ASYMPTOTIC EXISTENCE OF HADAMARD MATRICES

by

Ivan Livinskyi

A Thesis submitted to the Faculty of Graduate Studies of
The University of Manitoba
in partial fulfilment of the requirements of the degree of

MASTER OF SCIENCE

Department of Mathematics
University of Manitoba
Winnipeg

Abstract

We make use of a structure known as signed groups, and known sequences with zero autocorrelation to derive new results on the asymptotic existence of Hadamard matrices. For any positive odd integer p it is obtained that a Hadamard matrix of order $2^t p$ exists for all

$$t \geq \frac{1}{5} \log_2 \left(\frac{p-1}{2} \right) + 13.$$

Contents

Chapter 1

Introduction. Hadamard matrices

A *Hadamard matrix* H is a square (± 1)-matrix such that any two of its rows are orthogonal. In other words, a square (± 1)-matrix H is Hadamard if and only if

$$HH^\top = nI,$$

where n is the order of H and I is the identity matrix of order n.

The last equation is equivalent to

$$H^\top H = nI,$$

because every real matrix commutes with its inverse. Therefore, any two columns of a Hadamard matrix are orthogonal as well. Denote by $H(n)$ the set of all Hadamard matrices of order n. Consider some examples.

Obviously, there are two 1×1 Hadamard matrices: (1) and (-1). For convenience we will subsequently denote any -1 entry of a matrix or sequence by the one-byte symbol $-$. We use commas to indicate concatenation of sequences: (A, B) is the concatenation of sequences A and B. Furthermore, we denote by c_a a vector $(c, c, \ldots, c)$ of length a.

An example of Hadamard matrix of order 2 is:

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

Moreover, every Hadamard matrix of order two is obtained from the above matrix via row or column permutation or via row or column negation. There exist eight Hadamard matrices of order 2 in total.

In general, two Hadamard matrices are *equivalent* if one of them can be transformed into the other by the above mentioned operations. Let us restate this definition in a different way. A square $(0, \pm 1)$-matrix is called a *signed permutation matrix* if in every row and in every column there is exactly one non-zero entry, i.e., a monomial $(0, \pm 1)$-matrix. The set of all signed permutation matrices of order n is denoted by SP_n. There are $2^n n!$ signed permutation matrices of order n in total. Equivalence can be restated in the following way: Hadamard matrices $H, H' \in H(n)$ are equivalent if

$$H' = PHQ,$$

for some $P, Q \in SP_n$. This is an equivalence relation, since SP_n is a group with respect to matrix multiplication. Note, that matrix transposition is not considered as a part of equivalence definition; H and $H^\top$ may be inequivalent in general.

Hence, up to equivalence, there exists a unique Hadamard matrix of order two.

There is a general rule that allows a construction of a Hadamard matrix of order mn from Hadamard matrices of orders m and n. Let

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{pmatrix} \in H(m),$$

and

$$B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix} \in H(n)$$

be two Hadamard matrices. We are considering the Kronecker matrix product as the tensor product $A \otimes B$ in this work. Consider the matrix

$$C = A \otimes B =$$

$$\begin{pmatrix}
a_{11}b_{11} & a_{11}b_{12} & \cdots & a_{11}b_{1n} & \cdots & \cdots & a_{1m}b_{11} & a_{1m}b_{12} & \cdots & a_{1m}b_{1n} \\
a_{11}b_{21} & a_{11}b_{22} & \cdots & a_{11}b_{2n} & \cdots & \cdots & a_{1m}b_{21} & a_{2m}b_{22} & \cdots & a_{1m}b_{2n} \\
\vdots & \vdots & \ddots & \vdots & & & \vdots & \vdots & \ddots & \vdots \\
a_{11}b_{n1} & a_{11}b_{n2} & \cdots & a_{11}b_{nn} & \cdots & \cdots & a_{1m}b_{n1} & a_{1m}b_{n2} & \cdots & a_{1m}b_{nn} \\
\vdots & \vdots & & \vdots & \ddots & & \vdots & \vdots & & \vdots \\
\vdots & \vdots & & \vdots & & \ddots & \vdots & \vdots & & \vdots \\
a_{m1}b_{11} & a_{m1}b_{12} & \cdots & a_{m1}b_{1n} & \cdots & \cdots & a_{mm}b_{11} & a_{mm}b_{12} & \cdots & a_{mm}b_{1n} \\
a_{m1}b_{21} & a_{m1}b_{22} & \cdots & a_{m1}b_{2n} & \cdots & \cdots & a_{mm}b_{21} & a_{mm}b_{22} & \cdots & a_{mm}b_{2n} \\
\vdots & \vdots & \ddots & \vdots & & & \vdots & \vdots & \ddots & \vdots \\
a_{m1}b_{n1} & a_{m1}b_{n2} & \cdots & a_{m1}b_{nn} & \cdots & \cdots & a_{mm}b_{n1} & a_{mm}b_{n2} & \cdots & a_{mm}b_{nn}
\end{pmatrix}.$$

This is an $mn \times mn$-matrix having property

$$CC^\top = (A \otimes B)(A \otimes B)^\top = (A \otimes B)(A^\top \otimes B^\top) = (AA^\top \otimes BB^\top) = (mI \otimes nI) = mnI.$$

The middle equation is the distributive law of tensor product over ordinary matrix product [HJ].

Hence, a tensor product of two Hadamard matrices is again a Hadamard matrix. Therefore, there are Hadamard matrices of orders 2^t for all positive integers t, constructed from the 2×2 Hadamard matrix via tensoring. These Hadamard matrices were first described by Sylvester in 1867 [Sv] and are called *Sylvester Hadamard matrices.* Sylvester Hadamard matrices are representatives of the unique equivalence classes of $H(2)$, $H(4)$, $H(8)$. However, there are five equivalence classes in $H(16)$ [HSS]. Further, numbers of equivalence classes are too difficult to compute.

Not every positive integer is the order of a Hadamard matrix as we show now. Let H be a Hadamard matrix of order $n \geq 3$. Obviously, H is equivalent to another Hadamard matrix with first row being 1_n. Thus, without loss of generality, we can assume that the first row of H is 1_n. Similarly, we can assume that the second row equals $(1_k, -_l)$, where $k + l = n$. The dot product of first and second rows is equal to

$k-l$. Since H is a Hadamard matrix, this number should be equal to zero. Hence, $k=l$, and $n=2k=2l$ is an even number. Moreover, consider the third row of H. As before, we can permute columns in H to get the third row equal to $(1_a, -_b, 1_c, -_d)$, where

$$a+b=c+d=k=l=n/2.$$

Considering dot products of this row with previous ones, we get two new conditions

$$a-b+c-d=0, \quad a-b-c+d=0.$$

From these equations, we get $a-b=c-d=0$. Finally, we get $a=b=c=d=n/4$. Therefore, n is divisible by 4. Thus, except for two special cases $n=1$ and $n=2$, the order of a Hadamard matrix is always divisible by four.

The first order not equal to a power of two is 12. Up to equivalence, there is a unique matrix in $H(12)$ [HSS]:

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

An *automorphism* of a Hadamard matrix H is a pair (P,Q) of signed permutation matrices, such that $PHQ=H$. The set $\mathrm{Aut}(H)$ of all automorphisms is a group with respect to the multiplication $(P_1,Q_1)\cdot(P_2,Q_2)=(P_1P_2,Q_2Q_1)$. Moreover, the automorphism $(-I,-I)$ commutes with all other automorphisms. Clearly, equivalent Hadamard matrices have isomorphic automorphism groups. There is an interesting connection to Group Theory here, found originally by Marshall Hall [MH]. It is known that for a Hadamard matrix H of order 12, $\mathrm{Aut}(H)/\langle(-I,-I)\rangle \cong M_{12}$, where M_{12} is a Mathieu group — one of 26 sporadic groups. Furthermore, the map $(P,Q) \mapsto (Q^{-1}, P^{-1})$ extends to an outer automorphism of M_{12}.

In the next orders 20, 24, 28, Hadamard matrices also exist and there are 3, 60, and 487 equivalence classes respectively. For more about equivalence of Hadamard matrices see [HSS].

Hadamard matrices of orders 12 and 20 were constructed first by Hadamard in 1893 [H]. He conjectured that Hadamard matrices exist in all orders divisible by four. This statement is called the Hadamard conjecture:

Conjecture 1.1 ([H]). *For every positive integer k, the set $H(4k)$ is not empty.*

As of 2012, this hypothesis remains unresolved. In this thesis an asymptotic version of the Hadamard conjecture giving special block-circulant Hadamard matrices is presented and proved.

The smallest odd number p for which no Hadamard matrix of order $4p$ is known is currently 167. The previous unknown case $p = 107$ was solved by H. Kharagani and B. Tayfeh-Rezaie in 2004 [K428] by constructing corresponding Turyn sequences (see Section 4.5) with the help of computer computations.

Seberry [S1] showed that for every odd p there exists a power of two, 2^t, such that $H(2^t p) \neq \emptyset$. Hadamard conjecture states that we can always take $t = 2$. Seberry showed that we can take $t \geq \lfloor 2\log_2((p-3)/2) \rfloor$. This result was improved 17 years later by Craigen [C1] with a new bound $t \geq 4\lceil \frac{1}{6}\log_2((p-1)/2) \rceil + 2$. The latest bound [C8] is about $\frac{3}{8}\log_2((p-1)/2)$ and is also due to Craigen.

A $(\pm 1, 0)$-matrix W, satisfying similar condition

$$WW^\top = wI,$$

for some positive integer w, is called a *weighing matrix* of *weight* w. Thus, a weighing matrix has orthogonal rows (and columns) and every row (and column) has exactly w non-zero entries. The set of all weighing matrices of order n and weight w is denoted by $W(n,w)$. Clearly, $W(n,n) = H(n)$. The objects of principal interest for us are, of course, Hadamard matrices; however, we will prove some theorems dealing with weighing matrices as well.

Another useful generalization of Hadamard matrices allows entries to be complex units. A *complex Hadamard matrix* H is a square $(\pm 1, \pm i)$-matrix of size n, such that

$$HH^* = nI,$$

where H^* denotes the Hermitian adjoint matrix of H. It is convenient to use one-byte symbol j instead of $-i$.

Denote by $CH(n)$ the set of all complex Hadamard matrices of order n. Like in the real case, not every positive integer is the order of a complex Hadamard matrix.

Assume that H is a complex Hadamard matrix of order $n > 1$. Clearly, a complex Hadamard matrix will remain complex Hadamard, if any of its rows or columns is multiplied with ± 1 or $\pm i$. Thus, without loss of generality, we can assume that the first row of H equals 1_n. After performing some column permutations, we can make its second row equal to $(1_a, -_b, i_c, j_d)$. Since the first two rows are orthogonal, it follows that $a = b$ and $c = d$. Hence, n is even.

A *complex weighing matrix* W of order n and weight w is defined as an $n \times n$ $(0, \pm 1, \pm i)$-matrix satisfying the equation

$$WW^* = wI.$$

Denote the set of all such matrices as $CW(n, w)$.

The analogue of the Hadamard conjecture for complex Hadamard matrices states that they exist in all even orders.

Conjecture 1.2 ([T2]). *For every positive integer k, the set $CH(2k)$ is not empty.*

This conjecture implies the original Conjecture 1.1, since there is a way to construct a real Hadamard matrix from a complex one.

