1 & \bar{c} \\ i\bar{c} & ic & 1 & \bar{c} & -c & 1 \\ \hline 1 & -\bar{c} & c & -1 & i\bar{c} & ic \\ c & 1 & -\bar{c} & ic & -1 & i\bar{c} \\ -\bar{c} & c & 1 & i\bar{c} & ic & -1 \end{array} \right],$$

and exhibited an infinite family of MUB triplets in  $\mathbb{C}^6$ . We can improve on this result with our two-parameter bicirculant family  $X_6^{(2)}(\alpha)$  as follows.

**Corollary 2.4.22** (see [129]). *There is a two-parameter family of triplet of MUBs in  $\mathbb{C}^6$ , emerging from the family  $X_6^{(2)}(\alpha)$  (see Example 2.2.13) via Zauner's construction.*

*Remark 2.4.23.* One might wonder if further interesting results can be obtained from the consideration of four-circulant complex Hadamard matrices. The four-circulant property requires that  $n = 4m$ , however in such orders one can construct quartets of MUBs via Lemma 2.4.17 easily, and it seems that investigating and controlling the properties of such a quartet requires a rather delicate analysis.  $\square$

Nevertheless, we pose this as a

**Problem 2.4.24.** Investigate a possible “four-circulant” construction of quartet of MUBs in orders  $n = 4m$  which resembles to Zauner's construction (Theorem 2.4.20).

For additional results on MUBs consult [57].

Several authors considered the question of the existence of real MUBs. Clearly they can exist only in orders  $4m$ , moreover a triplet of real MUBs can be found only in square orders, as regular Hadamard matrices are required. Despite these strong restrictions the following result demonstrates that the general upper bound given by Corollary 2.4.15 can be met.

**Theorem 2.4.25** (Cameron–Seidel, [22]). *For each  $n = 2^{2i}$  with  $i$  any positive integer, there are  $n/2 + 1$  real MUBs in  $\mathbb{R}^n$ .*

For further reading on real MUBs we refer the reader to [66], [97].

### 2.4.3 Towards the solution of the MUB-6 problem

As we have mentioned earlier in the non prime power case the maximal number of MUBs is unknown. Even the simplest case  $n = 6$  is undecided, and we have the following long-standing

**Conjecture 2.4.26** (Zauner, [149]). *There are no more than three MUBs in  $\mathbb{C}^6$ .*

Extensive numerical searches confirm the truth of this conjecture, see e.g. [15], [16] and [116], as well as a systematic search for quartet of MUBs, coming from Butson-type complex Hadamard matrices [8]. However, none of these methods are conclusive.

One possible approach to the solution of the MUB problem in dimension  $d = 6$  has been proposed in our recent paper [71]. The main idea is a combination of a discretization and a computer-aided attack which we illustrate here as follows. We start

with the hypothesis that there are four unitary matrices in  $\mathbb{C}^6$  forming a set of MUBs  $\{I, \frac{1}{\sqrt{6}}H_2, \frac{1}{\sqrt{6}}H_3, \frac{1}{\sqrt{6}}H_4\}$  and try to reach a contradiction. Clearly, if such a set of four MUBs exist, then there is a collection of “approximate MUBs”  $\{I, \frac{1}{\sqrt{6}}H'_2, \frac{1}{\sqrt{6}}H'_3, \frac{1}{\sqrt{6}}H'_4\}$  as well, where the matrices  $H'_i$ ,  $2 \leq i \leq 4$  come from a finite set (very roughly speaking they are composed of some  $p$ th roots of unity for some large  $p$ ) and they satisfy the unitary and unbiasedness conditions up to some controllable error. If we find that no such set containing four “approximate MUBs” exists then we conclude that there is no four MUBs either. This is the core argument of the paper. This idea turned out to be powerful enough to deal with the generalized Fourier family  $F_6^{(2)}(a, b)$ . In particular, the following has been shown by means of an exhaustive computer search:

**Theorem 2.4.27** (see [71]). *None of the pairs  $\{I, \frac{1}{\sqrt{6}}F_6^{(2)}(a, b)\}$  can be extended to a MUB-quartet  $\{I, \frac{1}{\sqrt{6}}F_6^{(2)}(a, b), \frac{1}{\sqrt{6}}H_3, \frac{1}{\sqrt{6}}H_4\}$ .*

However, this approach is currently infeasible for the general problem due to the large number of possible candidate matrices  $\frac{1}{\sqrt{6}}H'_2$ . One realistic way to overcome this difficulty is to gain some insight into the structure of the MUB pairs  $\{I, \frac{1}{\sqrt{6}}H_2\}$ , or equivalently, to understand complex Hadamard matrices of order 6. In particular, a complete characterization of complex Hadamard matrices of order 6 would hopefully reduce the number of candidate matrices considerably. Based on the full characterization of complex Hadamard matrices of orders up to 5 a complete characterization of MUBs in  $\mathbb{C}^d$  has been obtained for  $d \leq 5$  very recently [17].

#### 2.4.4 MUBs and equiangular lines in $\mathbb{C}^n$

The purpose of this brief section is to relate MUBs and hence complex Hadamard matrices to equiangular sets of lines. A construction is given yielding large set of equiangular lines in real spaces, slightly improving on a recent construction of de Caen [39].

**Definition 2.4.28.** A set of lines in  $\mathbb{C}^n$ , spanned by the unit vectors  $v_1, v_2, \dots, v_r$  is *equiangular* if there exists a constant  $c$  such that  $|\langle v_i, v_j \rangle| = c$  for every  $1 \leq i < j \leq r$ .

*Remark 2.4.29.* The term “equiangular vectors” usually refers to a configuration in which the condition  $|\langle v_i, v_j \rangle| = c$  in Definition 2.4.28 is replaced by the stronger one  $\langle v_i, v_j \rangle = c$ .  $\square$

It is easy to obtain upper bound on the number of equiangular lines. The following is well-known.

**Lemma 2.4.30.** *There are at most  $n^2$  equiangular lines in  $\mathbb{C}^n$ , and at most  $n(n+1)/2$  equiangular lines in  $\mathbb{R}^n$ , respectively.*

*Proof (sketch).* If the lines are represented by the unit vectors  $v_1, v_2, \dots, v_m$ , then the self-adjoint (resp. symmetric) rank-1 matrices  $v_1^* v_1, v_2^* v_2, \dots, v_m^* v_m$  shall be linearly independent elements of the real vector space of the self-adjoint (resp. symmetric) matrices of order  $n$ . Therefore  $m$  cannot be larger than the dimension of these vector spaces from which the required bounds follow.  $\square$

The following, however, is a long-standing open

**Problem 2.4.31.** Determine the maximum number of equiangular lines in  $\mathbb{C}^n$  and  $\mathbb{R}^n$ , respectively.

**Example 2.4.32.** The following is a collection of four equiangular lines in  $\mathbb{C}^2$ , along with the corresponding Gram matrix:

$$L = \frac{1}{\sqrt{3}} \begin{bmatrix} \sqrt{3} & 0 \\ 1 & \sqrt{2} \\ 1 & \sqrt{2}\omega \\ 1 & \sqrt{2}\omega^2 \end{bmatrix}, \quad LL^* = \frac{1}{\sqrt{3}} \begin{bmatrix} \sqrt{3} & 1 & 1 & 1 \\ 1 & \sqrt{3} & -\mathbf{i} & \mathbf{i} \\ 1 & \mathbf{i} & \sqrt{3} & -\mathbf{i} \\ 1 & -\mathbf{i} & \mathbf{i} & \sqrt{3} \end{bmatrix}.$$

In this section we are primarily concerned with real equiangular lines. For a handful of small dimensional examples see [141].

**Example 2.4.33.** Six diagonals of the icosahedron form equiangular lines in  $\mathbb{R}^3$  as follows:

$$L = \frac{1}{\sqrt{10}} \begin{bmatrix} 0 & \sqrt{5+\sqrt{5}} & \sqrt{5-\sqrt{5}} \\ 0 & \sqrt{5+\sqrt{5}} & -\sqrt{5-\sqrt{5}} \\ \sqrt{5-\sqrt{5}} & 0 & \sqrt{5+\sqrt{5}} \\ -\sqrt{5-\sqrt{5}} & 0 & \sqrt{5+\sqrt{5}} \\ \sqrt{5+\sqrt{5}} & \sqrt{5-\sqrt{5}} & 0 \\ \sqrt{5+\sqrt{5}} & -\sqrt{5-\sqrt{5}} & 0 \end{bmatrix}.$$

*Remark 2.4.34.* Examples 2.4.32 and 2.4.33 demonstrate that the upper bounds given by Lemma 2.4.30 can be met.

It is easy to construct equiangular lines from Hadamard matrices (cf. Theorem 3.4.11).

**Lemma 2.4.35.** Let  $H$  be a symmetric, real Hadamard matrix with constant diagonal 1 of order  $n^2$ . Then there is an equiangular set of  $n^2$  lines in  $\mathbb{R}^{n(n-1)/2}$ .

*Proof.* The eigenvalues of  $H$  are  $\pm n$  with multiplicity  $n(n \pm 1)/2$ , respectively. Hence  $G := (-H + nI)/(n-1)$  is a positive semidefinite matrix of rank  $n(n-1)/2$ . Therefore  $G$  is the Gram matrix of the desired configuration.  $\square$

The first constructive quadratic lower bound on the number of real equiangular lines was obtained by de Caen, who proved the following

**Theorem 2.4.36** (de Caen, [39]). *For each  $n = 3 \cdot 2^{2t-1} - 1$ , with  $t$  any positive integer, there exists an equiangular set of  $\frac{2}{9}(n+1)^2$  lines in  $\mathbb{R}^n$ .*

It is clear that a collection of equiangular lines in  $\mathbb{R}^n$  can also be thought of as an equiangular configuration in  $\mathbb{R}^{n+1}$ . This observation together with de Caen's result leads easily to the following general quadratic lower bound on the number of real equiangular lines.

**Corollary 2.4.37.** *For every  $n \geq 1$  there exists an equiangular set of  $\frac{1}{72}(n+2)^2$  lines in  $\mathbb{R}^n$ .*

We remark that de Caen constructed the Gram matrix of the system, i.e. he exhibited a positive semidefinite matrix of order  $\frac{2}{9}(n+1)^2$  with rank  $n = 3 \cdot 2^{2t-1} - 1$ . We present here a related result leading to a slight improvement upon Corollary 2.4.37.

**Theorem 2.4.38.** *For each  $n = 3 \cdot 2^{2t-1} + 1$ , with  $t$  any positive integer, there exists an equiangular set of  $\frac{2}{9}(n-1)(n+2)$  lines in  $\mathbb{R}^n$ .*

*Proof.* Let  $t$  be a positive integer, set  $n = 3 \cdot 2^{2t-1} + 1$  and use Theorem 2.4.25 to exhibit a collection of  $2^{2t-1} + 1$  real MUBs in  $\mathbb{R}^{2^{2t}}$ . Now rescale all these vectors with a weight  $A$ , and extend each of them with  $2^{2t-1} + 1$  additional coordinates set to 0 (i.e. embed the vectors into  $\mathbb{R}^n$  in the natural way). Now for every  $i = 1, \dots, 2^{2t-1} + 1$  consider the vectors from the  $i$ th basis, and set their  $i$ th new coordinate to  $B$ . With the choice

$$A = \sqrt{\frac{2^t}{2^t + 1}}, \quad B = \frac{1}{\sqrt{2^t + 1}}$$

we obtain  $2^{2t}(2^{2t-1} + 1) = \frac{2}{9}(n-1)(n+2)$  equiangular lines in  $\mathbb{R}^n$  having a common angle (in absolute value) of  $\arccos(1/(2^t + 1))$ .  $\square$

**Example 2.4.39.** Let  $t = 1$ , set  $n = 7$  and consider the collection of 3 real MUBs in  $\mathbb{R}^4$  as follows:

$$\left\{ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \frac{1}{2} \begin{bmatrix} 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix} \right\}.$$

From these ingredients we build up the array  $L$ , which we display here in transposed

layout for typographical reasons as follows:

$$L^T = \frac{1}{\sqrt{6}} \left[ \begin{array}{cccc|cccc|cccc} 2 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 0 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 0 & 0 & 2 & 0 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 0 & 0 & 0 & 2 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ \hline \sqrt{2} & \sqrt{2} & \sqrt{2} & \sqrt{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \sqrt{2} & \sqrt{2} & \sqrt{2} & \sqrt{2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \sqrt{2} & \sqrt{2} & \sqrt{2} & \sqrt{2} \end{array} \right].$$

The column vectors of  $L^T$  give us the desired configuration of  $\frac{2}{9}(7-1)(7+2) = 12$  equiangular lines in  $\mathbb{R}^7$ .

Contrary to de Caen's approach, we obtained the lines directly, and it is straightforward from their structure how to exhibit large set of equiangular lines in smaller dimensions as well. For example, by simply neglecting the last row and the last four columns of the matrix  $L^T$  above, one immediately gets 8 equiangular lines in  $\mathbb{R}^6$ , etc. A detailed analysis of this idea led to the following improvement upon Corollary 2.4.37.

**Corollary 2.4.40.** *For every  $n \geq 1$  there exists an equiangular set of  $\frac{8}{1089}n(4n+33)$  lines in  $\mathbb{R}^n$ .*

*Proof.* For  $n \leq 25$  we have  $8n(4n+33)/1089 \leq n$ , and hence any orthonormal basis fulfills the claim. Therefore we can suppose that  $n \geq 26$ . Let  $t \geq 2$  be the unique integral number such that that  $d = 3 \cdot 2^{2t-1} + 1 < n \leq 3 \cdot 2^{2t+1} + 1$ . If  $n \leq 4^{t+1} + 2^{2t-3}$ , then use Theorem 2.4.38 to obtain  $2^{2t}(2^{2t-1} + 1)$  equiangular lines in  $\mathbb{R}^d$  and embed them into  $\mathbb{R}^n$  in the natural way. Otherwise, if  $4^{t+1} + 2^{2t-3} + 1 \leq n \leq 3 \cdot 2^{2t+1} + 1$  then use  $m = n - 4^{t+1} \geq 2^{2t-3} + 1$  MUBs of order  $4^{t+1}$ , and construct along the lines of Theorem 2.4.38  $4^{t+1}m \geq 4^{t+1}(2^{2t-3} + 1)$  equiangular lines in  $\mathbb{R}^n$ . One can conclude by fitting a quadratic polynomial to the set of points  $\{(4^{t+1} + 2^{2t-3}, 2^{2t}(2^{2t-1} + 1)) : t \geq 2\} \subset \mathbb{R} \times \mathbb{R}$ , and noting that the number of known equiangular lines in dimension  $n' = 4^{t+1} + 2^{2t-3} + 1$  is larger than the claimed lower bound  $8n'(4n' + 33)/1089$ .  $\square$

Our idea can be reformulated in the complex settings as well, but the results are nowhere near close to the following

**Theorem 2.4.41** (see e.g. [55]). *There is a configuration of  $n^2 - n + 1$  equiangular lines in  $\mathbb{C}^n$  when  $n - 1$  is a prime power.*

We shall revisit complex equiangular lines from a different perspective once again in Section 3.5.



## Chapter 3

# Complex Hadamard matrices of prime orders

Throughout this chapter we investigate the existence of complex Hadamard matrices of prime orders. Constructing infinite families of complex Hadamard matrices of prime orders is currently out of reach, apart from some sporadic examples of relatively small order. There are three major construction methods yielding some examples of complex Hadamard matrices of prime orders: Petrescu's construction leading to infinite families [113]; the general theory of circulant complex Hadamard matrices [10], [11]; and combinatorial constructions coming from design theory [24], [25] and [132]. In what follows we investigate these approaches in details. As a supplement, we extend this list with a fourth method by considering complex Hadamard matrices with circulant core in Appendix C.

In Section 3.2 we give a further look at Petrescu's construction and we utilize his method to obtain a  $BH(19, 6)$ ; in addition to this we exhibit a four-parameter family of complex Hadamard matrices of order 13 thus considerably extending the list of known complex Hadamard matrices of this order. In Section 3.3 we recall circulant complex Hadamard matrices of index  $k$  type and for every prime  $p \equiv 1 \pmod{8}$  we construct two new, previously unknown examples of circulant complex Hadamard matrices of order  $p$ . As a related result we give a full classification of cyclic 17-roots of simple index 4 in Appendix B. In Appendix C we investigate the existence of complex Hadamard matrices with circulant core and exhibit new examples of complex Hadamard matrices of order 7 and 11. We conclude this chapter with highlighting some connections between complex Hadamard matrices and equiangular tight frames.

Our contributions to this chapter are the relevant results from [130] and [132], while the additional new results presented here are subject to a series of forthcoming publications.

### 3.1 Preliminaries

We begin with the following finiteness result (cf. Theorem 1.2.4).

**Theorem 3.1.1** (Petrescu, [113]). *For every prime  $p$  the Fourier matrix  $F_p$  is isolated amongst all  $p \times p$  complex Hadamard matrices.*

Nicoară gave a new and independent proof of this theorem [107]. One of the consequences of Theorem 3.1.1 is that there is no “cheap” way to obtain infinite, parametric families of complex Hadamard matrices stemming from  $F_p$  in a similar spirit to Diță’s construction (cf. Corollary 1.2.5). In fact, once it was asked by Enflo (see [60] and the review article [120]), whether all complex Hadamard matrices of prime orders are isolated, which was refuted by a clever construction of Petrescu [113]. In particular, he proved the following

**Theorem 3.1.2** (Petrescu [113]). *For prime  $p = 7, 13, 19$  and  $31$  there are infinite, parametric families of complex Hadamard matrices of order  $p$ .*

Note that all mentioned orders are of the form  $p = 6s + 1$ . However, we do not have any understanding of the case  $p = 6s + 5$  (apart from the finiteness result of Haagerup concerning  $5 \times 5$  matrices). In particular, the following is already an open

**Problem 3.1.3.** Decide if there are infinitely many inequivalent complex Hadamard matrices of order 11.

It requires considerable efforts to exhibit complex Hadamard matrices of order 11 (but see [19] for a couple of explicit examples as well as Example C.2.11), and it seems even more difficult to construct an infinite family.

### 3.2 Petrescu’s construction revisited

In this section we recall the main ideas of Petrescu’s construction, but we advise the reader in advance that here we are only scratching the surface of what he has actually obtained in his PhD thesis [113]. We combine his ideas with an intelligent computer search to obtain a  $BH(19, 6)$  matrix the existence of which was listed undecided in [27]. The details are as follows.

**Definition 3.2.1.** We say that a complex Hadamard matrix  $H$  of order  $3s + 1$  is of *Petrescu-type*, if it has the following block form

$$H := \begin{bmatrix} X & Y & T \\ Y & X & T \\ T^* & T^* & D \end{bmatrix}, \quad (3.1)$$

where the matrices  $X$  and  $Y$  are of order  $s$ ,  $D$  is of order  $s + 1$  and finally  $T$  consists of  $s$  noninitial rows of a dephased complex Hadamard matrix of order  $s + 1$ .

It seems somewhat surprising already that one can embed four copies of an essentially complete complex Hadamard matrix into the array  $H$ , whose size are roughly  $n/3$  each. However, Petrescu illustrated that if  $T$  and  $D$  are chosen carefully enough, namely if they possess some further structural properties (e.g. circulant blocks, etc.), then not only some complex Hadamard matrices, but parametric families of complex Hadamard matrices can be obtained. After recalling that  $\omega$  denotes the principal cubic root of unity, we offer the following

**Example 3.2.2** (Petrescu, [113]). The array

$$P_7^{(1)}(a) = \left[ \begin{array}{cc|cc|ccc} 1 & a\omega^2 & \omega & -a\omega^2 & \omega & \omega^2 & 1 \\ \bar{a}\omega^2 & 1 & -\bar{a}\omega^2 & \omega & \omega^2 & \omega & 1 \\ \hline \omega & -a\omega^2 & 1 & a\omega^2 & \omega & \omega^2 & 1 \\ -\bar{a}\omega^2 & \omega & \bar{a}\omega^2 & 1 & \omega^2 & \omega & 1 \\ \hline \omega^2 & \omega & \omega^2 & \omega & -\omega^2 & 1 & 1 \\ \omega & \omega^2 & \omega & \omega^2 & 1 & -\omega^2 & 1 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & -\omega^2 \end{array} \right] \quad (3.2)$$

is a one-parameter family of Petrescu-type complex Hadamard matrices. The matrix  $P_7 = P_7^{(1)}(1)$  is equivalent to Brock's example [18].

However, from Petrescu's analysis it follows that in practice it is very difficult to meet the requirements of the parametrization property, and a general method, working for all primes  $p \equiv 1 \pmod{6}$  is yet to be discovered. We investigate Petrescu-type  $BH(n, q)$  matrices for small  $n$  and  $q$ , and seek for various parametric families of complex Hadamard matrices. The underlying structure of these matrices heavily restricts the search space and makes an intelligent computer search feasible even in those orders, where a straightforward brute force attack would be far out of reach.

We assume throughout this section, without any further comment, that the embedded (partial) complex Hadamard matrix  $T$  satisfies the following properties:

$$TT^* = (s + 1)I_s, \quad (3.3)$$

$$T^*T = (s + 1)I_{s+1} - J_{s+1}, \quad (3.4)$$

$$TJ = 0, \quad (3.5)$$

where  $J$  denotes the all 1 matrix, whose size should be clear from context.

*Remark 3.2.3.* We remark here that the arrangement of the four  $T$  blocks in the border of  $H$  forces the structure in the upper left corner; that is, the presence of two blocks

of  $X$  and  $Y$  is not a further simplifying assumption, but an easy consequence of the imposed structure. We omit the corresponding calculations.  $\square$

From the orthogonality relations the following can be deduced.

**Lemma 3.2.4.** *Under the assumptions on  $T$  the array  $H$  is complex Hadamard if and only if  $X, Y$  and  $D$  are unimodular matrices, moreover*

$$(X + Y)(X + Y)^* = (s - 1)I_s, \quad (3.6)$$

$$(X - Y)(X - Y)^* = (3s + 1)I_s, \quad (3.7)$$

$$DD^* = D^*D = (s - 1)I_{s+1} + 2J_{s+1}, \quad (3.8)$$

$$(X + Y)T + TD^* = 0. \quad (3.9)$$

*Proof.* The first two equations are equivalent to the sum and difference of

$$XX^* + YY^* = 2sI_s, \quad (3.10)$$

$$XY^* + YX^* = -(s + 1)I_s; \quad (3.11)$$

equation (3.9) is one of the orthogonality conditions; while (3.8) follows from the fact that  $H^*$  is Hadamard as well.  $\square$

In particular, by (3.8) the operator  $D$  is normal. Note also its following property.

**Lemma 3.2.5.** *Let  $H$  be a Petrescu-type complex Hadamard matrix of order  $3s + 1$ . Then*

$$|\det D|^2 = (s - 1)^s(3s + 1). \quad (3.12)$$

*In particular,  $D$  is invertible for  $s > 1$ .*

*Proof.* We use the folklore fact that  $\det(aI_n + bJ_n) = a^n + na^{n-1}b$ . Therefore the result follows from (3.8).  $\square$

Following Petrescu's ideas we attempt to reconstruct  $H$  via Lemma 3.2.4.

**Lemma 3.2.6** (Petrescu, [113]). *Suppose that (3.8) holds. Then (3.9) holds if and only if*

$$X + Y = -\frac{1}{s + 1}TD^*T^* \quad (3.13)$$

*and*

$$JD = DJ. \quad (3.14)$$

The proof is somewhat technical, yet we include it for the reader's convenience, because the original work of Petrescu [113] is not easily accessible. We denote by  $\text{Ker}A$  and  $\text{Im}A$  the kernel and the range of the operator  $A$ , respectively. Recall that the orthogonal complement of  $\text{Ker}A$ , which we denote by  $(\text{Ker}A)^\perp$ , is  $\text{Im}A$ .

*Proof.* Suppose that (3.13) and (3.14) holds. Write

$$\begin{aligned}(X + Y)T + TD^* &= -\frac{1}{s+1}TD^*T^*T + TD^* = -\frac{1}{s+1}TD^*((s+1)I - J) + TD^* \\ &= \frac{1}{s+1}TD^*J = \frac{1}{s+1}TJD^* = 0.\end{aligned}$$

To see the other direction, first multiply (3.9) by  $T^*$  to the right to get (3.13). Now substitute (3.13) back into (3.9) to get

$$TD^*J = 0$$

as before, and multiply it by  $T^*$  and rearrange to get

$$\frac{1}{q+1}D^*J = \frac{1}{(q+1)^2}JD^*J. \quad (3.15)$$

Now let us introduce the notation  $P := \frac{1}{q+1}J$ , and observe that  $P = P^2 = P^*$  is a self-adjoint projection. After taking adjoints in (3.15) we obtain

$$PD = PDP. \quad (3.16)$$

Our aim is to show that  $PD = DP$  holds, and hence (3.14) as well. Let  $x \in \text{Ker}P$ . Then, by (3.16),  $Dx \in \text{Ker}P$  as well, and therefore  $PDx = DPx = 0$ .

