universität wien

MASTERARBEIT

Titel der Masterarbeit

"Construction of Hadamard Matrices"

verfasst von

Christiane Schütz, BSc

angestrebter akademischer Grad

Master of Science (MSc)

Wien, 2015

Studienkennzahl lt. Studienblatt:	A 066 821
Studienrichtung lt. Studienblatt:	Masterstudium Mathematik
Betreuer:	ao. Univ. Prof. Dr. Christoph Baxa

Abstract

Hadamard matrices are an important topic in the field of combinatorical designs and many applications. In this master thesis all common constructions of Hadamard matrices are detailly explained. The first part is a short summary about the history of this topic and the second introduces the constructions of Sylvester, Williamson, Paley and Goethals/Seidl. In addition, a chapter concentrates on the equivalences classes that can be defined for Hadamard matrices. In between, the basic algebraic knowledge that is needed to understand some constructions is offered. A special focus of this thesis are Hadamard designs which are explained in Chapter five. Furthermore, the strong connection between bent functions and Hadamard matrices is presented at the end of chapter five. The last chapter has a look on the future of Hadamard constructions, namely cocyclic matrices.

Hadamard Matrizen sind ein wichtiges Thema in dem Gebiet der kombinatorischen Designs und vieler Anwendungen. Diese Masterarbeit beschäftigt sich mit den wichtigsten Konstruktionen von Hadamard Matrizen. Das erste Kapitel bietet eine historische Zusammenfassung dieses Themas. Das zweite Kapitel erklärt die Konstruktionen von Sylvester, Williamson, Paley und Goethals/Seidl. Zusätzlich konzentriert sich ein Kapitel vollständig auf die Äquivalenzklassen, die man für Hadamard Matrizen definieren kann. Dazwischen befindet sich ein Kapitel, das das wichtigste algebraische Wissen vermittelt, um alle Konstruktionen verstehen zu können. Diese Arbeit konzentriert sich weiters speziell auf Hadamard Designs. Diese werden im fünften Kapitel erklärt. Des Weiteren wird am Ende dieses Kapitels die starke Beziehung zwischen Bentfunktionen und Hadamard Matrizen präsentiert. Das letzte Kapitel betrachtet die Zukunft der Konstruktionen von Hadamard Matrizen, nämlich Kozyklische Matrizen.

Acknowledgement/Danksagung

Ich möchte mich bei meinem Betreuer Prof. Christoph Baxa bedanken, der mich das Thema meiner Masterarbeit frei auswählen ließ und dieses neue Gebiet mit mir gemeinsam erschloss.

Ein spezieller Dank gilt meiner Familie insbesondere meinen Eltern Irmgard und Josef Schütz, die mich immer unterstützt haben und für mich da waren; meine Freunden, die mich immer wieder motiviert haben.

Darüber hinaus waren Marvin Fuchs und Nora Tischler eine wichtige Unterstützung um die Masterarbeit sprachlich zu korrigieren.

Contents

1. Introduction and History

The following brief introduction and summary of Hadamard matrices is general and can be found in nearly all literature on this topic, but [19] and [10] can be highly recommended.

Hadamard Matrices have been a topic of interest for researchers for nearly 150 years. A Hadamard matrix A is an $n \times n$ matrix formed by ones and minus ones that satisfies a kind of orthogonality condition, namely that $AA^T = nI$. J. J. Sylvester was the first person interested in this kind of matrices in 1867 and his idea of constructing Hadamard matrices is still the easiest one (see [24]). Nevertheless, they are named after Jacques Salomon Hadamard who was the first to prove simple properties of of Hadamard matrices in 1893. What makes the matrices so interesting is the following: The easiest questions on that topic probably have the hardest answers. When you introduce the topic to a mathematical student who has never heard about it, the first questions that arise seem to be "left for practice "-questions. Do Hadamard matrices exist for every size? How many different Hadamard matrices are there of one size? But in fact these questions are still unsolved. There are various ways to tackle them.

The first way is to find a construction that leads to Hadamard matrices methodically. Many ways of constructing Hadamard matrices will be introduced on the next pages. Paley made a lot of progress on an algebraic way in 1933 [20].

Constructing Hadamard Matrices can also be done in a combinatorical way as Williamson matrices will show. Although combinatorical designs are still a subdomain of combinatorics, it has a strong connection to finite fields which will revise in the fourth chapter.

There are also attempts to show just an existence proof (see for instance [17]).

The question how many of them exist will lead to the equivalence classes of Hadamard matrices, but this topic is even more unresolved then the pure existence.

There is also a significant interest in circulant Hadamard matrices, in more-dimensional and also in complex Hadamard matrices.

The reason why the Hadamard Conjecture is still of interest now lies in the applications of the matrices in the field of coding theory, cryptology, signal processing, image analysis and so on.

Of course, as it is also a part of linear algebra, the determinant of a Hadamard matrix seems to be interesting, too. This question is easy to answer as it will be shown that it is $n^{\frac{n}{2}}$. That is just a small part of what Hadamard showed in his paper [6]. A big conjecture called "the Hadamard determinant problem" is: How can the entries of an $n \times n$ matrix be filled with 1s and -1s, so that it has maximum determinant? Hadamard proved in his paper that the upper bound of the determinant is $n^{\frac{n}{2}}$ and the maximum can be reached if and only if the matrix is Hadamard.

The second chapter will show the basic definitions, properties and the most common constructions of Hadamard matrices. The third one will give a sneak peek of the problem

to find the equivalence classes of Hadmard matrices and the fourth chapter will clarify some preliminaries that may be used before and needed for the last chapter. The fifth chapter explains combinatorical ways to find Hadamard matrices.

2. Basic definitions and properties

There are many ways to define Hadamard matrices. One alternative definition is proved as a lemma. The next section is mostly following [29], [28].

Definition 2.1. *An $n \times n$ matrix H_n is called a Hadamard matrix if all entries are 1 or -1 and the rows are orthogonal.*

Definition 2.2. *I_n denotes the unit matrix and it is often written I if the size is obvious. Similary the matrix J_n which is the $n \times n$ matrix consisting only of ones is sometimes written J. $e_n = (1, \ldots, 1)$ is the unit vector with length n and $e_n^T = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$*

Lemma 2.3. *Let A be an $n \times n$ matrix with entries that are 1 or -1. Then A is Hadamard if its columns are orthogonal. Or alternatively, A is Hadamard if and only if*

$$AA^T = nI.$$

Proof. The first part means that per definition a Hadamard matrix has orthogonal rows and columns. This follows from the second part. If the equation $AA^T = nI$ holds, then $\frac{1}{\sqrt{n}}A$ is orthogonal and hence also the columns must be orthogonal.
For the second part, suppose $A = (a_{ij})_{1 \leq i,j \leq n}$ to be Hadamard. All the off-diagonal entries in AA^T must be zero as A has orthogonal rows. The diagonal entries are $\sum_{i=1}^{n} a_{ki}^2 : \forall\, 1 \leq k \leq n$. The entries of A can only be 1 and -1. Consequently, the sum must be n. Putting all together it follows that $AA^T = nI$. On the other hand, from the equation $AA^T = nI$ it follows that for all $j \neq k$ the sum $\sum_{i=1}^{n} a_{ji} \cdot a_{ki}$ is 0. This means that the rows are orthogonal.

□

The following proposition leads to the Hadamard Conjecture.

Proposition 2.4. *There can only exist Hadamard matrices of the size 1,2 and a multiple of 4.*

Proof. A Hadamard matrix of size 1 is (1) and an example of a Hadamard matrix of size 2 is $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Let $A = (a_{ij})_{1 \leq i,j \leq n}$ be a Hadamard matrix and $n \geq 3$. By definition it

follows that

$$\sum_{k=1}^{n} a_{ik}a_{jk} = \begin{cases} 0, & \text{if } i \neq j \\ n, & \text{if } i = j \end{cases}.$$

Keeping that in mind, consider the sum

$$\sum_{k=1}^{n}(a_{1k}+a_{2k})(a_{1k}+a_{3k}) = \sum_{k=1}^{n}(a_{1k}^2 + a_{1k}a_{3k} + a_{2k}a_{1k} + a_{2k}a_{3k}) =$$

$$= \sum_{k=1}^{n} a_{1k}^2 + \underbrace{\sum_{k=1}^{n} a_{1k}a_{3k}}_{=0} + \underbrace{\sum_{k=1}^{n} a_{2k}a_{1k}}_{=0} + \underbrace{\sum_{k=1}^{n} a_{2k}a_{3k}}_{=0} = \sum_{k=1}^{n} 1 = n.$$

As A is Hadamard $(a_{1k} + a_{2k})$ and $(a_{1k} + a_{3k})$ can only be 2, 0 or -2. Therefore, n is divisible by 4 and therefore a multiple of 4.

□

Immediately the question arises if equivalence is true in the lemma, but this problem is still unsolved and called the Hadamard Conjecture.

Conjecture 2.5 (Hadamard conjecture)**.** *Does a Hadamard matrix exists for every multiple of 4?*

The ad-hoc attempt would be to create a construction that solves the problem and indeed there are many constructions that solve the problem for some multiple of 4, but not for all. Currently it seems quite unlikely to find a universal construction for Hadamard matrices, but most researchers believe that the conjecture is true.

First, some examples are given and basic properties stated.

Example. *Here are examples of Hadamard matrices of size 4 and 8.*

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

Proposition 2.6. *The determinant of an $n \times n$ Hadamard matrix is $n^{n/2}$.*

Proof. Let H_n be a Hadamard matrix, consequently the equation $H_n {H_n}^T = nI_n$ holds. From $\det(nI_n) = n^n$ it follows that $\det(H_n \cdot {H_n}^T) = n^n$. As $\det(H_n) = \det(H_n^T)$ the equation changes to $\det(H_n)^2 = n^n$, hence the property follows. □

There exists a lower bound of the size of a Hadamard matrix.

Proposition 2.7. *Let H_n be an $n \times n$ Hadamard matrix and J_m a submatrix, then $n \geq m^2$.*

To prove the proposition we need another important definition and property.

Definition 2.8. *A matrix is circulant if it is of the form*

$$C = \begin{pmatrix} c_0 & c_1 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & \cdots & c_{n-2} \\ \vdots & \vdots & \cdots & \vdots \\ c_1 & c_2 & \cdots & c_0 \end{pmatrix}. \tag{2.1}$$

As C can be deduced from one row, it is also written $C = circ(c_0, c_1, \ldots, c_{n-1})$.

Remark. *A square matrix C is circulant if and only if $C = PCP^T$, where P is the $n \times n$ primary circulant matrix*

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Both directions are easy to show by direct verification as left multiplication with P and right multiplication with P^T is shifting the first column and the first row to the end of the matrix.

For the proof of the following 2.10 a Lemma of linear algebra has to be revised.

Lemma 2.9. *Let f be a polynomial. If $A = f(P)$ for any matrices A, P and λ is an eigenvalue of P then $f(\lambda)$ is an eigenvalue of A.*

Proof. Let λ be an eigenvalue for P and v an eigenvector, then $Pv = \lambda v$. As f is a polynomial it follows that $Av = f(P)v = f(\lambda)v$. Consequently, $f(\lambda)$ is an eigenvalue of A. □

Lemma 2.10. *Let C be a circulant matrix of the form (2.1) with entries in $\mathbb{C}$ and consider the polynomial $f(\lambda) = c_0 + c_1\lambda + \cdots + c_{n-1}\lambda^{n-1}$. Then the eigenvalues of C are $f(\omega^k)$ where $k \in \{0, 1, \ldots, n-1\}$ and $\omega = e^{\frac{2\pi i}{n}}$ denotes the $n-$th complex root of unity.*

Proof. It is easy to see that $C = c_0 I_n + c_1 P + \cdots + c_{n-1}P^{n-1}$, where P is the primary circulant matrix (see remark above) and hence $f(P) = C$. As a result, it is sufficient to compute the eigenvalues of P (Lemma 2.9). Using Laplace expansion of determinant on the first column, it follows that $\det(\lambda I_n - P) = \lambda^n - 1$. Hence, the eigenvalues of P are ω^k for $k \in \{0, 1, \cdots n-1\}$ and the eigenvalues of C are $f(\omega^k)$. □

With this knowledge, proposition 2.7 can be proved.

Proof. By changing rows and columns it can be assumed without loss of generality (w.l.o.g.) that H_n can be written in the form

$$H_n = \begin{pmatrix} J_m & X \\ Y & Z_s \end{pmatrix}$$

with Z_s a $(\pm 1)-$ valued $s \times s$ matrix and $m + s = n$. As H_n is Hadamard it follows

$$\begin{aligned} H_n {H_n}^T &= (s+m)I_n \\ J_m^2 + XX^T &= (s+m)I_m \\ XX^T = (s+m)I_m - J_m^2 = (s+m)I_m - mJ_m &= \\ \begin{pmatrix} s & -m & \cdots & -m \\ -m & s & \cdots & -m \\ \vdots & \vdots & \vdots & \vdots \\ -m & -m & \cdots & s \end{pmatrix}&. \end{aligned}$$

That matrix is circulant and using Lemma 2.10 with the polynomial $f(X) = sX^0 - mX - mX^2 - \cdots - mX^{m-1}$ it follows that the eigenvalues are $f(1) = s - m(m-1) = s - m^2 + m$ and

$$f(\omega^k) = s - m(\omega^k + (\omega^k)^2 + \cdots + (\omega^k)^{m-1}) = s - m \cdot (-1) = s + m$$

for all $k \in \{1, \ldots, m-1\}$. Consequently, the eigenvalue $s + m$ has algebraic multiplicity $m - 1$. As XX^T is positive semi-definite per definition, it only has non-negative eigenvalues, so it follows that $m + s - m^2 \geq 0 \Rightarrow m + s = n \geq m^2$ □

Circulant Hadamard matrices are interesting, but they are rare. In fact, the following conjecture is nearly proved in [22].

Conjecture 2.11 (Ryser Conjecture)**.** *Let H_n be a circulant Hadamard matrix, then $n = 1$ or $n = 4$.*

Example. *Nevertheless, there are a lot of examples of circulant Hadamard matrices of order 4. For instance*

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

There are many other Hadamard matrices with additional properties. The following definitions list the most important ones. The next part is following mostly [28] and for partly more detailed proofs see [26].

Definition 2.12. *A Hadamard matrix is called regular if the sum of each row is equal which means that every row contains the same number of +1s, therefore also of (-1)s.*

Definition 2.13. *A Hadamard matrix is normalised if it is Hadamard and the first row and the first column contain only ones.*

Every Hadamard matrix can be normalised. This follows from the following proposition.

Proposition 2.14. *The set of Hadamard matrices is closed under the following transformations*

(1) *transposing*
(2) *negating rows or columns*
(3) *permuting rows or columns*

Proof. (1) follows from Lemma 2.3.
(2) and (3) are clear as definition 2.1 can be understood in the following way: A (± 1)-valued $n \times n$ matrix is Hadamard if and only if $\sum_{k=1}^{n} h_{ik} \cdot h_{jk} = 0 : i \neq j$. The equation still clearly holds under such transformation. □

Definition 2.15. *A Hadamard matrix H_n is skew if it can be written in the form $H_n = S + I_n$ with $S^T = -S$.*

Lemma 2.16. *Let H_n be a skew Hadamard matrix, then $SS^T = (n-1)I_n$.*

Proof. By definition $H_n H_n^T = nI_n$ and $H_n = S + I_n$ hold. Putting these together, it follows that

$$\begin{aligned}(I_n + S) \cdot (I_n + S)^T &= nI_n \\ I_n + S^T + S + SS^T &= nI_n \\ I_n + SS^T &= nI_n \\ SS^T &= (n-1)I_n.\end{aligned}$$

□

As a skew Hadamard matrix is $(\pm)1-$valued, it can be deduced from the condition $H_n = S + I_n$ that the entries on the diagonal of S can only be - 2 or 0, but -2 is impossible as S is skew-symmetric. Hence, S has a zero diagonal and by multiplying some rows or columns with (-1) can be chosen to have the form

$$S = \begin{pmatrix} 0 & e_{n-1} \\ -e_{n-1}^T & W \end{pmatrix}. \tag{2.2}$$

Definition 2.17. *Let H_n be a skew Hadamard matrix and $H_n = S + I_n$ where S is written in the form 2.2. W is called the kernel of H_n.*

Definition 2.18. *Let M and N be two $n \times n$ Hadamard matrices. M is skew and N is symmetric . The pair is called amicable Hadamard matrices if $MN = NM^T$, as a result MN is symmetric.*

Lemma 2.19. *Let M, N be two amicable $n \times n$ Hadamard matrices. Let $M = S + I_n$, then $SN = NS^T$, hence SN is also symmetric.*

Proof. Using $MN = NM^T$ leads to

$$\begin{aligned}(S + I_n)N &= N(S + I_n)^T \\ SN + N &= NS^T + N.\end{aligned}$$

□

2.1. **Sylvester Hadamard matrices**

In this part the first construction of Hadamard matrices is presented which was introduced by Sylvester in 1867. It can be found in [29], [8] or [28].

Definition 2.20. *The Kronecker product of $A = (a_{ij})_{1 \le i,j \le m}$ and an $n \times n$ - matrices $B_1, B_2 \cdots, B_m$ is*

$$\begin{pmatrix} a_{11}B_1 & a_{12}B_1 & \cdots & a_{1m}B_1 \\ a_{21}B_2 & a_{12}B_2 & \cdots & a_{1m}B_2 \\ \vdots & \vdots & \cdots & \vdots \\ a_{m1}B_m & a_{m2}B_m & \cdots & a_{mm}B_m \end{pmatrix}$$

or compactly written as $A \otimes [B_1, B_2, \cdots, B_m]$. If $B_1 = B_2 = \cdots = B_m = B$ then it is denoted by $A \otimes B = [a_{ij}B]_{1 \le i,j \le m}$.

Lemma 2.21. *If A, B, C and D are any matrices then*

$$\begin{aligned}(A \otimes B)^T &= A^T \otimes B^T \\ (A \otimes B)(C \otimes D) &= AC \otimes BD.\end{aligned}$$

For the second part AC and BD must exist.

Proof.

$$(A \otimes B)^T = \begin{pmatrix} a_{11}B & \cdots & a_{1m}B \\ \vdots & \cdots & \vdots \\ a_{m1}B & \cdots & a_{mm}B \end{pmatrix}^T = \begin{pmatrix} a_{11}B^T & \cdots & a_{m1}B^T \\ \vdots & \cdots & \vdots \\ a_{1m}B^T & \cdots & a_{mm}B^T \end{pmatrix} = A^T \otimes B^T$$

$(A \otimes B)(C \otimes D)$ has the $(i,j)-$block entry

$$\sum_k (a_{ik}B)(c_{kj}D) = \left(\sum_k a_{ik}c_{kj}\right) BD$$

The last bracket term is the $(i,j)-$ entry of AC and the lemma follows. □

Theorem 2.22. *If A is an $n \times n$ Hadamard matrix and B an $m \times m$ Hadamard matrix, then $A \otimes B$ is an $mn \times mn$ Hadamard matrix.*

Proof. (It is easy to see that the Kronecker product of A and B must be $(\pm 1)-$ valued, consequently it is left to prove that $(A \otimes B)(A \otimes B)^T = mnI_{mn}$. Using Lemma 2.21 it can be calculated that

$$\begin{aligned}(A \otimes B)(A \otimes B)^T &= (A \otimes B)(A^T \otimes B^T) \\ &= AA^T \otimes BB^T \\ &= mI_m \otimes nI_n \\ &= mnI_{mn} \\ &.\end{aligned}$$

The last equation follows by using the definition of the Kronecker product. □

Corollary 2.23. *Let A_i be a Hadamard matrix of order m_i for $1 \leq i \leq t$. Then $A_1 \otimes A_2 \otimes \cdots \otimes H_t = \bigotimes_{i=1}^t H_i$ is a Hadamard matrix of order $\prod_{i=1}^t m_i$.*

Proof. By induction using theorem 2.22. □

Corollary 2.24. *Let $S^1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, then S^1 is Hadamard and $S_t = \bigotimes^t S^1$ is a Hadamard matrix of order 2^t, for $t \geq 1$.*

Proof. By direct verification and 2.23. □

Definition 2.25. *The Hadamard matrices defined in 2.24 are called Sylvester matrices.*

This construction was not only the beginning of Hadamard matrix theory, but it is still one of the most important constructions as it leads **straightforward** to Hadamard matrices of size 2, 4, 8, 16, 32 and so on. With that construction many multiples of 4 can be covered!

2.2. **Williamson Hadamard matrices**

"The Williamson construction is the simplest of many powerful plug-in methods for finding Hadamard matrices." ([8], p.15.)

Lemma 2.26. *If there exist* $(\pm 1)-$ *valued matrices A,B,C and D of order n satisfying*

(1) $AA^T + BB^T + CC^T + DD^T = 4nI_n$
(2) $XY^T = YX^T$ *with* $X, Y \in \{A, B, C, D\}$

then

$$H_{4n} = \begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix}$$

is a $4n \times 4n$ *Hadamard matrix.*

Proof. The obviously (± 1)-valued matrix H_{4n} has to satisfy $H_{4n}H_{4n}^T = 4nI_{4n}$. Hence the diagonal element $AA^T + BB^T + CC^T + DD^T$ has to be $4nI_n$ and this is the precondition (1).
On the other hand the off-diagonal elements have to be zero. By direct verification via multiplication it is seen that it is true if $XY^T = YX^T$ with $X, Y \in \{A, B, C, D\}$. □

Definition 2.27. *The matrices* A, B, C *and* D *defined in 2.26 are called Williamson matrices, but often that term also refers to the resulting matrix* H_{4n}. *Note that* A, B, C *and* D *are not required to be symmetric and circulant, but it is often included in the definition of Williamson matrices.*

Keep in mind that if two matrices X, Y are required to be circulant then $XY = YX$. If they are in addition symmetric then $XY^T = XY = YX = YX^T$. In the following, it is required that Williamson matrices have to be circulant and symmetric. To comprehend the requirements, if A, B, C and D are Williamson matrices then the following three conditions are true

$$X = X^T \text{ for } X \in \{A, B, C, D\} \tag{2.3}$$

$$XY = YX \text{ for } X, Y \in \{A, B, C, D\} \tag{2.4}$$

$$A^2 + B^2 + C^2 + D^2 = 4nI_n. \tag{2.5}$$

In the next part, some ideas are presented that lead to an algorithm for finding Hadamard matrices. Williamson matrices are now described in a slightly different way. Consider the permutation matrix

$$U = \text{circ}(0, 1, 0, \cdots, 0) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

Now the Williamson matrices

$$\begin{aligned} A &= \operatorname{circ}(a_0, a_1, a_2, \cdots, a_{n-1}) \\ B &= \operatorname{circ}(b_0, b_1, b_2, \cdots, b_{n-1}) \\ C &= \operatorname{circ}(c_0, c_1, c_2, \cdots, c_{n-1}) \\ D &= \operatorname{circ}(d_0, d_1, d_2, \cdots, d_{n-1}) \end{aligned}$$

can be written by using U:

$$A = a_0 I_n + a_1 U + a_2 U^2 + \cdots + a_{n-1} U^{n-1} \tag{2.6}$$

$$B = b_0 I_n + b_1 U + b_2 U^2 + \cdots + b_{n-1} U^{n-1} \tag{2.7}$$

$$C = c_0 I_n + c_1 U + c_2 U^2 + \cdots + c_{n-1} U^{n-1} \tag{2.8}$$

$$D = d_0 I_n + d_1 U + d_2 U^2 + \cdots + d_{n-1} U^{n-1} \tag{2.9}$$

For a better understanding, right-multiplication with U shifts all the elements diagonally one position to the right as $U^n = I_n$. Multiplying with U^2 shifts all elements diagonally two positions to the right and so on. Consequently, for example A is

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-2} \\ \vdots & \vdots & \cdots & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}$$

As these matrices should be Williamson it follows that $a_{n-1} = a_1, a_{n-2} = a_2, \cdots$. So in general the entries satisfy

$$a_{n-i} = a_i, b_{n-i} = b_i, c_{n-i} = c_i, d_{n-i} = d_i \text{ for } 1 \leq i \leq n-1 \tag{2.10}$$

To summarize:

Lemma 2.28. *The matrices defined by 2.6-2.9 are circulant, symmetric Williamson matrices that are defined by equations 2.3 - 2.5 if 2.10 and 2.5 hold.*

Proof. It is clear that 2.3 and 2.5 hold. Condition 2.4 is verified directly via multiplication and using preliminary 2.10. □

Theorem 2.29. *If n is odd and the matrices A, B, C, D of order n defined by 2.6 - 2.9 satisfy 2.10 and 2.5, then the coefficients satisfy*

$$a_i + b_i + c_i + d_i = \pm 2 : 1 \leq i \leq n-1.$$

Further, let $W_1 = (A + B + C - D)/2$, $W_2 = (A + B - C + D)/2$, $W_3 = (A - B + C + D)/2$, $W_4 = (-A + B + C + D)/2$, then 2.5 is equivalent to $W_1^2 + W_2^2 + W_3^2 + W_4^2 = 4nI_n$.