Theorem 1.3 ([T2]). *If there exists a complex Hadamard matrix of order m, then there exists a real Hadamard matrix of order $2m$.*

The main idea of the proof is to perform the following replacement operations

$$\pm 1 \mapsto \pm \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix}, \qquad \pm i \mapsto \pm \begin{pmatrix} 1 & - \\ - & - \end{pmatrix}.$$

The constructed matrix will be twice as large and will be a real Hadamard matrix. For example, the complex Hadamard matrix

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

is mapped to a real matrix,

$$\left(\begin{array}{cc|cc|cc|cc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & - & 1 & - & 1 & - & 1 & - \\ \hline 1 & 1 & 1 & - & - & - & - & 1 \\ 1 & - & - & - & - & 1 & 1 & 1 \\ \hline 1 & 1 & - & - & 1 & 1 & - & - \\ 1 & - & - & 1 & 1 & - & - & 1 \\ \hline 1 & 1 & - & 1 & - & - & 1 & - \\ 1 & - & 1 & 1 & - & 1 & - & - \end{array}\right).$$

A complete proof of Theorem 1.3 will be given in the next chapter.

The tensor product works for complex Hadamard matrices as well.

Further properties and various constructions of Hadamard matrices can be found in [Hr] and [G].

In this work we will present an asymptotic construction for Hadamard matrices. For the construction of Hadamard matrices we shall develop corresponding machinery and prove some necessary propositions. We begin by introducing another generalization of a Hadamard matrix allowing entries to lie in a special structure called a *signed group*. The next chapter deals mostly with signed groups and presents a construction of Hadamard matrices from *signed group Hadamard matrices*. In Chapter 3 we present a construction of signed Hadamard matrices from sequences with a property called *zero autocorrelation.* In Chapter 4 we study and classify all known zero autocorrelation sequences. Finally, in Chapter 5 we summarize results and produce new asymptotic bounds. The last chapter contains some ideas that can be used for future constructions and computer development regarding this topic.

The main new results are Theorems 5.3, 5.4, and 5.5. All the new results are presented in Chapter 5.

Chapter 2

Signed groups and remreps

A *signed group* S is a group with a distinguished central element of order two. We will always denote the unit of a group as 1 and the special element of a signed group as -1. In every signed group the set $\langle -1 \rangle = \{1, -1\}$ always is a normal subgroup. For every element $x \in S$, define its *negation* $-x = -1 \cdot x$. We will call the number of elements in the quotient group $S/\langle -1 \rangle$ the *order* of signed group S. Thus, a signed group of order n is a group of order $2n$.

A *homomorphism* $\varphi : S \to T$ of a signed group S to a signed group T is a group homomorphism that preserves -1, i.e. a map with following properties:

- $\varphi(xy) = \varphi(x)\varphi(y)$, for all $x, y \in S$,
- $\varphi(-1) = -1$.

An *isomorphism* of signed groups is a homomorphism having an inverse map, which is also a signed group homomorphism.

A signed group T is called a *signed subgroup* of a signed group S, if T is a subgroup of S and the distinguished elements of S and T coincide. This relation will be denoted as $T \leq S$. If $T \leq S$ and $T \neq S$ then T is a *proper* signed subgroup; this will be denoted as $T < S$.

Consider some examples of signed groups:

1. The *trivial signed group* $T = S_{\mathbb{R}} = \{1, -1\}$ is a group of order 2. Obviously, every signed group contains an isomorphic copy of T as a signed subgroup.

2. Every group G of order n can be transformed into a signed group of order n via direct product with T. Such signed groups will be called *elementary*.

3. The *complex signed group* $S_{\mathbb{C}} = \langle i | i^2 = -1 \rangle = \{\pm 1, \pm i\}$ is a signed group of order two. This is the smallest non-trivial signed group.

4. The *Quaternion signed group* $Q = \langle j, k | j^2 = k^2 = -1, jk = -kj \rangle$.

5. The set of all monomial $(0, \pm 1)$-matrices of order n forms a signed permutation group SP_n. This is a group of order $2^n n!$ and a signed group of order $2^{n-1} n!$. This is the most important example of a signed group in this work.

6. The set $\mathrm{Aut}(H)$ of all automorphisms of a Hadamard matrix H is a signed group. Its distinguished element is $(-I, -I)$.

7. The set $\mathrm{GL}(n; \mathbb{C})$ of all $n \times n$ invertible complex matrices is a signed group of infinite order whose unique central element of order 2 is $-I$, where I is the identity matrix. Note that $SP_n < \mathrm{GL}(n; \mathbb{C})$.

There is an interesting analogue of Representation Theory for signed groups. For a signed group S, a *representation* of degree m is a signed group homomorphism $\pi : S \to \mathrm{GL}(m; \mathbb{C})$.

We will consider more special representations of signed groups, called *remreps*. A *remrep* (short for "real monomial representation") π of degree m is a representation of a signed group S, such that for every $s \in S$, $\pi(s) \in SP_m$. In other words, a remrep π of degree m is a signed group homomorphism $\pi : S \to SP_m$.

Consider some examples of remreps.

1. Not every signed group admits a remrep of degree 1. For example, the complex signed group $S_{\mathbb{C}}$ does not allow such a remrep. Moreover, the following proposition holds.

   Theorem 2.1. *A signed group S has a remrep of degree 1 if and only if it is elementary.*

Proof. Let S be a signed group. If S is elementary, it is isomorphic to some product $G \times T$. Then the projection on T is a remrep of degree 1.

Conversely, assume that S admits a remrep of degree 1. Let $G \subseteq S$ be the pre-image of 1. Since G is a subgroup of S of index 2, it is a normal subgroup not containing -1. Since G is normal, $G \cap \{\pm 1\} = \{1\}$, and $S = G \cup (-1 \cdot G)$, S is isomorphic to the direct product of G and $\{\pm 1\} \leq S$. Therefore, S is elementary. □

Hence, the existence of such a representation demonstrates that a signed group is elementary.

2. For the complex signed group there exists a remrep of degree 2, uniquely determined by the map

$$i \mapsto \begin{pmatrix} 0 & 1 \\ - & 0 \end{pmatrix}.$$

3. The Quaternion signed group has a representation of degree 2,

$$j \mapsto \begin{pmatrix} 0 & 1 \\ - & 0 \end{pmatrix}, \quad k \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

which is not a remrep, and another representation of degree 4,

$$j \mapsto \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ - & 0 & 0 & 0 \\ 0 & - & 0 & 0 \end{pmatrix}, \quad k \mapsto \begin{pmatrix} 0 & 0 & 0 & - \\ 0 & 0 & 1 & 0 \\ 0 & - & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

which is a remrep.

4. The signed group SP_n has a very nice remrep of degree n — the identity map.

Let S be a signed group. Define a $(0, S)$-*matrix* to be a matrix whose nonzero entries lie in S. To multiply $(0, S)$-matrices we will need an analogue of a group ring for a signed group. Recall that for every ring R and every group G there exists a group ring $R[G]$ that consists of all finite sums

$$r_1g_1 + r_2g_2 + \cdots + r_ng_n,$$

where $r_1, \ldots, r_n \in R$ and $g_1, \ldots, g_n \in G$. Addition and multiplication are defined in a natural way. Group elements form a basis of $R[G]$ considered as a free left R-module. The product of elements r_1g_1 and r_2g_2 is defined to be $(r_1r_2)(g_1g_2)$, where the first product is taken in R, and second in G. By distributivity multiplication is defined on the whole ring.

For signed groups the definition is slightly different. Every signed group has a distinguished element -1. If the ring R has a unit 1_R, its negation is -1_R. It is natural to require that in the *signed group ring*, the negation of the ring unit should be identified with the distinguished element -1 of the signed group. Therefore, for a unital ring R and a signed group S define the signed group ring $R[S]$ as a corresponding group ring modulo the principal ideal $(-1_S + 1_R)$, where -1_S is the distinguished element of S, and 1_R is the unit of R. That is,

$$R[S] = \left\{ \sum_{i=1}^{n} r_i s_i | r_i \in R,\ s_i \in P \right\},$$

where P is a set of coset representatives of S modulo $\langle -1_S \rangle$ and for $s \in P$, $r \in R$ we make the identification $-rs = r(-s)$. Addition is defined termwise and multiplication is defined by linear extension. We will consider only the simplest case $R = \mathbb{Z}$.

In particular, for the trivial signed group T, $\mathbb{Z}[T]$ is isomorphic to $\mathbb{Z}$. For the complex signed group, the corresponding signed group ring $\mathbb{Z}[S_{\mathbb{C}}]$ is isomorphic to the ring $\mathbb{Z}[i]$ of Gaussian integers. For the Quaternion signed group Q, the signed group ring $\mathbb{Z}[Q]$ is isomorphic to the Lipschitz quaternion ring

$$L = \{a + bj + ck + djk | a, b, c, d \in \mathbb{Z}\}.$$

For all $s \in S$ define $s^* = s^{-1}$. Extend this map linearly to the signed group ring $\mathbb{Z}[S]$. Obviously, the conjugation is an involution, i.e. $x^{**} = x$ for all $x \in \mathbb{Z}[S]$, and $(xy)^* = y^*x^*$ for all $x, y \in \mathbb{Z}[S]$.

For an $n \times m$-matrix $A = (a_{ij})$ with entries in $\mathbb{Z}[S]$ define its *adjoint* as an $m \times n$-matrix $A^* = (b_{ij})$, where $b_{ij} = a_{ij}^*$. In other words, A^* is the entry-wise conjugation of $A^\top$. For example, consider Q-matrices:

$$\begin{pmatrix} k & j & 1 \\ -1 & -k & j \end{pmatrix}^* = \begin{pmatrix} -k & -1 \\ -j & k \\ 1 & -j \end{pmatrix}.$$

Since $\mathbb{Z}[S]$ is a ring, we can define a product AB of two square matrices A, B of the same order with entries in $\mathbb{Z}[S]$ in a natural way. In particular, we can assume that A and B are just $(0, S)$-matrices. Moreover,

$$(AB)^* = B^* A^*.$$

Using signed groups we can generalize the notion of Hadamard and weighing matrices. Define a *signed group Hadamard* matrix A of order n over a signed group S to be an S-matrix of order n, such that

$$AA^* = nI.$$

Denote the set of all such matrices as $SH(n; S)$. Define a *signed group weighing matrix* W of order n and weight w to be a square $(0, S)$-matrix of order n satisfying similar condition

$$WW^* = wI.$$

Denote the set of all such matrices by $SW(n, w; S)$.

For example,

$$\begin{pmatrix} j & k \\ k & j \end{pmatrix}$$

is a circulant signed group Hadamard matrix in $SH(2; Q)$.

Since $\mathbb{Z}[S_{\mathbb{C}}] = \mathbb{Z}[i]$ we can see that $SH(n; S_{\mathbb{C}}) = CH(n)$. That is, signed group Hadamard matrices over the signed group $S_{\mathbb{C}}$ are just complex Hadamard matrices. Similarly, $SH(n; T) = H(n)$.

Using remreps there is a way to construct real Hadamard matrices from signed group ones. First, if we have a remrep $\pi : S \to SP_m$, extend it to a ring homomorphism $\mathbb{Z}[S] \to M_m(\mathbb{Z})$ linearly by

$$\pi(k_1 s_1 + \cdots + k_n s_n) = k_1 \pi(s_1) + \cdots + k_n \pi(s_n).$$

Since $P^{-1} = P^\top$ for every matrix $P \in SP_m$, for every $x \in \mathbb{Z}[S]$ we have $\pi(s^*) = \pi(s)^\top$. Consider the following theorem.

