2001

Boolean functions, Hadamard matrices, orthogonal designs applicable to security and communication

Tianbing Xia
University of Wollongong

Recommended Citation
NOTE

This online version of the thesis may have different page formatting and pagination from the paper copy held in the University of Wollongong Library.

UNIVERSITY OF WOLLONGONG

COPYRIGHT WARNING

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site. You are reminded of the following:

Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material. Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.
Boolean Functions, Hadamard Matrices, Orthogonal Designs Applicable to Security and Communication

A thesis submitted in fulfillment of the requirements for the award of the degree

Doctor of Philosophy

from

UNIVERSITY OF WOLLONGONG

by

Tianbing Xia

School of Information Technology and Computer Science
October 2001
© Copyright 2001
by
Tianbing Xia
All Rights Reserved
Dedicated to
my mother, father, wife
Declaration

This is to certify that the work reported in this thesis was done by the author, unless specified otherwise, and that no part of it has been submitted in a thesis to any other university or similar institution.

______________________________
Tianbing Xia
October 9, 2001
This thesis is about Boolean functions and their cryptographic properties, Hadamard matrices, orthogonal designs, and their applications.

An original definition of Boolean functions and their properties are given. After an introduction to the background of Boolean functions, different cryptographic properties of Boolean functions are described.

Bent functions play a most important role in cryptography. Several classes of bent functions are introduced. Some methods of construction high nonlinearity and balanced Boolean functions base on bent functions are described. In the thesis, the author shows some applications on Boolean functions. The author also introduced the relationship between coding theory and Boolean functions.

Hadamard matrices are introduced after Boolean functions. In the thesis the author shows the definitions and relationship between Hadamard matrices and difference sets (DS), supplementary difference sets (SDS), orthogonal designs (OD) and symmetric balanced incomplete block design (SBIBD). The author also re-states some methods of constructing Hadamard matrices. Since Hadamard matrices be sparked the interest in 1970s, Hadamard matrices can be implemented as a base in error correcting, data communication, cryptography, etc.

The thesis includes a preliminary section orthogonal designs, where the author gives some known results about orthogonal designs. Amicable orthogonal designs are also reminded in the thesis. Some applications of orthogonal designs in code theory are introduced.

New results about construction cubic homogeneous bent functions on $V_{2n}$ for all $n \geq 3$, $n \neq 4$ are given. There is no homogeneous bent function of degree $n$ exists on $V_{2n}$ for $n \geq 4$. New results about homogeneous functions with high nonlinearity in odd space are found.

Some new families of $C$–partitions and $T$–matrices are given, which can construct new Hadamard matrices. New results about $T$–matrices, difference sets, SBIBD and
Hadamard matrices are described.

The author also gives some new infinite families of orthogonal designs using Kharaghani arrays.
The author has some papers published and submitted. The papers are listed below and show how much work the author did in thesis.


- Jennifer Seberry, Tianbing Xia, Josef Pieprzyk and Chris Charnes, Homogeneous Bent Functions of degree $n$ in $2n$ variables do not exist for $n > 2$ (submitted).

- Jennifer Seberry, Tianbing Xia, Chenxin Qu and Josef Pieprzyk, Construction of Highly Non-linear Cubic Homogeneous Boolean Functions on $GF(2)^{2n+1}$ and their Properties (submitted).

- Tianbing Xia, Jennifer Seberry and Josef Pieprzyk, Regular Hadamard Matrix, Maximum Excess and SBIBD (submitted).

- Jennifer Seberry and Tianbing Xia, Some Infinite family of Orthogonal Design (prepared).
Symbols

\( GF(2) \) \hspace{1cm} \text{Galois field with parameter 2.}
\( V_n \) \hspace{1cm} An \( n \) entries of \( GF(2) \), also denoted as \( GF(2)^n \).
\( \alpha = (\alpha_1, \cdots, \alpha_n) \) \hspace{1cm} An vector in \( V_n \).
\( N_f \) \hspace{1cm} Nonlinearity of the Boolean functions \( f(x) \) on \( V_n \).
\( \xi, \eta, \cdots \) \hspace{1cm} Sequences of Boolean functions.
\( l_i \) \hspace{1cm} A sequence of a linear Boolean functions.
\( W(\alpha) \) \hspace{1cm} Hamming weight of the vector \( \alpha \), \( W(\alpha) = \sum_{i=1}^{n} \alpha_i \).
\( A \times B \) \hspace{1cm} Kronecker product of matrices \( A \) and \( B \).
\( \odot \) \hspace{1cm} Inner product.
\( \oplus \) \hspace{1cm} Boolean addition.
\( \ominus \) \hspace{1cm} Sets subtraction.
\( PC(k) \) \hspace{1cm} The \( k \)-th order propagation criteria.
\( SAC \) \hspace{1cm} Strict avalanche criteria, the order of \( PC \) is 1.
\( H_n \) \hspace{1cm} Hadamard matrix of order \( n \).
\( R_n \) \hspace{1cm} The back diagonal identity matrix of order \( n \).
\( I_n \) \hspace{1cm} The identity matrix of order \( n \).
\( J_n \) \hspace{1cm} The square matrix of order \( n \), which all entries are one.
\( BIBD \) \hspace{1cm} Balanced incomplete block designs.
\( PBIBD \) \hspace{1cm} Partial balanced incomplete block design.
\( SBIBD \) \hspace{1cm} Symmetric balanced incomplete block design.
\( DS \) \hspace{1cm} Difference set.
\( SDS \) \hspace{1cm} Supplementary difference sets.
\( OD(n; p_1, \cdots, p_u) \) \hspace{1cm} Orthogonal designs with \( u \) variables of order \( n \).
\( AOD \) \hspace{1cm} Amicable orthogonal designs.
\( DES \) \hspace{1cm} The Data Encryption Standard.
\( AES \) \hspace{1cm} The Advanced Encryption Standard.
\( CDMA \) \hspace{1cm} the code division multiple access.
I would like to thank

- Professor Jennifer Seberry, my supervisor, for suggesting a suitable problem, explaining, discussing, reading drafts of the thesis and always being a good friend. Without her invaluable guidance and assistance this study would not have been possible.

- Associate professor Josef Pieprzyk, for discussing, give me suggestions.

- Professor Reihaneh Safavi-Naini for the help she gave me whenever I needed it.

- The Center for Computer Security Research, for all their help and support during my work: Xianmo Zhang, Chenxin Qu, Willy Susilo.

- The staff of the department of School of IT and CS at the University of Wollongong, for their help and providing a pleasant workplace.

- Ms. Jasmine Croll, who proofread and helped the exposition.
Contents

Abstract v
Publications vii
Symbols viii
Acknowledgements ix

1 Introduction 1
  1.1 Contents and contribution of the thesis 2

2 Boolean Bent Functions 4
  2.1 Background 5
  2.2 “Good” criteria of Boolean functions 10
  2.3 Boolean bent functions and construction 14
  2.4 Classes of Boolean bent functions 15

3 Balanced Boolean Function with High Nonlinearity 23
  3.1 On $V_{2n+1}$ 24
  3.2 On $V_{2n}$ 25
  3.3 Applications on Boolean functions 28

4 Hadamard Matrices and Block Designs 33
  4.1 Definitions 33
  4.2 History 36
  4.3 Overview of construction of Hadamard matrices 37
  4.4 Background 38

5 Construction of Hadamard matrices and their applications 41
  5.1 Williamson type Hadamard matrices 41
5.2 Goethals-Seidel type Hadamard matrices ........................................ 46
5.3 Other results .............................................................. 48
5.4 Applications of Hadamard matrices ........................................... 50

6 Orthogonal designs ............................................................................. 55
  6.1 Preliminary and definition ......................................................... 56
  6.2 Construction of orthogonal designs ........................................... 59

7 Amicable orthogonal designs ................................................................. 63
  7.1 Introduction ............................................................................ 63
  7.2 Short amicable sets ................................................................. 66
  7.3 Construction of amicable orthogonal designs ...................... 69
  7.4 Applications of orthogonal designs and codes .................... 72

8 Homogeneous Boolean Functions .......................................................... 74
  8.1 Background ........................................................................... 75
  8.2 Cubic homogeneous Boolean bent functions ....................... 81
  8.3 Fourier transform of homogeneous bent function ............. 84
  8.4 The degree of homogeneous bent functions is less than $n$ on $V_{2n}$, $n \geq 4$. 87
  8.5 Homogeneous Boolean functions with high nonlinearity on $V_{2n+1}$ ... 93
    8.5.1 Homogeneous Boolean functions with high nonlinearity .... 97
    8.5.2 Cubic homogeneous functions on $V_5$ ......................... 103
    8.5.3 Cubic homogeneous functions on $V_7$ ......................... 103
    8.5.4 On $V_{2n+1}$, $n > 4$ .............................................. 107
    8.5.5 Properties of matrix transformation ....................... 108

9 A Family of C-Partitions and T-Matrices .............................................. 109
  9.1 Introduction ........................................................................... 109
  9.2 The definitions ....................................................................... 110
  9.3 The Relationship .................................................................... 110
  9.4 Constructing C-partitions ......................................................... 115

10 Regular Hadamard Matrix, Maximum Excess and SBIBD ...................... 120
  10.1 Background ......................................................................... 120
  10.2 Construction of SBIBD from SDS ....................................... 122
  10.3 Construction of SBIBD from SDS and T-matrices ............ 124
11 Some Infinite families of Orthogonal Design .......................... 131
11.1 Background .............................................................. 131
11.2 Construction of $OD(8(n + r + s); 2, 2, 2, 2k, 2k, 2k, 2k)$, $r \geq 1$, $s \geq n$ 133
11.3 Construction of $OD(8n; 1, 1, 1, 1, \frac{1}{2}k, \frac{1}{2}k, \frac{1}{2}k, \frac{1}{2}k)$ ................. 135
11.4 Construction of Orthogonal Designs from $T$-matrices and Williamson-type matrices ........ 137

A Results on cubic homogeneous functions on $V_5$ with nonlinearity equal 12 .......................... 138

B Some results on cubic homogeneous functions on $V_7$ with nonlinearity equal 56 ................. 140

Bibliography .......................... 153
<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Hadamard matrices of the Williamson type</td>
<td>52</td>
</tr>
<tr>
<td>5.2</td>
<td>Hadamard matrices of the Williamson type</td>
<td>53</td>
</tr>
<tr>
<td>5.3</td>
<td>Hadamard matrices of the Williamson Type</td>
<td>54</td>
</tr>
<tr>
<td>7.1</td>
<td>Disjoint amicable circulant matrices constructed from sequences</td>
<td>68</td>
</tr>
<tr>
<td>7.2</td>
<td>Order and type for 2-SCAS for all $n \geq 1$</td>
<td>68</td>
</tr>
<tr>
<td>7.3</td>
<td>$4-SCAS(n; p_1, p_2, p_3, p_4)$, $n$ small, $n \geq 1$</td>
<td>70</td>
</tr>
</tbody>
</table>
List of Figures

4.1 Relationship between SBIBD and Hadamard matrices. . . . . . . . . . . . . 38
Cryptography can be traced back to long ago. In ancient times, almost all ancient civilizations developed some kind of cryptography. Kahn [55] gives an exciting insight into the secret communication starting from ancient to modern times.

Traditional cryptography is concerned with communications in secure and usually secret form. It includes both cryptography and cryptanalysis. The former involves the study and application of the principles and techniques by which information is rendered unintelligible to all but the intended receiver, the latter is the science and art of solving cryptosystems to recover such information (The New Encyclopedia Britannica, vol. 3, page 768, 1988).

Modern cryptology focuses its attention on the design and evaluation of a wide range of methods and techniques for information protection, which covers not only information security, but also authentication, integrity, verifiability, non-repudiation and many more other specific security countermeasures.

Cryptography provides many tools to implement the information protection request. The collection of basic tools includes encryption algorithms, authentication codes, one-way functions, hashing functions, secret sharing schemes, signature schemes, key distribution systems, etc.

Shannon in his seminal work [131] laid the theoretical foundations of modern cryptography. He used information theory to analyze ciphers. He also considered the so-called product ciphers. Product ciphers use small substitution boxes connected by large permutation boxes. Substitution boxes (S-boxes) are controlled by a relatively short cryptographic key. They provided confusion because of the unknown secret key. The structure of permutation boxes (P-boxes) is fixed and cause diffusion. Product ciphers are termed substitution-permutation or S-P networks.

Feistel [30] used the S-P networks concept to design the Lucifer encryption algorithm. The Data Encryption Standard (DES) was developed from Lucifer (see [89]) and became a standard for encryption in banking and other non-military applications.
Cryptographic hashing became an important component of cryptographic primitives especially in the context of efficient generation of digital signatures. MD4 [102] and its extended version MD5 [103] are examples of the design which combines Festel structure with C language bitwise operations for fast hashing.

1.1 Contents and contribution of the thesis

In chapter 2 and 3, Boolean bent functions and "good" criteria Boolean functions are characterized from the view of cryptography. The author has restated and reproved, giving examples, previously known lemmas and theorems. In the section 3.3 the author shows some implementations which are using the Boolean functions to design their cipher algorithms.

In chapter 4 the author reviews the history of Hadamard matrices and discusses why Hadamard matrices play an important role in computer communication and security. The author also overviews the construction of Hadamard matrices.

In chapter 5 the author discusses the Williamson method and some other methods of the construction of Hadamard matrices. At the end of the chapter, the author shows that Hadamard matrix implemented in the area of error correcting codes, computer and communication security.

Orthogonal designs plays an important role in computer security. It is related to Hadamard matrices. In chapter 6 the author discusses preliminary results on orthogonal designs, and states some known construction of orthogonal designs.

In chapter 7 the author studies the most important construction of orthogonal designs - amicable orthogonal designs. Goethals-Seidel arrays and Kharaghani arrays are very useful in the construction of amicable orthogonal designs.

Various codes are used in many areas. In section 7.4 the author give some examples of applications on coding theory.

In chapter 8 the author studies the homogeneous Boolean functions which are very useful in cryptography, particular in hashing functions. In section 8.2, the author gives constructions of cubic homogeneous Boolean functions on all high spaces $V_{2n}$ when $n \geq 3$ and $n \neq 4$ ([124]). In section 8.4, the author proved that Homogeneous Bent Functions of degree $n$ in $2n$ variables do not exist for $n > 3$ ([125]). In section 8.5, the author also studied homogeneous Boolean functions with high nonlinearity and without linear structures in the odd space in which Boolean bent functions do not exist ([126]). The author proved that cubic homogeneous Boolean functions without
linear structures and with high nonlinearity equal $2^{2n} - 2^n$ exists on $V_{2n+1}$ for $n \geq 2$, $n \neq 4$. 80 percent of the work of this chapter is contributed by the author.

In chapter 9 the author studies $C$—partitions and $T$—matrices which are related to the construction of Hadamard matrices. In this chapter the author gives an infinite family of $C$—partitions, $T$—matrices and Hadamard matrices ([161]). 40 percent of the work is contributed by the author.

In chapter 10 the author studies Hadamard matrices, SBIBD, SDS, DS and $T$—matrices. The author gives new constructions of $SBIBD(4k^2, 2k^2 + k, k^2 + k)$ from SDS and $T$—matrices ([162]). 50 percent of the work is done by the author.

In chapter 11 the author uses Goethals-Seidel arrays and Kharaghani arrays, and constructs some new infinite families of orthogonal designs. 70 percent of the work is done by the author.
Chapter 2

Boolean Bent Functions

Many secret-key block ciphers are based on iterating a substitution function several times. The security of such iterated block ciphers depends mainly on the "strength" of the substitution function. It is known that the nonlinearity of the substitution function is curtailed for the "strength" of the iterated block cipher.

Boolean functions have always been in the center of interest of the designers of cryptographic algorithms. Shannon [131] was the first who observed that the design of a secure cipher amounts to the design of two components from which one provides confusion (a simple substitution block or S-box) and the other introduces diffusion (a permutation block or P-box). Rothaus [104], the first one who introduced and studied bent functions in the 1960s, discovered a class of bent functions whose approximations by a linear (or affine) Boolean functions are always the worst possible.

The linear cryptanalysis invented by Matsui [79], proved that high nonlinearity of an S-box is an essential cryptographic property. The basic idea of linear cryptanalysis is to find a linear relation among the plain text, cipher text and key bits. Such a relation usually occurs by a low nonlinearity of substitutions in block cipher. More precisely, S-boxes with low nonlinearity may still be used to design a cryptographically strong cipher but the number of necessary iterations could be excessively high making the cipher very slow. Needless to say, to design a fast cryptographic algorithm (with a small number of iterations), highly nonlinear S-boxes must be used.

The most successful and widely used block cipher has been the DES algorithm which was designed in the seventies last century. However, the key size being only 56 bits and is too small. In recent years the DES has been extensively analyzed in order to capture its properties of strength. Special attention has been focused on the nonlinearity properties of the round function, which is composed of permutations and eight small parallel substitution transformations, the S-boxes. It seems that the security can be increased only by the size of S-boxes or possibly by replacing the set of small parallel substitutions by one large transformation with desirable properties.
2.1 Background

Let $V_n = GF(2)^n$ be the set of all vectors with $n$ binary co-ordinates. $V_n$ contains $2^n$ different vectors from $\alpha_0 = (0,0,\ldots,0)$, $\alpha_1 = (0,\ldots,0,1)$, \ldots, $\alpha_{2^n-1} = (1,1,\ldots,1)$. A Boolean function $f : V_n \rightarrow GF(2)$ assigns binary values to vectors from $V_n$. Let $x = (x_1,\ldots,x_n)$ and $y = (y_1,\ldots,y_n)$ be two vectors in $V_n$. Throughout the thesis the following notations are used:

- **the inner product** of $x$ and $y$ defined as
  $$\langle x, y \rangle = x \odot y = x_1y_1 \oplus \cdots \oplus x_ny_n = \sum_{i=1}^{n} x_iy_i.$$

- **the inner addition** of $x$ and $y$ given by
  $$x \oplus y = (x_1 \oplus y_1, \ldots, x_n \oplus y_n).$$

Note that inner addition is equivalent to bit-by-bit XOR addition;

- **the extension** of vector $x \in V_n$ by a vector $y \in V_m$ is defined as
  $$x \otimes y = (x_1,\ldots,x_n,y_1,\ldots,y_m).$$
  The vector $x \otimes y \in V_{n+m}$.

- **the Hadamard product** of vector $a = (a_1,\ldots,a_n)^T$ and vector $b = (b_1,\ldots,b_n)^T$ given by
  $$a \ast b = (a_1b_1,\ldots,a_nb_n)^T$$
  where the symbol "$T$" means transpose of the vector or matrix.

**Definition 2.1 (Sequence and Truth table)** Let $f(x)$ be a Boolean function on $V_n$, $\alpha_i$, $0 \leq i \leq 2^n - 1$ as the vectors on $V_n$. The $(1,-1)$-sequence defined by $((-1)^{f(\alpha_i)}, \ldots, (-1)^{f(\alpha_{2^n-1})})$ is called the sequence of $f(x)$. The binary sequence defined by $(f(\alpha_0),\ldots,f(\alpha_{2^n-1}))$ is called the truth table of $f(x)$.

A Boolean function $f(x)$ on $V_n$ is called an affine function if $f(x) = a_1x_1 \oplus \cdots a_nx_n \oplus c$ where $a_i \in GF(2)$, $i = 1,\ldots,n$, $c \in GF(2)$. When $c = 0$, $f(x)$ is called a linear function. The sequence of an affine (or linear) function is called affine (or linear) sequence.
2.1. Background

Definition 2.2 (Hamming weight and distance) The Hamming weight of a vector $\alpha \in V_n$, denoted by $W(\alpha)$, is the number of ones in the vector. The Hamming weight of a Boolean function $f(x)$, denoted by $W(f)$, is the number of ones in its truth table. The distance between two vectors $\alpha$ and $\beta$, denoted by $d(\alpha, \beta)$, is the number of coordinates which are different. Clearly, $d(\alpha, \beta) = W(\alpha \oplus \beta)$. The distance between two Boolean functions $f(x)$ and $g(x)$, denoted by $d(f, g)$, is equal to $W(f(x) \oplus g(x))$.

The following lemma is very useful in calculating the distance between two functions.

Lemma 2.1 Let $f(x)$, $g(x)$ be two Boolean functions on $V_n$. Then

$$d(f(x), g(x)) = 2^{n-1} - \frac{1}{2} \langle \xi, \eta \rangle,$$

where $\xi$ and $\eta$ are sequences of Boolean function $f(x)$ and $g(x)$.

Proof. Let $\xi = a_0, \ldots, a_{2^n-1}$ and $\eta = b_0, \ldots, b_{2^n-1}$. Let $\rho_1$ and $\rho_2$ denote the numbers such that $a_i = b_i$ and $a_i \neq b_i$ respectively. Hence $\langle \xi, \eta \rangle = \rho_1 - \rho_2 = 2^n - 2\rho_2$. In this case $\rho_2 = 2^{n-1} - \frac{1}{2} \langle \xi, \eta \rangle$. It is obviously that $\rho_2 = d(f(x), g(x))$. The lemma is proved. $\square$

Definition 2.3 (Balanced) A function $f(x)$ on $V_n$ is balanced if and only if the Hamming weight of the truth table of $f(x)$ is equals to $2^{n-1}$.

Notation 2.1 (Autocorrelation) Let $\alpha$ be a vector in $V_n$, $f(x)$ be a Boolean function on $V_n$. $\delta_f(\alpha) = f(x) \oplus f(x \oplus \alpha)$ is denoted in the thesis as the autocorrelation of $\alpha$.

Definition 2.4 (Linear Structure) Let $f(x)$ be a Boolean function on $V_n$. A vector, $\alpha$, is called a linear structure of $f(x)$ if $\delta_f(\alpha)$ is constant. That is a linear structure has constant autocorrelation.

The zero vector is a linear structure for all Boolean functions. Linear structures indicate weaknesses for cryptographic proposes and will be avoided or minimized in cryptographic design. In this thesis a Boolean function which has no nonzero linear structure is denoted has no linear structure.

Lemma 2.2 Let $f(x)$, $g(y)$ be two Boolean functions on $V_n$ and $V_m$, respectively and $z = (x, y)$. Then $F(z) = f(x) \oplus g(y)$ has no linear structure if and only if both $f(x)$ and $g(y)$ have no linear structure.
Proof. Let \( \alpha = (\beta, \gamma) \), where \( \beta \in V_n \) and \( \gamma \in V_m \). Then

\[
\delta_F(\alpha) = F(z \odot \alpha) \odot F(z) = (f(x \odot \beta) \odot f(x)) \odot (g(y \odot \gamma) \odot g(y)).
\]

If \( f(x) \) and \( g(y) \) have no linear structure, then for \( (\beta, \gamma) \neq (0, 0) \), \( \delta_f(\beta) = f(x \odot \beta) \odot f(x) \) and \( \delta_g(\gamma) = g(y \odot \gamma) \odot g(y) \) are not constant simultaneously. This implies that \( F(z) \) has no linear structure.

Conversely, if \( \alpha \neq 0 \in V_{n+m} \) is a linear structure of \( F(z) \), then either \( \beta \neq 0 \in V_n \) or \( \gamma \neq 0 \in V_m \). So either \( f(x) \) or \( g(y) \) has a linear structure. \( \square \)

Definition 2.5 (Generation matrix) Each Boolean function \( f(x) \) on \( V_n \) associate a \( 2^n \times 2^n \) matrix \( M \), whose \((u, v)\)th entry is \((-1)^{f(u \oplus v)}\). Such a matrix is called generation matrix of Boolean function \( f(x) \).

A \((1, -1)-\)matrix \( H \) of \( n \times n \) is called a Hadamard matrix if \( HH^T = nI_n \), where \( I_n \) is the \( n \times n \) identity matrix. A special kind of Hadamard matrix, called Sylvester-Hadamard matrix or Walsh-Hadamard matrix, will be relevant to this thesis. A Sylvester-Hadamard matrix, denoted by \( H_n \), is generated by the following recursive relation

\[
H_0 = 1, \quad H_n = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \times H_{n-1}, \quad n = 1, 2, \ldots
\]

where \( \times \) denotes the Kronecker product.

Sylvester-Hadamard matrices are closely related to linear functions. As it is shown in the following lemma.

Lemma 2.3 Let \( l_0, \ldots, l_{2^n-1} \) denote sequences of all linear functions on \( V_n \) including \( f(x) = 0 \). Write \( H_n = \begin{pmatrix} l_0 \\ \vdots \\ l_{2^n-1} \end{pmatrix} \). Then \( H_n \) is a \( 2^n \times 2^n \) Sylvester-Hadamard matrix.

Conversely the rows of any Sylvester-Hadamard matrix are the sequences of linear functions on \( V_n \).

The “Fourier coefficients” of \((-1)^{f(x)}\) is defined as following

\[
\hat{f}(\alpha) = 2^{-\frac{n}{2}} \sum_{x \in V_n} (-1)^{f(x) + \langle \alpha, x \rangle},
\]

where \( \alpha \in V_n \). If \( \cap f(\alpha) = \pm 1 \), then they may be written in the form \( \cap f(\alpha) = (-1)^g(\alpha) \), where \( g(\alpha) \) is another function on \( V_n \). We call \( g \) the “Fourier transform” of \( f \) and denote it by \( F_f \), i.e. \( F_f(\alpha) = g(\alpha) \).

There is a excellent result from R. L. McFarland (see [76]).
Theorem 2.1 Let $f(x)$ be a real-valued function on $V_n$, and $\hat{f}(x)$ be the Fourier coefficients of $(-1)^{f(x)}$, Then
\[
2^{-\frac{n}{2}} H_n M H_n = 2^n \text{diag}(\hat{f}(\alpha_0), \cdots, \hat{f}(\alpha_{2^n-1})),
\] (2.1)
where $M$ be the generation matrix of $f(x)$.

Proof. The equation (2.1) will be proved.

Let $M = (m_{ij})$, $m_{ij} = (-1)^{f(y_i \oplus y_j)}$ be the generation matrix of $f(x)$. The $(i, j)$ entry on the left side of the (2.1) as following:

\[
\sum_{k,l} h_{ik}h_{lj}(-1)^{f(a_k \oplus a_l)} = \sum_{k,l} (-1)^{\langle a_i, a_k \rangle \oplus \langle a_j, a_l \rangle \oplus f(a_k \oplus a_l)}
\]
\[
= \sum_t (-1)^{f(a_t)} \sum_k (-1)^{\langle a_i, a_k \rangle \oplus \langle a_j, a_l \rangle \oplus \langle a_t, a_k \rangle}
\]
\[
= \sum_t (-1)^{f(a_t)} \oplus \langle a_j, a_l \rangle \sum_k (-1)^{\langle a_t, a_k \rangle}
\]
\[
= 2^n \delta_{ij} \sum_t (-1)^{f(a_t) \oplus \langle a_j, a_l \rangle}
\]
\[
= 2^n \delta_{ij} \langle \xi, l_j \rangle,
\]
(2.2)

where $\delta_{ij} = \begin{cases} 1, & \text{when } i = j, \\ 0, & \text{otherwise} \end{cases}$. Since $\hat{f}(\alpha_i) = 2^{-\frac{n}{2}} \sum (-1)^{f(x) \oplus \langle x, \alpha_i \rangle} = 2^{-\frac{n}{2}} \langle \xi, l_i \rangle$. Then the equation (2.1) is true. This complete the proof. \qed

Let $\xi$ be the sequence of a Boolean function $f(x)$ on $V_n$. Note that
\[
\xi H_n = (\langle \xi, l_0 \rangle, \cdots, \langle \xi, l_{2^n-1} \rangle).
\]

Hence $\xi H_n H_n \xi^T = \sum_{i=0}^{2^n-1} \langle \xi, l_i \rangle^2$, then $2^n \xi \xi^T = \sum_{i=0}^{2^n-1} \langle \xi, l_i \rangle^2$. This proves the Parseval’s equation (see P.416 of F. J. MacWilliams and N.J.A. Sloane [78])
\[
\sum_{i=0}^{2^n-1} \langle \xi, l_i \rangle^2 = 2^{2n}.
\]
(2.3)

Definition 2.6 (Nonlinearity) Let $N_f$ denote the non-linearity of the Boolean function $f(x)$ on $V_n$.
\[
N_f = \min \{ d(f, \varphi) \mid \varphi \text{ is an affine function} \}
\]

The following lemma is well known for the nonlinearity inequality (see [78] for details).
Lemma 2.4 (Nonlinearity Inequality) Let \( f(x) \) be an arbitrary Boolean function on \( V_n \). The nonlinearity of \( f(x) \),

\[
N_f \leq 2^{n-1} - 2^{\frac{n}{2} - 1}
\]

Definition 2.7 (Bent function) A function \( f(x) \) on \( V_n \) is a bent function if

\[
2^{-\frac{n}{2}} \sum_{x \in V_n} (-1)^{f(x) \oplus (\alpha, x)} = \pm 1
\]

for all \( \alpha \in V_n \). Alternatively, the Fourier transform of a bent function is +1 or -1.

From the definition it can be seen that the bent functions exist only on \( V_n \), \( n \) even. No bent function has linear structure. The sequence of a bent function is called a bent sequence. The nonlinearity of bent functions reach their upper bound. Unfortunately bent functions are not balanced.

Definition 2.8 (Propagation Criterion and Strict Avalanche Criteria - SAC) Let \( f(x) \) be a Boolean function on \( V_n \). It is said that \( f(x) \) satisfies the propagation criterion with respect to \( \alpha \) if \( f(x) \oplus f(x \oplus \alpha) \) is a balanced function, where \( \alpha \) is a non-zero vector on \( V_n \).

The propagation criterion of degree \( k \) if \( f(x) \) satisfies the propagation criterion with respect to all \( \alpha \in V_n \), \( 1 \leq W(\alpha) \leq k \). It is be denoted by \( SAC(k) \).

Strict avalanche criterion (SAC) if the propagation criterion degree of \( f(x) \) is 1.

Notation 2.2 Let \( GL(m,2) = \{T = (t_{ij})_{1 \leq i,j \leq m} \mid t_{ij} \in GF(2), T \) is nonsingular\}. If \( f(x) = g(xT) \) for some \( T \in GL(m,2) \), then \( f(x) \) and \( g(x) \) are equivalent under the action of \( GL(m,2) \) and denote this fact by \( f \sim g \).

Write the set of all Boolean functions on \( V_m \) as \( \mathcal{R}_m \).

Notation 2.3 Let \( AGL(m,2) = \{ \begin{bmatrix} T & 0 \\ \alpha & 1 \end{bmatrix} \mid T \in GL(m,2), \alpha \in V_m \} \}. For any \( \sigma \in AGL(m,2) \), \( f(x) \in \mathcal{R}_m \), define \( \sigma(f(x)) = f(xT \oplus \alpha) \). If \( \sigma(f(x)) = g(x) \) for some \( \sigma \in AGL(m,2) \), then \( f(x) \) and \( g(x) \) are equivalent under the actions of \( AGL(m,2) \), and denote this by \( f \approx g \).

Notation 2.4 Let \( G_m = AGL \times V_m \times V_1 \). For \( (\sigma, \beta, c) \in G_m, f(x) \in \mathcal{R}_m \), define \( (\sigma, \beta, c)(f(x)) = \sigma(f(x)) \oplus (x, \beta, \beta \oplus c) \). If \( (\sigma, \beta, c)(f(x)) = g(x) \) for some \( (\sigma, \beta, c) \in G_m \), then \( f(x) \) and \( g(x) \) are equivalent under the actions of \( G_m \) and denote this by \( f \cong g \).
2.2 "Good" criteria of Boolean functions

The strength of product ciphers mainly comes from properly designed S-boxes. Being more precise, having cryptographically strong S-boxes, it is relatively easy to design a strong cryptographic algorithm by a careful selection of P-boxes and the number of rounds. Weak S-boxes always lead to insecure designs.