Proof. It can assumed w.l.o.g. that $a_0 = b_0 = c_0 = d_0 = 1$, because if any of these entries is (-1) then multiplying with (-1) does not change the preliminaries. The Williamson matrices can be rewritten in the form $A = P_1 - N_1, B = P_2 - N_2, C = P_3 - N_3, D = P_4 - N_4$ with

$$P_1 = \sum_{\substack{0 \le i \le n-1 \\ a_i = 1}} U^i, \quad N_1 = \sum_{\substack{0 \le i \le n-1 \\ a_i = -1}} U^i$$
$$P_2 = \sum_{\substack{0 \le i \le n-1 \\ b_i = 1}} U^i, \quad N_2 = \sum_{\substack{0 \le i \le n-1 \\ b_i = -1}} U^i$$
$$P_3 = \sum_{\substack{0 \le i \le n-1 \\ c_i = 1}} U^i, \quad N_3 = \sum_{\substack{0 \le i \le n-1 \\ c_i = -1}} U^i$$
$$P_4 = \sum_{\substack{0 \le i \le n-1 \\ d_i = 1}} U^i, \quad N_4 = \sum_{\substack{0 \le i \le n-1 \\ d_i = -1}} U^i$$

Furthermore, it is easy to see that $N_i + P_i = J_n$ for $1 \le i \le 4$. From 2.28 it follows that $\sum_{i=1}^{4}(P_i - N_i)^2 = 4nI_n$ and that leads to $\sum_{i=1}^{4}(2P_i - J_n)^2 = 4nI_n$. As $U^i J_n = J_n = J_n U^i$, it follows that $P_i J_n = J_n P_i$ for all i. Let $\mathcal{P} = \{i \mid 0 \le i \le n-1 \wedge a_i = 1\}$ and let $p_1 = |\mathcal{P}|$ and p_2, p_3, p_4 defined analogously. This definition leads to $J_n P_i = P_i J_n = p_i J_n$ by definition of p_i. As a consequence the equation $\sum_{i=1}^{4}(2P_i - J_n)^2 = 4nI_n$ can be simplified to

$$\sum_{i=1}^{4}(4P_i^2 - 4P_i J_n + J_n^2) = 4nI_n$$
$$\sum_{i=1}^{4} 4P_i^2 - \sum_{i=1}^{4} 4P_i J_n + \sum_{i=1}^{4} J_n^2 = 4nI_n$$
$$4\sum_{i=1}^{4} P_i^2 - 4\sum_{i=1}^{4} p_i J_n + 4nJ_n = 4nI_n \quad | : 4$$
$$\sum_{i=1}^{4} P_i^2 = \left(\sum_{i=1}^{4} p_i - n\right) J_n + nI_n$$

Combining $a_0 = b_0 = c_0 = d_0 = 1$ and 2.10 with the fact that n is odd, leads to the conclusion that p_i has to be odd for all i. As a result, the sum of the four p_i is even and so $\sum_{i=1}^{4} p_i - n$ is odd. It follows that

$$\sum_{\substack{0 \le i \le n-1 \\ a_i = 1}} U^{2i} + \sum_{\substack{0 \le i \le n-1 \\ b_i = 1}} U^{2i} + \sum_{\substack{0 \le i \le n-1 \\ c_i = 1}} U^{2i} + \sum_{\substack{0 \le i \le n-1 \\ d_i = 1}} U^{2i} \equiv J_n + I_n \mod 2.$$

From the right side of the equation it follows that the sum on the left side has to be 0 mod 2 on the diagonal which appears naturally as it is assumed that $a_0 = b_0 = c_0 = d_0 = 1$. On the other hand, the sum has to be 1 mod 2 off-diagonal. A sum of possible four 1s

can only be 1 mod 2 if there appears only one 1 or if there are three 1s. In conclusion, the family $\{a_i, b_i, c_i, d_i\}, i \neq 0$ contains one or three ones. That leads to $a_i + b_i + c_i + d_i = \pm 2$. The equivalence of 2.5 and $W_1^2 + W_2^2 + W_3^2 + W_4^2 = 4nI_n$ is given as the matrices A, B, C, D are commutative by 2.4 and the following remark. □

Remark. *Note that A, B, C, D can easily be reconstructed from W_1, W_2, W_3, W_4 with $A = (W_1 + W_2 + W_3 - W_4)/2,\ B = (W_1 + W_2 - W_3 + W_4)/2,\ C = (W_1 - W_2 + W_3 + W_4)/2,\ D = (-W_1 + W_2 + W_3 + W_4)/2$.*

Lemma 2.30. *Let n be odd and A, B, C, D defined as in theorem 2.29. They exist if and only if there exist symmetric W_1, W_2, W_3, W_4 satisfying*

(1) $W_1^2 + W_2^2 + W_3^2 + W_4^2 = 4nI_n$
(2) $W_i = I \pm U^{j_1} \pm U^{j_2} \pm \cdots \pm U^{j_s}$
for $\{j_1, j_2, \ldots, j_s\} \subseteq \{1, 2, \ldots, n-1\}$
(3) *Every U^{j_s}-term from (2) appears in only one $W_i, 1 \leq i \leq 4$*

Proof. The if-part follows mainly from theorem 2.29.
As A, B, C, D are symmetric, $W_1 = (A+B+C-D)/2,\ W_2 = (A+B-C+D)/2,\ W_3 = (A-B+C+D)/2,\ W_4 = (-A+B+C+D)/2$ are symmetric, too.
The first proposition follows directly from 2.29. Furthermore, in theorem 2.29 it is shown that $a_i + b_i + c_i + d_i = \pm 2$ for $1 \leq i \leq n-1$. This leads to $a_i + b_i + c_i - d_i \in \{-4, 0, 4\}$ and comparing this with the definition of W_1 it leads to $W_1 = I \pm U^{j_1} \pm U^{j_2} \pm \cdots \pm U^{j_s}$ where $\{j_1, j_2, \ldots j_s\} \subseteq \{1, 2, \ldots, n-1\}$ and $a_{j_k} + b_{j_k} + c_{j_k} - d_{j_k} = \pm 4$ for $1 \leq k \leq s$. Of course, the same is valid for the other W_is. As $a_{j_k}, b_{j_k}, c_{j_k}, d_{j_k}$ can only be one or minus one, the sum $a_{j_k} + b_{j_k} + c_{j_k} - d_{j_k} = \pm 4$ implies that there are only two possibilities, namely $a_{j_k} = b_{j_k} = c_{j_k} = 1 \wedge d_{j_k} = -1$ or $a_{j_k} = b_{j_k} = c_{j_k} = -1 \wedge d_{j_k} = 1$. If in that sum the minus is changed to a plus and one plus to a minus, then the sum is zero. Therefore, (3) has been shown.
On the other hand, all conditions are fulfilled if the construction to get A, B, C, D back is used. □

From Lemma 2.10 it follows that U can be decomposed in $U = SDS^{-1}$ with D being the diagonal matrix $\mathrm{diag}(1, \omega^2, \cdots, \omega^{n-1})$ and S is a non-singular matrix. Consequently, from 2.30 it follows that the Williamson matrices W_i can be written in the form

$$W_i = S(I \pm D^{j_1} \pm \cdots \pm D^{j_s})S^{-1}.$$

And condition (3) in Lemma 2.29 changes to

$$\sum_{i=1}^{4} (I \pm D^{j_i} \pm \cdots \pm D^{j_s})^2 = 4nI_n.$$

Comparing the $(1, 1)$ entry on both sides of the matrix equation, it follows that

(2.11)
$$(1\pm2\pm2\pm\cdots\pm2)^2+(1\pm2\pm2\pm\cdots\pm2)^2+(1\pm2\pm2\pm\cdots\pm2)^2+(1\pm2\pm2\pm\cdots\pm2)^2=4n.$$

Keep in mind that there can only be $(n-1)$ summands ±2 in the whole sum on the left side (compare Lemma 2.29 (2), (3)).
The last step, before writing down the algorithm, is the following theorem by Lagrange. A proof can be found in nearly every number theory book.

Theorem 2.31 (Lagrange's four square theorem)**.** *Every positive integer n can be decomposed into the sum of squares $n=a^2+b^2+c^2+d^2$. Moreover, if n is odd, then 4n can be decomposed into the summation of four odd squares.*

Algorithm. (1) *For a given n decompose 4n into the sum of four odd squares.*
(2) *Compare the solution of (1) with equation 2.11 and note Lemma 2.30 (2),(3). Then the j_k of Lemma 2.30 are found.*
(3) *Calculate the W_is with Lemma 2.30 (2).*
(4) *Calculate A, B, C and D from the W_is with the use of 2.26.*

Example. *To give an easy example of how the algorithm works, we take n = 5. In this way a Hadamard matrix of size 20 can be found.*

(1) *To find a decomposition for 20 is not hard.* $20=3^2+3^2+1^2+1^2$.
(2) *As there are only four j_i to find, the possibilties to decompose the sum have to be* $(1\pm\_\pm\_\pm\_\pm\_)^2+(1\pm\_\pm\_\pm\_\pm\_)^2+(1\pm\_\pm\_\pm\_\pm\_)^2+(1+\pm\_\pm\_\pm\_\pm\_)^2$. *Keep in mind that if in one bracket an empty space is filled with 2 or -2, then the space is zero in the other brackets and of course the first two brackets have to sum up to three and the others to 1.*

One possibilty to decompose is

$$(1-2\pm0\pm0-2)^2+(1\pm0-2-2\pm0)^2+(1\pm0\pm0\pm0\pm0)^2+(1\pm0\pm0\pm0\pm0)^2.$$

A special order is chosen in this decomposition, but other orders also lead to Hadamard matrices which are maybe different or equivalent to other orders of the sum. In our order we have for $W_1: j_1=1, j_2=4, W_2: j_1=2, j_2=3, W_3, W_4: j_i=0$. *Finally, we have* $W_1=I_5-2U^1-2U^4, W_2=I_5-2U^2-2U^3, W_3=I_5=W_4$

(3) *It follows that*

$$W_1=\begin{pmatrix} 1 & -2 & 0 & 0 & -2\\ -2 & 1 & -2 & 0 & 0\\ 0 & -2 & 1 & -2 & 0\\ 0 & 0 & -2 & 1 & -2\\ -2 & 0 & 0 & -2 & 1\end{pmatrix}, W_2=\begin{pmatrix} 1 & 0 & -2 & -2 & 0\\ 0 & 1 & 0 & -2 & -2\\ -2 & 0 & 1 & 0 & -2\\ -2 & -2 & 0 & 1 & 0\\ 0 & -2 & -2 & 0 & 1\end{pmatrix}, W_3=W_4=I_5.$$

Obviously these matrices are symmetric. By computation it can be seen that $W_1^2+W_2^2+W_3^2+W_4^2=20I_5$.

(4) *Reconstructing A, B, C, D, leads to*

$$A = B = \begin{pmatrix} 1 & -1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 & -1 \\ -1 & -1 & 1 & -1 & -1 \\ -1 & -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & -1 & 1 \end{pmatrix}$$

$$C = \begin{pmatrix} 1 & -1 & 1 & 1 & -1 \\ -1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 1 \end{pmatrix} \quad D = \begin{pmatrix} 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 \end{pmatrix}.$$

Consequently,

$$H_{20} = \begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix}$$

is a Hadamard matrix of size 20.

2.3. **Paley Hadamard matrices**

The next chapter follows mostly [28] and [7].

Definition 2.32. *Let $GF(q)$ be a Galois field with q an odd prime power and the function χ on the cyclic group $GF(q)^*$ is defined as*

$$\chi(g) = \begin{cases} 1 & \text{if } g \text{ is a perfect square} \\ -1 & \text{if } g \text{ is not a perfect square.} \end{cases}.$$

It is extended on $GF(q)$ by $\chi(0) = 0$. An element g in $GF(q)$ is a perfect square if there exists an element a of $GF(q)$, so that $g = a^2$.

Consider that if q is a prime, then $\chi(g)$ is the Legendre symbol $\left(\frac{g}{q}\right)$. Some well-known properties of the Legendre symbol are also true for the map χ.

Lemma 2.33. *Let q be an odd prime power and let $g \in GF(q)^*$, then*

(1) $|PS(q)| = |NPS(q)| = \frac{q-1}{2}$, *if PS is the set of perfect squares and NPS is the set of non perfect squares of $GF(q)^*$,*

(2) $g^{\frac{q-1}{2}} = \begin{cases} 1 & \text{if and only if } g \text{ is a perfect square} \\ -1 & \text{if and only if } g \text{ is not a perfect square,} \end{cases}$

(3) $\chi(gh) = \chi(g)\chi(h) : \forall g, h \in GF(q)$ *and*

(4) $\chi : GF(q)^* \Rightarrow \{\pm 1\}$ *is a homomorphism.*

Proof. (1) As the multiplication group of $GF(q)$ has order $q-1$ and is cyclic with a primitive element a, the quadratic elements are $a^0, a^2, a^4, \ldots$. Hence, there are $\frac{q-1}{2}$ perfect squares and $\frac{q-1}{2}$ non perfect squares.

(2) The polynomial $X^{q-1}-1=0$ has $q-1$ solutions in $GF(q)$ as all elements a of $GF(q)^*$ fullfill $a^{q-1}=1$ (Lagrange). The factorization of this polynomial is $(X^{\frac{q-1}{2}}-1)\cdot(X^{\frac{q-1}{2}}+1)=0$ and both factors have $\frac{q-1}{2}$ different solutions. If g is a perfect square then $\exists a \in GF(q) : g=a^2 \Rightarrow g^{\frac{q-1}{2}}=a^{q-1}=1$. To sum it up all perfect squares are the roots of $X^{\frac{q-1}{2}}-1$ and the set $NPS(q)$ must be equal to the roots of $X^{\frac{q-1}{2}}+1$.

(3) Let $g,h \in GF(q)$ be two perfect squares then $\exists x,y \in GF(q) : g=x^2\ ,\ h=y^2 \Rightarrow gh=(xy)^2 \Rightarrow 1=\chi(gh)=1\cdot 1=\chi(g)\cdot\chi(h)$. If g or h is zero, then $gh=0$ and $0=\chi(gh)=\chi(g)\cdot\chi(h)$. If g and h are both non perfect squares, then (2) implies that $g^{\frac{q-1}{2}}\cdot h^{\frac{q-1}{2}}=(-1)\cdot(-1)=1$ and so the product of two non perfect squares is a perfect square $\Rightarrow 1=\chi(gh)=\chi(g)\cdot\chi(h)=(-1)\cdot(-1)$. The last case where one of g,h is not a perfect square, but the other is one, is similar to (2).

(4) This follows from (3) and clearly $\chi(1)=1$.

□

Definition 2.34. *Let q be an odd prime power and $GF(q)=\{g_0=0,\cdots,g_{q-1}\}$. The corresponding $q\times q$ Jacobsthal matrix is defined as*

$$Q=(\chi(g_i-g_j))_{0\le i,j\le q-1}.$$

As a result, the Jacobsthal matrix consists only of ones, zeros and minus ones. The following properties are important for constructing Paley Hadamard matrices.

Lemma 2.35. *Let Q be the $q\times q$ Jacobsthal matrix, then*

(1) $QJ_q=J_qQ=0$

(2) Q *is* $\begin{cases} \textit{symmetric} & \textit{for } q\equiv 1 \mod 4 \\ \textit{skew-symmetric} & \textit{for } q\equiv 3 \mod 4 \end{cases}$

(3) $QQ^T=qI_q-J_q$

(4) $Q+I_q$ *is circulant if q is a prime and $GF(q)$ has its natural order.*

Proof. (1) The first property follows from Lemma 2.33, because in other words (1) means that there are as many 1s as (-1)s in a row and in a column of Q.

(2) Let $q=p^n=2k+1$, as q is odd and a a primitive element of $GF(q)^*$. Then consider the equation $a^{q-1}=1\Rightarrow a^{2k}=1$. The equation $x^2-1=0$ has solutions $a^0=1$ and $a^k=-1$ in $GF(q)$. Consequently, if k is even then $\chi(-1)=1$, if it is odd then $\chi(-1)=-1$.

$$q=2k-1\equiv\begin{cases}1 \mod 4 & \text{if } k \text{ is even}\\ 3 \mod 4 & \text{if } k \text{ is odd}\end{cases}.$$

Denote the elements of Q by (q_{ij}), then

$$q_{ij} = \chi(g_i - g_j) = \chi(-1) \cdot \chi(g_j - g_i) = \begin{cases} \chi(g_j - g_i) = q_{ji} & \text{if } q \equiv 1 \bmod 4 \\ -\chi(g_j - g_i) = -q_{ji} & \text{if } q \equiv 3 \bmod 4 \end{cases}.$$

(3) Let $QQ^T = (r_{ij})_{0 \le i,j \le q-1}$, then

$$\begin{aligned} r_{ij} &= \sum_{k=0}^{q-1} \chi(g_i - g_k)\chi(g_j - g_k) \\ &= \sum_{k \neq i,j} \chi(g_i - g_k)\chi(g_j - g_k) \\ &= \sum_{k \neq i,j} \chi(g_i - g_k)\chi(g_j - g_i + g_i - g_k) \\ &= \sum_{k \neq i,j} \chi(g_i - g_k)\chi((g_i - g_k)[(g_j - g_i)(g_i - g_k)^{-1} + 1]) \\ &= \sum_{k \neq i,j} \underbrace{\chi(g_i - g_k)^2}_{=1} \chi((g_j - g_i)(g_i - g_k)^{-1} + 1) \end{aligned}$$

Hence if $i = j$ then $\sum_{k \neq i,j} \chi((g_j - g_i)(g_i - g_k)^{-1} + 1) = \sum_{k \neq i,j} \chi(1) = q - 1$. This shows that the diagonal elements of QQ^T are $q - 1$.
If $i \neq j$ then it is clear that the set $\{(g_j - g_i)(g_i - g_k)^{-1} + 1 | k \neq i, j\}$ cannot contain 0 or 1 ($(g_j - g_i)(g_i - g_k)^{-1} + 1 = 0 \Leftrightarrow (g_j - g_i)(g_i - g_k)^{-1} = -1 \Leftrightarrow g_j - g_i = g_k - g_i \Leftrightarrow k = j$ and $(g_j - g_i)(g_i - g_k)^{-1} + 1 = 1 \Leftrightarrow (g_j - g_i)(g_i - g_k)^{-1} = 0 \Leftrightarrow g_j - g_i = 0 \Leftrightarrow j = i$), but all others elements of the group $GF(q)$. Lemma 2.33 (1) implies that $\sum_{i=0}^{q-1} \chi(g_i) = 0$. That leads to

$$\sum_{k \neq i,j} \chi((g_j - g_i)(g_i - g_k)^{-1} + 1) = \sum_{i=0}^{q-1} \chi(g_i) - \chi(0) - \chi(1) = 0 - 0 - 1 = -1.$$

So the off-diagonal elements of QQ^T are -1.

(4) follows from the fact $GF(q) \cong \mathbb{Z}/q\mathbb{Z}$ and $\mathbb{Z}/q\mathbb{Z}$ has a natural ordering $0, 1, \ldots, q-1$.

□

Theorem 2.36. *Let $t \ge 0, l \ge 0, e_i \ge 1, p_i$ be a prime satisfying $p_i^{e_i} \equiv 3 \mod 4$ for $1 \le i \le l$. If $m = 2^t \prod_{i=1}^{l} (p_i^{e_i} + 1)$ then there exist amicable Hadamard matrices of order m.*

Proof. Denote by M, N the amicable Hadamard matrices that will be proved to exist. In the case that $m = 1$, the parameters t, l are both zero and $M = N = (1)$ and if $m = 2$,

then $t = 1,\ l = 0$ and

$$M = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix},\ \ N = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

are by definition amicable.

For a more general case let $m \neq 1, 2$ and $m = p^e + 1$, therefore $t = 0,\ l = 1,\ p_1 = p,\ e_1 = e$ and define $q := p^e$. As q is odd, it is possible to order $GF(q) = \{g_0 = 0, \cdots, g_{q-1}\}$ in a way that

$$g_{q-i} = -g_i : 1 \leq i \leq q-1.$$

Now define

$$A := \begin{pmatrix} 0 & -e \\ e^T & Q \end{pmatrix} \text{ where } Q \text{ is the Jacobsthal matrix.}$$

From 2.35 it follows

$$AA^T = \begin{pmatrix} ee^T & -eQ^T \\ -Qe^T & e^Te + QQ^T \end{pmatrix} = \begin{pmatrix} q & 0 \\ 0 & J_q + QQ^T \end{pmatrix}$$
$$= \begin{pmatrix} q & 0 \\ 0 & qI_q \end{pmatrix} = qI_{q+1} = qI_m.$$

Define $M = A + I_m$, then M is $\pm 1-$ valued and

$$MM^T = \begin{pmatrix} ee^T + 1 & e - eQ^T - eI_q \\ e^T - Qe^T - I_qe^T & e^Te + (Q + I_q)(Q^T + I_q) \end{pmatrix}$$
$$= \begin{pmatrix} q+1 & 0 \\ 0 & J_q + QQ^T + (I_qQ^T + QI_q) + I_qI_q \end{pmatrix}$$
$$= \begin{pmatrix} q+1 & 0 \\ 0 & qI_q + I_q \end{pmatrix} = (q+1)I_{q+1} = mI_m.$$

In conclusion M is a skew Hadamard matrix of order m.

To construct a symmetric Hadamard matrix of order m, define the $(q-1) \times (q-1)$ permutation matrix $P = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}$ and $V = \begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix}$. As $P^T = P, P^2 = I_{q-1}$ it follows that $V^T = V, V^2 = I_q$. Let $N := \begin{pmatrix} 1 & 0 \\ 0 & -V \end{pmatrix} \cdot M = \begin{pmatrix} 1 & -e \\ -e^T & -VQ - V \end{pmatrix}$. Consequently, N is symmetric if $(VQ)^T = VQ$.

Let $VQ = (b_{ij})_{0 \leq i,j \leq q-1} = \begin{pmatrix} \chi(g_0 - g_0) & \chi(g_0 - g_1) & \cdots & \chi(g_0 - g_{q-1}) \\ \chi(g_{q-1} - g_0) & \chi(g_{q-1} - g_1) & \cdots & \chi(g_{q-1} - g_{q-1}) \\ \vdots & \vdots & \cdots & \vdots \\ \chi(g_1 - g_0) & \chi(g_1 - g_1) & \cdots & \chi(g_1 - g_{q-1}) \end{pmatrix}$, then the

first row of VQ is (with the ordering of $GF(q)$ set above)

$$b_{0j} = \chi(g_0 - g_j) = \chi(-g_j - 0) = \chi(g_{q-j} - g_0) = b_{j0} \text{ for } j \geq 1.$$

For $i, j \neq 0$

$$b_{ij} = \chi(g_{q-i} - g_j) = \chi(-g_i - g_j)$$
$$b_{ji} = \chi(g_{q-j} - g_i) = \chi(-g_j - g_i)$$

$\Rightarrow b_{ij} = b_{ji}$. Hence, N is symmetric and

$$NN^T = \begin{pmatrix} 1 & 0 \\ 0 & -V \end{pmatrix} (mI_m) \begin{pmatrix} 1 & 0 \\ 0 & -V \end{pmatrix} = mI_m.$$

As a result, N is a symmetric Hadamard matrix of order m. To show that M, N is a pair of amicable Hadamard matrices, it is left to prove that $MN = NM^T$. As N is symmetric it is clear that $(MN)^T = MN$.

$$MN = M \cdot N^T = M \cdot M^T \cdot \begin{pmatrix} 1 & 0 \\ 0 & -V \end{pmatrix} = (q+1) \cdot \begin{pmatrix} 1 & 0 \\ 0 & -V \end{pmatrix}$$

$$(MN)^T = (q+1) \cdot \begin{pmatrix} 1 & 0 \\ 0 & -V \end{pmatrix}^T = (q+1) \cdot \begin{pmatrix} 1 & 0 \\ 0 & -V \end{pmatrix}.$$

The general case is still missing for $t + l \geq 2$. To show that $l > 1$ can be constructed, it is sufficient to show that: If there exists a pair of amicable Hadamard matrices of order m and h, then there exists a pair of amicable Hadamard matrices of order mh.
Let M_m, N_m be a pair of amicable Hadamard matrices of order m and M_h, N_h be a pair of amicable Hadamard matrices of order h, then by definition $M_m = S_m + I_m, M_h = S_h + I_h$ with S_m, S_h being anti-symmetric.

$$M_{hm} := I_h \otimes M_m + S_h \otimes N_m$$
$$N_{hm} := N_h \otimes N_m.$$

By definition of the Kronecker product N_{mh} is symmetric and M_{hm} is skew, because

$$\begin{aligned} M_{hm} - I_{hm} &= I_h \otimes (S_m + I_m) + S_h \otimes N_m - I_{hm} \\ &= I_h \otimes S_m + I_{hm} + S_h \otimes N_m - I_{hm} = I_h \otimes S_m + S_h \otimes N_m \\ (M_{hm} - I_{hm})^T &= I_h^T \otimes S_m^T + S_h^T \otimes N_m^T \\ &= I_n \otimes (-S_m) + (-S_h) \otimes N_m = -(M_{nm} - I_{nm}). \end{aligned}$$

Using Lemma 2.19 shows that M_{hm}, N_{hm} are amicable

$$\begin{aligned}
M_{hm}N_{hm} &= (I_h \otimes M_m + S_h \otimes N_m)(N_h \otimes N_m) \\
&= (I_h \otimes M_m)(N_h \otimes N_m) + (S_h \otimes N_m)(N_h \otimes N_m) \\
&= N_h \otimes M_m N_m + S_h N_h \otimes N_m^2 \\
&= N_h \otimes (M_m N_m)^T + N_h S_h^T \otimes N_m^2 \\
&= (N_h \otimes N_m)(I_h \otimes M_m^T) + (N_h \otimes N_m)(S_h^T \otimes N_m) \\
&= (N_h \otimes N_m)(I_h \otimes M_m^T + S_h^T \otimes N_m) \\
&= N_{hm} M_{hm}^T.
\end{aligned}$$

Using the construction of Sylvester (compare: Corollary 2.23) for every $2^t \prod_{i=1}^{l}(p_i^{e_i}+1)$ a pair of amicable Hadamard matrices can be constructed. □

Definition 2.37. *The Hadamard matrices constructed in theorem 2.36 are called Paley type I Hadamard matrices.*

This construction leads to Hadamard matrices of order $8 = 7+1, 12 = 11+1, 20 = 19+1, 24 = 23+1, \ldots$.

Example. *A Paley type I Hadamard matrix of size 12 = 11 + 1 will be constructed. As 11 is prime, $GF(11)$ is simply $\mathbb{Z}/11\mathbb{Z}$. Choosing as primitive element 2, then* $\{2^2 \equiv 4 \mod 11, 2^4 \equiv 5 \mod 11, 2^6 \equiv 9 \mod 11, 2^8 \equiv 3 \mod 11, 2^{10} \equiv 1 \mod 11\}$ *are the quadratic elements. The Jacobsthal matrix Q is circulant developed by the first row*

$$\begin{aligned}
&\begin{pmatrix} 0 & \chi(-1) & \chi(-2) & \chi(-3) & \chi(-4) & \chi(-5) & \chi(-6) & \chi(-7) & \chi(-8) & \chi(-9) & \chi(-10) \end{pmatrix} \\
&= \begin{pmatrix} 0 & \chi(10) & \chi(9) & \chi(8) & \chi(7) & \chi(6) & \chi(5) & \chi(4) & \chi(3) & \chi(2) & \chi(1) \end{pmatrix} \\
&= \begin{pmatrix} 0 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 \end{pmatrix}
\end{aligned}$$

and the Hadamard matrix of size 12 is $H_{12} = \begin{pmatrix} 1 & -e \\ e^T & Q + I_{11} \end{pmatrix}$.