Theorem 2.2. *Assume that for some signed group S there exists a signed weighing matrix $W \in SW(n, w; S)$ and a remrep π of degree m, where m is the order of a Hadamard matrix. Then there exists a weighing matrix $U \in W(mn, mw)$.*

Proof. Let $W = (w_{ij})$, and let H be a Hadamard matrix of order m. Construct a matrix U as a $n \times n$ block matrix $U = (\pi(w_{ij})H)_{i,j=1}^n$. Then $U^\top = (H^\top \pi(w_{ji})^\top)_{i,j=1}^n$. Let $UU^\top = (G_{ij})_{i,j=1}^n$. Then for fixed integers i, j we have

$$G_{ij} = \pi(w_{i1})HH^\top \pi(w_{1j})^\top + \cdots + \pi(w_{in})HH^\top \pi(w_{nj})^\top =$$
$$m(\pi(w_{i1})\pi(w_{1j}^*) + \cdots + \pi(w_{in})\pi(w_{nj}^*)) = m\pi(w_{i1}w_{1j}^* + \cdots + w_{in}w_{nj}^*) =$$
$$m\pi(w\delta_{ij} \cdot 1_S) = mw\delta_{ij} I.$$

where $\delta_{ij} = 1$ if $i = j$, and $\delta_{ij} = 0$ otherwise. Therefore, $UU^\top = mwI$ and U is a weighing matrix. □

In particular, this works when W is a signed group Hadamard matrix.

Corollary 2.3. *Assume that for some signed group S there exists a signed Hadamard matrix $H \in SH(n; S)$ and a remrep of degree m, where m is the order of a Hadamard matrix. Then there exists a Hadamard matrix of order mn.*

And a similar corollary for complex Hadamard matrices.

Corollary 2.4. *Assume that for some signed group S there exists a signed Hadamard matrix $H \in SH(n; S)$ and a remrep of degree m, where m is the order of a complex Hadamard matrix. Then there exists a complex Hadamard matrix of order mn.*

Now we can prove Theorem 1.3 from Chapter 1 regarding the construction of Hadamard matrices from complex Hadamard matrices.

Proof of Theorem 1.3. Let C be a complex Hadamard matrix. Then C can be viewed as a signed group Hadamard matrix over $S_{\mathbb{C}}$. On p. 12 we considered a remrep of the complex signed group of degree 2. Since there is a Hadamard matrix

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

according to Theorem 2.2, we may perform replacement operations

$$\pm 1 \mapsto \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix} = \pm \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix},$$

and

$$\pm i \mapsto \pm \begin{pmatrix} 0 & 1 \\ - & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix} = \pm \begin{pmatrix} 1 & - \\ - & - \end{pmatrix},$$

to obtain a Hadamard matrix. □

Since Q has a remrep of degree 4, we can construct a Hadamard matrix of order 8 from the signed group Hadamard matrix

$$\begin{pmatrix} j & k \\ k & j \end{pmatrix}$$

over Q. Using a Hadamard matrix

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

we construct a bigger one,

$$\left(\begin{array}{cccc|cccc}
1 & - & 1 & - & - & 1 & 1 & - \\
1 & - & - & 1 & 1 & - & 1 & - \\
- & - & - & - & - & - & 1 & 1 \\
- & - & 1 & 1 & 1 & 1 & 1 & 1 \\
\hline
- & 1 & 1 & - & 1 & - & 1 & - \\
1 & - & 1 & - & 1 & - & - & 1 \\
- & - & 1 & 1 & - & - & - & - \\
1 & 1 & 1 & 1 & - & - & 1 & 1
\end{array}\right).$$

We will use Corollaries 2.3 and 2.4 in the construction of Hadamard matrices to obtain the new asymptotic results mentioned in the introduction. In the next chapter we will describe a construction of a Hadamard matrix in $SH(p; SP_{2^n})$ for every odd integer p and some n.

Chapter 3

Construction of signed group Hadamard matrices from sequences

Let S be a signed group and let A be a $(0, S)$-matrix. Define the *support* of A, *supp*(A), as the set of positions of all nonzero entries of A. A is *quasisymmetric* if *supp*$(A^\top)$ = *supp*(A). A is called *normal* if it commutes with A^*. A is *circulant* if $A = (a_{i-j+1})_{i,j=1}^{n}$ for a sequence $(a_1, a_2, \ldots, a_n)$, which is identified with the first row of A, and $i - j$ is reduced modulo n. Pairwise disjoint matrices are *supplementary* if their sum has no zero entries.

Let us consider a few ways to construct bigger matrices from smaller ones while preserving certain properties.

Lemma 3.1 ([C1])**.** *Let A, B be normal, commuting, disjoint, quasisymmetric $(0, S)$-matrices of order n. Let*

$$C = \begin{pmatrix} A + B & A - B \\ A^* - B^* & -A^* - B^* \end{pmatrix}.$$

Then

$$CC^* = C^*C = 2I_2 \otimes (AA^* + BB^*).$$

If S has a remrep of degree m, then there exists a normal $(0,S')$-matrix D of order n with the same support as $A+B$, such that $DD^* = D^*D = AA^* + BB^*$, where $S' \geq S$ is a signed group having a remrep of order $2m$. Moreover, if A and B are circulant, then so is D.

Proof. Since A and B are disjoint, C is a $(0,S)$-matrix. By definition,

$$CC^* = \begin{pmatrix} A+B & A-B \\ A^*-B^* & -A^*-B^* \end{pmatrix} \begin{pmatrix} A^*+B^* & A-B \\ A^*-B^* & -A-B \end{pmatrix} =$$

$$\begin{pmatrix} (A+B)(A^*+B^*)+(A-B)(A^*-B^*) & (A+B)(A-B)-(A-B)(A+B) \\ (A^*-B^*)(A^*+B^*)-(A^*+B^*)(A^*-B^*) & (A^*-B^*)(A-B)+(A^*+B^*)(A+B) \end{pmatrix}$$

$$= \begin{pmatrix} 2(AA^*+BB^*) & 0 \\ 0 & 2(AA^*+BB^*) \end{pmatrix} = 2I_2 \otimes (AA^*+BB^*).$$

Similarly $C^*C = 2I_2 \otimes (A^*A + B^*B) = CC^*$.

The matrix D is obtained in the following way. Reorder the rows and columns of C so that the resulting matrix, D_0, is partitioned into 2×2 blocks whose entries are the (i,j), $(i+n,j)$, $(i,j+n)$, $(i+n,j+n)$ entries of C, $1 \leq i,j \leq n$. Applying the same reordering to $2I_2 \otimes (AA^*+BB^*)$ we will get the matrix $(AA^*+BB^*) \otimes 2I_2$. Therefore, $D_0D_0^* = (AA^*+BB^*) \otimes 2I_2$.

Since A and B are disjoint and quasisymmetric, each non-zero block of D_0 will have one of the forms

$$\begin{pmatrix} a & a \\ b & -b \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} a & -a \\ b & b \end{pmatrix},$$

where $a,b \in S$. Multiplying D_0 on the right by $M = \frac{1}{2}I_n \otimes \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix}$, we get a $(0,S)$-matrix D_1 whose non-zero 2×2 blocks are of the form

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}.$$

Such 2×2 $(0,S)$-matrices form another signed group, which we will denote by S'.

Since

$$MM^* = \frac{1}{4} \cdot I_n^2 \otimes \left[\begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix} \right] = \frac{1}{4} \cdot I_n \otimes 2I_2 = \frac{1}{2} \cdot I_{2n},$$

we have that

$$D_1 D_1^* = D_0 M M^* D_0^* = \frac{1}{2} \cdot D_0 D_0^* = (AA^* + BB^*) \otimes I_2.$$

Similarly, $D_1^* D_1 = (AA^* + BB^*) \otimes I_2$.

Consider the signed group S' in more detail. First, we can construct a remrep of S' from a remrep of S. Really, let $\pi : S \to SP_m$ be a remrep of S. Consider a map $\pi' : S' \to SP_{2m}$ defined by

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mapsto \begin{pmatrix} \pi(a) & 0_m \\ 0_m & \pi(b) \end{pmatrix}, \quad \begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix} \mapsto \begin{pmatrix} 0_m & \pi(a) \\ \pi(b) & 0_m \end{pmatrix},$$

where 0_m denotes the zero $m \times m$ matrix. Direct verification shows that π' is a signed group homomorphism and a remrep of degree $2m$.

Matrices of the form

$$a \otimes I_2 = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \quad a \in S,$$

form a signed subgroup of S', which is isomorphic to S; thus, we can identify this signed subgroup with S itself and consider S' as an extension of S.

Finally, we can replace every 2×2 block of D_1 with corresponding element of S' or zero, to obtain a $(0, S')$-matrix D. Since we identify 2×2-matrix $a \otimes I_2 \in S'$ with $a \in S$, we get $DD^* = D^*D = AA^* + BB^*$.

If A and B are circulant, then C consists of four circulant blocks, so both D_0 and D_1 are block-circulant with block size 2×2. Consequently, D is circulant. □

Here is the corresponding result for weighing matrices.

Corollary 3.2. *Let A, B be normal, commuting, disjoint, quasisymmetric weighing matrices of order n and weights v and w respectively. If S has a remrep of degree m, then there exists a matrix $D \in SW(n, v + w; S')$, where $S' \geq S$ has a remrep of degree $2m$. If both A and B are circulant, then so is D.*

Consider an example. Let

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 1 & - \\ - & 0 & 1 & 1 \\ 1 & - & 0 & 1 \\ 1 & 1 & - & 0 \end{pmatrix}$$

be two disjoint quasisymmetric circulant weighing matrices. The corresponding matrices from Lemma 3.1 are

$$C = \begin{pmatrix} 1 & 1 & 1 & - & 1 & - & - & 1 \\ - & 1 & 1 & 1 & 1 & 1 & - & - \\ 1 & - & 1 & 1 & - & 1 & 1 & - \\ 1 & 1 & - & 1 & - & - & 1 & 1 \\ 1 & 1 & - & - & - & 1 & - & - \\ - & 1 & 1 & - & - & - & 1 & - \\ - & - & 1 & 1 & - & - & - & 1 \\ 1 & - & - & 1 & 1 & - & - & - \end{pmatrix}, \ D_0 = \left(\begin{array}{cc|cc|cc|cc} 1 & 1 & 1 & - & 1 & - & - & 1 \\ 1 & - & 1 & 1 & - & - & - & - \\ \hline - & 1 & 1 & 1 & 1 & - & 1 & - \\ - & - & 1 & - & 1 & 1 & - & - \\ \hline 1 & - & - & 1 & 1 & 1 & 1 & - \\ - & - & - & - & 1 & - & 1 & 1 \\ \hline 1 & - & 1 & - & - & 1 & 1 & 1 \\ 1 & 1 & - & - & - & - & 1 & - \end{array}\right),$$

$$D_1 = \left(\begin{array}{cc|cc|cc|cc} 1 & 0 & 1 & 0 & 0 & - & - & 0 \\ 0 & 1 & 0 & - & 1 & 0 & 0 & 1 \\ \hline - & 0 & 1 & 0 & 1 & 0 & 0 & - \\ 0 & 1 & 0 & 1 & 0 & - & 1 & 0 \\ \hline 0 & - & - & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & - \\ \hline 1 & 0 & 0 & - & - & 0 & 1 & 0 \\ 0 & - & 1 & 0 & 0 & 1 & 0 & 1 \end{array}\right).$$

Matrices $a = \begin{pmatrix} 1 & 0 \\ 0 & - \end{pmatrix}$, $c = \begin{pmatrix} 0 & - \\ 1 & 0 \end{pmatrix}$ generate a signed group

$$S = \langle a, c | a^2 = 1, c^2 = -1, ac = -ca \rangle,$$

which has a remrep of degree 2. Finally,

$$D = \begin{pmatrix} 1 & a & c & -a \\ -a & 1 & a & c \\ c & -a & 1 & a \\ a & c & -a & 1 \end{pmatrix}$$

is a circulant signed group Hadamard matrix over S.