Each general cryptographic attack on product ciphers explores some weaknesses in S-boxes. In response, a new S-box criterion is introduced. If the criterion is incorporated into S-boxes, it makes the cryptographic algorithm immune against the attack. For instance, the differential attack caused that a “good” XOR profile was added to the list of S-box criteria.

There is a set of design criteria which are believed to be essential in the design of cryptographic algorithms. If S-boxes do not satisfy one of the criteria, the cryptographic design based on the S-boxes may be cryptographicall weak (or easy to attack). The collection of essential S-boxes design criteria are:

- Completeness,
- Balance,
- Nonlinearity,
- Propagation criterion and SAC,
- Good XOR profile,
- High algebraic degree.

The criterion completeness was introduced by Kam and Davida [56]. It is applicable to the whole cryptographic design (or S-P network) rather than a single S-box. Given S-boxes with a fixed structure, it is necessary to build up the cross dependencies so any binary output is a complex function of every binary input. The lack of these dependencies enables an opponent to use the “divide and conquer” strategy to analyze the design.

Balance and nonlinearity are discussed in the chapter 3.

SAC was introduced by Webster and Tavares [149]. The SAC characterizes the output when there is a single bit change on the input.

**Theorem 2.2** Let \( f(x) \) be a function on \( V_n \) and \( A \) be a \( n \times n \) nonsingular matrix with each entry \( \in GF(2) \). If \( f(x) \oplus f(x \oplus \alpha) \) is balanced for each row \( \alpha \in A \). Then \( \phi(x) = f(xA) \) satisfies the SAC.
Corollary 2.1 Let \( f(x) \) be a Boolean function on \( V_n \). Then

\[
\sum_{\alpha \in V_n} \delta_f^2(\alpha) = 2^{-n} \sum_{j=0}^{2^n-1} (\xi, l_i)^4.
\]

Denote \( \sigma(f) \) as following

\[
\sigma(f) = \sum_{\alpha \in V_n} \delta_f^2(\alpha) = 2^{-n} \sum_{j=0}^{2^n-1} (\xi, l_i)^4.
\]

Theorem 2.3 Let \( f(x) \) be a function on \( V_n \), then

1. \( 2^{2n} \leq \sigma(f) \leq 2^{3n} \),
2. \( \sigma(f) = 2^{2n} \) if and only if \( f(x) \) is a bent function,
3. \( \sigma(f) = 2^{3n} \) if and only if \( f(x) \) is an affine function.

Proof.

1. By Theorem 2.2 and Corollary 2.1

\[
\sigma(f) = 2^{-n} \sum_{i=0}^{2^n-1} (\xi, l_i)^4 \leq 2^{-n} \left( \sum_{i=0}^{2^n-1} (\xi, l_i)^2 \right)^2.
\]

From (2.3) we have that

\[
\sum_{i=0}^{2^n-1} (\xi, l_i)^2 = 2^{2n}.
\]

Thus

\[
\sigma(f) \leq 2^{-n} 2^{4n} = 2^{3n}.
\]

2. Note that \( \delta(0) = 2^n \).

\[
\sigma(f) = \sum_{\alpha \in V_n} \delta_f^2(\alpha) \geq \delta^2(0) = 2^{2n}.
\]

In this case \( \sigma(f) = 2^{2n} \) if and only if \( \Delta(\alpha) = 0 \) for any \( \alpha \neq 0 \). \( f(x) \) is a bent (see \([2]\) for details).

3. Set \( y_i = (\xi, l_i)^2 \). By Parseval's equation, \( \sum_{i=0}^{2^n-1} y_i = 2^{2n} \). It is not hard to see that

\[
\sigma(f) = 2^{3n} \iff 2^{-n} \sum_{i=0}^{2^n-1} y_i^2 = 2^{3n} \iff \sum_{i=0}^{2^n-1} y_i^2 = 2^{4n} \iff \sum_{i=0}^{2^n-1} y_i^2 = (\sum_{i=0}^{2^n-1} y_i)^2 \iff y_i y_j = 0 \text{ if } j \neq i \iff \text{there exists a } j_0 \text{ such that } y_{j_0} = 2^{2n} \text{ and } y_j = 0 \text{ if } j \neq j_0 \iff \text{there exists a } j_0 \text{ such that } (\xi, l_{j_0}) = \pm 2^n \text{ and } (\xi, l_j) = 0 \text{ if } j \neq j_0 \iff \text{there exist a } j_0 \text{ such that } \xi = \pm l_{j_0}, f(x) \text{ is an affine function.}
2.2. "Good" criteria of Boolean functions

Let \( \alpha = (\alpha_1, \ldots, \alpha_n) \in V_n \). Then \( D_\alpha \) is a function on \( V_n \) and defined by

\[
D_\alpha(x_1, \ldots, x_n) = (x_1 \oplus \alpha_1 \oplus 1) \cdots (x_m \oplus \alpha_n \oplus 1).
\]

Lemma 2.5 (J. Seberry, X. M. Zhang and Y. Zheng [118]) Let \( f_1(x_1, \ldots, x_n) \) and \( f_2(x_1, \ldots, x_n) \) be functions on \( V_n \), and let \( g(x_1, \ldots, x_{n+1}) \) on \( V_{n+1} \) be defined by

\[
g(x_1, \ldots, x_{n+1}) = (1 \oplus x_{n+1})f_1(x_1, \ldots, x_n) \oplus x_{n+1}f_2(x_1, \ldots, x_n).
\]

Suppose that \( \xi_1 \) and \( \xi_2 \) be the sequences of \( f_1(x_1, \ldots, x_n) \) and \( f_2(x_1, \ldots, x_n) \) respectively, satisfy \( \langle \xi_1, l \rangle \leq P_1 \) and \( \langle \xi_2, l \rangle \leq P_2 \) for any affine sequence \( l \) of length \( 2^n \), \( P_1, P_2 \) are positive integer. Then nonlinearity of \( g(x_1, \ldots, x_{n+1}) \) satisfies \( N_g \geq 2^n - \frac{1}{2}(P_1 + P_2) \).

The following result, as a special case of lemma 2.5, shows that such high nonlinearity functions can be obtained by concatenating bent functions.

Corollary 2.2 In the construction (2.5), both \( f_1(x_1, \ldots, x_n) \) and \( f_2(x_1, \ldots, x_n) \) are bent functions on \( V_{2k} \), then \( N_g \geq 2^{2k} - 2^k \).

This construction has been discovered by Meier and Staffelbach in [80].

A similar result can be obtained by concatenating four functions.

Lemma 2.6 ([118]) Let \( f_0, f_1, f_2, f_3 \) be Boolean functions on \( V_n \), whose sequences are \( \xi_0, \xi_1, \xi_2, \xi_3 \) respectively. If \( \langle \xi_i, l \rangle \leq P_i, 0 \leq i \leq 3 \) for each affine sequence \( l \). Then \( g \) on \( V_{n+2} \) defined by

\[
g(x_1, \ldots, x_n, x_{n+1}, x_{n+2}) = \bigoplus_{i=0}^{3} D_{\xi_i}(x_{n+1}, x_{n+2})f_i(x_1, \ldots, x_n)
\]

satisfies \( N_g \geq 2^{n+1} - \frac{1}{2} \sum_{i=0}^{3} P_i \). In particular, when \( n \) is even and \( f_i, 0 \leq i \leq 3 \) are all bent functions on \( V_n \), \( N_g \geq 2^{n+1} - 2^k + 1 \).

Lemma 2.7 (F. Chabaud and S. Vaudenay [16]) Let \( f(x) \) be a function on \( V_n, n \) odd. Then nonlinearity of \( f(x) \) is maximally if and only if \( W(f(x)) = \{0, \pm 2^{n+1}\} \).

Lemma 2.8 ([118]) Let \( f(x_1, \ldots, x_{2k}) \) be a bent function on \( V_{2k} \), \( \eta_0 \) be the sequence of \( f(0, x_2, \ldots, x_{2k}) \) and \( \eta_1 \) be the sequence of \( f(1, x_2, \ldots, x_{2k}) \). Then for any affine sequence \( l \) on \( V_{2k-1} \), there are \( -2^k \leq \langle \eta_0, l \rangle \leq 2^k \) and \( -2^k \leq \langle \eta_1, l \rangle \leq 2^k \).
Theorem 2.4 ([118]) For any integer \( k \geq 1 \), there exists a Boolean balanced function on \( V_{2^k} \) with \( \text{SAC} \) and nonlinearity \( 2^{2^k} - 2^k \).

For any \( k \geq 2 \), there exists a Boolean balanced function on \( V_{2^k} \) with \( \text{SAC} \) and nonlinearity \( 2^{2^k-1} - 2^k \).

The upper bound of nonlinearity of functions on \( V_{2^k+i} \) is \( 2^{2^k} - 2^{k-\frac{1}{2}} \).

Two fundamental results on Boolean functions satisfying \( \text{SAC}(k) \) were given by Preneel, Leekwijck, Linden, Govaerts and Vandewalle at [97].

Lemma 2.9 (B. Preneel, W. V. Leekwijck, L. V. Linden, R. Govaerts and J. Vandewalle [97]) Suppose \( f(x) \) is a Boolean function on \( V_n \), \( n \geq 2 \). If \( f(x) \) satisfies \( \text{SAC}(n-2) \), then \( f(x) \) has degree 2. If \( f(x) \) satisfies \( \text{SAC}(k) \), \( 1 \leq k \leq n-3 \), then \( \deg(f(x)) \leq n-k-1 \).

Lemma 2.10 ([97]) Suppose \( f(x) \) is a quadratic Boolean function on \( V_n \), \( n \geq 3 \). Then \( f(x) \) satisfies \( \text{SAC}(k) \), \( 1 \leq k \leq n-2 \), if and only if every variable \( x_i \) occurs in at least \( k+1 \) second degree terms of the algebraic normal form.

Define

\[
\begin{align*}
    f(x) = \sum_{1 \leq i < j \leq n} x_ix_j.
\end{align*}
\]

Then each variable \( x_i \) occurs exactly \( n-1 \) terms.

Lemma 2.11 (Lloyd [71]) There are \( 2^{n+1} \) Boolean functions on \( V_n \) which satisfy \( \text{SAC}(n-2) \), and they are exactly the functions \( f(x) \oplus g(x) \), where \( f(x) \) defined in (2.7) and \( g(x) \) is an affine function.

The fact that the function \( f(x) \) from \( V_n \) to \( V_k \) has good XOR profile is equivalent to the fact that for any vector \( \alpha \in V_n \), \( f(x) \oplus f(x \oplus \alpha) \) runs through a subset of \( 2^{k-1} \) vectors in \( V_k \) each \( 2^{n-k+1} \) times while \( x \) runs through \( V_n \) once, but does not take on the other \( 2^{k-1} \) vectors.

The criterion is not very restrictive as the designer of S-boxes needs to take care that the XOR profile does not contain entries with “large” numbers. In addition, the XOR profile must be considered in the context of the best round characteristics. It is possible to trade off the largest entries of XOR profile with the number of rounds.

Single Boolean functions are basic elements which can be used to construct more complex and useful structures called S-boxes. An \( n \times k \) S-box is a mapping from \( V_n \rightarrow V_k \) and

\[
S(x) = (f_1(x), \cdots, f_k(x))
\]
where \( n \geq k \) and \( f_i(x) \) is a Boolean function on \( V_n \), \( 1 \leq i \leq k \).

The collection of cryptographically essential properties include the following ones:

1. Any nonzero linear combination of \( f_i(x) \), \( 1 \leq i \leq k \), should be balanced.
2. Any nonzero linear combination of \( f_i(x) \), \( 1 \leq i \leq k \), should be highly nonlinear.
3. Any nonzero linear combination of \( f_i(x) \), \( 1 \leq i \leq k \), should satisfy the SAC.
4. The S-box should be regular, i.e. each vector in \( V_k \) should happen \( 2^{n-k} \) times while \( x \) runs through \( V_n \) once.
5. S-box should has a good XOR profile.

It is obvious that properties (2) and (4) are equivalent. Other properties may be hold at same time but a “reasonable” tradeoff can always be negotiated.

### 2.3 Boolean bent functions and construction

Bent functions play an important role in cryptography (for instance, in stream ciphers), as well as in error correcting coding.

The following results can be found in an excellent survey of bent functions by Dillon [27].

**Lemma 2.12** Let \( f(x) \) be a function on \( V_n \), \( \xi \) be the sequence of \( f(x) \). Then the following statements are equivalent:

(i) \( f(x) \) is bent.

(ii) \( \langle \xi, l \rangle = \pm 2^\frac{n}{2} \) for any affine sequence \( l \) on \( V_n \).

(iii) The autocorrelation \( \delta_f(\alpha) \) is balanced for any non-zero vector \( \alpha \in V_n \).

(iv) \( f(x) \oplus \langle \alpha, x \rangle \) assumes the value one \( 2^{n-1} \pm 2^\frac{n}{2}-1 \) times for any \( \alpha \in V_n \).

(v) The matrix of \( f(x) \), \( M \), is an Hadamard matrix.

(vi) The nonlinearity of \( f(x) \) satisfies \( N_f = 2^{n-1} - 2^\frac{n}{2}-1 \).

(vii) \( D = \{x \mid f(x) = 1\} \) is a difference set with parameters \( (2^n, 2^{n-1} \pm 2^{\frac{n}{2}-1}, 2^{n-2} \pm 2^{\frac{n}{2}-1}) \).
The proof can be found in many places in the literature, see [118], [163] for instance.

**Corollary 2.3** A function $f(x)$ on $V_n$ attains the upper bound for nonlinearity, $2^{n-1} - 2^{\frac{1}{2}n-1}$, if and only if $f(x)$ is bent.

From corollary 2.3, balanced functions cannot attain the upper bound of nonlinearity. The following propositions is given by O. S. Rothaus in [104].

**Proposition 2.1** The Fourier transform of a bent function is a bent function.

**Proposition 2.2** The Boolean function $f(x)$ is a bent function on $V_{2n}$ if and only if $f(x) \oplus \langle x, \alpha \rangle$ has $2^{2n-1} \pm 2^{n-1}$ zeros for all $\alpha \in V_{2n}$.

Note that if $g(x) = f(x) \oplus \langle x, \alpha \rangle$, then $\hat{g}(x) = \hat{f}(x \oplus \alpha)$, thus if $f(x)$ is bent, then $f(x) \oplus \langle x, \alpha \rangle$ is bent for all $\alpha \in V_{2n}$.

It is easy to see that if $f(x)$ is a function on $V_n$ and $g(y)$ is a function on $V_m$, then $f(x) \oplus g(y)$ is a bent function on $V_{n+m}$ if and only if both $f(x)$ and $g(y)$ are bent functions.

A polynomial on $V_n$ is decomposable if by a linear transformation of coordinates, it may be written as a sum of polynomials on disjoint variables. There is a proposition as following given by O. S. Rothaus,

**Proposition 2.3** If $f(x)$ is a bent function on $V_{2k}$, $k \geq 3$, of degree $k$, then $f(x)$ is indecomposable [104].

Finally note that $\chi = (-1)^{\langle x, \alpha \rangle}$ is a nonprinciple character of $V_{2n}$, $\alpha \neq 0$. Then

**Proposition 2.4** $f(x)$ on $V_{2n}$ is a bent function if and only if $\chi(f^{-1}[1]) = \pm 2^{n-1}$, where $f^{-1}[1] = \{ x : f(x) = 1 \}$, for all nonprincipal characters $\chi$ on $V_{2n}$.

### 2.4 Classes of Boolean bent functions

Bent functions have been studied since the publication of the significant paper by O. S. Rothaus [104] in 1976. Some papers have led to new results on the bent functions themselves. In fact, all quadratic bent functions are known (see P. J. Chase, J. F. Dillon and K. D. Lerche [17] for details). If $n \geq 4$, then any bent function has a degree at most $\frac{n}{2}$ (see [104]). Therefore, all bent functions on $V_2$ and $V_4$ are quadratic. If anyone want to obtain new bent functions, a simple way would be to use known ones and to alter them without losing their properties.
2.4. Classes of Boolean bent functions

Class 1 (O. S. Rothaus [104]) The function

\[ f(x, y) = \sum_{1 \leq i \leq n} x_i y_i \]  

(2.8)

is a bent function on \( V_{2n} \).

The type of Class 1 bent function is usually called the dot product and is written as

\[ f(x, y) = x \odot y, \]

and the Fourier transform of \( f(x, y) \) is itself.

Proposition 2.5 Let \( f(x) = \sum_{1 \leq i < j \leq 2n} x_i x_j \) denote the elementary symmetric function of degree 2 on \( V_{2n} \). Then \( f(x) \) is a bent function on \( V_{2n} \).

P. J. Chase, J. F. Dillon and K. D. Lerche (see [17]) has observed that every quadratic bent function is equivalent to the dot product of Class 1. Thus, the dot product is the only quadratic bent function on \( V_{2n} \).

In Rothaus's paper (see [104]) there are two other classes of bent functions.

Class 2 (O. S. Rothaus [104]) Let \( x, y \in V_n \) and \( g(x) \) be an arbitrary Boolean function on \( V_n \). Then the function \( Q(x, y) \) on \( V_{2n} \) given by

\[ Q(x, y) = \sum_{1 \leq i \leq n} x_i y_i \oplus g(x) \]  

(2.9)

is bent.

This result was discovered independently by P. Kesava Menon (see [82]) and R. J. Turyn (see [143]). The generator matrix of a bent function of Class 2 corresponding to a incidence matrix of Hadamard difference set in a group of order \( 4^n \).

When \( g(x) = 0 \), the bent function of Class 2 is the bent function of Class 1. Thus Class 1 \( \subset \) Class 2. The Fourier transform of the bent function in Class 2 is itself. Let \( g(x) = \prod_{1 \leq i \leq k} x_i, 1 \leq k \leq n \), then

\[
Q(x, y) = \sum_{1 \leq i \leq n} x_i y_i \\
Q(x, y) = \sum_{1 \leq i \leq n} x_i y_i \oplus x_1 x_2 x_3 \\
\vdots \\
Q(x, y) = \sum_{1 \leq i \leq n} x_i y_i \oplus \prod_{1 \leq i \leq n} x_i
\]

(2.10)

are obviously inequivalent bent functions on \( V_{2n} \).
2.4. Classes of Boolean bent functions

**Class 3** (O. S. Rothaus [104]) Let $f(x)$, $g(x)$ and $h(x)$ be bent functions on $V_n$ such that $f(x) \oplus g(x) \oplus h(x)$ is also bent. Let $y, z \in V_1$. Then the function

$$Q(x, y, z) = f(x)g(x) \oplus g(x)h(x) \oplus h(x)f(x) \oplus (f(x) \oplus g(x))y \oplus (f(x) \oplus h(x))z \oplus yz$$

(2.11)

is a bent function on $V_{n+2}$.

Note that the requirement that $f(x) \oplus g(x) \oplus h(x)$ be bent is very easily met by taking $f(x) = g(x) = h(x)$ for example, or by taking $f(x)$, $g(x)$ and $h(x)$ from Class 2. It should be remarked that Class 2 is included in Class 3, but Class 2 is given explicitly, while Class 3 has implicit features.

The Class 3 has most general polynomial form as following

$$A(x) \oplus B(x)y \oplus C(x)z \oplus yz.$$  

(2.12)

Any quadratic bent functions is of Class 3.

**Lemma 2.13** (J. F. Dillon [27]) Every cubic bent functions is equivalent to a bent function in Class 3

More generally

**Lemma 2.14** (J. F. Dillon [27]) The bent function $f(x)$ is equivalent to a bent function in Class 3 if some variables $x_i$ appear in no term of degree greater than three.

The next class of bent functions, a natural generalization of Class 2, was discovered by R. McFarland(see [77]).

**Class 4** (R. McFarland [77]) Let $P(x)$ be an arbitrary permutation on $V_n$, $g(x)$ be an arbitrary Boolean function on $V_n$, then

$$f(x, y) = (P(x), y) \oplus g(x)$$

is a Boolean bent function on $V_{2n}$.

If the permutation $P(x)$ defined as an identity mapping and $g(x) = 0$, then $f(x, y)$ is a bent function of Class 1. This construction has a very useful property, which was described by Nyberg in [90].

**Lemma 2.15** A bent function constructed by the method of Class 4 has maximal degree if the function $g(x)$ defined above takes the value one an odd number of times.
2.4. Classes of Boolean bent functions

Proof. The proof need to show that bent function constructed by the method of Class 4 has degree \( n \) if the function \( g(x) \) takes the value one an odd number of times. Hence

\[
\sum_{x \in V_n} g(x) = 1.
\]

Writing \( g(x) \) into a polynomial function of \( n \) variables, then \( g(x) \) must contain the term \( x_1 \cdots x_n \) once. In this case \( \text{deg}(g(x)) = n \). The function

\[
f(x, y) = (P(x), y) \oplus g(x) = \sum_{i=1}^{n} p_i(x)y_i \oplus g(x), \quad \text{where} \quad P(x) = (p_1(x), \cdots, p_n(x)).
\]

Clearly there is no such term \( x_1 \cdots x_n \) contained in the \( \sum_{i=1}^{n} p_i(x)y_i \). So \( \text{deg}(f(x,y)) \geq \text{deg}(g(x)) = n \). Recall that the maximal degree for a bent function on \( V_{2^n} \) is \( n \). So the maximal degree of bent function \( f(x,y) \) constructed by Class 4 is \( n \) if \( g(x) \) takes the value one an odd number of times. \( \square \)

Corollary 2.4 The Fourier transform of the bent function \( f(x,y) \) constructed by the method of Class 4 is

\[
F_f(x,y) = (x, P^{-1}(y)) \oplus g(P^{-1}(y)).
\]

Here is a useful characterization of permutations given by Maiorana.

Lemma 2.16 The function \( P(x) = (p_1(x), \cdots, p_n(x)) \) is a permutation of \( V_n \) if and only if every nonzero linear combination of the \( p_i(x) \), \( 1 \leq i \leq n \), is a balanced function on \( V_n \).

Proof. For each \( v \in V_n \), let \( G_p(v) \) be the number of vectors \( u \) such that \( P(u) = v \). Then the function \( e_1p_1(x) \oplus \cdots \oplus e_np_n(x) \) on \( V_n \) may be written as

\[
B_P(e) = \sum_{v \in V_n} G_p(v)(-1)^{(e,v)},
\]

where the function \( B_P(e) \) is the (unnormalized) Hadamard transform of \( G_p \).

Thus, \( P(x) \) is a permutation \( \iff \) \( G_p \) is the constant 1 function \( \iff \) \( B_P(e) \) is the function \( 2^n \delta_{0,e} \iff \sum e_i P(x) \) is balanced for all \( e \neq 0 \). \( \square \)

Class 5 (J. F. Dillon [27]) Let \( S_1, \cdots, S_{2^{n-1}} \) be \( n \)-dimensional subspaces of \( V_{2^n} \) such that

\[
S_i \cap S_j = \{0\}, \quad 1 \leq i < j \leq 2^n - 1,
\]

and let

\[
S_i^* = S_i - \{0\}, \quad 1 \leq i \leq 2^n - 1.
\]

Then \( D = \bigcup_{i \in E} S_i^* \) is a \( (4^n, 2 \cdot 4^{n-1} - 2^{n-1}, 4^{n-1} - 2^{n-1}) \)-difference set in \( V_{2^n} \) and the characteristic function of \( D \) is a bent function on \( V_{2^n} \).
Proof. For each $i$ let $\tilde{S}_i$ be the dual of $S_i$. Then for all nonprincipal characters $\chi$ of $V_{2n}$

$$\chi(D) = \sum \chi(S_i^*) = \begin{cases} -2^{n-1} & \text{if } \chi \notin \tilde{S}_i \text{ for all } i \\ 2^{n-1} & \text{otherwise.} \end{cases}$$

Thus, $\chi(D) = \pm 2^{n-1}$ for all nonprincipal characters $\chi$ of $V_{2n}$, and it follows from lemma 2.12 that $D$ is a difference set. 

Every bent function of Class 5 has degree $n$. In this case they are indecomposable.

Class 6 (J. F. Dillon [27]) Let $g(x)$ be a balanced function on $V_n$ which vanishes on 0. Let $G(y)$ be a Boolean function on $V_{2n}$ defined by

$$G(y) = g(y^{2^n-1}).$$

Then $G(y)$ is bent if and only if there exists a balanced function $h(x)$ on $V_n$ such that $h(x) = g(x^{-1})$ for all $x \in V_n$, where

$$\hat{f}(u) = \frac{1}{2^n} \sum_{x \in V_n} f(x) Tr_{V_n/V_2} (u \circ x) \text{ for all } u \in V_n.$$ 

The cardinality $2^{n-1}$ of difference sets in $V_{2n}$ suggests that they may be obtained as the disjoint union of certain "nice" $(2^n-1)$—subsets of $V_{2n}$. Indeed, Class 5 was obtained by taking the $(2^n-1)$—subset to be the set of nonzero elements in an $n$—dimensional subspace of $V_{2n}$. Similarly, these difference sets as disjoint union of certain "nice" $2^{n-1}$—subsets of $V_{2n}$ may be obtained.

Class 7 (J. F. Dillon [27]) Let $A_1, A_2, \cdots, A_{2^n+1}$ be pairwise disjoint $(n-1)$—dimensional affine subspaces of $V_{2n}$. Then $D = \bigcup A_i$ is a $(4^n, 2 \cdot 4^{n-1} - 2^{n-1}, 4^{n-1} - 2^{n-1})$—difference set in $V_{2n}$ if for each nonzero linear functional $l$ on $V_{2n}$:

(i) $l$ annihilates an odd number $L_{i1}, L_{i2}, \cdots, L_{ik+1}$ of $L_i$'s. i.e., $l(\alpha) = 0$, for any $\alpha \in L_i$, $i = 1, \cdots, 2k + 1$. And

(ii) $l$ is "almost balanced" on the corresponding $a_i$'s; i.e., $l$ vanishes on $k$ or $k-1$ of $a_{i1}, \cdots, a_{ik}$ where for each $i$, $1 \leq i \leq 2^n - 1$, $A_i$ is the translation by $a_i$ of the linear space $L_i$.

Class 7 contains the Maiorana bent functions of Class 4.
2.4. Classes of Boolean bent functions

Class 8 (C. Carlet [15]) Let $E$ be a $p$–dimensional linear subspace of $V_n$ and $\pi$ a permutation on $V_p$ such that, for any $(x, y) \in E$, the number $x \odot \pi(y) \equiv 0 \mod 2$. Then the function defined on $V_n$ as:

$$x \odot \pi(y) \oplus \phi_E(x, y)$$

is bent, and its Fourier transform is the function

$$y \odot \pi^{-1}(x) \oplus \phi_{E^\perp}(x, y).$$

The class of bent functions obtained cannot be considered as an effective one since there is no simple description of all the subspaces and permutations satisfying the conditions of Class 8. But there is a simple subcase:

When $E$ is equal to the cartesian product of two subspaces $E_1$ and $E_2$ of $V_p$ such that $\dim(E_1) + \dim(E_2) = p$ and $\pi(E_2) = E_1^\perp$. This will lead to the bent functions of class 8.

Class 9 (C. Carlet [15]) Let $E$ be a $p$–dimensional linear subspace of $V_n$. For any $(x, y)$ in $E$, if $p \geq 4$ and if the restriction of permutation $\pi$ to any linear hyperplane of $V_p$ is not affine, then the following function

$$(x, y) \longrightarrow \Pi_{i=1}^P x_i \oplus (x \oplus 1) \odot \pi(y)$$

is bent, where 1 denotes the all-one vector.

Proposition 2.6 (C. Carlet [15]) Let $x, y \in E$, $E$ be a $p$–dimensional linear subspace of $V_n$, then the following function

$$(x, y) \longrightarrow \Pi_{i=1}^P x_i \oplus (x \oplus 1) \odot y$$

is bent, where 1 denote the all-one vector.

Lemma 2.17 Let $f(x)$ and $g(x)$ be Boolean functions on $V_n$. $x = (x_1, \cdots, x_n) \in V_n$. Matrices $A$ and $B$ are generated by $f(x)$ and $g(x)$. Define

$$A = (a_{ij})_{1 \leq i, j \leq 2^n}, \quad a_{ij} = (-1)^{f(x_{i-1} \oplus x_{j-1})}$$

and

$$B = (b_{ij})_{1 \leq i, j \leq 2^n}, \quad b_{ij} = (-1)^{g(x_{i-1} \oplus x_{j-1})}.$$ 

Set $h(x_1, \cdots, x_n, x_{n+1}) = (1 \oplus x_{n+1})f(x_1, \cdots, x_n) \oplus x_{n+1}g(x_1, \cdots, x_n)$. If
2.4. Classes of Boolean bent functions

(i) $n$ is odd, and $A^2 + B^2 = 2^{n+1}I_{2^n}$, then $h(x_1, \ldots, x_n, x_{n+1})$ is a bent, and $N_f = N_g = 2^{n-1} - 2^{\frac{n-1}{2}}, AB = 0 = BA$.

(ii) $n$ is even, and $A^2 + B^2 = 2^{n+1}I_{2^n}$, then $f(x)$ and $g(x)$ are bent functions.

Proof.

(i) Set $\Delta_f = \text{diag}\{\langle \xi, l_0 \rangle, \ldots, \langle \xi, l_{2^n-1} \rangle\}$, $\Delta_g = \text{diag}\{\langle \eta, l_0 \rangle, \ldots, \langle \eta, l_{2^n-1} \rangle\}$, where $\xi$ is the sequence of $f(x)$ and $\eta$ is the sequence of $g(x)$. From the McFarland formula [76], there are

$$A = 2^{-n}H_n\Delta_fH_n, \quad B = 2^{-n}H_n\Delta_gH_n.$$  

Since that

$$A^2 + B^2 = 2^{-n}H_n(\Delta_f^2 + \Delta_g^2)H_n = 2^{n+1}I_{2^n},$$

then

$$\Delta_f^2 + \Delta_g^2 = 2^{n+1}I_{2^n}.$$  

That is $\langle \xi, l_i \rangle^2 + \langle \eta, l_i \rangle^2 = 2^{n+1}, \ i = 0, 1, \ldots, 2^n - 1$. Let $n = 2m + 1$, for each $i$, $0 \leq i \leq 2^n - 1$, there is $\langle \xi, l_i \rangle = \pm 2^{m+1}$ and $\langle \eta, l_i \rangle = 0$, or $\langle \xi, l_i \rangle = 0$ and $\langle \eta, l_i \rangle = \pm 2^{m+1}$ be true, $i = 0, \ldots, 2^n - 1$. Since $\sum_{i=0}^{2^n-1} \langle \xi, l_i \rangle^2 = 2^{2n} = \sum_{i=0}^{2^n-1} \langle \eta, l_i \rangle^2$, $\langle \xi, l_i \rangle (\langle \eta, l_i \rangle)$ can not all be zero, $i = 0, \ldots, 2^n - 1$. Then

$$\max_{i=0}^{2^{n-1}} |\langle \xi, l_i \rangle| = 2^{m+1} = \max_{i=0}^{2^{n-1}} |\langle \eta, l_i \rangle|.$$  

In this case

$$N_f = 2^{2m} - 2^m = 2^{n-1} - 2^{\frac{n-1}{2}} = N_g.$$  

Since $\Delta_f\Delta_g = 0$, then $AB = BA = 0$.