Theorem 2.38. *Let $t \geq 1, l \geq 0, e_i \geq 1, t \geq l, p_i$ be an odd prime satisfying $p_i^{e_i} \equiv 1 \mod 4$ for $1 \leq i \leq l$. If $m = 2^t \prod_{i=1}^{l}(p_i^{e_i}+1)$ then there exists a symmetric Hadamard matrix of order m.*

Proof. Let $P = \begin{pmatrix} 0 & e \\ e^T & Q \end{pmatrix}$ with Q Jacobsthal matrix for $q = p^e \equiv 1 \bmod 4$ and $R = P + I_{q+1}$. Obviously R is $\pm 1-$valued and P is symmetric by Lemma 2.35. Calculation of P^2 using Lemma 2.35 leads to

$$P^2 = PP^T = \begin{pmatrix} ee^T & eQ \\ Qe^T & J_q + QQ^T \end{pmatrix} = qI_{q+1}. \tag{2.12}$$

It will be shown that the symmetric matrix

$$H = \begin{pmatrix} -R & P - I_{q+1} \\ P - I_{q+1} & R \end{pmatrix} = \begin{pmatrix} -P - I_{q+1} & P - I_{q+1} \\ P - I_{q+1} & P + I_{q+1} \end{pmatrix}$$

is a Hadamard matrix of order $2(q+1)$. Clearly, H is ± 1-valued and it is symmetric as

$$\begin{pmatrix} -P - I_{q+1} & P - I_{q+1} \\ P - I_{q+1} & P + I_{q+1} \end{pmatrix}^T = \begin{pmatrix} -P^T - I_{q+1}^T & P^T - I_{q+1}^T \\ P^T - I_{q+1}^T & P^T + I_{q+1}^T \end{pmatrix} = \begin{pmatrix} -P - I_{q+1} & P - I_{q+1} \\ P - I_{q+1} & P + I_{q+1} \end{pmatrix}.$$

It is left to show that H is Hadamard. Multiplication gives

$$\begin{aligned} HH^T &= \begin{pmatrix} R^2 + (P - I_{q+1})^2 & -R(P - I_{q+1}) + R(P - I_{q+1}) \\ -R(P - I_{q+1}) + R(P - I_{q+1}) & (P - I_{q+1})^2 + R^2 \end{pmatrix} \\ &= \begin{pmatrix} 2P^2 + 2I_{q+1}^2 & 0 \\ 0 & 2P^2 + 2I_{q+1}^2 \end{pmatrix} \\ &= 2 \begin{pmatrix} qI_{q+1} + I_{q+1} & 0 \\ 0 & qI_{q+1} + I_{q+1} \end{pmatrix} = 2(q+1)I_{2(q+1)}. \end{aligned}$$

The rest follows from Lemma 2.21, because it shows that the Kronecker product of two symmetric matrices is again symmetric and from Corollary 2.23. □

Definition 2.39. *The matrix H defined in the proof of theorem 2.38 is called Paley-type II Hadamard matrix.*

2.4. Goethals - Seidel construction

There is another way to construct skew Hadamard matrices. The important plug-in construction was observed by Goethals and Seidel in 1969 [4].

Theorem 2.40. *If A, B, C, D are four square, circulant and $(\pm 1)-$valued matrices of order m and*

$$AA^T + BB^T + CC^T + DD^T = 4mI_m,$$

then the matrix

$$H = \begin{pmatrix} A & BR & CR & DR \\ -BR & A & -D^TR & C^TR \\ -CR & D^TR & A & -B^TR \\ -DR & -C^TR & B^TR & A \end{pmatrix}$$

is a $4m \times 4m$ Hadamard matrix with $R = (r_{ij})_{1 \le i,j \le m}$ being defined as

$$r_{ij} = \begin{cases} 1 & \text{if } i + j = m + 1 \\ 0 & \text{else} \end{cases}$$

.

Proof. R is the back-diagonal (0,1)-matrix. It has the matrix form: $R = \begin{pmatrix} \mathbf{0} & \cdots & 1 \\ & \iddots & \\ 1 & \cdots & \mathbf{0} \end{pmatrix}$. It is a circulant permutation matrix. Hence, it follows that $R^T = R = R^{-1}$ and $R^2 = I$. Furthermore, it is easy to see that $RX = X^T R$ for $X \in \{A, B, C, D\}$. As A, B, C, D are circulant, it was already stated that $XY = YX$ for $X, Y \in \{A, B, C, D\}$. Computation of HH^T shows that the diagonal entries are obviously $AA^T + BB^T + CC^T + DD^T = 4mI_m$ and the off-diagonal entries are zero as, for instance, the entry in the first row and second column is

$$\begin{aligned} A(-RB^T) + (BR)A^T + CR(-RD) + DRRC &= -ABR + BAR - CD + DC \\ &= (-AB + BA)R = \mathbf{0}. \end{aligned}$$

Similar computation can be done for all entries. □

Corollary 2.41. *Let B, C, D be four square, circulant and $(\pm 1)-$valued matrices of order m. Furthermore, let A be a skew matrix of order m with zero diagonal entries and all other entries are (± 1). If these matrices fulfill*

$$AA^T + BB^T + CC^T + DD^T = 4mI_m,$$

then the matrix

$$H = \begin{pmatrix} A+I & BR & CR & DR \\ -BR & A+I & -D^T R & C^T R \\ -CR & D^T R & A+I & -B^T R \\ -DR & -C^T R & B^T R & A+I \end{pmatrix}$$

is a $4m \times 4m$ skew Hadamard matrix with $R = (r_{ij})_{1 \le i,j \le m}$ being defined as

$$r_{ij} = \begin{cases} 1 & \text{if } i + j = m + 1 \\ 0 & \text{else} \end{cases}$$

.

Example. *The first example of a 36×36 Hadamard matrix was given in* [4]*. In their paper Goethals and Seidel used their construction with A being the circulant matrix developed by $\begin{pmatrix} 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 \end{pmatrix}$, B by $\begin{pmatrix} -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 \end{pmatrix}$, C by $\begin{pmatrix} 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 \end{pmatrix}$ and D by $\begin{pmatrix} 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 \end{pmatrix}$. Computation shows that $AA^T + BB^T + CC^T + DD^T = 4mI_m$ and a Hadamard matrix of size 36 was found.*

Remark. *This construction can easily be generalised, if A, B, C, D are required to be group-invariant (chapter 5). Group-invariant matrices are circulant. They are equivalent to orthogonal designs.* [14]

3. Equivalence classes

As long as not explicitly stated the chapter follows mainly [8] ,[22].

Having Lemma 2.14 in mind, the equivalence of two Hadamard matrices will be defined.

Definition 3.1. *Two Hadamard matrices are equivalent if one can be obtained from the other by permuting rows or columns or negations of rows or columns.*

It is obvious to see that:

Lemma 3.2. *The Hadamard equivalence is a equivalence relation and therefore Hadamard matrices can be ordered in equivalence classes.*

The number of equivalence classes of Hadamard matrices of order n is easy to compute **if** n is very small. On the other hand, this problem is very difficult if n is big.
In general, every equivalence class must contain one normalised representative as every Hadamard matrix can be normalised.
If $h(n)$ denotes the number of equivalence classes of Hadamard matrices of order n, then $h(1) = 1,\ h(2) = 1$. The second statement can be found by using the fact that in every equivalence class one normalised Hadamard matrix exists. Therefore it is sufficient, for finding the number of equivalence classes, to compute the number of normalised Hadamard matrices which are not equivalent to each other. For Hadamard matrices of order 2 that ansatz leads to $H_2 = \begin{pmatrix} 1 & 1 \\ 1 & x \end{pmatrix}$ which leads to the only possibility $x = -1$, but what is $h(4)$? With the same ansatz $H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & a_1 & b_1 & c_1 \\ 1 & a_2 & b_2 & c_2 \\ 1 & a_3 & b_3 & c_3 \end{pmatrix}$ we derive the equations $1 + a_i + b_i + c_i = 0 : 1 \leq i \leq 3$ and $1 + x_1 + x_2 + x_3 = 0 : x \in \{a, b, c\}$ as all rows (columns) are orthogonal to the first row (column). Only one of the three variables can be 1 and the other two must be -1. So there are six possibilities for H_4 and all of these are equivalent to each other by simple permutation of the rows. Consequently $h(4) = 1$. $h(8) = 1$ can be seen as there is only one normalised Hadamard matrix of size 2 and the Kronecker product of H_2 and H_4 is a normalised representative of H_8. By computation it can be seen that all other possibilities are equivalent to it.
Far more computation shows $h(12) = 1,\ h(16) = 5,\ h(20) = 3,\ h(24) = 60,\ h(28) = 487$. For $n = 32$ there are at least 3.578.000 equivalence classes! So the number can grow rapidly and for some larger n only lower bounds are investigated. The question how many equivalence classes exist for n = 32, 36, 40, 44,... might even be more difficult to answer than the Hadamard conjecture.

Lemma 3.3. *Two Hadamard matrices H, H' are equivalent if and only if two monomial matrices U, V exist so that $U^T H V = H'$. A matrix is monomial if it has only entries in $\{0, \pm 1\}$ and there is only one non-zero entry per row and column.*

Proof. A monomial matrix just performs combinatorial spoken the permutation of rows (if multiplied by left) and columns (if multiplied by right) and negation of some rows or columns, hence exactly the operations that are defined above for two matrices being equivalent. □

Lemma 3.4. *Let H and H' be Hadamard matrices, then*

(1) *-H is equivalent to H*
(2) *$H \otimes H'$ is equivalent to $H' \otimes H$*
(3) *H^T in general is not equivalent to H.*

Proof. (1) Multiplying every row with (-1)

(2) Using Lemma 3.3, we have to find two monomial matrices U, V so that

$$U \cdot (H' \otimes H) \cdot V^T = H \otimes H'.$$

Let H be a $n \times n$ matrix and H' a $m \times m$ matrix. The two monomial matrices that perfom that transformation are $mn \times mn$ matrices. We try to construct U intuitively by comparing $H' \otimes H$ and $H \otimes H'$. The first $m \times mn$ block of U must be of the form

$$\begin{pmatrix} \overbrace{1}^{1^{st}column} & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ 0 & \cdots & \overbrace{1}^{(n+1)^{th}column} & \cdots & 0 & \cdots & 0 \\ \vdots & \cdots & 0 & \cdots & \vdots & \cdots & 0 \\ 0 & \cdots & 0 & \cdots & \overbrace{1}^{((m-1)\cdot n+1)^{th}column} & \cdots & 0 \end{pmatrix}.$$

The second $m \times mn$ block of the n blocks that U will be filled with, is

$$\begin{pmatrix} 0 & \overbrace{1}^{2^{nd}column} & \cdots & 0 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \overbrace{1}^{(n+2)^{th}column} & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & 0 & \cdots & \vdots & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & \overbrace{1}^{((m-1)\cdot n+2)^{th}column} & \cdots & 0 \end{pmatrix}.$$

Completing the process, there can be seen by direct verification that

$$U \cdot (H' \otimes H) \cdot V^T = H \otimes H'$$

with $V = U$.

(3) To find a counterexample, we use that $h(1) = h(2) = h(4) = h(8) = h(12) = 1$, $h(16) = 5$ and the fact that transposing does not effect normalisation. That means that the class H_{16} can be the first equivalence class which can offer a counterexample and it does so with the matrix H. To see this requires a lot of work. It can be intuitively seen that negating or switching rows and columns will not bring H back from H^T. The remark following that Lemma will explain another more common and efficient method.

$$H = \begin{pmatrix}
+ & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + \\
+ & + & + & + & + & + & + & + & + & + & + & + & - & - & - & - \\
+ & + & + & + & - & - & - & - & + & + & + & + & - & - & - & - \\
+ & + & + & + & - & - & - & - & - & - & - & - & + & + & + & + \\
+ & + & - & - & + & + & - & - & + & + & - & - & + & + & - & - \\
+ & + & - & - & + & + & - & - & - & - & + & + & - & - & + & + \\
+ & + & - & - & - & - & + & + & + & + & - & - & - & - & + & + \\
+ & + & - & - & - & - & + & + & - & - & + & + & + & + & - & - \\
+ & - & + & - & + & - & + & - & + & - & + & - & + & - & + & - \\
+ & - & + & - & + & - & + & - & - & + & - & + & - & + & - & + \\
+ & - & + & - & - & + & - & + & + & - & - & + & + & - & - & + \\
+ & - & + & - & - & + & - & + & - & + & + & - & - & + & + & - \\
+ & - & - & + & + & - & - & + & + & - & - & + & + & - & - & + \\
+ & - & - & + & + & - & - & + & - & + & + & - & - & + & + & - \\
+ & - & - & + & - & + & + & - & + & - & + & - & - & + & - & + \\
+ & - & - & + & - & + & + & - & - & + & - & + & + & - & + & -
\end{pmatrix}$$

where $+ = 1$ and $- = -1$.

□

Remark. *"Precise determination of whether or not two given Hadamard matrices are equivalent is not easy, but it is possible to employ efficient computer programs. Perhaps the best approach uses the graph of a Hadamard matrix."*([26], *p.236)*
The graph of an $n \times n$ Hadamard matrix can be deduced in the following way. Interpret the rows with the symbols $r_1^+, r_2^+, \cdots, r_n^+$ and $r_1^-, r_2^-, \cdots, r_n^-$, the columns with $c_1^+, c_2^+, \cdots, c_n^+$ and $c_1^-, c_2^-, \cdots, c_n^-$ as vertices. As a result, the graph has $4n$ vertices. The edges are

$$\begin{cases}
\textit{loops} & \textit{on the vertices } r_i^+, r_i^- \\
\textit{between } r_i^+ \textit{ and } c_j^+ \textit{ resp. } r_i^- \textit{ and } c_j^- & \textit{if } h_{ij} = 1 \\
\textit{between } r_i^+ \textit{ and } c_j^- \textit{ resp. } r_i^- \textit{ and } c_j^+ & \textit{if } h_{ij} = -1
\end{cases}.$$

A proof showing that two such graphs are isomorphic if and only if the Hadamard matrices are equivalent can be found in [2]. *Many different algorithms exist to check if two graphs are isomorphic.*

Now a question arises: Do all the constructions discussed lead to the same equivalence class or to completely different ones?

Theorem 3.5. *Let $q \equiv 1 \mod 4$ be a prime power and P a Paley-Type II Hadamard matrix then P is equivalent to a Williamson matrix with circulant symmetric components.*

To prove this Lemma we have to give some definitions and prove an important property.

Definition 3.6. *A $(0, 1, -1)-$valued matrix $W := W(p, k), p \geq k$ of order p is called a weighing matrix of order p and weight k if $WW^T = kI_p$.*

Example. (1) *All $n \times n$ Hadamard matrices are weighing matrices of order n and weight n.*

(2) $W = \begin{pmatrix} 0 & e \\ (-1)^{(p-1)/2} e^T & Q \end{pmatrix}$ *with Q being the Jacobsthal matrix is a weighing matrix of order p+1 and weight p. (Compare proof of theorem 2.36 and 2.38.)*

Theorem 3.7. *Let $q \equiv 1 \mod 4$ be a prime power. Then there exists a weighing matrix $W(q+1, q)$ of the form $S = \begin{pmatrix} A & B \\ B & -A \end{pmatrix}$ where A and B are cyclic and symmetric and A has a zero diagonal.*

Proof. Let α be a primitive element of $GF(q^2)$. Let V be a basis of the vector space $GF(q^2)$ over $GF(q)$. Note that $\alpha^0, \alpha^{q+1}, \alpha^{2(q+1)}, \ldots, \alpha^{(q-1)(q+1)} \equiv 1$ is in $GF(q)$ and from this it follows that $\alpha^{\frac{q^2-1}{2}} = \alpha^{(q+1)\frac{q-1}{2}} \in GF(q)$ as q is odd. Also keep in mind that no smaller exponent k than $\frac{q+1}{2}$ achieves that $\alpha^{(q-1)\cdot k}$ is in $GF(q)$. Based on the basis, a matrix

$$(v) = 1/2 \begin{pmatrix} \alpha^{q-1} + \alpha^{1-q} & (\alpha^{q-1} - \alpha^{1-q})\alpha^{\frac{q+1}{2}} \\ (\alpha^{q-1} - \alpha^{1-q})\alpha^{-\frac{q+1}{2}} & \alpha^{q-1} + \alpha^{1-q} \end{pmatrix}$$

can be defined. The elements of (v) are in $GF(q)$, because $\alpha^{1-q} = \alpha^{q^2-1-(q-1)} = \alpha^{(q-1)q}$ and $(\alpha^{q-1} - \alpha^{1-q})\alpha^{\frac{q+1}{2}} = \alpha^{\frac{q^2-1}{2}} + \alpha^{-\frac{q^2-1}{2}} \in GF(q)$. Computation shows $\det(v) = 1$ and the eigenvalues are α^{q-1} and α^{1-q}. Consequently, (v) can be diagonalized and with the diagonal matrix

$$\begin{pmatrix} \alpha^{q-1} & 0 \\ 0 & \alpha^{1-q} \end{pmatrix}.$$

Therefore, (v) acts on the $(q+1)$ point of $PG(GF(q)) = \{\overline{(0,1)}\} \cup \{\overline{(1,x)} | x \in GF(q)\}$ as a permutation with period $(q+1)/2$ and without any fixed points. Hence, the points of $PG(GF(q))$ can be divided into two sets $|v_1| = |v_2| = \frac{q+1}{2}$. Furthermore, we define

$$(w) = \begin{pmatrix} 0 & \alpha^{q+1} \\ 1 & 0 \end{pmatrix}$$

and as α^{q+1} is in $GF(q)$, it follows that all elements of (w) are in $GF(q)$. In addition, $\det(w) = -\alpha^{q+1}$. The eigenvalues are $\alpha^{\frac{q+1}{2}}$ and $-\alpha^{\frac{q+1}{2}}$. Both squares of these eigenvalues

are in $GF(q)$. Consequently, (w) acts as a permutation of period 2 which maps each point of v_1 into v_2.

Keep in mind that $\chi \det(w) = \chi(-1)\chi(\alpha^{q+1}) = -\chi(-1) = -1$ as $q \equiv 1 \mod 4$ and α^{q+1} can not be a quadratic residue in $GF(q)$. In addition $wv = vw$.

We use the action of (w) and (v) on the set $PG(GF(q))$ to split the set into two as we want to split the rows and columns of S into two. The arguments above show that the set $x = x_1,\ vx = x_2,\ v^2x = x_3,\ \ldots,\ v^{\frac{q-1}{2}}x = x_{\frac{q+1}{2}},\ w(x) = x_{\frac{q+1}{2}+1},\ vw(x) = x_{\frac{q+1}{2}+2},\ v^2w(x) = x_{\frac{q+1}{2}+3},\ \ldots,\ v^{\frac{q-1}{2}}w(x) = x_{q+1}$ with any $x \in PG(GF(q))$ represents all different points of $PG(GF(q))$.

To define the weighting matrix S we use the map χ defined in the section of Paley matrices.

$$S = [\chi(\det(x_i, x_j))]_{1 \le i,j \le q+1}$$

with det being a bilinear form on V. Obviously, S is $(0, 1, -1)$-valued. Furthermore, $SS^T = (q+1)I$, because S is equivalent to $\begin{pmatrix} 0 & e \\ e^T & Q \end{pmatrix}$. To see this, choose $x_1 = \overline{(0,1)}$. It is obvious that the diagonal of S is zero. All off-diagonal elements of the first row and the first column are one, because $\chi(\det\left(\begin{pmatrix} 0 & 1 \\ 1 & x \end{pmatrix}\right) = \chi(1) = 1$ with $x \in GF(q)$. And all other elements have the form $\chi(\det\left(\begin{pmatrix} 1 & 1 \\ x & y \end{pmatrix}\right) = \chi(y - x)$ with $x, y \in GF(q)$ and this is the definition of Q. Choosing another x_1 produes an equivalent matrix S.

In the end, it is just left to prove that S has the form $\begin{pmatrix} A & B \\ B & -A \end{pmatrix}$ with

$$A = [\chi(\det(v^i x, v^j x))]_{0 \le i,j \le \frac{q-1}{2}}$$

and

$$B = [\chi(\det(v^i x, v^j w(x)))]_{0 \le i,j \le \frac{q-1}{2}}$$

being cyclic and symmetric. Keep in mind that $\det(Ax, Ay) = \det(A) \cdot \det(x, y)$ for all A being a linear mapping. Hence,

$$\det(v^i x, v^j x) = \det(v^i) \cdot \det(x, v^{j-i}x).$$

Consequently, A is circulant, analogously it follows that B is circulant.

$$\begin{aligned} \chi(\det(v^i w(x), v^j w(x))) &= \chi(\det(w)) \cdot \chi(\det(v^i x, v^j x)) \\ &= (-1) \cdot \chi(\det(v^i x, v^j x)) \\ \chi(\det(v^i x, v^j w(x))) &= -\chi(\det(v^i w(x), v^j x)) \\ &= \chi(\det(v^j x, v^i w(x))) \end{aligned}$$

These equations show that S has the form $\begin{pmatrix} A & B \\ B & -A \end{pmatrix}$ as required. From the fact that $\chi(-1) = 1$ it follows that both A, B are symmetric. □

Now it is possible to prove theorem 3.5.

Proof. From theorem 3.7 it follows that $\begin{pmatrix} 0 & e \\ e^T & Q \end{pmatrix}$ can be written in the form $\begin{pmatrix} A & B \\ B & -A \end{pmatrix}$ with A, B circulant and symmetric and A has a zero diagonal. So P can be rewritten (compare proof of theorem 2.38, matrix H)

$$P = \begin{pmatrix} -A-I & -B & A-I & B \\ -B & A-I & B & -A-I \\ A-I & B & A+I & B \\ B & -A-I & B & -A+I \end{pmatrix}.$$

Define the two monomial matrices

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, V = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

From Lemma 3.3 it follows that

$$P \sim U^T P V = \begin{pmatrix} -A-I & A-I & B & B \\ -A+I & -A-I & -B & B \\ -B & B & -A-I & -A+I \\ -B & -B & A-I & -A-I \end{pmatrix}$$

Let $A' = -A - I, B' = A - I, C' = B = D'$, then

$$P \sim U^T P V = \begin{pmatrix} A' & B' & C' & D' \\ -B' & A' & -D' & C' \\ -C' & D' & A' & -B' \\ -D' & -C' & B' & A' \end{pmatrix}.$$

and hence P is equivalent to a Williamson matrix. □

Remark. *Another method to study the equivalence class of Hadamard matrices is to consider the automorphism group $Aut(H)$ of a Hadamard matrix H. The automorphism group $Aut(H)$ of a Hadamard matrix H of size n is the ordered set of monomial matrices (U, V) so that $U^T H V = H$. These pairs clearly form a group with the operation $(U, V) \cdot (U', V') = (UU', VV')$ and $(I, I) \in Aut(H)$.*
Moreover, it is easy to see that if $H \sim H' \Rightarrow Aut(H) \sim Aut(H')$. In the article [12] *the automorphism group of the Paley-Type-I matrices are determined and in* [16] *the automorphism group of the Paley-Type-II matrices is fully described. As a result, it*

is possible to declare that these two constructions do not lead to equivalent Hadamard matrices if and only if the size of the Hadamard matrix is not 12.

Proposition 2.7 shows that there exists a lower bound on the size of Hadamard matrices. Analogously it is now proved that there is a lower bound on the number of Hadamard matrices with the help of $\mathbb{Z}$-equivalent classes. The next part can be reread in [26].

Definition 3.8. *Two matrices H, G are $\mathbb{Z}$-equivalent or integrally equivalent if G can be obtained by H by*

(1) *negating rows*
(2) *permuting rows*
(3) *adding a multiple of one row to another row*
(4) *doing the same actions on the columns*

In other words, these row operations can be fulfilled by left multiplication with a matrix with integer entries and its inverse is again an integer matrix, because there must be a matrix to undo these actions. It is easy to prove that:

Lemma 3.9. *Let A be an $n \times n$ matrix with integer entries, then there is an equivalence between*

(1) *A^{-1} has integer entries as well, and*
(2) $\det(A) = \pm 1$.

Proof. (1) $\Rightarrow$ (2)
In general the equation $1 = \det(A \cdot A^{-1}) = \det(A) \cdot \det(A^{-1})$ is true. As A and A^{-1} have integer entries, both $\det(A)$ and $\det(A^{-1})$ are in $\mathbb{Z}$, but this can only be possible if $\det(A) = \pm 1$ ($\Rightarrow \det(A^{-1}) = \pm 1$).
(2) $\Rightarrow$ (1)
That follows from the two facts that the determinant of a matrix with integer entries must be an integer, that the determinant is ± 1 and using the Cramer's rule. □

As a corollary from the previous Lemma, $\mathbb{Z}$-equivalence can also be seen as:

Corollary 3.10. *Two matrices A, B are $\mathbb{Z}$-equivalent if and only if there exist two unimodular matrices P, Q such that $PAQ = B$. A matrix is unimodular if it has only integer entries and its determinant is ± 1.*

Lemma 3.11. (1) *The inverse of a unimodular matrix is unimodular.*
(2) *The product of two unimodular matrices is unimodular.*
(3) *The Kronecker product of two unimodular matrices is unimodular.*
(4) *A matrix is $\mathbb{Z}$-equivalent to its transpose.*

Proof. (1), (2) trivial
(3) Let A be an $n \times n$ unimodular matrix and B an $m \times m$ unimodular matrix, then

$\det(A \otimes B) = \det(A)^n \cdot \det(B)^m = 1^n \cdot 1^m = 1$ and $A \otimes B$ obviously has integer entries. (4) Using basic linear algebra it is known that every matrix is row equivalent to its row echelon form and every transposed matrix is row equivalent to the column echelon form of the original matrix. □

3.10 and Lemma 3.3 result in the next Lemma which is the basis of the calculation of a **lower** bound on the number of Hadamard equivalence classes.

Lemma 3.12. *Two equivalent Hadamard matrices are $\mathbb{Z}$-equivalent.*

Proof. A monomial matrix is clearly unimodular and then Lemma 3.3, corollary 3.10. □

Remark. *To do some calculation on the number of $\mathbb{Z}$-equivalent matrices, a normal form for matrices is used, the Smith normal form. The proof of the Smith normal form can be found, for instance in* [3]. *It says that:*
Let R be a principal ideal ring and $A \in M_{m\times n}(R)$ with rank r, then

$$SAT = \begin{pmatrix} d_1 & 0 & 0 & \dots & 0 & \dots & 0 \\ 0 & d_2 & 0 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \dots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & d_r & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix},$$

where $S \in M_m(R)$ and $T \in M_n(R)$ and this matrix is called the Smith normal form of A. Both matrices are obtained by elementary row or column operations as explained in definition 3.8 . Furthermore, $d_i | d_{i+1}$ for $i = 1, \dots r-1$, d_i are unique up to multiplication with a unit and can be obtained by $d_i = \frac{d_i(A)}{d_{i-1}(A)}$ with $d_i(A)$ being the greatest common divisor of all $i \times i$ minors of A.

Lemma 3.13. *Let A be a square matrix with integer entries, then A is $\mathbb{Z}$-equivalent to a diagonal matrix $D = diag(d_1, d_2, \dots, d_k, 0, 0, \dots, 0)$, where r is the rank of the matrix A. The d_i are all positive and $d_i | d_{i+1}$. The greatest common divisor of the $k \times k$ subdeterminants of A is $d_1 d_2 \dots d_k$. If A is $\mathbb{Z}$-equivalent to*

$$\begin{pmatrix} D_1 & \boldsymbol{0} \\ \boldsymbol{0} & E \end{pmatrix},$$

with $D_1 = diag(d_1, d_2, \dots, d_k)$, then the greatest common divisor of the nonzero elements of E is d_{k+1}.