A circulant matrix can be identified by its first row. Let X be a finite $(0, S)$-sequence. Denote by *circ*(X) the circulant matrix having first row X. We will call a sequence X *quasisymmetric* if *circ*(X) is a quasisymmetric matrix. Similarly, two sequences X, Y of same length are *disjoint* if *circ*(X), *circ*(Y) are disjoint. Disjoint sequences are called *supplementary* if the corresponding circulant matrices are supplementary.

If $A = (a_1, a_2, \ldots, a_l)$ is a $(0, S)$-sequence of length l, denote by $N_A(j)$ its *non-periodic autocorrelation function*, which is defined by

$$N_A(j) = \sum_{i=1}^{l-j} a_i a_{i+j}^*,$$

for all $0 \leq j < l$ and equals zero for all other j. A set $X_1, X_2, \ldots, X_n$ of $(0, S)$-sequences is said to have *zero autocorrelation with weight* w if the sum

$$N_{X_1}(j) + N_{X_2}(j) + \cdots + N_{X_n}(j)$$

equals zero for all $j > 0$ and equals w for $j = 0$. Sequences having zero autocorrelation are also called *complementary.*

Further, denote by $P_A(j)$ the *periodic autocorrelation function* of A defined by

$$P_A(j) = \sum_{i=1}^{l} a_i a_{i+j}^* \ ,$$

where indices are all reduced modulo l. This is a periodic function with period l. Periodic autocorrelation function is useful because of the following statement.

Lemma 3.3. *Let $A = (a_1, \ldots, a_n)$ be an S-sequence. Then, $MM^* = (P_A(j-i))_{i,j=1}^n$, where $M = circ(A)$.*

Proof. By definition of circulant matrix, $M = (a_{i-j+1})_{i,j=1}^{n}$, $M^* = (a_{j-i+1}^*)_{i,j=1}^{n}$. The (i,j) entry of MM^* is equal to

$$\sum_{k=1}^{n} a_{i-k+1}a_{j-k+1}^* = P_A(j-i).$$

□

A set $X_1, X_2, \ldots, X_n$ of sequences of length q is said to have *zero periodic autocorrelation with weight w and period q* if the sum

$$P_{X_1}(j) + P_{X_2}(j) + \cdots + P_{X_n}(j)$$

equals w for $j \equiv 0 \pmod{q}$, and equals zero otherwise. By Lemma 3.3 this is equivalent to the equality

$$M_1M_1^* + M_2M_2^* + \cdots + M_nM_n^* = wI,$$

where $M_i = circ(X_i)$.

From now on we will be considering only $(0, \pm1, \pm i)$-sequences. Note, that for such sequences, the conjugation is the same as the usual complex conjugation $x \mapsto \overline{x}$. There is a connection between periodic and non-periodic autocorrelation for complex sequences.

Lemma 3.4. *Let $A = (a_1, \ldots, a_l)$ be a $(0, \pm1, \pm i)$-sequence. Then for all $k = 0, 1, \ldots, l-1$:*

$$P_A(k) = N_A(k) + N_{A^*}(l-k),$$

where $A^* = (a_l^*, \ldots, a_2^*, a_1^*)$ is the reverse sequence of A.

Proof. By definition,

$$P_A(k) = a_1a_{k+1}^* + \cdots + a_la_k^* = (a_1a_{k+1}^* + \cdots + a_{l-k}a_l^*) +$$
$$(a_1^*a_{l-k+1} + \cdots + a_k^*a_l) = N_A(k) + N_{A^*}(l-k).$$

□

Lemma 3.4 fails in general, when A is a $(0,S)$-sequence for some signed group S. Complex sequences of the same length with zero autocorrelation clearly have also zero periodic autocorrelation. Consider some additional results involving complex matrices.

Lemma 3.5. *Any two circulant complex matrices commute.*

Proof. Let $C = circ(a_1, \dots, a_n)$, $D = circ(b_1, \dots, b_n)$. Then the (i,j) entry of CD equals

$$\sum_{k=1}^{n} a_{i-k+1} b_{k-j+1} = \sum_{p+q=i-j+2} a_p b_q$$

Obviously, this is the same as the (i,j) entry of DC. □

Lemma 3.6. *All complex Hadamard, weighing, and circulant matrices are normal.*

Proof. Let $W \in CW(n,w)$, where $w \geq 1$. Then $WW^* = wI$. Thus, a complex matrix $\frac{1}{w}W^*$ is the inverse of W. Since every invertible complex matrix commutes with its inverse, we have $(\frac{1}{w}W^*)W = I$, or $W^*W = wI$. Thus, W is normal. Obviously, Hadamard matrices are just special weighing matrices.

Let C be a circulant complex matrix with the first row $(a_1, a_2, \dots, a_n)$. Then C^* is a circulant matrix with the first row $(a_1^*, a_n^*, \dots, a_2^*)$. By Lemma 3.5 $CC^* = C^*C$; thus, C is normal. □

Theorem 3.7 ([C1])**.** *Let $X_1, X_2, \dots, X_n$ be disjoint, quasisymmetric $(0,\pm 1)$-sequences having zero periodic autocorrelation of period q and weight w. Then there exists a circulant $SW(q,w;S)$ for a signed group S that admits a remrep of degree 2^{n-1}.*

Proof. Let $M_i = circ(X_i)$ for all $i = 1, 2, \dots, n$. Then these matrices are all normal, disjoint, commuting and quasisymmetric. Apply Lemma 3.1 to matrices M_1 and M_2 to obtain a circulant normal $(0,S_1)$-matrix N_1, such that $N_1N_1^* = M_1M_1^* + M_2M_2^*$, where $S_1 \geq \langle -1 \rangle$ is a signed group with a remrep of degree 2. Since $supp(N_1)$ is the union of supports $supp(M_1)$ and $supp(M_2)$, N_1 is quasisymmetric and disjoint from $M_3, M_4, \dots, M_n$.

Assume that we have constructed a circulant quasisymmetric normal $(0, S_i)$-matrix N_i, where S_i is a signed group with remrep of degree 2^i, such that N_i is disjoint from $M_{i+2}, \ldots, M_n$, and

$$N_i N_i^* = M_1 M_1^* + M_2 M_2^* + \cdots + M_{i+1} M_{i+1}^*.$$

Apply Lemma 3.1 to N_i and M_{i+2} to obtain a circulant normal $(0, S_{i+1})$-matrix N_{i+1} with similar properties, where $S_{i+1} \geq S_i$ is a signed group with remrep of degree 2^i.

Applying this procedure $n-2$ times, we will get a $(0, S_{n-1})$-matrix $N = N_{n-1}$ with the property

$$NN^* = M_1 M_1^* + M_2 M_2^* + \cdots + M_n M_n^* = wI,$$

where $S_{n-1} = S$ is a signed group having a remrep of degree 2^{n-1}. □

A complex version of Theorem 3.7 works similarly and produces a circulant $SW(q, w; S)$ for a signed group with a remrep of degree 2^n.

Corollary 3.8. *Let $X_1, X_2, \ldots, X_n$ be supplementary quasisymmetric $(0, \pm 1)$-sequences having zero periodic autocorrelation of period q. Then there exists a Hadamard matrix in $H(2^{n-1}q)$.*

Corollary 3.9. *Let $X_1, X_2, \ldots, X_n$ be supplementary quasisymmetric $(0, \pm 1, \pm i)$-sequences having zero periodic autocorrelation of period q. Then there exists a Hadamard matrix in $H(2^n q)$.*

There is a way to construct sequences with all these properties from any finite set of sequences of various lengths having zero autocorrelation, as follows.

Let p be an odd positive integer. Consider two (± 1)-sequences U and V of length $l \leq \frac{p-1}{2}$. Assume additionally that V^* has the same support as U (then in turn U^* has the same support as V). Construct two new sequences X_U and X_V in the following way. Take any two nonnegative integers a, b, such that $a + b = p - l - 1$, let

$$X_U = (0_{a+1}, U, 0_{2b+1}, V, 0_a), \quad X_V = (0_{b+1}, V, 0_{2a+1}, -U, 0_b).$$

These are both sequences of length $2p$. Since *supp* $U^* =$ *supp* V, X_U is quasisymmetric. The same condition holds for X_V. Moreover, we can always choose numbers a and b in a such way that X_U and X_V would be disjoint. Finally,

$$N_{X_U}(j) + N_{X_V}(j) = 2(N_U(j) + N_V(j)),$$

for all $j \in \mathbb{Z}$. Therefore, if U and V have zero autocorrelation, so do X_U and X_V.

Theorem 3.10 ([C1])**.** *Suppose that $A_1, B_1, \ldots, A_t, B_t$ are $2t$ (± 1)-sequences with zero autocorrelation, A_i, B_i both having length l_i, $i = 1, \ldots, t$, where $\sum_{i=1}^{t} l_i = L$. Then there exists a Hadamard matrix of order $4^{t+1}(2L+1)$.*

Proof. We can always embed a pair (A_i, B_i) to a quasisymmetric disjoint pair (X_{A_i}, X_{B_i}) of sequences of length $4L+2$ as discussed above. Define the sequences

$$\begin{aligned}
X_1 &= (1, 0_{4L+1}),\\
X_{A_i} &= (0, 0_{2(l_n+\cdots+l_{i+1})}, 0_{l_i}, A_i, 0_{2(l_{i-1}+\cdots+l_1)}, 0, 0_{2(l_1+\cdots+l_{i-1})}, B_i, 0_{l_i}, 0_{2(l_{i+1}+\cdots+l_n)}),\\
X_{B_i} &= (0, 0_{2(l_n+\cdots+l_{i+1})}, B_i, 0_{l_i}, 0_{2(l_{i-1}+\cdots+l_1)}, 0, 0_{2(l_1+\cdots+l_{i-1})}, 0_{l_i}, -A_i, 0_{2(l_{i+1}+\cdots+l_n)}),\\
X_2 &= (0_{2L+1}, 1, 0_{2L}),
\end{aligned}$$

Trivially, the sequences $X_1, X_2, X_{A_1}, X_{B_1}, \ldots, X_{A_t}, X_{B_t}$ are supplementary. Applying Corollary 3.8 we obtain a Hadamard matrix of order $2^{2t+1}(4L+2) = 4^{t+1}(2L+1)$. □

For the asymptotic constructions we shall discuss, it would be necessary for a length L to find the smallest possible set of supplementary sequences of total length $2L$ with zero autocorrelation.

Theorem 3.10 works similarly for complex sequences. However, we need our sequences to be divided into pairs of equal lengths. This holds automatically for any set of binary sequences with zero autocorrelation (see Lemma 4.1).

Theorem 3.11. *Suppose that $A_1, B_1, \ldots, A_t, B_t$ are $2t$ $(\pm 1, \pm i)$-sequences with zero autocorrelation, A_i, B_i both having length l_i, $i = 1, \ldots, t$, where $\sum_{i=1}^{t} l_i = L$. Then there exists a Hadamard matrix of order $2^{2t+3}(2L+1)$.*

Proof. Repeat the proof of Theorem 3.10 using Corollary 3.9. □

For example, let $U = (1, 1, -)$, $V = (1, i, 1)$. Then,

$$\begin{aligned} N_U(1) &= 1 \cdot 1 + 1 \cdot (-1) = 0, & N_V(1) &= 1 \cdot (-i) + i \cdot 1 = 0, \\ N_U(2) &= 1 \cdot (-1) = -1, & N_V(2) &= 1 \cdot 1 = 1. \end{aligned}$$

Therefore, U and V have zero autocorrelation. Then, the following four sequences

$$\begin{aligned} X_1 &= (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0), \\ X_U &= (0, 1, 1, -, 0, 0, 0, 0, 0, 0, 0, 1, i, 1), \\ X_2 &= (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0), \\ X_V &= (0, 0, 0, 0, 1, i, 1, 0, -, -, 1, 0, 0, 0). \end{aligned}$$

are complex supplementary quasisymmetric sequences with zero autocorrelation. By the complex analogue of Corollary 3.8, there exists a Hadamard matrix of order 112.