Let $\sigma$ be the sequence of $h(x_1, \ldots, x_{n+1})$ on $V_{n+1}$, $\sigma = (\xi, \eta)$. Let $\ell_i$ be the sequence of linear function $\langle \alpha, x \rangle$, $i = 0, \ldots, 2^n - 1$. When $0 \leq i \leq 2^n - 1$, $\ell_i = (l_i, l_i)$, $\ell_{2^n+i} = (l_i, -l_i)$. There is

$$\langle \sigma, \ell_i \rangle = \langle \xi, l_i \rangle + \langle \eta, l_i \rangle,$$

and

$$\langle \sigma, \ell_{2^n+i} \rangle = \langle \xi, l_i \rangle - \langle \eta, l_i \rangle,$$

$0 \leq i \leq 2^n - 1$. Then

$$\langle \sigma, \ell_i \rangle^2 = \langle \xi, l_i \rangle^2 + \langle \eta, l_i \rangle^2,$$
and
\[ (\sigma, \ell_{2^{n+1}})^2 = (\xi, l_i)^2 + (\eta, l_i)^2. \]

In all cases, \( (\sigma, \ell_i)^2 = 2^{n+1}, \) \( N_h = 2^n - 2^{n+1}. \) So \( h(x) \) is a bent function on \( V_{n+1}. \)

(ii) Let \( n = 2m. \) Since \( (\xi, l_i)^2 + (\eta, l_i)^2 = 2^{n+1} = 2^{2m+1}, \) then \( (\xi, l_i)^2 = (\eta, l_i)^2 = 2^{2m} = 2^n \) for \( 0 \leq i \leq 2^n - 1. \) In this case \( A^2 = B^2 = 2^n I_{2^n}, \) then \( f(x) \) and \( g(x) \) are bent functions on \( V_n. \)

This completes the proof. \( \Box \)
Balanced Boolean Function with High Nonlinearity

It is well known that the resistance of a product cipher to modern cryptanalytic attacks such as linear and differential cryptanalysis (see [12], [75]) depends critically upon the nonlinearity of the Boolean functions comprising the round function. Typically these functions must be balanced, so there is considerable interest in the design of highly nonlinear balanced Boolean functions. In addition, cipher functions should satisfy other cryptographic properties, such as correlation immunity ([133]) and strict avalanche criterion (SAC) ([149]). Previous work on the design of balanced functions includes [28], [51], [107], [121], [122]. The existing research concentrates on specific constructions, supported by algebraic proofs that the resulting Boolean functions will be both balanced and satisfy one or more other properties. Some publications ([84], [85]) address the issue of applying combinatorial optimization methods to the design of Boolean functions.

In this chapter the author recalls some constructions for balanced Boolean functions with highly nonlinearity.

**Lemma 3.1** Let \( g(x) = f(xA \oplus \alpha) \), where \( A \) is \( n \times n \) nonsingular matrix and vector \( \alpha \in V_n \). Then \( g(x) \) is balanced if and only if \( f(x) \) is balanced.

**Proof.** If \( A \) is nonsingular, then for \( x \) running through all values on space \( V_n \), \( y = xA \oplus \alpha \) also takes on the same collection of values. Hence as \( f(x) \) is balanced so is \( g(x) \) as permuted values of the functions \( f(x) \).

Bent functions have the largest nonlinearity and the smallest difference but are not balanced. The lack of balance in an S-box means that each time the S-box is used, it produces a bias in the output. So some output strings are more probable than others. Even worse, as any cryptographic design uses many rounds with the same S-box, the bias tends to accumulate making some output strings less and others more
probable. This opens up the design to all sorts of attacks which explores a non-uniform output string probability distribution. Thus bent functions cannot be used directly in cryptographic designs.

Affine Boolean functions except constant 0 and 1 are balanced, but their non-linearity are lowest. In this chapter the Boolean functions with balanced and high nonlinearity are discussed. Balanceness and high nonlinearity are the most important criteria for cryptographically strong Boolean functions.

Note that a bent sequence on $V_{2n}$ contains $2^{2n-1} + 2^{n-1}$ ones and $2^{2n-1} - 2^{n-1}$ zeros, or vice versa. It was observed by Meier and Staffelbach [80], changing $2^{n-1}$ positions in a bent sequence yields a balanced function having a nonlinearity of at least $2^{2n-1} - 2^n$.

In this chapter some methods of how to construct balanced Boolean function with high nonlinearity, and in some cases the balanced Boolean functions which satisfy the propagation criterion with respect to almost all non-zero vectors are introduced.

### 3.1 On $V_{2n+1}$

#### 3.1.1 Concatenating Bent Functions

Let $f(x_1, \cdots, x_{2n})$ be a bent function on $V_{2n}$ and define $g(x_1, \cdots, x_{2n}, x_{2n+1})$ as

$$g(x_1, \cdots, x_{2n+1}) = f(x_1, \cdots, x_{2n}) \oplus x_{2n+1}. \quad (3.1)$$

$g(x_1, \cdots, x_{2n+1})$ is balanced on $V_{2n+1}$ with nonlinearity $N_g \geq 2^{2n} - 2^n$.

**Lemma 3.2** Let $A$ be an nonsingular $(2n + 1) \times (2n + 1)$ matrix over $GF(2)$, $g(x)$ is defined as (3.1), set

$$g^*(x) = g(xA).$$

$g^*(x)$ is a balanced function on $V_{2n}$ and satisfies the propagation criteria with respect to all non-zero vectors except for the last row of $A^{-1}$. The nonlinearity of $g^*$ satisfies $N_{g^*} \geq 2^{2n} - 2^n$.

**Proof.** For any non-zero vector $\alpha \in V_{2n+1}$, consider $g(x) \oplus g(x \oplus \alpha)$.

Case 1: $\alpha \neq (0, \cdots, 0, 1)$, from the definition of $g(x)$, $g(x) \oplus g(x \oplus \alpha)$ is balanced, thus $\delta(\alpha) = 0$.

Case 2: $\alpha = (0, \cdots, 0, 1)$, from the definition of $g(x)$, $g(x) \oplus g(x \oplus \alpha) = 1$, thus $\delta(\alpha) = -2^{2n+1}$. 
3.2 On \( V_{2n} \)

3.2.1 Concatenating Sylvester-Hadamard matrix

Note that an even number \( n \geq 4 \) can be expressed as \( n = 4t \) or \( n = 4t + 2 \), where \( t \geq 1 \). The following lemma is proved in Seberry, Zhang and Zheng [121]

**Lemma 3.3** For any integer \( t \geq 1 \) there exists

(i) a balanced function \( f(x) \) on \( V_{4t} \) such that \( N_f \geq 2^{4t-1} - 2^{2t-1} - 2^t \),

(ii) a balanced function \( f(x) \) on \( V_{4t+2} \) such that \( N_f \geq 2^{4t+1} - 2^{2t} - 2^t \).
3.2. On $V_{2n}$

With the above result as a basis, an iterative procedure to improve further the nonlinearity of a function constructed is considered. Note that an even number $n \geq 4$ can be expressed as when $n = 2^m$, $m \geq 2$, or $n = 2^s(2t + 1)$, $s \geq 1$ and $t \geq 1$.

Consider the case when $n = 2^m$, $m \geq 2$. Start with the bent sequence obtained by concatenating the rows of Sylvester-Hadamard matrix $H_{2m-1}$, the sequence consists of $2^{2m-1}$ sequences of length $2^{2m-1}$. Now replace the all-one leading sequence with a bent sequence of the same length, which is obtained by concatenating the rows of $H_{2m-2}$. The replacing process is continued until the length of all-one leading sequence is 4. To finish this procedure, replace the all-one leading sequence $(1, 1, 1, 1)$ with $(1, -1, 1, -1)$. The last replacement makes the entire sequence balanced. By induction on $m = 2, 3, \cdots$, the nonlinearity of the function obtained by such method is at least

$$2^{2m-1} - \frac{1}{2}(2^{2m-1} + 2^{2m-2} + \cdots + 2^2 + 2^2).$$

For the case of $n = 2^s(2t + 1)$, $s \geq 1$, $t \geq 1$, is the same as that for the case of $n = 2^m$, $m \geq 2$, except for the last replacement. In this case the replacing process continues until the length of the all-one leading sequence is $2^{2t+1}$. The last all-one leading sequence is replaced by

$$(e_{2^t}, e_{2^t+1}, \cdots, e_{2^{2t+1}-1}),$$

where $e_i$, $i = 0, \cdots, 2^{t+1} - 1$, is the rows of Sylvester-Hadamard matrix $H_{t+1}$. Again by induction on $s = 1, 2, \cdots$, it can be proved that the nonlinearity of the function is at least

$$2^{2s(2t+1)-1} - \frac{1}{2}(2^{2s-1(2t+1)} + 2^{2s-2(2t+1)} + \cdots + 2^{2(2t+1)} + 2^{2t+1} + 2^{t+1}).$$

Theorem 3.2 (J. Seberry, X. Zhang and Y. Zheng [121]) For any even number $n \geq 4$, there exists a balanced function $f(x)$ on $V_n$ whose nonlinearity is

$$N_f \geq \begin{cases} 
2^{2m-1} - \frac{1}{2}(2^{2m-1} + 2^{2m-2} + \cdots) & n = 2^m \\
+2^2 + 2 \cdot 2^2) & \\
2^{2s(2t+1)-1} - \frac{1}{2}(2^{2s-1(2t+1)} + 2^{2s-2(2t+1)} + \cdots + 2^{2(2t+1)} + 2^{2t+1} + 2^{t+1}) & n = 2^s(2t + 1).
\end{cases}$$

Let $\xi = (\xi_0, \xi_1, \cdots, \xi_{2^k-1})$ be a sequence of length $2^{2k}$ obtained by modifying a bent sequence. Permuting and changing signs can also be applied to $\xi$. In this case there are $2^{2k} \cdot 2^k!$ different balanced functions, all of which have the same nonlinearity.

3.2.2 Concatenating Boolean bent functions.
3.2. On $V_{2^n}$

Let $f(x_1, \ldots, x_{2n})$ be a bent function on $V_{2n}$, and define

$$g(x_1, \ldots, x_{2n}, x_{2n+1}, x_{2n+2}) = f(x_1, \ldots, x_{2n}) \oplus x_{2n+1} \oplus x_{2n+2}.$$ 

Set $g^*(x) = g(xA)$ where $A$ is a $(2n + 2) \times (2n + 2)$ nonsingular matrix over $GF(2)$. By corollary 7 of [121], $g^*(x)$ is a balanced function on $V_{2n+2}$ with nonlinearity $N_{g^*} \geq 2^{2n+1} - 2^n + 1$ and satisfied the propagation criterion with respect to all but three non-zero vectors.

3.2.3 Concatenating Linear Functions

Let $m < n$, $y = (y_1, \ldots, y_m)$ and $x = (x_1, \ldots, x_n)$. Since there exist $2^n$ distinct linear functions on $V_n$, choose $2^m$ different those and give each a subscript $\delta \in V_m$ and denote the set by $\mathcal{R}_m$, i.e., $\mathcal{R}_m = \{ \phi_\delta | \delta \in V_m\}$, one can construct balanced, highly nonlinear Boolean functions satisfying the propagation criterion by following method

$$g(y, x) = \bigoplus_{\delta \in V_m} D_\delta(y) \phi_\delta(x),$$

where $D_\delta(y) = \begin{cases} 1, & \text{if } y = \delta, \\ 0, & \text{otherwise} \end{cases}$.

By lemma 3 of [119],

(i) $g(y, x)$ is balanced,

(ii) the nonlinearity of $g$ satisfies $N_g \geq 2^{n+m-1} - 2^{n-1},$

(iii) $g(y, x)$ satisfies the propagation criterion with respect to any $\gamma = (\beta, \alpha)$

with $\beta \neq (0, \ldots, 0)$, $\beta \in V_m$ and $\alpha \in V_n$,

(iv) the degree of $g(y, x)$ can be $m + 1$ if the $2^m$ linear functions are selected appropriate.

Let $\xi_\delta$ be the sequence of $\phi_\delta(x)$ and $\eta$ be the sequence of $g(y, x)$. By Lemma 1 of [118], $\eta$ is a concatenation of $2^m$ distinct $\xi_\delta$.

Let $H_m$ and $H_n$ are Sylvester-Hadamard matrices as defined before, $l'$ be a row of $H_m$ and $l''$ be a row of $H_n$. Note that $H_{n+m} = H_n \times H_m$, hence any row of $H_{n+m}$, say $L$, can be represented as $L = l' \times l''$. Since $H_m$ is a orthogonal matrix, then

$$\langle \eta, L \rangle = \begin{cases} \pm 2^n & \text{if } f \in \mathcal{R}_m, \\ 0 & \text{if } f \notin \mathcal{R}_m, \end{cases}$$

where $f$ be a linear functions of sequence $l''$. There are $2^m$ sequences of $l'' \in \mathcal{R}_m$. 
3.2.4 Concatenating Bent Functions and Linear Functions

Let \( f(x_1, \ldots, x_{2n-2}) \) be a bent function on \( V_{2n-2} \) whose sequence is \( \xi \). Let \( l_1, l_2, l_3 \) be the sequences of three different linear functions. Hence \( \xi \ast l_i, i = 1, 2, 3 \), are three bent sequences. Without loss of generality, suppose \( \xi \ast l_2 \) contains \( 2^{2n-3} + 2^{n-2} \) ones, \( 2^{2n-3} - 2^{n-2} \) negative ones. \( \xi \ast l_1 \) and \( \xi \ast l_3 \) contain \( (2^{2n-3} - 2^{n-2}) \) ones and \( (2^{2n-3} + 2^{n-2}) \) negative ones. Thus \( \gamma = (\xi, \xi \ast l_1, \xi \ast l_2, \xi \ast l_3) \) is a balanced sequence of length \( 2^{2n} \).

**Theorem 3.3** (J. Seberry and X. Zhang [118]) For any integer \( n \geq 2 \), there exists a balanced Boolean function on \( V_{2n} \) with SAC and its nonlinearity is \( 2^{2n-1} - 2^n \).

**Example 3.2** Let \( n = 3 \). Set \( \xi = (1, 1, 1, 1, -1, 1, -1, 1, 1, -1, 1, -1, 1, -1) \) be a bent sequence of length \( 2^4 = 16 \), whose Boolean function is \( f(x) = x_1 x_3 \oplus x_2 x_4 \). Choose linear Boolean functions \( g_1(x) = x_1, g_2(x) = x_1 \oplus x_2, g_3(x) = x_1 \oplus x_2 \oplus x_3 \) on \( V_4 \) and their sequences are

\[
\begin{align*}
    l_1 &= (1, 1, 1, 1, 1, 1, 1, 1, -1, -1, -1, -1, -1, -1, -1), \\
    l_2 &= (1, 1, 1, 1, -1, -1, -1, -1, -1, -1, -1, 1, 1, 1, 1), \\
    l_3 &= (1, 1, -1, -1, -1, -1, 1, 1, -1, -1, -1, 1, 1, 1, -1, -1)
\end{align*}
\]

respectively. Hence

\[
\begin{align*}
    \xi \ast l_1 &= (1, 1, 1, 1, 1, -1, 1, -1, -1, -1, -1, 1, 1, -1, 1, 1, -1), \\
    \xi \ast l_2 &= (1, 1, 1, 1, -1, 1, -1, -1, -1, -1, 1, 1, 1, 1, -1, 1), \\
    \xi \ast l_3 &= (1, 1, -1, -1, -1, -1, 1, 1, -1, -1, -1, 1, 1, 1, -1, 1)
\end{align*}
\]

are also bent sequences. Set the sequence \( \gamma = (\xi, \xi \ast l_1, -\xi \ast l_2, \xi \ast l_3) \). Then \( \gamma \) is a balanced sequence and the function is

\[
Q(y) = y_1 y_2 y_3 \oplus y_1 y_2 y_5 \oplus y_1 y_2 \oplus y_1 y_3 \oplus y_1 y_4 \oplus y_2 y_3 \oplus y_3 y_5 \oplus y_4 y_6 \oplus y_1,
\]

where \( y \in V_6 \). By Theorem 3.3, the function \( Q(y) \) is balanced on \( V_6 \) with SAC and \( N_Q = 2^{2n-1} - 2^n = 24 \).

### 3.3 Applications on Boolean functions

The terms *diffusion* and *confusion* were introduced by Claude Shannon to capture the two basic building blocks for any cryptographic system (see [131]).
In **diffusion**, the statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext. This is achieved by having each plaintext affect many ciphertext. The relationship between the plaintext and ciphertext should be as complex as possible in order to thwart attempts to deduce the key.

On the other hand, **confusion** seeks to make the relationship between the statistics of ciphertext and the value of the encryption key as complex as possible, again to thwart attempts to discover the key. This is achieved by the use of a complex substitution algorithm.

The most widely used encryption scheme is based on the **DES** adopted in 1977 by the National Bureau of Standards. The implementation of DES use $S-$boxes to provide confusion and $P-$boxes to provide diffusion, which $P-$boxes spread out the output bits to different $S-$boxes of the next round. $P-$boxes have usually a fixed permutation of input and output bits. The strength of the DES mainly comes from the "properly" designed $S-$boxes.

In the recent past, a number of criteria for designing strong $S-$boxes have been identified by researchers in the field, including Gordon and Retkin [38], Webster and Tavares [149], Adams and Tavares [1], [2], [3], O’Connor [21], and Seberry, Zhang and Zheng [119]. Some of the criteria include high nonlinearity, the SAC, high order propagation, high nonlinear order and correlation immunity.

Differential cryptanalysis and linear cryptanalysis, discovered by Biham and Shamir [12] and Matsui [75] respectively, are currently the most powerful cryptanalytic attacks against secret-key encryption ciphers (algorithms), especially against DES-like substitution-permutation ciphers. The attacks also apply to other cryptographic primitives such as one-way functions. Since the introduction of differential cryptanalysis, researchers have devoted considerable effort to the design of $S-$boxes which are the core of many modern private key data encryption and hashing algorithms such as DES, LOKI, CASE, MD4, MD5 and HAVAL. Mister and Adams [87] suggest that all linear combinations of $S-$Box columns should be bent.

One obvious characteristic of the $S-$box is its size. An $n \times m$ $S-$box has $n$ bits input and $m$ bits output. DES has $6 \times 4$ $S-$boxes. Both Blowfish and CAST, describe in B. Schneier [128] and [129], and Carlisle Adams [4], have $8 \times 32$ $S-$boxes. The designers of CAST make use of the theory of bent functions to design the $S-$boxes that have a high nonlinearity.

Larger $S-$boxes, by and large, are more resistant to differential and linear cryptanalysis ([130]). The larger the dimension $n$, the (exponentially) larger the lookup
3.3. Applications on Boolean functions

Thus, for practical reasons, a limit of $n$ equal to 8 or 10 is usually imposed. Another practical consideration is that the larger $S$–box is, the more difficult it is to design it properly.

The **LOKI** algorithm was designed by L. Brown, M. Kwan, J. Pieprzyk and J. Seberry. The first version called LOKI89 was published in [13]. The revised version LOKI91 can be found in [14]. The newest version of LOKI is “LOKI97”, which was one of the competitors for the Advance Encryption Standard (AES). LOKI applies many copies of a single $S$–Box which is based on cubic Boolean functions on $GF(2)^8$. The $S$–Boxes applied in LOKI is $12 \times 8$ $S$–Boxes.

Improvements in the speed and power of microprocessor chips have meant that the DES with its 56-bit key is subject to brute-force attacks that can be carried out by organizations of moderate size. The National Institute of Standards and Technology (NIST), a branch of the U. S. Government, has sought public submissions of an improved block cipher which would serve the specific purpose of protecting the unclassified communications of the U. S. Government as well as serve the public sector. The accepted block cipher will be called the Advanced Encryption Standard (AES). On October 2, 2000, the cipher **Rijndael** will serve as the Advanced Encryption Standard has been announced.

The **Rijndael** cipher was designed by Joan Daemen and Vincent Rijmen. It is selected by the NIST as proposed the Advanced Encryption Standard (AES) algorithm. The cipher works for three block sizes: 128, 192 and 256 bits. Rijndael applies the Shannon product cipher concept and cryptographic operations use heavily arithmetic in $GF(2)^8$. The designers use a $8 \times 8$ $S$–box, which the first step is to replace each byte with its reciprocal in the same $GF(2)^8$ in the Mix Column step, except that 0, which has no reciprocal, is replaced by itself (see website [165] or [166] for details).