Now suppose that  $x \in (\text{Ker}P)^\perp = \text{Im}P$ . It follows that  $Dx \in \text{Im}P$  as well, as  $Dx$  is orthogonal to any vector  $y$  belonging to  $\text{Ker}P$ . To see this, observe that by Lemma 3.2.5  $D$  is invertible, and hence it is enough to show that  $Dx$  is orthogonal to any  $Dy$ . Indeed:

$$\begin{aligned}\langle Dx, Dy \rangle &= \langle D^*Dx, y \rangle = \langle ((s-1)I + 2J)x, y \rangle = \langle ((3s+1)I - 2((s+1)I - J))x, y \rangle \\ &= (3s+1)\langle x, y \rangle - 2\langle T^*TPx, y \rangle = 0,\end{aligned}$$

where we have used (3.8), the identity  $Px = x$ , (3.5) and the fact that  $x$  and  $y$  are orthogonal. It follows that  $PDx = DPx = Dx$  and we are done.  $\square$

**Corollary 3.2.7.** *The system of equations (3.8), (3.13), (3.14) imply (3.6).*

### 3.2.1 Constructing a $BH(19, 6)$ matrix

Now we describe the construction of the anticipated  $BH(19, 6)$  matrix as follows. We begin by constructing a matrix  $D$  satisfying (3.8). Of course, there is absolutely no guarantee that an initial matrix  $D$  can be extended to a  $BH(19, 6)$  matrix  $H$ , and in order to avoid considering multiple instances of essentially the same matrices  $D$  we reduce them by a number of equivalence operations. In particular,  $D$  can be replaced by  $\lambda PDP^T$  where  $\lambda$  is unimodular and  $P$  is any permutation matrix, by considering  $\text{Diag}(\bar{\lambda}I_s, \bar{\lambda}I_s, \lambda P)H\text{Diag}(I_s, I_s, P^T)$  instead of the initial array  $H$  if it is necessary. The following is a further useful

**Lemma 3.2.8.** *Let  $H$  be a Petrescu-type complex Hadamard matrix of order  $n$ . Then*

$$JD = DJ = cJ,$$

where  $|c| = \sqrt{n}$ .

*Proof.* Multiply (3.8) by  $J$  from the left and right simultaneously, then use (3.14).  $\square$

Once  $D$  has been specified the second step is to obtain the complex Hadamard matrix  $T$ . We do this intelligently through (3.13) by constructing  $T$  row by row. We check, using the partial matrix  $T_r$ , consisting of  $r$  row vectors, if the resulting matrix

$$-\frac{1}{s+1}T_r D^* T_r^*$$

can be decomposed as a sum of two matrices  $X_r$  and  $Y_r$ , containing sixth roots of unity. The final step is to ensure (3.7), which, again, can be checked row-by-row by utilizing the partial matrices  $X_r$  and  $Y_r$ . After implementing a more-or-less naive algorithm in *Mathematica* we obtained a solution, virtually in seconds.

**Theorem 3.2.9.** *There exists a  $BH(19, 6)$  matrix.*

**Example 3.2.10.** The matrix

$$W_{19} = \text{EXP} \left( \frac{2\pi i}{6} L \right), \quad (3.17)$$

where

$$L = \begin{bmatrix} 3 & 0 & 1 & 1 & 0 & 0 & 5 & 4 & 3 & 5 & 3 & 2 & 1 & 1 & 3 & 5 & 4 & 3 & 0 \\ 0 & 0 & 1 & 3 & 3 & 1 & 4 & 2 & 4 & 5 & 1 & 5 & 1 & 4 & 3 & 3 & 1 & 5 & 0 \\ 0 & 0 & 1 & 4 & 2 & 4 & 2 & 4 & 3 & 2 & 4 & 1 & 3 & 3 & 1 & 4 & 5 & 1 & 0 \\ 1 & 2 & 4 & 2 & 1 & 2 & 4 & 4 & 2 & 4 & 5 & 0 & 3 & 5 & 1 & 1 & 3 & 4 & 0 \\ 2 & 5 & 4 & 3 & 2 & 0 & 4 & 2 & 0 & 1 & 4 & 2 & 4 & 1 & 5 & 3 & 1 & 3 & 0 \\ 0 & 3 & 5 & 4 & 5 & 0 & 4 & 5 & 3 & 1 & 3 & 4 & 5 & 3 & 4 & 1 & 3 & 1 & 0 \\ \hline 5 & 4 & 3 & 5 & 3 & 2 & 3 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 3 & 5 & 4 & 3 & 0 \\ 4 & 2 & 4 & 5 & 1 & 5 & 0 & 0 & 1 & 3 & 3 & 1 & 1 & 4 & 3 & 3 & 1 & 5 & 0 \\ 2 & 4 & 3 & 2 & 4 & 1 & 0 & 0 & 1 & 4 & 2 & 4 & 3 & 3 & 1 & 4 & 5 & 1 & 0 \\ 4 & 4 & 2 & 4 & 5 & 0 & 1 & 2 & 4 & 2 & 1 & 2 & 3 & 5 & 1 & 1 & 3 & 4 & 0 \\ 4 & 2 & 0 & 1 & 4 & 2 & 2 & 5 & 4 & 3 & 2 & 0 & 4 & 1 & 5 & 3 & 1 & 3 & 0 \\ 4 & 5 & 3 & 1 & 3 & 4 & 0 & 3 & 5 & 4 & 5 & 0 & 5 & 3 & 4 & 1 & 3 & 1 & 0 \\ \hline 5 & 5 & 3 & 3 & 2 & 1 & 5 & 5 & 3 & 3 & 2 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 3 \\ 5 & 2 & 3 & 1 & 5 & 3 & 5 & 2 & 3 & 1 & 5 & 3 & 0 & 0 & 1 & 3 & 0 & 1 & 0 \\ 3 & 3 & 5 & 5 & 1 & 2 & 3 & 3 & 5 & 5 & 1 & 2 & 1 & 3 & 0 & 0 & 0 & 1 & 0 \\ 1 & 3 & 2 & 5 & 3 & 5 & 1 & 3 & 2 & 5 & 3 & 5 & 0 & 1 & 0 & 1 & 0 & 4 & 1 \\ 2 & 5 & 1 & 3 & 5 & 3 & 2 & 5 & 1 & 3 & 5 & 3 & 1 & 0 & 4 & 1 & 1 & 0 & 0 \\ 3 & 1 & 5 & 2 & 3 & 5 & 3 & 1 & 5 & 2 & 3 & 5 & 1 & 0 & 1 & 0 & 4 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

is a  $BH(19, 6)$  matrix.

It is natural to ask if the matrix  $W_{19}$  admits an affine orbit, similarly to  $P_7^{(1)}(a)$  (see Example 3.2.2), but we were unable to calculate its defect due to the presence of irrational entries. Thus the following remained an unresolved

**Problem 3.2.11.** Decide if there is a Petrescu-type  $BH(19, 6)$  leading to an infinite, parametric family of complex Hadamard matrices.

Further Petrescu-type  $BH(n, q)$  matrices can be found in Appendix A; among them there is a four-parameter family of complex Hadamard matrices of order 13, which is the largest known family in this order.

### 3.2.2 Some non-existence results

There are three obvious necessary conditions restricting the existence of Petrescu-type  $BH(n, q)$  matrices: first, it is very well be possible that a  $BH(n, q)$  matrices cannot exist at all due to some number theoretic reasons; secondly we might not have access to a submatrix  $T$  with the required properties; and lastly the submatrix  $D$  might not exist. Throughout this section we investigate the roots of these obstructions. We begin with recalling the relevant case of Part 3 of Theorem 1.4.4.

**Theorem 3.2.12** (Winterhof, [146]). *Let  $n$  be odd. If the squarefree part of  $n$  is divisible by a prime  $p \equiv 5 \pmod{6}$  then there is no  $BH(n, 6)$  matrix.*

Winterhof's result is far more general than stated here, but this is enough for our purposes. The proof of this theorem relies on algebraic number theory, and exploits the fact that the square of the determinant of  $BH(n, 6)$  matrices must have a representation of the form  $A^2 + 3B^2$ . We shall use repeatedly the following number theoretic

**Lemma 3.2.13.** *Let  $A$  and  $B$  be integral numbers such that  $A^2 + 3B^2 = n$ . Then every prime divisor  $p$  of the squarefree part of  $n$  is either  $p = 3$  or  $p \equiv 1 \pmod{6}$ .*

*Proof.* It is well-known that every prime number  $p \equiv 1 \pmod{6}$  has the representation  $p = x^2 + 3y^2$  with  $x$  and  $y$  being integers (see Theorem 5 in [124, Chapter IX]), as well as  $3 = 0^2 + 3 \cdot 1^2$  and any square number  $q^2 = q^2 + 3 \cdot 0^2$ . If two numbers,  $n_1$  and  $n_2$ , have this form, say  $n_i = x_i^2 + 3y_i^2$ ,  $i = 1, 2$ , then so does their product  $n_1 n_2 = (x_1 x_2 + 3y_1 y_2)^2 + 3(x_1 y_2 - x_2 y_1)^2$ . Hence all of these numbers have the desired representation. Next we prove that the other numbers cannot have this form. Let us suppose that

$$A^2 + 3B^2 = q^2 r, \tag{3.18}$$

where  $r$  is squarefree. We can assume that  $A$ ,  $B$  and  $r$  are relatively prime, otherwise we can divide  $A$ ,  $B$  and  $q$  by their greatest common divisor.

If  $r$  is even, then both  $A$  and  $B$  are odd, and as a result the left hand side of (3.18) is divisible by 4, but not by 8, a contradiction.

If  $p > 3$  and  $p|r$ , then  $A^2 \equiv -3B^2 \pmod{p}$ , and as  $A$  and  $B$  are nonzero modulo  $p$  it follows that  $-3$  is a quadratic residue. Then, should we have  $p \equiv 5 \pmod{6}$ , we would find that

$$\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{3}{p}\right) = (-1)^{p-1} \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

a contradiction. □

Now we turn to the

*Proof of Theorem 3.2.12.* The determinant of a  $BH(n, 6)$  matrix is an integral linear combination of 1 and  $\omega$ , and hence, by referring to Lemma 1.4.7 we have

$$|A + B\omega| = n^{n/2},$$

which, after squaring and by a multiplication of 4 becomes

$$(2A - B)^2 + 3B^2 = 4n^n,$$

and hence Lemma 3.2.13 applies. In particular, the squarefree part of  $4n^n$ , which is easily seen to be the same as the squarefree part of  $n$  (as  $n$  is odd) cannot have a prime divisor  $p \equiv 5 \pmod{6}$ . □

Obviously, to obtain a Petrescu-type  $BH(3s+1, q)$  matrix, one needs a  $BH(s+1, q)$  matrix in place of  $T$  as a main ingredient. This, again, is heavily constrained by Theorem 3.2.12 above. We state the following trivial

**Lemma 3.2.14.** *If there is no  $BH(s+1, q)$  matrix, then there is no Petrescu-type  $BH(3s+1, q)$  matrix either.*

Another restriction comes from the submatrix  $D$  via Lemma 3.2.5.

**Theorem 3.2.15.** *If the squarefree part of  $(3s+1)(s-1)^s$  is even or divisible by a prime  $p \equiv 5 \pmod{6}$  then there is no Petrescu-type  $BH(3s+1, 6)$  matrix.*

*Proof.* From Lemma 3.2.5 we see that the determinant of  $D$ , which is an integral linear combination of 1 and  $\omega$ , after taking absolute value, squaring and multiplying by 4 reads

$$(2A - B)^2 + 3B^2 = 4(3s+1)(s-1)^s = 4|\det D|^2,$$

hence we can apply Lemma 3.2.13. □



*Remark 3.2.16.* One might wonder if a similar restriction can be stated via Lemma 3.2.8 by exploiting the fact that  $s + 1$  sextic roots of unity are needed adding up to  $\sqrt{3s + 1}$  in absolute value, from which one can conclude that the number  $3s + 1$  alone should met the conditions of Lemma 3.2.13. This property, however is already captured by Theorem 3.2.15. Similarly, by considering the determinant of the matrices  $X \pm Y$  via (3.6) and (3.7) we do not get any further restriction.  $\square$

Table 3.1: Existence of  $BH(n, 6)$  matrices for  $n \leq 39$ ,  $n$  odd.

$n$	Existence	Petr.-type	Remark	$n$	Existence	Petr.-type	Remark
1	$F_1$	Yes		21	$F_3 \otimes P_7$	-	See (3.2)
3	$F_3$	-		23	-	-	
5	-	-		25	$W_{25}$	?	See (1.10)
7	$P_7$	Yes	See (3.2)	27	$F_3 \otimes F_3 \otimes F_3$	-	
9	$F_3 \otimes F_3$	-		29	-	-	
11	-	-		31	?	No	
13	$X_{13}$	No	See [28]	33	-	-	
15	-	-		35	-	-	
17	-	-		37	?	?	
19	$W_{19}$	Yes	See (3.17)	39	$F_3 \otimes X_{13}$	-	See [28]

Table 3.1 summarizes the existence of  $BH(n, 6)$  matrices of small orders (cf. Table 1.2). One can see that  $n = 37$  is the next interesting odd order where a Petrescu-type matrix might exists. Order 25 might be possible, but a  $BH(25, 6)$  matrix already exists by Theorem 1.4.41, while order 31 is not possible due to the lack of  $BH(11, 6)$  matrices (see Lemma 3.2.14).

To conclude, Petrescu's array seems to be a reasonable way to construct interesting matrices of prime orders. It would be nice to find additional examples of  $BH(n, 6)$  matrices coming from this construction.

**Problem 3.2.17.** Decide if a Petrescu-type  $BH(37, 6)$  matrix exist.

*Remark 3.2.18.* Unfortunately, Petrescu's construction cannot yield new examples of real Hadamard matrices as either  $3s + 1$  or  $s + 1$  is not divisible by 4.  $\square$

It is worthwhile noting that the method might lead to new examples of  $BH(n, 4)$  matrices. Unfortunately, however, Petrescu-type  $BH(70, 4)$  matrices do not exist due to restrictions on the submatrix  $D$  and hence the smallest open case of  $BH(n, 4)$  matrices cannot be constructed this way. Petrescu's construction might yield new examples of (generalized) weighing matrices as well [88]. The following is an intriguing

**Example 3.2.19.** The following is a three-parameter family of Petrescu-type weighing matrices of order 10.

$$W_{10}^{(3)}(a, b, c) = \begin{bmatrix} 0 & a & b & 1 & -a & -b & 1 & 1 & -1 & -1 \\ \bar{a} & 0 & b\bar{a} & -\bar{a} & 1 & -b\bar{a} & 1 & -1 & c & -c \\ \bar{b} & a\bar{b} & 0 & -\bar{b} & -a\bar{b} & 1 & 1 & -1 & -c & c \\ \hline 1 & -a & -b & 0 & a & b & 1 & 1 & -1 & -1 \\ -\bar{a} & 1 & -b\bar{a} & \bar{a} & 0 & b\bar{a} & 1 & -1 & c & -c \\ -\bar{b} & -a\bar{b} & 1 & \bar{b} & a\bar{b} & 0 & 1 & -1 & -c & c \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & -1 & 1 & 0 & 1 & 1 \\ -1 & \bar{c} & -\bar{c} & -1 & \bar{c} & -\bar{c} & 1 & 1 & 0 & 1 \\ -1 & -\bar{c} & \bar{c} & -1 & -\bar{c} & \bar{c} & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Additionally, as  $W_{10}^{(3)}(a, b, c)$  is a self-adjoint family, we find that

$$H_{10}^{(3)}(a, b, c) := W_{10}^{(3)}(a, b, c) + \mathbf{i}I_{10}$$

is a three-parameter family of complex Hadamard matrices, stemming from a  $BH(10, 4)$  matrix. The family is equivalent to  $D_{10}^{(3)}(a, b, c)$  from [135].

We conclude this section with the following fundamental open

**Problem 3.2.20.** Investigate if there is a construction, analogous to Petrescu's method resulting in infinite families of complex Hadamard matrices of orders  $6s + 5$ .

### 3.3 Circulant complex Hadamard matrices

Another source of complex Hadamard matrices of prime orders is the pool of circulant complex Hadamard matrices. These objects were heavily investigated during the early 1990s by the pioneering work of Björck [9] (see also [10], [40] and [106]). Let us consider a circulant complex Hadamard matrix of order  $n$  whose first row is given by  $x = (x_0, x_1, \dots, x_{n-1})$ . For convenience, let us fix  $x_0 = 1$  (which we can do up to equivalence). Then, by orthogonality, we have

$$\begin{cases} x_0 = 1, \\ \frac{x_1}{x_0} + \frac{x_2}{x_1} + \dots + \frac{x_0}{x_{n-1}} = 0, \\ \frac{x_2}{x_0} + \frac{x_3}{x_1} + \dots + \frac{x_1}{x_{n-1}} = 0, \\ \vdots \\ \frac{x_{n-1}}{x_0} + \frac{x_0}{x_1} + \dots + \frac{x_{n-2}}{x_{n-1}} = 0. \end{cases} \quad (3.19)$$

We have the following well-known

**Example 3.3.1.** For  $n \geq 2$  let  $(\alpha, \beta) \in \mathbb{Z}_n^* \times \mathbb{Z}_n$  and consider the vector  $x^{(\alpha, \beta)}$  with coordinates

$$x_i^{(\alpha, \beta)} = \begin{cases} \exp\left(\frac{2\pi i}{n} \left(\frac{\alpha i^2}{2} + \beta i\right)\right), & i \in \mathbb{Z}_n, \quad n \text{ even}, \\ \exp\left(\frac{2\pi i}{n} \left(\frac{\alpha i(i-1)}{2} + \beta i\right)\right), & i \in \mathbb{Z}_n, \quad n \text{ odd}. \end{cases} \quad (3.20)$$

These solutions of (3.19) are called the classical solutions leading to the Fourier matrices.

It is easy to see that if  $x$  is a unimodular solution of (3.19) then the Fourier-transformed vector  $\widehat{x}$  is unimodular as well:

$$|x_i| = |\widehat{x}_i| = 1, \quad i \in \mathbb{Z}_n, \quad (3.21)$$

as

$$|\widehat{x}_k|^2 = \frac{1}{n} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} e^{\frac{2\pi i}{n}(k-1)(i-j)} x_i \overline{x_j} = \frac{1}{n} \sum_{i=0}^{n-1} e^{\frac{2\pi i}{n}(k-1)i} \sum_{j=0}^{n-1} \frac{x_{i+j}}{x_j} = 1.$$

In 1983 Enflo asked [120] whether the vectors

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

given by (3.20) are the only solutions to the bi-unimodular problem (3.21) for prime  $p$ . It turns out, that this is only true for  $p = 2, 3$  and  $5$ , as starting from  $p \geq 7$  there are non-classical solutions to the problem, yielding non-classical circulant complex Hadamard matrices which are inequivalent from the Fourier matrix [9], [40], [106].

Motivated by Enflo's question, Björck reformulated (3.19) in [9] by passing to the quotients  $z_i := x_{i+1}/x_i$ ,  $i = 0, 1, \dots, n-1$ , where the indices are taken modulo  $n$  and found that the system of equations (3.19) boils down to

$$\begin{cases} z_0 + z_1 + \dots + z_{n-1} = 0, \\ z_0 z_1 + z_1 z_2 + \dots + z_{n-1} z_0 = 0, \\ \vdots \\ z_0 z_1 \dots z_{n-2} + z_1 z_2 \dots z_{n-1} + \dots + z_{n-1} z_0 \dots z_{n-3} = 0, \\ z_0 z_1 \dots z_{n-1} = 1. \end{cases} \quad (3.22)$$

A solution of (3.22),  $z = (z_0, z_1, \dots, z_{n-1})$ , is called a cyclic  $n$ -root. Clearly, by the last equation  $z_i \neq 0$ , and hence any unimodular cyclic  $n$ -root  $z$  can be transformed to a solution  $x$  of (3.19), namely

$$x = (1, z_0, z_0 z_1, \dots, z_0 z_1 z_2 \dots z_{n-2}). \quad (3.23)$$

The vector  $x$  is called a cyclic  $n$ -root on the  $x$ -level. Let us recall some recent advances.

**Theorem 3.3.2** (Haagerup, [59]). *For every prime  $p$  there are exactly  $\binom{2p-2}{p-1}$  solutions to the cyclic  $p$ -root problem, counted with multiplicity. In particular, there are at most  $\binom{2p-2}{p-1}$  circulant complex Hadamard matrices with diagonal 1 of order  $p$ .*

*Remark 3.3.3.* The multiplicity of an isolated zero is an analytic property; the precise definition can be found in [59] (which actually refers to the monograph [2]). In triangular systems

$$\begin{cases} f_1(x_1) = 0, \\ f_2(x_1, x_2) = 0, \\ \vdots \\ f_n(x_1, x_2, \dots, x_n) = 0, \end{cases}$$

with finitely many solutions only (i.e. if all solutions are isolated) the multiplicity of a zero  $y = (y_1, \dots, y_n)$  is exactly  $\prod_{i=1}^n m_i$ , where  $m_i$  is the multiplicity of the univariate polynomial  $f_i(y_1, \dots, y_{i-1}, x_i)$  for every  $i = 1, \dots, n$ . For a proof see [150].  $\square$

In contrast, square multiple  $n$  always gives rise to an infinite family of solutions.

**Theorem 3.3.4** (Backelin, [5]). *If  $m^2$  divides  $n$ , then there is an at least  $(m-1)$ -dimensional family of solutions to the cyclic  $n$ -root problem, namely*

$$z = (z_0, z_1, \dots, z_{m-1}, \alpha z_0, \alpha z_1, \dots, \alpha z_{m-1}, \dots, \alpha^{n/m-1} z_0, \dots, \alpha^{n/m-1} z_{m-1}),$$

where  $z_0, z_1, \dots, z_{m-2}$  are free parameters,  $z_0 z_1 \dots z_{m-1} = 1$  and  $\alpha$  is any primitive  $n/m$ -th root of unity.

The proof can be seen by substituting back to (3.22). We omit the (lengthy) details.

**Example 3.3.5.** Let  $n = 12$ ,  $2^2|12$  so we expect to find a one-parameter family of circulant complex Hadamard matrices of order 12. Let  $\alpha = -\omega^2$ , the primitive sixth root of unity, and consider the one-parameter family of cyclic 12-roots

$$z(a) = (a, \bar{a}, -\omega^2 a, -\omega^2 \bar{a}, \omega a, \omega \bar{a}, -a, -\bar{a}, \omega^2 a, \omega^2 \bar{a}, -\omega a, -\omega \bar{a}).$$

It is readily verified that  $z(a)$  is a solution to (3.22) for any unimodular number  $a$ , and hence induces a circulant complex Hadamard matrix via (3.23) as

$$C_{12}^{(1)}(a) = \text{Circ}(1, a, 1, -\omega^2 a, \omega, \omega^2 a, 1, -a, 1, \omega^2 a, \omega, -\omega^2 a).$$

It is easily seen, after dephasing the matrix  $C_{12}^{(1)}(a)$ , that the one degree of freedom does not vanish, and therefore  $C_{12}^{(1)}(a)$  is a one-parameter family of circulant complex Hadamard matrices, as expected. It follows, that the triplet  $\{I_{12}, F_{12}, C_{12}^{(1)}(a)\}$  is a one-parameter family of triplet of MUBs in  $\mathbb{C}^{12}$  (see Section 2.4).

Finally, let us recall the following

**Theorem 3.3.6** (Faugère, [51], [52]). *All cyclic  $n$ -roots are known up to order  $n \leq 10$ .*

We advise the reader that these solutions are rather complicated. Further, all cyclic 11-roots are known numerically [38] while starting from order 12 only partial results are known [119]. The cyclic  $n$ -root problem turned out to be a challenging problem in symbolic computation, mostly because of its large number of solutions and in practice it is used for various benchmarking purposes. As the problem of fully classifying cyclic  $n$ -roots and circulant complex Hadamard matrices seems far out of reach, one is interested in special, more structural solutions giving access to examples in infinitely many orders.