Thus, we construct Hadamard matrices from sets of sequences with zero autocorrelation. In the next chapter we consider basic properties and examples of such sequences.

Chapter 4

Some classes of sequences with zero autocorrelation

Any set of complementary (± 1)-sequences of lengths greater than one can be partitioned into pairs of sequences having equal lengths. We denote by $l(A)$ the length of a sequence A.

Lemma 4.1 ([C8])**.** *Let S be a finite set of n binary sequences of various lengths, all greater than 1, with zero autocorrelation. Then n is even. Further, the number of sequences in S of any given length is even.*

Proof. Let $S = \{A_1, \ldots, A_n\}$. Denote $N(x) = N_{A_1}(x) + \cdots + N_{A_n}(x)$. Moreover, assume that $l_1 > l_2 > \ldots > l_k > 1$ are all possible lengths of sequences in S. We prove by induction that the number of sequences having length l_i is even for all i.

Consider $0 = N(l_1 - 1) = \sum_{l(A_j)=l_1} N_{A_j}(l_1 - 1)$. Since $N_{A_j}(l_1 - 1) = \pm 1$ for all j such that $l(A_j) = l_1$, the number of sequences of length l_1 should be even.

Let i be a positive integer. Assume that number of sequences of length l_{i_0} is even for all $i_0 < i$. Consider $N(l_i - 1)$. Obviously,

$$N(l_i - 1) = \sum_{l(A_j)=l_i} N_{A_j}(l_i - 1) + \sum_{l(A_j)>l_i} N_{A_j}(l_i - 1).$$

However, values $N_{A_j}(l_i - 1)$ have the same parity for all A_j's of the same length. By induction assumption, the number of such sequences is even. Therefore,

$$N(l_i - 1) \equiv \sum_{l(A_j)=l_i} N_{A_j}(l_i - 1) \pmod 2.$$

Since $l_i - 1 > 0$, we have $N_{A_j}(l_i - 1) = \pm 1$, for all j such that $l(A_j) = l_i$. Therefore, the number of sequences of length l_i is also even. □

Consider some general properties of complementary sequences. Obviously, we can take any two sets of complementary sequences and unite them together to get a bigger set. The total length of the new set is the sum of total lengths of the original sets. There are a few more operations we can do with complementary sequences.

Lemma 4.2. *If $A_1, A_2, \ldots, A_{2n}$ are complementary $(0, \pm 1, \pm i)$-sequences of total length l, then there exist complementary $(0, \pm 1, \pm i)$-sequences $B_1, B_2, \ldots, B_{2n}$ of total length $2l$.*

Proof. For $i = 1, 2, \ldots, n$ define $B_{2i-1} = (A_{2i}, A_{2i-1})$, $B_{2i} = (A_{2i}, -A_{2i-1})$. Then,

$$N_{B_{2i-1}}(j) + N_{B_{2i}}(j) = 2(N_{A_{2i-1}}(j) + N_{A_{2i}}(j)),$$

for all $j \in \mathbb{Z}$. Therefore, $B_1, B_2, \ldots, B_{2n}$ are complementary of total length $2l$. □

We can also multiply sets of complementary sequences. The *tensor product* of two sequences $A = (a_1, a_2, \ldots, a_m)$ and $B = (b_1, b_2, \ldots, b_n)$ is the sequence

$$A \otimes B = (a_1 b_1, a_2 b_1, \ldots, a_m b_1, \ldots, a_1 b_n, a_2 b_n, \ldots, a_m b_n).$$

Lemma 4.3 ([C8])**.** *If $A_1, A_2, \ldots, A_{2n}$ are complementary (± 1)-sequences of total length $2x$, and $B_1, B_2, \ldots, B_{2m}$ are complementary $(\pm 1, \pm i)$-sequences of total length $2y$, then there exists a set of $2mn$ $(\pm 1, \pm i)$-sequences with zero autocorrelation and total length $2xy$.*

Proof. Without loss of generality, assume that all pairs A_i, A_{i+n}, and B_j, B_{j+m}, for $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, m$ consist of sequences of equal lengths. Then the sequences

$$\frac{A_i + A_{i+n}}{2} \otimes B_j + \frac{A_i - A_{i+n}}{2} \otimes B_{j+m}, \frac{A_i + A_{i+n}}{2} \otimes B^*_{j+m} - \frac{A_i - A_{i+n}}{2} \otimes B^*_j,$$

$i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, m$, form a set of $2mn$ complementary sequences with total length $2xy$. □

Lemma 4.3 generalizes Lemma 4.2 in the following way. Every set of complementary binary sequences can be multiplied by any Golay number, not only doubled, as we now discuss.

4.1 Golay sequences

Lemma 4.1 implies that every set of complementary binary sequences contains at least two sequences of the same length. The case when there are only two sequences was first considered by M. Golay in 1949 [G1].

Golay sequences are two (± 1)-sequences having zero autocorrelation. The length of a Golay sequence is called a *Golay number*. Denote by $GS(l)$ the set of all pairs of Golay sequences of length l.

For the length $l = 1$ any pair of real units forms a Golay pair; $GS(1)$ has four elements.

For the length $l = 2$ we have the pair $A = (1, 1)$, $B = (1, -)$. All pairs in $GS(2)$ can be obtained from $(A; B)$ by replacing, reversing, or negating one of the sequences. There are 8 pairs in $GS(2)$ in total.

For the length $l = 3$ there are no Golay pairs.

The following product constructs a Golay pair of length mn from Golay pairs of lengths m and n (first described by R. Turyn in 1974 [T1]).

Theorem 4.4 ([C6])**.** *If $(A; B) \in GS(m)$ and $(C; D) \in GS(n)$, then*

$$\left(\frac{1}{2}[(A+B)\otimes C + (A-B)\otimes D^*];\ \frac{1}{2}[(A+B)\otimes D - (A-B)\otimes C^*]\right) \in GS(mn).$$

Note that this is a special case of Lemma 4.3.

Therefore, 2^k is a Golay number for all k. Golay pairs that can not be constructed by this multiplication are of special interest. Golay showed in [G2] that 10 and 26 are Golay numbers by constructing a pair

$$A = (1, 1, -, 1, -1, 1, -, -1, 1, 1), \qquad B = (1, 1, -, 1, 1, 1, 1, 1, -, -)$$

of length 10, and another pair

$$\begin{aligned}
A &= (1,1,1,1,-,1,1,-,-,1,-,1,-,1,-,-,1,-,1,1,1,-,-,1,1,1),\\
B &= (1,1,1,1,-,1,1,-,-,1,-,1,1,1,1,1,-,1,-,-,-,1,1,-,-,-)
\end{aligned}$$

of length 26. Thus, Golay sequences exist in all lengths of the form $2^\alpha 10^\beta 26^\gamma$ for all $\alpha, \beta, \gamma \geq 0$. As of early 2012, there had been no Golay pairs found with a different length. Lengths up to 100 were considered in [BF]. For lengths not greater than 200, only 106, 116, 122, 130, 136, 146, 148, 164, 170, 178, 194 remain unsettled.

There is also the following general non-existence result.

Theorem 4.5 ([E]). *No Golay number g is divisible by a number congruent to* 3 *modulo* 4*.*

4.2 Base sequences

Let us consider sets of four complementary sequences with one or two distinct lengths.

Base sequences are four (± 1)-sequences of lengths $m, m, m+q, m+q,\ q \geq 0$ having zero autocorrelation. Denote by $BS(m, m+q)$ the set of all quadruples of base sequences of lengths m, m, $m+q$, $m+q$.

For example, $(A;B;C;D) \in BS(3,4)$, where

$$\begin{aligned}
A &= (1,1,1), & C &= (1,1,-,1),\\
B &= (1,-,1), & D &= (1,1,-,-),
\end{aligned}$$

because

$$\begin{aligned}
N_A(1) &= 2; & N_C(1) &= -1;\\
N_A(2) &= 1; & N_C(2) &= 0;\\
& & N_C(3) &= 1;\\
N_B(1) &= 0; & N_D(1) &= -1;\\
N_B(2) &= 1; & N_D(2) &= -2;\\
& & N_D(3) &= -1;
\end{aligned}$$

Base sequences of $BS(m, m+1)$ have been studied extensively. In [K1] examples are presented for all $m \leq 30$. Base sequences up to length $m = 35$ are presented on Christos Koukouvinos' personal website [K5]. Further examples for $m = 36$, 37, 38 appeared in [D2].

Lemma 4.3 implies that any quadruple of base sequences can be multiplied with any Golay pair to obtain another quadruple.

Base sequences with $q = 1$ are of special interest because of the following theorem.

Theorem 4.6 ([Y])**.** *If there exist base sequences of lengths m, m, $m+1$, $m+1$ and n, n, $n+1$, $n+1$, then there exist four complementary (± 1)-sequences of length $(2m+1)(2n+1)$.*

Since $BS(n, n+1)$ is not empty for all $1 \leq n \leq 38$, Theorem 4.6 provides many new base sequences. Theorem 4.6 is usually called by *Yang multiplication.*

The following slight generalization of Yang multiplication requires only one quadruple to have $q = 1$.

Theorem 4.7 ([K3])**.** *If there are base sequences of lengths m, m, $m+q$, $m+q$ and n, n, $n+1$, $n+1$, then there are four complementary (± 1)-sequences of length $(2m+q)(2n+1)$.*

Consider the following generalization of base sequences. *Complex base sequences* are four $(\pm 1, \pm i)$-sequences of lengths $m, m, m+q, m+q$ having zero autocorrelation. It seems that this definition does not appear in the literature. Denote by $CBS(m, m+q)$ the set of all quadruples of complex base sequences of lengths m, m, $m+q$, $m+q$. Another form of Yang multiplication works in this case.

Theorem 4.8 ([C2])**.** *If there exist complex base sequences of lengths m, m, $m+q$, $m+q$ and n, n, $n+1$, $n+1$, then there are four complementary $(\pm 1, \pm i)$-sequences of length $2(2m+q)(2n+1)$.*

Proof. For sequences $X = (x_1, x_2, \ldots, x_{n+1})$, $Y = (y_1, y_2, \ldots, y_n)$ we write X/Y for the sequence $(x_1, y_1, x_2, y_2, \ldots, x_n, y_n, x_{n+1})$. Let the first sequences be P, Q, R, S

and the second T, U, V, W. The four sequences

$$A = (P, 0_{m+q}, 0_{m+q}, Q), \qquad B = (P, 0_{m+q}, 0_{m+q}, -Q),$$
$$C = (0_m, R, S, 0_m), \qquad D = (0_m, R, -S, 0_m)$$

of length $2(2m+q)$ have zero autocorrelation, as do the four sequences

$$E = V/0_n, \quad F = 0_{n+1}/T, \quad G = W/0_n, \quad H = 0_{n+1}/U$$

having length $2n+1$. Then, the four sequences

$$\begin{gathered} E \otimes A + F^* \otimes B + G^* \otimes C + H^* \otimes D, \\ -E^* \otimes B + F \otimes A + G^* \otimes D^* - H^* \otimes C^*, \\ -E^* \otimes C - F^* \otimes D^* + G \otimes A + H^* \otimes B^*, \\ -E^* \otimes D + F^* \otimes C^* - G^* \otimes B^* + H \otimes A, \end{gathered}$$

have zero autocorrelation. Verifying the claim is straight-forward. □

Furthermore, by Lemma 4.3 the product of four base sequences and a complex Golay pair is a set of four complex base sequences. This will be used further in Chapter 5.