The **Serpent** cipher was submitted for AES competition. It was designed by Ross Anderson, Eli Biham and Lars Knudsen. Serpent handles 128–bit message and cryptograms using a cryptographic key which can be either 128 or 192 or 256–bit long. It implements Shannon $S$–$P$ network. $S$–boxes are $4 \times 4$. There are 8 different $S$–Boxes $S_0, \ldots, S_7$. The $i$–th round applies 32 copies of the same $S$–box $S_i$, $i = 0, \ldots, 7$. $S$–boxes used in Serpent are generated from DES $S$–Boxes. The following procedure is used to generate the necessary eight $S$–Boxes (see website [167] for details).

```plaintext
index = 0

do

    currentSBox = index mod 32
```

```
for i = 0 to 15
    j = sbox[(currentSBox+l) mod 32][serpent[i]]
    swapEntries(sbox[currentSBox][i], sbox[currentSBox][j])
    if sbox[currentSBox] has the desired properties, then save it
    index = index + 1
until eight S-boxes have been saved

The intention of the designers of Serpent was to convince potential users that the S-boxes have been designed without trapdoor.

The Twofish algorithm was an AES candidate designed by It is a Feistel cipher with 16 uniform rounds. The round function consists of two copies of the function $g$, which is built on four 8-bit S-Boxes. Each S-Box is a permutation controlled by a cryptographic key. The outputs from the four S-Boxes are mixed using maximum distance separable code. The outputs from the two copies of $g$ are combined by using modular addition. Each S-box is formed as follows (see website [165] and [168] for details):

- The input byte is split into its most significant and least significant halves, A and B.
- The new value of A is the XOR of the old values of A and B.
- The new value of B is the XOR of the old value of A, B rotated right one bit, and 8 if the old value of A was odd.
- A and B are then replaced by their substitutes in the 16-bit S-boxes T0 and T1 respectively.
- The new value of A is the XOR of the old values of A and B.
- The new value of B is the XOR of the old value of A, B rotated right one bit, and 8 if the old value of A was odd.
- A and B are then replaced by their substitutes in the 16-bit S-boxes T2 and T3 respectively.
- A and B are then combined in reverse order to form the result byte.

Based on early work in [2], [25], [26], [91], [141], Seberry and X-M Zhang identified the three principles for strong difference distribution tables of S-boxes which
is captured by a measurement called \textit{robustness}. So far no efficient method has been found to generate $S$-boxes having good difference distributions and also satisfying other criteria.
Chapter 4

Hadamard Matrices and Block Designs

The application of Hadamard matrices touch on statistics, error correction coding theory, communications signaling, Boolean function analysis and synthesis, image processing, sequence theory and signal representation.

In this chapter the author introduced notations of M. Xia which may not be widely disseminated.

4.1 Definitions

Definition 4.1 (Hadamard matrix) An Hadamard matrix $H$ of order $n$ is an $n \times n$ matrix with entries $\pm 1$, such that

$$HH^T = nI_n,$$

where $I_n$ is an $n \times n$ identity matrix. That is, the row (or column) of $H$ are pairwise orthogonal.

Let $G$ be an abelian group of order $v$ with the addition $\oplus$ and the subtraction $\ominus$, respectively. Consider the polynomials in the elements of $G$ over the field of rational numbers $\sum_{g \in G} a(g)g$ and define the addition

$$(\sum_g a(g)g) + (\sum_g b(g)g) = \sum_g (a(g) + b(g))g$$

In this polynomials the element "0" of $G$ is denoted by $\theta$, and write

$$T = \sum_{g \in G} g, \quad T^* = T - \theta$$

When $G$ is a finite field, define the multiplication

$$(\sum_g a(g)g)(\sum_h b(h)h) = \sum_k \left(\sum_{gh=k} a(g)b(h)\right)k$$
4.1. Definitions

For subsets $A, B$ of $G$, write

$$A \Theta B = \sum_{a \in A, b \in B} (a \Theta b), \quad \Delta A = A \Theta A,$$

$$\Delta (A, B) = (A \Theta B) + (B \Theta A).$$

Obviously, $\Delta (A, A) = 2 \Delta A$ and $\Delta \phi = 0, \Delta (\phi, A) = 0$ for any $A \subset G$.

**Definition 4.2 (DS)** A subset of $k$ elements $D = \{a_1, \ldots, a_k\}$ of a group $G = G(v, +)$ is called a $(v, k, \lambda)$—difference set (DS), if among the collection of elements $\{a_i - a_j : i \neq j, 1 \leq i, j \leq k\}$ all the non-zero elements of $G$ occur $\lambda$ times.

**Definition 4.3 (SDS)** Let $D_i \subset G, |D_i| = k_i, i = 1, \ldots, r$. If

$$\sum_{i=1}^{r} \Delta D_i = (\sum_{i=1}^{r} k_i - \lambda) \theta + \lambda T,$$

$\lambda \geq 0$, then $D_1, \ldots, D_r$ are $r - \{v; k_1, \ldots, k_r; \lambda\}$ supplementary difference sets (SDS), where $v = |G|$.

When $r = 4$ and $\lambda = \sum_{i=1}^{4} k_i - v$, $D_1, D_2, D_3$ and $D_4$ can be used to form an Hadamard matrix. They are denoted as SDS of type $H$.

If $k_1 = \cdots = k_r = k$, $D_1, \ldots, D_r$ can be simplified as $r - \{v; k; \lambda\}$ SDS. When $r = 1$, the SDS become the DS in the usual sense (see [117], [152], [154], [155], [156], [157], [160], [159] for details).

Hadamard matrices can be constructed using difference sets (DS), and can also be constructed using supplementary difference sets (SDS). Only $r = 4$ and $\lambda = \sum_{i=1}^{4} k_i - v$ be considered in this thesis. In this case, $D_1, D_2, D_3, D_4$ are called type $H$–SDS.

**Definition 4.4 (Regular Hadamard matrix)** An Hadamard matrix $H$ is said to be regular if the sum of all the elements in each row or column is a constant value $k$. Hence $HJ = JH = kJ$, where $J$ is the matrix of all ones.

**Definition 4.5 (Kronecker product)** If $M = (m_{ij})$ is a $m \times n$ matrix and $N = (n_{ij})$ is a $p \times q$ matrix, then the Kronecker product $M \times N$ is the $mp \times nq$ matrix given by

$$M \times N = \begin{pmatrix}
  m_{11}N & m_{12}N & \cdots & m_{1n}N \\
  m_{21}N & m_{22}N & \cdots & m_{2n}N \\
  \vdots & \vdots & \ddots & \vdots \\
  m_{m1}N & m_{m2}N & \cdots & m_{mn}N
\end{pmatrix}. $$
4.1. Definitions

**Definition 4.6 (Amicable)** $X$ and $Y$ are said to be amicable if $XY^T = YX^T$.

**Definition 4.7 (C-partitions)** $A_1, A_2, \ldots, A_8$ are called C-partitions of an abelian group $G$ of order $v$, if the following three conditions are satisfied:

(i) $A_i \cap A_j = \emptyset$, $i \neq j$;

(ii) $\cup_{i=1}^{8} A_i = G$;

(iii) $\sum_{i=1}^{8} \Delta A_i = v\theta + \sum_{i=1}^{4} \Delta(A_i, A_{i+4})$.

**Definition 4.8 (T-matrices)** $(0, \pm 1)$ matrices $T_1, T_2, T_3, T_4$ of order $t$ are called T-matrices, if the following four conditions are satisfied:

1. They are mutually commutative;

2. There is a monomial matrix $R$ of order $t$, $R^T = R$, $R^2 = I$, such that $(T_i R)^T = T_i R$, $i = 1, 2, 3, 4$;

3. Write $T_i \left( t_{ijk}^{(i)} \right)_{1 \leq j, k \leq t}$, then $\sum_{i=1}^{4} |t_{ijk}^{(i)}| = 1$, $1 \leq j, k \leq t$, $i = 1, 2, 3, 4$;

4. $\sum_{i=1}^{4} T_i T_i^T = tI$;

The condition that T-matrices are circulant is not necessary. It has been replaced by (1) and (2). In an abelian case they are very easy satisfied.

**Definition 4.9 (Type H0)** The collection $\{(D_1, D_2, D_3, D_4) : D_1, D_2, D_3, D_4$ are SDS of type $H\}$ is defined as the class $H_0$. The orders, $v$, for which $D_1, D_2, D_3, D_4$ exist is denote $H_0(v)$.

**Definition 4.10 (Type H1)** Let $D_1, D_2, D_3, D_4 \subset G$ be SDS of order $v$. $|D_i| = k_i$, $i = 1, 2, 3, 4$. $D_1, D_2, D_3, D_4 \in H_1$ if and only if

$$\sum_{i=1}^{4} \Delta D_i = v\theta + \lambda T,$$

and

$$\Delta(D_1, D_2) + \Delta(D_3, D_4) = \lambda T,$$

where $\lambda = k_1 + k_2 + k_3 + k_4 - v$.

**Definition 4.11 (Type W0)** $(D_1, D_2, D_3, D_4) \in W_0$ if and only if $-D_i = D_i$, $i = 1, 2, 3, 4$ and

$$\sum_{i=1}^{4} \Delta D_i = v\theta + (k_1 + k_2 + k_3 + k - 4 - v)T$$

where $k_i$ is the number of elements in $D_i$, $i = 1, 2, 3, 4$. 

4.2 History

More than one hundred years ago, in 1893, Jacques Hadamard [39] found square matrices of order 12 and 20, with entries ±1, which had all their rows (and columns) pairwise orthogonal. These matrices, \( X = (x_{ij}) \), satisfied the equality of the following inequality,

\[
| \det X |^2 \leq \prod_{i=1}^{n} \sum_{j=1}^{n} | x_{ij} |^2,
\]

and so had maximal determinant among matrices with entries ±1. This is discussed in further detail in the survey by J. Seberry and M. Yamada [117].

In 1984, M. Xia introduced \( C \)-partitions, and used some special supplementary difference sets on Abelian group to construct \( T \)-matrices [152]. After 1990, he defined some new classes of supplementary difference sets: \( H_0, H_1, W_0, W_2 \), which used to construct \textit{Hadamard} matrices. This enhanced the methods of using the known \textit{Hadamard} matrices to construct new \textit{Hadamard} matrices [153]. In 1991, M. Xia and G. Liu proved that for any prime power \( q \equiv 1(\mod 4) \), \( W_0(q^2) \neq \phi \) and there exists Williamson type \textit{Hadamard} matrix of order \( 4q^2 \) [154]. In 1992, M. Xia proved that for any prime power \( q \equiv 3(\mod 4) \), \( W_2(N^2) \neq \phi \) and there exist \((4N^2,2N^2 - N,N^2 - N)\) difference sets and special Williamson type \textit{Hadamard} matrices, where \( N = 2^a 3^b (p_1^{r_1} \cdots p_n^{r_n})^2 \), \( p_j \equiv 3(\mod 4) \) be prime, integers \( a,b,r_j \geq 0, j = 1,\ldots,n \). [155]. In 1994, M. Xia and T. Xia proved that for any prime power \( q \equiv 5(\mod 8) \), \( H_1(q^2N^2) \neq \phi \), where exist \((4N^2,2N^2 - N,N^2 - N)\) \textit{Hadamard} difference sets [156]. In 1996, M. Xia and G. Liu proved that for any prime power \( q \equiv 3(\mod 8) \), \( H_0(q^2) \neq \phi \), and there exist
4.3 Overview of construction of Hadamard matrices

In 1997, Y. Chen proved that for any \( q \equiv 1 \mod 2 \) be a prime power, there exists \((4q^4, 2q^4 - q^2, q^4 - q^2)\) supplementary difference set, in this case there exists \((4N^2, 2N^2 - N, N^2 - N)\) difference set and special Williamson type Hadamard matrices of order \( N^2 \), where \( N = 2^a3^b m^2 \), \( a, b = 0 \) or 1, \( m \) be an arbitrary integer [18]. Since then, one can say for any integer \( m \), there exists Hadamard matrix of order \( 4m^4 \). In 1999, M. Xia and T. Xia proved that there exist \( T \)-matrices of order \( q^2 \), where \( q \equiv 3 \mod 8 \) be a prime power [161]. This is the first infinite class of \( T \)-matrices got by using supplementary difference sets on Abelian groups.

4.3 Overview of construction of Hadamard matrices

In this section, an overview of construction methods for Hadamard matrices is given. Constructions for Hadamard matrices can be roughly classified into three types:

1. Multiplication theorems;
2. Direct constructions;
3. "Plug-in" methods;

Hadamard’s original construction for Hadamard matrices is a “multiplication theorem” as it uses the fact that the Kronecker product of Hadamard matrices of order \( 2^a m \) and \( 2^b n \) is an Hadamard matrix of order \( 2^{a+b} mn \). In [5] Agaian shows how to multiply these Hadamard matrices to get an Hadamard matrix of order \( 2^{a+b-1} mn \).

Paley’s “direct” construction in 1933 [92], which gives Hadamard matrices of order \( \Pi_{i,j}(p_i + 1)(2(q_j + 1)), \) \( p_i \equiv 3 \mod 4 \), \( q_j \equiv 1 \mod 4 \) are prime power, is extremely productive of Hadamard matrices.

In 1944, J. Williamson [150], who coined the name Hadamard matrices, first constructed what have come to be called Williamson matrices, or with a small set of conditions, Williamson type matrices. These matrices are used to replace the variables of a formally orthogonal matrix. Williamson type matrices are “plugged-in” to the second matrix. The matrices that can be “plugged-in” to arrays of variables are called suitable matrices. Generally the arrays into which suitable matrices are plugged are orthogonal designs, which have formally orthogonal rows (and columns) but may have variations such as Goethals-Seidel arrays, Agaian families, Kharaghani’s methods, and
4.4. Background

A square matrix with elements $\pm 1$ and order $h$, whose distinct row vectors are orthogonal is an Hadamard matrix of order $h$. The smallest examples are

\[
\begin{pmatrix}
1 & 1 \\
1 & -1
\end{pmatrix},
\begin{pmatrix}
-1 & 1 & 1 & 1 \\
1 & -1 & 1 & 1 \\
1 & 1 & -1 & 1 \\
1 & 1 & 1 & -1
\end{pmatrix}
\]
4.4. Background

These were first studied by J. J. Sylvester [139] who observed that if $H$ is a Hadamard matrix, then

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

is also an Hadamard matrix. Indeed, using the Hadamard matrix of order 2,

**Lemma 4.1** (Sylvester [139]) There is an Hadamard matrix of order $2^t$ for all integers $t$.

The matrices of order $2^t$ constructed by Sylvester's construction are Sylvester-Hadamard matrices.

Ahmed and Rao (1975) provide an exponential definition for Hadamard matrix $H_n$ by writing it directly as

$$H_n = (h_{ij}), \quad h_{ij} = (-1)^{(i,j)},$$

where $(i,j)$ is the inner product of two vectors on $GF(2)^n$ (see [164] for details).

Arguing further, as per Harwit and Sloane (1979), consider a Hadamard matrix for which order $n > 2$. For orthogonality to obtain, for any two distinct rows, $i$ and $j$, not involving the all ones (or all minus ones) row, there must exist $\frac{n}{4}$ columns where the elements of rows $i$ and $j$ are both +1, $\frac{n}{4}$ columns where the elements of rows $i$ and $j$ are +1 and −1 respectively, $\frac{n}{4}$ columns where the elements of rows $i$ and $j$ are −1 and +1 respectively, and $\frac{n}{4}$ columns where the elements of rows $i$ and $j$ are both −1. Thus, a Hadamard matrix cannot exist for an order $n$ greater than 2 which is $n \neq 0 (mod 4)$.

Two Hadamard matrices are said to be Hadamard equivalent (or just equivalent) if one can be obtained from the other by a sequence of operations of the following types:

1. Permute rows (or columns),
2. Multiply any row (or columns) by −1.

Recall some basic properties of Hadamard matrices.

**Lemma 4.2** Let $H$ be an Hadamard matrix of order $h$, the following hold:

1. $HH^T = hI_h$,
2. $|\det H| = h^{\frac{h}{2}}$,
3. $HH^T = H^TH$, 


4. Every Hadamard matrix is equivalent to an Hadamard matrix that has every element of its first row and column +1 (matrices of this latter form are called normalized),

5. \( h = 1, 2, \) or \( 4n, \) \( n \) is an integer,

6. If \( H \) is a normalized Hadamard matrix of order \( 4n, \) then every row (column) except the first has \( 2n \) minus ones and \( 2n \) positive ones, further, \( n \) minus ones in any row (column) overlap with \( n \) minus ones in each other row (column).

**Lemma 4.3** (Hadamard [39]) Let \( H_1 \) and \( H_2 \) be Hadamard matrices of orders \( h_1 \) and \( h_2. \) Then \( H = H_1 \times H_2 \) is an Hadamard matrix of order \( h_1 h_2. \)

The stronger result than Hadamard’s, first proved by Agayan and Sarukhanyan, and then strengthened by Seberry and Yamada [115] and Agayan-Sarukhanyan [5]. These theorems have the advantage of reducing the power of two in the resulting Hadamard matrix.

**Lemma 4.4** (The multiplication theorem of Agayan-Sarukhanyan [5]). Let \( H_1 \) and \( H_2 \) be Hadamard matrices of orders \( 4h \) and \( 4k, \) then there is an Hadamard matrix of order \( 8hk. \)

There are Hadamard matrices of orders 12 and 20. Sylvester’s lemma guarantees the existence of an Hadamard matrix of order 240, while the Agayan-Sarukhanyan guarantees the existence of order 120.

This can also be strengthened.

**Theorem 4.1** (Craigen, Seberry and Zhang [24]) Suppose that there are Hadamard matrices of orders \( 4a, 4b, 4c, 4d. \) Then there is an Hadamard matrix of order \( 16abcd. \)

The strongest construction theorems for Hadamard matrices is given below. These theorems do not give all the known orders but give the vast majority of those known.

**Theorem 4.2** (Paley [92]) Let \( p \equiv 3(\text{mod } 4) \) be a prime power. Then there is an Hadamard matrix of order \( p + 1. \)

**Theorem 4.3** (Paley [92]) Let \( p \equiv 1(\text{mod } 4) \) be a prime power. Then there is an Hadamard matrix of order \( 2(p + 1). \)

**Theorem 4.4** (Goethals-Seidel [37]) Suppose that there is an Hadamard matrix of order \( h. \) Then there is a regular symmetric Hadamard matrix with constant diagonal of order \( h^2. \)
Chapter 5

Construction of Hadamard matrices and their applications

In this chapter some methods of constructing Hadamard matrices are introduced. In section 5.1 the Williamson methods of constructing Hadamard matrices is introduced. In section 5.2 and 5.3 the other methods of constructing Hadamard matrices are introduced. At the end of the chapter, there is a table of Williamson type Hadamard matrices. 10 percent of the results in the table is due to the author of this thesis. Unfortunately, no new matrices were found as a result of the searches run so far. However, independent verification of results from previous searches has been provided.

5.1 Williamson type Hadamard matrices

**Definition 5.1** (Williamson matrices and Williamson-type matrices) Four circulant symmetric ±1 matrices $A, B, C, D$ of order $w$ that satisfy $AA^T + BB^T + CC^T + DD^T = 4wI_w$ will be called Williamson matrices.

Four ±1 matrices $A, B, C, D$ of order $w$ that satisfy

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

and $AA^T + BB^T + CC^T + DD^T = 4wI_w$ will be called Williamson-type matrices.

Analogously, eight circulant symmetric ±1 matrices $A_1, A_2, \ldots$ and $A_8$ of order $w$ which satisfy

$$\sum_{i=1}^{8} A_iA_i^T = 8wI_w \quad (5.1)$$

will be called 8—Williamson matrices.

Eight ±1 amicable matrices $A_1, A_2, \ldots$ and $A_8$ of order $w$ which satisfy (5.1) and

$$A_iA_j^T = A_jA_i^T, \quad i, j = 1, \ldots, 8,$$

will be called 8—Williamson-type matrices.
Theorem 5.1 (Williamson) Suppose there exist four symmetric \((1,-1)\) matrices of order \(n\) which commute in pairs. Further, suppose

\[ A^2 + B^2 + C^2 + D^2 = 4nI_n \quad (5.2) \]

Then

\[
H = \begin{bmatrix}
A & B & C & D \\
-B & A & -D & C \\
-C & D & A & -B \\
-D & -C & B & A
\end{bmatrix} \quad (5.3)
\]

is an Hadamard matrix of order \(4n\) of Williamson type or quaternion type.

When \(A, B, C, D\) are all polynomials in the same matrix, they certainly commute in pairs. Let

\[
T = \begin{bmatrix}
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
& & \cdots & \cdots & \cdots \\
0 & 0 & 0 & \cdots & 1 \\
1 & 0 & 0 & \cdots & 0
\end{bmatrix} \quad (5.4)
\]

and note

\[
T^n = I, \quad (T^i)^* = (T^i)^t = T^{n-i} \quad (5.5)
\]

Let

\[
\begin{align*}
A & = \sum_{i=0}^{n-1} a_i T^i, & a_i = \pm 1, a_{n-i} = a_i \\
B & = \sum_{i=0}^{n-1} b_i T^i, & b_i = \pm 1, b_{n-i} = b_i \\
C & = \sum_{i=0}^{n-1} c_i T^i, & c_i = \pm 1, c_{n-i} = c_i \\
D & = \sum_{i=0}^{n-1} d_i T^i, & d_i = \pm 1, d_{n-i} = d_i
\end{align*} \quad (5.6)
\]

Theorem 5.2 (Williamson) If there exist solutions to the equations

\[
\mu_i = 1 + 2 \sum_{j=1}^{s} t_{ij} (\omega^j + \omega^{n-j}), \quad i = 1, 2, 3, 4 
\]

where \(s = \frac{1}{2}(n-1)\), \(\omega\) is a \(n\)th root of unity, exactly one of \(t_{1j}, t_{2j}, t_{3j}, t_{4j}\) is nonzero and equals \(\pm 1\) for each \(1 \leq j \leq s\), and

\[
\mu_1^2 + \mu_2^2 + \mu_3^2 + \mu_4^2 = 4n
\]
then there exist solutions to the equations.

\[
\begin{align*}
A &= \sum_{i=0}^{n-1} a_i T^i, \quad a_0 = 1, a_i = a_{n-i} = \pm 1 \\
B &= \sum_{i=0}^{n-1} b_i T^i, \quad b_0 = 1, b_i = b_{n-i} = \pm 1 \\
C &= \sum_{i=0}^{n-1} c_i T^i, \quad c_0 = 1, c_i = c_{n-i} = \pm 1 \\
D &= \sum_{i=0}^{n-1} d_i T^i, \quad d_0 = 1, d_i = d_{n-i} = \pm 1
\end{align*}
\]

That is, there exists an Hadamard matrix of order 4n.

Assume

\[
\begin{align*}
2A &= -\mu_1 + \mu_2 + \mu_3 + \mu_4 = 2 \left( 1 + \sum_{j=1}^{s} (-t_{1j} + t_{2j} + t_{3j} + t_{4j}) (\omega^{j} + \omega^{n-j}) \right) \\
2B &= \mu_1 - \mu_2 + \mu_3 + \mu_4 = 2 \left( 1 + \sum_{j=1}^{s} (t_{1j} - t_{2j} + t_{3j} + t_{4j}) (\omega^{j} + \omega^{n-j}) \right) \\
2C &= \mu_1 + \mu_2 - \mu_3 + \mu_4 = 2 \left( 1 + \sum_{j=1}^{s} (t_{1j} + t_{2j} - t_{3j} + t_{4j}) (\omega^{j} + \omega^{n-j}) \right) \\
2D &= \mu_1 + \mu_2 + \mu_3 - \mu_4 = 2 \left( 1 + \sum_{j=1}^{s} (t_{1j} + t_{2j} + t_{3j} - t_{4j}) (\omega^{j} + \omega^{n-j}) \right)
\end{align*}
\]

(5.8)

If \( t_{ij} \neq 0 \) then the coefficient of \( \omega^{j} + \omega^{n-j} \) in an equation of (5.8) is different from the coefficient of \( \omega^{j} + \omega^{n-j} \) in the other equations. Thus with (5.7),

\[
\begin{align*}
a_j &= -t_{1j} + t_{2j} + t_{3j} + t_{4j} \\
b_j &= t_{1j} - t_{2j} + t_{3j} + t_{4j} \\
c_j &= t_{1j} + t_{2j} - t_{3j} + t_{4j} \\
d_j &= t_{1j} + t_{2j} + t_{3j} - t_{4j}
\end{align*}
\]

From here assume that \( n \) is odd. Let

\[
A = P_1 - N_1
\]

(5.9)

where \( P_1 \) is the sum of positive terms in \( A \), \( N_1 \) is the negative terms in \( A \). So

\[
P_1 = \sum_{j} a_j T^j, a_j = 1; \quad -N_1 = \sum_{j} a_j T^j, a_j = -1;
\]

(5.10)

In the same way write

\[
B = P_2 - N_2; \quad C = P_3 - N_3; \quad D = P_4 - N_4
\]

(5.11)

Since \( a_0 = 1 \), and \( a_{n-i} = a_i, i = 1, \ldots, n - 1 \), the positive terms except \( a_0 \) occur in pairs, hence \( p_1 \), the number of terms in \( P_1 \), is an odd number. Similarly, \( p_2, p_3, p_4 \) are odd numbers.

Let us write

\[
G = I + T + T^2 + \cdots + T^{n-1}
\]

(5.12)
Then

\[ P_i + N_i = G, \ i = 1, 2, 3, 4 \quad (5.13) \]

From (5.2) there is

\[ (2P_1 - G)^2 + (2P_2 - G)^2 + (2P_3 - G)^2 + (2P_4 - G)^2 = 4n \quad (5.14) \]

Since \( T_j G = G \) for all \( j \), then \( P_j G = p_j G \) and \( G^2 = nG \). So (5.14) takes the form

\[ 4(P_1^2 + P_2^2 + P_3^2 + P_4^2) - 4(p_1 + p_2 + p_3 + p_4)G + 4nG = 4nI_n \quad (5.15) \]

Divided by 4 becomes

\[ P_1^2 + P_2^2 + P_3^2 + P_4^2 = (p_1 + p_2 + p_3 + p_4 - n)G + nI_n \quad (5.16) \]

Since each \( p_i \) is odd and \( n \) is odd, \( p_1 + p_2 + p_3 + p_4 - n \) on the right side of (5.16) must be odd number. In \( P_i^2 = (\sum T^k)^2, k \) in a subset of 0, 1, \( \cdots, n - 1 \). Then \( P_i^2 \equiv \sum T^{2k} \pmod{2} \). Hence, every \( T^j = (T^k)^2, j = 1, \cdots, n - 1 \), to appear with an odd coefficient on the left side of (5.16), must occurs exactly one or three times in the set of \( P_1, P_2, P_3, P_4 \).

**Theorem 5.3 (Williamson)** Let \( n \) be odd, and matrices \( A, B, C, D \) satisfy (5.2) and (5.6), suppose \( a_0 = b_0 = c_0 = d_0 = 1 \), then exactly three of \( a_j, b_j, c_j, d_j, 1 \leq j \leq n - 1 \), have the same sign.

**Example 5.1** Let \( n = 9, 4 \times 9 = 36 = 1^2 + 1^2 + 3^2 + 5^2 \). So

\[
\begin{align*}
\mu_1 &= 1 \\
\mu_2 &= 1 \\
\mu_3 &= 1 - 2(\omega^2 + \omega^7) \\
\mu_4 &= 1 + 2(\omega + \omega^8) + 2(\omega^3 + \omega^6) - 2(\omega^4 + \omega^5)
\end{align*}
\]

Now

\[
\mu_1^2 + \mu_2^2 + \mu_3^2 + \mu_4^2
\]

\[
= 1^2 + 1^2 + (1 - 2\omega^2 - 2\omega^7)^2 + (1 + 2\omega + 2\omega^8 + 2\omega^3 + 2\omega^6 - 2\omega^4 - 2\omega^5)^2
\]

\[
= 1^2 + 1^2 + (9 + 4\omega^4 + 4\omega^5 - 4\omega^2 - 4\omega^7) + (25 + 4\omega^2 + 4\omega^7 - 4\omega^4 - 4\omega^5)
\]

\[
= 1^2 + 1^2 + 3^2 + 5^2
\]

If \( \omega = 1 \)

\[ \mu_1 = \mu_2 = 1; \ \mu_3 = -3; \ \mu_4 = 5, \]

\[ 5.1. \text{ Williamson type Hadamard matrices} \]

44
equation (5.8) can be written by \( v_i = \omega_i + \omega^{n-i} \).

\[
\begin{align*}
2A &= 2(1 + v_1 - v_2 + v_3 - v_4) \\
2B &= 2(1 + v_1 - v_2 + v_3 - v_4) \\
2C &= 2(1 + v_1 + v_2 + v_3 - v_4) \\
2D &= 2(1 - v_1 - v_2 - v_3 + v_4)
\end{align*}
\]

Then writing \( S_i = T^i + T^{n-i} \)

\[
\begin{align*}
A &= I + S_1 - S_2 + S_3 - S_4 \\
B &= I + S_1 - S_2 + S_3 - S_4 \\
C &= I + S_1 + S_2 + S_3 - S_4 \\
D &= I - S_1 - S_2 - S_3 + S_4
\end{align*}
\]

and using them as (5.3) gives Hadamard matrix of order 36.

**Theorem 5.4 (Whiteman)** Let \( q \) be a prime power \( \equiv 1 \pmod{4} \) and put \( n = (q + 1)/2 \). Let \( \gamma \) be a primitive root of \( GF(q^2) \). Put \( \gamma^k = ax + b \), where \( a, b \in GF(q) \) and define

\[
a_k = \chi(a), b_k = \chi(b), \quad (5.17)
\]

where

\[
\chi(i) = \begin{cases} 
0, & \text{if } i = 0, \\
-1, & \text{if } i \text{ is a non-square of } GF(q), \\
1, & \text{if } i \text{ is a non-zero square of } GF(q), 
\end{cases} 
\]

Then the sums

\[
f(\xi) = \sum_{i=0}^{n-1} a_{4i} \xi^i, \quad g(\xi) = \sum_{i=0}^{n-1} b_{4i} \xi^i, \quad (5.18)
\]

satisfy the identity

\[
f^2(\xi) + g^2(\xi) = q \tag{5.19}
\]

for each \( n \)th root of unity \( \xi \) including \( \xi = 1 \).

Note that when \( \xi = 1 \) the identity (5.19) reduces to the classical result that every prime \( \equiv 1 \pmod{4} \) is representable as the sum of two squares of integers.

**Corollary 5.1** Let \( q = 2n - 1 \) be a prime power \( \equiv 1 \pmod{4} \). Put

\[
\psi_1(\xi) = 1 + f(\xi), \quad \psi_2(\xi) = 1 - f(\xi), \quad \psi_3(\xi) = \psi_4(\xi) = g(\xi)
\]
5.2. Goethals-Seidel type Hadamard matrices

where \( f(\xi) \) and \( g(\xi) \) are the polynomials defined by (5.18). Then the identity

\[
\psi_1^2(\xi) + \psi_2^2(\xi) + \psi_3^2(\xi) + \psi_4^2(\xi) = 4n
\]

is satisfied for each \( n \)th root of unity \( \xi \) including \( \xi = 1 \).