Following Björck and Haagerup [9], [60] now we recall the concept of cyclic  $p$ -roots of simple index  $k$  as follows. Let  $p$  be a prime and let  $k \in \mathbb{N}$  be a number that divides  $p - 1$ . The group  $\mathbb{Z}_p^*$  has a unique subgroup  $G_0$  of index  $k$ , namely the subgroup of the  $k$ th residues as follows:

$$G_0 = \{x^k, x \in \mathbb{Z}_p^*\}.$$

Moreover, if  $g \in \mathbb{Z}_p^*$  is a generator of  $\mathbb{Z}_p^*$  then the  $k - 1$  nontrivial cosets of  $G_0$  in  $\mathbb{Z}_p^*$  are given by

$$G_i = g^i G_0, \quad 1 \leq i \leq k - 1. \quad (3.24)$$

Note that it follows that  $g \in G_1$ . Following the notation of [11], a cyclic  $p$ -root  $z$  has simple index  $k$  if the corresponding cyclic  $p$ -root on the  $x$ -level (3.23) is of the following form:

$$\begin{cases} x_i = c_k, & \text{if } i \in G_k, 1 \leq i \leq p - 1; \quad \text{and} \\ x_0 = 1, \end{cases} \quad (3.25)$$

where  $(c_0, c_1, \dots, c_{k-1}) \in (\mathbb{C}^*)^k$ . These special cyclic  $p$ -roots were introduced by Björck in [9], who fully classified the case  $k = 2$  through the following useful reformulation of the problem.

**Proposition 3.3.7** (Björck, [9]). *If  $x = (x_0, x_1, \dots, x_{p-1})$  has the form (3.25), then the equations (3.19) can be reduced to the following  $k$  rational equations in  $c_0, c_1, \dots, c_{k-1}$ :*

$$c_a + \frac{1}{c_{a+m}} + \sum_{i,j=0}^{k-1} n_{ij} \frac{c_{a+j}}{c_{a+i}} = 0, \quad 0 \leq a \leq k - 1, \quad (3.26)$$

where all indices are calculated modulo  $k$ . In (3.26) the number  $m$  is determined by  $p - 1 \in G_m$  and  $n_{ij}$  denote the transition numbers of order  $k$ , namely, the number of  $b \in G_i$  for which  $b + 1 \in G_j$ ,  $0 \leq i, j \leq k - 1$ , with respect to the generator  $g$  of  $\mathbb{Z}_p^*$ .

We remark that the system of equations (3.26) is independent of the choice of  $g$  up to relabelling the variables. Curiously enough, the number of solutions is known.

**Theorem 3.3.8** (Haagerup, [59]). *For every  $k \in \mathbb{N}$  and for every prime number  $p$  for which  $k$  divides  $p - 1$  the number of solutions  $(c_0, c_1, \dots, c_{k-1}) \in (\mathbb{C}^*)^k$  to (3.26) counted with multiplicity is equal to  $\binom{2k}{k}$ .*

Throughout this chapter we are interested in the unimodular cyclic  $n$ -roots only, i.e. the ones that correspond to complex Hadamard matrices.

### 3.3.1 Cyclic $p$ -roots of simple index 2

The following are the index 2 type cyclic complex Hadamard matrices.

**Theorem 3.3.9** (Björck, [9]). *Let  $p \equiv 3 \pmod{4}$  be a prime and consider the decomposition  $J = I + S + N$  where  $S$  and  $N$  are  $(0, 1)$  circulant matrices whose first rows are the characteristic vector of the quadratic residues and nonresidues modulo  $p$ , respectively. Then the matrix  $H := I + S + \alpha N$  is complex Hadamard, where*

$$\alpha = -\frac{p-1}{p+1} \pm \mathbf{i} \frac{2\sqrt{p}}{p+1}.$$

Similarly, we have

**Theorem 3.3.10** (Björck, [9]). *Let  $p \equiv 1 \pmod{4}$  be a prime and consider the decomposition  $J = I + S + N$  where  $S$  and  $N$  are  $(0, 1)$  circulant matrices whose first row are the characteristic vector of the quadratic residues and nonresidues modulo  $p$ , respectively. Then the matrices  $H := I + \alpha S + \bar{\alpha} N$  and  $\bar{H}$  are complex Hadamard, where*

$$\alpha = \frac{-1 \pm \sqrt{p}}{p-1} + \mathbf{i} \frac{\sqrt{p^2 - 3p \pm 2\sqrt{p}}}{p-1},$$

where the  $\pm$  signs agree.

For  $p \geq 7$  Theorem 3.3.9 and Theorem 3.3.10 give rise to nonclassical circulant complex Hadamard matrices. These results were subsequently rediscovered in [106] and [40].

*Remark 3.3.11.* Theorems 3.3.9 and 3.3.10 essentially exploit the fact that the underlying objects, namely the Hadamard design (when  $p \equiv 3 \pmod{4}$ ) and the core of a conference matrix (when  $p \equiv 1 \pmod{4}$ ), have very rich combinatorial structure. We have generalized these constructions for non-prime orders as well [132] (cf. Theorems 3.4.5 and 3.4.18, respectively).  $\square$

### 3.3.2 Cyclic $p$ -roots of simple index 3

In a recent paper Björck and Haagerup continued investigating the cyclic  $n$ -root problem by giving a full algebraic classification of all cyclic  $p$ -roots of index 3 [11]. We recall their result in the following

**Theorem 3.3.12** (Björck–Haagerup, [11]). *For every prime  $p \equiv 1 \pmod{6}$  all cyclic  $p$ -roots of index 3 can be described by closed analytic formulae.*

The resulting formulas they obtained are highly non trivial, and here we recall the unimodular solutions as follows.

**Theorem 3.3.13** (Björck–Haagerup, [11]). *For every prime  $p \equiv 1 \pmod{6}$  and for  $k = 3$  there are exactly 12 unimodular solutions of the system of equations (3.26), given by  $(c_0^{(j)}, c_1^{(j)}, c_2^{(j)})$ ,  $j = 1, 2$  and their cyclic permutation and their conjugate, where*

$$c_i^{(j)} = \alpha^{(j)} + \beta^{(j)} \cos\left(\theta - \frac{2\pi}{3}i\right) + \gamma^{(j)} \sin\left(\theta - \frac{2\pi}{3}i\right), \quad i = 0, 1, 2, \quad j = 1, 2,$$

where

$$\theta = \frac{1}{3} \arccos\left(\frac{A\sqrt{p}}{2p}\right),$$

and

$$\begin{aligned} \alpha^{(1)} &= \frac{pA - 2p - 2A}{2(p^2 - 3p - A)} + \mathbf{i} \frac{3\sqrt{3}\sqrt{p}\sqrt{p-4}B}{2(p^2 - 3p - A)}, \\ \beta^{(1)} &= -\frac{\sqrt{p}(p-4)(A+2)}{2(p^2 - 3p - A)} - \mathbf{i} \frac{3\sqrt{3}\sqrt{p-4}(p-2)B}{2(p^2 - 3p - A)}, \\ \gamma^{(1)} &= -\frac{3\sqrt{3}\sqrt{p}(p-4)B}{2(p^2 - 3p - A)} + \mathbf{i} \frac{\sqrt{p-4}(pA - 2p - 2A)}{2(p^2 - 3p - A)}, \end{aligned}$$

and

$$\begin{aligned} \alpha^{(2)} &= -\frac{u^2 - uv - 4}{2(u^2 + uv + 2)} + \mathbf{i} \frac{u\sqrt{4+u-v}\sqrt{4-u+v}}{2(u^2 + uv + 2)}, \\ \beta^{(2)} &= \frac{u(A+2)}{u^2 + uv + 2} + \mathbf{i} \frac{(u^2 + uv + 4)\sqrt{4+u-v}\sqrt{4-u+v}}{4(u^2 + uv + 2)}, \\ \gamma^{(2)} &= \frac{3\sqrt{3}uB}{u^2 + uv + 2} + \mathbf{i} \frac{(u^2 - uv - 4)\sqrt{u+v+4}\sqrt{u+v-4}}{4(u^2 + uv + 2)}, \end{aligned}$$

where  $u = \sqrt{p}$ ,  $v = \sqrt{p+4A+16}$  and  $A \equiv 1 \pmod{3}$ ,  $B > 0$  comes from the Gaussian decomposition  $4p = 27A^2 + B^2$ . Additionally, the generator  $g$  of  $\mathbb{Z}_p^*$  should be chosen in a way that the nontrivial cosets (see (3.24))  $G_1$  and  $G_2$  are defined to meet  $n_{01} < n_{02}$  with respect to  $g$ .

We offer the following enlightening

**Example 3.3.14.** Let  $p = 7$ . Then the Gaussian decomposition  $4p = A^2 + 27B^2$  implies  $A = B = 1$ . Let us choose a generator of  $\mathbb{Z}_7^*$  as  $g = 2$ . Then we find that  $G_0 = \{1, 6\}$ ,  $G_1 = \{2, 5\}$  and  $G_2 = \{3, 4\}$ , but as the transition numbers read  $n_{01} = 1, n_{02} = 0$  we should interchange the rôle of  $G_1$  and  $G_2$  (or equivalently, choose another generator, say

$g = 3$ ). Therefore, we define the first row of the index 3 circulant complex Hadamard matrix  $H$  as follows:  $x = (1, c_0, c_2, c_1, c_1, c_2, c_0)$ , where

$$c_i^{(j)} = \alpha^{(j)} + \beta^{(j)} \cos\left(\theta - \frac{2\pi}{3}i\right) + \gamma^{(j)} \sin\left(\theta - \frac{2\pi}{3}i\right), \quad i = 0, 1, 2, \quad j = 1, 2,$$

where

$$\theta = \frac{1}{3} \arccos\left(\frac{\sqrt{7}}{14}\right),$$

and

$$\alpha^{(1)} = -\frac{1}{6} + \mathbf{i}\frac{\sqrt{7}}{6}, \quad \beta^{(1)} = -\frac{\sqrt{7}}{6} - \frac{5}{6}\mathbf{i}, \quad \gamma^{(1)} = -\frac{\sqrt{21}}{6} - \mathbf{i}\frac{\sqrt{3}}{6},$$

and

$$\begin{aligned} \alpha^{(2)} &= \frac{6 - \sqrt{21}}{6} + \mathbf{i}\frac{\sqrt{-63 + 14\sqrt{21}}}{6}, & \beta^{(2)} &= \frac{7\sqrt{3} - 3\sqrt{7}}{12} + \mathbf{i}\frac{\sqrt{-18 + 26\sqrt{21}}}{12}, \\ \gamma^{(2)} &= \frac{7 - \sqrt{21}}{4} - \mathbf{i}\frac{\sqrt{-54 + 14\sqrt{21}}}{4}. \end{aligned}$$

We remark that for  $j = 1$  the first set of solutions gives  $(w^4, w, w^2)$  yielding the Fourier matrix  $F_7^{(0)} = \text{Circ}(1, w^4, w^2, w, w, w^2, w^4)$  where  $w = \mathbf{e}^{2\pi\mathbf{i}/7}$  is the principal 7th root of unity; in contrast, the numbers  $(c_0^{(2)}, c_1^{(2)}, c_2^{(2)})$  arising from the second set of solutions have the following minimal polynomial:

$$c^{12} - 12c^{11} + 24c^{10} + 4c^9 - 9c^8 + 27c^7 - 21c^6 + 27c^5 - 9c^4 + 4c^3 + 24c^2 - 12c + 1.$$

### 3.3.3 Cyclic $p$ -roots of simple index 4

In this section we consider cyclic  $p$ -roots of simple index 4 focusing especially on the case  $p \equiv 1 \pmod{8}$ . In this case  $-1$  is a quartic residue and therefore the system of equations (3.26) is “symmetric” in the sense that  $m = 0$ . We exhibit a new, previously unknown family of circulant complex Hadamard matrices, and outline a general method obtaining all cyclic  $p$ -roots of simplex index 4 for any given  $p \equiv 1 \pmod{8}$ . We give detailed results for  $p = 17$  in Appendix B.

We have already seen in the simple index 3 case that some number theoretic properties of the prime  $p$  played important rôle in the determination of the cyclotomic numbers. Here we have an analogous phenomenon.

**Theorem 3.3.15** (Katre–Rajwade, [79]). *Let  $p \equiv 1 \pmod{8}$  be a prime and let  $g$  be a generator of  $\mathbb{Z}_p^*$ . Define  $s \equiv 1 \pmod{4}$  uniquely by  $p = s^2 + t^2$ , and then the sign of  $t$  uniquely by  $t \equiv sg^{3(p-1)/4} \pmod{p}$ . Then the transition numbers of order 4 for  $\mathbb{Z}_p$ , with respect to the generator  $g$ , are given by*

$$n_{00} = \frac{p - 11 - 6s}{16},$$



$$\begin{aligned}
n_{01} = n_{10} = n_{33} &= \frac{p-3+2s+4t}{16}, \\
n_{02} = n_{20} = n_{22} &= \frac{p-3+2s}{16}, \\
n_{03} = n_{30} = n_{11} &= \frac{p-3+2s-4t}{16}, \\
n_{12} = n_{21} = n_{13} = n_{31} = n_{23} = n_{32} &= \frac{p+1-2s}{16}.
\end{aligned}$$

*Remark 3.3.16.* We can choose a generator  $g$  of  $\mathbb{Z}_p^*$  in a way that

$$n_{01} > n_{03}, \quad (3.27)$$

or equivalently,  $t > 0$  in the decomposition of  $p$ . This can be always achieved by passing to a new generator (if it is necessary)  $g' := g^{4i+3}$  for some  $i$  where  $4i+3$  is relative prime to  $p-1$ . As  $g \in G_1$  and  $g' \in G_3$  this will interchange  $G_1$  and  $G_3$  and thus we have arrived at (3.27).  $\square$

Some relations amongst the numbers  $n_{ij}$  are easy to see, for example, for  $p \equiv 1 \pmod{8}$   $-1$  is a quartic residue, and therefore  $n_{ij} = n_{ji}$ ,  $i, j = 0, 1, 2, 3$ . Further,

$$\sum_{j=0}^3 n_{ij} = \#\{(G_i \setminus \{p-1\})\},$$

and therefore

$$\sum_{j=0}^3 n_{0j} = \frac{p-1}{4} - 1, \quad \sum_{j=0}^3 n_{1j} = \sum_{j=0}^3 n_{2j} = \sum_{j=0}^3 n_{3j} = \frac{p-1}{4}.$$

There are further nontrivial relations in-between these numbers and some ideas how to obtain them are highlighted in [11]. Now by Proposition 3.3.7 the cyclic  $p$ -roots of simple index 4 on the  $x$ -level can be described by the solutions  $(c_0, c_1, c_2, c_3)$  of the following four equations:

$$\begin{aligned}
c_0 + \frac{1}{c_0} &= -\frac{p-5}{4} - n_{01} \left( \frac{c_0}{c_1} + \frac{c_1}{c_0} \right) - n_{02} \left( \frac{c_0}{c_2} + \frac{c_2}{c_0} \right) - n_{03} \left( \frac{c_0}{c_3} + \frac{c_3}{c_0} \right) \\
&\quad - n_{12} \left( \frac{c_1}{c_2} + \frac{c_2}{c_1} + \frac{c_1}{c_3} + \frac{c_3}{c_1} + \frac{c_2}{c_3} + \frac{c_3}{c_2} \right), \quad (3.28)
\end{aligned}$$

$$\begin{aligned}
c_1 + \frac{1}{c_1} &= -\frac{p-5}{4} - n_{01} \left( \frac{c_1}{c_2} + \frac{c_2}{c_1} \right) - n_{02} \left( \frac{c_1}{c_3} + \frac{c_3}{c_1} \right) - n_{03} \left( \frac{c_1}{c_0} + \frac{c_0}{c_1} \right) \\
&\quad - n_{12} \left( \frac{c_2}{c_3} + \frac{c_3}{c_2} + \frac{c_2}{c_0} + \frac{c_0}{c_2} + \frac{c_3}{c_0} + \frac{c_0}{c_3} \right), \quad (3.29)
\end{aligned}$$

$$\begin{aligned}
c_2 + \frac{1}{c_2} &= -\frac{p-5}{4} - n_{01} \left( \frac{c_2}{c_3} + \frac{c_3}{c_2} \right) - n_{02} \left( \frac{c_2}{c_0} + \frac{c_0}{c_2} \right) - n_{03} \left( \frac{c_2}{c_1} + \frac{c_1}{c_2} \right) \\
&\quad - n_{12} \left( \frac{c_3}{c_0} + \frac{c_0}{c_3} + \frac{c_3}{c_1} + \frac{c_1}{c_3} + \frac{c_0}{c_1} + \frac{c_1}{c_0} \right), \quad (3.30)
\end{aligned}$$

$$c_3 + \frac{1}{c_3} = -\frac{p-5}{4} - n_{01} \left( \frac{c_3}{c_0} + \frac{c_0}{c_3} \right) - n_{02} \left( \frac{c_3}{c_1} + \frac{c_1}{c_3} \right) - n_{03} \left( \frac{c_3}{c_2} + \frac{c_2}{c_3} \right) - n_{12} \left( \frac{c_0}{c_1} + \frac{c_1}{c_0} + \frac{c_0}{c_2} + \frac{c_2}{c_0} + \frac{c_1}{c_2} + \frac{c_2}{c_1} \right), \quad (3.31)$$

with  $n_{01}, n_{02}, n_{03}$  and  $n_{12}$  being given by Theorem 3.3.15.

*Remark 3.3.17.* It is easy to see that if  $(c_0, c_1, c_2, c_3)$  is a solution to the above system of equations, then so are  $(\overline{c_0}, \overline{c_1}, \overline{c_2}, \overline{c_3})$ ,  $(1/c_0, 1/c_1, 1/c_2, 1/c_3)$  and  $(1/\overline{c_0}, 1/\overline{c_1}, 1/\overline{c_2}, 1/\overline{c_3})$  as well as any cyclic permutation of these four.  $\square$

One can solve this system of equations by a straightforward application of the theory of Gröbner basis. There are two arising problems with this method, however. The first is that one encounters high degree (i.e. larger than 8) irreducible palindromic polynomials and it is unclear how to solve them by radicals. The second problem is that it is unclear how to describe the resulting Gröbner basis by explicit formulas depending on the prime  $p$ .

Currently we cannot solve this problem in full generality but we extract some solutions “by hand” in order to find the splitting field of the polynomials forming a pure lexicographic Gröbner basis of the system of equations (3.28)-(3.31). In particular, we solve the case  $(c_0, c_1, c_2, c_3) = (a, b, \bar{a}, \bar{b})$ , where  $a$  and  $b$  are unimodular, which is our main contribution to this section.

**Theorem 3.3.18.** *Let  $p$  be a prime number,  $p \equiv 1 \pmod{8}$ ,  $p = s^2 + t^2$  such that  $s \equiv 1 \pmod{4}$  and  $t > 0$ . Then there are two symmetric circulant complex Hadamard matrices of order  $p$  of simple index 4, corresponding to the two values of  $\zeta_{\pm} = \frac{2(-1 \pm \sqrt{p})}{p-1}$ , where  $(c_0, c_1, c_2, c_3) = (a, b, \bar{a}, \bar{b})$ , or any cyclic permutation of it, where*

$$a = \frac{\zeta_{\pm}}{2} + \sqrt{A + B\sqrt{p}} - \sqrt{C + D\sqrt{p}} + \mathbf{i} \sqrt{1 - \left( \frac{\zeta_{\pm}}{2} + \sqrt{A + B\sqrt{p}} - \sqrt{C + D\sqrt{p}} \right)^2}, \quad (3.32)$$

$$b = \frac{\zeta_{\pm}}{2} - \sqrt{A + B\sqrt{p}} + \sqrt{C + D\sqrt{p}} + \mathbf{i} \sqrt{1 - \left( \frac{\zeta_{\pm}}{2} - \sqrt{A + B\sqrt{p}} + \sqrt{C + D\sqrt{p}} \right)^2}, \quad (3.33)$$

where

$$A = \frac{2p(p-2s+1)}{t^2(p-1)^2}, \quad B = \pm \frac{2(p(s-2)+s)}{t^2(p-1)^2} \quad (3.34)$$

$$C = \frac{p(p(t^2+2)-4s-3t^2+2)}{t^2(p-1)^2}, \quad D = \pm \frac{2(p(s-2)+s+t^2)}{t^2(p-1)^2}, \quad (3.35)$$

such that the  $\pm$  signs in  $B$  and  $D$  agree with the sign in  $\zeta_{\pm}$ .

*Remark 3.3.19.* Note that  $a$  and  $b$  under (3.32) and (3.33) are well-defined, as

$$t^2(p-1)^2(A + B\sqrt{p}) = 2(-1 \pm \sqrt{p})^2 \sqrt{p}(\sqrt{p} \pm s) > 0, \text{ and}$$

$$t^2(p-1)^2(C + D\sqrt{p}) = (-1 \pm \sqrt{p})^2 \sqrt{p} (t^2(\sqrt{p} \pm 2) + 2(\sqrt{p} \pm s)) > 0,$$

where the  $\pm$  sign agrees with the sign in  $\zeta_{\pm}$ .  $\square$

*Proof.* We consider the system of equations (3.28)-(3.31) coming from Proposition 3.3.7 and impose the simplifying assumption  $c_2 = \overline{c_0}$  and  $c_3 = \overline{c_1}$  and relabel the variables  $a := c_0$  and  $b := c_1$  to avoid the excessive usage of the subscripts. As we are interested in constructing complex Hadamard matrices, we further assume that  $a$  and  $b$  are unimodular, and in particular  $a + 1/a = a + \overline{a} = 2\Re[a]$ . Therefore we find that the problem of solving the four equations (3.28)-(3.31) boils down to solving

$$2\Re[a] + \frac{p+2s-3}{4}\Re[a]^2 + \frac{p-2s+1}{4}\Re[b]^2 + \frac{p+2t-1}{4}\Re[a/b] + \frac{p-2t-1}{4}\Re[ab] = 1, \quad (3.36)$$

$$2\Re[b] + \frac{p+2s-3}{4}\Re[b]^2 + \frac{p-2s+1}{4}\Re[a]^2 + \frac{p+2t-1}{4}\Re[ab] + \frac{p-2t-1}{4}\Re[a/b] = 1. \quad (3.37)$$

Sum up and multiply by 2 (3.36)-(3.37), then expand  $\Re[ab]$  and  $\Re[a/b]$  to obtain

$$(p-1)(\Re[a] + \Re[b])^2 + 4(\Re[a] + \Re[b]) - 4 = 0.$$

In particular, we have arrived at a formula involving  $\zeta_{\pm}$ :

$$\Re[a] + \Re[b] = \frac{2(-1 \pm \sqrt{p})}{p-1} = \zeta_{\pm}.$$

Now let us substitute  $\Re[b] = \zeta_{\pm} - \Re[a]$  into (3.37) to get

$$4t\Im[a]\Im[b] = 2(\zeta_{\pm} - 2\Re[a])(2 + \zeta_{\pm}(s-1)). \quad (3.38)$$

Square both sides and eliminate  $\Im[a]^2 \equiv 1 - \Re[a]^2$ , rearrange to get

$$\begin{aligned} 16t^2\Re[a]^4 - 32t^2\zeta_{\pm}\Re[a]^3 + 16(\zeta_{\pm}^2(t^2 - (s-1)^2) + 4\zeta_{\pm}(1-s) - 2t^2 - 4)\Re[a]^2 \\ + 8(\zeta_{\pm}^3(ps - p + 2s^2 - 5s + 3) + 2\zeta_{\pm}^2(p + 6s - 7) + 4\zeta_{\pm}(t^2 - s + 5) - 8)\Re[a] \\ + 16t^2(1 - \zeta_{\pm}^2) - (\zeta_{\pm}^2(p + 2s - 3) + 8\zeta_{\pm} - 4)^2 = 0 \end{aligned} \quad (3.39)$$

Now it is easy to see that for a fixed  $\zeta_{\pm}$  the four roots of (3.39) are exactly the numbers

$$\Re[a]_{1,2,3,4} = \frac{\zeta_{\pm}}{2} \pm \sqrt{A + B\sqrt{p}} \pm \sqrt{C + D\sqrt{p}}, \quad (3.40)$$

by factoring out  $16t^2(\Re[a] - \Re[a]_1)(\Re[a] - \Re[a]_2)(\Re[a] - \Re[a]_3)(\Re[a] - \Re[a]_4)$  and reducing modulo the identity  $p = s^2 + t^2$  in order to obtain (3.39).