4.3 Complex Golay sequences

According to the previous definition, *complex Golay sequences* are two $(\pm 1, \pm i)$-sequences having zero autocorrelation. Complex Golay sequences appeared first in 1970s under the name *quadriphase pairs* [T2]. By 1980 some computer searches were done that gave examples of such sequences in various lengths not exceeding 13.

The length of any complex Golay sequence is called a *complex Golay number*. Some constructions that worked for Golay sequences can be generalized to the complex case. Denote by $CGS(l)$ the set of all complex Golay pairs of length l.

Theorem 4.9 ([C6]). *If $(A; B) \in CGS(m)$ and $(C; D) \in CGS(n)$, then*

1. $\Big((A \otimes C, B \otimes D^*);\ (A \otimes D, -B \otimes C^*)\Big) \in CGS(2mn)$.

2. If we further assume that A and B are real, then

$$\left(\frac{1}{2}[(A+B)\otimes C+(A-B)\otimes D^*];\frac{1}{2}[(A+B)\otimes D-(A-B)\otimes C^*]\right)\in CGS(mn).$$

There is no construction for direct multiplication of complex Golay numbers, as in the real case. It is known that there is no complex Golay pair of length 15, though both 3 and 5 are complex Golay numbers. Here is another multiplication construction for complex Golay numbers that comes close to this (in a certain respect).

Theorem 4.10 ([C7]). *If g_1, g_2 are complex Golay numbers and g is an even Golay number, then gg_1g_2 is a complex Golay number.*

Prime complex Golay numbers are of special interest. The following complex Golay sequences of prime lengths g are known.

$$\begin{aligned}
g=2:&\qquad A=(1,1),\qquad B=(1,-);\\
g=3:&\qquad A=(1,1,-),\qquad B=(1,i,1);\\
g=5:&\qquad A=(i,i,1,-,1),\qquad B=(i,1,1,i,-);\\
g=11:&\qquad A=(1,i,-,1,-,i,j,-,i,i,1),\\
&\qquad B=(1,1,j,j,j,1,1,i,-,1,-);\\
g=13:&\qquad A=(1,1,1,i,-,1,1,j,1,-,1,j,i),\\
&\qquad B=(1,i,-,-,-,i,-,1,1,j,-,1,j).
\end{aligned}$$

Examples of complex Golay sequences of lengths 11 and 13 appeared first in [HK]. Applying Theorem 4.3, we have the following set of complex Golay numbers.

Corollary 4.11 ([C7]). *All numbers of the form $2^{a+u}3^b5^c11^d13^e$, where $a, b, c, d, e, u \geq 0$, $b+c+d+e \leq a+2u+1$, $u \leq c+e$, are complex Golay numbers.*

In [C7] complex Golay sequences were exhaustively studied for all lengths $g \leq 21$. The numbers shown above are the only prime complex Golay numbers known so far, and numbers presented in Corollary 4.11 are the only known complex Golay numbers. By an exhaustive computer search it has been proven that there is no complex Golay pair of lengths 7, 9, 15, 17, 19, 21. However, other prime complex Golay numbers may exist.

4.4 Normal sequences

Normal sequences of length n are three sequences A, B, C of length n with zero autocorrelation such that A is a (± 1)-sequence, while B and C are supplementary and quasisymmetric $(0, \pm 1)$-sequences. Denote by $NS(n)$ the set of all Normal sequences of length n.

For example, $(A; B; C) \in NS(3)$, where

$$A = (1, 1, -), \qquad B = (1, 0, 1), \qquad C = (0, -, 0),$$

because

$$\begin{aligned} &N_A(1) = 0; && N_B(1) = 0; && N_C(1) = 0; \\ &N_A(2) = -1; && N_B(2) = 1; && N_C(2) = 0. \end{aligned}$$

Any Golay pair $(A; B)$ can be easily transformed to a triple of Normal sequences by adding a third sequence C consisting of all zeros.

Consider the following non-existence theorem for Normal sequences of lengths not exceeding 40.

Theorem 4.12 ([D2]). *For $n \leq 40$, $NS(n) = \emptyset$ if and only if*

$$n \in \{6, 14, 17, 21, 22, 23, 24, 27, 28, 30, 31, 33, 34, 35, 36, 37, 38, 39\}.$$

All other known Normal sequences are of Golay lengths. It also known that there is no Normal sequences of lengths 46, 56, 62, 78, 94. The smallest unresolved length is $n = 41$.

Base sequences may be constructed from Normal sequences, as follows.

Theorem 4.13 ([K2]). *Let $(A; B; C) \in NS(n)$. Then*

$$\Big((A, 1); (A, -); B + C; B - C\Big) \in BS(n, n + 1).$$

Corollary 4.14. *If g is a Golay number, then $BS(g, g + 1) \neq \emptyset$.*

Corollary 4.14 provides sequences suitable for Yang multiplication.

Another form of Yang multiplication allows multiplication of Normal sequences directly with base sequences.

Theorem 4.15 ([Y, K3]). *If $BS(m, m+q) \neq \emptyset$ and $NS(n) \neq \emptyset$, then $BS((2m+q)n, (2m+q)n) \neq \emptyset$.*

Examples of Normal sequences and some facts about them can be found in [K2]. Normal sequences and the above versions of Yang multiplication were used extensively throughout the computer computations described in the next chapter.

4.5 Turyn sequences

Four (± 1)-sequences X, Y, Z, W of lengths $n, n, n, n-1$ are said to be of *Turyn type* (or just *Turyn sequences*), if $N_X(j) + N_Y(j) + 2N_Z(j) + 2N_W(j) = 0$ for all $j > 0$.

For example,

$$\begin{aligned} X &= (-, 1, 1, 1, 1, 1, 1, 1); \\ Y &= (1, -, -, -, 1, 1, 1, -); \\ Z &= (-, 1, -, 1, 1, 1, 1, -); \\ W &= (1, -, 1, 1, -, -, 1); \end{aligned}$$

are Turyn sequences with $n = 8$.

Sequences of Turyn type were first presented by Richard Turyn [T1].

Theorem 4.16 ([T1]). *If X, Y, Z, W are Turyn sequences of lengths $n, n, n, n-1$, then $\Big((Z, W); (Z, -W); X; Y\Big) \in BS(n, 2n-1)$.*

Examples of Turyn sequences for $n = 10, 12, 14, 16, 18, 20, 22, 24$ were presented in [K2]. Further sequences with $n = 26, 28, 30, 32, 34$ are presented in [KS].

Turyn sequences for $n = 36$ provided the construction of a Hadamard matrix of order 428 [K428]. We will need these sequences only for obtaining the corresponding base sequences.

Sequences of Turyn type with $n > 36$ are not known yet.

4.6 Other sequences

The following sequences were not used in our computer search; however, some of their properties can be used in future constructions. We summarize a few important instances briefly here.

T-sequences are four supplementary $(0,\pm 1)$-sequences with zero autocorrelation. Denote by $TS(n)$ the set of all T-sequences of length n.

T-sequences are very helpful in Hadamard matrix construction because of the next theorem.

Theorem 4.17 ([K2]). *If $(T_1;T_2;T_3;T_4) \in TS(n)$ then there exists a Hadamard matrix of order $4n$.*

Proof. Define

$$\begin{aligned} A_1 &= circ(T_1) + circ(T_2) + circ(T_3) + circ(T_4), \\ A_2 &= -circ(T_1) + circ(T_2) + circ(T_3) - circ(T_4), \\ A_3 &= -circ(T_1) - circ(T_2) + circ(T_3) + circ(T_4), \\ A_4 &= -circ(T_1) + circ(T_2) - circ(T_3) + circ(T_4). \end{aligned}$$

Let

$$H = \begin{pmatrix} A_1 & A_2R & A_3R & A_4R \\ -A_2R & A_1 & A_4^\top R & -A_3^\top R \\ -A_3R & -A_4^\top R & A_1 & A_2^\top R \\ -A_4R & A_3^\top R & -A_2^\top R & A_1 \end{pmatrix},$$

where

$$R = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 1 & 0 \\ \vdots & ⋰ & \vdots & \vdots \\ 1 & \cdots & 0 & 0 \end{pmatrix}$$

is an $n \times n$ back diagonal identity matrix. Direct verification shows that H is a Hadamard matrix. □

There is a natural way to construct T-sequences from base sequences.

Theorem 4.18 ([K2])**.** *If $(A;B;C;D) \in BS(n,n+q)$, then*

$$\Big(((A+B)/2, 0_n); ((A-B)/2, 0_n); (0_{n+q}, (C+D)/2); (0_{n+q}, (C-D)/2)\Big) \in TS(2n+q).$$

Corollary 4.19. *If $BS(n,n+q) \neq \emptyset$, then there exists a Hadamard matrix of order $4(2n+q)$.*

There exists another form of Yang multiplication for T-sequences and Normal sequences.

Theorem 4.20 ([Y])**.** *If there exist $TS(t) \neq \emptyset$ and $NS(n) \neq \emptyset$, then $BS(tn,tn) \neq \emptyset$.*

And another construction of T-sequences from Normal and base sequences.

Theorem 4.21 ([Y])**.** *If $BS(m,m+q) \neq \emptyset$ and $NS(n) \neq \emptyset$ then there exist $TS((2m+q)(2n+1)) \neq \emptyset$.*

Ternary complementary pairs (*TCPs*) are pairs of $(0,\pm1)$-sequences with zero autocorrelation. In particular, Golay sequences are a special case of TCPs. A sequence is called *reduced* if its first and last entry is non-zero. A TCP is called reduced if it consists of two reduced sequences. Denote the set of all TCPs of length n and weight w by $TCP(n,w)$. The *deficiency* of a pair in $TCP(n,w)$ is the number $\delta = 2n - w$, which equals the number of zeros in the two sequences. The Golay sequences are exactly TCPs with zero deficiency.

Theorem 4.22 ([C5])**.** *If $w \neq 0$ has a factor congruent to 3 modulo 4, then $TCP(n,w)$ is empty.*

There is also a multiplication construction for TCPs.

Theorem 4.23 ([C5])**.** *Suppose $(A;B) \in TCP(m,w)$ and $(C;D) \in TCP(n,z)$ and one of the pairs is disjoint. Then,*

$$U = A \otimes C + B \otimes D;$$
$$V = A \otimes D^* - B \otimes C^*$$

is a $TCP(mn, wz)$.

Near-normal sequences of even length n are four (±1)-sequences $(A; B; C; D)$ of lengths $n+1$, $n+1$, n, n (n has to be even) with zero autocorrelation, such that $A = (a_1, a_2, \ldots, a_{n+1})$, and $B = (b_1, b_2, \ldots, b_{n+1})$ are related by $b_i = (-1)^i a_i$, $i = 1, \ldots, n+1$. The set of all quadruples of near-normal sequences of length n is denoted by $NN(n)$. Clearly, $NN(n) \subseteq BS(n, n+1)$.

Near normal-sequences were introduced in [Y], where it was conjectured that such sequences exist for all positive even lengths n. It is known that $NN(n)$ is non-empty for all even $n \leq 34$. The classification of all sequences in $NN(n)$ up to $n \leq 30$ was done in [D3].

Yang-type multiplication theorems and further constructions on near-normal sequences can be found in [K4].