**Theorem 5.5 (Turyn's theorem, proof by Whiteman)** Let \( q = 2n-1 \) be a prime power \( \equiv 1 \pmod{4} \). Then there exists a Williamson matrix of order \( 4n \) in which \( A \) and \( B \) agree only on the main diagonal and moreover, \( C = D \).

Let \( a_0 = 1, b_0 = 1 \). The successive elements in the first row of \( A \) are \( 1, a_4, a_8, \ldots, a_{4(n-1)} \). The successive elements in the first row of \( B \) are \( 1, -a_4, -a_8, \ldots, -a_{4(n-1)} \). The successive elements in the first rows of \( C \) and \( D \) are \( 1, b_4, b_8, \ldots, b_{4(n-1)} \). The matrices \( A, B, C, D \) are circulants.

**Theorem 5.6 (Turyn)** There exists Williamson matrices of order \( 9^t \) with constant diagonal.

**Theorem 5.7** (M. Xia and G. Liu [154]) There exists Williamson type matrices of order \( q^2 \) where \( q \equiv 1 \pmod{4} \) a prime power.

**Theorem 5.8** (R. J. Turyn [143], M. Xia [155] and Y. Q. Chen [18]) There exists Williamson type matrices of special kind of order \( m^2 \) for \( m = 2^a3^b n^2 \), \( a, b = 0 \) or \( 1 \), \( n \) integer.

### 5.2 Goethals-Seidel type Hadamard matrices

**Theorem 5.9 (Goethals and Seidel)** Suppose there exist four type 1 \((1, -1)\) matrices \( A, B, C, D \) of order \( n \) satisfying

\[
AA^t + BB^t + CC^t + DD^t = 4nI_n,
\]

and a monomial matrix \( R \) of order \( n \), \( R^T = R \), \( R^2 = I_n \), such that \((XR)^T = XR\), \( X \in \{A, B, C, D\} \). Then

\[
H = \begin{bmatrix}
A & BR & CR & DR \\
-BR & A & -D^TR & C^TR \\
-CR & D^TR & A & -B^TR \\
-D^TR & -C^TR & B^TR & A
\end{bmatrix}
\]

is a Hadamard matrix of order \( 4n \).
Notation 5.1 The Hadamard matrix $H$ defined in (5.20) is a Goethals-Seidel type Hadamard matrix.

Theorem 5.10 Suppose there exists $4 - \{v; k_1, k_2, k_3, k_4, \sum_{i=1}^{4} k_i - v\}$ SDS with circulant incidence matrices. Then there exists an Hadamard matrix of Goethals-Seidel type of order $4v$.

Notation 5.2 SDS of the type described in Theorem 5.10 are called $H_4$–type.

Theorem 5.11 Suppose there exists $H_4$–type SDS $S_1, S_2, S_3, S_4$. Suppose $A, B, D$ are the type 1 $(1, -1)$ matrices of $S_1, S_2, S_4$, respectively, and $C$ is the type 2 $(1, -1)$ matrix of $S_3$. Then

$$H = \begin{bmatrix} A & B & C & D \\ -B^T & A^T & -D & C \\ -C & D^T & A & -B^T \\ -D^T & -C & B & A^T \end{bmatrix} \quad (5.21)$$

is an Hadamard matrix of order $4v$.

Theorem 5.12 (Wallis-Whiteman) Suppose there exist $H_4$–type SDS $S_1, S_2, S_3, S_4$. Let $R_1, R_2, R_4$ be the type 1 $(1, -1)$ matrices of $S_1, S_2, S_4$ respectively, and $R_3$ be the type 2 $(1, -1)$ matrix of $S_3$. Choose $A = \pm R_1$ according as $R_1J = \pm J$. Similarly choose $B = \pm R_2, C = \pm R_3, D = \pm R_4$ according as $R_2J = \pm J, R_3J = \pm J, R_4J = \pm J$ respectively. Then

$$H = \begin{bmatrix} -1 & -1 & -1 & -1 & e & e & e & e \\ 1 & -1 & 1 & -1 & -e & e & -e & e \\ 1 & -1 & -1 & 1 & -e & e & e & -e \\ 1 & 1 & -1 & -1 & -e & -e & e & e \end{bmatrix} \quad (5.22)$$

which may be written as

$$\begin{bmatrix} -H(1,1,1,1) & H(e,e,e,e) \\ H(e^T,e^T,e^T,e^T) & H(A,B,C,D) \end{bmatrix}$$

is an Hadamard matrix of order $4(v + 1)$. 
5.3 Other results

Theorem 5.13 Suppose there exists \( 2 - \{ q; k_1, k_2; k_1 + k_2 + \frac{1-q}{2} \} \) SDS in \( GF(q) \) for \( q \) a prime power, then there exists an Hadamard matrix of order \( 4q \).

Proof. Let \( D_1, D_2 \) be the \( 2 - \{ q; k_1, k_2; k_1 + k_2 + \frac{1-q}{2} \} \) SDS. Since \( q \) is a prime power, the sets

\[ D_3 = \{ g : g \text{ is non-zero square element of } GF(q) \} \]

and

\[ D_4 = \{ h : h \text{ is nosquare in } GF(q) \} \]

are \( 2 - \{ q; \frac{1}{2}(q - 1); \frac{1}{2}(q - 3) \} \) SDS. So \( D_1, D_2, D_3 \) and \( D_4 \) are \( 4 - \{ q; k_1, k_2, \frac{1}{2}(q - 1), \frac{1}{2}(q - 1); k_1 + k_2 - 1 \} \) SDS. From Theorem 5.9, the theorem 5.13 has been proved.

Notation 5.3 SDS of the type described in Theorem 5.13 are called \( H_2 \)-type.

Example 5.2 Suppose \( C \) and \( D \) are the circulant incidence matrices of \( 2 - \{ m; k_1, k_2; k_1 + k_2 + \frac{1-m}{2} \} \) SDS \( X \) and \( Y \). Then

\[ CC^t + DD^t = \frac{(m-1)}{2} I + (k_1 + k_2 + \frac{1-m}{2}) J \quad (5.23) \]

Set \( A = J - 2C \) and \( B = J - 2D \).

\[ AA^t + BB^t = 2(m - 1) I + 2J \]

Corollary 5.2 If there exist polynomials \( C(\omega) \) and \( D(\omega) \) of degree \( m - 1 \) in \( \omega \) with coefficients \( \pm 1 \), where \( \omega \) is an \( m \)th root of unity and \( m \) is a prime, satisfying

\[ |C(\omega)|^2 + |D(\omega)|^2 = \frac{(m-1)}{2} \]

then there exists an Hadamard matrix of order \( 4m \).

Corollary 5.3 There exists Hadamard matrices of Goethals-Seidel type of order \( 4\omega \) for \( \omega \in 3, 5, 7, 13, 19, 23, 31 \).

Theorem 5.14 (Yang) Suppose there exists \( 2 - \{ m; k_1, k_2; k_1 + k_2 - \frac{m}{2} \} \) SDS \( X \) and \( Y \) with circulant incidence matrices \( P \) and \( Q \). Write \( Q^T = J - Q \), then with

\[ S = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & 1 \\ 1 & 0 & \cdots & 0 \end{pmatrix} \]
5.3. Other results

\[ P_2 = P(S^2) + S^k Q(S^2) \]

and

\[ Q_2 = P(S^2) + S^k Q^T(S^2) \]

with \( k \) any odd integers, are \( 2 - \{2m; k_1 + k_2, k_1 - k_2 + m; 2k_1\} \) SDS with circulant incidence matrices, where \( S \) is of order 2m.

**Theorem 5.15** (M. Xia and G. Liu [158]) There exist \( 4 - \{q^2; \frac{1}{2}q(q - 1); q(q - 2)\} \) SDS and Hadamard matrices of order \( 4q^2 \) with \( q \equiv 3(\mod 8) \) prime power.

**Theorem 5.16** (M. Xia and T. Xia [156]) For every \( v = p^2 m^2, p \equiv 5(\mod 8) \) a prime, \( m = 3^a n^2, a = 0 \) or 1, \( r \geq 0, n \geq 1 \) integers, there exist \( 2 - \{2v; k_1, k_2; k_1 + k_2 - v\} \) SDS and Hadamard matrices of order \( 4v \) of the form

\[
H_{4v} = \begin{pmatrix}
A & B \\
-B^T & A^T
\end{pmatrix}
\]

where \( A \) and \( B \) are type 1 matrices, and satisfy

\[ AA^T + BB^T = 4vI_{2v}. \]

**Theorem 5.17** ([157]) For every \( v = qm^2, q \in \{5, 13, 17, 25, 37, 41, 61\}, m \) is given as in theorem 5.16, there exist \( 2 - \{2v; k_1, k_2; k_1 + k_2 - v\} \) SDS and Hadamard matrices of order \( 4v \) with the form as (5.24).

The type of matrices defined in (5.24) is called *Williamson like* or *Williamson tight* type. It is very useful to construct Hadamard matrices.

If \( A, B, C, D \) are symmetric circulant matrices of order \( n \) such that \( H_{4n} \) as given in (5.3), then \( H_{12n} \) can be constructed as follows:

\[
H_{12n} = \begin{bmatrix}
\end{bmatrix}
\]

(5.25)

This construction was found by L.Baumert.
5.4 Applications of Hadamard matrices

Error correcting codes (E-codes) invented to detect and hopefully correct errors that occurred during the transmission of messages via a noisy channel (see F. J. MacWilliams and N. J. A. Sloane [74]).

Give a vector space $GF(q)^n$. A vector $v = (v_1, \ldots, v_n) \in GF(q)^n$ contains $n$ coordinates on $GF(q)$. The Hamming distance between two vectors $x, y \in GF(q)^n$ is the number of differences of coordinates in two vectors, denoted by $d(x, y)$. An $(n, l, k)$ E-code is a set of $l$ vectors in $GF(q)^n$ such that the Hamming distance between any two vectors is at least $d$.

In the 1960's the U.S. Jet Propulsion Laboratories (JPL) was working toward building the Mariner and Voyager space probes to visit Mars and the other planets of the solar system. The first black and white television pictures from the first landing on the moon were extremely poor quality. Now we take the high quality colour pictures of Jupiter, Saturn, Uranus, Neptune and their moons for granted.

In brief, these high quality colour pictures are taken by using three black and white pictures taken in turn through red, green and blue filters. Each picture is then considered as a thousand by a thousand matrix of black and white pixels. Each picture is graded on a scale of, say, one to sixteen, according to its grayness. So white is one and black is sixteen. These grades are then used to choose a codeword in, say, an eight error correction code based on, say, the Hadamard matrix of order 32. The codeword is transmitted to Earth, error corrected, the three black and white pictures reconstructed and then a computer used to reconstruct the colored pictures.

Hadamard matrices were used for these codewords for two reasons, first, error correction codes based on Hadamard matrices have maximal error correction capability for a given length of codeword and, second, the Hadamard matrices of powers of two are analogous to the Walsh functions, thus all the computer processing can be accomplished using additions (which are very fast and easy to implement in computer hardware) rather than multiplications (which are far slower).

It was S. W. Golomb, L. Baumert and M. Hall Jr. [6] working with JPL who sparked the interest in Hadamard matrices in the past thirty years. They pioneered the use of computing in the construction of Hadamard matrices, the existence of which is an NPC problem (or a problem which has computational resources exponential in the input to find the answer but easy to check the answer once it has been given).

Sylvester's original construction for Hadamard matrices is equivalent to finding Walsh functions [44] which are the discrete analogue of Fourier Series.
Just as any curve can be written as an infinite Fourier series
\[ \sum_n (a_n \sin nt + b_n \cos nt) \] the curve can be written in terms of Walsh functions
\[ \sum_n (a_n \text{sal}(i, t) + b_n \text{cal}(i, t)) = \sum_n c_n \text{wal}(i, t). \]

The hardest curve to model with Fourier series is the step function \( \text{wal}_2(0, t) \) and
errors lead to the Gibbes phenomenon. Similarly, the hardest curve to model with
Walsh functions is the basic \( \sin 2\pi t \) or \( \cos 2\pi t \) curve. Still, we see that we can transform
from one to another.

Many problems require Fourier transforms to be taken, but Fourier transforms re­
quire many multiplications which are slow and expensive to execute. On the other
hand, the fast Walsh-Hadamard transform uses only additions and subtractions (addi­tion of the complement) and so is extensively used, as the foundation of the Fast
Fourier Transform, to transform power sequence spectrum density, band compression
of television signals or facsimile signals or image processing.

Walsh functions are easy to extend to higher dimensions (and higher dimensional
Hadamard matrices) to model surfaces in three and higher dimensions - Fourier series
are more difficult to extend. Walsh-Hadamard transforms in higher dimensions are
also effected using only additions (and subtractions).

Some of the first significant papers describing Walsh-Hadamard transforms in higher
dimensions is J. Hammer and J. Seberry [42], [43].

Hadamard matrices and bent functions are used in the study of the design of
S-boxes which are fundamental to the construction of cryptographically strong SPN
algorithms (substitution-permutation-network) for private key cryptography.
The strength of a cryptographic algorithm is primarily determined by that of the
S-boxes employed by the algorithm and its key schedule which determines how to
incorporate the secret key.

Seberry and her colleagues X. M. Zhang and Y. Zheng [123] used group Hadamard
matrices, which are closely related to Bhaskar Rao designs [112], and generalized
Hadamard matrices [111] to obtain extremely secure cryptographic Boolean functions.
### Table 5.1: Hadamard matrices of the Williamson type

<table>
<thead>
<tr>
<th>( t )</th>
<th>( n )</th>
<th>( \mu_1^2 + \mu_2^2 + \mu_3^2 + \mu_4^2 )</th>
<th>( \mu_1 )</th>
<th>( \mu_2 )</th>
<th>( \mu_3 )</th>
<th>( \mu_4 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>12</td>
<td>( 1^2 + 1^2 + 1^2 + 3^2 )</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>20</td>
<td>( 1^2 + 1^2 + 3^2 + 3^2 )</td>
<td>1</td>
<td>1</td>
<td>1-2( w_1 )</td>
<td>1-2( w_2 )</td>
</tr>
<tr>
<td>7</td>
<td>28</td>
<td>( 1^2 + 1^2 + 1^2 + 5^2 )</td>
<td>1</td>
<td>1</td>
<td>1+2( w_1 - 2w_2 )</td>
<td>1+2( w_3 )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( 1^2 + 3^2 + 3^2 + 3^2 )</td>
<td>1</td>
<td>1</td>
<td>1+2( w_2 - 2w_3 )</td>
<td>1+2( w_1 )</td>
</tr>
<tr>
<td>9</td>
<td>36</td>
<td>( 1^2 + 1^2 + 3^2 + 5^2 )</td>
<td>1</td>
<td>1</td>
<td>1-2( w_1 )</td>
<td>1-2( w_2 + 2w_3 ) +2( w_4 )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( 1^2 + 3^2 + 3^2 + 5^2 )</td>
<td>1</td>
<td>1</td>
<td>1-2( w_2 )</td>
<td>1+2( w_1 + 2w_3 ) -2( w_4 )</td>
</tr>
<tr>
<td>11</td>
<td>44</td>
<td>( 1^2 + 3^2 + 3^2 + 5^2 )</td>
<td>1</td>
<td>1</td>
<td>1+2( w_1 - 2w_2 )</td>
<td>1-2( w_4 )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( 1^2 + 3^2 + 5^2 + 5^2 )</td>
<td>1</td>
<td>1</td>
<td>1+2( w_1 + 2w_4 )</td>
<td>1-2( w_2 )</td>
</tr>
<tr>
<td>13</td>
<td>52</td>
<td>( 1^2 + 1^2 + 5^2 + 7^2 )</td>
<td>1</td>
<td>1</td>
<td>1+2( w_1 - 2w_4 ) +2( w_5 - 2w_6 )</td>
<td>1-2( w_2 - 2w_3 )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( 1^2 + 3^2 + 5^2 + 5^2 )</td>
<td>1</td>
<td>1</td>
<td>1+2( w_1 - 2w_4 ) +2( w_5 - 2w_6 )</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>( 1^2 + 3^2 + 3^2 + 5^2 )</td>
<td>1</td>
<td>1</td>
<td>1+2( w_1 - 2w_3 ) +2( w_5 )</td>
<td>1+2( w_6 )</td>
</tr>
<tr>
<td>15</td>
<td>60</td>
<td>( 1^2 + 1^2 + 3^2 + 7^2 )</td>
<td>1</td>
<td>1</td>
<td>1-2( w_1 - 2w_5 ) +2( w_7 )</td>
<td>1+2( w_2 - 2w_3 ) -2( w_4 - 2w_6 )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( 1^2 + 3^2 + 5^2 + 5^2 )</td>
<td>1</td>
<td>1</td>
<td>1-2( w_5 )</td>
<td>1+2( w_6 )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( 1^2 + 3^2 + 5^2 + 3^2 )</td>
<td>1</td>
<td>1</td>
<td>1-2( w_3 - 2w_5 ) +2( w_7 )</td>
<td>1+2( w_4 + 2w_5 ) -2( w_6 )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( 1^2 + 3^2 + 3^2 + 7^2 )</td>
<td>1</td>
<td>1</td>
<td>1-2( w_2 - 2w_4 ) +2( w_5 )</td>
<td>1-2( w_1 - 2w_3 ) -2( w_8 )</td>
</tr>
<tr>
<td>17</td>
<td>68</td>
<td>( 1^2 + 3^2 + 3^2 + 7^2 )</td>
<td>1</td>
<td>1</td>
<td>1-2( w_2 - 2w_4 ) +2( w_5 )</td>
<td>1-2( w_2 - 2w_6 )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( 1^2 + 3^2 + 3^2 + 3^2 )</td>
<td>1</td>
<td>1</td>
<td>1-2( w_4 - 2w_5 ) +2( w_6 )</td>
<td>1-2( w_1 - 2w_3 ) -2( w_7 )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( 1-2w_3 - 2w_5 ) +2( w_6 + 2w_7 )</td>
<td>1-2( w_2 )</td>
<td>1-2( w_3 )</td>
<td>1-2( w_1 - 2w_4 )</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>( 1+2w_3 + 2w_5 ) -2( w_6 - 2w_7 )</td>
<td>1-2( w_1 )</td>
<td>1-2( w_4 )</td>
<td>1-2( w_3 - 2w_8 )</td>
<td></td>
</tr>
</tbody>
</table>
### Table 5.2: Hadamard matrices of the Williamson type

<table>
<thead>
<tr>
<th>t</th>
<th>n</th>
<th>(\mu_1^2 + \mu_2^2 + \mu_3^2 + \mu_4^2)</th>
<th>(\mu_1)</th>
<th>(\mu_2)</th>
<th>(\mu_3)</th>
<th>(\mu_4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>68</td>
<td>(3^2 + 3^2 + 5^2 + 5^2)</td>
<td>(-2w_2)</td>
<td>(-2w_8)</td>
<td>(-2w_1 + 2w_3)</td>
<td>(+2w_5 - 2w_4)</td>
</tr>
<tr>
<td>19</td>
<td>76</td>
<td>(1^2 + 1^2 + 5^2 + 7^2)</td>
<td>1</td>
<td>1</td>
<td>(+2w_1 - 2w_3)</td>
<td>(+2w_2 - 2w_4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(+2w_8)</td>
<td>(-2w_5 + 2w_6)</td>
<td>(-2w_7 - 2w_9)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(-2w_9)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(-2w_2 - 2w_8)</td>
<td>(-2w_4 + 2w_7)</td>
<td>(+2w_3 + 2w_6)</td>
<td>(-2w_1 - 2w_5)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(-2w_4 - 2w_8)</td>
<td>(-2w_2 - 2w_5)</td>
<td>(+2w_1)</td>
<td>(-2w_3 - 2w_6)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(-2w_3 + 2w_5)</td>
<td>(-2w_1 - 2w_7)</td>
<td>(+2w_3 + 2w_5)</td>
<td>(-2w_1 - 2w_3)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(-2w_3 - 2w_5)</td>
<td>(-2w_1 - 2w_3)</td>
<td>(-2w_3 + 2w_5)</td>
<td>(-2w_1 - 2w_3)</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>84</td>
<td>(1^2 + 1^2 + 2^2 + 9^2)</td>
<td>1</td>
<td>1</td>
<td>(-2w_5 - 2w_8)</td>
<td>(+2w_1 + 2w_2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(+2w_7 + 2w_9)</td>
<td>(-2w_3 + 2w_4)</td>
<td>(+2w_8 - 2w_10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(-2w_6 + 2w_9)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(-2w_2 - 2w_3)</td>
<td>(-2w_1 + 2w_9)</td>
<td>(+2w_1 + 2w_4)</td>
<td>(+2w_5 - 2w_7)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(-2w_3 + 2w_10)</td>
<td>(-2w_1 + 2w_9)</td>
<td>(+2w_1 + 2w_4)</td>
<td>(+2w_5 - 2w_7)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(-2w_2 + 2w_10)</td>
<td>(-2w_1 + 2w_9)</td>
<td>(+2w_1 + 2w_4)</td>
<td>(+2w_5 - 2w_7)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(-2w_2 + 2w_6)</td>
<td>(-2w_1 + 2w_9)</td>
<td>(+2w_1 + 2w_4)</td>
<td>(+2w_5 - 2w_7)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(-2w_2 + 2w_7)</td>
<td>(-2w_1 + 2w_9)</td>
<td>(+2w_1 + 2w_4)</td>
<td>(+2w_5 - 2w_7)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(-2w_2 + 2w_8)</td>
<td>(-2w_1 + 2w_9)</td>
<td>(+2w_1 + 2w_4)</td>
<td>(+2w_5 - 2w_7)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(-2w_2 + 2w_9)</td>
<td>(-2w_1 + 2w_9)</td>
<td>(+2w_1 + 2w_4)</td>
<td>(+2w_5 - 2w_7)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(-2w_3 + 2w_10)</td>
<td>(-2w_1 + 2w_9)</td>
<td>(+2w_1 + 2w_4)</td>
<td>(+2w_5 - 2w_7)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(-2w_3 - 2w_10)</td>
<td>(-2w_1 + 2w_9)</td>
<td>(+2w_1 + 2w_4)</td>
<td>(+2w_5 - 2w_7)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(-2w_3 - 2w_11)</td>
<td>(-2w_1 + 2w_9)</td>
<td>(+2w_1 + 2w_4)</td>
<td>(+2w_5 - 2w_7)</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>92</td>
<td>(1^2 + 1^2 + 3^2 + 9^2)</td>
<td>(-2w_2 - 2w_8)</td>
<td>(-2w_5 + 2w_9)</td>
<td>(+2w_1 + 2w_4)</td>
<td>(-2w_10)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(-2w_8)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(-2w_4 - 2w_8)</td>
<td>(-2w_10)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(-2w_2 + 2w_10)</td>
<td>(-2w_10)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(-2w_7 + 2w_11)</td>
<td>(-2w_10)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>100</td>
<td>(1^2 + 1^2 + 7^2 + 7^2)</td>
<td>1</td>
<td>1</td>
<td>(-2w_2 - 2w_3)</td>
<td>(-2w_1 - 2w_4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(-2w_5 + 2w_6)</td>
<td>(+2w_8 + 2w_9)</td>
<td>(-2w_7 + 2w_12)</td>
<td>(-2w_10 - 2w_{11})</td>
</tr>
</tbody>
</table>
Table 5.3: Hadamard matrices of the Williamson Type

<table>
<thead>
<tr>
<th>$t$</th>
<th>$n$</th>
<th>$\mu_1^2 + \mu_2^2 + \mu_3^2 + \mu_4^2$</th>
<th>$\mu_1$</th>
<th>$\mu_2$</th>
<th>$\mu_3$</th>
<th>$\mu_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>100</td>
<td>1 + 2w_3 - 2w_7</td>
<td>1 - 2w_1 + 2w_4</td>
<td>1 + 2w_8 - 2w_9</td>
<td>-2w_10 - 2w_11</td>
<td>1 - 2w_3 - 2w_9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 + 2w_3 - 2w_9</td>
<td>1 + 2w_4 - 2w_12</td>
<td>1 - 2w_1 - 2w_7</td>
<td>1 - 2w_3 - 2w_5</td>
<td>+2w_6 + 2w_8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$1^2 + 3^2 + 3^2 + 9^2$</td>
<td>1 - 2w_1 + 2w_3</td>
<td>1 + 2w_4 - 2w_7</td>
<td>1 + 2w_2 + 2w_5</td>
<td>-2w_8 + 2w_10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$5^2 + 5^2 + 5^2 + 5^2$</td>
<td>1 + 2w_1 - 2w_6</td>
<td>1 + 2w_7 - 2w_8</td>
<td>1 + 2w_2 - 2w_4</td>
<td>1 - 2w_3 + 2w_10</td>
</tr>
<tr>
<td>27</td>
<td>108</td>
<td>$1^2 + 1^2 + 5^2 + 9^2$</td>
<td>1</td>
<td>1</td>
<td>1 - 2w_1 - 2w_3</td>
<td>+2w_6 + 2w_8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$1^2 + 3^2 + 5^2 + 9^2$</td>
<td>1 + 2w_3 - 2w_4</td>
<td>+2w_6 - 2w_9</td>
<td>-2w_10 + 2w_11</td>
<td>+2w_13</td>
</tr>
</tbody>
</table>
As discussed before, Hadamard matrices and their generalizations to weighing matrices, have long been of interest to workers in combinatorics and also to applied statisticians, coding theorists and other applied mathematicians. Orthogonal Designs is a heavy "borrower" of mathematics. Results from, for example, algebraic number theory, quadratic forms, difference sets, representation theory, coding theory, finite geometry and cyclotomy are used.

An orthogonal design with no zeros and in which each of the entries is replaced by ±1 is a Hadamard matrix. A special orthogonal design, the $OD(4n; n, n, n, n)$ is especially useful in the construction of Hadamard matrices.

The task can be simply described as follows: Find necessary and sufficient conditions on the set of integers $\{n; s_1, \ldots, s_u\}$ such that there exists an orthogonal design in order $n$ of type $\langle s_1, \ldots, s_u \rangle$.

The generality of the question includes many other problems which have been extensively studied and provide an umbrella under which these problems may be considered simultaneously. Also, in this generality the connections between these classical combinatorial problems and some of the great mathematics of the past centuries have been illuminated. More particularly, the general approach has shown the close connection in the combinatorial problems studied have the classification theorems of quadratic forms over $\mathbb{Q}$, the rational numbers, these classification theorems, largely the work of Minkowski, are among the few complete mathematical triumphs of the last century. The theory gives the hope that they will continue a deeper investigation of these combinatorial problems and the unresolved problem of the classification of quadratic forms over $\mathbb{Z}$.

The first focus of attack on the general problem concerns the maximum number of distinct variables that can appear in an orthogonal design of order $n$. The maximum number of variables in orthogonal designs and amicable orthogonal designs is intimately related with algebraic forms and has been determined over 20 years ago. An account
of this theory is given in [36]. For the purposes of this chapter that the maximum number of variables in orthogonal designs of orders \(\equiv 2 \pmod{4}\), \(\equiv 4 \pmod{8}\) and \(\equiv 8 \pmod{16}\), is 2, 4, and 8 need to be known, respectively. The maximum number of variables \(u + v\) in amicable orthogonal designs of orders \(\equiv 2 \pmod{4}\) and \(\equiv 4 \pmod{8}\) is 4 and 6 respectively. The theorem 6.2 is given by the author.

6.1 Preliminary and definition

Definition 6.1 (Orthogonal Design) An orthogonal design of order \(n\) and type \((s_1,\ldots,s_u)\), \(s_i\) positive integer, is an \(n \times n\) matrix \(X\), with entries \(\{0, \pm x_1, \ldots, \pm x_u\}\) \((x_i\) commuting indeterminate) satisfy

\[
XX^T = \left( \sum_{i=1}^{u} s_ix_i^2 \right) I_n.
\]

Write this as OD\((n; s_1,\ldots,s_u)\).

Definition 6.2 (Weight matrix) A weight matrix \(A\) of weight \(k\) and order \(n\) is an \(n \times n\) matrix with entries \(\{0, \pm 1\}\), such that \(AA^T = A^TA = kI_n\). The weight matrix of order \(n\) with weight \(k\), denoted by \(W(n,k)\).

Such matrices have already appeared naturally as the “coefficient” matrices of an orthogonal design (see [99] and [100] for details). Hence \(W\) satisfies \(WW^T = kI_n\), and \(W\) is equivalent to an orthogonal design OD\((n;k)\). The number \(k\) is called the weight of \(W\). If \(k = n\), that is, all the entries of \(W\) are \(\pm 1\) and \(WW^T = nI_n\). \(W\) is called an Hadamard matrix of order \(n\).

A matrix \(W = \text{circ}(w_1,\ldots,w_n)\), \(w_i \in \{0, \pm 1\}\) which satisfies \(WW^T = kI_n\) is called a circulant weighing matrix of order \(n\) and weight \(k\) (or CW\((n,k)\)).

When \(k = n\), then \(W(n,n)\) is what is usually referred to in the literature as an Hadamard matrix.

An OD\((12;3,3,3,3)\) was first found by L. Baumert and M. Hall, Jr. [7], and OD\((20;5,5,5,5)\) by Welch. OD\((4n; n,n,n,n)\) are sometimes called Baumert-Hall arrays.

Theorem 6.1 (p74, p79 in [36]) If there exists an orthogonal design OD\((n; u_1,\ldots,u_s)\), then there exist following orthogonal designs

(i) OD\((2n; e_1u_1,\ldots,e_su_s)\) where \(e_i = 1\) or 2, \(1 \leq i \leq s\),
6.1. Preliminary and definition

(ii) OD(2n; u_1, u_1, f u_2, \ldots, f u_s) where f = 1 or 2,

(iii) OD(4n; u_1, \ldots, u_{s-1}, u_s, u_s, u_s),

(iv) OD(8n; u_1, \ldots, u_{s-1}, u_s, u_s, u_s, u_s),

(v) OD(16n; u_1, u_2, \ldots, u_{s-1}, u_s, u_s, u_s, u_s, u_s, u_s, u_s).

Lemma 6.1 (Equating and Killing lemma) If A is an orthogonal design of order n with type \((u_1, \ldots, u_s)\), then there exist orthogonal design of order n with type \((u_1, \ldots, u_i + u_j, \ldots, u_s)\) and with type \((u_1, \ldots, u_{j-1}, u_{j+1}, \ldots, u_s)\).

Lemma 6.2 (P. J. Robinson) All full 6-tuples orthogonal designs OD\((32; u_1, u_2, u_3, u_4, u_5, 32-E i=1 u_i)\) exist, except possibly OD\((32; 1, 1, 1, 1, 1, 27)\), \(1 \leq u_1, u_2, u_3, u_4, u_5 < 32, \Sigma_{i=1}^5 u_i \leq 32\).

Corollary 6.1 All OD\((32; u_1, u_2, u_3, u_4, u_5)\) exist, except possibly OD\((32; 1, 1, 1, 1, 27)\), \(\Sigma_{i=1}^5 u_i \leq 32\). All OD\((32; u_1, \ldots, u_m)\), \(m = 1, 2, 3, 4\), exist too.

Proposition 6.1 (p77, p211 in [36]) If there is an orthogonal design OD\((n; a, b)\), then

(i) there exists an orthogonal design OD\((2n; a, a, b, b)\);

(ii) there exists an orthogonal design OD\((4n; a, a, 2a, b, b, 2b)\).

(iii) there exist orthogonal design OD\((8n; a, a, 2a, 2a, 2a, 8b)\) and OD\((8n; a, 2a, 2a, 3a, 2b, 6b)\).

Lemma 6.3 (p394 in [36]) All full 7-tuples OD\((n; u_1, \ldots, u_7)\) exist except possibly 86 given in Appendix D of [36].

Lemma 6.4 (P. J. Robinson) All orthogonal designs of type \((1, 1, a, b, c)\), \(a + b + c = 2^t - 2\), exist in order \(2^t\), \(t \geq 3\).

Lemma 6.5 (J. Wallis) All orthogonal designs of type \((a, b, 2^t - a - b)\) exist in order \(2^t\).

The following theorems are true.

Theorem 6.2 (1) There exists orthogonal design of type \((u_1, u_2, u_3, u_4, u_5)\) with all 5-tuples in order 64.