We proceed by showing that for  $\zeta_{\pm}$  fixed either of the sign choice  $(+, -)$  or  $(-, +)$  in (3.40) implies that  $|\Re[a]| \leq 1$ . Note that

$$C + D\sqrt{p} - (A + B\sqrt{p}) = \frac{\sqrt{p}(p\sqrt{p} - 3\sqrt{p} \pm 2)}{(p-1)^2} \geq 0 \quad (3.41)$$

for all relevant primes  $p$ , where the sign choice agrees with the sign choice of  $\zeta_{\pm}$ .

We begin by investigating the sign choice  $(+, -)$ . The case  $\Re[a] \leq 1$  is trivial by (3.41). To see the other bound rearrange to obtain, again, by (3.41)

$$0 \leq \sqrt{C + D\sqrt{p}} - \sqrt{A + B\sqrt{p}} \leq 1 + \frac{\zeta_{\pm}}{2}.$$

Now square in order to get, after a considerable amount of calculations,

$$\frac{2(-1 \pm \sqrt{p})^2(2p - 2t^2 \pm \sqrt{p}(2s - t^2))}{t^2(p - 1)^2} \leq 2\sqrt{AC + BDp + (AD + BC)\sqrt{p}},$$

which becomes, after squaring again

$$\frac{(-1 \pm \sqrt{p})^4(2p - 2t^2 \pm \sqrt{p}(2s - t^2))^2}{t^4(p - 1)^4} \leq \frac{2(-1 \pm \sqrt{p})^4 p (\sqrt{p} \pm s)(\sqrt{p}(2 + t^2) \pm 2(s + t^2))}{t^4(p - 1)^4}$$

which holds if and only if

$$0 \leq (2 \pm \sqrt{p})^2 t^2 (\sqrt{p} \pm s)^2.$$

The sign choice  $(-, +)$  follows along similar lines. The case  $-1 \leq \Re[a]$  is again trivial, while the other direction leads to equation

$$0 \leq \sqrt{C + D\sqrt{p}} - \sqrt{A + B\sqrt{p}} \leq 1 - \frac{\zeta_{\pm}}{2}.$$

After squaring and rearrangement we get

$$\frac{2(-1 \pm \sqrt{p})^2 \sqrt{p}(2\sqrt{p} \pm (2s + t^2))}{t^2(p - 1)^2} \leq 2\sqrt{AC + BDp + (AD + BC)\sqrt{p}},$$

which, after an additional squaring amounts to

$$\frac{(-1 \pm \sqrt{p})^4 p (2\sqrt{p} \pm (2s + t^2))^2}{t^4(p - 1)^4} \leq \frac{2(-1 \pm \sqrt{p})^4 p (\sqrt{p} \pm s)(\sqrt{p}(2 + t^2) \pm 2(s + t^2))}{t^4(p - 1)^4}.$$

Rearrange and reduce modulo  $s^2 + t^2 = p$  to finally obtain

$$0 \leq t^2(2p \pm 2\sqrt{p}s - t^2) = t^2(s \pm \sqrt{p})^2.$$

To conclude, observe that the sign of  $\Im[b]$  is determined by the sign of  $\zeta_{\pm} - 2\Re[a]$ , as the second factor of (3.38) is positive, and hence  $b$  is uniquely determined by  $a$ . It is easy to see that the solutions coming from any of the four possible values of  $a$  (for a fixed  $\zeta_{\pm}$ ) are exactly the four cyclic permutations of the initial solution  $(c_0, c_1, c_2, c_3) = (a, b, \bar{a}, \bar{b})$ , where  $a$  and  $b$  are given by (3.32) and (3.33).  $\square$

*Remark 3.3.20.* The reader might amuse him or herself by proving that the two-two other roots corresponding to the sign choice  $(+, +)$  and  $(-, -)$  in (3.40) will not lead to unimodular solutions. We do not include the details of this fruitless calculation.  $\square$

We do offer, however, the following enlightening

**Example 3.3.21.** Let  $p = 17$ . Choose a generator  $g = 3$  of  $\mathbb{Z}_{17}^*$ . Then we find that  $(s, t) = (1, 4)$ ,  $t > 0$  as required by (3.27), so we keep this generator and proceed. The four sets,  $G_0, G_1, G_2$  and  $G_3$  are defined as  $G_i := \{g^{4j+i} : j = 0, \dots, 16\}$ . We obtain  $G_0 = \{1, 4, 13, 16\}$ ,  $G_1 = \{3, 5, 12, 14\}$ ,  $G_2 = \{2, 8, 9, 15\}$  and  $G_3 = \{6, 7, 10, 11\}$ . Then for  $\zeta_+ = \frac{1}{8}(-1 + \sqrt{17})$  we find that  $(A, B, C, D) = \frac{1}{128}(17, -1, 17, 0)$  and we define

$$\begin{aligned}\Re[c_0] &:= \frac{-1 + \sqrt{17}}{16} + \sqrt{\frac{17}{128} - \frac{1}{128}\sqrt{17}} - \sqrt{\frac{17}{128}}, & \Im[c_0] &:= \sqrt{1 - \Re[c_0]^2}, \\ \Re[c_1] &:= \frac{-1 + \sqrt{17}}{16} - \sqrt{\frac{17}{128} - \frac{1}{128}\sqrt{17}} + \sqrt{\frac{17}{128}}, & \Im[c_1] &:= \sqrt{1 - \Re[c_1]^2}, \\ c_2 &= \overline{c_0}, & c_3 &= \overline{c_1}.\end{aligned}$$

Then  $H = \text{Circ}(1, c_0, c_2, c_1, c_0, c_1, c_3, c_3, c_2, c_2, c_3, c_3, c_1, c_0, c_1, c_2, c_0)$  is a circulant complex Hadamard matrix.

Similarly, for  $\zeta_- = \frac{1}{8}(-1 - \sqrt{17})$  we find that  $(A, B, C, D) = \frac{1}{128}(17, 1, 17, 0)$  and we define

$$\begin{aligned}\Re[c_0] &:= \frac{-1 - \sqrt{17}}{16} + \sqrt{\frac{17}{128} + \frac{1}{128}\sqrt{17}} - \sqrt{\frac{17}{128}}, & \Im[c_0] &:= \sqrt{1 - \Re[c_0]^2}, \\ \Re[c_1] &:= \frac{-1 - \sqrt{17}}{16} - \sqrt{\frac{17}{128} + \frac{1}{128}\sqrt{17}} + \sqrt{\frac{17}{128}}, & \Im[c_1] &:= \sqrt{1 - \Re[c_1]^2}, \\ c_2 &= \overline{c_0}, & c_3 &= \overline{c_1}.\end{aligned}$$

Then  $H = \text{Circ}(1, c_0, c_2, c_1, c_0, c_1, c_3, c_3, c_2, c_2, c_3, c_3, c_1, c_0, c_1, c_2, c_0)$  is a circulant complex Hadamard matrix. The two matrices are inequivalent, as they have different fingerprint.

A further useful contribution of Theorem 3.3.18 is that it reveals a field extension where additional cyclic  $p$ -roots of simple index 4 live. The following is an intriguing

**Corollary 3.3.22.** *All cyclic 17-roots of simple index 4 can be described by closed analytic formulae.*

*Proof.* Non-trivial use of computer algebra. Consult Appendix B for the details.  $\square$

The case  $p \equiv 5 \pmod{8}$  seems more difficult as we lose the symmetry in equation (3.26) of Proposition 3.3.7 as  $-1$  is not a quartic residue any longer. Despite the result highlighted in Corollary 3.3.22 the simple index 4 case remains open in general.

**Problem 3.3.23.** Give a detailed algebraic classification of all cyclic  $p$ -roots of simple index 4.

Finally, it is natural to ask if there are real circulant complex Hadamard matrices (cf. Conjecture 1.4.14). We offer the following possible attack to Ryser's conjecture.

**Problem 3.3.24.** Investigate if there are real cyclic  $n$ -roots by studying (3.19) and its possible real solutions.

Having investigated circulant complex Hadamard matrices it is also natural to study complex Hadamard matrices with circulant core. This topic is the subject of Appendix C, where we present some additional constructions along with some sporadic examples of complex Hadamard matrices. Some of the results are similar in spirit (cf. Propositions C.1.8 and C.1.9 with Theorem 3.3.18), while others are rather technical (see Theorem C.2.6), and rely heavily on computer algebra. The main result of the supplement is the discovery of a new complex Hadamard matrix of order 7, which we summarize in the following

**Example 3.3.25.** Let

$$\alpha = \frac{40169}{3} + \frac{50\sqrt{1993741}}{3} \cos \left( \frac{1}{3} \arccos \left( \frac{2731019453\sqrt{1993741}}{1993741^2} \right) - \frac{4\pi}{3} \right), \quad (3.42)$$

$$\begin{aligned} h(u) = & 2054570000u^6 + 4109140000u^5 + (16\alpha^2 + 9768064\alpha - 5227993936)u^4 \\ & + (1956\alpha^2 + 64132324\alpha - 12170223176)u^3 + (11393\alpha^2 + 427075897\alpha \\ & + 1676016222)u^2 + (4644\alpha^2 + 2280446676\alpha + 8524444776)u \\ & - 17074\alpha^2 + 3269963754\alpha + 2727593304. \end{aligned} \quad (3.43)$$

The six real roots of  $h(u)$ ,  $r_1 < r_2 < r_3 < r_4 < r_5 < r_6$ , describe twice the real part of six unimodular numbers  $z_i = r_i/2 + \mathbf{i}\sqrt{1 - r_i^2/4}$ ,  $i = 1, 2, \dots, 6$ . In particular,  $\text{Circ}([z_1, z_3, \overline{z_2}, z_4, \overline{z_5}, \overline{z_6}])$ , bordered by a row and column of numbers 1 is a new example of complex Hadamard matrices of order 7, which we call  $Q_7$ . We remark here that the entries of  $Q_7$  can be expressed by radicals (see Proposition C.2.10).

### 3.4 Hadamard matrices with few different entries

In the preceding section we found examples of complex Hadamard matrices containing only a “few” different entries. This restriction on the matrices allowed us to solve the otherwise extremely complicated orthogonality equations resulting in analytic examples of complex Hadamard matrices. It is natural to investigate this problem in more generality. As a trivial warm-up result we note that the Fourier matrix  $F_1$  is the only complex Hadamard matrix in which all entries are equal.

### 3.4.1 Two different entries

Real Hadamard matrices contain two different entries only, and it is natural to ask what other complex Hadamard matrices have this property. Clearly, if  $H$  is such a matrix, then so is  $aH$  for all unimodular numbers  $a$ , and therefore we can suppose, up to equivalence, that one of the two entries in  $H$  is 1.

**Example 3.4.1.** The following are complex Hadamard matrices with two different entries. Note that they are not scalar multiples of the real Hadamard matrix  $F_2$ .

$$\begin{bmatrix} 1 & \mathbf{i} \\ \mathbf{i} & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & -\mathbf{i} \\ -\mathbf{i} & 1 \end{bmatrix}, \quad \begin{bmatrix} \mathbf{i} & 1 \\ 1 & \mathbf{i} \end{bmatrix}, \quad \begin{bmatrix} -\mathbf{i} & 1 \\ 1 & -\mathbf{i} \end{bmatrix}.$$

We have given a non-trivial construction of complex Hadamard matrices with two different entries in [132] (cf. [133]) by design theoretical means.

**Definition 3.4.2.** A  $2$ -( $v, k, \lambda$ ) *design* is a  $v \times v$   $(0, 1)$ -matrix  $X$  such that  $XJ = JX = kJ$  and  $XX^T = (k - \lambda)I + \lambda J$ . We say that a  $2$ -( $4m - 1, 2m - 1, m - 1$ ) design is a *Hadamard design*.

*Remark 3.4.3.* If  $X$  is a Hadamard design, then  $2X - J$  is the core of a real Hadamard matrix. Conversely, if  $H$  is a dephased real Hadamard matrix, then its core becomes a Hadamard design after replacing its  $-1$  entries with 0.  $\square$

*Remark 3.4.4.* If  $X$  is  $2$ -( $v, k, \lambda$ ) design, then  $J - X$  is  $2$ -( $v, v - k, v - 2k + \lambda$ ) design. We say that  $X$  and  $J - X$  are the complement of each other.  $\square$

**Theorem 3.4.5** (see [132], [133]). *Let  $X$  be a Hadamard design, and replace every number 0 in it with the complex unimodular number*

$$a = -1 + \frac{1}{2m} \pm \mathbf{i} \frac{\sqrt{4m - 1}}{2m}. \quad (3.44)$$

*Then the obtained matrix is a complex Hadamard matrix with two different entries.*

*Remark 3.4.6.* We readily see that if  $H = X + a(J - X)$  is a complex Hadamard matrix, coming from Theorem 3.4.5, then  $\bar{a}H = (J - X) + \bar{a}(J - (J - X))$ . Hence the same construction works when  $X$  is the complement of a Hadamard design.  $\square$

**Example 3.4.7.** By considering the  $2$ -( $7, 3, 1$ ) Hadamard design  $X$ , one can obtain a complex Hadamard matrix  $H$  of order 7, with two different entries as follows:

$$X = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix} \rightsquigarrow H = \begin{bmatrix} a & 1 & a & 1 & a & 1 & a \\ 1 & a & a & 1 & 1 & a & a \\ a & a & 1 & 1 & a & a & 1 \\ 1 & 1 & 1 & a & a & a & a \\ a & 1 & a & a & 1 & a & 1 \\ 1 & a & a & a & a & 1 & 1 \\ a & a & 1 & a & 1 & 1 & a \end{bmatrix}, \quad a = -\frac{3}{4} + \mathbf{i} \frac{\sqrt{7}}{4}.$$

Note that the matrix  $H$  is equivalent to a circulant one (cf. Theorem 3.3.9).

Chan and Godsil investigated inverse-orthogonal (or type-II) matrices with two different entries. From their analysis it follows that the aforementioned examples are the only possibilities.

**Theorem 3.4.8** (Chan–Godsil, [25]). *Let  $X$  be a  $(0, 1)$ -matrix. Then  $H = X + a(J - X)$  is a complex Hadamard matrix if and only if*

- (a)  $H$  is a real Hadamard matrix; or
- (b)  $H$  is one of the  $2 \times 2$  complex Hadamard matrices from Example 3.4.1; or
- (c)  $X$  or  $J - X$  is a Hadamard design and hence  $H$  comes from Theorem 3.4.5.

Therefore complex Hadamard matrices with two different entries are scalar multiples of these examples. Note that for every prime  $p \equiv 3 \pmod{4}$  Part (c) leads to complex Hadamard matrices of order  $p$  (cf. Theorem 1.1.17).

### 3.4.2 Three different entries

A full classification of complex Hadamard matrices with three different entries is currently not available, and as far as we can tell is far out of reach. In what follows we enlist several constructions yielding various examples, but it is unknown whether our list is exhaustive.

The principal examples are, of course, the  $BH(n, 3)$  matrices (see Definition 1.4.1). From Part 1 of Theorem 1.4.4 it follows that they can exist only if  $n \equiv 0 \pmod{3}$ . We mention here two constructions, coming from real Hadamard matrices.

Contrary to the two-entry case, there is no restriction on the entries here in general. The following was pointed out by R. Craigen:<sup>1</sup>

**Lemma 3.4.9.** *Let  $H$  be a normalized real Hadamard matrix of order  $n \geq 2$ . Then, after multiplying the first row of  $H$  by a nonreal unimodular complex number  $a$  one obtains a complex Hadamard matrix with three different entries.*

Of course, we do not get new examples of complex Hadamard matrices this way as all these matrices are equivalent to the underlying real Hadamard matrix.

**Example 3.4.10.** Let  $a \neq \pm 1$ . Then the following is a complex Hadamard matrix with three different entries:

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

---

<sup>1</sup>Private communication.



It turns out, however, that in square orders one can obtain inequivalent matrices as well. We recall the following powerful construction.

**Theorem 3.4.11** (see e.g. [66]). *For every positive integer  $n$  there is a self-adjoint complex Hadamard matrix of order  $n^2$  with constant diagonal.*

*Proof.* Let  $H$  be any complex Hadamard matrix of order  $n$ , and let us denote its rows by  $h_1, h_2, \dots, h_n$ . Consider the following block matrix, where the  $(i, j)$ th entry of  $K$  is the rank-1 block  $h_j^* h_i$ :

$$K = \begin{bmatrix} h_1^* h_1 & \cdot & \cdot & h_n^* h_1 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ h_1^* h_n & \cdot & \cdot & h_n^* h_n \end{bmatrix}. \quad (3.45)$$

We show that  $K$  is Hadamard. Indeed: consider its  $i$ th row. We have

$$\sum_{k=1}^n (h_k^* h_i)(h_i^* h_k) = \sum_{k=1}^n h_k^* (h_i h_i^*) h_k = n \sum_{k=1}^n h_k^* h_k = n^2 I_n. \quad (3.46)$$

Also, for rows  $i \neq j$  recalling that the rows of  $H$  are complex orthogonal

$$\sum_{k=1}^n (h_k^* h_i)(h_j^* h_k) = \sum_{k=1}^n h_k^* (h_i h_j^*) h_k = O_n, \quad (3.47)$$

where  $O_n$  stands for the all 0 matrix of order  $n$ . Clearly,  $K$  is self-adjoint by construction, and its diagonal is constant 1.  $\square$

This construction naturally leads to parametric families of complex Hadamard matrices.

**Proposition 3.4.12** (see [132]). *Suppose that  $H$  is a dephased complex Hadamard matrix of order  $n$  with  $m$  free parameters. Then there is a complex Hadamard matrix of order  $n^2$  with  $m + (n-1)^2$  free parameters, moreover there is a self-adjoint complex Hadamard matrix with constant diagonal featuring  $m + (n-1)(n-2)/2$  free parameters.*

*Proof.* Indeed, as one is free to replace the blocks of  $K$   $h_j^* h_i$  in (3.45) with  $x_{i,j} h_j^* h_i$  for  $2 \leq i, j \leq n$  in Theorem 3.4.11, as this operation does not affect the validity of equations (3.46) and (3.47). Moreover, if the unimodular variables  $x_{i,j}$  are chosen in a way that  $x_{i,i} = 1$  and  $x_{i,j} = \bar{x}_{j,i}$  for every  $2 \leq i, j \leq n$ , then the resulting matrix is a self-adjoint complex Hadamard matrix with constant diagonal, as required. Note that the first  $m$  variables are featured in the first  $n$  rows of  $K$ , and therefore they are independent from the rest.  $\square$

**Corollary 3.4.13.** *If a real Hadamard matrix of order  $n$  exists, then so does a one-parameter family of complex Hadamard matrices with three different entries of order  $n^2$ .*

*Proof.* Consider a normalized real Hadamard matrix  $H$  of order  $n$ , and use Theorem 3.4.11 to obtain a normalized real Hadamard matrix of order  $n^2$ . Now observe that its upper left  $n \times n$  submatrix is  $J$ , and hence replacing it with  $aJ$ ,  $a \neq \pm 1$  will result in a one-parameter family of complex Hadamard matrices with three different entries, up to equivalence.  $\square$

Note that after dephasing the matrix the one-parameter remains in it, which however will contain four different entries:  $\{1, -1, a, -a\}$ .

**Example 3.4.14.** Let  $n = 2$ , and consider the real Hadamard matrix  $F_2$  from which we obtain the  $4 \times 4$  real Hadamard matrix via Theorem 3.4.11 and the corresponding parametric family it induces:

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \rightsquigarrow \left[ \begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ \hline 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{array} \right] \rightsquigarrow \left[ \begin{array}{cc|cc} a & a & 1 & 1 \\ a & a & -1 & -1 \\ \hline 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{array} \right].$$

Recall that  $C$  is a conference matrix of order  $n$  if  $C_{i,i} = 0$ ,  $i = 1, 2, \dots, n$  and all off-diagonal entries are  $\pm 1$ , such that  $CC^T = (n-1)I$ . We use symmetric conference matrices and show three additional methods resulting in complex Hadamard matrices with three different entries. The first is a folklore construction (cf. Theorem 1.4.18).

**Lemma 3.4.15.** *Let  $C$  be a symmetric conference matrix of order  $n$ . Then  $H = C \pm \mathbf{i}I$  is a complex Hadamard matrix with three different entries.*

*Proof.* Clearly  $H$  is unimodular, and

$$HH^* = (C \pm \mathbf{i}I)(C^T \mp \mathbf{i}I) = CC^T \pm \mathbf{i}(C^T - C) + I = nI. \quad \square$$

We give the following variation of this result.

**Proposition 3.4.16.** *Let  $C$  be a normalized, symmetric conference matrix of order  $n \geq 6$ . Then consider the matrix  $C + I$ , and replace in its core the off diagonal entries  $(1, -1)$  with  $(a, \bar{a})$ , respectively, where*

$$a = -\frac{2}{n-2} \pm \mathbf{i} \frac{\sqrt{n(n-4)}}{n-2}.$$

*The resulting matrix is a complex Hadamard matrix with three different entries  $\{1, a, \bar{a}\}$ .*

*Proof.* Consider the complex Hadamard matrix  $H$ , arising from the construction. Both of the numbers  $a$  and  $\bar{a}$  appear  $(n-2)/2$  times in every noninitial rows of  $H$ , and hence the first row is orthogonal to all subsequent one. It remains to be seen that the

noninitial rows are pairwise orthogonal. Consider the underlying conference matrix  $C$ . Clearly any two noninitial rows of it are permutation equivalent to either of the following  $2 \times n$  matrices:

$$\begin{bmatrix} 0 & 1 & \left| & 1 & 1 & -1 & -1 \right. \\ 1 & 0 & \left| & 1 & -1 & 1 & -1 \right. \end{bmatrix}, \quad \begin{bmatrix} 0 & -1 & \left| & 1 & 1 & -1 & -1 \right. \\ -1 & 0 & \left| & 1 & -1 & 1 & -1 \right. \end{bmatrix},$$

$n_1 \quad n_2 \quad n_3 \quad n_4 \qquad n_5 \quad n_6 \quad n_7 \quad n_8$

where the column labels  $n_1, n_5, n_2, n_6, n_3, n_7$  and  $n_4, n_8$  are nonnegative integral numbers describing how many columns of type  $(1, 1)^T, (1, -1)^T, (-1, 1)^T$  and  $(-1, -1)^T$  are present in the matrices, respectively. From the orthogonality of  $C$  it is elementary to deduce that

$$n_1 = n_2 = n_3 = n_4 = \frac{n-2}{4}, \quad n_5 = \frac{n+2}{4}, \quad n_6 = n_7 = \frac{n-2}{4}, \quad n_8 = \frac{n-6}{4}$$

and as a result the orthogonality conditions between the noninitial rows of  $H$  read

$$\begin{aligned} 1 + a + \bar{a} + \frac{n-6}{4} + \frac{n-2}{4} (a^2 + \bar{a}^2) + \frac{n-2}{4} &= 0, \\ 1 + a + \bar{a} + \frac{n-2}{4} + \frac{n-2}{4} (a^2 + \bar{a}^2) + \frac{n-6}{4} &= 0. \end{aligned}$$

These two conditions are the same, which hold identically by the choice of  $a$ .  $\square$

*Remark 3.4.17.* By setting  $n = 6$  in Proposition 3.4.16 we obtain the  $BH(6, 3)$  matrix  $S_6^{(0)}$  (see Example 2.2.1).  $\square$

Another construction from [132] is the following.

**Theorem 3.4.18** (see [132], [133]). *Let  $C$  be a normalized, symmetric conference matrix of order  $n \geq 6$ . Discard the first row and column of  $C$  and replace in the remaining matrix the numbers  $(0, 1, -1)$  with  $(1, a, \bar{a})$ , respectively, where*

$$a = \frac{-1 \pm_A \sqrt{n-1}}{n-2} \pm_B \mathbf{i} \frac{\sqrt{n^2 - 5n + 4 \pm_A 2\sqrt{n-1}}}{n-2},$$

where  $\pm_A$  is the sign of  $\sqrt{n-1}$  and  $\pm_B$  is the sign of the nested radical, respectively. The resulting matrix is a complex Hadamard matrix of order  $n-1$  with three different entries  $\{1, a, \bar{a}\}$ .

*Remark 3.4.19.* By setting  $n = 6$  in Theorem 3.4.18 we obtain the Fourier matrix  $F_5$ . For  $n = 10$  we get a  $BH(9, 3)$  matrix along with an additional example. In general the construction describes at least two inequivalent complex Hadamard matrices.  $\square$

The constructions given by Theorems 3.4.5 and 3.4.18 contain Theorems 3.3.9 and 3.3.10 as special cases, and hence they describe various complex Hadamard matrices of prime orders. It would be particularly interesting to find analogous constructions in the simple index 3 and 4 cases as well.