Proof. Using the remark above $SAT = \mathrm{diag}(d_1, d_2, \dots, d_r, 0, 0, \dots, 0)$ with S, T being unimodular. With corollary 3.10 the first part of the proposition is shown. That all d_i are positive results from the fact that all d_i are unique up to multiplication with a unit

and hence the d_i can be chosen positive. The rest can be seen directly if the remark is used. □

If we consider the Smith normal form of an $n \times n$ Hadamard matrix H, then we know that no diagonal element is zero as H has rank $n = 4m$. Consequently, the diagonal matrix has the form $D = \text{diag}(d_1, d_2, \ldots, d_{4m})$.

Lemma 3.14. *Let H be a $4m \times 4m$ matrix with Smith normal form*

$$D = diag(d_1, d_2, \ldots, d_{4m}),$$

then

$$d_i \cdot d_{4m-i+1} = 4m$$

for $i \in \{1, \ldots, 4m\}$.

Proof. Using Lemma 3.13, there exist unimodular matrices P, Q such that $PHQ = D$ and

$$(PHQ)(Q^{-1}H^TP^{-1}) = PHH^TP^{-1} = 4mPP^{-1} = 4mI.$$

As PHQ is D and the inverse of D is $\text{diag}\left(\frac{1}{d_1}, \frac{1}{d_2}, \ldots, \frac{1}{d_{4m}}\right)$, it follows that $Q^{-1}H^TP^{-1} = \text{diag}\left(\frac{4m}{d_1}, \frac{4m}{d_2}, \ldots, \frac{4m}{d_{4m}}\right)$. After reordering, this diagonal matrix, H^T has the Smith normal form

$$\text{diag}\left(\frac{4m}{d_{4m}}, \frac{4m}{d_{4m-1}}, \ldots, \frac{4m}{d_1}\right),$$

because then the condition $d_i' | d_{i+1}'$ is fulfilled. Lemma 3.11 (4) shows that a matrix is $\mathbb{Z}$-equivalent to its transpose and as a result H and H^T are $\mathbb{Z}$-equivalent. Therefore the equations

$$\begin{aligned} \text{diag}\left(\frac{4m}{d_{4m}}, \frac{4m}{d_{4m-1}}, \ldots, \frac{4m}{d_1}\right) &= \text{diag}(d_1, d_2, \ldots, d_{4m}) \\ \Leftrightarrow \frac{4m}{d_{4m-i+1}} &= d_i \end{aligned}$$

hold and the proof is completed. □

Theorem 3.15. *Let H be a $4m \times 4m$ matrix with Smith normal form*

$$D = diag(d_1, d_2, \ldots, d_{4m})$$

and m square-free, then D has the form

$$\begin{pmatrix}
1 & 0 & 0 & \ldots & 0 & \ldots & 0 & 0 \\
0 & 2 & 0 & \ldots & 0 & \ldots & 0 & 0 \\
\vdots & & \ddots & & \vdots & \ldots & \vdots & \vdots \\
0 & 0 & 0 & 2 & 0 & \ldots & 0 & 0 \\
0 & \ldots & \ldots & 0 & 2m & \ldots & 0 & 0 \\
0 & \ldots & \ldots & 0 & 0 & \ldots & 2m & 0 \\
0 & \ldots & \ldots & 0 & 0 & \ldots & 0 & 4m
\end{pmatrix}.$$

($2m^{th}$ row, $2m+1^{th}$ row, $4m-1^{th}$ row, $4m^{th}$ row)

Proof. W.l.o.g. it is assumed that H is normalised. Start by subtracting the first row from every other and the first column from every other column, then H has the form $\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & K \end{pmatrix}$ and every element in K has to be zero or ± 2. Hence, $d_1 = 1$. By reordering rows and multiplying with -1, it can be assumed that $d_2 = 2$. Consequently, $d_{4m} = 4m$ and $d_{4m-1} = 2m$ using Lemma 3.14. These facts are true in general, from now on it is used that m is square-free.
For $i \leq 2m$ it is true that $d_i | d_{4m-i+1}$. Consequently, there $\exists \alpha$ with $d_{4m-i+1} = \alpha d_i$ and the equation of Lemma 3.14 leads to $\alpha d_i^2 = 4m$. As m is square-free d_i must be 1 oder 2. Of course $d_1 = 1$, but if $i \neq 1$, then $d_2 = 2$ divides d_i. So there are $(2m-1)$ d_is that are 2 and the others must be $2m$. □

Corollary 3.16. *Any two Hadamard matrices of size $4m$ with m being square-free are $\mathbb{Z}$-equivalent.*

There is a lower bound for the entry 2 in the Smith normal form of a Hadamard matrix. That can be proved by using a Lemma that was shown in the paper [25].

Lemma 3.17. *Let A be an $n \times n$ matrix with entries 0 or 1 and $\det(A) \neq 0$, then A has at least $\lfloor \log_2 n \rfloor + 1$ entries 1 in its Smith normal form.*

Sketch of proof. Let t denote $\lfloor \log_2 n \rfloor$. This means that t is the unique solution of the inequality chain $2^t \leq n < 2^{t+1}$. It will be proved that A is $\mathbb{Z}-$equivalent to $\begin{pmatrix} I_t & 0 \\ 0 & D \end{pmatrix}$ and the greatest common divisor of the entries in D is 1.
The first step is done by an algorithm that leads to a matrix where the $2i-1$th and the

$2i$th column have the same entries for the first $i-1$ rows and then different entries in row i, for $i \in \{1, \ldots, t\}$.

Algorithm. (1) *Choose two columns which have two different entries in the first row. Reorder A so that these two columns are now the first two columns of A.*

(2) *Choose two columns which have the same entry in the first row and and then reorder the other rows in such a way that the second row has two different entries. Reorder the columns after the two columns chosen in the first step.*

(k) *Choose from the remaining $n-(2k-2)$ columns in the matrix resulting from step $k-1$ two columns which are similar in the first $k-1$ rows and then reorder the rows so that entries in the k-th row differ.*

These steps can always be performed if $k \leq t$, because no columns can be identical as $\det(A) \neq 0$ and there are only 2^{k-1} different $(0,1)$-vectors with length $k-1$.
The second step is to find two columns a, b that have the same entries for the first t rows and then reorder the other rows in a way that the $t+1$th row has different entries. If this step is not possible, because there are no further two columns that have the same entries in the first t rows, then $n = 2^t$. In that case the first 2^t rows present all the different possible 2^t $(0,1)$-vectors. Therefore, there is one column, say a, that has only zeros in the first t rows. Reorder the rows in a way that there is a one in the $t+1$th row. In the end, reorder the columns in a way that in the new matrix the number a is even and if b was chosen before, the number of the column should be even as well. The last step is also an algorithm that leads to the Smith normal form.

Algorithm. *For $i = 1, \ldots, t$:*
Subtract column $2k$ from $2k-1$. Then the $(k, 2k-1)$-entry is ± 1. Add a suitable multiple of the $2k-1$th column to all the following columns so that the entry of the row k is zero in these columns. As a result, only the entry $(k, 2k-1)$ is nonzero in the row k.

If in step k a certain multiple of the column $2k-1$ was added to column $2i$, then the same multiple was added to $2i-1$, because the entries $(k, 2i)$ and $(k, 2i-1)$ are the same as the previous algorithm ensures. That is the reason why the algorithm works at every step. The same arguments show that if in the second step, two columns were chosen then these columns still differ by one after the algorithm. If just the column a is chosen in the second step then the last algorithm does not alter this column, because the first t entries in the column are zero and therefore they need not to be changed.
Finally, reorder the first $t-1$ odd columns so that they are the first columns. Then the matrix A has the form

$$\begin{pmatrix} I_t & 0 \\ 0 & D \end{pmatrix},$$

where D has two entries which differ by one, or one entry is 1. Therefore, the common divisor of the entries in D is one. $\square$

Corollary 3.18. *A Hadamard matrix of size $4m$ has at least $\lfloor \log_2(4m-1) \rfloor + 1$ entries 2 in its Smith normal form.*

Proof. W.l.o.g. let H be normalised and subtract the first row from any other row and the first column from any other column, then the matrix has the form $\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & -2B & \\ 0 & & & \end{pmatrix}$ with B being a $4m-1 \times 4m-1$ matrix with entries zero or 1, and $\det(B) \neq 0$. Using Lemma 3.17 and multiplying with (-1) shows that there are at least $\lfloor \log_2(4m-1) \rfloor + 1$ entries 2 in the Smith normal form. □

Definition 3.19. *Let H be a $4m \times 4m$ matrix and $m = f \cdot g^2$, where f, g are coprime and square-free. Then $d_1 = 1$ and $d_{4m} = 4m$ in the Smith normal form. There are at least $\lfloor \log_2(4m-1) \rfloor + 1$ entries 2 and therefore as many entries that are $2m$. All the others d_i must be divisors of $4m$. From Lemma 3.14 it follows that $d_i | d_{i+1}$, $4m/d_i$ must also be an entry in the Smith normal form and therefore especially that $2|d_i$. As a result, only $2g$ and $2fg$ can be entries in the Smith normal form of H, because all others combinations would not work as f, g are supposed to be coprime. The Smith normal form is*

$$diag(1, 2^{(\alpha \text{ times})}, 2g^{(\beta \text{ times})}, 2fg^{(\beta \text{ times})}, 2m^{(\alpha \text{ times})}, 4m),$$

with $2\alpha + 2\beta = 4m - 2$. As a result, α completely describes the Smith normal form and is therefore called the Smith class of H.

Example. *The Smith class of the Hadamard matrices of size $16 = 4 \cdot 4$ is now described. It gives a lower bound for the $\mathbb{Z}-$equivalence of Hadamard matrices of order 16. Corollary 3.18 shows that $\alpha \geq \lfloor \log_2(15) \rfloor + 1 = 3 + 1 = 4$ and by definition 3.19 the equation $\alpha + \beta = 7 = 2 \cdot 4 - 1$ has to be fulfilled. Consequently, α can only be 4,5,6 or 7, hence there are at least four equivalence classes. Above it is described that $h(16) = 5$. In the proof of Lemma 3.4 (3) the matrices H and H^T can be found. These are examples of Hadamard matrices with size 16 and with Smith class 7.*

4. Some Theory

In the next chapters some theory that was already used or will be used for the next part is provided. Proofs may occasionally be left out.

4.1. **Finite Fields**

Some of the basic definitions and results of the theory of finite fields are listed in the next chapter. As the chapter is intended to be a small summary of well-known facts, the proofs ar omitted, but can be looked up in [18], [11].

Definition 4.1. *A finite field $(X, +, \cdot)$ is a field with finite set of elements X.*

Definition 4.2. *For a prime p, let $\mathbb{F}_p$ be $\{0, 1, \ldots, p-1\}$ and $\chi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{F}_p, \chi([a]) = a : a \in \mathbb{Z}/p\mathbb{Z}$. Then $\mathbb{F}_p$ endowed with the field structure induced by χ is a finite field, called the Galois field of order p.*

Definition 4.3. *$\mathbb{F}_p[x]$ (or later $GF(p)[x]$) denotes the ring of polynomials in the indeterminante x with coefficients in $\mathbb{F}_p$ (or later $GF(p)$).*

Theorem 4.4. *Let $\mathbb{F}_p$ be a field and $f \in \mathbb{F}_p[x]$ with $\deg(f) = n \geq 0$. The residue class ring $\mathbb{F}_p/(f)$ is a field if and only if f is irreducible. The number of elements of $\mathbb{F}_p/(f)$ is p^n.*

Example. *Consider the irreducible polynomial $f(x) = x^2+x+1 \in \mathbb{F}_2[x]$. As $\deg(f) = 2$, the number of elements of $\mathbb{F}_2/(f)$ is $2^2 = 4$. $[0], [1]$ must be elements of $GF(2)[x]/(f)$ and the others are $[x]$ and $[x+1]$. As a result, the tabels are*

$+$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[1]$	$[1]$	$[0]$	$[x+1]$	$[x]$
$[x]$	$[x]$	$[x+1]$	$[0]$	$[1]$
$[x+1]$	$[x+1]$	$[x]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[x]$	$[0]$	$[x]$	$[x+1]$	$[1]$
$[x+1]$	$[0]$	$[x+1]$	$[1]$	$[x]$

This is the first example of a finite field of 2^2 elements, obviously not a prime.

Theorem 4.5. *For every prime p and and every positive integer n there exists a finite field with p^n elements. Any finite field with $q = p^n$ elements is isomorphic to the splitting field of $x^q - x$ over $\mathbb{F}_p$. This uniqueness leads to the notation to denote **the** finite field or the Galois field with q elements by $GF(q)$.*

Theorem 4.6. *For every finite field $GF(q)$ the multiplication group $GF(q)^*$ is cyclic, of order $q-1$ and has $\phi(q-1)$ generators (primitive elements) where ϕ denotes Euler's totient function.*

Corollary 4.7. *If $GF(r)$ is a field extension of $GF(q)$, then $GF(r)$ is a simple algebraic extension of $GF(q)$. Let α be a primitive element of $GF(r)$, then $GF(q)(\alpha) = GF(r)$.*

Corollary 4.8. *For $n \geq 1$ there exists an irreducible polynomial of degree n in $GF(q)[x]$.*

Theorem 4.9. *Consider the finite field $GF(q)$ and an irreducible polynomial f of degree m in $GF(q)[x]$, then f has a root α in $GF(q^m)$. All the roots of f are simple and given by $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$.*

Corollary 4.10. *If f is an irreducibel polynomial of degree n of $GF(q)[x]$, then the splitting field of f over $GF(q)$ is $GF(q^n)$.*

A finite field $F = GF(q^n)$ can be seen as a vector space over the field $K = GF(q)$ with dimension n over K. Using the notation that results in:

Corollary 4.11. *If α is a root of an irreducible polynomial f in $K[x]$ with $\deg(f) = n$, then $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for the vector space $F = K(\alpha)$.*

Lemma 4.12. *Let the number of $k-$dimensional subspaces of a vector space $V = GF(q^n)$ over $GF(q)$ be $G(n,k)$, then*

$$G(n,k) = \frac{(q^n-1)\cdot(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)\cdot(q^{k-1}-1)\cdots(q-1)}.$$

Proof. Denote the number of all $k-$tupels of linearly indepedent vectors of V with $N(n,k)$. This number is calculated combinatorically: There are $q^n - 1$ possibilities to choose the first vector of such a tupel, as there are q^n different vectors, but per definition the null vector is always linearly dependent. To choose the second vectors there are $q^n - 1$ possible vectors, but $q - 1$ are multiples of the first vector. Let the first $i - 1$ vectors be $v_1, \ldots, v_{i-1}$. In general, choosing the next v_i has $(q^n - 1) - (q^{i-1} - 1)$ possibilities. To see that, mind that there are $q^n - 1$ vectors, but the set $\{v_1, \ldots, v_i\}$ has to be linearly indepedent. Hence the number of v_is not to choose is the same number as choosing $a_j \in GF(q) : 1 \leq j \leq i-1$ for $a_1v_1 + a_2v_2 + \cdots a_iv_{i-1} (= v_i)$. This number is q^{i-1}, but of course $a_1 = \cdots = a_{i-1} = 0$ is not allowed.
Now counting in two ways will be used as $N(n,k)$ can also be found by choosing a $k-$dimensional subspace W of V and then choosing a $k-$tupel of linearly independent vectors of W. This number is denoted by $L(k,k)$ and is $(q^k-1)\cdot(q^k-q)\cdots(q^k-q^{k-1})$. In the end, it is shown that $L(k,k)\cdot G(n,k) = N(n,k)$ and therefore

$$G(n,k) = \frac{N(n,k)}{L(k,k)},$$

and the proposition is shown. □

Definition 4.13. *Let $V = GF(q^n)$ be the vector space over $K = GF(q)$. Let $\alpha \in V$, then the trace of α is defined by*

$$Tr_{V/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}.$$

Lemma 4.14. *The trace function defined in 4.13 is a linear mapping from V into K.*

Sketch of proof. It is easy to see that $Tr_{V/K}(\alpha)^q = Tr_{V/K}(\alpha)$. The fixpoints of the Frobenius mapping $x \to x^q$ are the roots of the polynomial $x^q - x = 0$, but these are the all

the elements of $GF(q) = K$. Therefore, $Tr_{V/K}$ mappes V into K. This mapping is linear using Freshman's Rule $(x+y)^q = x^q + y^q$ and the fact that $c^{q^i} = c : \forall i \geq 0, \forall c \in K$. □

Lemma 4.15. *The kernel of the trace function $Tr_{V/K}$ defined in 4.13 has dimension $n-1$ over K.*

Proof. Clear as

$$\dim(\text{kernel}(Tr_{V/K})) + \dim(\text{im}(Tr_{V/K})) = \dim(GF(q^n))$$
$$\dim(\text{kernel}(Tr_{V/K})) + 1 = n.$$

□

There is even a stronger theorem for the elements that are in the kernel of the trace function:

Theorem 4.16. *Let the trace function be defined as 4.13 and $\alpha \in V$, then $Tr(\alpha) = 0 \Leftrightarrow \exists \beta \in V$ such that $\alpha = \beta^q - \beta$.*

Sketch of proof. The sufficiency of the condition follows from Lemma 4.14 and its proof. For the necessity, let $\alpha \in V$ with $Tr_{V/K}(\alpha) = 0$ and β a root of $x^q - x - \alpha$ in an extension field of V. Then $\beta^q - \beta = \alpha$ and

$$0 = Tr_{V/K}(\alpha) = Tr_{V/K}(\beta^q - \beta) = \beta^{q^n} - \beta \Leftrightarrow \beta = \beta^{q^n} \Leftrightarrow \beta \in V.$$

□

The next theorem is very important in general and will be used later:

Theorem 4.17. *The notations of the definition 4.14 are used. All the linear transformations from V into K are exactly the mappings $L_\beta : \beta \in V$ where $L_\beta(\alpha) = Tr_{V/K}(\beta\alpha)$ for $\alpha \in V$. In addition, $L_\beta \neq L_\gamma$ if $\beta \neq \gamma, \beta, \gamma \in V$.*

Proof. As $\beta \in V$ and $|V| = q^n$, L_β yields q^n different linear transformations from V into K. On the other hand, a linear mapping from V into K can be done by assigning the q elements of K to the n elements of the basis of V. There are q^n possibilities for that.
If $\beta \neq \gamma, \beta, \gamma \in V$, then for a suitable $\alpha \in V$ the equation chain $L_\beta(\alpha) - L_\gamma(\alpha) = Tr_{V/K}(\beta\alpha) - Tr_{V/K}(\gamma\alpha) = Tr_{V/K}((\beta - \gamma)\alpha) \neq 0$ holds. □

Corollary 4.18. *Let K be a finite field and V a finite field extension of K, then the number of linear mappings from V into K is the number of distinct elements of V.*

4.2. Finite Geometry

Definition 4.19. *A finite affine plane is a finite set of points P and a non-empty multiset L of subsets of P that are called lines. They fulfill the conditions that*

A1 *There is one and only one line containing two given points.*

A2 *There are four points no three of which belong to the same line.*

A3 *If a line l does not contain a point p, then there must be exactly one line q containing p, but l and q do not intersect. Consequently, l is parallel to q.*

By A2 every affine plane has at least four points. There is a plane with four points which is denoted by $AG(2,2)$. It has 6 lines and three pairs with parallel lines.

Lemma 4.20. *A finite affine plane is characterised by a parameter n. Every line contains n points and every point lies on $n+1$ lines. Therefore, an affine plane is denoted by $AG(2,n)$.*

Proof. If the points of the plane are contained in two lines, then it is $AG(2,2)$. So it can be assumed that not all points are contained in two lines. Let these two lines be l and m and p a point that lies on neither one of them. There is a parallel line q of l that contains the point p. Suppose that the line l contains n points, namely $a_1, \ldots, a_n$. Then consider the set D of $n+1$ lines through p and a_1, p and $a_2, \ldots, p$ and a_n, q. A3 shows that there is one line parallel to m as p does not lie on m, but that line must intersect l in a point a_i. Therefore, this parallel line is the line through a_i and p. The other n lines of D meet m in n points. Suppose there were more lines that intersect m, then these lines would have to be parallel to l (as these lines would not have intersection points with l). Let a be an intersection point of one of these lines with m. Then the line through a and p would be parallel to l and contain p, but this is a contradiction to A3. As l, m, p were chosen arbitrary every line contains n points and, every point lies on $n+1$ lines. □

An affine plane $AG(2,n)$ is a BIBD!

Theorem 4.21. *Consider the points of an $AG(2,n)$ as treatments and the lines as blocks, then it is BIBD with parameters $(n^2, n^2+n, n+1, n, 1)$.*

Proof. Lemma 4.20 shows that $k = n$ and $r = n+1$. A1 implies that $\lambda = 1$. Using 5.3 (2) then we have $v = n^2$ and with (1) $b = n(n+1)$. □

Remark. *The converse of theorem 4.21 is of course also true, but the proof is left out.*

Definition 4.22. *A finite projective plane consists of a finite set P of points and a multiset L of subsets of P. A set of L is a line. They fulfill:*

P1 *Any two points lie exactly on one line.*

P2 *There exist four points no three of which belong to the same line.*

P3 *Two lines always have exactly one point in common.*

Like $AG(2,n)$, projective planes also have an unique parameter n, hence they can be denoted by $PG(2,n)$. They can be constructed from affine planes which is shown in the next Lemma.

Lemma 4.23. *There exists an $AG(2,n)$ and therefore a $(n^2, n^2+n, n+1, n, 1)-$BIBD if and only if a $(n^2+n+1, n+1, 1)-$SBIBD exists.*

Sketch of proof. It is quite easy to see that the set of lines with size $n^2 + n$ can be partitioned into $n + 1$ sets with n members that represent the parallel class of lines. Let these subsets of L be $L_1, L_2, \ldots, L_{n+1}$. The new design (i.e. $PG(2, n)$) is formed by adding $n + 1$ points of infinity denoted by $p_1, p_2, \ldots, p_{n+1}$. So the design has $n^2 + n + 1$ treatments. The new blocks and hence the new lines are formed by the next algorithm: If the line l belongs to a set L_i then let the new line be $l^* = l \cup p_i$ and additionally add $l_\infty = \{p_1, p_2, \ldots, p_{n+1}\}$. Therefore the design has $n^2 + n + 1$ blocks. (Keep in mind that adding these $p_i s$ makes it possible that P3 can be fulfilled, as every pair of parallel lines now has a point in common.) It is left to prove that that design is still balanced with $\lambda = 1$. Every pair of points from the original set of points P that belonged to a line l now still belongs only to l^*. The pair $(p, p_i) : p \in P$ only belongs to the one line of L_i that contains p. Finally (p_i, p_j) belongs only to l_∞. □

The last proof results in:

Theorem 4.24. *The projective plane is a* $(n^2 + n + 1, n + 1, 1)-$*SBIBD. Every line contains* $n + 1$ *points and can therefore be denoted by* $PG(2, n)$.

Example. $PG(2, 2)$ *is the four point projetive plane. Consider* $GF(2)$ *and the affine plane* $AG(2, 2)$. *The set of points is* $P = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$. *There are six lines containing each two points of* P.

(1) $y = 0$ *containing* $(0, 0), (1, 0)$
(2) $x = 0$ *containing* $(0, 0), (0, 1)$
(3) $y + 1 = 0$ *containing* $(0, 1), (1, 1)$
(4) $x + 1 = 0$ *containing* $(1, 0), (1, 1)$
(5) $x + y = 0$ *containing* $(0, 0), (1, 1)$
(6) $x + y + 1 = 0$ *containing* $(1, 0), (0, 1)$

(1) and (3), (2) and (4), (5) and (6) are parallel, respectively. Adding three points p_1, p_2, p_3 *to* P *and to the lines (blocks) in the way that was described in the proof of Lemma 4.23, then the lines of* $PG(2, 2)$ *are*

$$\{(0, 0), (1, 0), p_1\}, \{(0, 1), (1, 1), p_1\}, \{(0, 0), (0, 1), p_2\}, \{(1, 0), (1, 1), p_2\},$$
$$\{(1, 1), (0, 0), p_3\}, \{(0, 1), (1, 0), p_3\}, \{p_1, p_2, p_3\}.$$

There is a strong existence statement: For every prime n there exists such a projective plane $PG(2, n)$.

Theorem 4.25. *For every prime power* $q \geq 2$ *there exists a projective plane of order* q. *Therefore, a* $(q^2 + q + 1, q + 1, 1)-$*SBIBD exists.*

Proof. Consider $GF(q)$ and let V be the three-dimensional space over $GF(q)$. The vectors of this space are denoted by (x_1, x_2, x_3). This vector space has subspaces of dimension one

and two. Let V_1 consist of all one-dimensional subspaces and V_2 of the two-dimensional subspaces. For all $W \in V_2$, define the set

$$A_W = \{A \in V_1 : A \subseteq W\}$$

and let $\mathcal{A}$ be the multiset of all these sets $A_W : W \in V_1$. It is left to prove that $(V_1, \mathcal{A})$ is the projective plane of order q.
Lemma 4.12 shows $|V_1| = G(3,1) = \frac{q^3-1}{q-1} = q^2 + q + 1$ and $|V_2| = G(3,2) = \frac{(q^3-1)(q^3-q)}{(q^2-1)(q^2-q)} = q^2 + q + 1$. Therefore, the design $(V_1, \mathcal{A})$ has $q^2 + q + 1$ treatments and as many blocks, because for every two dimensional subspace there is a block A_W. Let C be in V_1 and $W \in V_2$. Observe that $|C| = q$ and $|W| = q^2$. The sets $C \setminus \{(0,0,0)\}$ partition the set $W \setminus \{(0,0,0)\}$. Therefore $|A_B| = \frac{|W|-1}{|C|-1} = \frac{q^2-1}{q-1} = q + 1$. That means that the symmetric design has blocks with $q + 1$ elements. It is left to show that the covalency number is 1. $C, D \in V_1$ with $C \neq D$. There is a unique two-dimensional space B that contains both C and D. B determines the one block that contains both C and D. □

The theorem and also its proof can be generalised:

Theorem 4.26. *Let $q \geq 2$ be a prime power and $d \geq 2$ is an integer. Then there is a*

$$\left(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}\right) - \textit{SBIBD.}$$

Proof. Let $V = GF(q^{d+1})$ and V_1 be again the set of all one-dimensional subspaces. Furthermore, let V_d be the set of all $d-$dimensional subspaces. Every $d-$subspace gives rise to a block as in the proof of theorem 4.25. □

Remark. *The design of Theorem 4.26 also corresponds to a geometric object, namely the finite geometry of dimension d over $GF(q)$. They are often termed $PG(d, n)$.*

5. Hadamard matrices and combinatorial designs

5.1. Basics

The first question is: "What is design theory? Architecture in mathematics?". This is not completely false. It is a part of combinatorical mathematics and a design is a way of picking subset of a finite set under special conditions. For example, a graph $G(V, E)$ with vertices V and edges E is a design. Block designs will be of particular interest to us. The next chapter is a short summary of [26].