(2) There exists all 6-tuples type of \((u_1, u_2, u_3, u_4, u_5, u_6)\), orthogonal design in order 64.

**Proof.**

(i) From Corollary 6.1 all 5-tuples, except \((1,1,1,1,27)\), there exists the orthogonal design of this type in order 32, say \(OD(32; u_1, u_2, u_3, u_4, u_5)\), \(\{u_1, u_2, u_3, u_4, u_5\} \neq \{1,1,1,1,27\}\). From theorem 6.1 there exists 5-tuples type of \((e_1u_1, e_2u_2, e_3u_3, e_4u_4, e_5u_5)\) and 6-tuples type of \((fu_1, fu_2, fu_3, fu_4, u_5, u_5)\) orthogonal design in order 64, \(e_i = 1 \text{ or } 2, i = 1,2,3,4,5, f = 1 \text{ or } 2\). Let \(u'_1 = e_1u_1 + u_5\), \(u'_i = e_iu_i, 2 \leq i \leq 5\). From Lemma 6.1 that there exists 5-tuples type of \((u'_1, u'_2, u'_3, u'_4, u'_5)\) orthogonal design in order 64, except possibly \(\{u'_1, u'_2, u'_3, u'_4, u'_5\} = \{(1,1,1,1,28), (1,1,1,2,27), (1,1,1,1,54), (1,1,1,27,28)\}\). Since \(OD(32;1,1,1,1,28)\) and \(OD(32;1,1,1,1,27)\) exist, then \(OD(64;1,1,1,1,28)\) and \(OD(64;1,1,1,1,27)\) exist.

From Lemma 6.2 that there exists \(OD(32;1,1,1,1,2,26)\). According to the Theorem 6.1 that there exists type of \((1,1,1,1,2,26,26)\) orthogonal design in order 64. The from Lemma 6.1, there exist type of \((1,1,1,27,28)\) and type of \((1,1,1,1,54)\) orthogonal design in order 64. This proof the (i) part of the theorem.

(ii) From Lemma 6.2 and Corollary 6.1, there exist all 5-tuples, except possibly \((1,1,1,1,27)\), all 6-tuples, except possibly \((1,1,1,1,1,27)\), orthogonal design in order 32. Similarity there exists all 6-tuples, except possibly \((1,1,2,2,2,54), (2,2,2,2,27,27)\), are the type of orthogonal design in order 64.

Since \(OD(32;1,1,1,1,2,25)\) exists, then \(OD(64;1,1,2,2,2,4,50)\) exists, so \(OD(64;1,1,2,2,2,54)\) exists.

From corollary 6.4 and lemma 6.1, there exists orthogonal design of type \((2,6,6)\). From corollary 6.5, there exists orthogonal design of type \((2,7,7)\). Since corollary 7.1 is true, there exists orthogonal design of type \((2,2,2,21,21,2,6,6)\). Then according to lemma 6.1, there exists orthogonal design of type \((2,2,2,27,27)\).

This proof the (ii) part of the theorem.
Proposition 6.2 A necessary and sufficient condition that there exists an OD(n; s₁, ..., sₚ) is that there exist matrices A₁, ..., Aₚ satisfying:

(i) the Aᵢ are (0, ±1) matrices, 1 ≤ i ≤ p;

(ii) Aᵢ Aⱼ = 0 for 1 ≤ i ≠ j ≤ p;

(iii) Aᵢ Aᵢᵀ = sᵢIₙ, 1 ≤ i ≤ p;

(iv) Aᵢ Aⱼᵀ + Aⱼ Aᵢᵀ = 0, 1 ≤ i ≠ j ≤ p.

Koukouvinos and Seberry [64] have extended the construction of Holzmann and Kharaghani [48] to find infinite families of Plotkin type arrays, and in [65] orthogonal arrays OD(8t; k, k, k, k, k, k) in 6 variables for odd t.

6.2 Construction of orthogonal designs

Let Aᵢ, i = 1, 2, 3, 4 be circulant matrices of order n with entries in {0, ±x₁, ±x₂, ..., ±xₚ} satisfying

\[ \sum_{i=1}^{4} Aᵢ Aᵢᵀ = \sum_{i=1}^{n} (sᵢ xᵢ^2) Iₙ. \]

Then the Goethals-Seidel array

\[
G = \begin{pmatrix}
A₁ & A₂ R & A₃ R & A₄ R \\
-A₂ R & A₁ & A₄ R & -A₃ R \\
-A₃ R & -A₄ R & A₁ & A₂ R \\
-A₄ R & A₃ R & -A₂ R & A₁
\end{pmatrix}
\]

where R is the back-diagonal identity matrix, is an OD(4n; s₁, s₂, ..., sₚ). The Goethals-Seidel (or Wallis-Whiteman) array (see [37] for details), has proven to be the most useful tool for constructing orthogonal designs.

Theorem 6.3 ([36]) Suppose there is an orthogonal design OD(n; p₁, ..., pₚ). Let A₁, ..., Aₚ be circulant (type 1) matrices of order m with entries \{0, ±y₁, ..., ±yₚ\} which satisfy

\[ p₁ A₁ A₁ᵀ + \cdots + pₚ Aₚ Aₚᵀ = k Iₘ. \]

Further suppose

(1) all Aᵢ, 1 ≤ i ≤ p, are symmetric, or
(2) at most one is not symmetric, or

(3) $A_1, \cdots, A_{j-1}$ are symmetric and $A_j, \cdots, A_u$ are skew symmetric.

Then if $k = q_1 y_1^2 + \cdots + q_v y_v^2$, there is an orthogonal design $OD(nm; q_1, \cdots, q_v)$.

Germita and Seberry provide a number of $8 \times 8$ arrays which are, as they put it, part Williamson and part Goethals-Seidel.

**Lemma 6.6** ([36]) Suppose $A_1, \cdots, A_8$ are eight circulant (type 1) matrices of order $n$ satisfy

1. $A_i, 1 \leq i \leq 8$, with entries $\{0, \pm x_1, \cdots, x_u\}$ and
2. $\sum_{i=1}^{8} A_i A_i^T = kI_n$.

Further suppose

(i) $A_i, 1 \leq i \leq 8$ are all symmetric or all skew, or

(ii) $A_1 = \cdots = A_i$, and $A_{i+1}, \cdots, A_8$ are all symmetric or all skew, $1 \leq i \leq 8$, or

(iii) $A_2 = A_3 = A_4$ and $A_5, A_6, A_7, A_8$ are all symmetric or all skew, or

(iv) $A_1 A_2^T = A_2 A_1^T$, $A_3 = A_4$ and $A_5, A_6, A_7, A_8$ are all symmetric, or

(v) $A_1, \cdots, A_i$ are all skew and $A_{i+1}, \cdots, A_8$ all symmetric, or

(vi) $A_2, A_3, A_4$ are all skew and $A_5, A_6, A_7, A_8$ are all symmetric, or

(vii) $A_i A_{i+4}^T = A_{i+4} A_i^T$, $i = 1, 2, 3, 4$.

Then, with $k = \sum_{i=1}^{u} p_i x_i^2$, there exists an orthogonal design $OD(8n; p_1, \cdots, p_u)$.

**Proof.** Use the following constructions

(i) When $\{A_i\}_{i=1}^8$ be circulant (type 1) symmetric (or skew) matrices, set

\[
M_1 = \begin{pmatrix}
A_1 & A_2 & A_3 & A_4 & A_5 & A_6 & A_7 & A_8 \\
-A_2 & A_1 & A_4 & -A_3 & A_6 & -A_5 & -A_8 & A_7 \\
-A_3 & -A_4 & A_1 & A_2 & A_7 & A_8 & -A_5 & -A_6 \\
-A_4 & A_3 & -A_2 & A_1 & A_8 & -A_7 & A_6 & -A_5 \\
-A_5 & -A_6 & -A_7 & A_8 & A_1 & A_2 & A_3 & A_4 \\
-A_6 & A_5 & -A_8 & A_7 & -A_2 & A_1 & -A_4 & A_3 \\
-A_7 & A_8 & A_5 & -A_6 & -A_3 & A_4 & A_1 & -A_2 \\
-A_8 & -A_7 & A_6 & A_5 & -A_4 & -A_3 & A_2 & A_1
\end{pmatrix}.
\]
(ii) When \( A_1 = \cdots = A_i \), then \( A_1 R_n = \cdots = A_i R_n \), \( R_n \) be a back identity matrix of order \( n \). Use \( A_1 R_n, \cdots, A_i R_n \) to replace the \( A_1, \cdots, A_i \) in construction (6.2). Then \( M_1 \) is the required orthogonal design.

(iii) When \( A_2 = A_3 = A_4 \) and \( A_5, A_6, A_7, A_8 \) are all symmetric or all skew, set

\[
M_2 = \begin{pmatrix}
A_1 R_n & A_2 & A_3 & A_4 & A_5 & A_6 & A_7 & A_8 \\
-A_2 & A_1 R_n & A_2 & -A_2 & A_5 & -A_5 & -A_8 & A_7 \\
-A_2 & -A_2 & A_1 R_n & A_2 & A_7 & A_8 & -A_5 & -A_6 \\
-A_2 & A_2 & -A_2 & A_1 R_n & A_8 & -A_7 & A_6 & -A_5 \\
-A_5 & -A_6 & -A_7 & -A_8 & A_1 R_n & A_2^T & A_2^T & A_2^T \\
-A_6 & A_5 & -A_8 & A_7 & -A_2^T & A_1 R_n & -A_2^T & A_2^T \\
-A_7 & A_8 & A_5 & -A_6 & -A_2^T & A_2^T & A_1 R_n & -A_2^T \\
-A_8 & -A_7 & A_6 & A_5 & -A_2^T & -A_2^T & A_2^T & A_1 R_n 
\end{pmatrix}
\]  

(6.3)

(iv) When \( A_1 A_2^T = A_2 A_1^T, A_3 = A_4 \), and \( A_5, A_6, A_7, A_8 \) are all symmetric, set

\[
M_3 = \begin{pmatrix}
A_1 R_n & A_2 R_n & A_3 & A_3 & A_5 & A_5 & A_6 & A_7 & A_8 \\
-A_2 R_n & A_1 R_n & A_3 & -A_3 & A_6 & -A_5 & -A_8 & A_7 \\
-A_3 & -A_3 & A_1 R_n & A_2 R_n & A_7 & A_8 & -A_5 & -A_6 \\
-A_3 & A_3 & -A_2 R_n & A_1 R_n & A_8 & -A_7 & A_6 & -A_5 \\
-A_5 & -A_6 & -A_7 & -A_8 & A_1 R_n & A_2 R_n A_3^T & A_3^T \\
-A_6 & A_5 & -A_8 & A_7 & -A_2 R_n & A_1 R_n & -A_3^T & A_3^T \\
-A_7 & A_8 & A_5 & -A_6 & -A_3^T & A_3^T & A_1 R_n & -A_2 R_n \\
-A_8 & -A_7 & A_6 & A_5 & -A_3^T & -A_3^T & A_2 R_n & A_1 R_n 
\end{pmatrix}
\]  

(6.4)

(v) When \( A_1, \cdots, A_i \) are all skew and \( A_{i+1}, \cdots, A_8 \) are all symmetric, use \( A_1 R_n, \cdots, A_i R_n, A_{i+1}, \cdots, A_8 \) to replace \( A_1, \cdots, A_8 \) in the design (6.2). The matrix \( M_1 \) is the desired orthogonal design.

(vi) When \( A_2, A_3, A_4 \) are all skew and \( A_5, A_6, A_7, A_8 \) are all symmetric, set

\[
M_4 = \begin{pmatrix}
A_1 R_n & A_2 & A_3 & A_4 & A_5 & A_6 & A_7 & A_8 \\
-A_2 & A_1 R_n & A_4 & -A_3 & A_6 & -A_5 & -A_8 & A_7 \\
-A_3 & -A_4 & A_1 R_n & A_2 & A_7 & A_8 & -A_5 & -A_6 \\
-A_4 & A_3 & -A_2 & A_1 R_n & A_8 & -A_7 & A_6 & -A_5 \\
-A_5 & -A_6 & -A_7 & -A_8 & A_1 R_n & A_2^T & A_2^T & A_2^T \\
-A_6 & A_5 & -A_8 & A_7 & -A_2^T & A_1 R_n & -A_2^T & A_2^T \\
-A_7 & A_8 & A_5 & -A_6 & -A_3^T & A_4^T & A_1 R_n & -A_2^T \\
-A_8 & -A_7 & A_6 & A_5 & -A_4^T & -A_3^T & A_2^T & A_1 R_n 
\end{pmatrix}
\]  

(6.5)
(vii) When $A_iA_{i+4}^T = A_{i+4}A_i^T$, $i = 1, 2, 3, 4$, set

$$M_5 = \begin{pmatrix}
A_1 & A_2R_n & A_3R_n & A_4R_n & A_5 & A_6R_n & A_7R_n & A_8R_n \\
-A_2R_n & A_1 & A_4^TR_n & -A_3^TR_n & A_6R_n & -A_5 & -A_8^TR_n & A_7^TR_n \\
-A_3R_n & -A_4^TR_n & A_1 & A_2^TR_n & A_7R_n & A_8^TR_n & -A_5 & -A_6^TR_n \\
-A_4R_n & A_3^TR_n & -A_2^TR_n & A_1 & A_6R_n & -A_7^TR_n & A_8^TR_n & -A_5 \\
-A_5 & -A_6R_n & -A_7R_n & -A_8R_n & A_1 & A_2R_n & A_3R_n & A_4R_n \\
-A_6R_n & A_5 & -A_8^TR_n & A_7^TR_n & -A_2R_n & A_1 & -A_4^TR_n & A_3^TR_n \\
-A_7R_n & A_8^TR_n & A_5 & -A_6^TR_n & -A_3R_n & A_4^TR_n & A_1 & -A_2^TR_n \\
-A_8R_n & -A_7^TR_n & A_6^TR_n & A_5 & -A_4R_n & -A_3^TR_n & A_2^TR_n & A_1
\end{pmatrix} \tag{6.6}$$

This complete the proof.

Kharaghani in his recent paper [58] shows the construction of orthogonal designs by using 8 amicable circulant matrices. Such arrays are essential for constructing orthogonal designs with more than four variables. In chapter 7 and chapter 11 will discuss some other methods of construction of orthogonal designs.
Chapter 7

Amicable orthogonal designs

Amicable orthogonal designs is very useful in constructing amicable Hadamard matrices. When constructing Hadamard matrices, a knowledge of the power of 2 is crucial. Also one can see that some previously known results on Hadamard matrices can be generalized by using amicable orthogonal designs.

In J. Wallis [147] the study of pairs of Hadamard matrices $W = I + S$ and $M$, where $W, M$ have order $n$, $S = -S^T$, $M = M^T$ and $WM^T = MW^T$, was extensively pursued and many examples discovered. These amicable Hadamard matrices are an important special case of amicable orthogonal designs. They have type $(1, n - 1; n)$ of order $n$.

In this chapter the author restates results of amicable orthogonal designs.

7.1 Introduction

Definition 7.1 A pair of matrices $X$, $Y$ is said to be amicable (anti-amicable) if $XY^T - YX^T = 0$ ($XY^T + YX^T = 0$).

Let $X$ be $OD(n; p_1, p_2, \cdots, p_u)$ on variables $\{x_1, \cdots, x_u\}$ and $Y$ be $OD(n; q_1, q_2, \cdots, q_v)$ on variables $\{y_1, \cdots, y_v\}$. $X$ and $Y$ are said to be amicable orthogonal designs of $AOD(n; p_1, p_2, \cdots, p_u; q_1, q_2, \cdots, q_v)$ if

$$XY^T = YX^T.$$ 

Writing $Z = XY^T$, then

$$ZZ^T = (p_1x_1^2 + \cdots + p_u x_u^2)(q_1y_1^2 + \cdots + q_v y_v^2)I_n.$$ 

So amicable orthogonal designs are related to symmetric $Z$ which have inner product factorization into quadratic forms.

The maximum number of variables in orthogonal designs and amicable orthogonal designs is intimately related with algebraic forms and has been determined over 20 years ago. An account of this theory is given in [36].
Now, let $X$ and $Y$ be $AOD(n; p_1, \ldots, p_u; q_1, \ldots, q_v)$. Write $X = \sum_{i=1}^{u} A_i x_i$, $Y = \sum_{j=1}^{v} B_j y_j$. The fact that the $x$'s and $y$'s are assumed to commute and has properties:

(i) The $A_i$ and $B_j$ are all $\{0, \pm 1\}$ matrices, and $A_i \ast A_l = 0$, $1 \leq i \neq l \leq u$, $B_j \ast B_k = 0$, $1 \leq j \neq k \leq v$.

(ii) $A_i A_i^T = p_i I_n$, $1 \leq i \leq u$, $B_j B_j^T = q_j I_n$, $1 \leq j \leq t$.

(iii) $A_i A_i^T + A_i A_i^T = 0$, $1 \leq i \neq l \leq u$, $B_j B_j^T + B_k B_k^T = 0$, $1 \leq j \neq k \leq v$.

(iv) $A_i B_j^T = B_j A_i^T$, $1 \leq i \leq u$, $1 \leq j \leq v$.

It is clear that conditions (i)- (iv) are necessary and sufficient for the existence of amicable orthogonal designs of type $(n; p_1, \ldots, p_u; q_1, \ldots, q_v)$.

**Notation 7.1** (Williamson matrices and Williamson type matrices) Four $\{\pm 1\}$ circulant and symmetric matrices $X_1$, $X_2$, $X_3$, $X_4$ of order $n$ are called four Williamson matrices if they satisfy

$$X_1^2 + X_2^2 + X_3^2 + X_4^2 = 4n I_n.$$ 

Four $\{\pm 1\}$ matrices $X_1$, $X_2$, $X_3$, $X_4$ of order $n$ are called four Williamson type matrices if they are pairwise amicable and satisfy

$$X_1 X_1^T + X_2 X_2^T + X_3 X_3^T + X_4 X_4^T = 4n I_n.$$ 

Following [58] a set $\{A_1, A_2, \ldots, A_{2m}\}$ of square real matrices is said to be amicable if

$$\sum_{i=1}^{2m} \left( A_{\sigma(2i-1)} A_{\sigma(2i)}^T - A_{\sigma(2i)} A_{\sigma(2i-1)}^T \right) = 0 \quad (7.1)$$

for some permutation $\sigma$ of the set $\{1, 2, \ldots, 2m\}$. For simplicity, take $\sigma(i) = i$ unless otherwise specified. So

$$\sum_{i=1}^{2m} \left( A_{2i-1} A_{2i}^T - A_{2i} A_{2i-1}^T \right) = 0 \quad (7.2)$$

A set $\{A_i\}_{i=1}^{m}$ of order $n$ with entries in $\{0, \pm x_1, \ldots, \pm x_u\}$ is said to satisfy an additive property of type $(p_1, \ldots, p_u)$ if

$$\sum_{i=1}^{m} A_i A_i^T = \sum_{i=1}^{u} (p_i x_i^2) I_n. \quad (7.3)$$
A set of matrices \( \{A_1, A_2, \ldots, A_m\} \) of order \( n \) with entries in \( \{0, \pm x_1, \pm x_2, \ldots, \pm x_u\} \) is called an amicable set satisfying the additive property of type \((p_1, \cdots, p_u)\) in variables \(x_1, x_2, \ldots, x_u\), if it is an amicable set and satisfies the additive property.

Given the sequence \( A = \{a_1, a_2, \ldots, a_n\} \) of length \( n \) the non-period autocorrelation function \( N_A(s) \) is defined as

\[
N_A(s) = \sum_{i=1}^{n-s} a_i a_{i+s}, \quad s = 0, 1, \ldots, n-1, \quad (7.4)
\]

If \( A(z) = a_1 + a_2 z + \ldots + a_n z^{n-1} \) is the associated polynomial of the sequence \( A \), then

\[
A(z)A(z^{-1}) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_i a_j z^{i-j} = N_A(0) + \sum_{s=1}^{n-1} N_A(s)(z^s + z^{-s}), \quad z \neq 0. \quad (7.5)
\]

Given \( A \) as above of length \( n \) the periodic autocorrelation function \( P_A(s) \) is defined, reducing \( i + s \) modulo \( n \), as

\[
P_A(s) = \sum_{i=1}^{n} a_i a_{i+s}, \quad s = 0, 1, \ldots, n-1. \quad (7.6)
\]

**Definition 7.2** (Amicable Family) An amicable family of type \((p_1, \cdots, p_u; q_1, \cdots, q_v)\) in order \( n \) is a collection of rational matrices of order \( n \), \( \{A_1, \cdots, A_u; B_1, \cdots, B_v\} \) satisfying properties (i)-(iv) above, where the \( p_1, \cdots, p_u, q_1, \cdots, q_v \) are positive rational numbers.

Suppose \( C = circ(c_0, c_1, \ldots, c_{n-1}) \) is a circulant matrix of order \( n \). Let

\[
T_n = \begin{pmatrix}
0 & 1 & 0 & 0 & \cdots & 0 \\
0 & 0 & 1 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 1 \\
1 & 0 & 0 & 0 & \cdots & 0
\end{pmatrix} \quad (7.7)
\]

of order \( n \), be the shift matrix. Then write \( C = c_0 I_n + c_1 T_n + \ldots + c_{n-1} T_n^{n-1} \). Note that \( T_n^n = I_n \) the identity matrix of order \( n \). Denote the Hall polynomial of \( C \) is \( Hall(C) = \sum_{i=0}^{n-1} c_i x^i \). The Hall polynomial of \( C^T \) is \( Hall(C^T) = \sum_{i=0}^{n-1} c_i x^{n-i} \).

**Proposition 7.1** Let \( \{A_1, \cdots, A_u; B_1, \cdots, B_v\} \) be an amicable family of type \((p_1, \cdots, p_u; q_1, \cdots, q_v)\) in order \( n \), and let \( P \) and \( Q \) be rational matrices of order \( n \) satisfying \( PP^T = a I_n \), \( QQ^T = b I_n \). Then \( \{PA_1 Q, \cdots, PA_u Q; PB_1 Q, \cdots, PB_v Q\} \) is an amicable family of type \((p_1 ab, \cdots, p_u ab; q_1 ab, \cdots, q_v ab)\).
Lemma 7.1 (Geramita-wallis) Suppose there exists amicable orthogonal designs of order $n$ and types $((u_1, \ldots, u_p); (v_1, \ldots, v_q))$. Then since there are product designs of type $(1,1,1; 1,1,1)$ in order 4, there exist orthogonal designs of type

(i) $(u_1, u_1, u_1, 3u_2, \ldots, 3u_p, v_1, \ldots, v_q)$ and

(ii) $(u_1, u_1, u_1, w, w, w, v_1, \ldots, v_q)$

in order $4n$ where $w = u_2 + u_3 + \cdots + u_p$.

7.2 Short amicable sets

Definition 7.3 (Short Amicable Set) A set $\{A_i\}_{i=1}^m$ of matrices of order $n$ is said to be a short amicable set (SAS) of order $n$ and type $(p_1, \ldots, p_u)$ if (7.2) and (7.3) are satisfied for $m = 2$ or 4.

When the set $\{A_i\}_{i=1}^m$ be circulant matrices of order $n$, it is said to be a short circulant amicable set (SCAS) of order $n$ and type $(p_1, \ldots, p_u)$.

Short amicable sets were introduced in [35] where they are used to find infinite families of orthogonal designs. They remain an attractive area for theoretical and practical research. The short amicable set $\{A_i\}_{i=1}^4$ denoted by $4$-SAS$(n; p_1, p_2, p_3, p_4)$.

Let $A_1, A_2, A_3, A_4$ be circulant matrices of order $n$ with entries in $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ (or $\{0, \pm 1\}$) satisfying

$$\sum_{i=1}^4 A_i A_i^T = \sum_{i=1}^u (p_i x_i^2) I_n \quad \text{(or} \quad \sum_{i=1}^4 A_i A_i^T = k I_n).$$

Then the Goethals-Seidel array

$$G = \begin{pmatrix}
A_1 & A_2 R_n & A_3 R_n & A_4 R_n \\
-A_2 R_n & A_1 & A_4^T R_n & -A_3^T R_n \\
-A_3 R_n & -A_4^T R_n & A_1 & A_3^T R_n \\
-A_4 R_n & A_3^T R_n & -A_2 R_n & A_1
\end{pmatrix} \quad \text{(7.8)}$$

is an $OD(4n; p_1, p_2, \ldots, p_u)$ (See page 107 of [36] for details).

The short Kharaghani array

$$K = \begin{pmatrix}
A_1 & A_2 & A_3 R_n & A_4 R_n \\
-A_2 & A_1 & A_4 R_n & -A_3 R_n \\
-A_3 R_n & -A_4 R_n & A_1 & A_2 \\
-A_4 R_n & A_3 R_n & -A_2 & A_1
\end{pmatrix} \quad \text{(7.9)}$$
7.2. Short amicable sets

is an $OD(4n; p_1, \cdots, p_u)$, where $A_1$, $A_2$, $A_3$ and $A_4$ are amicable.

The short amicable set $\{A_i\}_{i=1}^{2}$ denoted by $2 - SAS(n; p_1, p_2)$.

Clearly

1) If there exists $2 - SAS(n; p_1, p_2)$ and $2 - SAS(n; p_3, p_4)$, then there exists a $4 - SAS(n; p_1, p_2, p_3, p_4)$.

2) If there exists $2 - SAS(n; p_1, p_2)$, $2 - SAS(n; p_3, p_4)$, $2 - SAS(n; p_5, p_6)$ and $2 - SAS(n; p_7, p_8)$, then there exists an $8 - AS(n; p_1, \cdots, p_8)$.

3) If there exists $4 - SAS(n; p_1, p_2, p_3, p_4)$ and $4 - SAS(n; p_5, p_6, p_7, p_8)$, then there exists an $8 - AS(n; p_1, \cdots, p_8)$.

Thus one can obtain many classes of $4 - SAS$ combining together two pairs of the given $2 - SAS$.

**Theorem 7.1** (S. Georgious, C. Koukouvinos and J. Seberry [35]) Let $A_1$, $A_2$ be $(0, \pm 1)$ circulant matrices of order $n$ that satisfying

$$A_1 A_1^T + A_2 A_2^T = kI_n, \quad A_1 A_2^T - A_2 A_1^T = 0, \quad A_1 A_2 = 0$$

then there exists a $2 - SCAS(n; k, k)$.

**Proof.** Set

$$B_1 = aA_1 + bA_2 \quad B_2 = -bA_1 + aA_2,$$

then $B_1$ and $B_2$ are two circulant matrices and satisfying

$$B_1 B_1^T + B_2 B_2^T = (ka^2 + kb^2)I_n$$

and

$$B_1 B_2^T - B_2 B_1^T = 0.$$ 

Thus $B_1$ and $B_2$ is a $2 - SCAS(n; k, k)$. \hfill \Box

**Lemma 7.2** ([35]) If there exists a circulant weighting matrix $W = CW(n, k)$, then there exists a $2 - SCAS(n; k, k)$.

**Proof.** Set $A = aW$ and $B = bW$. The lemma can be easily proved. \hfill \Box

Using sequences given in table 7.2 with theorem 7.1, there exists $2 - SCAS$ for orders and types are described in table 7.2.
### Table 7.1: Disjoint amicable circulant matrices constructed from sequences.

<table>
<thead>
<tr>
<th>$n \geq 1$</th>
<th>Weight</th>
<th>Sequence of $A_1$</th>
<th>Sequence of $A_2$</th>
<th>Zero</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>NPAF</td>
</tr>
<tr>
<td>$2n$</td>
<td>2</td>
<td>1, 0</td>
<td>0, 1</td>
<td>NPAF</td>
</tr>
<tr>
<td>$4n$</td>
<td>4</td>
<td>0, 1, 0, 1</td>
<td>1, 0, -1, 0</td>
<td>NPAF</td>
</tr>
<tr>
<td>$6n$</td>
<td>4</td>
<td>0, 0, 1, 0, 0, 1</td>
<td>0 -1, 0, 0, 1, 0</td>
<td>NPAF</td>
</tr>
<tr>
<td>$6n$</td>
<td>5</td>
<td>0, 1, 0, -1, 0, 1</td>
<td>0, 0, 1, 0, 1, 0</td>
<td>NPAF</td>
</tr>
<tr>
<td>$7n$</td>
<td>4</td>
<td>0, 0, 1, 0, 1, 1, -1</td>
<td>0, 0, 0, 0, 0, 0</td>
<td>PAF</td>
</tr>
<tr>
<td>$8n$</td>
<td>8</td>
<td>1, 1, 1, 0, -1, 1, -1, 0</td>
<td>0, 0, 0, 1, 0, 0, 1</td>
<td>NPAF</td>
</tr>
<tr>
<td>$10n$</td>
<td>9</td>
<td>0, 1, 0, 1, 0, -1, 0, 1, 0, 1</td>
<td>0, 0, 1, 0, -1, 0, -1, 0, 1, 0</td>
<td>PAF</td>
</tr>
<tr>
<td>$12n$</td>
<td>8</td>
<td>0, 1, 1, 0, 1, 0, -1, 1, 0, -1, 0</td>
<td>0, 0, 0, 0, 1, 0, 0, 0, 0, 1</td>
<td>PAF</td>
</tr>
<tr>
<td>$13n$</td>
<td>9</td>
<td>0, 0, 1, 0, 1, 1, -1, -1, 0, 1, -1, 1</td>
<td>0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0</td>
<td>PAF</td>
</tr>
<tr>
<td>$14n$</td>
<td>8</td>
<td>0, 0, 1, 0, 1, 0, -1, 0, 0, 0, 0, 0, 1</td>
<td>0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, -1</td>
<td>PAF</td>
</tr>
<tr>
<td>$14n$</td>
<td>10</td>
<td>1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0</td>
<td>0, 0, 1, 0, -1, 0, 1, 0, 1, 0, -1, 0, -1, 0, -1</td>
<td>NPAF</td>
</tr>
<tr>
<td>$14n$</td>
<td>13</td>
<td>0, 1, 0, 1, 0, -1, 0, 1, 0, -1, 0, 1, 0, 1</td>
<td>0, 0, 1, 0, 1, 0, -1, 0, -1, 0, 1, 0, 1</td>
<td>PAF</td>
</tr>
</tbody>
</table>

### Table 7.2: Order and type for 2-SCAS for all $n \geq 1$.

<table>
<thead>
<tr>
<th>Order</th>
<th>type</th>
<th>Order</th>
<th>type</th>
<th>Order</th>
<th>type</th>
<th>Order</th>
<th>type</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n$</td>
<td>(1, 1)</td>
<td>$6n$</td>
<td>(4, 4)</td>
<td>$10n$</td>
<td>(4, 4)</td>
<td>$14n$</td>
<td>(8, 8)</td>
</tr>
<tr>
<td>$2n$</td>
<td>(2, 2)</td>
<td>$6n$</td>
<td>(5, 5)</td>
<td>$10n$</td>
<td>(9, 9)</td>
<td>$14n$</td>
<td>(10, 10)</td>
</tr>
<tr>
<td>$4n$</td>
<td>(1, 4)</td>
<td>$7n$</td>
<td>(4, 4)</td>
<td>$12n$</td>
<td>(8, 8)</td>
<td>$14n$</td>
<td>(13, 13)</td>
</tr>
<tr>
<td>$4n$</td>
<td>(4, 4)</td>
<td>$8n$</td>
<td>(8, 8)</td>
<td>$13n$</td>
<td>(9, 9)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Theorem 7.2 ([35]) Suppose $A_1$, $A_2$ are two disjoint \{0, ±1\} sequences of length $n$ and weight $k$ with zero PAF (or zero NPAF). Then there are two inequivalent $4$-SCAS($m; k, k, k, k$), $m \geq n$.

**Proof.** Suppose $±a$, $±b$, $±c$ and $±d$ are commuting variables. Let

$$
B_1 = aA_1 + bA_2, \quad B_2 = dA_1 + cA_2,
$$

$$
B_3 = -bA_1 + aA_2, \quad B_4 = cA_1 - dA_2
$$

and

$$
B_1 = aA_1 + bA_2, \quad B_2 = -dA_1 + cA_2,
$$

$$
B_3 = -bA_1 + aA_2, \quad B_4 = cA_1 + dA_2.
$$

Then $B_1$, $B_2$, $B_3$ and $B_4$ are required $4$-SCAS($m; k, k, k, k$), $m \geq n$. This complete the proof.

**Example 7.1** Let $A_1 = \{1, 0, 0, 0, 0, 0, 0, 1, 0, -1, 0\}$ and $A_2 = \{0, 1, 0, 1, 1, 0, 0, 1, 0, -1, 0\}$ be two disjoint sequences of length 11 and weight 9. Using these sequences set $B_1$, $B_2$, $B_3$ and $B_4$ as (7.10) and (7.11) to obtain $4$-SCAS(11; 9, 9, 9, 9).

### 7.3 Construction of amicable orthogonal designs

**Lemma 7.3** (Wolfe) Suppose there are amicable orthogonal designs $A = x_1 A_1 + \cdots + x_u A_u$ and $B = y_1 B_1 + \cdots + y_v B_v$ in order $n$ of type $((p_1, \cdots, p_u); (q_1, \cdots, q_v))$. Further suppose there are amicable orthogonal designs $C = s_1 C_1 + \cdots + s_w C_w$ and $Z$ in order $m$ of type $((r_1, \cdots, r_w); (z))$. Then there exist amicable orthogonal designs in order $mn$ of types $((zp_1, \cdots, zp_{i-1}, r_1, r_1 p_1, \cdots, r_w p_i, zp_{i+1}, \cdots, zp_u); (zq_1, \cdots, zq_v))$.

**Proof.** The required matrices in the variables $a_1, \cdots, a_{i-1}$, $b_1, \cdots, b_w$, $a_{i+1}, \cdots, a_u$, $c_1, \cdots, c_v$ are

$$
a_1 A_1 \times Z + \cdots + a_{i-1} A_{i-1} \times Z + \sum_{j=1}^{w} (b_j A_i \times W_j) + a_{i+1} A_{i+1} \times Z + \cdots + a_u A_u \times Z,
$$

and

$$
\sum_{j=1}^{v} c_j B_j \times Z.
$$

This complete the proof.
### Table 7.3: $4 - SCAS(n;p_1,p_2,p_3,p_4)$, $n$ small, $n \geq 1$.

<table>
<thead>
<tr>
<th>Type</th>
<th>$A_1$</th>
<th>$A_2$</th>
<th>$A_3$</th>
<th>$A_4$</th>
<th>Zero Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(3,3)$</td>
<td>$(a,b)$</td>
<td>$(a,0)$</td>
<td>$(b,0)$</td>
<td>$(b,-a)$</td>
<td>NPAF $2n$</td>
</tr>
<tr>
<td>$(5,5)$</td>
<td>$(a,a,-a)$</td>
<td>$(b,b,-b)$</td>
<td>$(a,a,-a)$</td>
<td>NPAF $3n$</td>
<td></td>
</tr>
<tr>
<td>$(6,6)$</td>
<td>$(a,-b,a)$</td>
<td>$(b,a,b)$</td>
<td>$(b,b,-b)$</td>
<td>NPAF $3n$</td>
<td></td>
</tr>
<tr>
<td>$(1,1,5)$</td>
<td>$(-a,a,a)$</td>
<td>$(0,0,0)$</td>
<td>$(0,0,0)$</td>
<td>NPAF $3n$</td>
<td></td>
</tr>
<tr>
<td>$(1,1,4,4)$</td>
<td>$(a,b,-a)$</td>
<td>$(c,0,c)$</td>
<td>$(c,d,c)$</td>
<td>NPAF $4n$</td>
<td></td>
</tr>
<tr>
<td>$(1,1,2,8)$</td>
<td>$(0,-c,a,c)$</td>
<td>$(0,c,0,c)$</td>
<td>$(0,-c,b,c)$</td>
<td>NPAF $6n$</td>
<td></td>
</tr>
<tr>
<td>$(1,1,5,5)$</td>
<td>$(-c,a,c,0)$</td>
<td>$(c,d,c,0)$</td>
<td>$(-d,b,d,0)$</td>
<td>NPAF $7n$</td>
<td></td>
</tr>
<tr>
<td>$(1,1,8,8)$</td>
<td>$(0,-c,-d,a,d,c)$</td>
<td>$(0,c,-d,0,-d,c)$</td>
<td>$(0,-c,d,b,-d,c)$</td>
<td>NPAF $9n$</td>
<td></td>
</tr>
<tr>
<td>$(2,2,8,8)$</td>
<td>$(d,a,-d,-c,b,c)$</td>
<td>$(c,0,c,d,0,d)$</td>
<td>$(c,0,c,-d,0,-d)$</td>
<td>NPAF $9n$</td>
<td></td>
</tr>
<tr>
<td>$(6,6,12)$</td>
<td>$(c,a,c,b,-c,a)$</td>
<td>$(c,a,c,-a,c,-a)$</td>
<td>$(c,a,c,-b,c,-b)$</td>
<td>NPAF $9n$</td>
<td></td>
</tr>
<tr>
<td>$(14,14)$</td>
<td>$(a,b,-b,-b,a,a)$</td>
<td>$(-b,a,-b,a,-b,b)$</td>
<td>$(a,b,a,b,a,a,-a,a)$</td>
<td>NPAF $9n$</td>
<td></td>
</tr>
<tr>
<td>$(13,13)$</td>
<td>$(c,0,-c,-c,c,0,0,c,c)$</td>
<td>$(c,c,-c,c,c,0,0,-c)$</td>
<td>$(d,0,-d,d,-d,0,0,d,d)$</td>
<td>PAF $9n$</td>
<td></td>
</tr>
<tr>
<td>$(17,17)$</td>
<td>$(a,-a,a,a,a,-a,a,0)$</td>
<td>$(a,-a,-a,a,a,a,-a,a)$</td>
<td>$(a,-a,a,a,a,a,-a,a,0)$</td>
<td>NPAF $9n$</td>
<td></td>
</tr>
</tbody>
</table>
Corollary 7.1 Suppose there exist amicable orthogonal designs of types \(((p_1, \cdots, p_u); (q_1, \cdots, q_v))\) in order \(n\). Further suppose there exist amicable Hadamard matrices of order \(m\) and among them there is a skew matrix. Then there exist amicable orthogonal designs of types \(((p_1, (m-1)p_1, mp_2, \cdots, mp_u); (mq_1, \cdots, mq_v))\) in order \(mn\).

There exist amicable orthogonal designs of type \(((1,1); (1,1))\) in order 2. Setting the variables in the second design equal to each other, then there exist amicable Hadamard matrices of order 2. From corollary 7.1 that there exist amicable orthogonal designs of type \(((1,1,2,4,\cdots, 2^u); (2^u, 2^u))\) and \(((1,2^{u+1}-1); (2^u, 2^u))\) in order \(2^{u+1}\). and well-known fact that amicable Hadamard matrices exist in orders which are a power of 2.