**Problem 3.4.20.** Generalize the simple index 3 and simple index 4 type complex Hadamard matrices for non-prime orders as well.

Finally, we remark here that Chan has given an algebraic description of those complex Hadamard matrices  $H = I + aX + b(J - I - X)$ , where  $X$  is the adjacency matrix of a strongly regular graph very recently [24], and hence obtained complex Hadamard matrices with at most three different entries. It would be very interesting to see if the following more general problem can be treated by purely algebraic methods as well.

**Problem 3.4.21.** Give a complete characterization of complex Hadamard matrices with three different entries.

### 3.5 Application: Equiangular tight frames

In this section we give another application of complex Hadamard matrices and relate them to complex equiangular tight frames. The concepts are similar to what was discussed in Section 2.4.4 but in contrast here we are interested in equiangular lines having a prescribed angle. The main objects we are concerned with is described in the following

**Definition 3.5.1.** Let  $\mathcal{H}$  be a complex Hilbert space, and let  $F = \{f_i\}_{i \in I} \subset \mathcal{H}$  be a subset. We call  $F$  a *frame* for  $\mathcal{H}$  provided that there are two constants  $C, D > 0$  such that the inequality

$$C \|x\|^2 \leq \sum_{i \in I} |\langle x, f_i \rangle|^2 \leq D \|x\|^2$$

holds for every  $x \in \mathcal{H}$ . When  $C = D = 1$  then the frame is called normalized, tight (also called a Parseval frame).

Real and complex equiangular tight frames have been heavily investigated recently (see e.g. [12], [23], [46], [53] and [117]) as they have applications in coding [65] and quantum information theory [122]. Here we shall discuss only Parseval frames for the  $k$  dimensional complex Hilbert space, equipped with the usual inner product. We use the term  $(n, k)$  frame to refer to a Parseval frame consisting of  $n$  vectors in  $\mathbb{C}^k$ . Every such Parseval frame induces an isometric embedding of  $\mathbb{C}^k$  into  $\mathbb{C}^n$  with the map

$$V: \mathbb{C}^k \rightarrow \mathbb{C}^n, (Vx)_j = \langle x, f_j \rangle, \text{ for all } 1 \leq j \leq n$$

which is called the analysis operator of the frame. As  $V$  is linear, we can identify it with an  $n \times k$  matrix and the frame vectors  $\{f_1, \dots, f_n\}$  are the respective columns of  $V^*$ . A standard argument shows [65] that an  $(n, k)$  frame is determined up to a

natural unitary equivalence by its Gram matrix  $VV^*$ , which is a self-adjoint projection of rank  $k$ , moreover, if the frame is uniform and equiangular (i.e.  $\|f_i\|^2$  and  $|\langle f_i, f_j \rangle|$  are constants for all  $1 \leq i \leq n$  and for all  $i \neq j$ ,  $1 \leq i, j \leq n$ , respectively), it follows that the Gram matrix of the frame reads

$$VV^* = \frac{k}{n}I_n + \sqrt{\frac{k(n-k)}{n^2(n-1)}}Q,$$

where  $Q$  is a self-adjoint matrix with vanishing diagonal and unimodular off-diagonal entries. We refer to such frames as equiangular tight frames. The matrix  $Q$  is called the Seidel matrix [99], signature matrix (or a generalized conference matrix, [25]) associated with the  $(n, k)$  frame. Recall from Lemma 2.4.30 that  $n \leq k^2$ . The following provides an elegant characterization of complex equiangular frames (see [99] and [100] for the real case).

**Theorem 3.5.2** (Holmes–Paulsen, [65]). *Let  $Q$  be a self-adjoint  $n \times n$  matrix with  $Q_{ii} = 0$  and  $|Q_{ij}| = 1$  for all  $i \neq j$ . Then the following are equivalent:*

- (a)  $Q$  is the signature matrix of an equiangular  $(n, k)$  frame for some  $k$ ;
- (b)  $Q^2 = (n-1)I + \mu Q$  for some necessarily real  $\mu$ ; and
- (c)  $Q$  has exactly two eigenvalues.

Note that the value  $k$  above depends on  $n$  and  $\mu$  only. In particular (see [12]), we have

$$k = \frac{n}{2} - \frac{\mu n}{2\sqrt{4(n-1) + \mu^2}}. \quad (3.48)$$

It follows that if  $Q$  is a signature matrix of an  $(n, k)$  frame, then  $-Q$  is a signature matrix of an  $(n, n-k)$  frame. Let us recall here a quick

**Example 3.5.3** (Bodmann et al. [13]). The matrix

$$Q_9 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \omega & \omega & \omega & \omega^2 & \omega^2 & \omega^2 \\ 1 & 1 & 0 & \omega^2 & \omega^2 & \omega^2 & \omega & \omega & \omega \\ 1 & \omega^2 & \omega & 0 & \omega & \omega^2 & 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega & \omega^2 & 0 & \omega & \omega & \omega^2 & 1 \\ 1 & \omega^2 & \omega & \omega & \omega^2 & 0 & \omega^2 & 1 & \omega \\ 1 & \omega & \omega^2 & 1 & \omega^2 & \omega & 0 & \omega^2 & \omega \\ 1 & \omega & \omega^2 & \omega^2 & \omega & 1 & \omega & 0 & \omega^2 \\ 1 & \omega & \omega^2 & \omega & 1 & \omega^2 & \omega^2 & \omega & 0 \end{bmatrix}, \quad (3.49)$$

where  $\omega$  is the principal cubic root of unity, is a  $9 \times 9$  nontrivial cube root signature matrix of an equiangular  $(9, 6)$ -frame.

The matrix  $Q_9$  was the original object which raised our interest in frame theory. One can observe immediately, that the matrix  $Q_9$  is “almost” a complex Hadamard matrix: indeed,  $H = Q_9 + I$  is complex Hadamard. The following result explains this phenomenon.

**Theorem 3.5.4** (see [130], cf. [24]). *Let  $Q$  be a self-adjoint  $n \times n$  matrix with  $Q_{ii} = 0$  and  $|Q_{ij}| = 1$  for all  $i \neq j$ . Then the following are equivalent:*

- (a)  $Q^2 = (n-1)I + \mu Q$  for some necessarily real  $-2 \leq \mu \leq 2$ ; and
- (b)  $H := Q + \lambda I$  is a complex Hadamard matrix for  $\lambda = -\mu/2 \pm \mathbf{i}\sqrt{1 - |\mu|^2/4}$ .

*Proof.* Suppose that we have a signature matrix  $Q$  satisfying (a). Then, as the number  $\lambda$  defined in (b) is unimodular we find that  $H = Q + \lambda I$  is a unimodular matrix, moreover we have

$$HH^* = (Q + \lambda I)(Q^* + \bar{\lambda}I) = nI + \mu Q + 2\Re[\lambda]Q = nI,$$

as required. Conversely, let us suppose that we have a complex Hadamard matrix  $H$  with constant diagonal  $\lambda$ , such that the matrix  $Q := H - \lambda I$  is self-adjoint. Then, we find that

$$Q^2 = QQ^* = (H - \lambda I)(H^* - \bar{\lambda}I) = (n+1)I - \lambda(Q + \lambda I)^* - \bar{\lambda}(Q + \lambda I) = (n-1)I - 2\Re[\lambda]Q,$$

and, as  $\lambda$  is unimodular, the statement (a) follows.  $\square$

In [12]  $n$ th root signature matrices were investigated extensively where the following result was obtained.

**Theorem 3.5.5** (Bodmann–Elwood, [12]). *For every  $n \geq 2$  there is a self-adjoint complex Hadamard matrix of order  $n^2$  with constant diagonal composed of  $n$ th roots of unity. Consequently there is a nontrivial  $n$ th root signature matrix corresponding to an equiangular  $(n^2, n(n+1)/2)$  frame.*

Bodmann and Elwood used a direct, elementary argument concluding that the Fourier matrices of order  $n$  can be lifted to order  $n^2$  yielding the result. This, however, still left unanswered an earlier question from [13], namely whether or not an equiangular  $(36, 21)$  frame, whose signature matrix is composed from cubic root of unity exists. Our observation is that Theorem 3.5.5 follows from Theorem 3.4.11 rather easily and in particular various Butson-Hadamard matrices (see Definition 1.4.1) can be used instead of the Fourier matrices resulting in signature matrices, composed from roots of unity.

**Corollary 3.5.6.** *For every prime  $p$  there is a nontrivial  $p$ th root signature matrix of order  $4^a p^{2b}$  for all  $0 \leq a \leq b$  corresponding to an equiangular  $(4^a p^{2b}, 2^a p^b(2^a p^b + 1)/2)$  frame.*

*Proof.* Combine Part 2 of Theorem 1.4.4 with Theorem 3.4.11.  $\square$

Setting  $p = 3$  and  $a = b = 1$  in Corollary 3.5.6 above, we immediately get an answer to one of the questions raised in [13].

**Corollary 3.5.7.** *There is a nontrivial cube root signature matrix of order 36 leading to an equiangular  $(36, 21)$  frame.*

In the corollary above we used the matrix  $S_6^{(0)}$  (see Example 2.2.1).

The case  $|\mu| = 2$  in Part (b) of Theorem 3.5.4 corresponds to self-adjoint complex Hadamard matrices with constant diagonal which, however, can exist in square orders only (see Lemma 2.2.10).

Next we give examples of frames in which the corresponding complex Hadamard matrices are not self-adjoint. In particular,  $|\mu| \neq 2$ . We recall that a  $2-(4m-1, 2m-1, m-1)$  Hadamard-design  $A$  is skew if  $A + A^T + I = J$ . We have the following

**Proposition 3.5.8.** *Suppose that we have a skew Hadamard design  $U$  of order  $n$ . Then there exists a complex Hadamard matrix  $H$  of order  $n$  with diagonal entries  $\lambda$ , such that the matrix  $Q := H - \lambda I$  is self-adjoint.*

*Proof.* Use Theorem 3.4.5 to exhibit a complex Hadamard matrix  $K = U + aU^T + aI$  where  $a$  is the unimodular complex number defined in (3.44). Now multiply this matrix with the unimodular number  $\sqrt{a}$  to obtain the matrix  $H = \sqrt{a}K = \sqrt{a}U + \sqrt{a}U^T + \sqrt{a}I$ .  $\square$

It is well-known that the Paley-type Hadamard designs of prime orders, described by Theorem 1.1.17 are skew, moreover it is conjectured that skew Hadamard designs exist for every order  $n = 4m - 1$  [89]. Therefore we have infinitely many equiangular tight frames coming from Proposition 3.5.8. In particular, we have the following

**Corollary 3.5.9** (Renes, [117]). *Suppose that we have a skew Hadamard design of order  $n \geq 3$ . Then there are equiangular  $(n, (n-1)/2)$  and  $(n, (n+1)/2)$  frames.*

Hence, if the conjecture regarding the existence of skew Hadamard matrices is true, then we have equiangular tight frames with parameters  $(2k - (-1)^k, k)$  for every  $k$ .

An interesting question is to ask if it is possible to construct  $(k^2, k)$  equiangular frames from complex Hadamard matrices. These type of frames are equivalent to SIC-POVMs [82], [122], and have many interesting applications in quantum information

theory. Unfortunately, equation (3.48) leads to  $\mu = \sqrt{k+1}(k-2)$  which, combined with the bound  $|\mu| \leq 2$ , implies that  $k = 2$  or  $3$ . The case  $k = 2$  easily leads to the signature matrix described in Example 2.4.32, while the case  $k = 3$  implies that  $\mu = 2$  which corresponds to, for example, the one-parameter signature matrix  $-Q_9(a)$ , where  $Q_9(a) + I$  is the family of complex Hadamard matrices coming from Proposition 3.4.12, applied to the starting-point complex Hadamard matrix  $Q_9 + I$  (see formula (3.49)).

So far the ideas mentioned in this section considered the Gram matrix of the configurations. However, in all known construction methods of  $(k^2, k)$  equiangular tight frames the frame vectors are obtained directly via the following way. We start with a so-called fiducial vector  $\phi \in \mathbb{C}^k$  and a group  $G$  of  $k \times k$  matrices. The group is fixed, and the idea is to choose  $\phi$  so that  $\{M\phi : M \in G\}$  spans a set of equiangular lines. We illustrate this approach throughout the following remarkable

**Example 3.5.10** (Hoggar, [64]). Let  $X$ ,  $Y$  and  $Z$  be the Pauli matrices, namely

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad Y = \mathbf{i}XZ = \begin{bmatrix} 0 & -\mathbf{i} \\ \mathbf{i} & 0 \end{bmatrix},$$

and let  $G = \{I, X, Y, Z\}^{\otimes 3}$  and

$$\phi = \frac{\sqrt{3}}{12} \begin{bmatrix} 0, 0, \tau, \bar{\tau}, \tau, -\tau, 0, \sqrt{2} \end{bmatrix}^T,$$

where  $\tau = (1 + \mathbf{i})/\sqrt{2}$  is the principal eighth root of unity. Then  $V^* = \{A\phi : A \in G\}$  is an equiangular  $(64, 8)$  frame. Moreover, the Gram matrix of the configuration reads

$$VV^* = \frac{1}{8}I + \frac{1}{24}Q,$$

where the signature matrix  $Q$  is composed of fourth roots of unity.

One cannot but wonder what combinatorial objects correspond to the signature matrices of  $(k^2, k)$  equiangular tight frames for  $k \geq 4$ .



# Bibliography

- [1] S. S. AGAIAN: *Hadamard Matrices and Their Applications*, Springer-Verlag: Lecture Notes in Mathematics, (1985).
- [2] I. A. AIZENBERG, A.P. YUZHAKOV: *Integral representations and Residues in Multidimensional Complex Analysis*, Translations of Mathematical Monographs, **58**, Amer. Math. Soc (1983).
- [3] D. M. APPLEBY, I. BENGTTSSON, S. BRIERLEY, M. GRASSL, D. GROSS, J.-Å. LARSSON: *The monomial representations of the Clifford group*, Preprint, arXiv: 1102.1268v2 [quant-ph] (2011).
- [4] K. T. ARASU, W. DE LAUNEY, S. L. MA: *On circulant complex Hadamard matrices*, *Designs, Codes and Cryptography*, **25**, 123–142 (2002).
- [5] J. BACKELIN: *Square multiples  $n$  gives infinite many cyclic  $n$ -roots*, *Reports, Matematiska Institutionen, Stockholms Universitet*, **8**, (1989).
- [6] K. BEAUCHAMP, R. NICOARĂ: *Orthogonal maximal Abelian  $*$ -subalgebras of the  $6 \times 6$  matrices*, *Linear Algebra and its Applications*, **428**, 1833–1853 (2008).
- [7] V. BELEVITCH: *Theory of  $2n$ -terminal networks with application to conference telephony*, *Elect. Commun.*, **27**, 231–234 (1950).
- [8] I. BENGTTSSON, W. BRUZDA, Å. ERICSSON, J.-Å. LARSSON, W. TADEJ, K. ŻYCKOWSKI: *Mutually unbiased bases and Hadamard matrices of order 6*, *J. Math. Phys.*, **48**, 052106 (2007).
- [9] G. BJÖRCK: *Functions of modulus one on  $\mathbb{Z}_p$ , whose Fourier transform have constant modulus, and “cyclic  $n$ -roots”*, *Recent Advances in Fourier Analysis and its Applications* (J. S. Byrnes and J. F. Byrnes, eds.), NATO Adv. Sci. Inst. Ser. C: Math. Phys. Sci., Kluwer, **315**, 131–140 (1989).
- [10] 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).

- [11] G. BJÖRCK, U. HAAGERUP: *All cyclic  $p$ -roots of index 3 found by symmetry-preserving calculations*, Preprint, arXiv: 0803.2506v1 [math.AC] (2008).
- [12] B. G. BODMANN, H. J. ELWOOD: *Complex Equiangular Parseval Frames and Seidel Matrices containing  $p$ th roots of unity*, Proceedings of the American Mathematical Society, **138**, 4387–4404 (2010).
- [13] B. G. BODMANN, V. I. PAULSEN, M. TOMFORDE: *Equiangular tight frames from complex Seidel matrices containing cube roots of unity*, Linear Algebra and its Applications, **430**, 396–417 (2009).
- [14] S. BOUGUEZEL, M. O. AHMED, M. N. S. SWAMI: *A new class of reciprocal-orthogonal parametric transforms*, IEEE Trans. Circuits and Syst. I, **56**, 795–805 (2009).
- [15] S. BRIERLEY, S. WEIGERT: *Constructing Mutually Unbiased Bases in Dimension Six*, Phys. Rev. A, **79**, 052316 (2009).
- [16] S. BRIERLEY, S. WEIGERT: *Maximal Sets of Mutually Unbiased Quantum States in Dimension Six*, Phys. Rev. A, **78**, 042312 (2008).
- [17] S. BRIERLEY, S. WEIGERT, I. BENGTTSSON: *All Mutually Unbiased Bases in Dimensions Two to Five*, Quantum Info. & Comp., **10**, 0803–0820 (2010).
- [18] B. W. BROCK: *Hermitian congruence and the existence and completion of generalised Hadamard matrices*, J. Combin. Theory A, **49**, 233–261 (1988).
- [19] W. BRUZDA, W. TADEJ, K. ŻYCZKOWSKI: *On-line repository of complex Hadamard matrices*, <http://chaos.if.uj.edu.pl/~karol/hadamard>
- [20] B. BUCHBERGER: *An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal*, PhD thesis, Mathematical Institute, University of Innsbruck, Austria, (1965).
- [21] A. T. BUTSON: *Generalized Hadamard matrices*, Proc. Am. Math. Soc., **13**, 894–898 (1962).
- [22] P. J. CAMERON, J. J. SEIDEL: *Quadratic forms over  $GF(2)$* , Indag. Math., **35**, 1–8 (1973).
- [23] P. G. CASAZZA, D. REDMOND, J. C. TREMAIN: *Real Equiangular Frames*, CISS Meeting, Princeton, NJ (available at <http://www.framerc.org>) (2008).

- [24] A. CHAN: *Complex Hadamard Matrices and Combinatorial Structures*, Preprint, (2011).
- [25] A. CHAN, C. GODSIL: *Type-II Matrices and Combinatorial Structures*, *Combinatorica*, **30**, 1–24 (2010).
- [26] A. COHN: *Über die Anzahl der Wurzeln einer algebraischen Gleichung in einem Kreise*, *Math. Zeit.*, **14**, 110–148 (1922).
- [27] C. J. COLBOURN, J. DINITZ, eds.: Chapter V., *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, (1996).
- [28] B. COMPTON, R. CRAIGEN, W. DE LAUNEY: *Unreal  $BH(n, 6)$ 's and Hadamard matrices*, Preprint, (2008).
- [29] J. COOPER, J. MILAS, W. D. WALLIS: *Lecture Notes in Mathematics*, Volume 686/1978, 126–135 (1978).
- [30] D. COPPERSMITH, J. STEINBERGER: *On the entry sum of cyclotomic arrays*, *Integers*, **6**, 2206 (2007).
- [31] E. M. COVEN, A. D. MEYEROWITZ: *Tiling the integers with translates of one finite set*, *J. Algebra*, **212**, 161–174 (1999).
- [32] R. CRAIGEN: *Constructions for Orthogonal Matrices*, PhD thesis, University of Waterloo, (1991).
- [33] R. CRAIGEN: *Embedding rectangular matrices in Hadamard matrices*, *Linear and Multilinear Algebra*, **29**, 91–92 (1991).
- [34] R. CRAIGEN: *Equivalence classes of inverse orthogonal and unit Hadamard matrices*, *Bull. Austral. Math. Soc.*, **44**, 109–115 (1991).
- [35] R. CRAIGEN: *Personal Web page*,  
<http://home.cc.umanitoba.ca/~craigennr/PWP/> (accessed October 1, 2011).
- [36] R. CRAIGEN: *Signed Groups, Sequences, and the Asymptotic existence of Hadamard matrices*, *J. Combin. Th. Ser. A*, **71**, 241–254 (1995).
- [37] R. CRAIGEN, W. HOLZMANN, H. KHARAGHANI: *Complex Golay Sequences: Structure and applications*, *Discrete Math.*, **252**, 73–89 (2002).
- [38] Y. DAI, S. KIM, M. KOJIMA: *Computing All Nonsingular Solutions of Cyclic- $n$  Polynomial Using Polyhedral Homotopy Continuation Methods*, *J. of Computational and Applied Mathematics*, **152**, 83–97 (2003).

- [39] D. DE CAEN: *Large equiangular sets of lines in Euclidian space*, The Electronic J. Combin., **7**, Research Paper 55, 3 pp. (2000).
- [40] 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).
- [41] W. DE LAUNEY, D. M. GORDON: *A comment on the Hadamard conjecture*, Journal of Combinatorial Theory Series A, **95**, 180–184 (2001).
- [42] W. DE LAUNEY, D. M. GORDON: *On the density of the set of known Hadamard orders*, Cryptography and Communications: Discrete Structures, Boolean Functions and Sequences, **2**, 233–246 (2010).
- [43] P. DIȚĂ: *Hadamard Matrices from mutually unbiased bases*, J. Math. Phys., **51**, 072202 (2010).
- [44] P. DIȚĂ: *Some results on the parametrization of complex Hadamard matrices*, J. Phys. A: Math. Gen., **37**, 5355–5374 (2004).
- [45] D. Ž. ĐOKOVIĆ: *Hadamard matrices of order 764 exist*, Combinatorica, **28**, 487–489 (2008).
- [46] D. M. DUNCAN, TH. R. HOFFMAN, J. P. SOLAZZO: *Equiangular tight frames and fourth root Seidel matrices*, Linear Algebra and its Applications, **432**, 2816–2823 (2010).
- [47] T. DURT, B.-G. ENGLERT, I. BENGTSSON, K. ŻYCKOWSKI: *On mutually unbiased bases*, Intl. J. Quantum Inf., **8**, 535–640 (2010).
- [48] P. ERDŐS, J. SPENCER: *Probabilistic methods in combinatorics*, Academic Press, Inc., New York (1974).
- [49] B. FARKAS, M. MATOLCSI, P. MÓRA: *On fuglede’s conjecture and the existence of universal spectra*, J. Fourier Anal. Appl., **12**, 483–494 (2006).
- [50] B. FARKAS, SZ. RÉVÉSZ: *Tiles with no spectra in dimension 4*, Math. Scand., **98**, 44–52, (2006).
- [51] J.-C. FAUGÈRE: *A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)*, Proceedings of the 2002 international symposium on Symbolic and algebraic computation, (ISSAC) (ACM Press): 75–83 (2002).
- [52] 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).

- [53] M. FICKUS, D. MIXON, J. C. TREMAIN: *Steiner equiangular tight frames*, preprint, arXiv: 1009.5730v1 [math.FA] (2010).
- [54] B. FUGLEDE: *Commuting self-adjoint partial differential operators and a group theoretic problem*, J. Funct. Anal., **16**, 101–121 (1974).
- [55] C. GODSIL, A. ROY: *Equiangular lines, mutually unbiased bases, and spin models*, European Journal of Combinatorics, **30**, 246–262 (2009).
- [56] F. M. GOODMAN, P. DE LA HARPE, V. F. R. JONES: *Coxeter Graphs and Towers of Algebras*, Math. Sciences Res. Inst. Publ. Springer Verlag (1989).
- [57] R. GOW: *Generation of mutually unbiased bases as powers of a unitary matrix in 2-power dimensions*, Preprint, arXiv: math/0703333v2 [math.RT] (2007).
- [58] M. GRASSL: *On SIC-POVMs and MUBs in Dimension 6*, Proceedings of the 2004 ERATO Conference on Quantum Information Science (Tokyo), 60–61 (2004).
- [59] U. HAAGERUP: *Cyclic  $p$ -roots of prime length  $p$  and related complex Hadamard matrices*, Preprint, arXiv: 0803.2629v1 [math.AC] (2008).
- [60] 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).
- [61] J. HADAMARD: *Résolution d’une question relative aux déterminants*, Bulletin des Sciences Mathématiques, **17**, 240–246 (1893).
- [62] M. HALL, JR.: *Hadamard matrices of order 16*, Technical Report, Jet Propulsion Laboratory, Pasadena, 36–10, (1965).
- [63] M. HARADA, C. LAM, V. D. TONCHEV: *Symmetric  $(4, 4)$ -nets and Generalized Hadamard Matrices Over Groups of Order 4*, Designs, Codes and Cryptography, **34**, 71–87 (2005).
- [64] S. G. HOGGAR: *64 lines from a quaternionic polytope*, Geom. Dedicata, **69**, 287–289 (1998).
- [65] R. B. HOLMES, V. I. PAULSEN: *Optimal frames for erasures*, Linear Algebra Appl., **377**, 31–51 (2004).
- [66] W. H. HOLZMANN, H. KHARAGHANI, W. ORRICK: *On the real unbiased Hadamard matrices*, Contemporary Mathematics, Combinatorics and Graphs, **531**, 243–250 (2010).