Definition 5.1. *A design is formed of the set S. The members of the universal set S are called treatments or varieties. If the formed subsets of S are just unordered sets, then*

the combinatorical design is called block design. If all blocks are different, the design is called simple.

Example. *An example of a design that is not a block design is a Latin square. It is a $n \times n$ matrix picked from a set with n treatments and its entries satisfy the condition that each row and each column is a permutation of the set S. For example*

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}$$

is a Latin square of size 3. Ever row or every column can be interpreted as an ordered set and therefore is not a block design.

Definition 5.2. *A regular block design is a block design where each treatment occurs equally often in a block. The size of the set of treatments is denoted by v. The number of occurrence of a treatment is r and r is universal if it is a regular block design. It is also called replication number or frequency. The size of a block is k and the number of blocks is b. Consequently a block design is a $(v, b, r, k)-$design.*
A design is called incomplete if $k \neq v$, otherwise it is called complete.
It is very interesting to study the covalency number or index λ_{xy} for two treatments x, y. That number is the number of blocks which contain both x and y. A balanced incomplete block design is an incomplete block design where λ_{xy} is constant and therefore independent of the choice of x, y. As a result, this design is referred to BIBD in short or a $(v, b, r, k, \lambda)-$design. If $\lambda = 0$, then the design would be trivial, but since a BIBD should not be complete, the special law is excluded and the index is restricted to $\lambda \geq 1$.

Proposition 5.3. *In a $(v, b, r, k, \lambda)-$design the parameters fulfill:*

(1) $bk = vr$
(2) $r(k-1) = \lambda(v-1)$

Proof. (1) The proof technique of counting in two ways is used. On the one hand, the pairs (x, z) where a treatment x belongs to a block z, is counted and this number is vr as every of the v treatments belongs to r blocks. On the other hand there are b blocks and every treatments belongs to k of the blocks and therefore there are also bk such pairs (x, z).

(2) A special treatment x occurs in r blocks. If we list all the treatments that are in all of these r blocks, then x will be listed r times and all the other $(v-1)$ treatments λ times. In the end the list has rk entries. So it follows that

$$rk = \underbrace{r}_{\text{occurrence of x}} + \underbrace{\lambda(v-1)}_{\text{occurrence of the other treatments in the list}}.$$

Bringing r on the other side of the equation shows the property.

□

Definition 5.4. *Consider a $(v, b, r, k, \lambda)-$design. A treatment x_i is incident with a block b_j if $x_i \in b_j$. This connection can be shown in the $v \times b$ incidence matrix $A = (a_{ij})_{1 \leq i \leq v, 1 \leq j \leq b}$ with*

$$a_{ij} = \begin{cases} 0 & \text{if } x_i \notin b_j \\ 1 & \text{if } x_i \in b_j \end{cases}.$$

Example. *Let S be $\{1, 2, 3, 4, 5, 6\}$ and hence $v = 6$. 10 blocks are chosen from the set with size 3 and every treatment has to belongto 5 of these blocks. For instance*

$$123, 124, 135, 146, 145, 236, 245, 256, 345, 346$$

is such a design and the incidence matrix is

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

Definition 5.5. *Two block designs are isomorphic if the incidence matrix can be transformed by permuting rows or columns.*

Proposition 5.6. *If A is the incidence matrix of a $(v, b, r, k, \lambda)-$design then*

$$AA^T = (r - \lambda)I_v + \lambda J_v \text{ and } J_v A = kJ_{v \times b}.$$

Conversely, if there is a $v \times b$ matrix A with entries zero or one that satisfies these two equations, then the equations

$$v = \frac{r(k-1)}{\lambda} + 1 \text{ and } b = \frac{vr}{k}$$

hold and therefore, A is the incidence matrix of a $(v, b, r, k, \lambda)-$design.

Proof. Let A be an incidence matrix of a $(v, b, r, k, \lambda)-$design. The entry (i, j) of AA^T is $\sum_{n=1}^{b} a_{in}a_{jn}$ and $a_{in}a_{jn}$ is not zero if both x_i and x_j belong to the same block n. If $i = j$, then x_i belongs to r blocks, but if $i \neq j$, then x_i and x_j are only together in λ blocks. It results in $AA^T = (r - \lambda)I_v + \lambda J_v$. The second equation follows easily as multiplication with J sums up the entries of a column which means to sum up the treatments that belong to a certain block, and this number is k.
On the other hand, let A be a $v \times b$ matrix with entries zero or one that satisfies the equations then an incomplete block design can be produced. Blocks $B_1, B_2, \ldots, B_b$ are formed of treatments $t_1, t_2, \ldots, t_v$ in such a way that

$$t_i \in B_j \Leftrightarrow a_{ij} = 1.$$

Similar arguments show that it is a $(v, b, r, k, \lambda)-$design and the rest follows from Proposition 5.3.

□

Lemma 5.7. *Consider a $(v, b, r, k, \lambda)-$design and its incidence matrix A. The determinant of AA^T is $(r-\lambda)^{v-1}(r+(v-1)\lambda)$.*

Proof. Proposition 5.6 shows that AA^T has the form

$$\begin{pmatrix} r & \lambda & \dots & \lambda \\ \lambda & r & \dots & \lambda \\ \vdots & & \ddots & \vdots \\ \lambda & \lambda & \dots & r \end{pmatrix}.$$

Transform the matrix by subtracting the first column from every other column then the matrix has the form:

$$\det \begin{pmatrix} r & \lambda - r & \dots & \lambda - r \\ \lambda & r-\lambda & \dots & \mathbf{0} \\ \vdots & & \ddots & \vdots \\ \lambda & \mathbf{0} & \dots & r-\lambda \end{pmatrix} = \det \begin{pmatrix} r+(v-1)\lambda & 0 & \dots & 0 \\ \lambda & r-\lambda & \dots & \mathbf{0} \\ \vdots & & \ddots & \vdots \\ \lambda & \mathbf{0} & \dots & r-\lambda \end{pmatrix}$$
$$= (r+(v-1)\lambda)(r-\lambda)^{v-1}.$$

In the second step all other rows are added to row 1. □

Theorem 5.8 (Fischer's inequality)**.** *In a $(v, b, r, k, \lambda)-$design the inequality $b \geq v$ holds.*

Proof. Let A be the incidence matrix of that design. Since k must be naturally smaller than v, the equality $\lambda(v-1) = r(k-1)$ shows $r > \lambda$ and using Lemma 5.7 shows that $\det(AA^T) \neq 0$, and therefore $\operatorname{rank}(AA^T) = v$. As $v = \operatorname{rank}(AA^T) \leq \operatorname{rank}(A) \leq \min(v, b)$ the inequality $b \geq v$ holds. □

Definition 5.9. *The dual of a regular $(v, b, r, k)-$ design with incidence matrix A is a $(b, v, k, r)-$design with incidence matrix A^T.*

It is easy to see that if a design is incomplete, then its dual is incomplete, too.
If an incomplete block design is balanced then Fischer 's inequality gives $b \geq v$ and consequently its dual is balanced, as well, if and only if $v = b$. It is proved in Lemma 5.39 in detail.

Definition 5.10. *A $(v, b, r, k, \lambda)-$design is symmetric if $v = b$ and with Proposition 5.3 it follows that $r = k$. As a result, these designs are $(v, r, \lambda)-$designs and are denoted by SBIBD.*

Theorem 5.11. *A Hadamard matrix of size $n = 4m$ exists if and only if a $(4m-1, 2m-1, m-1)-$SBIB design exists.*

Proof. Proposition 5.6 is used to show that the Hadamard matrix H_{4m} leads to the incidence matrix of a $(4m-1, 2m-1, m-1)-$ design and conversely. Let H_{4m} be normalised, then

$$H_{4m} = \begin{pmatrix} 1 & e \\ e^T & Q \end{pmatrix}.$$

Q is called the core. It is a matrix with row sum and columns sum (-1), as every row or column must be orthogonal to the first row or first column, respectively. In other words $QJ_{4m-1} = J_{4m-1}Q = -J_{4m-1}$. As $HH^T = 4mI$, it follows that $QQ^T = 4mI - J$. Let $C = \frac{1}{2}(Q + J)$, then C is $(0,1)-$valued.

$$J_{4m-1}C =$$

$$\frac{1}{2}J(Q+J) = \frac{1}{2}(JQ + JJ) = \frac{1}{2}(-J + (4m-1)J) = \frac{1}{2}(4m-2)J = (2m-1)J_{4m-1}$$

$$CC^T =$$

$$\frac{1}{2}(Q+J)\frac{1}{2}(Q^T + J^T) = \frac{1}{4}(QQ^T + QJ + JQ^T + JJ) =$$

$$\frac{1}{4}(4mI - J - J - J + (4m-1)J) = \frac{1}{4}(4mI + (4m-4)J) = mI + (m-1)J$$

Consequently, from Proposition 5.6 it follows that C is the incidence matrix of a design with parameters $v = 4m-1 = b$, $k = 2m-1$ and $\lambda = m-1$. By solving the equation $r - \lambda = m$ it can be concluded that $r = 2m-1$, and H_{4m} leads to a $(4m-1, 2m-1, m-1)-$SBIBD.

On the other hand, let A be the incidence matrix of a $(4m-1, 2m-1, m-1)-$design and define $B = 2A - J$. Furthermore set

$$C = \begin{pmatrix} 1 & e \\ e^T & B \end{pmatrix}.$$

It is left to prove $CC^T = 4mI_{4m}$. Using Proposition 5.6

$$\begin{aligned} CC^T &= \begin{pmatrix} 1 & e \\ e^T & 2A - J \end{pmatrix}\begin{pmatrix} 1 & e \\ e^T & 2A^T - J^T \end{pmatrix} = \begin{pmatrix} 1 + ee^T & e + 2eA - eJ \\ e^T + 2Ae^T - Je^T & ee^T + (2A-J)(2A^T - J) \end{pmatrix} \\ &= \begin{pmatrix} 4m & e + 2(2m-1)e - (4m-1)e \\ e^T + 2(2m-1)e^T - (4m-1)e^T & J + 4AA^T - 2AJ - 2JA^T + JJ \end{pmatrix} \\ &= \begin{pmatrix} 4m & 0 \\ 0 & J + 4(mI + (m-1)J) - 2(2m-1)J - 2(2m-1)J + (4m-1)J \end{pmatrix} \\ &= \begin{pmatrix} 4m & 0 \\ 0 & 4mI \end{pmatrix} = 4mI_{4m}. \end{aligned}$$

□

Definition 5.12. *The $SBIBD-$designs with parameters $v = 4m-1, k = 2m-1, \lambda = m-1$ are called Hadamard (2-)designs.*

Definition 5.13. *Consider a $(v, b, r, k, \lambda)-$design with blocks $B_1, B_2, \ldots, B_b$ formed from the set S. Then the complementary design is the design with sets $S\backslash B_1, S\backslash B_2, \ldots, S\backslash B_b$. Obviously its treatments are from S.*

Example. *In the example above a $(6, 10, 5, 3, 2)-$design is shown. The complementary design of*

$$123, 124, 135, 146, 145, 236, 245, 256, 345, 346$$

is

$$456, 356, 246, 235, 236, 145, 136, 134, 126, 125.$$

Proposition 5.14. *The complementary designs of a $(v, b, r, k, \lambda)-$design is a BIBD-design with parameters $(v, b, b-r, v-k, b-2r+\lambda)$, if $b-2r+\lambda \neq 0$.*

Proof. It is easy to see that the complementary design will still have v treatments and b blocks. A treatment that was previously in r blocks will then belong to $b-r$ blocks. Furthermore, the cardinality of a block in a complementary design is $v-k$. The orginal design fulfills $vr = bk$ and the complementary design $(v, b, b-r, v-k)$ still fulfills this equation with $v \cdot (b-r) = b \cdot (v-k)$. Finally, if two treatments x, y both belonged to λ sets of the original design then there are $2 \cdot (r-\lambda)$ blocks which contain only one of the treatments x, y. In the original design there are $b-\lambda$ blocks which do not contain x and y and $2 \cdot (r-\lambda)$ blocks which do not contain just one of them. In the end, there are $b-2r+\lambda$ blocks which do not contain x or y and this is the number of covalency in the complementary design. □

Theorem 5.15. *If there is a Hadamard matrix of size $n = 4m$, then there are BIBDs with the parameters*

(1) $(2m-1, 4m-2, 2m-2, m-1, m-2)$
(2) $(2m, 4m-2, 2m-1, m, m-1)$
(3) $(2m-1, 4m-2, 2m, m, m)$.

Proof. In the proof of theorem 5.11 it is shown that a $4m \times 4m$ Hadamard matrix leads to a $(4m-1, 2m-1, m-1)-$SBIB design. Let A be the incidence matrix of the design. Then in every column of A there are $2m-1$ ones as $k = 2m-1$, and therefore every treatment is element of $2m-1$ blocks. As a result, there are $4m-1-(2m-1) = 2m$ elements that are zero in every column. Consequently, A can be reordered as

$$\begin{pmatrix} e & B \\ \mathbf{0} & C \end{pmatrix},$$

where e is the unit vector of length $2m-1$. Taking theorem 5.6 in account, the equation

$$mI + (m-1)J = \begin{pmatrix} ee^T + BB^T & BC^T \\ CB^T & CC^T \end{pmatrix} = \begin{pmatrix} J + BB^T & BC^T \\ CB^T & CC^T \end{pmatrix}$$

follows. If the left and right sides of the above equation is compared, then it can be concluded that

$$\begin{aligned} mI_{2m-1} + (m-1)J_{2m-1} &= J_{2m-1} + BB^T \\ mI_{2m-1} + (m-2)J_{2m-1} &= BB^T \\ mI_{2m} + (m-1)J_{2m} &= CC^T \end{aligned}$$

On the other hand, A^T is also an incidence matrix of a $(4m-1, 2m-1, m-1)-$design and therefore

$$mI + (m-1)J = \begin{pmatrix} ee^T & e^TB \\ B^Te & B^TB + C^TC \end{pmatrix} = \begin{pmatrix} 2m-1 & e^TB \\ B^Te & B^TB + C^TC \end{pmatrix}.$$

Again comparing the left and right sides shows that $e^TB = (m-1)(1, \ldots, 1)$ and therefore $JB = (m-1)J$ is true, as well. In other words B has $(m-1)$ ones in every column and therefore the diagonal of B^TB must be a vector where all $4m-2$ entries are $m-1$. As $B^TB + C^TC$ must be $mI + (m-1)J$, the diagonal entry of C^TC is $m + (m-1) - (m-1) = m$. By the same argumentation it follows that $JC = mJ$. Using theorem 5.6, it is shown that a $(2m-1, 4m-2, 2m-2, m-1, m-2)-$design and a $(2m, 4m-2, 2m-1, m, m-1)-$design exist. (3) is just the complementary design of (1). □

Often it is important to know explicitly the elements of the set of treatments and the blocks of a design. As a result, $(X, \mathcal{A})$ is a $(v, b, r, k, \lambda)-$BIBD if X is the $v-$set of treatments and $\mathcal{A}$ is the multiset of blocks with size k. $\mathcal{A}$ must contain b blocks. Every treatment occurs in r blocks and λ must be the covalency number.

Definition 5.16. *Consider two designs $(X, \mathcal{A})$ and $(Y, \mathcal{B})$ with $|X| = |Y|$. These two designs are isomorphic if there exists a bijection $\alpha : X \to Y$ such that*

$$\{\{\alpha(x) : x \in A\} : A \in \mathcal{A}\} = \mathcal{B}.$$

Every block of $\mathcal{A}$ is transformed to a block of $\mathcal{B}$.

Example.

$$X = \{1, 2, 3, 4, 5, 6, 7\}, \mathcal{A} = \{123, 145, 167, 246, 257, 347, 356\}$$

$$Y = \{a, b, c, d, e, f, g\}, \mathcal{B} = \{abd, bce, cdf, deg, aef, bfg, acg\}$$

$(X, \mathcal{A})$ and $(Y, \mathcal{B})$ are isomorphic through

$$\alpha(1) = a, \alpha(2) = b, \alpha(3) = d, \alpha(4) = c, \alpha(5) = g, \alpha(6) = e, \alpha(7) = f.$$

Remark. *The next two facts are easy to verify:*
Let $A = (a_{ij})_{1\le i\le v, 1\le j\le b}$, $B = A = (b_{ij})_{1\le i\le v, 1\le j\le b}$ *be two incidence matrices of two* $(v, b, r, k, \lambda)-$ *BIBD.*

(1) *Then these two designs are isomorphic if and only if*

$$a_{ij} = b_{\beta(i),\gamma(j)}$$

where β *and* γ *are permutations of* $\{1, \dots, v\}$ *and* $\{1, \dots, b\}$*, respectively.*

(2) *Then these two designs are isomorphic if and only if there exist two permutation matrices* P *with size* v *and* Q *with size* b *such that*

$$A = QBP.$$

Definition 5.17. *An automorphism of a design* $(X, \mathcal{A})$ *is an isomorphism of the design with itself. It is easy to see that the set of automorphisms of a design form a group* $Aut(X, \mathcal{A})$*. It is a subgroup of the symmetric group* $S_{|X|}$*.*

The identity mapping of X is of course always an automorphism, but there are also other automorphisms.

Example.

$$X = \{1, 2, 3, 4, 5, 6, 7\}, \mathcal{A} = \{123, 145, 167, 246, 257, 347, 356\}$$

$$\alpha(1) = 1, \alpha(2) = 2, \alpha(3) = 3, \alpha(4) = 5, \alpha(5) = 4, \alpha(6) = 7, \alpha(7) = 6$$

α *is an automorphism.*

Suppose that $(X, \mathcal{A})$ is a $(v, k, \lambda)-$ SBIBD and $\alpha \in \mathrm{Aut}(X, \mathcal{A})$. Then α is a permutation of X and can therefore be written in a composition of disjoint cycles whose lengths sum up to v. Hence, it is possible to talk about the cycle type of α or fixed points of α, but α also induces a permutation α^* on the multiset of the blocks $\mathcal{A}$. A block that will be fixed through α^* is called a fixed block.

Lemma 5.18. $(X, \mathcal{A})$ *is a* $(v, k, \lambda)-$ *SBIBD and* α *an automorphism with* f *fixed points, then* α^* *fixes* f *blocks.*

Proof. Let F be the number of blocks that will be fixed by α^* and

$$I = \{(x, A) : x \in X, A \in \mathcal{A} \text{ and } \{x, \alpha(x)\} \subseteq A\}$$

$|I|$ will be computed in two different ways. First it is considered that the number of treatments determine $|I|$. Secondly, $|I|$ is also determined by the blocks of $\mathcal{A}$. # means

'number of '.

$$\begin{aligned}|I| &= \sum_{x\in X} |\{A \in \mathcal{A} : \{x, \alpha(x)\} \subseteq A\}| \\ &= \sum_{\substack{x\in X \\ \alpha(x)=x}} \underbrace{|\{A \in \mathcal{A} : \{x, \alpha(x)\} \subseteq A\}|}_{\#\text{ blocks which contain one treatment } x} + \sum_{\substack{x\in X \\ \alpha(x)\neq x}} \underbrace{|\{A \in \mathcal{A} : \{x, \alpha(x)\} \subseteq A\}|}_{\#\text{ blocks in which } x,\alpha(x) \text{ belong}} \\ &= fk + (v-f)\lambda\end{aligned}$$

$$\begin{aligned}|I| &= \sum_{A\in\mathcal{A}} |\{x \in X : \{x, \alpha(x)\} \subseteq A\}| \\ &= \sum_{\substack{A\in\mathcal{A} \\ \alpha^*(A)=A}} \underbrace{|\underbrace{\{x \in X : \{x, \alpha(x)\} \subseteq A\}}_{=A \text{ as } \alpha^*(A)=A\Rightarrow\alpha(x)\in A:\forall x\in A}|}_{=k} + \sum_{\substack{A\in\mathcal{A} \\ \alpha^*(A)\neq A}} \underbrace{|\underbrace{\{x \in X : \{x, \alpha(x)\} \subseteq A\}}_{\{x,\alpha(x)\}\Leftrightarrow x\,\in\, A\cap(\alpha^*)^{-1}(A)}|}_{=\lambda} \\ &= Fk + (v-F)\lambda\end{aligned}$$

$$\Rightarrow fk + (v-f)\lambda = Fk + (v-F)\lambda$$
$$k(f-F) = \lambda(f-F).$$

From Proposition 5.3 it follows that in a SBIBD $\lambda \neq k$. Therefore, the equation before shows $f = F$. □

A similar statement is true for the cycle length. This will be proved with a useful combinatorical technique.

Definition 5.19. *The Möbius function $\mu : \mathbb{N} \to \{-1, 0, 1\}$ is defined as*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ is square-free and } k \text{ is the number of distinct prime factors of } n\,. \\ 0 & \text{if } n \text{ has squared prime factors.} \end{cases}$$

Theorem 5.20 (Möbius Inversion Formula)**.** *Let $f, g : \mathbb{N} \to \mathbb{R}$ be functions and*

$$f(j) = \sum_{i|j} g(i),$$

then

$$g(i) = \sum_{j|i} \mu\left(\frac{i}{j}\right) f(j).$$

Lemma 5.21. *$(X, \mathcal{A})$ a symmetric $(v, k, \lambda)-$SBIBD and $\alpha \in Aut(X, \mathcal{A})$. The cycle type of the induced permutation α^* is the same as the cycle type of α.*

Proof. Let c_i be the number of cycles of length i of a permutation α of a finite set and f_j the number of fixpoints of α^j. Then

$$f_j = \sum_{i|j} i \cdot c_i.$$

The Möbius inversion formula shows with $g(i) = ic_i$ and $f_j = f(j)$ that

$$i \cdot c_i = \sum_{j|i} \mu\left(\frac{i}{j}\right) f_j$$

and therefore,

$$c_i = \frac{1}{i} \sum_{j|i} \mu\left(\frac{i}{j}\right) f_j. \tag{5.1}$$

If $\alpha \in \mathrm{Aut}(X, \mathcal{A})$, then $\alpha^j \in \mathrm{Aut}(X, \mathcal{A})$. Lemma 5.18 shows that f_j is the same number for α^j as for the induced automorphism $(\alpha^*)^j$. From equation 5.1 it follows that the cycle type is the same for both automorphisms. □

These two lemmata will be used in the next chapter.

5.2. Difference sets

If not stated otherwise this chapter follows mainly the chapter "difference sets" in [23].

Definition 5.22. *Let $(G, +)$ be a finite group of order v with identity element 0. Let λ and k be positive integers with $2 \leq k < v$. Then a $(v, k, \lambda)-$difference set in $(G, +)$ is a subset B with k elements and the multiset $\{x - y | x, y \in B, x \neq y\}$ contains every element of the set $G \setminus \{0\}$ λ times.*

Remark. *G need not to be Abelian, but in examples $G = \mathbb{Z}_n = (\mathbb{Z}/n\mathbb{Z}, +)$ is often used.*

Here are some examples of difference sets.

Examples. (1) *Let $G = \mathbb{Z}/7\mathbb{Z} = \mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ and $B = \{1, 2, 4\}$. Obviously $v = b = 7$ and $k = r = 3$. This is a difference set with $\lambda = 1$, because*

$(1, 2)$ has difference 1
$(2, 4)$ has difference 2
$(1, 4)$ has difference 3
$(4, 1)$ has difference $-3 = 4$
$(4, 2)$ has difference $-2 = 5$
$(2, 1)$ has difference $-1 = 6$
and no other combinations are possible.

(2) *$G = \mathbb{Z}_5$ and $B = \{1, 2, 3, 4\}$. B is a (5,4,3) difference set.*

(3) *Let $G = \mathcal{S}_3 = \{id, \pi_1 = (12), \pi_2 = (23), \pi_3 = (13), \sigma_1 = (132), \sigma_2 = (123)\}$, obviously a non-Abelian group. Then G has 6 elements. We want to find a difference*

set in this group. For the size of the difference set B, it is impossible to choose 2,3 or 4, as the multiset $\{x-y|x,y\in B, x\neq y\}$ would have 2, 6 or 12 members. Thus, it is impossible that the multiset would contain every member of $|\mathcal{S}\setminus id|=5$ exactly λ times. If B had 5 elements, then the multiset would have 20 elements. It would be possible if $\lambda=4$. Try $D=\{\pi_1,\pi_2,\pi_3,\sigma_1,\sigma_2\}$. Using the group table of $\mathcal{S}_3$,

$\circ$	id	π_1	π_2	π_3	σ_1	σ_2
id	id	π_1	π_2	π_3	σ_1	σ_2
π_1	π_1	id	σ_1	σ_2	π_2	π_3
π_2	π_2	σ_2	id	σ_1	π_3	π_1
π_3	π_3	σ_1	σ_2	id	π_1	π_2
σ_1	σ_1	π_3	π_1	π_2	σ_2	id
σ_2	σ_2	π_2	π_3	π_1	id	σ_1

it is easily seen that that the set D is a $(6,5,4)-$difference set.

Difference sets can be used to generate SBIBDs.

Definition 5.23. *Let B be a $(v,k,\lambda)-$difference set of the group $(G,+)$ with order v, then the design generated from B consists of the blocks*

$$\{B+g|g\in G\}.$$

A set $B+g$ is called translate of B and $Dev(B)$ is the collection of all v translates of B.

So it follows that the design generated from B is a block design with v treatments and v blocks. Every block consists of k treatments. An $h\in G$ satisfies $h\in B+g$ if and only if $g\in B-h$. There are exactly $|B|=k$ such g and therefore $r=k$.

Under which conditions the design is balanced is explained by the next Lemma.

This proof can be found in [26], but not in such a detail.

Lemma 5.24. *If the subset B of an abelian group $(G,+)$ with order v contains λ_i ordered pairs whose difference is g_i and x, y is a pair in G whose difference is g_i, then x,y is a subset of λ_i blocks in the design generated by B.*

Proof. Let $(a_1,b_1),(a_2,b_2),\cdots,(a_{\lambda_i},b_{\lambda_i})$ be all the ordered pairs in B^2 that have difference $b_j-a_j=g_i:\forall j\in\{1,\ldots,\lambda_i\}$. If x,y is a pair in G with difference $x-y=g_i$, then x,y is contained in the blocks $B+(x-b_1),B+(x-b_2),\cdots,B+(x-b_{\lambda_i})$. To understand this statement consider for example the first block: $b_1\in B\Rightarrow b_1+(x-b_1)=x$ and $a_1\in B\Rightarrow a_1+(x-b_1)=x+(a_1-b_1)=x-g_i=y$. As all these blocks are different, the pair x,y is contained in at least λ_i blocks. Suppose x,y is contained in $B+d$. Then $g_i=x-y=(x-d)-(y-d)$, but $x-d$ and $y-d$ are in B. In other words $(y-d,x-d)$ must be one of the pairs (a_j,b_j) listed above. Consequently, exactly λ_i blocks contain x,y. □

From Lemma 5.24 follows:

Corollary 5.25. *The design $(G, Dev(B)$ generated from a (v, k, λ) difference set is a $(v, k, \lambda)-SBIBD$.*

Using Proposition 5.3 the next corollary can be easily seen.