Chapter 5

Asymptotic Existence results

Let $p > 1$ be an odd positive number. Denote by t the least positive integer such that a Hadamard matrix of order $2^t p$ exists. Of course, t is a function of p. Since any order of a Hadamard matrix greater than 2, is divisible by four, we have that $t \geq 2$. The Hadamard conjecture states that $t = 2$ for all such p. Similarly, define s to be the least positive such that a complex Hadamard matrix of order $2^s p$ exists. We will give here some upper bounds for t, based on constructions using zero autocorrelation sequences. All bounds come from Theorems 3.10 and 3.11. All logarithms shown will be to the base 2: $\log = \log_2$. All further asymptotic results are based on a computer search which we describe later.

5.1 Asymptotic formulas based on Golay sequences

A simple bound for t can be obtained from Golay sequences. Denote by $b(m)$ the number of units in the binary expansion of m. Consider the binary expansion of the number $(p-1)/2$. Each nonzero digit corresponds to a power of 2. It is known that there exists a Golay pair of length equal to any power of 2. Collect the Golay pairs corresponding to every nonzero digit of expansion of $(p-1)/2$ and apply Theorem 3.10 to them, obtaining a Hadamard matrix. Altogether we have $b\left(\frac{p-1}{2}\right) = b(p)-1$ Golay pairs that give $2b(p)$ sequences of length $2p$ having zero autocorrelation with weight $2p$. So, Theorem 3.10 gives a Hadamard matrix of order $2^t p$, where $t = 2b(p)$. The total number of binary digits in the binary expansion of m is equal to $\lfloor \log m \rfloor + 1$, so $b(m) \leq \lfloor \log m \rfloor + 1$. Thus, we have the first asymptotic bound.

Theorem 5.1 ([C1]). $t \leq 2b(p) \leq 2(\lfloor \log p \rfloor + 1) < 2 \log p + 2$.

A slightly better construction is easily obtained in the following way. Consider the expansion of $(p-1)/2$ to the base 32. Every positive integer between 1 and 31 is equal to the sum of at most three Golay numbers:

$1 = 1,$

$2 = 2,$

$3 = 1 + 2,$

$4 = 4,$

$5 = 1 + 4,$

$6 = 2 + 4,$

$7 = 1 + 2 + 4,$

$8 = 8,$

$9 = 1 + 8,$

$10 = 10,$

$11 = 1 + 10,$

$12 = 4 + 8,$

$13 = 1 + 2 + 10,$

$14 = 4 + 10,$

$15 = 1 + 4 + 10,$

$16 = 16,$

$17 = 1 + 16,$

$18 = 2 + 16,$

$19 = 1 + 2 + 16,$

$20 = 20,$

$21 = 1 + 20,$

$22 = 2 + 20,$

$23 = 1 + 2 + 20,$

$24 = 8 + 16,$

$25 = 1 + 8 + 16,$

$26 = 26,$

$27 = 1 + 26,$

$28 = 2 + 26,$

$29 = 1 + 2 + 26,$

$30 = 10 + 20,$

$31 = 1 + 10 + 20.$

Therefore, each positive integer m is a sum of at most $3\lfloor \log_{32} m \rfloor + 3$ Golay numbers. Hence, for number p there are at most $6\lfloor \log_{32}(\frac{p-1}{2}) \rfloor + 8$ sequences of length $2p$ having zero autocorrelation with weight $2p$. This gives a nice bound for t, still based only on Golay numbers:

Theorem 5.2. $t \leq 6\lfloor \log_{32}(\frac{p-1}{2}) \rfloor + 8 = 6\lfloor \frac{1}{5} \log(\frac{p-1}{2}) \rfloor + 8 \leq \frac{6}{5} \log(\frac{p-1}{2}) + 8$.

This construction will not work on next Golay number base 40, since 39 is not equal to a sum of any three Golay numbers. However, up to 198, any number is a sum of at most four Golay numbers. Therefore, we could repeat the above construction using expansion to the base 160, since 160 is the maximal Golay number less than

199. We get immediately a new bound

$$t \leq 8 \left\lfloor \log_{160} \left(\frac{p-1}{2} \right) \right\rfloor + 10.$$

With the help of a computer we establish some further similar results.

Define h_n to be the least positive integer that is not equal to any sum of up to n Golay numbers and let g_n be the greatest Golay number not exceeding h_n. Then

$$t \leq 2n \left\lfloor \log_{g_n} \left(\frac{p-1}{2} \right) \right\rfloor + 2(n+1) \leq c_n \log \left(\frac{p-1}{2} \right) + 2(n+1),$$

where $c_n = 2n/\log g_n$.

By a computer search we get that $h_7 \geq 233963479$ and $g_7 \geq 224972800$ (we have only inequalities here, since we do not know whether or not we know all Golay numbers). Thus, we have the following theorem:

Theorem 5.3. $t \leq 14 \left\lfloor \log_{224972800}(\frac{p-1}{2}) \right\rfloor + 16 < 0.505 \log(\frac{p-1}{2}) + 16.$

Since any number up to 233963479 is equal to a sum of at most seven Golay numbers, we get that actually for any odd $p \leq 467926957$, the corresponding value t, constructed only using Golay sequences, is at most 16.

The result of our computer search is summarized in Table 5.1.

Table 5.1: Results obtained from Golay sequences

n	$h_n \geq$	$g_n \geq$	$c_n \leq$
2	7	4	2
3	39	32	1.2
4	199	160	1.0926
5	11999	10816	0.7462
6	637399	562432	0.6382
7	233963479	224972800	0.5046

New values of the sequences g_n and h_n, or their asymptotics, would produce great improvement to the asymptotic existence results for Hadamard matrices. However, finding such bounds is a problem in additive number theory that seems to be very difficult. Some ideas about this approach are presented in Chapter 6.

5.2 Hadamard matrices from complex Golay sequences

With complex Golay sequences there is more freedom than in the real case. Define $c_n^{(k)}$ to be the smallest positive integer divisible by k which can not be presented as a sum of up to n complex Golay numbers. By Theorem 4.10, we have $c_n^{(gk)} \geq gc_n^{(k)}$ for every Golay number g and positive integers k, n.

An asymptotic result giving $s \leq 4\left\lfloor \frac{\log(p-1)}{10} \right\rfloor + 5$, based mainly on two complex Golay pairs, was established by Craigen, Holzmann and Kharagani in [C2]. In particular, it was calculated that $c_2^{(2)} \geq 1598 = 2 \cdot 799$. We do some computations with three and four complex Golay pairs to present another asymptotic bound. Results are presented in Table 5.2.

Table 5.2: Results obtained from complex Golay sequences

n	$c_n^{(1)} \geq$	$c_n^{(2)} \geq$	$c_n^{(4)} \geq$	$c_n^{(8)} \geq$	$c_n^{(16)} \geq$
2	87	1598	3836	7672	15344
3	24175	1657166	26120804	186128248	1255960976
4	77217575	2^{30}	2^{31}	2^{32}	2^{33}

Similarly, we have only lower bounds for these numbers, since we do not know all complex Golay numbers yet.

Consider the expansion of $q = (p-1)/2$ to the base $2^{26} = 67108864$:

$$q = q_0 + 2^{26}q_1 + 2^{26\cdot 2}q_2 + \cdots + 2^{26\cdot s}q_s,$$

where $s = \left\lfloor \frac{1}{26} \log q \right\rfloor$. From the bounds above, we get that q_0 equals to a sum of at most four complex Golay numbers. Since $c_3^{(16)} \geq 2^{30}$ and $2^{26i}q_i = 2^{26i-4} \cdot 16q_i$ for $i > 0$, $2^{26\cdot i}q_i$ equals to a sum of at most three complex Golay numbers for all $i > 0$. Thus, at most $6\left\lfloor \frac{1}{26} \log q \right\rfloor + 8$ sequences are needed to construct a set of complementary sequences of total length q required in Theorem 3.11. We have the following result.

Theorem 5.4. $t \leq 6\left\lfloor \frac{1}{26} \log(\frac{p-1}{2}) \right\rfloor + 11 \leq \frac{3}{13} \log(\frac{p-1}{2}) + 11.$

This construction shows an improvement over the previous asymptotic bound featuring constant 3/8 times the logarithm [C8].

5.3 Hadamard matrices from all complementary sequences considered

Using more sequences with zero autocorrelation a better asymptotic bound is constructed. As before, we rely on computer computations.

Previous computations with only three complex Golay pairs required a huge amount of memory. We consider sets of at most six complementary complex sequences. Improvement of the following results using eight sequences does not seem to be feasible yet, since it deals with very big numbers.

Complex Golay pairs are added to complex base sequences. In turn, complex base sequences are constructed from Normal, Turyn, Golay and complex Golay sequences. Theorems 4.7 and 4.15 regarding Yang multiplication were used extensively during the computations.

Define the following sets of integers:

1. G: the set of all Golay numbers;

2. C: the set of all complex Golay numbers;

3. N: the set of lengths of Normal sequences;

4. D: the set of all integers $2n+1$, such that base sequences of lengths n, n, $n+1$, $n+1$ exist;

5. B: the set of all integers $2n+q$, such that base sequences of lengths n, n, $n+q$, $n+q$ exist;

6. T: the set of all integers n, such that Turyn sequences of lengths n, n, n, $n-1$ exist;

7. S_{2k}: the set of all lengths s such that $2k$ complex complementary sequences $X_1, X_2, \ldots, X_{2k}$ of total length $2s$ exist, where X_{2i} and X_{2i-1} have the same length for every $1 \leq i \leq k$ (e.g. S_4 is the set of numbers $2n+q$, such that $CBS(n, n+q) \neq \emptyset$).

Small-case letters g, c, n, d, b, t respectively are used to indicate an arbitrary element in each of the first 6 sets. Subscripts are used to distinguish more than one number from the same set.

For any sets A, B of positive integers, define $A+B$ to be the set containing all sums $a+b$, where $a \in A$, $b \in B$. Similarly, for any integers p, q, define $pA+q$ as a set containing all numbers $pa+q$, $a \in A$.

The following properties of sets G, C, N, D, B, T were used during our computations. All of them were described in the previous chapter.

1. $0,\ 1,\ 2,\ 10,\ 26,\ g_1g_2 \in G$;
2. $0,\ 1,\ 2,\ 3,\ 5,\ 11,\ 13,\ c_1c_2g \in C$;
3. $\{2m+1 | 1 \leq m \leq 38\} \subseteq D,\ 2n+1 \in D$;
4. $3,\ 5,\ 7,\ 9,\ 11,\ 12,\ 13,\ 15,\ 18,\ 19,\ 25,\ 29,\ g \in N$;
5. $\{2m | 5 \leq m \leq 18\} \subseteq T$;
6. $d,\ 3t-1,\ 2nb,\ 2bd \in B$
7. $c_1+c_2,\ cb \in S_4$;

Since D contains all odd numbers up to 77, and S_4 contains any product of such number with any Golay number, without any computer computations we can see that all numbers up to 77 belong to S_4. Therefore, with expansion to the base 64 we have an asymptotic bound

$$t \leq 4 \left\lfloor \log_{64}\left(\frac{p-1}{2}\right) \right\rfloor + 7 \leq \frac{2}{3} \log\left(\frac{p-1}{2}\right) + 7.$$

This bound is similar to one given in [C1].

Let $b_n^{(k)}$ the smallest positive integer divisible by k that does not belong to S_{2n}.

With the help of computer computations we establish some lower bounds for numbers $b_n^{(k)}$. Computations are done in the following way. The set S_4 is constructed first, and then complex Golay numbers are added to all numbers in S_4. We consider numbers, which are less than the upper bound M, which is taken to be slightly greater than 2^{32}. Here is a sketch of our algorithm.