- [67] K. J. HORADAM: *Hadamard Matrices and Their Applications*, Princeton University Press, (2007).
- [68] R. HOSOYA, H. SUZUKI: *Type II Matrices and Their Bose-Mesner Algebras*, J. Algebraic Combinatorics, **17**, 19–37 (2003).
- [69] A. IOSEVICH, N. KATZ, T. TAO: *The Fuglede spectral conjecture holds for convex bodies in the plane*, Math. Res. Letters, **10**, 559–570 (2003).
- [70] I. D. IVANOVIC: *Geometrical description of quantal state determination*, J. Phys. A: Math. Gen., **14**, 3241 (1981).
- [71] PH. JAMING, M. MATOLCSI, P. MÓRA, F. SZÖLLŐSI, M. WEINER: *A generalized Pauli problem and an infinite family of MUB-triplets in dimension 6*, J. Phys. A: Math. Theor., **42**, 245305 (2009).
- [72] V. F. R. JONES: *Planar Algebras I*, Preprint, arXiv: math/9909027v1 [math.QA] (1999).
- [73] W. M. KANTOR: *MUBs inequivalence and affine planes*, Preprint, arXiv: 1104.3370v2 [math.CO] (2011).
- [74] A. KARABEGOV: *A mapping from the unitary to doubly stochastic matrices and symbols on a finite set*, AIP Conf. Proc., **1079**, 39–50 (2008).
- [75] B. R. KARLSSON:  *$H_2$ -reducible Hadamard matrices of order 6*, Linear Algebra and its Applications, **434**, 239–246 (2011).
- [76] B. R. KARLSSON: *Three-parameter complex Hadamard matrices of order 6*, Linear Algebra and its Applications, **434**, 247–258 (2011).
- [77] B. R. KARLSSON: *Two-parameter complex Hadamard matrices for  $N = 6$* , J. Math. Phys., **50**, 082104 (2009).
- [78] P. KASKI, P. ÖSTERGÅRD: *Classification Algorithms for Codes and Designs*, Springer-Verlag, Berlin, (2006).
- [79] S. A. KATRE, A. R. RAJWADE: *Resolution of the sign ambiguity in the determination of the cyclotomic numbers of order 4 and the corresponding Jacobsthal sum*, Math. Scand., **60**, 52–52 (1987).
- [80] H. KHARAGHANI, B. TAYFEH-REZAIE: *A Hadamard matrix of order 428*, Journal of Combinatorial Designs, **13**, 435–440 (2005).

- [81] H. KHARAGHANI, B. TAYFEH-REZAIE: *On the classification of Hadamard matrices of order 32*, J. Combin. Designs, **18**, 328–336 (2010).
- [82] M. KHATIRINEJAD: *On Weyl-Heisenberg orbits of equiangular lines*, J. Algebraic Combinatorics, **28**, 333–349 (2008).
- [83] C. KOUKOUVINOS, E. LAPPAS, M. MITROULI, J. SEBERRY: *An algorithm to find formulae and values of minors for Hadamard matrices: II.*, Linear Algebra Appl., **371**, 111–124 (2003).
- [84] M. KOLOUNTZAKIS, M. MATOLCSI: *Complex hadamard matrices and the spectral set conjecture*, Collect. Math., Vol. Extra, 281–291 (2006).
- [85] M. KOLOUNTZAKIS, M. MATOLCSI: *Tiles with no spectra*, Forum Math., **18**, 519–528 (2006).
- [86] M. KOLOUNTZAKIS, M. MATOLCSI: *Tilings by translation*, La Gaceta de la Real Sociedad Espanola, **13**, (2010).
- [87] J. KONVALINA, V. MATACHE: *Palindrome-Polynomials with Roots on the Unit Circle*, Comptes Rendus Mathematiques, **26**, 390–44 (2004).
- [88] C. KOUKOUVINOS, J. SEBERRY: *New weighing matrices and orthogonal designs constructed using two sequences with zero autocorrelation function – a review*, J. Statist. Plann. Inference, **81**, 153–182 (1999).
- [89] C. KOUKOUVINOS, S. STYLIANOU: *On skew-Hadamard matrices*, Discrete Mathematics, **308**, 2723–2731 (2008).
- [90] P. LAKATOS, L. LOSONCZI: *Polynomials with all zeros on the unit circle*, Acta Math. Hungar., **125**, 341–356 (2009).
- [91] T. Y. LAM, K. H. LEUNG: *On vanishing sums of roots of unity*, J. of Algebra, **224**, 91–109 (2000).
- [92] P. LAMPIO, F. SZÖLLŐSI, P. ÖSTERGÅRD: *The quaternary complex Hadamard matrices of orders 10, 12 and 14*, Preprint, (2011).
- [93] P. LAMPIO, P. ÖSTERGÅRD: *Classification of difference matrices over cyclic groups*, Journal of Statistical Planning and Inference, **141**, 1194–1207 (2011).
- [94] I. ŁABA: *Fuglede’s conjecture for a union of two intervals*, Proc. Amer. Math. Soc., **129**, 2965–2972 (2001).

- [95] S. LANDAU, G. L. MILLER: *Solvability by Radicals Is in Polynomial Time*, J. Computer and System Sciences, **30**, 179–208 (1985).
- [96] D. LAZARD: *Thirty years of Polynomial System Solving, and now?*, J. Symbolic Computation, **44**, 222–231 (2009).
- [97] N. Lecompte, W. J. MARTIN, W. OWENS: *On the equivalence between real mutually unbiased bases and a certain class of association schemes*, European Journal of Combinatorics, **31**, 1499–1512 (2010).
- [98] M. H. LEE, V. VL. VAVREK: *Jacket conference matrices and Paley transformation*, Eleventh International Workshop on Algebraic and Combinatorial Coding Theory, Pamporovo, Bulgaria, 181–185 (2008).
- [99] P. W. H. LEMMENS, J. J. SEIDEL: *Equiangular lines*, J. Algebra, **24**, 494–512 (1973).
- [100] J. H. VAN LINT, J. J. SEIDEL: *Equilateral point sets in elliptic geometry*, Indag. Math., **28**, 335–348 (1966).
- [101] L. LOVÁSZ: Unpublished, (1984).
- [102] M. MATOLCSI, J. RÉFFY, F. SZÖLLŐSI: *Constructions of complex Hadamard matrices via tiling Abelian groups*, Open Sys. & Inf. Dyn., **14**, 247–263 (2007).
- [103] M. MATOLCSI, F. SZÖLLŐSI: *Towards the classification of  $6 \times 6$  complex Hadamard matrices*, Open Sys. & Inf. Dyn., **15**, 1–16 (2008).
- [104] T. S. MICHAEL, W. D. WALLIS: *Skew-Hadamard matrices and the Smith normal form*, Des. Codes Crypt., **13**, 173–176 (1998).
- [105] G. E. MOORHOUSE: *The 2-Transitive Complex Hadamard Matrices*, Preprint, <http://www.uwo.edu/moorhouse/pub/complex.pdf> (2001).
- [106] A. MUNEMASA, Y. WATATANI: *Orthogonal Pairs of  $\ast$ -Subalgebras and Association Schemes*, C. R. Acad. Sci. Paris, **314**, 329–331 (1992).
- [107] R. NICOARĂ: *A finiteness result for commuting squares of matrix algebras*, J. Operator Theory, **55**, 101–116 (2006).
- [108] R. NICOARĂ: *Limit points of commuting squares*, Indiana University Mathematics Journal, to appear (2011).
- [109] K. NOMURA: *Type II matrices of size five*, Graphs and Combinatorics, **15**, 79–92 (1999).



- [110] W. P. ORRICK: *Switching Operations for Hadamard matrices*, SIAM Journal on Discrete Mathematics, **22**, 31–50 (2008).
- [111] R. E. A. C. PALEY: *On orthogonal matrices*, Journal of Mathematics and Physics, **12**, 311–320 (1933).
- [112] V. PAULSEN: *Completely Bounded Maps and Operator Algebras*, Cambridge University Press, (2003).
- [113] M. PETRESCU: *Existence of continuous families of complex Hadamard matrices of certain prime dimensions*, PhD thesis, UCLA, (1997).
- [114] D. PETZ, A. SZÁNTÓ, M. WEINER: *Complementarity and the algebraic structure of 4-level quantum systems*, Infinite Dimensional Analysis, Quantum Probability and Related Topics, **12**, 99–116 (2009).
- [115] S. POPA: *Classification of subfactors: the reduction to commuting squares*, Invent. Math., **101**, 19–43 (1990).
- [116] PH. RAYNAL, X. LÜ, B.-G. ENGLERT: *Mutually unbiased bases in dimension six: The four most distant bases*, Phys. Rev. A, **83**, 062303 (2011).
- [117] J. M. RENES: *Equiangular tight frames from Paley tournaments*, Linear Algebra and its Applications, **426**, 497–501 (2007).
- [118] H. J. RYSER: *Combinatorial mathematics*, Wiley, New York, (1963).
- [119] R. SABETI: *Numerical-symbolic exact irreducible decomposition of cyclic-12*, LMS Journal of Computation and Mathematics, **14**, 155–172 (2011).
- [120] B. SAFFARI: *Some polynomial extremal problems which emerged in the twentieth century*, Twentieth Century Harmonic Analysis – A celebration, Proceedings of the NATO Advanced Study Institute, **33**, 201–233, Springer (2001).
- [121] B. SCHMIDT: *Cyclotomic integers and finite geometry*, J. Amer. Math. Soc., **12**, 929–952 (1999).
- [122] A. J. SCOTT, M. GRASSL: *SIC-POVMs: A new computer study*, J. Math. Phys., **51**, 042203 (2010).
- [123] J. SEBERRY-WALLIS: *On the existence of Hadamard matrices*, J. Combin. Th. Ser. A, **21**, 188–195 (1976).
- [124] W. SIERPIŃSKI: *Elementary Theory of Numbers*, PWN, Warszawa, A. Schinzel ed., (1987).

- [125] A. J. SKINNER, V. A. NEWELL, R. SANCHEZ: *Unbiased bases (Hadamards) for six-level systems: Four ways from Fourier*, J. Math. Phys., **50**, 012107 (2009).
- [126] E. SPENCE: *Classification of Hadamard matrices of order 24 and 28*, Discrete Math., **140**, 185–243 (1995).
- [127] J. J. SYLVESTER: *Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers*, Philosophical Magazine, **34**, 461–475 (1867).
- [128] S. SZABÓ: *A type of factorization of finite abelian groups*, Discrete Math., **54**, 121–124 (1985).
- [129] F. SZÖLLŐSI: *A two-parameter family of complex Hadamard matrices of order 6, induced by hypocycloids*, Proc. Amer. Math. Soc., **138**, 921–928 (2010).
- [130] F. SZÖLLŐSI: *Complex Hadamard matrices and equiangular tight frames*, Linear Algebra and its Applications (Special Issue), to appear (2011).
- [131] F. SZÖLLŐSI: *Complex Hadamard matrices of order 6: a four-parameter family*, J. London Math. Soc., to appear (2011).
- [132] F. SZÖLLŐSI: *Exotic complex Hadamard matrices and their equivalence*, Cryptography and Communications: Discrete Structures, Boolean Functions and Sequences, **2**, 187–198 (2010).
- [133] F. SZÖLLŐSI: *Komplex Hadamard mátrixok konstrukciója és paraméterezése*, (in Hungarian) [Construction and parametrization of complex Hadamard matrices], Master's thesis, BUTE, Budapest, Hungary (2008).
- [134] F. SZÖLLŐSI: *On quaternary complex Hadamard matrices of small orders*, Advances in Mathematics of Communications, **5**, 309–315 (2011).
- [135] F. SZÖLLŐSI: *Parametrizing complex Hadamard matrices*, European J. of Combin., **29**, 1219–1234 (2008).
- [136] W. TADEJ: *Defect of a Kronecker product of unitary matrices*, Preprint, arXiv: 1009.4037v2 [math.OA] (2010).
- [137] W. TADEJ: *Permutation equivalence classes of Kronecker products of unitary Fourier matrices*, Linear Algebra and its Applications, **418**, 719–736 (2006).

- [138] W. TADEJ, K. ŻYCZKOWSKI: *A concise guide to complex Hadamard matrices*, Open Systems & Infor. Dyn., **13**, 133–177 (2006).
- [139] W. TADEJ, K. ŻYCZKOWSKI: *Defect of a unitary matrix*, Linear Algebra and its Applications, **429**, 447–481 (2008).
- [140] T. TAO: *Fuglede’s conjecture is false in 5 and higher dimensions*, Math. Res. Letters, **11**, 251–258 (2004).
- [141] J. C. TREMAIN: *Concrete Constructions of Real Equiangular Line Sets*, Preprint, arXiv:0811.2779v1 [math.MG] (2008).
- [142] R. J. TURYN: *On  $C$ -matrices of arbitrary powers*, Can. J. Math., **23**, 531–535 (1971).
- [143] J. WALLIS: *Combinatorial Matrices*, PhD thesis, La Trobe University, (1970).
- [144] R. F. WERNER: *All teleportation and dense coding schemes*, J. Phys. A, **34**, 7081–7094 (2001).
- [145] M. WEINER: *A gap for the maximum number of mutually unbiased bases*, Preprint, arXiv: 0902.0635v2 (2010).
- [146] A. WINTERHOF: *On the non-existence of generalised Hadamard matrices*, J. Statist. Plann. Inference, **84**, 337–342 (2000).
- [147] P. WOCJAN, TH. BETH: *New construction of mutually unbiased bases in square dimensions*, Quantum Information & Computation, **5**, 93–101 (2005).
- [148] W. K. WOOTERS, B. D. FIELDS: *Optimal state-determination by mutually unbiased measurements*, Ann. Phys. (NY), **191**, 363–381 (1989).
- [149] G. ZAUNER: *Quantendesigns: Grundzüge einer nichtkommutativen Designtheorie*, (in German) [Quantumdesigns: The foundations of a noncommutative design theory], PhD thesis, Universität Wien, (available at the Web page <http://www.mat.univie.ac.at/~neum/ms/zauner.pdf>), (1999).
- [150] Z. ZHIHAI, F. TIAN, X. BICAN: *Real solution isolation with multiplicity of zero-dimensional triangular systems*, Science China, Information Sciences, **54**, 60–69 (2011).



# Appendix A

## Petrescu-type Hadamard matrices

Here we list a handful of Petrescu-type  $BH(n, q)$  matrices. Recall that  $\omega = \mathbf{e}^{2\pi\mathbf{i}/3}$ .

### A.1 Some small dimensional examples

**Example A.1.1.**  $F_2 \otimes F_2$  is the only real, Petrescu-type Hadamard matrix:

$$P_4^{(1)}(a) = \left[ \begin{array}{c|c|c|c} a & -a & -1 & 1 \\ \hline -a & a & -1 & 1 \\ \hline -1 & -1 & 1 & 1 \\ \hline 1 & 1 & 1 & 1 \end{array} \right].$$

**Example A.1.2.** The following is four-parameter family of complex Hadamard matrices, stemming from a  $BH(13, 30)$  matrix (cf. [19]). We have  $P_{13A}^{(4)}(a, b, c, d) =$

$$\left[ \begin{array}{cccc|cccc|ccccc} \omega & a & b & c & -1 & -a & -b & -c & w & w^2 & w^3 & w^4 & 1 \\ \frac{d^2\omega}{a} & \omega & -\frac{bde}{a} & -\frac{cd\omega}{ae} & -\frac{d^2\omega}{a} & -1 & \frac{bde}{a} & \frac{cd\omega}{ae} & w^2 & w^4 & w & w^3 & 1 \\ \frac{\omega}{b} & -\frac{a\omega}{bde} & -1 & \frac{c\omega}{bde} & -\frac{\omega}{b} & \frac{a\omega}{bde} & \omega & -\frac{c\omega}{bde} & w^3 & w & w^4 & w^2 & 1 \\ \frac{\omega}{c} & -\frac{ae}{cd} & \frac{be}{cd} & -1 & -\frac{\omega}{c} & \frac{ae}{cd} & -\frac{be}{cd} & \omega & w^4 & w^3 & w^2 & w & 1 \\ \hline -1 & -a & -b & -c & \omega & a & b & c & w & w^2 & w^3 & w^4 & 1 \\ -\frac{d^2\omega}{a} & -1 & \frac{bde}{a} & \frac{cd\omega}{ae} & \frac{d^2\omega}{a} & \omega & -\frac{bde}{a} & -\frac{cd\omega}{ae} & w^2 & w^4 & w & w^3 & 1 \\ -\frac{\omega}{b} & \frac{a\omega}{bde} & \omega & -\frac{c\omega}{bde} & \frac{\omega}{b} & -\frac{a\omega}{bde} & -1 & \frac{c\omega}{bde} & w^3 & w & w^4 & w^2 & 1 \\ -\frac{\omega}{c} & \frac{ae}{cd} & -\frac{be}{cd} & \omega & \frac{\omega}{c} & -\frac{ae}{cd} & \frac{be}{cd} & -1 & w^4 & w^3 & w^2 & w & 1 \\ \hline w^4 & w^3 & w^2 & w & w^4 & w^3 & w^2 & w & 1 & \omega^2 & \omega^2 & \omega^2 & \omega^2 \\ w^3 & w & w^4 & w^2 & w^3 & w & w^4 & w^2 & \omega^2 & 1 & \omega^2 & \omega^2 & \omega^2 \\ w^2 & w^4 & w & w^3 & w^2 & w^4 & w & w^3 & \omega^2 & \omega^2 & 1 & \omega^2 & \omega^2 \\ w & w^2 & w^3 & w^4 & w & w^2 & w^3 & w^4 & \omega^2 & \omega^2 & \omega^2 & 1 & \omega^2 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & 1 \end{array} \right],$$

where  $w = \mathbf{e}^{2\pi\mathbf{i}/5}$  and  $\Re[e\omega] = -\Re[d]/2$ . The parameters  $a, b$  and  $c$  were introduced via Theorem 1.2.16 resulting in the largest known family of order 13.

**Example A.1.3.** The following is a  $BH(16, 4)$  matrix of Petrescu-type:

$$\left[ \begin{array}{ccccc|ccccc|ccccc} 1 & 1 & \mathbf{i} & 1 & 1 & -1 & -\mathbf{i} & -1 & -1 & -1 & 1 & -1 & -1 & -\mathbf{i} & \mathbf{i} & 1 \\ \mathbf{i} & -1 & -1 & -\mathbf{i} & -\mathbf{i} & -\mathbf{i} & -\mathbf{i} & -\mathbf{i} & \mathbf{i} & \mathbf{i} & \mathbf{i} & \mathbf{i} & -\mathbf{i} & -1 & -\mathbf{i} & 1 \\ 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & \mathbf{i} & -\mathbf{i} & -1 & 1 \\ \mathbf{i} & 1 & -\mathbf{i} & -1 & \mathbf{i} & -\mathbf{i} & -1 & \mathbf{i} & \mathbf{i} & -1 & -1 & -\mathbf{i} & -1 & \mathbf{i} & 1 & 1 \\ 1 & -1 & -\mathbf{i} & -\mathbf{i} & \mathbf{i} & -1 & 1 & \mathbf{i} & -1 & 1 & -\mathbf{i} & -1 & 1 & \mathbf{i} & -1 & 1 \\ \hline -1 & -\mathbf{i} & -1 & -1 & -1 & 1 & 1 & \mathbf{i} & 1 & 1 & 1 & -1 & -1 & -\mathbf{i} & \mathbf{i} & 1 \\ -\mathbf{i} & -\mathbf{i} & -\mathbf{i} & \mathbf{i} & \mathbf{i} & \mathbf{i} & -1 & -1 & -\mathbf{i} & -\mathbf{i} & \mathbf{i} & \mathbf{i} & -\mathbf{i} & -1 & -\mathbf{i} & 1 \\ 1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & \mathbf{i} & -\mathbf{i} & -1 & 1 \\ -\mathbf{i} & -1 & \mathbf{i} & \mathbf{i} & -1 & \mathbf{i} & 1 & -\mathbf{i} & -1 & \mathbf{i} & -1 & -\mathbf{i} & -1 & \mathbf{i} & 1 & 1 \\ -1 & 1 & \mathbf{i} & -1 & 1 & 1 & -1 & -\mathbf{i} & -\mathbf{i} & \mathbf{i} & -\mathbf{i} & -1 & 1 & \mathbf{i} & -1 & 1 \\ \hline 1 & -\mathbf{i} & -1 & -1 & \mathbf{i} & 1 & -\mathbf{i} & -1 & -1 & \mathbf{i} & 1 & 1 & 1 & 1 & 1 & -1 \\ -1 & -\mathbf{i} & 1 & \mathbf{i} & -1 & -1 & -\mathbf{i} & 1 & \mathbf{i} & -1 & 1 & 1 & 1 & 1 & -1 & 1 \\ -1 & \mathbf{i} & -\mathbf{i} & -1 & 1 & -1 & \mathbf{i} & -\mathbf{i} & -1 & 1 & 1 & 1 & \mathbf{i} & -\mathbf{i} & 1 & 1 \\ \mathbf{i} & -1 & \mathbf{i} & -\mathbf{i} & -\mathbf{i} & \mathbf{i} & -1 & \mathbf{i} & -\mathbf{i} & -\mathbf{i} & \mathbf{i} & -\mathbf{i} & 1 & 1 & 1 & 1 \\ -\mathbf{i} & \mathbf{i} & -1 & 1 & -1 & -\mathbf{i} & \mathbf{i} & -1 & 1 & -1 & -\mathbf{i} & \mathbf{i} & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -\mathbf{i} & \mathbf{i} & 1 & 1 \end{array} \right].$$

**Example A.1.4.** Our last example is a  $BH(16, 6)$  matrix, which can be obtained by considering  $H = \text{EXP}\left(\frac{2\pi\mathbf{i}}{6}L\right)$ , where

$$L = \left[ \begin{array}{ccccc|ccccc|ccccc} 0 & 0 & 0 & 0 & 0 & 3 & 0 & 3 & 3 & 3 & 0 & 2 & 2 & 4 & 4 & 0 \\ 0 & 0 & 0 & 2 & 4 & 0 & 3 & 3 & 5 & 1 & 0 & 4 & 4 & 2 & 2 & 0 \\ 0 & 0 & 3 & 4 & 2 & 3 & 3 & 3 & 1 & 5 & 3 & 0 & 3 & 0 & 3 & 0 \\ 0 & 2 & 4 & 2 & 3 & 3 & 5 & 1 & 5 & 3 & 3 & 2 & 5 & 4 & 1 & 0 \\ 0 & 4 & 2 & 3 & 4 & 3 & 1 & 5 & 3 & 1 & 3 & 4 & 1 & 2 & 5 & 0 \\ \hline 3 & 0 & 3 & 3 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 4 & 4 & 0 \\ 0 & 3 & 3 & 5 & 1 & 0 & 0 & 0 & 2 & 4 & 0 & 4 & 4 & 2 & 2 & 0 \\ 3 & 3 & 3 & 1 & 5 & 0 & 0 & 3 & 4 & 2 & 3 & 0 & 3 & 0 & 3 & 0 \\ 3 & 5 & 1 & 5 & 3 & 0 & 2 & 4 & 2 & 3 & 3 & 2 & 5 & 4 & 1 & 0 \\ 3 & 1 & 5 & 3 & 1 & 0 & 4 & 2 & 3 & 4 & 3 & 4 & 1 & 2 & 5 & 0 \\ \hline 0 & 0 & 3 & 3 & 3 & 0 & 0 & 3 & 3 & 3 & 0 & 0 & 0 & 0 & 0 & 3 \\ 4 & 2 & 0 & 4 & 2 & 4 & 2 & 0 & 4 & 2 & 0 & 0 & 0 & 0 & 3 & 0 \\ 4 & 2 & 3 & 1 & 5 & 4 & 2 & 3 & 1 & 5 & 0 & 0 & 0 & 3 & 0 & 0 \\ 2 & 4 & 0 & 2 & 4 & 2 & 4 & 0 & 2 & 4 & 0 & 0 & 3 & 0 & 0 & 0 \\ 2 & 4 & 3 & 5 & 1 & 2 & 4 & 3 & 5 & 1 & 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 \end{array} \right].$$

# Appendix B

## All cyclic 17-roots of simple index 4

Throughout this section we give a concise guide to cyclic 17-roots of simple index 4. In particular, we solve case  $p = 17$  and  $k = 4$  of (3.26) with Gröbner basis techniques and discover new examples of complex Hadamard matrices of order 17.