Corollary 5.26. *A (v, k , λ) difference set satisfies $(v-1)\lambda = k(k-1)$.*

Example. *Above we have seen that $B = \{1, 2, 4\}$ is a $(7, 3, 1)-$difference set in $G = \mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. The design generated from B and therefore the multiset $Dev(B)$ is*

$$(1, 2, 4), (2, 3, 5), (3, 4, 6), (0, 4, 5), (1, 5, 6), (0, 2, 6), (0, 1, 3).$$

The design has the incidence matrix

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

The question arises if corollary 5.25 also has a converse. Indeed, with some preconditions there is a converse.

Theorem 5.27. *Let $(X, \mathcal{A})$ be a $(v, k, \lambda)-SBIBD$ and $\alpha \in Aut(X, \mathcal{A})$ with α having only one cycle (therefore, the cycle has length v). Then there is a $(v, k, \lambda)-$ difference set in $(\mathbb{Z}/v\mathbb{Z} = \mathbb{Z}_v, +)$.*

Proof. W.l.o.g. it is assumed that for the set $X = \{x_0, x_1, \ldots, x_{v-1}\}$ the automorphism α is $\alpha(x_i) = x_{i+1 \bmod v} : 0 \leq i \leq v-1$. As a result,

$$\alpha = (x_0\ x_1 \ldots\ x_{v-1}).$$

Choose a block $A_0 \in \mathcal{A}$ and define

$$A_j = \{\alpha^j(x) : x \in A_0\} = \{x_{i+j \bmod v} : x_i \in A_0\}.$$

A_j is a block in $\mathcal{A}$ as $\alpha^j \in \mathrm{Aut}(X, \mathcal{A})$. Clearly $\alpha(A_j) = A_{j+1 \bmod v}$ and from Lemma 5.21 it follows that α^* is a cycle of length v. In conclusion it is proved that

$$\mathcal{A} = \{A_0\ (= A_v), A_1, \ldots, A_{v-1}\} \text{ and } \alpha^* = (A_0\ A_1 \ldots A_{v-1}).$$

The difference set D of $(\mathbb{Z}_v, +)$ can now be defined as

$$D = \{i : x_i \in A_0\}.$$

D has k members, as every block of $\mathcal{A}$ has size k and is a subset of $\mathbb{Z}_v$. Keep in mind that if $A_{i_l} \in \mathcal{A}$ and $x_k \in A_{i_l}$, then the definition of the blocks A_j implies that $x_{k-i_l} \in A_0$. That will be used in the to show that D is a difference set.
Let $g \in \mathbb{Z}_v, g \neq 0$. The pair $\{x_0, x_g\}$ appears in λ blocks, say $A_{i_1}, \ldots, A_{i_\lambda}$.

$$\{x_0, x_g\} \subseteq A_{i_j} \Leftrightarrow \{x_{-i_j \bmod v}, x_{g-i_j \bmod v}\} \subseteq A_0 \Rightarrow \{-i_{j \bmod v}, g - i_{j \bmod v}\} \subseteq D$$

$$\Leftrightarrow (g - i_{j \bmod v}) - (-i_{j \bmod v}) = g.$$

In other words, there are λ distinct pairs in D with difference g. As g was chosen arbitrarily it is proved that D is a (v, k, λ) difference set of $(\mathbb{Z}_v, +)$. □

The theorem can be generalised for arbitary finite groups by using sharply transitive groups.

Definition 5.28. *Suppose that $G \subseteq S_v$ is a permutation group acting on the v-set X. G acts sharply transitive if $\forall x_1, x_2 \in X\ \exists! g \in G : g(x_1) = x_2$.*

Similar to the proof of theorem 5.27 it is proved in [1] that:

Theorem 5.29. *Let G be a finite group and D a proper subset. Then the following statements are equivalent.*

(1) *D is a (v, k, λ) difference set in G.*
(2) *$Dev(D)$ is a $(v, k, \lambda)-$SBIBD with G a sharply transitive subgroup of $Aut(X, \mathcal{A})$.*

Theorem 5.30. *Let $v = 4t - 1$ be a prime power congruent 3 mod 4, then there exists a $(4t - 1, 2t - 1, t - 1)-$ difference set.*

Proof. Let D be the set of all perfect squares of the cyclic multiplicative group of $G = GF(v)$ which has $v - 1 = 4t - 2$ elements. The group D has $2t - 1$ elements as Lemma 2.33 showed. Simple combinatorics shows that there are $(2t - 1)(2t - 2) = (t - 1)(4t - 2)$ pairs of different elements of D. We need to prove that for every element of $a \in GF(v)$ there are $\lambda = t - 1$ such pairs that have difference a.
Let x, y be a pair in D that has difference 1 and suppose there are λ such pairs. The proof will show that there are $x, y \in D$ with $x - y = 1$. Multiplying with any perfect squares q leads to $qx - qy = q$ and as qx and qy are perfect square themselves, the pair $(qx, qy) \in D^2$ has difference q. Hence, there are λ pairs in D that have difference q. On the other hand if a pair x, y has differnce q then $q^{-1}x, q^{-1}y$ has difference 1.
Considering that every element which is not a perfect square is a negative of a perfect square: Let a be a perfect square, then $\chi(a) = 1 \Rightarrow \chi(-a) = \chi(-1)\chi(a) = -1$. As the number of perfect squares is $2t - 1$, this leads to $2t - 1$ non perfect squares and adding (-1) these are all the non perfect squares.
The pair (qy, qx) has difference $-q$ and there are λ of these pairs. With the help of corollary 5.26 every element of $GF(v)$ must appear $\frac{(4t-2)(t-1)}{4t-2} = t - 1$ times in a block.
□

Definition 5.31. *The difference sets constructed in theorem 5.30 are called Paley difference sets. Generally, difference sets with parameters* $(4t-1, 2t-1, t-1)$ *are called Hadamard difference sets.*

Clearly, every Hadamard difference set leads to a Hadamard matrix due to theorem 5.11. Sometimes difference sets with the parameters $\left(q, \frac{q-1}{2}, \frac{q-3}{4}\right)$ are called Paley difference sets, but keep in mind that this is the same as if $4t-1$ is substituted by q.

There are three big families of Hadamard difference sets:

(1) Paley difference sets with parameters $(q, \frac{q-1}{2}, \frac{q-3}{4})$ in $(GF(q), +)$.
(2) Singer difference sets with parameters $(2^t-1, 2^{t-1}-1, 2^{t-2}-1)$ with $t \geq 2$. (Clearly they also fulfill the parameters of Hadamard difference sets).
(3) Twin prime power difference sets with parameters $(q(q+2), \frac{q(q+2)-1}{2}, \frac{q(q+2)-3}{4})$ with q and $q+2$ both being prime powers.

In design theory Singer difference sets are more general and this difference sets will be explained now. For the next proof recall theorem 4.25 and theorem 4.26.

Theorem 5.32. *If* q *is a prime power,then there exists a* $(q^2+q+1, q+1, 1)$ *difference set in* $(\mathbb{Z}_{q^2+q+1}, +)$.

Proof. As in the proof of theorem 4.25 $V = GF(q^3)$. V_1 contains all the one-dimensional vector spaces over $GF(q)$ and V_2 the two-dimensional spaces over $GF(q)$. Let ω be a primitive element of $GF(q^3)$ and define the mapping $f : V \to V, f(z) = \omega z$. f is a $GF(q)-$linear mapping and therefore preserves subspaces of V. Consequently every subspace of V_1 or V_2 is mapped into a subspace of V_1 or V_2, respectively. Section 5.2 shows that f is an automorphism of the resulting $(q^2+q+1, q+1, 1)-$SBIBD. It was already used before that $GF(q) = \{w^{(q^2+q+1)\cdot i} : 0 \leq i \leq q-2\} \cup \{(0,0,0)\}$. This explains $f^{q^2+q+1}(W) = W$ for any subspace W of V. As a consequence, f permutes every element of V_1 in a single cycle of length q^2+q+1. Applying theorem 5.27 shows the statement. □

Similar to Section 5.2, identical arguments show:

Theorem 5.33. *Suppose* q *is a prime power and* $d \geq 2$ *is an integer, then there exists a*

$$\left(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}\right)$$

idifference set in $\mathbb{Z}_{(q^{d+1}-1)/(q-1)}, +)$.

Definition 5.34. *The difference sets from theorem 5.33 are called Singer difference sets. As mentioned before, they are Hadamard difference sets for* $q = 2$ *and* $d+1 = t$.

Although Singer difference sets are very interesting and there are a lot of different possibilities to construct them, they are equivalent to an important class of Hadamard matrices, namely Sylvester Hadamard matrices. This will be shown by using two different

construction possibilities for these two kind of matrices. The definitions of the next part can be found in [8], p. 11, 15.

Sylvester Hadamard matrices were defined by using corollary 2.24. The definition shows straightforwardly that:

Lemma 5.35. *Using the notation of corollary 2.24, for* $t \geq 1$

$$S^t = S^1 \otimes S^{t-1}$$

Lemma 5.36. *Let* $S^t = (s_{i,j})_{0 \leq i,j \leq 2^t-1}$ *be the Sylvester of size* 2^t*, then*

$$S^t = \left((-1)^{<i,j>}\right)_{0 \leq i,j \leq 2^t-1} \tag{5.2}$$

where i, j *are the indices of* S^t *written in binary representation as a vector of length* t *over* $GF(2)$ *and* $<,>=<,>_2$ *is the scalar product of two vectors over* $GF(2)$*, hence* $<(x_1x_2\ldots x_n),(y_1y_2\ldots y_n)>_2 = x_1 \cdot y_1 + x_2 \cdot y_2 + \cdots + x_n \cdot y_n \ mod\ 2$.

Proof. From Lemma 5.35 it follows that the Sylvester Hadamard matrices can be defined recursively. Mathematical induction is used to proof the statement.
Let $t = 1$, then

$$S^1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1_{(0,0)} & 1_{(0,1)} \\ 1_{(1,0)} & -1_{(1,1)} \end{pmatrix} = \begin{pmatrix} (-1)^{<0,0>} & (-1)^{<0,1>} \\ (-1)^{<1,0>} & (-1)^{<1,1>} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Suppose that the statement holds for $t-1$. The inductive step shows that the statement holds for S^t, as well. Using Lemma 5.35 shows that

$$\begin{aligned}
S^t = S^1 \otimes S^{t-1} &= \begin{pmatrix} (-1)^{<0,0>} & (-1)^{<0,1>} \\ (-1)^{<1,0>} & (-1)^{<1,1>} \end{pmatrix} \otimes [(-1)^{<i,j>}]_{0 \leq i,j \leq 2^t-2} \\
&= \begin{pmatrix} (-1)^{<0,0>} \cdot [(-1)^{<i,j>}]_{0 \leq i,j \leq 2^t-2} & (-1)^{<0,1>} \cdot [(-1)^{<i,j>}]_{0 \leq i,j \leq 2^t-2} \\ (-1)^{<1,0>} \cdot [(-1)^{<i,j>}]_{0 \leq i,j \leq 2^t-2} & (-1)^{<1,1>} \cdot [(-1)^{<i,j>}]_{0 \leq i,j \leq 2^t-2} \end{pmatrix} \\
&= \begin{pmatrix} [(-1)^{<0,0>+<i,j>}]_{0 \leq i,j \leq 2^t-2} & [(-1)^{<0,1>+<i,j>}]_{0 \leq i,j \leq 2^t-2} \\ [(-1)^{<1,0>+<i,j>}]_{0 \leq i,j \leq 2^t-2} & [(-1)^{<1,1>+<i,j>}]_{0 \leq i,j \leq 2^t-2} \end{pmatrix} \\
&= \begin{pmatrix} [(-1)^{<0i,0j>}]_{0 \leq i,j \leq 2^t-2} & [(-1)^{<0i,1j>}]_{0 \leq i,j \leq 2^t-2} \\ [(-1)^{<1i,0j>}]_{0 \leq i,j \leq 2^t-2} & [(-1)^{<1i,1j>}]_{0 \leq i,j \leq 2^t-2} \end{pmatrix} \\
&= \left((-1)^{<i,j>}\right)_{0 \leq i,j \leq 2^t-1}.
\end{aligned}$$

□

Now the Singer difference sets are proved to exists using the trace function. The next proof was more general given in [5] and adapted.

Lemma 5.37. *Let* q *be a prime power and* $q \geq 3$*. Consider* $F = GF(q^n)$ *which is a vector space over* $K = GF(q)$*. Let* α *be a primitive element of* F^**, hence* $\alpha^{q^n-1} = 1$*. The*

trace (compare: 4.13) can be used to define

$$D = \{\alpha^i : 0 \leq i < q^n - 1, Tr_{F^*/K^*}(\alpha^i) = 0\}. \tag{5.3}$$

D is a Singer difference sets with parameters $(\frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}, \frac{q^{n-2}-1}{q-1})$ in the quotient group $GF(q^n)^*/GF(q)^*$.

Proof. Obviously the quotient group $GF(q^n)^*/GF(q)^*$ has $\frac{q^n-1}{q-1}$ elements and is a group. By definition D is a subset of this group. From Lemma 4.15 it follows that D has $\frac{q^{n-1}-1}{q-1}$ elements. It is left to prove that in the set of differences, each element of F^*/K^* occurs exactly λ times. The set of differences is

$$\{\alpha^{-i+j} : i, j \subset \{0, 1, \ldots, q^n - 2\}, Tr_{F^*/K^*}(\alpha^i) = 0 \text{ and } Tr_{F^*/K^*}(\alpha^j) = 0\}.$$

Let α^b be any (non zero) element in F^* and $\alpha^b \notin K$. It is claimed that there exist α^i and α^j in D such that $\alpha^b = \alpha^{-i} \cdot \alpha^j$. Then $\alpha^{b+i} = \alpha^j \Rightarrow Tr_{F^*/K^*}(\alpha^j) = Tr_{F^*/K^*}(\alpha^{b+i}) = 0$. Using the notation of theorem 4.17, it can be rewritten as $L_{\alpha^j}(1) = L_{\alpha^i}(\alpha^b) = 0$. Corollary 4.18 shows that there are $\frac{q^{n-1}-1}{q-1}$ different linear L_{α^j} mappings. Again the kernel of the mapping has dimension $\frac{q^{n-2}-1}{q-1}$. In conclusion, every element α^b occurs $\lambda = \frac{q^{n-2}-1}{q-1}$ times in the difference set of D.

□

The next proof is from [8], p.19.

Theorem 5.38. *The Hadamard matrix that is constructed from the difference set 5.37 with $F = GF(q^t)$ is equivalent to the Sylvester matrices defined by 5.36.*

Sketch of proof. Let α be a generator of $GF(2^t)^*$ and $GF(2^t)$ is ordered by the induced order, therefore $GF(2^t) = \{0, \alpha^i : 0 \leq i \leq 2^{t-1}\}$. Let

$$A = [Tr_{GF(2^t)/GF(2)}(gh)]_{g,h \in GF(2^t)} \text{ and } H = [(-1)^{Tr_{GF(2^t)/GF(2)}(gh)}]_{g,h \in GF(2^t)}$$

Keep in mind that H is the incidence matrix induced by the Singer difference. This is a consequence of $(-1)^{\alpha^i} = 1 \Leftrightarrow Tr_{GF(2^t)^*/GF(2)^*}(\alpha^i) = 0 \Leftrightarrow \alpha^i$ is an element of the Singer difference set. Furthermore, the first row and column in the Hadamard matrix of a design (compare the proof of theorem 5.11) has to be the unit vector e or e^T.
As the trace function is a linear map from $(GF(2)^t, +)$ to $\{0, 1\}$, A has rank t over $GF(2)$. Therefore, a set of t linearly indepedent vectors of A exists and A has columns consisting of every vector in $(\mathbb{Z}/2\mathbb{Z})^t$. Consider the map $\log : (-1)^k \mapsto k$. Then $A_{2^t} = [\log((-1)^{<i,j>})]_{0 \leq i,j \leq 2^t-1}$ is the binary version of S_t. As the log function is also a linear transformation, A_{2^t} has also t lineary indepedent rows and columns consisting of every vector of $(\mathbb{Z}/2\mathbb{Z})^t$. Hence, there is a column permutation that changes the t linearly indepedent rows of A to the t linearly indepedent rows of A_{2^t}. These column permutation expanded to all rows of A convert also H to S_t. □

5.3. Regular Hadamard matrices and their designs

Recalling the definition 2.12, a Hadamard matrix is regular if every row has the same number of ones. There is an important connection between special SBIBD and regular Hadamard matrices. To prove that we need a generalization of proposition 5.6.

Lemma 5.39. *Let A be a $v \times v$ nonsingular matrix with entries one or zero that satisfies one of*

(A1) $AA^T = (k-\lambda)I + \lambda J$
(A2) $A^TA = (k-\lambda)I + \lambda J$

and one of

(B1) $JA = kJ$
(B2) $JA^T = kJ$.

Then A satisfies all four equations and it is an incidence matrix of a $(v,k,\lambda)-$SBIBD. Furthermore, the equation

$$k(k-1) = \lambda(v-1)$$

holds.

Proof. Proposition 5.6 shows that if (A1) and (B2) are true, then A is an incidence matrix of a $(v,k,\lambda)-$SBIBD and $k(k-1) = \lambda(v-1)$ are true as well.
As A is nonsingular, it follows that both AA^T and A^TA have nonzero determinant and as a result, Lemma 5.7 implies that

$$k - \lambda \neq 0 \text{ and } \lambda(v-1) + k \neq 0.$$

First it is shown that (A1) and (B1) imply (A2) and (B2).
Multiplying (A1) with J from the left gives

$$\begin{aligned} JAA^T &= (k-\lambda)J_v \cdot I_v + \lambda J_v^2 \\ kJA^T &= (k-\lambda)J_v + \lambda v J_v \\ kJA^T &= (k-\lambda+\lambda v)J. \end{aligned}$$

In the second equation (B1) is used. Now multiplying again with J from the right:

$$\begin{aligned} kJA^TJ &= (k-\lambda+\lambda v)J^2 \\ kJ(JA)^T &= (k-\lambda+\lambda v)J^2 \\ kJ(kJ)^T &= (k-\lambda+\lambda v)J^2 \\ k^2J^2 &= (k-\lambda+\lambda v)J^2. \end{aligned}$$

$\Rightarrow k^2 = k - \lambda + \lambda v = \lambda(v-1) + k \neq 0$. Substituting this in $kJA^T = (k - \lambda + \lambda v)J$ leads to $kJA^T = k^2 J$. As $k \neq 0$, (B2) is shown. (A2) can be seen as $AJ = (JA^T)^T = (kJ)^T = kJ = JA$ and that is substituted in

$$\begin{aligned} A^T A &= (A^{-1}A)A^T A = A^{-1}(AA^T)A \\ &= (k-\lambda)A^{-1}IA + \lambda A^{-1}JA \\ &= (k-\lambda)I + \lambda A^{-1}AJ \\ &= (k-\lambda)I + \lambda J. \end{aligned}$$

Next suppose that (A1) and (B2) are true and (A2) and (B1) have to be shown. Using the precondition, (A1) in the next equation chain shows that

$$A^T = A^{-1}(AA^T) = (k-\lambda)A^{-1} + \lambda A^{-1}J.$$

It follows from (B2) that $AJ = kJ$ and so

$$J = kA^{-1}J. \tag{5.4}$$

Therefore,

$$A^T = (k-\lambda)A^{-1} + \lambda k^{-1}J. \tag{5.5}$$

Substituting A^T in (B2) shows that

$$\begin{aligned} kJ &= JA^T \\ &= (k-\lambda)JA^{-1} + \lambda k^{-1}J^2 \\ &= (k-\lambda)JA^{-1} + \lambda k^{-1}vJ \end{aligned}$$

This equation is now transformed in a way that JA^{-1} is isolated. It is possible as $k - \lambda \neq 0$. A subsequent mulitiplication with J from the right results in

$$JA^{-1}J = \frac{(k - \lambda k^{-1}v)J^2}{k-\lambda} = \frac{k - \lambda k^{-1}v}{k-\lambda}(vJ). \tag{5.6}$$

On the other hand we have $vk^{-1}J = k^{-1}J^2 \underbrace{=}_{\text{equation 5.4}} k^{-1}J(kA^{-1}J) = JA^{-1}J$. Using this in equation 5.6 shows $vk^{-1}J = \frac{k-\lambda k^{-1}v}{k-\lambda}(vJ)$. As v can be cancelled out, comparing the entries of these two matrices gives

$$k^{-1} = \frac{k - \lambda k^{-1}v}{k-\lambda}. \tag{5.7}$$

It can be reduced to

$$k - \lambda = k^2 - \lambda v$$
$$k(k-1) = \lambda(v-1)$$

and therefore a part of the claim is shown. Using equation 5.7 in equation 5.6 shows (B1). Returning to equation 5.5 and using (B1) shows (A2):

$$\begin{aligned} A^T A &= (k-\lambda)A^{-1}A + \lambda k^{-1} JA \\ &= (k-\lambda)I + \lambda k^{-1} kJ \\ &= (k-\lambda)I + \lambda J. \end{aligned}$$

The other two cases are just A replaced by A^T and therefore are shown analogously. □

Corollary 5.40. *The dual of a balanced incomplete block design is balanced if and only if the design is symmetric.*

Proof. (1) If $b > v$ then its dual would have more treatments than blocks and that would contradict Fischer's inequality.
(2) If $b = v$ then Lemma 5.39 shows that its dual is a BIBD, too.
(3) $b < v$ is impossible because of it would contradict Fischer's inequality, too.

□

Theorem 5.41. *The existence of a $4m \times 4m$ regular Hadamard matrix is equivalent to the existence of a symmetric balanced incomplete block design with parameters.*

(1) $v = b = 4m$
(2) $k = r = 2m \pm m^{1/2}$
(3) $\lambda = m \pm m^{1/2}$

Proof. $\Rightarrow$
Let H be a regular Hadamard matrix. Then every row has the same number of ones, say h and so every row has $4m - h$ minus ones. From theorem 2.3 it follows that

$$HH^T = 4mI$$
$$HJ = hJ - (4m-h)J = (2h - 4m)J.$$

The last equation is true as multiplying with J from the right is a summation of the row entries. Let $A = \frac{1}{2}(H + J)$. Then A is a $4m \times 4m$ matrix with entries zero or one. We

want to use Lemma 5.39 and therefore (A1) und (B2) are shown.

$$\begin{aligned}
AA^T &= \frac{1}{4}(H+J)\cdot(H^T+J^T)\\
&= \frac{1}{4}(HH^T+HJ^T+JH^T+JJ^T)\\
&= \frac{1}{4}(4mI+(2h-4m)J+(HJ^T)^T+4mJ)\\
&= mI+\frac{1}{4}(2hJ-4mJ+2hJ-4mJ+4mJ) = mI+hJ-mJ\\
AJ &= \frac{HJ+J^2}{2}\\
&= \frac{(2h-4m+4m)J}{2} = hJ.
\end{aligned}$$

Therefore, A is the incidence matrix of a SBIBD with parameters $v=b=4m, k=r=h, \lambda=h-m$. Equation $r(k-1)=\lambda(v-1)$ leads to $h\cdot(h-1)=(h-m)\cdot(4m-1)$. Multiplication and using the quadratic formula shows $h=2m\pm\sqrt{4m^2-4m^2+m}=2m\pm\sqrt{m}$. Consequently, one direction is shown.
On the other hand, let A be the incidence matrix of a $(4m, 2m\pm\sqrt{m}, m\pm\sqrt{m})-$design, then $AA^T=mI+(m\pm\sqrt{m})J$ and $JA=JA^T=AJ=(2m\pm\sqrt{m})J$. Let H be $2A-J$, then H is a regular Hadamard matrix, because

$$\begin{aligned}
HH^T &= 4AA^T-2AJ-2JA^T+JJ^T\\
&= 4mI+4(m\pm\sqrt{m})J-4(2m\pm\sqrt{m})J+4mJ\\
&= 4mI\\
HJ &= 2AJ-J^2\\
&= \pm 2\sqrt{m}J \Rightarrow He = \pm 2\sqrt{m}e.
\end{aligned}$$

Therefore, H is a Hadamard matrix with every row having the same sum and consequently it is regular. □

Corollary 5.42. *If there exists a regular Hadamard matrix of size n, then n is a perfect square.*

Proof. The proof of theorem 5.41 shows that if $n=4m$, then m is a perfect square and therefore n is a perfect square, too, as $4=2^2$. It is easily shown that there is no regular Hadamard matrix of order 2 and there is only the trivial Hadamard matrix (1) of size 1 which can be assumed regular as $1^2=1$. □

Corollary 5.43. *Let H be an $n\times n$ regular Hadamard matrix and $n=4u^2$, then H is equivalent to a $(4u^2, 2u^2\pm u, u^2\pm u)-$SBIBD.*

Proof. Theorem 5.41 and using $m=u^2$. □

From this corollary another corollary follows, namely:

Corollary 5.44. *The three properties are equivalent:*

(1) *H is a regular Hadamard matrix.*
(2) *H^T is a regular Hadamard matrix, hence H has regular columns.*
(3) *H has the same number of ones in every column and every row, therefore the row sum and column sum is constant.*

Proof. corollary 5.43 shows that the design is symmetric if and only if H has regular rows, therefore H^T has regular columns, but H^T is also equivalent to this design as the dual of an SBIBD has the same parameters. □

Lemma 5.45. *If two Hadamard matrices are regular, then the Kronecker product is regular, too.*

Proof. Recall the Kronecker product of $A = (a_{ij})_{1 \leq i,j \leq m}$ and an $n \times n$ - matrix B is

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ a_{21}B & a_{12}B & \cdots & a_{1m}B \\ \vdots & \vdots & \cdots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mm}B \end{pmatrix}.$$

If A has l ones in a row (column) and B has k ones in a row (column), then in every column of $A \otimes B$ are l blocks with k ones in a row (column) and $(m-l)$ blocks with $(n-l)$ ones in a row (column). In the end the sum of every column is $l \cdot k + (m-l) \cdot (n-l)$ and so $A \otimes B$ is regular. □

Corollary 5.46. *If regular Hadamard matrices of size n and m exist, then a regular Hadamard matrix of size $n \cdot m$ exists. In particular, for $m = n$ there is a regular Hadamard matrix of size n^2 always if a Hadmard matrix of size n was found.*

It is easy to obtain an infinite class of regular Hadamard matrices by:

Proposition 5.47. *Let a, b be non-negative integers and $a \geq b$, then there exists a regular matrix of size $4^a 9^b$.*

Proof. If $a = b = 0$, then (1) is the trivial regular Hadamard matrix. If $a = 1$, then eg. $\mathrm{circ}(-1, 1, -1, -1)$ is regular and therefore $a + b \geq 1$ can be assumed. Rewrite $4^a 9^b = 4^a 4^{-b} 4^b 9^b = 4^{a-b} 36^b$ and by computation it is seen that

$$D = \{(0, i) : 1 \leq i \leq 5\} \cup \{(i, 0) : 1 \leq i \leq 5\} \cup \{(i, i) : 1 \leq i \leq 5\}$$

is a $(35, 15, 6)-$difference set in $(\mathbb{Z}_6 \times \mathbb{Z}_6, +)$. Therefore, corollary 5.43 shows that a regular Hadamard matrix of size 36 exists. Using Lemma 5.45 shows that regular Hadamard matrices of size 4^{a-b} and 36^b exist and the product of these is of course also a regular Hadamard matrix. □

Before group-developed matrices and their connection with regular Hadamard are explained matrices, the interesting term "excess", is shortly explained.