Theorem 7.3 ([36]) Let \(p \equiv 3(\text{mod } 4)\) be a prime power, then there exist amicable orthogonal designs of order \(p+1\) and types \(((1,p); (1,p))\).

Proof. Let \(a_0, a_1, \cdots, a_{p-1}\) be the elements of \(GF(p)\) numbered so that \(a_0 = 0, \ a_{p-i} = -a_i, \ i = 1, \cdots, p-1\). Define \(Q = (q_{ij})\) by

\[
q_{ij} = \begin{cases} 
0 & \text{if } i = j, \\
1 & \text{if } a_j - a_i = y^2 \text{ for some } y \in GF(p), \\
-1 & \text{otherwise.}
\end{cases}
\]

Now \(Q\) is a type 1 matrix which satisfying

\[
QQ^T = pI - J, \quad QJ = JQ = 0, \quad Q' = (-1)^{\frac{1}{2}(p-1)}Q.
\]

Let \(U = cI + dQ\), where \(c, d\) are commuting variables. Define \(R = (r_{ij})\) by

\[
r_{ij} = \begin{cases} 
1 & a_i + a_j = 0, \\
0 & \text{otherwise.}
\end{cases}
\]

Then \(UR\) is a symmetric matrix of type 2. Let \(a, b\) be commuting variables. Then for \(p \equiv 3(\text{mod } 4)\)

\[
A = \begin{pmatrix} 
a & b & \cdots & b \\
-b & \cdots & aI + bQ \\
& \cdots & \ddots & \cdots \\
& & -b & \end{pmatrix}
\text{ and } B = \begin{pmatrix} 
-c & d & \cdots & d \\
d & \cdots & \cdots & \cdots \\
& d & \cdots & \cdots \\
& & \cdots & (cI + dQ)R
\end{pmatrix},
\]

are the required amicable designs of type \(((1,p); (1,p))\) in order \(p+1\). \(\square\)
Theorem 7.4 Suppose $A_1$, $A_2$, $A_3$ and $A_4$ are orthogonal designs of order $n$ such that $(A_1, A_2)$ and $(A_3, A_4)$ are both amicable designs of type $((p_1, \cdots, p_u); (q_1, \cdots, q_v))$. Further suppose that there exists a weight matrix $W = W(n, k)$ such that
\[
A_1W^T = W A_3, \quad A_2W^T = -W A_4^T.
\]
Then there exist amicable designs of order $2n$ of type $((k, p_1, \cdots, p_u); (k, q_1, \cdots, q_v))$.

Proof. The desired matrices are
\[
\begin{pmatrix}
A_1 & xW \\
-xW & A_3
\end{pmatrix}
\quad \text{and} \quad
\begin{pmatrix}
A_2 & yW \\
yW & A_4
\end{pmatrix}.
\]
This completes the proof. \qed

7.4 Applications of orthogonal designs and codes

Codes are widely used in TV, satellites communication, telephone network, mobile services for both domestic and international, data compression, cryptography, and error correcting.

Arithmetic coding provides an effective mechanism for removing redundancy in the encoding of data. It can achieve compression ratio bounds so it is widespread acceptance as an optimal data compression algorithm (see Bell, Cleary and Witten in [8], Witten, Neal and Cleary in [151]).

A synchronous code division multiple access (CDMA) system is used to improve the bandwidth efficiency for today’s communications systems. Walsh codes and orthogonal Gold codes are used implement for CDMA in communications (Garg, Smolik and Wilkes [33]), Tachikawa [140]).

Self-dual codes are used in error correcting (see [74], [101] for details).

Self-dual codes and orthogonal designs have been studied for a long time as separate research areas. J. S. Leon, V. Pless and N. J. A. Sloane in [70], S. Georgiou and C. Koukouvinos in [34] gave some new methods to construct linear self-dual codes over $GF(5)$.

Consider an orthogonal design $OD(n; s_1, s_2)$ in commuting variables $x_1, x_2$. When $x_1$ be replaced by 1 and $x_2$ be replaced by 2, the orthogonal design still holds. Usually take the elements of $GF(5)$ to be either $\{0, 1, 2, 3, 4\}$ or $\{0, \pm 1, \pm 2\}$. 
**Lemma 7.4** ([34]) If \( c = \sum_{i=1}^{2} s_i x_i^2 \), then matrix \( C = (aI_n, A) \) is the generator matrix of a \([2n, n, d; 5]\) linear self-dual code if and only if \( \sum_{i=1}^{2} s_i x_i^2 + a^2 \) is divisible by 5, where \( A \) is the orthogonal design with \( x_1, x_2 \) be replaced by 1 and 2.

**Example 7.2** Consider the following orthogonal design \( OD(8; 2, 6) \):

\[
D = \begin{pmatrix}
  b & a & a & -b & b & b & -b & b \\
  a & b & -b & a & b & b & -b & -b \\
  -a & b & b & a & -b & b & -b & -b \\
  b & -a & a & b & -b & b & b & -b \\
  -b & -b & b & -b & b & a & a & -b \\
  -b & b & b & b & -b & a & a & b \\
  b & b & b & -a & b & b & -a & a \\
  -b & b & b & b & -a & a & b & b \\
\end{pmatrix}
\]

Replace \( a \) with 1 and \( b \) with 2. The matrix

\[
A = \begin{pmatrix}
  2 & 1 & 1 & 3 & 2 & 2 & 3 & 2 \\
  1 & 2 & 3 & 1 & 2 & 2 & 2 & 3 \\
  4 & 2 & 2 & 1 & 3 & 2 & 3 & 3 \\
  2 & 4 & 1 & 2 & 2 & 3 & 3 & 3 \\
  3 & 3 & 2 & 2 & 1 & 1 & 3 & 3 \\
  3 & 3 & 3 & 2 & 1 & 2 & 3 & 1 \\
  2 & 3 & 2 & 2 & 4 & 2 & 2 & 1 \\
  3 & 2 & 2 & 2 & 4 & 1 & 2 & 1 \\
\end{pmatrix}
\]

generate the matrix \( C = (2I_8, A) \) is the generator matrix of a \([16, 8, 6; 5]\) linear self-dual code.
Homogeneous Boolean Functions

Homogeneity becomes a highly desirable property when efficient evaluation of the function is important. It was argued in [94], that for cryptographic algorithms which are based on the structure of MD4 and MD5 algorithms, homogeneous Boolean functions can be an attractive option; they have the property that they can be evaluated very efficiently by re-using evaluations from previous iterations.

Some arguments from [94] can be used to justify the interest in homogeneous functions. Note that in the MD-type hashing (such as MD4 or MD5 or HAVAL), a single Boolean function is used for a number of rounds (in MD4 and MD5 this number is 16, in HAVAL it is 32). In two consecutive rounds, the same function is evaluated with all variables the same except one. More precisely, in the \(i\)-th round the function \(f(x)\) is evaluated for \((x_1, \ldots, x_n)\). In the \((i+1)\)-th round, the same function is evaluated for \(f(x_2, \ldots, x_n, y_1)\) where \(y_1\) is a new variable generated in the \(i\)-th round. Note that variables are rotated between two rounds. It can be proved that evaluations from the \(i\)-th round can be re-used if \(f(x) = f(\text{ROT}(x))\). These Boolean functions create a class of rotation-symmetric functions. An important property of rotation-symmetric functions is that they can be decomposed into one or more homogeneous parts. To keep a round function \(f(x)\) short, one would prefer a homogeneous rotation-symmetric function.

Section 8.2 is based on the paper by J. Seberry, T. Xia, J. Pieprzyk [124]. More than 85 percent of the results are due to the second author. In section 8.2 the author shows how to construct cubic homogeneous bent functions in \(GF(2)^{2n}\) where \(n \geq 3\) and \(n \neq 4\).

Section 8.4 is based on the paper by J. Seberry, T. Xia, J. Pieprzyk and C. Charnes [125]. More than 80 percent of the results are due to the second author. In section 8.4 the author proves there does not exist homogeneous bent functions of degree \(n\) in \(GF(2)^{2n}\) when \(n > 3\).

Section 8.5 is based on the paper by J. Seberry, T. Xia, C. Qu and J. Pieprzyk [126].
80 percent of the results are due to the second author. In section 8.5 the author proves that there exist cubic homogeneous Boolean functions with high nonlinearity and without linear structures in odd space $V_{2n+1}$, $n \geq 2$, $n \neq 4$. The author also shows some methods to construct such cubic homogeneous Boolean functions. However, the construction of high degree homogeneous bent functions has remained an open problem.

### 8.1 Background

**Definition 8.1 (Homogeneous Boolean Function)** A Boolean function $f : V_n \rightarrow GF(2)$ is homogeneous of degree $k$ if it can be represented as

$$f(x) = \bigoplus_{1 \leq i_1 \leq \cdots \leq i_k \leq n} a_{i_1 \cdots i_k} x_{i_1} \cdots x_{i_k},$$

where $x = (x_1, \ldots, x_n)$. Each term $x_{i_1} \cdots x_{i_k}$, $a_{i_1 \cdots i_k} \in GF(2)$ is a product of precisely $k$ co-ordinates.

**Theorem 8.1** Let $f(x)$ be a Boolean function in $GF(2)^n$ and $g(y)$ be a Boolean function in $GF(2)^m$. $f(x) \oplus g(y)$ is a homogeneous bent function of degree $k$ in $GF(2)^{n+m}$ if and only if both $f(x)$ and $g(y)$ are homogeneous bent functions of degree $k$.

**Proof.** If $f(x)$ and $g(y)$ are homogeneous bent functions of degree $k$, it is easy to see $H(z) = f(x) \oplus g(y)$ is a homogeneous bent function of degree $k$ where $z = x \otimes y$.

On the other hand, if $H(z) = f(x) \oplus g(y)$ is a homogeneous bent function of degree $k$ where $z = x \otimes y$, it is easy to know $f(x)$ and $g(y)$ are bent functions, too. Obviously $f(x)$ and $g(y)$ are homogeneous bent functions of degree $k$. The proof is complete. \(\square\)

For $0 \leq t \leq n$, let $S_t^n$ be the set of all $t$-subsets of $\{1, \ldots, n\}$. For any $I \subseteq S_t^n$, write $X_I = \prod_{j \in I} x_j$. Let $t_1, t_2 \geq 0$ with $t_1 + t_2 = t$, and $f = \sum_{I \subseteq S_t^n} a_I X_I \in R(t,n)/R(t-1,n)$, where $a_I \in GF(2)$. Define an $\left( \begin{array}{c} n \\ t_1 \end{array} \right) \times \left( \begin{array}{c} n \\ t_2 \end{array} \right)$ matrix $B_{t_1,t_2}(f)$ over $GF(2)$ as follows:

1. The rows and columns of $B_{t_1,t_2}(f)$ are labeled by the elements of $S_{t_1}^n$ and the elements of $S_{t_2}^n$, respectively.
2. $a_I = 0$ for $I \subseteq \{1, \ldots, n\}$ with $|I| < t$.

**Definition 8.2** Let $m \geq 1$, $F \in \mathbb{R}_m$. The ranks $r_i(F)$, $1 \leq i \leq m$ are defined inductively on $\text{deg}(F)$:
1. When $\deg(F) \leq 1$

$$r_i(F) = \text{rank}(B_{1_{m-i}}^{(i,m)}(F(x))).$$

where $t \leq i \leq m$.

2. When $\deg(F) = t > 1$, let $r_i(F)$, $1 \leq i \leq m$ be given by (8.2). Write $F \sim f(x_1, \cdots, x_r) \oplus g(x_1, \cdots, x_m)$ where $\deg(f) = t$, $r = r_t(F)$, $\deg(g) < t$, and

$$r_i(F) = r_i(g(0, \cdots, 0, x_{r+1}, \cdots, x_m)), \ 1 \leq i < t \quad (8.3)$$

The meaning of the rank is: If $\deg(F) = t$, then $r_i(F) = 0$ for $i > t$, and $r_t(F)$ is the least number of independent linear combinations of $x_1, \cdots, x_m$ needed in the degree $t$ part of $F$. Setting these linear combinations equal to 0, the resulting function is used to define $r_i(F)$ for $i < t$(see Hou [53]).

**Theorem 8.2** (Hou[53]) Let $F$ be a cubic bent function on $V_{2n}$.

1. If $r_2(F) > 0$, then

$$F \sim P(x_1, \cdots, x_{2n-2}) \oplus x_{2n-1}x_{2n}, \quad (8.4)$$

where $P$ is a cubic bent function on $V_{2n-2}$.

2. If $r_3(F) < n$, then $r_2(F) > 0$.

3. If $r_3(F) = n$ and $r_2(F) = 0$, then

$$F \sim Q(x_1, \cdots, x_n) \oplus \sum_{i=1}^{n} x_i x_{n+i} \quad (8.5)$$

for some $Q \in V_n$.

**Theorem 8.3** Let $F(X)$ be a cubic bent function on $V_{2n}$ and $G(X)$ be a homogeneous cubic bent function on $V_{2n}$. If $F \sim G$, then $r_2(F) = 0$ and $r_3(F) \geq n$.

**Proof.** Since $F \sim G$, from the results of the work[53], there is $r_i(F) = r_i(G)$, $i = 2, 3$. Because $G$ is a homogeneous bent function, then $r_2(G) = 0$, $r_2(F) = r_2(G) = 0$. From Theorem 8.2 that $r_3(F) \geq n$ is true. This completes the proof. \qed

**Lemma 8.1** Let $A = (a_{ij})$ be an $n \times n$ matrix, $a_{ij} \in GF(2)$, $1 \leq i, j \leq n$, and $X$ is a vector in $V_n$. Then $XAX^T$ is a linear Boolean function if and only if $A = A^T$. 
Proof. If $XAX^T$ is a linear Boolean function, then there exists a vector $b \in V_n$, such that

$$XAX^T = (X, b)$$

(8.6)

for all $X \in V_n$. As $b = (b_1, \cdots, b_n)$, and $X = (x_1, \cdots, x_n)$, rewrite (8.6) in the following form:

$$\sum_{i,j=1}^{n} a_{ij}x_ix_j = \sum_{i=1}^{n} b_ix_i.$$  

(8.7)

For any fixed $i$, $1 \leq i \leq n$, let $x_i = 1$ and $x_j = 0$, $j \neq i$, $1 \leq j \leq n$, then from (8.7) there is

$$a_{ii} = b_i, i = 1, \cdots, n.$$  

(8.8)

For any pair of $i, j$, $i \neq j$, $1 \leq i, j \leq n$, Let $x_i = x_j = 1$, $x_k = 0$, $k \neq i$ and $k \neq j$, $1 \leq k \leq n$, then from (8.7) there is

$$a_{ii} + a_{jj} + a_{ij} + a_{ji} = b_i + b_j.$$  

(8.9)

From (8.8) and (8.9) there are

$$a_{ij} = a_{ji} \quad 1 \leq i, j \leq n,$$  

(8.10)

and $A = AT$.

Assume that $A = AT$. The following is obtained:

$$XAX^T = \sum_{i,j=1}^{n} a_{ij}x_ix_j$$

$$= \sum_{i=1}^{n} a_{ii}x_i^2 + \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} (a_{ij} \oplus a_{ji})x_ix_j = \sum_{i=1}^{n} a_{ii}x_i$$

is a linear Boolean function. This completes the proof. \qed

Let $F(X)$ be a cubic bent function on $V_{2n}$, $r = r_3(F) \geq n$, $r_2(F) = 0$, then

$$F(X) = \sum_{(i,j,k) \in E} x_i x_j x_k \oplus \sum_{(u,v) \in D} x_u x_v,$$  

(8.11)

$i \neq j, j \neq k, k \neq i, u \neq v$. Suppose $E$ is a collection of unordered triples, and further suppose $D$ is a collection of unordered pairs. Since $r = r_3(F)$, the cubic part of $F(X)$ can be represented as

$$f(x_1, \cdots, x_r) = \sum_{(i,j,k) \in E} x_i x_j x_k.$$  

(8.12)
Denote
\[ X = (x_1, \cdots, x_{2n}) = X^{(1)} \otimes X^{(2)}, \]
\[ X^{(1)} = (x_1, \cdots, x_r), \quad X^{(2)} = (x_{r+1}, \cdots, x_{2n}). \]  
(8.13)

The quadratic part of \( F(X) \) can be represented as
\[ g(x_1, \cdots, x_{2n}) = \sum_{(u,v) \in D} x_u x_v = XQX^T_{(1)}, \]  
(8.14)
where \( Q = (Q_{ij}) \) is a \( 2n \times r \) matrix with
\[ q_{ij} = \begin{cases} 1, & i > j \text{ and } (i,j) \in D, \\ 0, & \text{otherwise}, \end{cases} \]  
(8.15)
where \( 1 \leq i \leq 2n, \ 1 \leq j \leq r \). It is known that \( r_3(F) = r_3(f) \). One can construct a matrix \( B^{(3,r)}_{1,2}(f) \) with \( r \) rows and \( \frac{r(r-1)}{2} \) columns. The columns of the matrix are ordered \( (1,2), \cdots, (1,r), (2,3), \cdots, (2,r), \cdots, (r-1,r) \), and the rows of the matrix are ordered \( 1, \cdots, r \). Then the \( i \)th row and \((j,k)\)th column of the matrix is 1, if \((i,j,k) \in E\), or is 0, if \((i,j,k) \notin E\).

**Notation 8.1** Let \( T = (t_{ij}), 1 \leq i \leq n, 1 \leq j \leq p \). The \( j \)th column of the matrix is denoted as \( t_j \), then \( T = (t_1, \cdots, t_p) \). Let
\[ T^* = (t_1 \ast t_2, \cdots, t_1 \ast t_p, t_2 \ast t_3, \cdots, t_2 \ast t_p, \cdots, t_{p-1} \ast t_p). \]  
(8.16)

Let \( X = (x_1, \cdots, x_n) \in V_n \), denote
\[ X^* = (x_1 x_2, x_1 x_3, \cdots, x_1 x_n) \]  
(8.17)

\( T^* \) is a matrix with \( n \) rows and \( \frac{p(p-1)}{2} \) columns. Denote
\[ C = C(f) = B^{(3,r)}_{1,2}(f)^T. \]  
(8.18)

Then
\[ f(x_1, \cdots, x_r) = X^*_1 C X^T_{(1)}, \]  
(8.19)
where \( X^{(1)}, C, X^*_1 \) are defined as (8.13), (8.18), (8.17).

From (8.11), (8.12), (8.13), (8.14), and (8.19) there is
\[ F(X) = X^*_1 C X^T_{(1)} \oplus XQX^T_{(1)}. \]  
(8.20)
Theorem 8.4 Let \( F(X) \) be a cubic bent function in \( V_{2n} \), which is defined by (8.20). The function \( F(X) \) possesses a cubic homogeneous equivalent if and only if there exists a nonsingular \( 2n \times 2n \) matrix \( T = (T_{(1)}, T_{(2)}) \), and
\[
(T_{(1)}^* C \oplus TQ) T_{(1)}^T = T_{(1)} (T_{(1)}^* C \oplus TQ)^T,
\]
where \( T_{(1)} \) is a matrix with \( 2n \) rows and \( r = r_3(F) \) columns. \( T_{(1)}^* \) is defined by (8.16).

Proof. From formula (8.12) the cubic part of \( F(X) \) is following:
\[
f(X_{(1)}) = \sum_{(i,j,k) \in E} x_i x_j x_k,
\]
Fix \( (i,j,k) \in E \), when \( Y = XT \), \( T = (T_1, \ldots, T_{2n}) \), where \( T_i \) is the \( i \)th column of matrix \( T \), and \( t_{ui} \) denote the \( u \)th row and \( i \)th column of the matrix \( T \), \( 1 \leq u, i \leq 2n \).
\( y_i, y_j, y_k \) becomes \( XT_i, XT_j, XT_k \).
\[
y_i y_j y_k = XT_i XT_j XT_k = \sum_{u,v,w=1}^{2n} x_u t_{ui} x_v t_{vj} x_w t_{wk} = S_1 \oplus S_2,
\]
in which
\[
S_1 = \sum_{u \neq v, v \neq w, w \neq u} t_{ui} t_{vj} t_{wk} x_u x_v x_w = \delta_{ijk}
\]
is a cubic homogeneous polynomial, and
\[
S_2 = \left( \sum_{u=v \neq w}^{2n} \sum_{u \neq v \neq w}^{2n} \sum_{u \neq v \neq w}^{2n} \sum_{u \neq v \neq w}^{2n} \right) t_{ui} t_{vj} t_{wk} x_u x_v x_w
\]
\[
= \left( \sum_{u=v \neq w}^{2n} \sum_{u \neq v \neq w}^{2n} \right) \left( \sum_{u=v \neq w}^{2n} \sum_{u \neq v \neq w}^{2n} \right) \left( \sum_{u=v \neq w}^{2n} \sum_{u \neq v \neq w}^{2n} \right) t_{ui} t_{vj} t_{wk} x_u x_v x_w
\]
\[
= \sum_{u=1}^{2n} t_{ui} t_{uj} x_u \sum_{w=1}^{2n} t_{wk} x_w + \sum_{u=1}^{2n} t_{ui} t_{uj} x_u \sum_{v=1}^{2n} t_{vj} x_v + \sum_{v=1}^{2n} t_{vj} t_{vk} x_v \sum_{u=1}^{2n} t_{ui} x_u
\]
\[
= X(T_i * T_j).XT_k \oplus X(T_i * T_k).XT_j \oplus X(T_j * T_k).XT_i.
\]
So,
\[
f(X_{(1)}) = \sum_{(i,j,k) \in E} \sum_{(i,j,k) \in E} \delta_{ijk}
\]
\[
\oplus \sum_{(i,j,k) \in E} \sum_{(j,k) \in E_i} \left( \sum_{(j,k) \in E_i} X(T_j * T_k) \right) XT_i
\]
\[
= \sum_{(i,j,k) \in E} \delta_{ijk} \oplus \sum_{i=1}^{r} \left( \sum_{(j,k) \in E_i} X(T_j * T_k) \right) XT_i
\]
\[
= \sum_{(i,j,k) \in E} \delta_{ijk} \oplus XT_{(1)}^* C(XT_{(1)})^T,
\]
where \( E_i = \{(j,k)| (i,j,k) \in E\}, i = 1, \ldots, r \). Let

\[
H(X) = \sum_{(i,j,k) \in E} \delta_{ijk}. \tag{8.27}
\]

Now

\[
F(XT) = f(XT\mathbf{l}) \oplus XTQ(XT\mathbf{l})^T = H(X) \oplus X(T^{*}_{\mathbf{l}}C \oplus TQ)T^T_{\mathbf{l}}X^T. \tag{8.28}
\]

So the necessary and sufficient condition for \( F(X) \sim H(X) \) is that there exists a nonsingular matrix \( T \) that makes \( X(T^{*}_{\mathbf{l}}C \oplus TQ)T^T_{\mathbf{l}}X^T \) be the linear function of \( X \). From Lemma 8.1, \( (T^{*}_{\mathbf{l}}C \oplus TQ)T^T_{\mathbf{l}} \) must be a symmetric matrix. The proof is now completed. \( \square \)
8.2 Cubic homogeneous Boolean bent functions

In this section homogeneous bent functions are discussed.

The type of class 1 is quadratic homogeneous Boolean bent function. One can easily construct cubic bent function \( f(x) \) on \( V_{2n} \), which is the type of class 2 with \( r_3(f) = n \).

**Theorem 8.5** Let \( F(X) \) be a cubic bent function on \( V_{2n} \) with the type given by (2.9). Set a nonsingular \( 2n \times 2n \) matrix \( T \) which has the following structure:

\[
T = \begin{pmatrix}
I & 0 \\
A & M
\end{pmatrix},
\]  

(8.29)

where \( I \) is a \( n \times n \) identity matrix, \( 0 \) is a \( n \times n \) zero matrix, \( M \) is a \( n \times n \) nonsingular matrix, \( A = (a_{ij}) \), \( a_{ij} \in GF(2) \), \( i, j = 1, \ldots, n \). Then \( F(XT) \) is a cubic homogeneous bent function if and only if

\[
A^* C = M,
\]  

(8.30)

where \( C \) is defined in (8.18), and \( A^* \) is defined as (8.16).

**Proof.** For an arbitrary cubic bent function \( F(X) \), it is probably can be represented in the form (8.20). When \( C \) and \( Q \) are uniquely defined, according to the theorem 8.4, there exists a matrix \( T_{(1)} \) of the form (8.21). Let \( Q \) and \( T_{(1)} \) defined as

\[
Q = \begin{pmatrix}
0 \\
I
\end{pmatrix}, \quad T_{(1)} = \begin{pmatrix}
I \\
A
\end{pmatrix},
\]  

(8.31)

then

\[
T_{(1)}^* = \begin{pmatrix}
I \\
A
\end{pmatrix}^* = \begin{pmatrix}
0 \\
A^*
\end{pmatrix}, \quad TQ = \begin{pmatrix}
0 \\
M
\end{pmatrix}.
\]  

(8.32)

\( F(X) \sim H(X) \) where \( H(X) \) is a cubic homogeneous function if and only if formula (8.21) holds. Now

\[
(T_{(1)}^* C \oplus TQ)T_{(1)}^T = \begin{pmatrix}
0 \\
A^* C \oplus M
\end{pmatrix}(I, A^T) = \begin{pmatrix}
0 \\
A^* C \oplus M 
\end{pmatrix} A^* C A^T \oplus M A^T
\]  

(8.33)

The result matrix is symmetric if and only if \( A^* C \oplus M = 0 \). The proof is completed. \( \square \)
Theorem 8.6 Let $F(X) = f(x_1, \cdots, x_n) + \sum_{i=1}^{n} x_i x_{i+n}$ be a bent function on $V_{2^n}$, where $f$ is a homogeneous cubic function of $(x_1, \cdots, x_n)$ and $r_3(f) = n$. Then there exists a nonsingular matrix $T$ such that $F(XT)$ is a cubic homogeneous bent function.

**Proof.** Let $C$ be the $\frac{n(n-1)}{2} \times n$ matrix defined as that in (8.18). Since $\text{rank}(C) = n$, there are $n$ rows of $C$, say, $(j_1, k_1), \cdots, (j_n, k_n)$, such that the matrix $M$ which consists of these $n$ rows is nonsingular matrix. $A = (a_{ij})_{1\leq i, j \leq n}$ is defined as follows:

\[
a_{ij} = \begin{cases} 
1, & \text{if } j = j_i \text{ or } j = k_i, \\
0, & \text{otherwise,}
\end{cases} \quad i = 1, \cdots, n. \tag{8.34}
\]

Let $T = \begin{pmatrix} I & 0 \\ A & M \end{pmatrix}$, where $I$ is $n \times n$ identity matrix, $0$ is $n \times n$ zero matrix. Obviously, $T$ is a nonsingular matrix.

For any fixed $i$, $1 \leq i \leq n$, in the $i$th row of $A^*$, $a_{i1}a_{i2}, \cdots, a_{i1}a_{im}, \cdots, a_{in-1}a_{in}$, only one component $a_{ij} = 1$ and others are all 0. So the matrix product of the $i$th row of $A^*$ with $C$ gives the $(j_i, k_i)$-th row of $C$. That is $A^*C = M$, the (8.30) holds and $F(XT)$ is a cubic homogeneous bent function. This completes the proof. \( \square \)

Let $E$ be an unordered triple set: $E = \{(i, j, k) : 1 \leq i, j, k \leq n\}$, write $E_i = \{(j, k) : (i, j, k) \in E\}, 1 \leq i \leq n$.

**Definition 8.3 (Regular unordered triplet set)** The unordered triplet set $E$ is called regular if $E_i \setminus (\cup_{j \neq i} E_j) \neq \phi, 1 \leq i \leq n$.

Theorem 8.7 Let $F(X) = \sum_{(i,j,k) \in E} x_i x_j x_k + \sum_{i=1}^{n} x_i x_{i+n}$, $r_3(F) = n$ be a Boolean function in $GF(2)^{2n}$. If $E$ is a regular unordered triple set, then there exists a square matrix $A$ which satisfies the equation (8.30) with $M = I$, and $F(XT)$ is a cubic homogeneous bent function.

**Proof.** Let the left side of (8.30) expanded. Hence

\[
\left( \sum_{(j,k) \in E_i} a_j * a_k, \cdots, \sum_{(j,k) \in E_n} a_j * a_k \right) = I, \tag{8.35}
\]

in which $a_i, 1 \leq i \leq n$ is the $i$th column of matrix $A$. Since $E$ is regular, $E_i \setminus (\cup_{j=1}^{n} E_j) \neq \phi$, there exists at least one unordered pair $(j, k) \in E_i \setminus (\cup_{j=1}^{n} E_j)$, so choose

\[
a_{ik} = a_{ij} = 1, \quad a_{il} = 0, \quad j \neq l \neq k, 1 \leq l \leq n.
\]
In this case, only \( a_{ij}a_{ik} = 1 \), and if \((u, v) \neq (j, k)\), \( a_{iu}a_{iv} = 0 \). Now the \( i \)th row of left side of (8.35) becomes \( (0, \ldots, 0, 1, 0, \ldots, 0) \), this is identical with the \( i \)th row of right side of (8.35). Hence equation (8.35) holds. Consequently, \( F(XT) \) is a cubic homogeneous bent function. The proof is completed.

**Theorem 8.8** For all \( n \geq 3 \) and \( n \neq 4 \), there exist cubic homogeneous bent functions on \( V_{2n} \).

**Proof.** There are three cases:

1. \( n \equiv 0 \pmod{3} \). Write \( n = 3m \) for some positive integer \( m \), \( m \geq 1 \). Let

\[
F(X) = \sum_{i=1}^{m} x_{2i-2}x_{2i-1}x_{2i} \oplus x_{1}x_{4}x_{3m+1} \oplus \sum_{i=1}^{3m} x_{i}x_{i+3m} \tag{8.36}
\]

Then \( F(X) \) is a bent function of class 2. Now

\[
E = \{(3i - 2, 3i - 1, 3i) : 1 \leq i \leq m\}
\]

is the regular un-ordered triple set and \( F(X) \) be a cubic bent function on \( V_{2n} \) with the form of (2.9). Hence from Theorem 8.5 there exists a \( 2n \times 2n \) nonsingular matrix \( T \) with the form of (8.29) which makes (8.30) hold. So \( F(XT) \) is cubic homogeneous bent function.

2. \( n \equiv 1 \pmod{3}, n \neq 4 \). Write \( n = 3m + 1 \) for some positive integer \( m \), \( m \geq 2 \). Let

\[
F(X) = \sum_{i=1}^{m} x_{2i-2}x_{2i-1}x_{2i} \oplus x_{1}x_{4}x_{3m+1} \oplus \sum_{i=1}^{3m+1} x_{i}x_{i+3m+1}. \tag{8.37}
\]

It is a bent function. In this case, let

\[
E = \{(3i - 2, 3i - 1, 3i) : 1 \leq i \leq m\} \cup \{(1, 4, 3m + 1)\}, \tag{8.38}
\]

which is regular and \( F(X) \) be a bent function on \( V_{2n} \) with the form of (2.9), the conclusion of Theorem 8.8 is also valid.

3. \( n \equiv 2 \pmod{3} \). Write \( n = 3m + 2 \) for some \( m \), \( m \geq 1 \). Let

\[
F(X) = \sum_{i=1}^{m} x_{2i-2}x_{2i-1}x_{2i} \oplus x_{1}x_{3m+1}x_{3m+2} \oplus \sum_{i=1}^{3m+2} x_{i}x_{i+3m+2}, \tag{8.39}
\]

and

\[
E = \{(3i - 2, 3i - 1, 3i) : 1 \leq i \leq m\} \cup \{(1, 3m + 1, 3m + 2)\}. \tag{8.40}
\]

The proof of this case is the same as before.

Hence the statement of the theorem is true and the proof is completed.
8.3 Fourier transform of homogeneous bent function

Lemma 8.2 Let \( Z = X \otimes Y \), where \( X = (x_1, \cdots, x_n) \in GF(2)^n \), \( Y = (y_1, \cdots, y_n) \in GF(2)^n \), \( T \) is a \( 2n \times 2n \) matrix and \( T = \begin{pmatrix} L & 0 \\ A & M \end{pmatrix} \), where \( L, A, M \) are \( n \times n \) matrix and \( L^{-1} \) and \( M^{-1} \) exist. \( f(Z) = P(X) \oplus (X, Y) \) and \( g(Z) = f(ZT) \) are bent functions in \( GF(2)^{2n} \). The Fourier transform of \( g(Z) \) is:

\[
\mathcal{F} g(Z) = P((Y \oplus X(AL^{-1})^T)(M^T)^{-1}) \oplus ((Y \oplus X(AL^{-1})^T)(M^T)^{-1}, X(L^T)^{-1}).
\]

Proof. Let \( W = U \otimes V, U = (u_1, \cdots, u_n), V = (w_{n+1}, \cdots, w_{2n}) \). From the Fourier transform definition,

\[
(-1)^{\mathcal{F} g(Z)} = 2^{-n} \sum_{W \in GF(2)^{2n}} (-1)^{\eta(W) \oplus (W, Z)}
\]

\[
= 2^{-n} \sum_{U, V \in GF(2)^n} (-1)^{f(U \oplus V A) \oplus (UL \oplus VA, VM) \oplus (U, X) \oplus (V, Y)}
\]

\[
= 2^{-n} \sum_{V \in GF(2)^n} (-1)^{f(U \oplus V A) \oplus (UL \oplus VA, VM) \oplus (UL \oplus VA, X(L^T)^{-1})}
\]

\[
\sum_{U \in GF(2)^n} (-1)^{f(U \oplus V A) \oplus (UL \oplus VA, VM) \oplus (UL \oplus VA, X(L^T)^{-1})}
\]

\[
= 2^{-n} \sum_{V \in GF(2)^n} (-1)^{f(U \oplus V A) \oplus (UL \oplus VA, VM) \oplus (UL \oplus VA, X(L^T)^{-1})}
\]

\[
= 2^{-n} \sum_{S \in GF(2)^n} (-1)^{f(S) \oplus (S, X(L^T)^{-1})} \sum_{V \in GF(2)^n} (-1)^{f(U \oplus V A) \oplus (UL \oplus VA, VM) \oplus (UL \oplus VA, X(L^T)^{-1})}
\]

\[
= (-1)^{f((Y \oplus X(AL^{-1})^T)(M^T)^{-1}) \oplus ((Y \oplus X(AL^{-1})^T)(M^T)^{-1}, X(L^T)^{-1})}.
\]

\[\Box\]

Lemma 8.3 Let \( g(X, Y) = f(X \oplus YA) \oplus (X \oplus YA, Y) \), where \( A = A^T \) and \( X, Y \in V_n \). Then \( \mathcal{F} g(X, Y) = g(Y, X) \). If \( g(X, Y) \) is an homogeneous bent function. \( \mathcal{F} g \) is an homogeneous bent function, too.