### B.1 The polynomial describing the solutions

After calculating a pure lexicographic Gröbner basis we found that the solutions of (3.26) for  $p = 17$ ,  $k = 4$ , i.e. the cyclic 17-roots of simple index 4 on the  $x$ -level can be obtained by considering the roots of the following polynomial of degree 70:

$$\begin{aligned} \mathcal{C}_{17}(x) = & (x^2 + 15x + 1) (4x^4 + x^3 + 7x^2 + x + 4) \\ & \times (4x^8 + 2x^7 - 41x^6 - 3x^5 + 59x^4 - 3x^3 - 41x^2 + 2x + 4) \\ & \times (4x^8 + 2x^7 - 7x^6 - 3x^5 - 9x^4 - 3x^3 - 7x^2 + 2x + 4) \\ & \times (4x^{16} - 64x^{15} + 344x^{14} - 744x^{13} + 1364x^{12} + 4288x^{11} - 6048x^{10} + 1772x^9 \\ & + 21577x^8 + 1772x^7 - 6048x^6 + 4288x^5 + 1364x^4 - 744x^3 + 344x^2 - 64x + 4) \\ & \times (8788x^{32} - 143312x^{31} - 6737120x^{30} + 66098104x^{29} + 317898992x^{28} \\ & - 1844667456x^{27} - 5388129896x^{26} + 4288299156x^{25} + 16518934433x^{24} \\ & + 9515028816x^{23} + 6237511690x^{22} + 5188763380x^{21} - 7207401x^{20} \\ & - 9833239192x^{19} - 6468787876x^{18} - 4434709436x^{17} - 10393530091x^{16} \\ & - 4434709436x^{15} - 6468787876x^{14} - 9833239192x^{13} - 7207401x^{12} \\ & + 5188763380x^{11} + 6237511690x^{10} + 9515028816x^9 + 16518934433x^8 \\ & + 4288299156x^7 - 5388129896x^6 - 1844667456x^5 + 317898992x^4 \\ & + 66098104x^3 - 6737120x^2 - 143312x + 8788). \end{aligned}$$

Our goal is to find, among the roots of  $\mathcal{C}_{17}(x)$ , all quadruples  $(c_0, c_1, c_2, c_3) \in (\mathbb{C}^*)^4$  which solve (3.26). It turns out that in almost all cases if one of the values  $c_0, c_1, c_2$

or  $c_3$  is a root of a given factor of  $\mathcal{C}_{17}(x)$  then all additional one is a root of the same factor. As a result the problem naturally can be divided into subcases by considering these factors separately. In order to do this, let us denote by  $V_1(x), V_2(x), \dots, V_6(x)$  the six factors of  $\mathcal{C}_{17}(x)$  in the same order as they appear above, respectively.

In what follows we account all 70 solutions of the problem (see Theorem 3.3.8) and show how to describe them by radicals. The general strategy is to exploit the symmetry of (3.26) and introduce the new variables

$$h_i := c_i + \frac{1}{c_i}, \quad i = 0, 1, 2, 3. \quad (\text{B.1})$$

This standard trick effectively halves the degrees of the polynomials  $V_i(x)$ ,  $i = 1, 2, \dots, 6$  whose solutions are hopefully more easily accessible by radicals. The following is the way to recover the values of  $c_i$  once the values of  $h_i$ ,  $i = 0, \dots, 3$  are determined.

**Lemma B.1.1** (Lifting formula). *Suppose that  $x + \frac{1}{x} = a + \mathbf{i}b$ , where  $a, b \in \mathbb{R}$ . Then*

$$x_{1,2} = \begin{cases} \frac{a}{2} \pm \mathbf{i} \frac{\sqrt{4-a^2}}{2}, & \text{if } b = 0, |a| \leq 2; \\ \frac{a}{2} \pm \frac{\sqrt{a^2-4}}{2}, & \text{if } b = 0, |a| > 2; \\ \mathbf{i} \left( \frac{b}{2} \pm \frac{\sqrt{b^2+4}}{2} \right), & \text{if } b \neq 0, a = 0; \\ \frac{a}{2} \pm \frac{1}{4} \sqrt{2a^2 - 2b^2 - 8 + 2\sqrt{4a^2b^2 + (a^2 - b^2 - 4)^2}} \\ + \mathbf{i} \left( \frac{b}{2} \pm \frac{1}{4} \operatorname{sgn}(ab) \sqrt{-2a^2 + 2b^2 + 8 + 2\sqrt{4a^2b^2 + (a^2 - b^2 - 4)^2}} \right), & \text{otherwise,} \end{cases}$$

such that the  $\pm$  signs in the last part agree and  $\operatorname{sgn}(ab)$  is the sign of  $ab$ . Note that  $x_1x_2 = 1$  and hence  $x_2 = 1/x_1$ .

We remark that if  $x$  is complex unimodular then the first case applies. With the notations above let us introduce the lifting operator, mapping complex numbers  $z = a + \mathbf{i}b$ ,  $a, b \in \mathbb{R}$  to  $x_1$ :

$$\mathcal{L}(a + \mathbf{i}b) = x_1.$$

By using this shorthand notation we can avoid the excessive usage of the square roots.

## B.2 Analysing the solutions

Now we analyse each of the factors  $V_i$ ,  $i = 1, \dots, 6$  and count and classify the solutions they induce.



### B.2.1 Solutions coming from $V_1(x)$

First we suppose that one of  $c_0, c_1, c_2$  or  $c_3$  is a root of  $V_1(x)$ . It turns out that in this case  $c_0 = c_1 = c_2 = c_3$  and we obtain the “ $\varepsilon$ -solutions” (in the sense of [9]):

$$(c_0, c_1, c_2, c_3) = \left( \frac{-15 + \sqrt{221}}{2}, \frac{-15 + \sqrt{221}}{2}, \frac{-15 + \sqrt{221}}{2}, \frac{-15 + \sqrt{221}}{2} \right), \quad (\text{B.2})$$

and its reciprocal  $(1/c_0, 1/c_1, 1/c_2, 1/c_3)$ . These two real solutions are invariant up to cyclic permutations and conjugation.

### B.2.2 Solutions coming from $V_2(x)$

Next we suppose that one of  $c_0, c_1, c_2$  or  $c_3$  is a root of  $V_2(x)$ . It turns out that this case corresponds to the cyclic 17-roots of simple index 2, yielding the well-known solutions

$$(c_0, c_1, c_2, c_3) = (c, \bar{c}, c, \bar{c}), \quad (\text{B.3})$$

described by Theorem 3.3.10, where

$$c = -\frac{1 \pm \sqrt{17}}{16} + \mathbf{i} \frac{\sqrt{238 \pm 2\sqrt{17}}}{16},$$

where the  $\pm$  signs agree. These two solutions are unimodular; two additional one can be obtained by complex conjugation.

### B.2.3 Solutions coming from $V_3(x)V_4(x)$

Starting from the factor  $V_3(x)$  the degree of these polynomials are larger than 4 and hence there is no straightforward way to obtain the solutions by radicals (but see [95]). Therefore we use the substitution (B.1) (or more precisely Lemma C.2.2), applied to the factor  $V_3(x)V_4(x)$  to obtain, e.g.

$$\begin{aligned} h_0(\pm_A, \pm_B) &= -\frac{1 \pm_A 5\sqrt{17}}{8} \pm_B \frac{\sqrt{34 \pm_A 2\sqrt{17}}}{8}, \\ h_1(\pm_A, \pm_B) &= \frac{-1 \pm_A 3\sqrt{17}}{8} \pm_B \frac{\sqrt{34 \pm_A 2\sqrt{17}}}{8}, \end{aligned}$$

where the signs  $\pm_A$  and  $\pm_B$  describe the sign of  $\sqrt{17}$  and the sign of the nested radical, respectively. We remark here that in general this case corresponds to an irreducible polynomial over  $\mathbb{Q}$  of degree 16; it could have been factored in this case into the product  $V_3(x)V_4(x)$  because in the canonical decomposition  $17 = s^2 + t^2$  we have  $s = 1$  and as a result  $D = 0$  in (3.35).

The 16 solutions, in which  $c_2 = 1/c_0$ ,  $c_3 = 1/c_1$  are:

$$(c_0, c_1, c_2, c_3) = (\mathcal{L}(h_0(+, +)), \mathcal{L}(h_1(+, -)), 1/\mathcal{L}(h_0(+, +)), 1/\mathcal{L}(h_1(+, -))), \quad (\text{B.4})$$

$$(c_0, c_1, c_2, c_3) = (\mathcal{L}(h_0(-, -)), 1/\mathcal{L}(h_1(-, +)), 1/\mathcal{L}(h_0(-, -)), \mathcal{L}(h_1(-, +))), \quad (\text{B.5})$$

$$(c_0, c_1, c_2, c_3) = (\mathcal{L}(h_0(+, -)), 1/\mathcal{L}(h_1(+, +)), 1/\mathcal{L}(h_0(+, -)), \mathcal{L}(h_1(+, +))), \quad (\text{B.6})$$

$$(c_0, c_1, c_2, c_3) = (\mathcal{L}(h_0(-, +)), \mathcal{L}(h_1(-, -)), 1/\mathcal{L}(h_0(-, +)), 1/\mathcal{L}(h_1(-, -))) \quad (\text{B.7})$$

and their cyclic permutations. The first two set of solutions are unimodular and coincide with the solutions coming from Theorem 3.3.18 (cf. Example 3.3.21), whereas the last two are real.

### B.2.4 Solutions coming from $V_5(x)$

After factoring the transformed polynomial  $T_{V_5}(u)$ , coming from Lemma C.2.2, in the field extension  $\mathbb{Q}(\mathbf{i}, \sqrt{17})$  we find that four values of  $h_0$  can be obtained from

$$h_0(\pm_A, \pm_B) = 2 \pm_A \frac{\sqrt{34 + 18\sqrt{17}}}{4} \pm_B \frac{\sqrt{34 \pm_A 4\sqrt{17\sqrt{17}} + 2\sqrt{289 + 136\sqrt{17} \pm_A 68\sqrt{17\sqrt{17}}}}}{4} \pm_A \mathbf{i} \\ \times \left( -\frac{\sqrt{-34 + 18\sqrt{17}}}{4} \mp_B \frac{\sqrt{-34 \mp_A 4\sqrt{17\sqrt{17}} + 2\sqrt{289 + 136\sqrt{17} \pm_A 68\sqrt{17\sqrt{17}}}}}{4} \right).$$

With this notation the solution read

$$(c_0, c_1, c_2, c_3) = (\mathcal{L}(h_0(+, +)), 1/\mathcal{L}(h_0(-, -)), \mathcal{L}(h_0(+, -)), \mathcal{L}(h_0(-, +))), \quad (\text{B.8})$$

and its conjugate, reciprocal, conjugate-reciprocal and the cyclic permutations of these four. In total 16 complex (non real, non unimodular) solutions are found.

### B.2.5 Solutions coming from $V_6(x)$

As  $V_6(x)$  is of degree 36 we, again, investigate the roots of the transformed polynomial  $T_{V_6}(u)$ . Unfortunately it turns out that the roots are cannot be described by nested square roots any longer, as cubic roots appear during the solution of some degree 4 polynomials. Therefore instead of describing the values of  $h_0, h_1, h_2$  and  $h_3$  we rather describe the degree four polynomials, encoding the essentially different solutions (i.e. the unordered set  $\{h_0, h_1, h_2, h_3\}$ ) coming from the factor  $V_6(x)$ . The aforementioned polynomials can be obtained via their coefficients which however can be expressed by the elementary symmetric polynomials of  $h_i$ ,  $i = 0, 1, 2, 3$ , coming from (B.1). Let us use the following notations:

$$\sigma_1 = h_0 + h_1 + h_2 + h_3,$$

$$\begin{aligned}\sigma_2 &= h_0 h_1 + h_0 h_2 + h_0 h_3 + h_1 h_2 + h_1 h_3 + h_2 h_3, \\ \sigma_3 &= h_0 h_1 h_2 + h_0 h_1 h_3 + h_0 h_2 h_3 + h_1 h_2 h_3, \\ \sigma_4 &= h_0 h_1 h_2 h_3.\end{aligned}$$

Then, by calculating various Gröbner bases, we find that the following hold:

$$\begin{aligned}13\sigma_1^4 - 212\sigma_1^3 - 17584\sigma_1^2 - 512\sigma_1 + 1024 &= 0, \\ 169\sigma_2^4 - 96328\sigma_2^3 + 8248259\sigma_2^2 + 64168790\sigma_2 + 119444818 &= 0, \\ 2197\sigma_3^4 - 1603714\sigma_3^3 + 232154357\sigma_3^2 - 48071520\sigma_3 - 857293956 &= 0, \\ 8788\sigma_4^4 + 47418572\sigma_4^3 + 31284060733\sigma_4^2 - 68872842666\sigma_4 + 34518025937 &= 0.\end{aligned}$$

Now we build up, by trial and error, four polynomials  $\mathcal{I}_4^{(i)}(x)$ ,  $i = 0, 1, 2, 3$ , each describing a set  $\{h_0^{(i)}, h_1^{(i)}, h_2^{(i)}, h_3^{(i)}\}$  corresponding to a solution coming from  $V_6(x)$ . We have

$$\mathcal{I}_4^{(i)}(x) = x^4 - \sigma_1^{(i)}x^3 + \sigma_2^{(i)}x^2 - \sigma_3^{(i)}x + \sigma_4^{(i)}, \quad i = 0, 1, 2, 3,$$

where

$$\begin{aligned}\sigma_1^{(1)} &= \sigma_1(+, -), \quad \sigma_2^{(1)} = \sigma_2(+, -), \quad \sigma_3^{(1)} = \sigma_3(+, -), \quad \sigma_4^{(1)} = \sigma_4(+, +), \\ \sigma_1^{(2)} &= \sigma_1(-, +), \quad \sigma_2^{(2)} = \sigma_2(-, -), \quad \sigma_3^{(2)} = \sigma_3(-, -), \quad \sigma_4^{(2)} = \sigma_4(-, +), \\ \sigma_1^{(3)} &= \sigma_1(-, -), \quad \sigma_2^{(3)} = \sigma_2(-, +), \quad \sigma_3^{(3)} = \sigma_3(-, +), \quad \sigma_4^{(3)} = \sigma_4(-, -), \\ \sigma_1^{(4)} &= \sigma_1(+, +), \quad \sigma_2^{(4)} = \sigma_2(+, +), \quad \sigma_3^{(4)} = \sigma_3(+, +), \quad \sigma_4^{(4)} = \sigma_4(+, -),\end{aligned}$$

where

$$\begin{aligned}\sigma_1(\pm_A, \pm_B) &= \frac{53 \pm_A 59\sqrt{17}}{13} \pm_B \frac{\sqrt{63546 \pm_A 6358\sqrt{17}}}{13}, \\ \sigma_2(\pm_A, \pm_B) &= \frac{48164 \pm_A 7130\sqrt{17}}{338} \pm_B \frac{\sqrt{3307173846 \pm_A 705523222\sqrt{17}}}{338}, \\ \sigma_3(\pm_A, \pm_B) &= \frac{801857 \pm_A 89585\sqrt{17}}{4394} \pm_B \frac{4\sqrt{48275292054 \pm_A 8767889417\sqrt{17}}}{4394}, \\ \sigma_4(\pm_A, \pm_B) &= \\ &= -\frac{11854643 \pm_A 2053159\sqrt{17}}{8788} \pm_B \frac{2\sqrt{53118166790942 \pm_A 12183750689646\sqrt{17}}}{8788},\end{aligned}$$

where  $\pm_A$  and  $\pm_B$  describe the sign of  $\sqrt{17}$  and the sign of the nested radical, respectively. Once the four roots of  $\mathcal{I}_4^{(i)}(x)$  are found we can lift them via Lemma B.1.1 to obtain the values of  $(c_0, c_1, c_2, c_3)$  up to their order and reciprocal. Now if the four real roots of  $\mathcal{I}_4^{(i)}(x)$ , denoted by  $r_j^{(i)}$ ,  $i, j = 1, 2, 3, 4$  satisfy  $r_1^{(i)} < r_2^{(i)} < r_3^{(i)} < r_4^{(i)}$ , then we find that the values of  $c_0, c_1, c_2$  and  $c_3$  in the correct order are

$$(c_0, c_1, c_2, c_3) = \left( \mathcal{L}\left(r_1^{(1)}\right), \mathcal{L}\left(r_3^{(1)}\right), \mathcal{L}\left(r_4^{(1)}\right), 1/\mathcal{L}\left(r_2^{(1)}\right) \right), \quad (\text{B.9})$$

$$(c_0, c_1, c_2, c_3) = \left( \mathcal{L} \left( r_1^{(2)} \right), \mathcal{L} \left( r_2^{(2)} \right), \mathcal{L} \left( r_4^{(2)} \right), 1/\mathcal{L} \left( r_3^{(2)} \right) \right), \quad (\text{B.10})$$

$$(c_0, c_1, c_2, c_3) = \left( \mathcal{L} \left( r_1^{(3)} \right), \mathcal{L} \left( r_2^{(3)} \right), \mathcal{L} \left( r_3^{(3)} \right), 1/\mathcal{L} \left( r_4^{(3)} \right) \right), \quad (\text{B.11})$$

$$(c_0, c_1, c_2, c_3) = \left( \mathcal{L} \left( r_1^{(4)} \right), 1/\mathcal{L} \left( r_2^{(4)} \right), 1/\mathcal{L} \left( r_3^{(4)} \right), 1/\mathcal{L} \left( r_4^{(4)} \right) \right), \quad (\text{B.12})$$

and their reciprocal and their cyclic permutations. The first two set of solutions are complex unimodular whereas the last two are real. In particular, we obtain two new, previously unknown complex Hadamard matrices of order 17.

### B.3 Concluding remarks

We summarize the results of this section in the following

**Theorem B.3.1.** *The set of equations (3.26) has exactly 70 solutions in  $\mathbb{C}^4$  for  $p = 17$  and  $k = 4$  as follows:*

1. *The real  $\varepsilon$ -solution (B.2) and its reciprocal;*
2. *Two unimodular simple index 2 type solutions (B.3) and their reciprocal;*
3. *The simple index 4 type solutions:*
  - (a) *Two unimodular (B.4)-(B.5) and two real solutions (B.6)-(B.7), and their cyclic permutations;*
  - (b) *Two unimodular (B.9)-(B.10) and two real solutions (B.11)-(B.12), their cyclic permutations and reciprocal;*
  - (c) *A complex solution (B.8), its cyclic permutations, conjugate, reciprocal and conjugate-reciprocal.*

*Among these there are 26 real; 28 complex unimodular; and 16 additional solutions. Each of the solutions can be described by radicals.*

It remains an open problem to describe the solutions coming from  $V_6(x)$  in an elegant way by radicals. To solve the simple index 4 case in full generality one needs to find a way to control the cyclic order of the roots which we avoided as we could compare our analytic formulas with precalculated numerical solutions.

# Appendix C

## Complex Hadamard matrices with circulant core

In Section 3.3 we have seen that there are various general constructions yielding circulant complex Hadamard matrices of prime orders. It is natural to consider complex Hadamard matrices with circulant core as well. Through this section we work out an analogous theory to the circulant case with appropriate modifications, and give a full classification of complex Hadamard matrices with circulant core up to order 7. This classification results in the discovery of a new  $7 \times 7$  complex Hadamard matrix (see Example 3.3.25). We exhibit two additional examples of order 11 and for every prime  $p \equiv 1 \pmod{8}$  new examples of order  $p + 1$ .

### C.1 The general theory

Let us consider a dephased complex Hadamard matrix of order  $n + 1$  with circulant core, the first row of which is given by  $x = (x_0, x_1, \dots, x_{n-1})$ . Then, by orthogonality, we have

$$\left\{ \begin{array}{l} x_0 = -\frac{1}{1 + \frac{x_1}{x_0} + \frac{x_1 x_2}{x_0 x_1} + \dots + \frac{x_1 x_2 \dots x_{n-1}}{x_0 x_1 \dots x_{n-2}}}, \\ \frac{x_1}{x_0} + \frac{x_2}{x_1} + \dots + \frac{x_0}{x_{n-1}} = -1, \\ \frac{x_2}{x_0} + \frac{x_3}{x_1} + \dots + \frac{x_1}{x_{n-1}} = -1, \\ \vdots \\ \frac{x_{n-1}}{x_0} + \frac{x_0}{x_1} + \dots + \frac{x_{n-2}}{x_{n-1}} = -1. \end{array} \right. \quad (\text{C.1})$$

Note that the first equation is just a useful reformulation of the trivial condition coming from orthogonality to the first row:

$$x_0 = -1 - x_1 - \dots - x_{n-1},$$

and therefore it follows that  $x_0$  is uniquely determined by the quotients  $x_{i+1}/x_i$ , where  $i = 0, \dots, n-1$ . Note also that it can be further simplified if one assumes that the variables  $x_i$  are unimodular.

We offer the following well-known solution to the problem (C.1) when the size of the matrix  $n+1$  is prime.

**Example C.1.1.** Let  $g$  be a generator of the multiplicative group  $\mathbb{Z}_p^*$ . Then the vector  $x^{(g)}$ , with coordinates

$$x_i^{(g)} = \exp\left(\frac{2\pi\mathbf{i}}{p}g^i\right), i = 0, \dots, p-2$$

will give us the core of a  $BH(p, p)$  matrix (see Definition 1.4.1).

Other well-known solutions yielding complex Hadamard matrices of order  $n+1$  with circulant core come from the Paley matrix when the order of the core is prime (see Theorems 1.1.17 and 1.4.18).

Next we work out a general framework to study these objects in every order  $n$  by slightly modifying the cyclic  $n$ -root problem. Let us introduce the quotients  $z_i := x_{i+1}/x_i$  for  $i = 0, 1, \dots, n-1$ , where indices are taken modulo  $n$ . We have the following

**Theorem C.1.2.** *Any unimodular solution  $x$  of (C.1) gives rise to a unimodular solution  $z$  of the following system of equations*

$$\begin{cases} z_0 + z_1 + \dots + z_{n-1} = -1, \\ z_0 z_1 + z_1 z_2 + \dots + z_{n-1} z_0 = -1, \\ \vdots \\ z_0 z_1 \cdots z_{n-2} + z_1 z_2 \cdots z_{n-1} + \dots + z_{n-1} z_0 \cdots z_{n-3} = -1, \\ z_0 z_1 \cdots z_{n-1} = 1, \end{cases} \quad (\text{C.2})$$

and vice versa: any unimodular solution  $z$  of (C.2) can be lifted to a unimodular solution  $x$  of (C.1).

Note that the first equation of (C.1) does not appear amongst the equations (C.2). In particular, if all the quotients  $z_i$  are unimodular, then so is  $x_0$ .

*Proof.* The first direction is immediate: any unimodular solution  $x$  of (C.1) corresponds to a unimodular solution of (C.2) after passing to the quotients  $z_i := x_{i+1}/x_i$ . To see the other direction, suppose that we have a unimodular solution  $z$  of (C.2), and let us construct the corresponding solution  $x$  of (C.1). For simplicity, let us introduce the following new quantity

$$S := z_0 + z_0 z_1 + z_0 z_1 z_2 + \dots + z_0 z_1 \cdots z_{n-1}. \quad (\text{C.3})$$

Now observe that if we sum up the first  $n - 1$  equations plus  $n$  times the last one of (C.2) we get

$$S \left( 1 + \frac{1}{z_0} + \frac{1}{z_0 z_1} + \dots + \frac{1}{z_0 z_1 \dots z_{n-2}} \right) = 1, \quad (\text{C.4})$$

however, note that the second factor of (C.4) can be rewritten by the last equation of (C.2) and as a result we have

$$S\bar{S} = |S|^2 = 1.$$

From a given unimodular solution  $z$  one can reconstruct  $x$  up to an unknown phase, say  $x_0$ , giving  $x = x_0(1, z_0, z_0 z_1, \dots, z_0 z_1 \dots z_{n-2})$ . However, the first coordinate of  $x$ , which is  $x_0$ , is constrained by the first equation of (C.1). In particular, we need to have

$$x_0 = -\frac{1}{S} = -\bar{S}.$$

To conclude, we found that the solution on the  $x$ -level coming from  $z$  reads

$$x = -\bar{S}(1, z_0, z_0 z_1, \dots, z_0 z_1 \dots z_{n-2}),$$

where  $S$  is given by (C.3). Clearly, the identification  $x \leftrightarrow z$  is one-to-one.  $\square$

We have the following natural

**Problem C.1.3.** For a given  $n \in \mathbb{N}$  classify all solutions of (C.2). In particular, classify all complex Hadamard matrices of order  $n$  possessing a circulant core.