Definition 5.48. *The excess of an $n \times n$ Hadamard matrix $H = (h_{ij})$ is defined as*

$$excess(H) = \sum_{1 \le i,j \le n}^{n} h_{ij}.$$

Therefore, the excess is the sum of all row sums (column sums) or, taking into account that the name is excess, it is the number of 1s that exceeds the number of (-1)s.

Definition 5.49.

$$\sigma(n) = \max\{excess(H) : H \textit{is a Hadamard matrix of order } n\}$$

Of course, $\sigma(n)$ can only be defined if a Hadamard matrix of order n exists.

The following simple, but important lemma gives an upper bound for the maximum excess of a Hadamard matrix. This was also proved in [13]. In this paper it is also shown how the excess can be used to construct Hadamard matrices. J. Seberry gives a short overview of this topic in [27].

Lemma 5.50. $\sigma(n) \le n \times \sqrt{n}$.

Proof. Let $H = (h_{ij})_{1 \le i,j \le n}$ be a Hadamard matrix. Define the column sum of the $k-$th column as

$$s_k = \sum_{i=1}^{n} h_{i,k}.$$

Clearly, the excess is the sum of all s_ks. Therefore

$$\text{excess}(H) = \sum_{k=1}^{n} s_k. \tag{5.8}$$

Let $r_1, \ldots, r_n$ be the row vectors of H, then the sum $\sum_{i=1}^{n} \sum_{j=1}^{n} < r_i, r_j >$ will be counted in two ways. On the one hand, it is obvious that $< r_i, r_j >= n$ if and only if $i = j$ and zero if $i \neq j$ as H is Hadamard. Hence,

$$\sum_{i=1}^{n} \left(\sum_{j=1}^{n} < r_i, r_j > \right) = \sum_{i=1}^{n} n = n \cdot n = n^2.$$

On the other hand,

$$\begin{aligned} \sum_{i=1}^{n} \sum_{j=1}^{n} < r_i, r_j > &= \sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{k=1}^{n} h_{i,k} h_{j,k} \\ &= \sum_{k=1}^{n} \left(\sum_{i=1}^{n} h_{ik} \right) \left(\sum_{j=1}^{n} h_{jk} \right) \\ &= \sum_{k=1}^{n} s_k \cdot s_k = \sum_{k=1}^{n} s_k^2. \end{aligned}$$

Consequently,

$$\sum_{k=1}^{n} s_k^2 = n^2.$$

Using the Cauchy-Schwartz inequality $\left(\sum_{k=1}^{n} x_k y_k\right)^2 \leq \left(\sum_{k=1}^{n} x_k^2\right) \cdot \left(\sum_{k=1}^{n} y_k^2\right)$ where $x_1, \ldots, x_n$, $y_1, \ldots, y_n$ are real numbers, it follows that

$$\left(\sum_{k=1}^{n} x_k \cdot s_k\right)^2 \leq \left(\sum_{k=1}^{n} x_k^2\right) \cdot \left(\sum_{k=1}^{n} s_k^2\right).$$

If $x_k = 1 : k \in \{1, \ldots, n\}$, then the equation simplifies to

$$\left(\sum_{k=1}^{n} s_k\right)^2 \leq n \cdot \left(\sum_{k=1}^{n} s_k^2\right).$$

Therefore,

$$n^2 = \sum_{k=1}^{n} s_k^2 \geq \frac{\left(\sum_{k=1}^{n} s_k\right)^2}{n}$$

and using 5.8 shows that $\sigma(n) \leq n^{3/2}$. □

Proposition 5.51. *Let H be a Hadamard matrix of order $n = 4m$. Then $\sigma(4m) = \sigma(n) = n^{3/2} = 8m^{3/2}$ if and only if H is regular.*

Proof. Let h denote the constant number of ones in a row (column), then $h = \frac{n \pm \sqrt{n}}{2}$. This was shown in the proof of theorem 5.41. W.l.o.g., it can be assumed that $h = \frac{n+\sqrt{n}}{2}$ (as it is the dual design), then $-H$ has $n - \frac{n+\sqrt{n}}{2} = \frac{n-\sqrt{n}}{2}$ ones in every row (column). Hence the regular Hadamard matrix H has excess

$$n\left(\frac{n+\sqrt{n}}{2} - \frac{n-\sqrt{n}}{2}\right) = n^{3/2}.$$

To prove the necessary condition, it is used that equality occurs in the Cauchy-Schwarz inequality if and only if $\frac{y_1}{x_1} = \cdots = \frac{y_k}{x_k}$. Consequently,

$$\left(\sum_{k=1}^{n} s_k\right)^2 = n \cdot \left(\sum_{k=1}^{n} s_k^2\right) \Leftrightarrow s_1 = \cdots = s_k.$$

As a result H has regular columns and from corollary 5.44 it follows that H is regular. □

To summarize proposition 5.51 and corollary 5.43:

Corollary 5.52. *The following three conditions are equivalent:*

(1) *There exists a regular Hadamard matrix of order $4m$.*
(2) *There exists a Hadamard matrix of order $4m$ with maximum excess $8m^{3/2}$.*
(3) *There exits a SBIBD with parameters $(4m, 2m \pm \sqrt{m}, m \pm \sqrt{m})$.*

5.4. **Group-developed Hadamard matrices**

In the beginning of this chapter group-developed matrices are defined and then their equivalence to a difference set is proved. See [8] and [22].

Definition 5.53. *Let $(G, \cdot)$ be a group of order v with a fixed order $\{g_1, g_2, \ldots, g_v\}$ and S a set. Index the entries of a matrix H with entries from S by the elements of G, then $H = (h_{i,j})$ is group developed over G or G-developed if a map $\phi : G \to S$ exists such that $h_{i,j} = h_{g_i,g_j} = \phi(g_i g_j)$. A G-developed matrix induced by ϕ is denoted by*

$$[\phi(g_i g_j)]_{1 \leq i,j \leq v}.$$

A group-invariant or G-invariant has the entry $\phi(g_i g_j^{-1})$ for $1 \leq i, j \leq v$.

Schmidt [22] defines a group-invariant as:

Definition 5.54. *If G is a group of order n and $H = (h_{a,b})_{a,b \in G}$ a matrix indexed by elements of G, then H is group-invariant or G-invariant if $h_{ac,bc} = h_{a,b}$ for all $a, b, c \in G$.*

It is easy to see that these definitions are equivalent, but it is also proved in the next lemma. A matrix is called group-developed and also group-invariant as it can be constructed from one single row (or column). This is clear observing definition 5.54. Let H be a group-developed matrix defined by 5.53 and $g \in G$ a fixed element, then the row $[\phi(gg_i)]_{1 \leq i \leq v}$ indexed by g can be obtained by the row $[\phi(g_i)]_{1 \leq i \leq v}$ indexed by the unit element 1.

Lemma 5.55. *There is an equivalence between the two definitions 5.53 and 5.54 of group invariant matrices.*

Proof. Let $H = h_{i,j} = h_{g_i,g_j} = \phi(g_i g_j)$ be group-invariant as defined in 5.53. Then,

$$h_{ik,jk} = h_{g_i g_k, g_j g_k} = \phi(g_i g_k (g_j g_k)^{-1}) = \phi(g_i g_j^{-1}) = h_{i,j}.$$

On the other hand, let $H = (h_{a,b})_{a,b \in G}$ be a group-invariant matrix as defined in 5.54 and S the set of entries of H. There is per definition 5.54 a special order of the elements (that order is already set by the first row). Let $\phi : G \to S$ be a map determined by the first row of H. Then,

$$h_{ac,bc} = h_{a,b} \Leftrightarrow \phi(acbc) = \phi(ab) : \forall a, b, c \in G.$$

If $c = b^{-1}$ in the equation above, then $\phi(ab^{-1}) = \phi(ab)$. □

Lemma 5.56. *Let H be a G-developed matrix as defined in 5.53 with entries in an ablian group $(S, +)$, then H has constant row sum and column sum.*

Proof. The lemma follows from the fact that a group-developed matrix can be constructed from one row (column). Therefore, the row (column) sum of each row (column) is always the same sum with a different order of the summands. Hence, these sums are equal if and only if S is abelian. □

Corollary 5.42 shows that a regular Hadamard matrix exists only if the order is a perfect square. Therefore a Hadamard matrix can only be group-developed if its order is a perfect square. But as group-developed matrices are defined more generally, a more general statement is true.

Corollary 5.57. *Let $W = W(m, n)$ be a G-developed weighing matrix (defined in chapter 3 with entries only ± 1), then $n = s^2$ for some integer s. The number of entries 1s in each row (column) is $s(s+1)/2$.*

Proof. Recall that $WW^T = nI_m$. On the one hand, $(WW^T)J$ can be easily computed by $(WW^T)J = (nI)J = nJ$. On the other hand, let s be the sum of all entries in each row (column), then $(WW^T)J = W(W^TJ) = WsJ = s(WJ) = s^2J$. Hence $n = s^2$ and $s = s_1 - (s^2 - s_1)$, where s_1 is the number of 1s in a row (column). □

Example. *An example of a group-developed Hadamard matrix will be given in the cyclic group $(\mathbb{Z}_4, +)$. Hence, the $\mathbb{Z}_4$-developed matrices have to be circulant, too. For instance, define $\phi(0) = \phi(1) = \phi(2) = -1$ and $\phi(3) = 1$. The table of the group and the group-developed matrix is*

$+$	*0*	*1*	*2*	*3*
0	*0*	*1*	*2*	*3*
1	*1*	*2*	*3*	*0*
2	*2*	*3*	*0*	*1*
3	*3*	*0*	*1*	*2*

$$\overset{\phi}{\to} \begin{pmatrix} -1 & -1 & -1 & 1 \\ -1 & -1 & 1 & -1 \\ -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & -1 \end{pmatrix}.$$

This matrix is back-circulant, but it is not group-invariant as $\phi(3) = \phi(0+3) \neq \phi(0+1) = \phi(1)$, whereas the following matrix is $\mathbb{Z}_4$ - invariant and circulant:

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

Remark. *To find group-developed matrices the natural approach would be to search in the cyclic group $\mathbb{Z}/4u^2\mathbb{Z} = \mathbb{Z}_{4u^2}$ with u an integer, but the only example of a group-developed matrix over the cyclic groups $\mathbb{Z}_{4u^2}$ that was ever found, is the example above with $u = 1$. In fact, this strongly supports the Ryser Conjecture 2.11. Schmidt showed in* [26] *with the help of algebraic number theory, that there is no circulant Hadamard matrix of order $4u^2 = v \leq 10^{11}, v \neq 4$ with the possible exceptions of $u \in \{164, 11715, 82005\}$.*

Group-developed (and hence regular) Hadamard matrices have a combinatorical construction. In [9], Horadam showed the next theorem.

Theorem 5.58. *Let G be a group of order $v = 4u^2$ and $\phi : G \to \{\pm 1\}$ a set map. Let H be a G-developed matrix as defined in 5.53, then H is Hadamard if and only if $\{g \in G : \phi(g) = -1\}$ is a $(4u^2, 2u^2 \pm u, u^2 \pm u)$ difference set in G.*

Definition 5.59. *Difference sets with the parameters $(4u^2, 2u^2 \pm u, u^2 \pm u)$ are called Menon difference sets or Menon-Hadamard difference sets.*

We will prove the equivalence between group-invariant matrices and Menon-Hadamard difference sets. Before the equivalence can be proved, some basic definitions from homological algebra will be revised.

Definition 5.60. *Let G be a group, then the (left) G-module is a pair (A, ε) where A is an abelian group and $\varepsilon : G \to Aut(A)^{op}$ a homomorphism.*

Remark. *$Aut(A)^{op}$ is chosen in the definition above as the left group action is standard, but in the automorphism group usually right multiplication is used. Denote a category by $\mathcal{C}$, then switching in the opposite category $\mathcal{C}^{op}$ solves the problem .*

Lemma 5.61. *The G-module (A, ε) defined in 5.60 is indeed a (classically defined) G-module.*

Proof. Let $g \in G$ and $a \in A$, then the expression $\varepsilon_{(g)}(a)$ will be simplified to $g.(a)$ or $g.a$. Hence, ε induces a map $G \times A \to A, (g, a) \mapsto \varepsilon_g(a) = g.a$ and as ε is a homomorphism the following statements are true

(1) $g.(a + b) = g.a + g.b : \forall g \in G : \forall a, b \in A$,
(2) $1.a = a : \forall a \in A$,
(3) $(gh).a = g.(h.a) : \forall g, h \in G : \forall a \in A$.

Therefore, A is a (classically defined) G-module. □

The question rises if there exists a ring R, such that a $G-$module is a R-module. The answer is given by the following definition and the next lemma.

Definition 5.62. *Let $(G, +)$ be an abelian group, then the group ring $\mathbb{Z}[G]$ is defined as the formal sums*

$$a = a(x) = \sum_{g \in G} a_g x^g,$$

where $a_g \in \mathbb{Z}$ are the coefficients with $a_g = 0$ for all, but finitely many g and x is an indeterminante. Let $\mathbb{Z}[G] \ni a = \sum_{g \in G} a_g x^g$ and $\mathbb{Z}[G] \ni b = \sum_{g \in G} b_g x^g$, then the sum and the product can be defined as

$$a + b = a(x) + b(x) = \sum_{g \in G} (a_g + b_g) x^g \text{ and } a \cdot b = a(x) \cdot b(x) = \sum_{g \in G} \sum_{h \in G} (a_g b_h) x^{g+h}.$$

With these operations $\mathbb{Z}[G]$ is clearly a commutative ring, where the additive unit element is $0 = \sum_{g \in G} 0 \cdot x^g$ and the unit element of multiplication is $1 = 1 \cdot x^0 + \sum_{g \neq 0} 0 \cdot x^g$.

Remark. *The operation of G is written additively as the multiplication of two elements of $\mathbb{Z}[G]$ looks quite familiar. Also in the definition of a difference set the group was written additive. Nevertheless, keep in mind that in the definition 5.53 the group was written multiplicatively. We will have to switch between the two notations, when required.*

Lemma 5.63. *(A, ε) is a G-module if and only if it is a $\mathbb{Z}[G]$-module.*

Proof. If (A, ε) is a G-module and $r = \sum_{g \in G} r_g x^g \in \mathbb{Z}[G]$, then set

$$r \cdot a = \left(\sum_{g \in G} r_g x^g \right) a = \sum_{g \in G} r_g (g.a) : \forall a \in A.$$

It is easy to verify that the module properties are fulfilled and therefore (A, ε) is a $\mathbb{Z}[G]$-module. On the other, the restriction of the scalar multiplication $\mathbb{Z}[G] \times A \to A$ on G induces a map $G \times A \to A$. Consequently, a $\mathbb{Z}[G]$-module is a G-module. □

Definition 5.64. *Some notations have to be defined. Let $(G, +)$ be an abelian group, $\mathbb{Z}[G]$ the group ring and $a(x) = \sum_{g \in G} a_g x^g \in \mathbb{Z}[G]$, then define*

$$a(x^m) = \sum_{g \in G} a_g x^{mg}, \qquad a(x^{-1}) = \sum_{g \in G} a_g x^{-g},$$
$$a(1) = \sum_{g \in G} a_g, \qquad G(x) = \sum_{g \in G} x^g.$$

Suppose that D is a difference set in G. Finally, define $D(x) = \sum_{g \in D} x^g$.

Lemma 5.65. *Let $(G, +)$ be an abelian group. D is (v, k, λ) difference set if and only if*

$$D(x)D(x^{-1}) = \lambda G(x) + (k - \lambda)x^0. \tag{5.9}$$

Proof. Taking a closer look at $D(x)D(x^{-1})$ shows that

$$D(x)D(x^{-1}) = \sum_{g,h \in D} x^{g-h} = \sum_{d \in D} \alpha_d x^d,$$

where $\alpha_d = |\{(g, h) \in D \times D : g - h = d\}|$. The definition of a difference set shows that

$$\alpha_d = \begin{cases} k & \text{if } d = 0 \\ \lambda & \text{if } d \neq 0 \end{cases} \Leftrightarrow D \text{ is a}(v, k, \lambda) \text{ difference set.}$$

Furthermore,

$$\alpha_d = \begin{cases} k & \text{if } d = 0 \\ \lambda & \text{if } d \neq 0 \end{cases} \Leftrightarrow \sum_{d \in D} \alpha_d x^d = \lambda G(x) - \lambda x^0 + k x^0.$$

□

Definition 5.66. *A G-invariant matrix $H = (h_{g,k})$ can be identified with the element $\sum_{g\in G} h_{1,g}x^g$ of $\mathbb{Z}[G]$. Therefore,*

$$H(x) = \sum_{g\in G} h_{1,g}x^g.$$

.

This definition makes sense as every group-invariant matrix can be constructed by its first row and therefore, it is completely determined by the first row. In addition, $H^T(x) = H(x^{-1})$, because if $H = (h_{a,b}) = (h_{1,b-a})$ is identified with $\sum_{g\in G} h_{1,g}x^g$, then $H^T = (h_{b,a}) = (h_{1,a-b})$ can be identified with $\sum_{g\in G} h_{1,g}x^{-g}$.

Lemma 5.67. *A matrix H is a G-invariant weighing matrix $W(m,n)$ if and only if*

$$H(x)H(x^{-1}) = n.$$

Proof. H is a G-invariant weighing matrix $W(m,n)$ if and only if the equation chain

$$\sum_{g\in G} h_{i,g}h_{j,g} = \sum_{g\in G} h_{1,i-g}h_{1,j-g} = \delta_{i,j}n$$

holds as $HH^T = nI_m$. Furthermore, $H(x)H(x^{-1}) = \sum_{g,k\in G} h_{1,g}h_{1,k}x^{g-k}$. Set $l = g - k$, then the sum changes to $\sum_{l\in G}\left(\sum_{g\in G} h_{1,g}h_{1,g-l}\right)x^l$. Hence, if H is a G-invariant weighing matrix, then $H(x)H(x^{-1}) = \sum_{l\in G} n\ \delta_{0,l}x^l = n$. In turn, if $H(x)H(x^{-1}) = n$ the equation above holds. □

Theorem 5.68. *A G-invariant Hadamard matrix of order $|G| > 1$ exists if and only if there is a Menon-Hadamard difference set in G.*

Proof. Let $(G,+)$ be an abelian group and H a G-invariant matrix, then by corollary 5.57 it can be assumed that $|G| = 4u^2$ for some integer u. Define

$$D_*(x) = (G(x) + H(x))/2.$$

Since $H(x)$ has only coefficients ± 1 and $G(x)$ has only coefficients 1, the coefficients of $D_*(x)$ can only be $0, 1$. Hence $D_*(x)$ determines a subset D of G. Note that H has $2u^2 \pm u$ ones in a row and therefore, its row sum is $\pm 2u$. Obviously, $G(x) = G(x^{-1})$. For a better understanding it is useful to show $a(x)G(x) = a(1)G(x) : \forall a(x) \in \mathbb{Z}[G]$.

$$\begin{aligned} a(x)G(x) &= \sum_{g,h\in G} a_g x^{g+h} \\ &= \sum_{i\in G}\left(\sum_{g\in G} a_g\right)x^i \quad \text{where } g+h=i \\ &= \sum_{i\in G} a(1)x^{g+h} = a(1)G(x) \end{aligned}$$

Hence using lemma 5.67 shows,

$$\begin{aligned} 4D_*(x)D_*(x^{-1}) &= H(x)H(x^{-1}) + H(x)G(x) + H(x^{-1})G(x) + G(x)G(x) \\ &= H(x)H(x^{-1}) + H(1)G(x) + H(1)G(x) + G(1)G(x) \\ &= 4u^2 + (\pm 2u \pm 2u + 4u^2)G(x). \end{aligned}$$

As a result, $D_*(x)D_*(x^{-1}) = u^2x^0 + (u^2 \pm u)G(x)$ and 5.65 shows that D is a Menon difference set. Conversely, lemmata 5.65 and 5.67 show that $H := 2D - G$ gives a Menon difference set. □

5.5. **Bent functions**

The existence of bent functions is, on the one hand, equivalent to the existence of a Hadamard matrix and on the other hand, equivalent to a special difference set. Furthermore, bent functions are important in the application of Hadamard matrices in cryptography, see [8]. The following can be reread in [26].

Definition 5.69. *A function $f : (\mathbb{Z}/2\mathbb{Z})^n = \mathbb{Z}_2^n \to \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2$ is called boolean of n variables. For every boolean function the vector of its values is denoted by $\psi(f)$. Note that the vector $\psi(f)$ has length 2^n and $\psi(f) \in (\mathbb{Z}_2)^{2^n}$. Let $\mathcal{B}_n$ be the set of boolean functions of n variables, then obviously $|\mathcal{B}_n| = 2^{2^n}$. Furthermore, define for every $f \in \mathcal{B}_n$ the function $(-1)^f : (\mathbb{Z}_2)^n \to \mathbb{Z}_2, ((-1)^f)(x) \mapsto (-1)^{f(x)}$. In other words, $(-1)^f$ replaces 0 by 1 and 1 by -1. For the inner product $< x, y >: x, y, \in (\mathbb{Z}_2)^n$ the short form $x \cdot y$ will be used. Finally, define the Fourier transform $\widehat{F}(x) = \sum_{y \in (\mathbb{Z}_2)^n} (-1)^{x \cdot y} F(y)$ of a function $F : (\mathbb{Z}_2)^n \to \mathbb{R}$.*

Lemma 5.70. *Let $y \in (\mathbb{Z}_2)^n$ and $\boldsymbol{0}$ the null vector, then the following equation holds:*

$$\sum_{x \in (\mathbb{Z}_2)^n} (-1)^{x \cdot y} = 2^n \delta_{y,\boldsymbol{0}}.$$

Proof. If $y \neq \mathbf{0}$, then the sum clearly contains the same number of ones and minus ones and is therefore zero. If $y = \mathbf{0}$, then obviously the sum is 2^n. □

In the following, let S^n be the Sylvester matrix defined by the equation 5.36. Note that S^n is symmetric by definition and hence $2^n I_n = S^n S^n = (S^n)^2$.

Lemma 5.71. *Let a real function F be defined on $(\mathbb{Z}_2)^n$, then $\psi(\widehat{F}) = \psi(F)S^n$.*

Proof. The equation follows directly from comparing the definition of the Fourier transform and the Sylvester matrix. □

Lemma 5.72. *Suppose that $F : \{0,1\}^n \to \mathbb{R}$. Then $\widehat{\widehat{F}} = 2^n F$.*

Proof.

$$\begin{aligned}
\psi(\widehat{F}) &= \psi(F)S^n \\
\psi(\widehat{F})S^n &= \psi(F)S^nS^n \\
\psi(\widehat{\widehat{F}}) &= \psi(F)2^nI_{2^n} \quad (S_n \text{ is Hadamard and symmetric and 5.71}) \\
\widehat{\widehat{F}} &= 2^nF.
\end{aligned}$$

□

Example. *Suppose that* $n = 2$ *and let* $f(x_1, x_2) = x_1x_2, F = (-1)^f$, *then* $\psi(f) = (f(0,0), f(0,1), f(1,0), f(1,1)) = (0,0,0,1)$ *and* $\psi(F) = (1,1,1,-1)$.

$$S_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \Rightarrow \psi(\widehat{F}) = (1,1,1,-1) \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = (2,2,2,-2).$$

Note that the absolute value of the Fourier transform $\widehat{F}(x)$ *is 2 for all* $x \in (\mathbb{Z}_2)^n$.

Theorem 5.73. *Suppose that* $f \in \mathcal{B}_n, F = (-1)^f, y \in (\mathbb{Z}_2)^n$, *then*

$$\sum_{x \in (\mathbb{Z}_2)^n} \widehat{F}(x)\widehat{F}(x+y) = \begin{cases} 2^{2n} & \text{if } y = \boldsymbol{0} \\ 0 & \text{if } y \neq \boldsymbol{0} \end{cases}.$$

Proof.

$$\begin{aligned}
\sum_{x \in (\mathbb{Z}_2)^n} \widehat{F}(x)\widehat{F}(x+y) &= \sum_{x \in (\mathbb{Z}_2)^n} \sum_{u \in (\mathbb{Z}_2)^n} (-1)^{x \cdot u} F(u) \left(\sum_{v \in (\mathbb{Z}_2)^n} (-1)^{(x+y) \cdot v} F(v) \right) \\
&= \sum_{x \in (\mathbb{Z}_2)^n} \sum_{u \in (\mathbb{Z}_2)^n} \sum_{v \in (\mathbb{Z}_2)^n} (-1)^{x \cdot u + (x+y) \cdot v} F(u)F(v) \\
&= \sum_{u \in (\mathbb{Z}_n)^n} \sum_{v \in (\mathbb{Z}_2)^n} (-1)^{y \cdot v} F(u)F(v) \left(\sum_{x \in (\mathbb{Z}_2)^n} (-1)^{x \cdot (u+v)} \right).
\end{aligned}$$

From lemma 5.70 it follows that the sum $\sum_{x \in (\mathbb{Z}_2)^n} (-1)^{x \cdot (u+v)}$ is $2^n\delta_{u+v,\mathbf{0}}$, but $\delta_{u+v,\mathbf{0}} = \delta_{u,-v} = \delta_{u,v}$ as $u, v \in (\mathbb{Z}_2)^n$. Note, that it has not been used yet that $F = (-1)^f$, hence the simplification

$$\sum_{x \in (\mathbb{Z}_2)^n} \widehat{F}(x)\widehat{F}(x+y) = \sum_{u \in (\mathbb{Z}_n)^n} \sum_{v \in (\mathbb{Z}_2)^n} (-1)^{y \cdot v} F(u)F(v)2^n\delta_{u,v} = 2^n \sum_{u \in (\mathbb{Z}_n)^n} (-1)^{y \cdot v} F(u)^2$$

holds for any real valued function F defined on $(\mathbb{Z}_2)^n$. Now, it is used that $F = (-1)^f$ can only have values ± 1, therefore $F(u)^2 = 1$.

$$\sum_{x\in(\mathbb{Z}_2)^n} \widehat{F}(x)\widehat{F}(x+y) = 2^n \sum_{u\in(\mathbb{Z}_n)^n} (-1)^{y\cdot v} \overset{5.70}{=} 2^n \cdot 2^n \delta_{y,\mathbf{0}} = 2^{2n}\delta_{y,\mathbf{0}}.$$

□

In the proof of the last theorem it was already stressed that most of the proof is true for a general F.