1. Initialize all lists of integers G, C, N, D, T, S_4, S_6 to be empty;

2. Add 1, 2, 10, 26 to G. Fill G further by its multiplicative property (prop. 1);

3. Add 1, 2, 3, 5, 11, 13 to C. Fill C further by its multiplicative property (prop. 2);

4. Add numbers 3, 5, 7, 9, 11, 12, 13, 15, 18, 19, 25, 29 to N. Add Golay numbers to N (prop. 4);

5. Add all odd lengths between 3 and 77 to D. Add all numbers from $2N+1$ to D (prop. 3);

6. Add all even numbers between 10 and 36 to T (prop. 5);

7. Add all numbers from D to the empty list S_4. Add all numbers from $3T-1$ to S_4 (prop. 6);

8. Add all numbers of the form gb to S_4, where $g \in G$, $b \in S_4$ (prop. 7).

9. Add all sums $c_1 + c_2$, where $c_1, c_2 \in C$ to S_4 (prop. 7).

10. Add all numbers of the form $(2n+1)b$ to S_4, where $b \in S_4$, $n \in N$ (prop. 6,7).

11. Add all numbers of the form db to S_4, where $b \in S_4$, $d \in D$ (prop. 6,7).

12. Construct S_6 as $S_4 + C$;

13. Obtain bounds for numbers $b_n^{(k)}$ from S_6 and S_4.

Table 5.3: Results obtained from all complementary sequences considered

n	$b_n^{(1)} \geq$	$b_n^{(2)} \geq$	$b_n^{(4)} \geq$	$b_n^{(8)} \geq$
2	127	1934	4124	8248
3	142919	61161358	2^{32}	2^{33}

Bounds for $b_n^{(k)}$ obtained by our computations are presented in Table 5.3.

Consider the expansion of $q = (p-1)/2$ to the base 2^{30}:

$$q = q_0 + 2^{30}q_1 + 2^{30\cdot 2}q_2 + \cdots + 2^{30\cdot s}q_s,$$

where $s = \left\lfloor \frac{1}{30} \log q \right\rfloor$. Then q_0 is equal to a half of the total length of at most five pairs of sequences, since every even number up to 2^{30} is a sum of four complex Golay numbers. Since $2^{30\cdot i}q_i = 2^{30\cdot i-2} \cdot 4q_i$ and $b_3^{(4)} \geq 2^{32}$, all numbers $2^{30\cdot i}q_i$, $i > 0$ are equal to a half of the total length of at most six complex complementary sequences. Therefore, q is equal to a half of the total length at most $6 \left\lfloor \frac{1}{30} \log q \right\rfloor + 10$ complex complementary sequences. We now apply Theorem 3.11 to obtain a new bound from all sequences discussed here.

Theorem 5.5. $t \leq \frac{1}{5} \log(\frac{p-1}{2}) + 13$.

A similar result regarding the existence of complex Hadamard matrices can be obtained in the same way.

Chapter 6

Thoughts about further development

Our computations revealed that among all complementary sequences the complex Golay sequences are most useful for us. Since the last computer search for them was done more than ten years ago, it looks as if a new search may produce new results.

Another search is needed for Base sequences. Examples of $BS(m, m+1)$ for $m = 36,\ 37,\ 38$ were found only recently with the help of massive computer computations. It seems that new base sequences will be presented in the near future after similar computer development. Moreover, the following "Base sequence conjecture" implies the Hadamard conjecture:

Conjecture 6.1 ([D4])**.** *For any positive integer n, $BS(n, n+1)$ is not empty.*

This conjecture is verified to be true for all $n \leq 38$ [D2]. Similarly, there is a "T-conjecture" regarding T-sequences:

Conjecture 6.2 ([D2])**.** *For any positive integer n, $TS(n)$ is not empty.*

The T-conjecture follows from the Base sequence conjecture and also implies the Hadamard conjecture. It has been verified to be true for all $n \leq 100$ apart from two undecided cases $n = 79$ and $n = 97$ [D2].

However, any bound of the form $t \leq c \log p + d$ (t is defined in Chapter 5) even in the light of Theorem 5.3 looks too crude. The following additive number theory development could improve such bounds considerably.

Let $n_1, n_2, \ldots, n_k$ be positive integers. Define $S(n_1, n_2, \ldots, n_k)$ to be the smallest multiplicatively closed set containing $n_1, n_2, \ldots, n_k$ and 1. Further, for any set of positive integers S, define $l_m(S)$ to be the smallest positive integer that is not equal to any sum of at most m numbers from S, i.e.,

$$l_m(S) = \min\left(\mathbb{N} \setminus \bigcup_{n=1}^{m} (\underbrace{S + S + \cdots + S}_{n})\right),$$

where $\mathbb{N}$ denotes the set of all positive integers.

For example, if $k = 1$ and $S = S(2) = \{1, 2, 2^2, 2^3, \ldots\}$, then $l_m(S) = 2^{m+1} - 1$, since this is the smallest integer that has m units in its binary expansion. If $S = S(2,3) = \{1, 2, 3, 4, 6, 8, 9, 12, 16, 18, \ldots\}$, then the first values of the sequence $l_m(S)$ are $5, 23, 431, 18431, 3448733, 1441896119, \ldots$ [BI]. We did not establish any results regarding asymptotics of this sequence; however, it looks as if $l_m(S(2,3))$ is growing much faster than any exponent. Moreover, it seems that $\exp \frac{m(m+1)}{2}$ is very close to this sequence.

Asymptotics for $l_m(S(2,10,26))$ are of special interest for us, since $S(2,10,26) \subseteq G$, where G is the set of all Golay numbers.

Assume that $l_m(S(2,10,26)) \geq Ca^{n^2}$ for some positive real constants C, a, where $a > 1$. Then any positive integer q equals to a sum of at most $\left\lceil \sqrt{\log_a(q/C)} \right\rceil$ Golay numbers. Therefore, such an asymptotics for $l_m(S(2,10,26))$ implies existence of a Hadamard matrix of order $2^t p$, for all

$$t \geq 2\left\lceil \sqrt{\log_a\left(\frac{p-1}{2C}\right)} \right\rceil + 2$$

by Theorem 3.10. This bound would be considerably better than any existing asymptotic bound for t.

However, we did not manage to prove any asymptotic results of this kind. Similar development involving complex Golay sequences or complex base sequences could produce significant improvement too.

All the new results are described in Chapter 5. In this thesis a new statement regarding asymptotic existence of Hadamard matrices was proved. A similar result regarding asymptotic existence of complex Hadamard matrices can be proven also using the results of our computer search.

Bibliography

[BI] V. Berthe and L. Imbert, *Diophantine Approximation, Ostrowski Numeration and the Double-Base Number System*, Discrete Mathematics and Theoretical Computer Science, vol. 11:1, (2009), 153-172.

[BF] P. B. Borwein and R. A. Ferguson, *A complete description of Golay pairs for lengths up to 100*, Mathematics of Computation, 73 (2003), 967–985.

[C1] R. Craigen, *Signed groups, sequences and the asymptotic existence of Hadamard matrices*, J. Combinatorial theory, A 71, (1995), 241–254.

[C2] R. Craigen, W. H. Holzmann and H. Kharagani, *On the asymptotic existence of complex Hadamard matrices*, Journal of Combinatorial Designs, 5, (1996), 319–327.

[C3] R. Craigen and H. Kharagani, *Hadamard matrices from weighing matrices via signed groups*, Designs, Codes and Cryptography, 12, (1997), 49–58.

[C4] R. Craigen, *Boolean and ternary complementary pairs*, J. Combinatorial theory, A 104, (2003), 1–16.

[C5] R. Craigen and C. Koukouvinos *A theory of ternary complementary pairs* J. Combinatorial theory, A 96, (2001), 358–375.

[C6] R. Craigen, *Complex Golay sequences*, J. of Comb. Math. and Comb. Comp., 15, (1994), 161–169.

[C7] R. Craigen, W. Holzmann, H. Kharagani, *Complex Golay sequences: structure and applications*, Discrete mathematics, 252, (2002), 73–89.

[C8] R. Craigen, D. Tiessen, *Improved asymptotic existence results for Hadamard matrices*, (unpublished).

[D1] D. Dokovic, *Some new near-normal sequences*, arXiv:0907.31290v1.

[D2] D. Dokovic, *On the base sequence conjecture*, arXiv:1003.1454.

[D3] D. Dokovic, *Classification of near-normal sequences*, Discrete Mathematics, Algorithms and Applications, 1, No. 3 (2009), 389399, arXiv:0903.4390v2.

[D4] D. Dokovic, *Aperiodic complementary quadruples of binary sequences*, J. of Comb. Math. and Comb. Comp. 27 (1998), 3-31. Correction: ibid 30 (1999), p. 254.

[E] S. Eliahou, M. Kervaire, and B. Saffari, *A new restriction on the lengths of Golay complementary sequences*, J. Combinatorial theory, 55 (1990), 49–59.

[G] A. Geramita, J. Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, Marcel Dekker, inc. 1979, 460p.

[G1] M. J. E. Golay, *Multislit spectroscopy*, J. Opt. Soc. Amer. 39: 437-444, (1949).

[G2] M. J. E. Golay, *Complementary series*, IRE Trans. Inform. Theory, IT-7, pp. 82-87, Apr. 1961.

[H] J. Hadamard, *Résolution d'une question relative aux déterminants*, Bull. Sciences Math. (2), 17 (1893), 240–246.

[HJ] R. A. Horn, C. R. Johnson, *Topics in Matrix Analysis*, Cambridge University Press, 1991.

[HK] W. H. Holzmann and H. Kharaghani, *A computer search for complex Golay sequences*, Australasian J. Combinatorics, 10 (1994), 251258.

[Hr] K. J. Horadam, *Hadamard Matrices and their Applications*, Princeton University Press, 2007, 263 p.

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

[K1] C. Koukouvinos, S. Kounias, and K. Sotirakoglou, *On base and Turyn sequences*, Mathematics of Computation, 55, (1990), 825–837.

[K2] C. Koukouvinos, S. Kounias, J. Seberry, C. H. Yang and J. Yang, *On sequences with zero autocorrelation*, Des. Codes Cryptogr. 4 (1994), 327-340.

[K3] C. Koukouvinos, J. Seberry, *Addendum to further results on base sequences, disjoint complementary sequences, $OD(4t; t, t, t, t)$, and the excess of Hadamard matrices*, Congr. Numer., 82 (1991), 97-103.

[K4] C. Koukouvinos, S. Kounias, J. Seberry, C. H. Yang and J. Yang, *Multiplication of sequences with zero autocorrelation*, Austral. J. Combin. 10 (1994), 5-15.

[K5] C. Koukouvinos, *Base sequences*, `http://www.math.ntua.gr/~ckoukouv/`

[K428] H. Kharaghani, B. Tayfeh-Rezaie, *A Hadamard matrix of order 428*, Journal of Combinatorial Designs, 13, (6), 435-440.

[KS] S. Kounias and K. Sotirakoglou, *Construction of orthogonal sequences*, Proceedings of the 14th Greek Statistical Conference, 2001, 229-236, (in Greek).

[MH] M. Hall, Jr., *Note on the Mathieu group M_{12}*, Arch. Math. 13 (1962), 334-340.

[S1] J. S. Wallis, *On the existence of Hadamard matrices*, J. Combin. Theory A 21, (1976), 188–195.

[Sv] J. J. Sylvester, *Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers*, Philosophical Magazine, 34, 461-475, (1867)

[T1] R. J. Turyn, *Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings*, J. Combin. Theory (A) 16 (3): 313-333, 1974.

[T2] R. J. Turyn, *Complex Hadamard matrices*, Combinatorial Structures and Their Applications, 435–437, New York, 1970.

[Y] C. H. Yang, *On composition of four-symbol δ-codes and Hadamard matrices*, Proc. Amer. Soc. 107 (1989), 763–776.