We shall return to Problem C.1.3 in Section C.2.

### C.1.1 Circulant core of index $k$ type

Here we introduce complex Hadamard matrices with index  $k$  type circulant core in a completely analogous way as simple index  $k$  type circulant complex Hadamard matrices were defined in Section 3.3. Note that the matrices we obtain here are not of prime order, but have a prime order core instead.

Let  $p$  be a prime and let  $k \in \mathbb{N}$  a number that divides  $p - 1$ . Consider  $G_0$ , the unique subgroup of  $\mathbb{Z}_p^*$  of index  $k$  and its nontrivial cosets  $G_1, \dots, G_{k-1}$ . We say that a solution  $z$  of (C.2) has index  $k$ , if the corresponding solution on the  $x$  level (C.1) is constant on the cosets  $G_j$ ,  $j = 0, \dots, k - 1$ , namely

$$\begin{cases} x_i = c_j, & \text{if } i \in G_j, \quad 1 \leq i \leq p - 1; \\ x_0 = -\frac{p-1}{k}(c_0 + c_1 + \dots + c_{k-1}) - 1, \end{cases} \quad \text{and} \quad (\text{C.5})$$

where  $(c_0, c_1, \dots, c_{k-1}) \in (\mathbb{C}^*)^k$ . The following is the relevant analogue of Proposition 3.3.7.

**Proposition C.1.4.** *If  $x = (x_0, x_1, \dots, x_{p-1})$  has the form (C.5), then the equations (C.1) can be reduced to the following  $k$  rational equations in  $c_0, c_1, \dots, c_{k-1}$ :*

$$1 + \frac{c_a}{x_0} + \frac{x_0}{c_{a+m}} + \sum_{i,j=0}^{k-1} n_{ij} \frac{c_{a+j}}{c_{a+i}} = 0, \quad 0 \leq a \leq k-1, \quad (\text{C.6})$$

where all indices are calculated modulo  $k$ . In (C.6) the number  $m$  is determined by  $p-1 \in G_m$  and  $n_{ij}$  denote the transition numbers of order  $k$ , namely, the number of  $b \in G_i$  for which  $b+1 \in G_j$ ,  $0 \leq i, j \leq k-1$ , with respect to the generator  $g$  of  $\mathbb{Z}_p^*$ .

Again, the system of equations (C.6) is independent of the choice of  $g$  up to relabelling the variables. Here we are interested in the unimodular solutions only, i.e. the ones that correspond to complex Hadamard matrices.

The following two results describe complex Hadamard matrices with index 2 type circulant core coming from Proposition C.1.4. The first one is the analogue of Theorem 3.3.9 (cf. Theorem 1.1.17).

**Lemma C.1.5.** *Let  $p \geq 7$  be a prime,  $p \equiv 3 \pmod{4}$ , and suppose that  $H$  is a complex Hadamard matrix of order  $p+1$  with circulant core of index 2 type. Then  $H$  is equivalent to the real Paley-Hadamard matrix.*

The second result is the analogue of Theorem 3.3.10 (cf. Theorem 1.4.18).

**Lemma C.1.6.** *Let  $p$  be a prime,  $p \equiv 1 \pmod{4}$ , and suppose that  $H$  is a complex Hadamard matrix of order  $p+1$  with circulant core of index 2 type. Then  $(c_0, c_1) = (a, \bar{a})$ , where*

$$a = \pm \mathbf{i}; \text{ or } a = -\frac{2}{p-1} \pm \mathbf{i} \frac{\sqrt{(p-1)^2 - 4}}{p-1}.$$

*Remark C.1.7.* For  $p = 5$  we get the well-known complex Hadamard matrices  $D_6^{(1)}(1)$  and  $S_6^{(0)}$  (see Examples 2.2.2 and 2.2.1), respectively. The  $BH(p+1, 4)$  matrices are well-known examples of complex Hadamard matrices (see Theorem 1.4.18) while the other set of examples are just a special case of Proposition 3.4.16.  $\square$

We did not find any examples of complex Hadamard matrices with index 3 type circulant core, however we can harvest some additional fruits from the theory of index 4 type circulant matrices as follows. Interestingly both constructions yield complex Hadamard matrices with real diagonal.

**Proposition C.1.8.** *Let  $p$  be a prime number,  $p \equiv 1 \pmod{8}$ ,  $p = s^2 + t^2$  such that  $s \equiv 1 \pmod{4}$  and  $t > 0$ . Then there is a complex Hadamard matrix  $H$  of order  $p+1$  with circulant core of index 4 type, where  $(c_0, c_1, c_2, c_3) = (a, -a, \bar{a}, -\bar{a})$ , or any cyclic permutation of it, where*

$$a = \frac{1 - \sqrt{1+t^2}}{t} + \mathbf{i} \frac{\sqrt{-2 + 2\sqrt{1+t^2}}}{t}.$$



**Proposition C.1.9.** *Let  $p$  be a prime number,  $p \equiv 1 \pmod{8}$ ,  $p = s^2 + t^2$  such that  $s \equiv 1 \pmod{4}$  and  $t > 0$ . Then there is a complex Hadamard matrix  $H$  of order  $p+1$  with circulant core of index 4 type, where  $(c_0, c_1, c_2, c_3) = (a, b, \bar{a}, \bar{b})$ , or any cyclic permutation of it, where*

$$a = -\frac{2}{p-1} + \sqrt{A - \sqrt{B}} + \mathbf{i} \sqrt{1 - \left( \frac{2}{p-1} - \sqrt{A - \sqrt{B}} \right)^2}, \quad (\text{C.7})$$

$$b = -\frac{2}{p-1} - \sqrt{A - \sqrt{B}} - \mathbf{i} \sqrt{1 - \left( \frac{2}{p-1} + \sqrt{A - \sqrt{B}} \right)^2}, \quad (\text{C.8})$$

where

$$\begin{aligned} A &= \frac{t^2 (p^2 + 2(s-2)^2 + 1) + 2(s-1)^4}{t^2(p-1)^2}, \\ B &= \frac{4(t^2(p + (s-2)^2 + 2) + (s-1)^4)}{t^4(p-1)^4} \\ &\quad \times (t^2(t^2(2s^2 + t^2 - 1) + ((s+1)^2 + 2)(s-1)^2) + (s-1)^4). \end{aligned}$$

*Remark C.1.10.* Formulas (C.7)-(C.8) are well defined, as clearly  $A > 0$ ,  $B > 0$  and

$$(p-1)^4(A^2 - B) = (p+1)^2(p-3)^2 > 0$$

for all relevant primes  $p$ . □

The proof of Propositions C.1.8 and C.1.9 is completely analogous to the proof of Theorem 3.3.18, the only difference being that we rely on Proposition C.1.4 instead of Proposition 3.3.7.

## C.2 Classification up to order 7

In what follows we launch a brute-force attack against Problem C.1.3 via Gröbner basis techniques and classify all complex Hadamard matrices with circulant core up to order 7. We report new complex Hadamard matrices of order 7 and 11 which are the main contribution of this section.

We shall encounter various self-inversive polynomials with real coefficients (see Definition 2.3.29) during the sequel and therefore we recall the following

**Definition C.2.1.** A complex polynomial  $f(x) = a_0 + a_1x + \dots + a_dx^d$  of degree  $d$  with real coefficients is called *palindromic* if  $a_{d-k} = a_k$  for every  $k = 0, \dots, d$ .

If  $f(x)$  is a palindromic polynomial of even degree  $d$ , then it is a standard trick to consider  $f(x)/x^{d/2}$  instead which can be rewritten as a polynomial of degree  $d/2$  in the new variable  $u = x + 1/x$ . This operation is investigated in the following

**Lemma C.2.2** (cf. [87]). *Let  $f(x)$  be a palindromic polynomial of even degree  $d$ . Then  $f(x)$  has a unimodular root  $x_0$  if and only if the transformed polynomial*

$$T_f(u) \equiv f\left(\frac{u + \sqrt{u^2 - 4}}{2}\right) \cdot \left(\frac{u - \sqrt{u^2 - 4}}{2}\right)^{d/2}$$

*has a real root  $|u_0| \leq 2$ .*

*Proof.* Suppose that  $f(x)$  has a unimodular root  $x_0$ . Then  $u_0 := x_0 + \frac{1}{x_0} = x_0 + \overline{x_0} = 2\Re[x_0]$  and hence  $u_0$  is real root of  $T_f(u)$  such that  $|u_0| \leq 2$ . To see the converse direction, suppose that the polynomial  $T_f(u)$  has a real root  $u_0$  such that  $|u_0| \leq 2$ . Then the numbers  $x_0$  defined via the roots of the quadratic equation  $x^2 - u_0x + 1 = 0$  are easily seen to be unimodular roots of  $f(x)$ .  $\square$

Lemma C.2.2 gives a characterization of unimodularity via an inequality whose validity can be more easily checked than the unimodularity condition itself. However, it is not entirely obvious how to separate the real roots from those who have some negligible (but still nonzero) imaginary part.

We shall apply repeatedly the following useful “averaging”

**Lemma C.2.3.** *Let  $n, m$  be positive integers,  $S \subset \{0, 1, \dots, n-1\}$  and consider the system of  $m+1$  complex equations in  $n+1$  variables  $(u, x_0, x_1, \dots, x_{n-1}) \in \mathbb{C}^{n+1}$ :*

$$\begin{cases} f_1(x_0, x_1, \dots, x_{n-1}) &= 0, \\ f_2(x_0, x_1, \dots, x_{n-1}) &= 0, \\ &\vdots \\ f_m(x_0, x_1, \dots, x_{n-1}) &= 0, \\ u \prod_{i \in S} x_i &= 1. \end{cases} \quad (\text{C.9})$$

*Let us define the projected solution set with respect to the index set  $S$  by*

$$U_S := \{u \in \mathbb{T} : (u, x_0, x_1, \dots, x_{n-1}) \text{ is a solution of (C.9) for some } x_0, x_1, \dots, x_{n-1}\}.$$

*If  $U_S$  is empty, then the system of equations does not have any unimodular solution.*

*Proof.* The Lemma is trivial. If  $(u, x_0, x_1, \dots, x_{n-1}) \in \mathbb{T}^{n+1}$  is a unimodular solution of (C.9), then  $u \in U_S$ .  $\square$

Lemma C.2.3 exploits the fact that by looking at the possible values of the products of some of the variables  $x_i$  (indexed by the set  $S$ ), or equivalently, the values of the “dummy” variable  $u$  only, one can conclude immediately that (C.9) has no unimodular solutions. Also, calculating the possible values of  $u$  might be computationally cheaper than calculating the individual values of  $x_0, x_1, \dots, x_{n-1}$  directly.

Based on the full classification of complex Hadamard matrices up to order 5 the following is easy to see (and in fact can be calculated by hand):

**Lemma C.2.4.** *The complex Hadamard matrices with circulant core of orders  $2 \leq n+1 \leq 5$  are equivalent to  $F_2, F_3, F_2 \otimes F_2$  and  $F_5$ .*

Note that the Fourier matrix  $F_4$  is not equivalent to a complex Hadamard matrix with circulant core. The next result, however, is an entirely not obvious

**Proposition C.2.5.** *The complex Hadamard matrices with circulant core of order  $n+1=6$  are equivalent to  $S_6^{(0)}$  or  $D_6^{(1)}(1)$  (see Examples 2.2.1 and 2.2.2, respectively).*

*Proof.* By calculating a pure lexicographic Gröbner basis for the system of equations (C.1), which we extended with an additional equation

$$ux_0x_1x_2x_3x_4 - 1 = 0 \quad (\text{C.10})$$

to avoid zero solutions, as usual, we found that there are finitely many solutions only. In particular, the polynomial, whose roots describe all possible values of the variable  $x_0$  (and due to cyclic symmetry account for all possible values of any of the variables  $x_i, i = 0, 1, \dots, 4$ ) reads

$$\begin{aligned} \mathcal{X}_5(x) = & (x-1)(x+1)(x^2+1)(x^2-14x+1)(x^2+x+1)(x^2+4x+1)(x^{10}+2x^9 \\ & +15x^8+108x^7+420x^6+672x^5+420x^4+108x^3+15x^2+2x+1). \end{aligned}$$

Now it is easy to recover the (known) solutions  $S_6^{(0)}$  and  $D_6^{(1)}(1)$  as they correspond to the factors  $(x-1)(x^2+x+1)$  and  $(x+1)(x^2+1)$ , respectively. The factor  $(x^2-14x+1)(x^2+4x+1)$  does not have any unimodular roots. It remains to show that the degree 10 factor, which we denote by  $g(x)$ , does not lead to any unimodular solutions  $(x_0, x_1, x_2, x_3, x_4) \in \mathbb{T}^5$ . By using Lemma C.2.2 we see that  $g(x)$  has unimodular roots, so the question is whether a unimodular root of it can be extended to a unimodular solution (i.e. if we can find additional unimodular numbers  $x_1, \dots, x_4$ , satisfying (C.1)). Now we use Lemma C.2.3 by adding  $g(x_0)$  to the initial system of equations (C.1) accompanied again by (C.10), and by calculating a Gröbner basis we find that the polynomial

$$u^2 + 322u + 1 \quad (\text{C.11})$$

is a member of the ideal, generated by the aforementioned polynomials. From this we see that as (C.11) does not have any unimodular roots the projected solution set  $U_S$ , with respect to the index set  $S = \{0, 1, 2, 3, 4\}$  is empty. Therefore the factor  $g(x)$ , although has some unimodular roots, does not lead to unimodular solutions.  $\square$

So it turns out that all complex Hadamard matrices with circulant core up to order 6 are well-known. This is not the case for order 7, as we have discovered a new, previously unknown complex Hadamard matrix,  $Q_7$ . The following is true.

**Theorem C.2.6.** *The complex Hadamard matrices with circulant core of order  $n+1 = 7$  are equivalent to one of  $F_7$ ,  $P_7 := P_7^{(1)}(1)$ ,  $P_7^*$  (see Example 3.2.2),  $Q_7$  or  $Q_7^*$  (see Example 3.3.25).*

*Remark C.2.7.* The list above might be redundant as it is unknown whether or not the matrices  $Q_7$  and  $Q_7^*$  are equivalent.  $\square$

*Proof.* Similarly to the  $n+1 = 6$  case we managed to compute a pure lexicographic Gröbner basis for the system of equations (C.1), which we extended with

$$ux_0x_1x_2x_3x_4x_5 = 1 \quad (\text{C.12})$$

as usual. Again, we found that there are finitely many solutions only and the polynomial  $\mathcal{X}_6(x)$ , describing all possible roots of the system of equations (C.1) is of degree 69. It is easy to recover the solutions corresponding to the known matrices  $F_7$  and  $P_7$  and additionally eliminate the factors without any unimodular roots. We are left with two polynomials, dividing  $\mathcal{X}_6(x)$ , namely

$$\begin{aligned} g_{7A}(x) &= 2x^6 + 2x^5 + 2x^4 - 5x^3 + 2x^2 + 2x + 2, \quad \text{and} \\ g_{7B}(x) &= 16x^{36} + 96x^{35} + 3584x^{34} + 54800x^{33} + 516276x^{32} + 3534368x^{31} + \dots, \end{aligned}$$

of degree 6 and 36, respectively, having unimodular roots. The polynomial  $g_{7A}(x)$  does not lead to any unimodular solutions, which can be seen in a similar way as we have excluded the degree 10 factor of order 6 during the proof of Proposition C.2.5. In particular, we should add  $g_{7A}(x_0)$  along with the dummy equations (C.12) and  $vx_0x_1x_2x_3 - 1 = 0$  to (C.1) and compute a Gröbner basis to find that the polynomial

$$v^6 + v^5 - 6v^4 - 13v^3 - 6v^2 + v + 1 \quad (\text{C.13})$$

is member of the ideal, generated by the aforementioned polynomials. By an application of Lemma C.2.2 we see that (C.13) does not have any unimodular roots and hence by Lemma C.2.3 (with  $S = \{0, 1, 2, 3\}$ ) there are no unimodular solutions in this case either.

It remains to deal with the degree 36 factor  $g_{7B}(x)$ . We start by transforming it through Lemma C.2.2 to obtain

$$T_{g_{7B}}(u) = 16u^{18} + 96u^{17} + 3296u^{16} + 53168u^{15} + 461092u^{14} + 2723792u^{13} + \dots \quad (\text{C.14})$$

By evaluating  $T_{g_{7B}}(u)$  at various rational points within the interval  $[-3, 3]$ , one can detect at least 6 real roots within the interval  $[-2, 2]$ . Therefore  $g_{7B}(x)$  has at least 12 distinct unimodular roots. By calculating various Gröbner basis with respect to various monomial ordering, one can see that if any of  $x_0, x_1, \dots, x_5$  comes from  $g_{7B}(x)$ , then the values of all additional variables are roots of  $g_{7B}(x)$  as well. Therefore, after solving (e.g. numerically) one of the obtained Gröbner basis containing  $g_{7B}(x_0)$ , we see that the unimodular solutions are being given by

$$\begin{aligned}(x_0, x_1, x_2, x_3, x_4, x_5) \approx & (-0.843295 + 0.537451\mathbf{i}, -0.627425 + 0.778677\mathbf{i}, \\ & -0.68299 - 0.730428\mathbf{i}, 0.0470571 + 0.998892\mathbf{i}, \\ & 0.342548 - 0.9395\mathbf{i}, 0.764105 - 0.645092\mathbf{i}),\end{aligned}$$

its reversed form, i.e.  $(x_5, x_4, x_3, x_2, x_1, x_0)$ , the conjugate of both and the cyclic permutations of all four, featuring the unimodular roots we detected through  $T_{g_{7B}}(u)$ . Hence, they correspond to a complex Hadamard matrix and its adjoint which we call  $Q_7$ .

Finally one should see that the matrices  $F_7$ ,  $P_7$ ,  $P_7^*$ ,  $Q_7$  and  $Q_7^*$  are inequivalent. It is trivial to distinguish the  $BH(7, 7)$  and  $BH(7, 6)$  matrices via Haagerup's invariant, while the inequivalence of  $P_7$  and  $P_7^*$  can be checked directly with a computer search. Lemma 1.4.8 guarantees that  $Q_7$  cannot be a Butson-Hadamard matrix as in its dephased form there are entries which are not roots of unity. Finally,  $Q_7$  and  $Q_7^T$  are trivially equivalent, but we do not know if the same holds for  $Q_7$  and  $Q_7^*$ .  $\square$

We are left with the following unsolved

**Problem C.2.8.** Investigate if the matrices  $Q_7$  and  $Q_7^*$  are equivalent.

More generally, we need to find new methods to distinguish a complex Hadamard matrix from its adjoint, conjugate and transpose in an efficient way.

**Problem C.2.9.** Find new criteria distinguishing a complex Hadamard matrix from its adjoint, conjugate and transpose, respectively.

There is some interest in describing roots of polynomial systems by radicals. A notable example is the problem of the existence of  $d^2$  equiangular lines in  $\mathbb{C}^d$  (see Section 2.4.4), where exact solutions are known only for  $d \leq 16$  and for  $d \in \{19, 24, 35, 48\}$ . These examples along with their closed analytic descriptions were found by various symmetry considerations and clever use of Gröbner-basis techniques, see e.g. [3], [122] and the references therein.

It seems that Landau and Miller [95] found a polynomial time algorithm to construct the splitting field of a polynomial whose roots can be described by radicals. Both their method and our elementary (but rather technical) considerations are far beyond the scope of this thesis, and we just mention the following without any further comment.

**Proposition C.2.10.** *The matrix  $Q_7$  can be described by radicals*

*Proof.* Let  $\alpha$  as in (3.42) and observe that  $\alpha^3 - 40169\alpha^2 + 122486812\alpha + 124134308 = 0$  and hence  $\alpha$  can be described by radicals. Define further

$$r = \frac{1}{2} \sqrt{\frac{-1394249317\alpha^2 + 4934112167907\alpha + 5004997560582}{3595497500}} + 2,$$

and  $\beta = 343\sqrt{7}(r + i\sqrt{1-r^2})$ . Then the degree 18 polynomial  $T_{g_{7B}}(u)$  (C.14) can be factored in the field extension  $\mathbb{Q}(\alpha)$  into a product of polynomials of degree 6 and 12, where the degree 6 factor  $h(u)$  encodes (twice) the real part of the entries of  $Q_7$  (see (3.43)). Additionally,  $h(u)$  can be factored in the field extension  $\mathbb{Q}(\alpha, \beta)$ , and hence all of its roots can be described by radicals, as stated.  $\square$

We were unable to proceed any further and classify higher order complex Hadamard matrices with circulant core due to insufficient computing power. However, in higher orders one might try conducting various numerical experiments in order to discover at least some examples of complex Hadamard matrices. One reasonable approach is attempting to minimize the function

$$F(x_0, \dots, x_{(n-1)^2}) = \|H(x_0, \dots, x_{(n-1)^2})H^*(x_0, \dots, x_{(n-1)^2}) - nI\|,$$

where  $H$  is a dephased matrix of order  $n$  with an otherwise unspecified core. These type of searches are (in general) inconclusive due to the large number of variables, because the minima values found are not necessarily capture the global minimum of the function. However, if one significantly reduces the number of variables (as in the case when circulant matrices or Hadamard matrices with circulant core are considered) then there might be some hope to extract some interesting examples.

Such a numerical method was used in [6] and in our Master's thesis [133], where new examples of complex Hadamard matrices were obtained. In particular, we exhibited a  $9 \times 9$  complex Hadamard matrix  $Q_9$  with circulant core, whose core was induced by a vector  $x = (a, b, c, d, \bar{a}, \bar{b}, \bar{c}, \bar{d})$ . The entries  $a, b, c$  and  $d$  are rather complicated, nevertheless they can be described by closed analytic formulae. Here we report on new examples of order 11 which were, again, first discovered by the numerical method indicated above, and then their existence was confirmed by Gröbner basis techniques.

**Example C.2.11.** Here we describe two symmetric complex Hadamard matrices of order 11 with circulant core. The core is induced by the vector  $x = (a, b, \bar{b}, c, \bar{c}, \bar{a}, \bar{c}, c, \bar{b}, b)$ , where the values of  $a, b$  and  $c$  can be obtained as follows. Let

$$\gamma = \frac{1}{3} \sqrt{396 + 18 \sqrt[3]{8468 + 12\sqrt{12309}} + 3 \sqrt[3]{1829088 - 2592\sqrt{12309}}},$$

and let  $a_1, a_2 \neq \overline{a_1}$  and their conjugate be the four roots of the polynomial

$$1008a^4 - (336\gamma - 1344)a^3 - (\gamma^5 - 132\gamma^3 - 56\gamma^2 + 1088\gamma + 1232)a^2 - (336\gamma - 1344)a + 1008.$$

It is easy to see (either by transforming the polynomial via Lemma C.2.2 or by an application of Theorem 2.3.30) that both  $a_1$  and  $a_2$  are unimodular. Further, let

$$b + c = -\frac{1}{48} (30a^7 + 53a^6 - 83a^5 - 56a^4 + 117a^3 - 176a^2 + 103a + 59).$$

From this last equation  $b$  and  $c$  can be obtained via the Decomposition formula (see Lemma 2.3.4). For a fixed value of  $a$  the order of  $b$  and  $c$  is irrelevant, as both choices lead to a complex Hadamard matrix or its conjugate. It is unknown whether or not these matrices are equivalent. However, the two essentially different matrices, arising from  $a_1$  and  $a_2$ , have different fingerprints, and as a result they correspond to inequivalent complex Hadamard matrices of order 11. We call these matrices  $Q_{11A}$  and  $Q_{11B}$ , respectively.

Despite the efforts of this chapter the existence of complex Hadamard matrices with circulant core remains an open problem in general. We conclude with the following

**Problem C.2.12.** For every  $n \geq 1$  construct a complex Hadamard matrix with circulant core of order  $n$ , or show that no such a matrix exists.