Corollary 5.74. *Let $F : (\mathbb{Z}_2)^n \to \mathbb{R}$ and $y \in (\mathbb{Z}_2)^n$, then the equation*

$$\sum_{x\in(\mathbb{Z}_2)^n} \widehat{F}(x)\widehat{F}(x+y) = 2^n \sum_{u\in(\mathbb{Z}_n)^n} (-1)^{y\cdot v} F(u)^2$$

holds.

Corollary 5.75 (Parseval's Equation)**.** *Suppose that $f \in \mathcal{B}_n$ and $F = (-1)^f$, then*

$$\sum_{x\in(\mathbb{Z}_2)^n} \left(\widehat{F}(x)\right)^2 = 2^{2n}.$$

Proof. Special case of theorem 5.73 ($y = \mathbf{0}$). □

Definition 5.76. *Let $f, g \in \mathcal{B}_n$, then the distance between f and g is defined as*

$$d(f,g) = |\{x \in (\mathbb{Z}_2)^n : f(x) \neq g(x)\}|.$$

A boolean function f is linear if $\exists a \in (\mathbb{Z}_2)^n$ such that $f(x) = L_a = a \cdot x : \forall x \in (\mathbb{Z}_2)^n$. f is an affine function if $\exists a \in (\mathbb{Z}_2)^n$ such that $f = L_a$ or $f = L_a + 1$.

The number of linear boolean functions in $\mathcal{B}_n$ is obviously 2^n and the number of affine functions is $2^n + 2^n = 2^{n+1}$. The distance of two function f, g is equivalent to the Hamming distance between the vectors $\phi(f)$ and $\phi(g)$.

Theorem 5.77. *Suppose that $f \in (\mathbb{Z}_2)^n$ and $F = (-1)^f$. Let $a \in (\mathbb{Z}_2)^n$. Then*

$$d(f, L_a) = 2^{n-1} - \frac{1}{2}\widehat{F}(a) \text{ and } d(f, L_a + 1) = 2^{n-1} + \frac{1}{2}\widehat{F}(a).$$

Proof.

$$\begin{aligned}
\widehat{F}(a) &= \sum_{y\in(\mathbb{Z}_2)^n} (-1)^{a\cdot y}(-1)^{f(y)} = \sum_{y\in(\mathbb{Z}_2)^n} (-1)^{a\cdot y + f(y)} \\
&= \underbrace{|\{y \in (\mathbb{Z}_2)^n : a \cdot y = f(y)\}|}_{|\{y\in(\mathbb{Z}_2)^n\}| - |\{y\in(\mathbb{Z}_2)^n : a\cdot y \neq f(y)\}|} - |\{y \in (\mathbb{Z}_2)^n : a \cdot y \neq f(y)\}| \\
&= 2^n - 2|\{y \in (\mathbb{Z}_2)^n : a \cdot y \neq f(y)\}| \\
&= 2^n - 2d(f, L_a)
\end{aligned}$$

$\Rightarrow d(f, L_a) = 2^{n-1} - \frac{1}{2}\widehat{F}(a)$.
The other equation follows from the fact that $f(y) = a \cdot y + 1 \Leftrightarrow f(y) \neq a \cdot y$ and hence,

$$d(f, L_a + 1) = 2^n - d(f, L_a).$$

□

Definition 5.78. *The nonlinearity of a boolean function f, denoted by N_f, is defined as $N_f = \min\{d(f, L_a), d(f, L_a + 1) : a \in (\mathbb{Z}_2)^n\}$. f is a bent function if $|\widehat{F}(x)| = 2^{n/2} : \forall x \in (\mathbb{Z}_2)^n$ and $F = (-1)^f$.*

A bent function can only exist if n is even, because $\widehat{F}(x)$ is always an integer. In the example given before, f is clearly bent.

From theorem 5.77 it follows that:

Corollary 5.79. $N_f = 2^{n-1} - \frac{1}{2}\max\{|\widehat{F}(a)| : a \in (\mathbb{Z}_2)^n\}$.

Proposition 5.80. *Let $f \in \mathcal{B}_n$, then $N_f \leq 2^{n-1} - 2^{n/2-1}$ and equality holds if and only if f is a bent function.*

Proof. Define $M = \max\{|\widehat{F}(a)| : y \in (\mathbb{Z}_2)^n\}$ then from corollary 5.79 it follows that, $N_f = 2^{n-1} - M/2$. The Parseval's equation will be used next.

$$2^{2n} = \sum_{x \in (\mathbb{Z}_2)^n} (\widehat{F}(x))^2 \leq \sum_{x \in (\mathbb{Z}_2)^n} M^2 = 2^n M^2$$

$\Rightarrow M \geq 2^{n/2}$ and $M = 2^{n/2} \Leftrightarrow |\widehat{F}(x)| = 2^{n/2}$ for all $x \in (\mathbb{Z}_2)^n$. □

In the following, the equivalence between bent functions and Hadamard matrices will be proved.

Theorem 5.81. *Let $f \in \mathcal{B}_n$ and $F = (-1)^f$. Define $H_f = (h_{x,y}) = (F(x + y)) : \forall x, y \in (\mathbb{Z}_2)^n$ where the elements of $(\mathbb{Z}_2^n)$ are lexicographically ordered. Then H_f is Hadamard if and only if f is a bent function.*

Proof. For the necessary condition, suppose that f is bent and define $G = \frac{1}{2^{n/2}}\widehat{F}$. Using Lemma 5.72, then the Fourier transform of G is $\widehat{G} = \frac{1}{2^{n/2}}\widehat{\widehat{F}} = \frac{1}{2^{n/2}}2^n F = 2^{n/2}F$.

$$\begin{aligned}
\sum_{z \in (\mathbb{Z}_2)^n} h_{x,z} h_{y,z} &= \sum_{z \in (\mathbb{Z}_2)^n} F(x + z)F(y + z) \\
&= \sum_{w \in (\mathbb{Z}_2)^n} F(w)F(x + y + w) \\
&= \frac{1}{2^{n/2}} \cdot \frac{1}{2^{n/2}} \sum_{w \in (\mathbb{Z}_2)^n} \widehat{G}(w)\widehat{G}(x + y + w)
\end{aligned}$$

In the last step it is used that $F = \frac{1}{2^{n/2}}\widehat{G}$. Note that there has to be a function $g \in \mathcal{B}_n$ such that $(-1)^g = G$ as f is bent and therefore theorem 5.73 can be used to show that

$$\sum_{z\in(\mathbb{Z}_2)^n} h_{x,z}h_{y,z} = \frac{1}{2^n}2^{2n}\delta_{x+y,\mathbf{0}} = 2^n\delta_{x,y}.$$

Hence, H_f is Hadamard.
Conversely, suppose that H_f is Hadamard and define again the real valued function $G = \frac{1}{2^{n/2}}\widehat{F}$. As H_f is Hadamard, the equation $2^n\delta_{x,y} = \sum_{z\in(\mathbb{Z}_2)^n} h_{x,z}h_{y,z} : \forall x, y \in (\mathbb{Z}_2)^n$ holds. Choose $y = \mathbf{0}$. Therefore,

$$\begin{aligned}
2^n\delta_{x,\mathbf{0}} &= \sum_{z\in(\mathbb{Z}_2)^n} h_{x,z}h_{\mathbf{0},z} \\
&= \sum_{z\in(\mathbb{Z}_2)^n} F(x+z)F(z) \\
&= \frac{1}{2^{n/2}}\frac{1}{2^{n/2}} \sum_{z\in(\mathbb{Z}_2)^n} \widehat{G}(z)\widehat{G}(x+z) \\
&= \sum_{z\in(\mathbb{Z}_2)^n} (-1)^{x\cdot z}G(z)^2 && \text{Corollary 5.74} \\
&= \frac{1}{2^n} \sum_{z\in(\mathbb{Z}_2)^n} (-1)^{x\cdot z}(\widehat{F}(z))^2.
\end{aligned}$$

$\Rightarrow 2^{2n}\delta_{x,\mathbf{0}} = \sum_{z\in(\mathbb{Z}_2)^n}(-1)^{x\cdot z}(\widehat{F}(z))^2$
$\delta_{x,\mathbf{0}} \neq 0 \Leftrightarrow x = \mathbf{0} \Leftrightarrow \delta_{x,\mathbf{0}} = 1$
Furthermore, using lemma 5.36 it is possible to obtain that (Now it is used that $(\mathbb{Z}_2)^n$ is ordered lexographically)

$$\begin{aligned}
2^{2n}(1,0,\ldots,0) &= \psi(\widehat{F}(z)^2)S^n \\
2^{2n}(1,0,\ldots,0)S_n &= \psi(\widehat{F}(z)^2)S^nS^n \\
2^{2n}(1,1,\ldots,1) &= 2^n\psi(\widehat{F}(z)^2) \\
2^n(1,1,\ldots,1) &= \psi(\widehat{F}(z)^2).
\end{aligned}$$

$|\widehat{F}(z)| = 2^{n/2} : \forall z \in (\mathbb{Z}_2)^n \Rightarrow f$ is bent. □

The next theorem will show the equivalence between bent functions and difference sets.

Theorem 5.82. *The existence of a bent function $f : (\mathbb{Z}_2)^n \to \mathbb{Z}_2$ is equivalent to the existence of a $(2^n, 2^{n-1} \pm 2^{(n-2)/2}, 2^{n-2} \pm 2^{(n-2)/2})$ difference set in $(\mathbb{Z}_2)^n$.*

Proof. First, suppose that f is bent, then H_f is a Hadamard matrix by 5.81. H_f is regular, as every row is a permutation of the values $F(x) : x \in (\mathbb{Z}_2)^n$. H_f is a Hadamard matrix of order 2^n. Using theorem 5.41 with $4u^2 = 2^n \Rightarrow u = 2^{(n-2)/2}$, H_f is equivalent to a $(2^n, 2^{n-1} \pm 2^{(n-2)/2}, 2^{n-2} \pm 2^{(n-2)/2})-$SBIBD. It will be shown that $(\mathbb{Z}_2)^n$ is a sharply transitive automorphism group of H_f and therefore of the design induced by H_f. Let

$w \in (\mathbb{Z}_2)^n$, then define $t_w : (\mathbb{Z}_2)^n \to (\mathbb{Z}_2)^n, x \mapsto x + w$. It is clear that t_w is a bijection and hence a permutation for all $w \in (\mathbb{Z}_2)^n$. Consider the set

$$T = \{t_w : w \in (\mathbb{Z}_2)^n\},$$

then $|T| = 2^n$ and as a consequence T is sharply transitive. In addition, every t_w is an automorphism of H_f, because

$$h_{t_w(x),t_w(y)} = h_{w+x,w+y} = F(w + x + w + y) = F(x + y) = h_{x,y}.$$

From theorem 5.29 follows that a $(2^n, 2^{n-1} \pm 2^{(n-2)/2}, 2^{n-2} \pm 2^{(n-2)/2})$ difference set exists in $(\mathbb{Z}_2)^n$.
From the existence of a $(2^n, 2^{n-1} \pm 2^{(n-2)/2}, 2^{n-2} \pm 2^{(n-2)/2})$ difference set follows the existence of a $(2^n, 2^{n-1} \pm 2^{(n-2)/2}, 2^{n-2} \pm 2^{(n-2)/2})-$SBIBD with $(\mathbb{Z}_2)^n$ a sharply transitive group. From theorem 5.41 it follows that the Hadamard matrix of order 2^n induced by the symmetric block design is a regular matrix with $(\mathbb{Z}_2)^n$ as a sharply transitive automorphism group. By the definition of a sharply transitive group, the equation

$$h_{u+x,u+y} = h_{x,y}$$

holds $\forall u, x, y \in (\mathbb{Z}_2)^n$. Furthermore, define the boolean function f as

$$f(x) = \begin{cases} 0 & \text{if } h_{x,\mathbf{0}} = 1 \\ 1 & \text{if } h_{x,\mathbf{0}} = -1 \end{cases}.$$

Hence,

$$h_{x,y} = h_{x+y,y+y} = h_{x+y,\mathbf{0}} = (-1)^{f(x+y)} : \forall x, y \in (\mathbb{Z}_2)^n.$$

In summary, it is shown that $h_{x,y} = F(x+y)$, where $F = (-1)^f$. Theorem 5.81 completes the proof. □

Corollary 5.83. *Let $f \in \mathcal{B}_n$. Then the following three statements are equivalent.*

(1) *f is bent.*
(2) *The $(\mathbb{Z}_2)^n$-developed matrix $[(-1)^{f(u+v)}]$ is a Menon Hadamard matrix.*
(3) *There exists a Menon difference set with parameters $(2^n, 2^{n-1} \pm 2^{(n-2)/2}, 2^{n-2} \pm 2^{(n-2)/2})$. These difference sets are called elementary Hadamard difference sets.*

Proof. These equivalences follow from theorem 5.82, 5.81 and 5.58. □

Remark. *It is not hard to see that for every $n = 2m$ the a boolean function*

$$f(x_1, x_2, \ldots, x_{2m}) = x_1x_2 + x_3x_4 + \ldots, x_{2m-1}x_{2m} \mod 2$$

is bent.

6. Cocyclic Hadamard matrices

"To date, cocyclic construction of Hadamard matrices is the most successful uniform technique known."([29], p. 114)

The cocyclic construction of matrices is based on ideas of group cohomology. To give a proper explanation of this construction would exceed this work by far, but an introduction and the link between the constructions that were already explained, is provided. Padraig O Cathain, who is now a reseacher on the field of cocyclic matrices, focused only on cocyclic Hadamard matrices in his master thesis and described in detail the theory which mostly K. Horadam, W. de Launey and D. Flannery developed in the last 20 years. The next chapter is mostly based on [14], [8]. For a basic introduction in cohomology [21] can be recommended.

In the next definition the term G-module will be used again. Recall definition 5.60.

Definition 6.1. *Let (A, ε) be a G-modul. For $n \geq 0$, define $C^n(G, A)$ as the set of n-cochains which are the functions $f : G^n \to A, f(x_1, \ldots, x_n) = 0$ if $x_i = 1$ for some i. Define $C^0 \cong \{0\}$.*

Note that $C^n(G, A)$ is an abelian group with the group operation given by pointwise addition, as A is abelian.

To obtain a cochain complex, the bar resolution $\partial_n(f) : C^n(G, A) \to C^{n+1}(G, A)$ is used. It is defined by

$$\partial_n(f)(x_1, \ldots, x_{n+1}) = x_1.f(x_2, \ldots, x_{n+1}) + \sum_{i=1}^{n}(-1)^i f(x_1, \ldots, x_{i-1}, x_i x_{i+1}, \ldots, x_{n+1}) + (-1)^{n+1} f(x_1, \ldots, x_n).$$

Hence,

$$\cdots \leftarrow^{\partial_3} C^3(G, A) \leftarrow^{\partial_2} C^2(G, A) \leftarrow^{\partial_1} C^1(G, A) \leftarrow^{\partial_0} \{0\}$$

is a complex, therefore $\partial_n \circ \partial_{n-1} = 0$. These maps are called coboundaries. Furthermore, define $Z^n_\varepsilon(G, A) = kernel(\partial_n)$, $B^n_\varepsilon(G, A) = im(\partial_{n-1})$ and $H^n_\varepsilon(G, A) = Z^n_\varepsilon(G, A)/B^n_\varepsilon(G, A)$. $Z^n_\varepsilon(G, A)$ is the additive group of cocycles and $B^n_\varepsilon(G, A)$ is the addtive group of coboundaries. $H^n_\varepsilon(G, A) = Z^n_\varepsilon(G, A)/B^n_\varepsilon(G, A)$ is the n^{th}-cohomology group.

Examples. (1) $n = 0$

A 0-cochain is a function $\{0\} = G^0 \to A$ and therefore just a constant $a \in A$. The 1-coboundary is the map

$$\partial_0 : G \to A : g \mapsto g.a - a.$$

As a result the 0-cocycles are the elements of $a \in A$ that are fixed by g. If G acts trivial on A then, $\partial_0 = 0$ and the 0-cocycles are all the elements of A.

(2) $n = 1$

A 1-cochain is a function $f : G \to A$ with $f(1) = 0$ and its 2-coboundary is the map

$$\partial_1(f) : G \times G \to A, (g, h) \mapsto g.f(h) - f(gh) + f(g).$$

The 1-cocycles are the functions $f^* : G \to A$ that satisfy $0 = g.f^*(h) - f^*(gh) + f^*(g)$. If G acts trivial on A, then the 1-cocycles are the homomorphisms $G \to A$. It is obvious that every 1-coboundary is a 1-cocycle.

(3) $n = 2$

A 2-cochain is a function $f : G \times G \to A$. Its 3-coboundary is

$$\partial_3(f) : G^3 \to A, (g, h, k) \mapsto g.f(h, k) - f(gh, k) + f(g, hk) - f(g, h).$$

The 2-cocycles are the functions $f^* : G \times G \to A$ with $f(gh, k) + f(g, h) = g.f(h, k) + f(g, hk)$ for $g, h, k \in G$.

For the rest of this chapter the group G will act trivial ($\varepsilon = 1$) on the G-modul A. It is easy to check that f is a cochain if and only $-f$ is a cochain. So, w.l.o.g. this change is made. In addition, only 2-coboundaries and 2-cocycles will be interesting. From now on, A will be written multiplicatively and denoted by C. Finally, **the** definition for cocycles and coboundaries is given that will be used to construct Hadamard matrices.

Definition 6.2. *Let $(C, \varepsilon = 1)$ be a G-modul. Then a normalised cocycle is a map $\psi : G \times G \to C$ and the equations*

$$\psi(gh, k) + \psi(g, h) = \psi(h, k) + \psi(g, hk) \text{ and } \psi(g, 1) = 1 = \psi(1, g)$$

hold for $g, h, k \in G$.
Let $\phi : G \to C$ be a 1-cochain, then the coboundary $\partial\phi$ is a cocycle of the form $\partial\phi(g, h) = \phi(g)^{-1}(\phi(h))^{-1}\phi(gh)$.

Definition 6.3. *Let G be a finite group of order v and C be an abelian group. A $v \times v$ matrix with entries in C is a $G-$cocycle matrix over C if there are a cocycle $\psi \in Z^2(G, C)$ and an ordering of G such that M is equivalent in the sense of 3.1 to the normalised matrix*

$$M_\psi = [\psi(g_i, g_j)]_{1 \le i,j \le v}.$$

In the end, nearly all Hadamard matrices constructed until now are cocycle.

6.0.1. Menon difference sets/Group-developed matrix

Using the definition of a 1-cochain $\phi : G \to C$, it is easy to see that $[\phi(g_i, g_j)]_{1 \le i,j \le v}$ is a group-developed matrix over C. Its normalisation has the entries $\phi(g_i)^{-1}\phi(g_j)^{-1}\phi(g_i g_j) : \forall 1 \le i, j \le v$. Hence, the entries of the normalised group-developed matrix takes the same value as the coboundary $\partial\phi(g_i, g_j)$. If $\phi(1) = 1$, then

$$\partial\phi(1, h) = \partial\phi(g, 1) = 1.$$

Hence, the coboundary is a cocycle and if G is finite then $M_{\partial\phi}$ is the normalised version of a group-developed matrix.

6.0.2. Syvlvester matrices/Singer difference sets

Let $G = ((\mathbb{Z}_2)^n, +)$ and $C = \{\pm 1\} \cong (\mathbb{Z}_2, +)$, then G is obviously finite. The vector product is a cocycle ψ, where $\psi(u, v) = (-1)^{<u,v>}$ as defined in Chaper 5.2, because

$$\begin{aligned} &(-1)^{<u,v>} + (-1)^{<u+v,z>} - (-1)^{<v,z>} - (-1)^{<u,v+z>} \\ = &(-1)^{<u,v>} + (-1)^{<u,z>} + (-1)^{<v,z>} - (-1)^{<v,z>} - (-1)^{<u,v>} - (-1)^{<u,z>} \\ &= 0 : \forall u, v, z \in (\mathbb{Z}_2)^n. \end{aligned}$$

Note that $(-1)^{<a,b>+<a,c>} = (-1)^{<a,b>} + (-1)^{<a,c>} : \forall a, b, c \in (\mathbb{Z}_2)^n$ follows from the fact that $< a, b >$ can only be ± 1. Furthermore, $\psi(\mathbf{0}, v) = \psi(u, \mathbf{0}) = -1$. As a result, Sylvester matrices are cocycle matrices.

6.0.3. Paley Type II matrices/Williamson matrices

In [15] it is proved that Williamson matrices are $\mathbb{Z}_t \times (\mathbb{Z}_2)^2$-cocyclic.

6.0.4. Paley Type II matrices

The fact that Paley Type II matrices are cocyclic is shown by using that the automorphism group of these matrices is fully described [12], [16].

Every Hadamard matrix of order ≤ 20 is cocycle. This can be reread in detail in the master thesis of Padraig O Cathain. It was already shown that:

Theorem 6.4. *A cocycle Hadamard matrix is known for $4t \leq 200$ except $t = 47$.*

Hence, the following unsolved question rises:

Conjecture 6.5. *There is a cocycle Hadamard matrix for every multiple of 4.*

Nevertheless, one construction was not showed to be cocyclic and this problem is still open, too.

Conjecture 6.6. *Is the Goethals-Seidl Hadamard matrix cocyclic?*

References

[1] Beth, Th.; Jungnickel D. and Lenz, H.: Design Theory. BI- Wiss.- Verlag, Mannheim, 1985.

[2] Brouwer, A. E.; Cohen, A. M. and Neumaier, A.: Distance-regular Graphs. Springer Verlag, Berlin, 1989.

[3] Gockenbach, M.: Finite-Dimensional Linear Algebra. CRC Press, Boca Raton, 2011.

[4] Goethals, J. M. and Seidel, J.J: A skew Hadamard matrix of order 36. Journal of the Australian Mathematical Society Journal, 1970: 11 p. 343–344.

[5] Gordon, B.; Mills, W. H. and Welch, L. R.: Some new difference set. Canadian Journal of Mathematics, 1962: 9 p. 614-625.

[6] Hadamard, J.S.: Resolution d'une question relative aux déterminants. Bulletin des Sciences Mathématiques, 1893: 17 p. 240–246.

[7] Hedayat, A.S.; Sloane, N.J.A. and Stufken, J.: Orthogonal arrays. Springer, New York, 1999.

[8] Horadam, K.J.: Hadamard Matrices and their Application. Princeton University Press, Princeton, 2007.

[9] Horadam, K. J.: Progress in cocyclic matrices. Congr. Numer. 118, 1996: p. 161-171.

[10] Ionin, Y. J. and Shrikhande M. S.: Combinatorics of symmetric designs. Cambridge University Press, Cambridge; New York, 2006.

[11] Jungnickel, D.: Finite Fields: structure and arithmetics. BI-Wiss.-Verlag, Mannheim, 1993.

[12] Kantor, W.M.: Automorphism groups of Hadamard matrices. J. Combinatorical Theory, 1969: A 6 p. 279-281.

[13] Kounias, S. and Farmakis, N.: On the excess of Hadamard matrices. Discrete Mathematics Volume, 1988: 68 p. 59-69.

[14] Launey, de W. and Flannery, D.: Algebraic Design Theory. American Mathematical Society, Providence, 2011.

[15] Launey, de. W.; Flannery, D.L. and Horadam, K.J.: Cocyclic Hadamard matrices and difference sets. Discrete Applied Mathematics, 2000: 102 p. 47-61.

[16] Launey, de W. and Stafford, R. M.: On the automorphisms of Paley's Type II Hadamard matrix. Discrete Mathematics Volume, 2008: 308 p. 2910–2924.

[17] Launey, de W. and Gordon D. M.: Survey of the Hadamard Conjecture. J. Comb. Theory, 2001: Ser. A 95(1) p. 180-184.

[18] Lidl, R. and Niederreiter, H.: Introduction to finite fields and their applications. Cambridge University Press, Cambridge; New York, 1986.

[19] Mohan, R.N.: On Hadamard Conjecture. Relaesed as e-paper and hold as a lecture in April, 2006.

[20] Paley, R.E.A.C.: On orthogonal matrices. J. Math. Phys. 1933: 12 p. 311–320.

[21] Rotman, J. J.: Introduction to homological algebra. Academic Press Inc., New York, 1979.

[22] Schmidt, B.: Characters and Cyclotomic Fields in Finite Geometry. Springer, New York, 2002.

[23] Stinson, D. R.: Combinatorical Designs: constructions and analysis. Springer Verlag, New York, 2004.

[24] Sylvester, J.J.: 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, 1867: 34 p. 461–475.

[25] Wallis, W. D.: Integral equivalence of Hadamard matrices. J. Combinatorical Theory, 1969: 7 p. 359-368.

[26] Wallis, W.D.: Introduction to combinatorial Designs. Chapman & Hall/CRC Press, Boca Raton, 2007.

[27] Xia, T.; Xia, M. and Seberry, J.: Regular Hadamard Matrices, Maximum Excess and SBIBD. Australasian Journal of Combinatorics , 2003: 27 p. 263–275.

[28] Yang, Y. X.; Niu, X. X. and Xu, C. Q.: Theory and Applications of higher-dimensional Hadamard Matrices. Science Press, Beijing; CRC Press, Boca Raton, 2010.

[29] Zhang, F.: Matrix Theory, Basic Results and Techniques. Springer-Verlag Inc., New York, 1990.

CV

Persönliche Daten

Name:	Christiane Schütz, BSc
Geburtsdatum:	13.12.1989
Geburtsort:	Wien
Staatsbürgerschaft:	Österreich

Schulausbildung

4 Jahre	Volksschule (Wilhelm-Kressplatz 32)
8 Jahre	Realgymnasium (BG/BRG Schwechat) mit ausgezeichnetem Abschluss der Reifeprüfung (4.06.2008)

Universitätsbildung

10.2008 – 07.2011	Universität Wien: Bachelorstudium Mathematik mit Schwerpunkt: Mathematik in den Anwendungen, Abschluss mit Notendurchschnitt 1,77
	Universität Wien: Masterstudium Mathematik (Abschluss mit Erfolg möglich)
10.2011 bis voraussichtlich 03.2015	Nebenfach: Technische Universität Wien: Masterstudium Computermathematik Masterarbeit: Constructions of Hadamard Matrices

Besondere Auszeichnungen

Teilnahme am Projekt: Wir koopieren mit der Wirtschaft 2006 (3. Platz)

Weitere Qualifikationen

Sprachkenntnisse	Deutsch (Muttersprache), Englisch (ausgezeichnet), (Latein)
EDV-Kenntnisse	Microsoft Word, Microsoft Excel, Microsoft Powerpoint, C (Grundkenntnisse), Visual Basic (Grundkenntnisse), Erfahrung mit objektorientierten Programmieren (gute Kenntnisse), LaTex, MatLab, SPSS, Derive, GeoGebra (sehr gute Kenntnisse)