Proof. Now \( L = M = I, A = A^T \). From lemma 8.2 there is

\[
\mathcal{F} g(X, Y) = f(Y \oplusXA) \oplus (Y \oplusXA, X) = g(Y, X).
\]

The rest of lemma is trivial.

\[\Box\]
Lemma 8.4 There exist cubic homogeneous bent functions $g(X)$ in $GF(2)^{2n}$ when $n \geq 3$, $n \neq 4$, and their Fourier transforms are also cubic homogeneous bent functions.

Proof. Let $J_n$ denote $n \times n$ matrix with all one entries. Set

$$A_1 = J_3 - I_3, \quad A_2 = J_5 - I_5, \quad A_3 = J_7 - I_7.$$ 

1. When $n = 3m$, $m \geq 1$. Let

$$f(x) = \bigoplus_{i=1}^{m} x_{3i-2}x_{3i-1}x_{3i} \oplus \bigoplus_{j=1}^{3m} x_jx_{j+3m}.$$ 

$f(x)$ is a cubic bent function on $V_{2n}$ and set

$$T = \begin{pmatrix} I_n & 0 \\ A & I_n \end{pmatrix}, \quad \text{(8.43)}$$

and

$$A = \begin{pmatrix} A_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & A_1 \end{pmatrix}.$$ 

Then $g(x) = f(xT)$ is a homogeneous bent function. Since $A^T = A$, from lemma 8.3 we obtain that $\mathcal{F}_g$ is an homogeneous bent function.

2. When $n = 3m + 1$, $m \geq 2$. Let

$$f(x) = x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_1x_6x_7 \oplus x_2x_4x_6 \oplus x_2x_5x_7 \oplus x_3x_4x_6 \oplus x_3x_5x_7 \oplus \bigoplus_{i=1}^{m-2} x_{3i+6}x_{3i+7}x_{3i+8} \oplus \bigoplus_{j=1}^{3m+1} x_jx_{j+3m+1}.$$ 

When $m = 2$, suppose $\bigoplus_{i=1}^{6} x_{3i+5}x_{3i+6}x_{3i+7} = 0$. It is easy to verify that $f(x)$ is a cubic bent function. Suppose matrix $T$ is the form of (8.43) and set

$$A = \begin{pmatrix} A_3 & 0 & \cdots & 0 \\ 0 & A_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_1 \end{pmatrix}.$$ 

Then $g(x) = f(xT)$ is a cubic homogeneous bent function. Since $A^T = A$, from lemma 8.3 it is true that $\mathcal{F}_g$ is a cubic homogeneous bent function, too.
3. When \( n = 3m + 2, \ m \geq 1 \). Let

\[
 f(x) = x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_3 x_5 \oplus x_2 x_4 x_5 \oplus x_3 x_4 x_5 \quad \text{(8.44)}
\]

\[
 \oplus \left( \bigoplus_{i=1}^{m-1} x_{3i+3} x_{3i+4} x_{3i+5} \right) \oplus \left( \bigoplus_{j=1}^{3m+2} x_j x_{j+3m+2} \right). \quad \text{(8.45)}
\]

It is easy to verify that \( f(x) \) is a cubic bent function. Let \( T \) be the matrix as (8.43) and set

\[
 A = \begin{pmatrix}
 A_2 & 0 & \cdots & 0 \\
 0 & A_1 & \cdots & 0 \\
 \vdots & \vdots & \ddots & \vdots \\
 0 & 0 & \cdots & A_1
\end{pmatrix}.
\]

Then \( g(x) = f(xT) \) is a cubic homogeneous bent function. Since \( A^T = A \), from lemma 8.3 it is true that \( \mathcal{F}_g \) is a cubic homogeneous bent function.

The proof is completed. \( \square \)
8.4 The degree of homogeneous bent functions is less than \( n \) on \( V_{2^n}, n \geq 4 \).

Rothaus [104] showed that bent functions in \( 2n \) variables exist only if their degree is less than or equal to \( n \). In this section the author shows that the homogeneous requirement influences the degree of bent functions. The homogeneous bent functions of degree \( n \) on \( V_{2^n} \) does not exist for \( n > 4 \). The proof uses a certain decomposition of a Menon difference set, which corresponds to any bent function. In particular, there is no homogeneous bent function of degree 4 on \( V_8 \). The only exceptions are the 3-homogeneous Boolean functions of 6 variables, and the 2-homogeneous Boolean functions of 4 variables.

The difference between two sets is defined as following:

**Definition 8.4** (Difference) Given two sets \( A, B \subset V_n \). The difference between two sets is

\[
A - B = \sum_{x \in A; \ y \in B} (x \oplus y).
\]

In particular, if \( A = B \), the difference is denoted as

\[
\Delta A = A - A.
\]

If \( A \neq B \) then the following notation is useful

\[
\Delta(A, B) = (A - B) + (B - A).
\]

If \( A = \emptyset \), then

\[
\Delta \emptyset = 0 \text{ and } \Delta(\emptyset, B) = 0.
\]

where \( B \in V_n \).

By convention, for sets \( A, B \subset V_n \), the difference \( A - B \) is a set of vectors \( x \oplus y \) where vectors \( x \) and \( y \) run through the sets \( A \) and \( B \), respectively.

Let \( f : V_{2n+2} \rightarrow GF(2) \) be a Boolean function. For the function \( f(x) \), one can determine the set

\[
D = \{ x \in V_{2n+2} \mid f(x) = 1 \},
\]

and

\[
D_1 = \{ x \in V_{2n} \mid f(x, 0, 0) = 1 \},
\]

\[
D_2 = \{ x \in V_{2n} \mid f(x, 0, 1) = 1 \},
\]

\[
D_3 = \{ x \in V_{2n} \mid f(x, 1, 0) = 1 \},
\]

\[
D_4 = \{ x \in V_{2n} \mid f(x, 1, 1) = 1 \}
\]
8.4. The degree of homogeneous bent functions is less than \( n \) on \( V_{2n}, n \geq 4 \).

where \( x = (x_1, \ldots, x_{2n}) \) is a binary vector. Let introduce the following notation:

\[
P_1 = (0, 0), \quad P_2 = (0, 1), \quad P_3 = (1, 0), \quad P_4 = (1, 1).
\]  

(8.47)

Clearly, the set \( D \) can be represented as

\[
D = \bigcup_{i=1}^{4} (D_i \otimes P_i)
\]

(8.48)

where the set \( D_i \otimes P_i \) contains all vectors from \( D_i \) extended by the vector \( P_i; \ i = 1, 2, 3, 4 \). Consider the difference set \( \Delta D \). From the definition, there is

\[
\Delta D = \sum_{x \in D; \ y \in D} x \oplus y = \sum_{x \in \bigcup_{i=1}^{4} (D_i \otimes P_i); \ y \in \bigcup_{j=1}^{4} (D_j \otimes P_j)} x \oplus y
\]

\[
= \sum_{i,j=1}^{4} (D_i \otimes P_i - D_j \otimes P_j).
\]

After rearranging the differences, then

\[
\Delta D = \sum_{i=1}^{4} \Delta(D_i \otimes P_i) + \sum_{i=1}^{3} \sum_{j=i+1}^{4} \Delta ((D_i \otimes P_i), (D_j \otimes P_j)).
\]  

(8.49)

Sets \( D_i \) can be characterized by the minimum weight of their vectors and

\[
t_i = \min_{x \in D_i} W(x) \text{ for } i = 1, 2, 3, 4.
\]  

(8.50)

**Lemma 8.5** Given a homogeneous function \( f : V_{2n+2} \to GF(2) \) of degree \( n + 1 \) and its sets \( D_i; i = 1, 2, 3, 4 \), then

\[
t_1 \geq n + 1, \quad t_2 \geq n, \quad t_3 \geq n, \quad t_4 \geq n - 1.
\]

where \( t_i \) is defined by Equation (8.50).

**Proof.** (By contradiction) Suppose \( t_1 < n + 1 \). This means that there is a vector \( x = (x_1, \ldots, x_{2n}, 0, 0) \) whose weight \( W(x) \leq n \). Then at most \( n \) co-ordinates \( x_i; i = 1, \cdots, 2n \) take on the value 1. The remainder co-ordinates take on the value zero. However, since \( f(x) \) is a homogeneous Boolean function of degree \( n + 1 \) over \( V_{2n+2} \) each term of the function has precisely \( n + 1 \) co-ordinates and so each term of the function is zero. Hence \( f(x) = 0 \) which implies that \( x \notin D_1 \). This contradicts the definition of \( D_1 \) and therefore, \( t_1 > n \). The proof for other cases is similar and is omitted. \( \Box \)
Lemma 8.6 Given a positive integer \( n \). Then
\[
2^{n+1} < \binom{2n}{n} \tag{8.51}
\]
if and only if \( n \geq 3 \).

The proof for next proposition via difference sets.

Proposition 8.1 Given a Boolean bent function \( f : V_{2n+2} \to GF(2) \) (not necessary homogeneous) and sets \( D_i \) for \( i = 1, 2, 3, 4 \) defined for the bent function \( f(x) \) according to Formula (8.46). Let \( k_i \) denote the cardinality of sets \( D_i \) (or \( k_i = |D_i| \)) for \( i = 1, 2, 3, 4 \). Then

1. three of \( k_1, k_2, k_3, k_4 \) are equal and the remaining one is different, and
2. \( \min(k_1, k_2, k_3, k_4) \geq 2^{2n-1} - 2^n \).

Proof. Define \( T = \sum_{x \in V_{2n+2}} x \) which is the set of all vectors from \( V_{2n+2} \) and denote the vector \((0, \cdots, 0) \in V_{2n+2} \) as \( \theta \). The function \( f(x) \) is bent if and only if its set \( D = \{ x \in V_{2n+2} | f(x) = 1 \} \) generates the difference set with parameters \((v, k, \lambda) = (2^{2n+2}, 2^{2n+1} \pm 2^n, 2^{2n} \pm 2^n) \) (see [69]). That is
\[
\Delta D = (k - \lambda)\theta + \lambda T = 2^{2n}\theta + (2^n \pm 2^n)T \tag{8.52}
\]

On the other hand, according to Equation (8.49), there is
\[
\Delta D = \left( \sum_{i=1}^{4} \Delta D_i \right) \otimes P_i
\]

If compare (8.52) with (8.53), one can get the following system of equations (see [155])
\[
\sum_{i=1}^{4} \Delta D_i = 2^{2n}\theta T + \lambda T^T
\]
\[
\Delta(D_1, D_2) + \Delta(D_3, D_4) = \lambda T^T \tag{8.54}
\]
\[
\Delta(D_1, D_3) + \Delta(D_2, D_4) = \lambda T^T
\]
\[
\Delta(D_1, D_4) + \Delta(D_2, D_3) = \lambda T^T
\]
where \( \theta^T \) is the zero vector in \( V_{2n} \) and \( T^T = \sum_{x \in V_{2n}} x \). Count the number of terms on both sides of \((8.54)\) and obtain the following equations:

\[
\begin{align*}
    k_1^2 + k_2^2 + k_3^2 + k_4^2 &= 2^{2n} + \lambda 2^{2n} \quad (8.55) \\
    2k_1k_2 + 2k_3k_4 &= \lambda 2^{2n} \quad (8.56) \\
    2k_1k_3 + 2k_2k_4 &= \lambda 2^{2n} \quad (8.57) \\
    2k_1k_4 + 2k_2k_3 &= \lambda 2^{2n} \quad (8.58)
\end{align*}
\]

Without loss of generality, assume that

\[
k_1 \leq k_2 \leq k_3 \leq k_4 \quad (8.59)
\]

From \((8.55)\), \((8.56)\), \((8.57)\) and \((8.58)\) one can get

\[
\begin{align*}
    (k_1 - k_2)^2 + (k_3 - k_4)^2 &= 2^{2n}, \\
    (k_4 - k_1)(k_3 - k_2) &= 0, \\
    (k_2 - k_1)(k_4 - k_3) &= 0.
\end{align*}
\]

Thus \( k_1 = k_2 = k_3 < k_4 \) or \( k_1 < k_2 = k_3 = k_4 \). This completes the part (1) of the proof.

Assume that \( k_1, k_2, k_3 \) equals to \( k \) and \( k_4 \) equals to \( k^T \). Now equation \((8.55)\) reduces to

\[
3k^2 + k^T = 2^{2n} + \lambda 2^{2n}. \quad (8.60)
\]

The cardinality of the set \( D \) is the sum of numbers of vectors in \( D_1, D_2, D_3, D_4 \), so

\[
3k + k^T = 2^{2n+1} \pm 2^n. \quad (8.61)
\]

First suppose the right side of the equation \((8.61)\) is \( 2^{2n+1} - 2^n \). Then \( \lambda = 2^{2n} - 2^n \).

From \((8.60)\) and \((8.61)\) one can get

\[
\begin{align*}
    k &= 2^{2n-1} \quad \text{and} \quad k^T = 2^{2n-1} - 2^n, \\
    \text{or} \\
    k &= 2^{2n-1} - 2^{n-1} \quad \text{and} \quad k^T = 2^{2n-1} + 2^{n-1}.
\end{align*}
\]

In this case

\[
min(k_1, k_2, k_3, k_4) = min(k, k^T) \geq 2^{2n-1} - 2^n. \quad (8.63)
\]
8.4. The degree of homogeneous bent functions is less than \( n \) on \( V_{2n} \), \( n \geq 4 \).

When the right side of the equation (8.61) is \( 2^{2n+1} + 2^n \), then \( \lambda = 2^{2n} + 2^n \). From (8.60) and (8.61) there is

\[
k = 2^{2n-1} + 2^{n-1} \quad \text{and} \quad k^T = 2^{2n-1} - 2^{n-1},
\]

or

\[
k = 2^{2n-1} \quad \text{and} \quad k^T = 2^{2n-1} + 2^n.
\]

Equation (8.63) holds as well. This proves the part (2) and completes the proof of the proposition.

\[\square\]

Theorem 8.9 Let \( f : V_{2n+2} \rightarrow GF(2) \) be a homogeneous Boolean function of degree \( n + 1 \) and let \( n \geq 3 \). Then \( f(x) \) is not bent.

Proof. (By contradiction) Suppose \( f(x) \) is a bent function. Then the set \( D = \{ x | f(x) = 1 \} \) is a difference set with parameters \( (2^{2n+2}, 2^{2n+1} \pm 2^n, 2^{2n} \pm 2^n) \). Moreover,

\[
D = \bigcup_{i=1}^{4} (D_i \otimes P_i)
\]

where the sets \( D_i \) are defined by Equation (8.46). From Lemma 8.5 that the minimum weight of vectors in \( D_1 \) (denoted as \( t_1 \)) is \( t_1 \geq n + 1 \). From Proposition (8.1), the number of vectors in \( D_1 \) (denoted as \( k_1 \)) is \( k_1 \geq 2^{2n-1} - 2^n \). Consider the following set

\[
D_0 = \{ (x_1, \cdots, x_{2n}) \in V_{2n} | W(x) \geq n + 1 \}.
\]

It is obvious that \( D_0 \supseteq D_1 \). Denote the number of elements in \( D_0 \) by \( k_0 \). Clearly \( k_0 \geq k_1 \). But

\[
k_0 = \sum_{i=1}^{n} \left( \binom{2n}{n+i} \right) = \frac{1}{2} \left( \sum_{i=0}^{2n} \left( \binom{2n}{i} - \binom{2n}{n} \right) \right)
\]

\[
= \frac{1}{2} \left( 2^{2n} - \binom{2n}{n} \right) = 2^{2n-1} - \frac{1}{2} \binom{2n}{n}.
\]

From Lemma 8.6, one can establish the following relation

\[
k_0 < 2^{2n-1} - 2^n \leq k_1
\]

if \( n \geq 3 \). This leads to the contradiction which also completes the proof.

\[\square\]

Theorem (8.9) demonstrates that the homogeneous requirement restricts dramatically a possible selection of bent (and homogeneous) functions. One can formulate the following observations:
any homogeneous bent function $f : V_{2n} \to GF(2)$ is of degree smaller than $n$ for all $n > 3,$

in particular, for $V_6$, there is a collection of homogeneous bent functions of degree 3. For $V_6$, there is no homogeneous bent function of degree 4. This persists for all higher (and even) dimensions.
8.5 Homogeneous Boolean functions with high nonlinearity on $V_{2n+1}$

In this section highly nonlinear Boolean functions on $V_{2n+1}$ are studied, i.e. for the dimensions where bent functions do not exist. There exist Boolean functions on $V_{2n+1}$ with non-linearity greater than or equal to $2^{2n} - 2^n$ and without linear structures, $n \geq 2$. Note that the non-existence of linear structures makes the functions similar to the bent ones. Moreover, for $n \geq 2$, $n \neq 4$, there exist cubic homogeneous Boolean functions on $V_{2n+1}$ with non-linearity at least $2^{2n} - 2^n$ and without linear structures.

**Lemma 8.7** Let $A$ be a nonsingular $n \times n$ matrix, $\alpha$ be a vector from $V_n$, and $\varphi(x)$ be an affine function on $V_n$. Then an arbitrary Boolean function $f(x) : V_n \rightarrow GF(2)$ and $g(x) = f(xA \oplus \alpha) \oplus \varphi(x)$ share the same nonlinearity, or

$$N_f = N_g.$$  

**Lemma 8.8** If $f(x)$ on $V_n$ is a bent function, then $f(x)$ has no linear structure.

**Theorem 8.10** Suppose $f(x)$ is a Boolean function on $V_{2m+1}$ with $N_f \geq 2^{2m} - 2^m$ which has no linear structure. Then there exists a Boolean function $F(x)$ on $V_{2n+1}$ that has no linear structure and its non-linearity $N_f \geq 2^{2n} - 2^n$ for every $n \geq m$.

**Proof.** When $n = m$, the conclusion is trivial. Suppose $n > m$. Let $g(x)$ be a bent function on $V_{2(n-m)}$. Set $F(z) = f(x) \oplus g(y)$, where $z = (x, y), x \in V_{2m+1}, y \in V_{2(n-m)}$. Clearly, $F(z)$ has no linear structure.

For any affine function $\varphi$ on $V_{2n+1}$, write $\varphi(z) = \varphi(x) \oplus \psi(y)$ where $\phi(x)$ and $\psi(y)$ are affine functions on $V_{2m+1}$ and $V_{2(n-m)}$. Let $\alpha, \beta, \gamma, \zeta, \xi, \eta$ denote the sequences of $F(z), f(x), g(y), \varphi(z), \phi(x)$ and $\psi(y)$, respectively. Then

$$\langle \alpha, \zeta \rangle = \sum_z (-1)^{F(z) \oplus \varphi(z)} = \langle \beta, \xi \rangle \langle \gamma, \eta \rangle$$

Since $N_f = \min_{\varphi} \{2^{2m} - \frac{1}{2} \langle \beta, \xi \rangle \} \geq 2^{2m} - 2^m$ and $g(y)$ is a bent on $V_{2(n-m)}$, then

$$| \langle \beta, \xi \rangle | \leq 2^{m+1} \text{ and } | \langle \gamma, \eta \rangle | = 2^{n-m},$$

So $| \langle \alpha, \zeta \rangle | \leq 2^{n+1}$ and

$$d(F, \varphi) = 2^{2n} - \frac{1}{2} \langle \alpha, \zeta \rangle \geq 2^{2n} - \frac{1}{2} | \langle \alpha, \zeta \rangle | \geq 2^{2n} - 2^n$$

This completes the proof. □

From Theorem 8.10 the following corollaries are true.
Corollary 8.1 There exist Boolean functions on $V_{2n+1}$ with no linear structure and with high non-linearity, $N_f \geq 2^{2n} - 2^n$, for $n \geq 2$.

Proof. On $V_5$ set $f(x) = x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5$. It is easy to verify that $f(x)$ has no linear structure and $N_f = 2$. By Theorem 8.10 the conclusion of Corollary 8.1 is valid. □

Corollary 8.2 Let $f(x)$ be a Boolean function on $V_{2n+1}$ with $N_f \geq 2^{2n} - 2^n$ and $g(y)$ be a bent function on $V_{2m}$. Then $F(z) = f(x) \oplus g(y)$ is the Boolean function on $V_{2(n+m)+1}$ with $N_F \geq 2^{2(n+m)} - 2^{n+m}$.

Lemma 8.9 Let $f(x)$ be a Boolean function on $V_n$, and $g(x) = f(xT \oplus \alpha) \oplus \varphi(x)$ where $T$ is an $n \times n$ nonsingular matrix, $\alpha \in V_n$ and $\varphi$ is an affine function on $V_n$. Then $g(x)$ has linear structure if and only if $f(x)$ does, and the numbers of linear structures of $f(x)$ and $g(x)$ are the same.

Proof. Suppose $\beta$ is a linear structure of $f(x)$, so $f(x \oplus \beta) \oplus f(x)$ is constant. Then
\[
g(x \oplus \beta T^{-1}) \oplus g(x) = f(xT \oplus \beta \oplus \alpha) \oplus \varphi(x \oplus \beta T^{-1}) \oplus f(xT \oplus \alpha) \oplus \varphi(x)
= (f((xT \oplus \alpha) \oplus \beta) \oplus f(xT \oplus \alpha)) \oplus (\varphi(x \oplus \beta T^{-1}) \oplus \varphi(x)).
\]
If $\beta \neq 0 \in V_n$ and $T$ is a nonsingular matrix, then $\beta T^{-1} \neq 0 \in V_n$. Since $\varphi(x)$ is affine Boolean function, $\varphi(x \oplus \beta T^{-1}) \oplus \varphi(x)$ is constant. Thus
\[
f((xT \oplus \alpha) \oplus \beta) \oplus f(xT \oplus \alpha) = f(y \oplus \beta) \oplus f(y)
\]
is constant. $\beta T^{-1}$ is a linear structure of $g(x)$. The reverse is obvious. Since the mapping from $\beta$ to $\beta T^{-1}$ is one to one, the numbers of linear structures of $f(x)$ and $g(x)$ are the same. □

Lemma 8.10 Suppose $n$ is odd and $n \times n$ symmetric matrix $A = (a_{ij})_{1 \leq i,j \leq n}$ with $a_{ii} = 0$, $i = 1, \ldots, n$. Then $\det |A| = 0 \pmod{2}$.

Proof. There is
\[
\det |A| = \bigoplus_S a_{1k_1} \cdots a_{nk_n} \text{ where } S = \{(k_1, \ldots, k_n) \mid \{k_1, \ldots, k_n\} = \{1, 2, \ldots, n\}\}.
\]
Let
\[ S_1 = \{(k_1, \ldots, k_n) | \{(1, k_1), \ldots, (n, k_n)\} = \{(k_1, 1), \ldots, (k_n, n)\}, (k_1, \ldots, k_n) \in S\} \]
\[ S_2 = \{(k_1, \ldots, k_n) | \{(1, k_1), \ldots, (n, k_n)\} \neq \{(k_1, 1), \ldots, (k_n, n)\}, (k_1, \ldots, k_n) \in S\} \]
and \( S = S_1 \cup S_2, S_1 \cap S_2 = \emptyset \) (the empty set).

If \((k_1, \ldots, k_n) \in S_1\), set \( E = \{ r | r \neq k_r, 1 \leq r \leq n \}\). For any \( r, 1 \leq r \leq n \), there exists \( r', 1 \leq r' \leq n \), such that
\[
(r, k_r) = (k_{r'}, r'),
\tag{8.65}
\]
If \( r \in E \), then \( r \neq k_r \). From (8.65),
\[
r = k_{r'} \neq k_r = r'.
\]
So \( r' \in E \). In this case, the number of elements in set \( E \) is even. Because \( n \) is odd, there exists at least one number, say \( t, 1 \leq t \leq n, t \notin E \), such that \( t = k_t \) and \( a_{tk_t} = 0 \), so the term \( a_{1k_1} \cdots a_{nk_n} = 0 \).

If \((k_1, \ldots, k_n) \in S_2\), define permutations such that \( k_r = p(r), 1 \leq r \leq n \). So
\[
\{(k_1, 1), \ldots, (n, n)\} = \{(1, p^{-1}(1)), \ldots, (n, p^{-1}(n))\}.\]
Since \( A \) is a symmetric matrix, \( a_{ij} = a_{ji}, 1 \leq i, j \leq n \). Then
\[
a_{1k_1} \cdots a_{nk_n} = a_{k_11} \cdots a_{k_n n} = a_{1p^{-1}(1)} \cdots a_{np^{-1}(n)}
\]
and
\[
a_{1k_1} \cdots a_{nk_n} \oplus a_{1p^{-1}(1)} \cdots a_{np^{-1}(n)} = 0. \tag{8.66}
\]
From (8.65) and (8.66), \( \det | A | = 0 \) (mod 2) is true. This completes the proof. \( \square \)

**Lemma 8.11** Let \( F(z) = f(x) \oplus g(y) \), where \( z = (x, y) \) and \( x = (x_1, \ldots, x_n) \in V_n \), \( y = (y_1, \ldots, y_m) \in V_m \), \( m \) is odd. If \( \deg(g(y)) < 3 \), then \( F(z) \) has a linear structure.

**Proof.** If \( \deg(g(y)) < 3 \), it has the following form:
\[
g(y) = \bigoplus_{1 \leq i < j \leq m} a_{ij} y_i y_j \oplus \bigoplus_{i \leq k \leq m} b_k y_k \oplus c,
\]
where \( a_{ij}, b_k \in GF(2) \). Set a \( m \times m \) matrix:
\[
Q = (q_{ij})_{1 \leq i, j \leq m}, \quad \text{where } q_{ij} = \begin{cases} a_{ji}, & \text{if } i > j \\ 0, & \text{otherwise} \end{cases}
\]
Then \( g(y) = yQy^T \oplus (b, y) \oplus c \), where \( b = (b_1, \ldots, b_m) \). Let \( \alpha = (\alpha_1, \ldots, \alpha_m) \) and
\[
g(y \oplus \alpha) \oplus g(y) = \alpha Q y^T \oplus y Q \alpha^T \oplus b \alpha^T \oplus \alpha Q \alpha^T,
\]
Now \( Q \oplus Q^T \) is a symmetric \( m \times m \) matrix with all zero diagonal. Since \( m \) is odd, from lemma 8.10 that \( Q \oplus Q^T \) is singular. There exists an \( \alpha \neq 0 \in V_m \) satisfying \( \alpha (Q \oplus Q^T) = 0 \in V_m \). Consequently, for this \( \alpha \), \( g(y \oplus \alpha) \oplus g(y) = b \alpha \oplus \alpha Q \alpha^T \) is constant. So \( \alpha \) is a linear structure of \( g(y) \).

All affine sequences on \( V_n \) have Hamming weight either \( 2^{n-1} \), \( 2^n \) or 0 only. According to the definition of non-linearity, it is easy to verify that if a Boolean function, \( f(x) \), on \( V_n \) has Hamming weight less than or equal to \( 2^{n-2} \), then its non-linearity equals its Hamming weight (i.e. \( N_f = W(f) \) if \( W(f) \leq 2^{n-2} \)).

**Theorem 8.11** If \( f(x) \) is a Boolean function on \( V_3 \) and \( N_f = 2 \), then \( f(x) \) has a linear structure.

**Proof.** Since \( N_f = 2 \), there exists an affine function \( \varphi(x) \) that
\[
d(f, \varphi) = W(f(x) \oplus \varphi(x)) = 2. \tag{8.67}
\]
Suppose \( \alpha = (\alpha_0, \ldots, \alpha_7) \) and \( \beta = (\beta_0, \ldots, \beta_7) \) are truth tables of \( f(x) \) and \( \varphi(x) \), let \( r, s \) be the numbers of ones in \( \alpha \) and \( \beta \). Set \( E = \{i | \alpha_i = 1 = \beta_i, 0 \leq i \leq 7\} \) and denote \( |E| = t \). From (8.67) there is
\[
(r - t) + (s - t) = r + s - 2t = 2. \tag{8.68}
\]
Any affine function contains even number of ones. \( r \) is even too.

Now, every Boolean function can be expressed as:
\[
f(x) = (\alpha_0, \ldots, \alpha_7)B(1, x_1, x_2, x_1x_2, x_3, x_1x_3, x_2x_3, x_1x_2x_3)^T, \tag{8.69}
\]
where
\[
B = \begin{pmatrix} A & A \\ 0 & A \end{pmatrix} \quad \text{and} \quad A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{8.70}
\]
From (8.69) and (8.70) there is
\[
f(x) = c_0 \oplus c_1x_1 \oplus c_2x_2 \oplus c_3x_3 \oplus c_4x_1x_2 \oplus c_5x_1x_3 \oplus c_6x_2x_3 \oplus c_7x_1x_2x_3 \tag{8.71}
\]
where $c_0 = \alpha_0$, $c_1 = \alpha_0 \oplus \alpha_1$, \ldots, $c_7 = \alpha_0 \oplus \cdots \oplus \alpha_7$. Since $r$ is even, $c_7 = 0$, therefore $\deg(f(x)) < 3$. From lemma 8.11 the conclusion of this theorem is obtained. \qed

**Corollary 8.3** Let $f(x)$ be a Boolean function on $V_{2n+1}$. If $N_f > 2^{2n} - 2^n$, then $n > 1$.

**Lemma 8.12** Let $f(x)$ be a function on $V_n$, and

$$g(y) = g(x_1, \ldots, x_n, x_{n+1}, x_{n+2}) = f(x) \oplus x_{n+1}x_{n+2}.$$  

If $f(x)$ is a bent function on $V_n$, $g(y)$ is a bent function on $V_{2n+2}$. If $N_f \geq 2^{n-1} - 2^{\frac{n-1}{2}}$, $n$ odd, $N_g \geq 2^{n+1} - 2^{\frac{n+1}{2}}$.

**Corollary 8.4** The function

$$f(x) = \bigoplus_{1 \leq i < j \leq n} x_ix_j$$

is bent when $n$ is even, and it has high non-linearity, $N_f = 2^{n-1} - 2^{\frac{n-1}{2}}$, when $n$ is odd.

Suppose $n \geq 3$. The function can also be written as

$$f(x) = x_1(x_2 \oplus \cdots \oplus x_n) \oplus x_2(x_3 \oplus \cdots \oplus x_n) \oplus x_{n-1}(x_{n-1} \oplus x_n) \oplus x_{n-1}x_n$$

$$= x_1(x_2 \oplus \cdots \oplus y_{n-1}) \oplus x_2(x_3 \oplus \cdots \oplus y_{n-1}) \oplus x_{n-2}y_{n-1} \oplus y_{n-1}x_n \oplus x_n$$

$$= x_1(x_2 \oplus \cdots \oplus y_{n-1}) \oplus x_2(x_3 \oplus \cdots \oplus y_{n-1}) \oplus y_{n-1}(x_{n-2} \oplus x_n) \oplus x_n,$$

where $y_{n-1} = x_{n-1} \oplus x_n$. One can see that the restriction of the above function to the subspace $V_{n-1}$ is bent. Thus

$$N_f = 2^{n-1} - 2^{\frac{n-1}{2}}$$

as required.

### 8.5.1 Homogeneous Boolean functions with high nonlinearity

In this section the existence of cubic homogeneous Boolean functions with high nonlinearity $\geq 2^{2n} - 2^n$ on $V_{2n+1}$ is investigated.

Let $A_1, \ldots, A_n$ be $n \times n$ matrices and $\alpha_1, \ldots, \alpha_n \in V_1$. The matrices $A_1, \ldots, A_n$ are called linearly dependent if there exists a sequence $(\alpha_1, \ldots, \alpha_n) \neq 0$ such that

$$\bigoplus_{i=1}^{n} \alpha_i A_i = 0$$

Otherwise the matrices are called linearly independent.
Let \( \alpha = (a_1, \ldots, a_n) \). Then the derivative of a degree-3 homogeneous function \( f(x) \) on \( V_n \) is as follows:

\[
f(x) \oplus f(x \oplus \alpha) = \bigoplus_{i=1}^{n} (a_i X A_i X^T \oplus \alpha A_i \alpha^T x_i) \oplus f(\alpha)
\]

(8.72)

where \( X = (x_1, x_2, \ldots, x_n) \) and \( A_1, A_2, \ldots, A_n \) are \( n \times n \) matrices uniquely determined by the function.

**Lemma 8.13** Let the matrices \( A_1, A_2, \ldots, A_n \) characterise the derivative of a homogeneous function \( f : V_n \rightarrow GF(2) \) of degree 3. If the matrices \( A_1, A_2, \ldots, A_n \) are linearly independent, then the function \( f(x) \) has no linear structure.

**Proof.** Suppose \( f \) has a linear structure \( \alpha \). \( \delta_f(\alpha) = f(x) \oplus f(x \oplus \alpha) \) is constant, then \( \alpha A_i \alpha^T = 0, i = 1, \ldots, n \). In this case \( X(\bigoplus_{i=1}^{n} a_i A_i)X^T = 0 \) for any \( X \in V_n \). So \( \bigoplus_{i=1}^{n} a_i A_i = 0 \). This is contradict with the condition that \( A_1, \ldots, A_n \) are linear independent. This complete the proof. \( \square \)

**Lemma 8.14** Given a homogeneous function \( f : V_n \rightarrow GF(2) \) of degree 3 with its derivate determined by the sequence of matrices \( A_1, A_2, \ldots, A_n \). If

1. the matrices \( A_1, A_2, \ldots, A_n \) are linearly dependent, i.e. there exists a vector \( \alpha = (c_1, c_2, \ldots, c_n) \neq 0 \) such that

\[
c_1 A_1 \oplus \cdots \oplus c_{k-1} A_{k-1} \oplus c_{k+1} A_{k+1} \oplus \cdots \oplus c_n A_n = c_k A_k \quad 1 \leq k \leq n,
\]

2. and there exists at least one \( A_i \) such that \( \alpha A_i \alpha^T \neq 0 \),

then the function satisfies the propagation criterion with respect to the vector \( (c_1, c_2, \ldots, c_n) \).

**Proof.** Consider Formula (8.72). If the function satisfies the first condition, the quadratic terms disappear. The second condition prevents the function from being a constant affine function. Therefore the function \( f(x) \) satisfies the propagation criterion with respect to the vector \( (c_1, c_2, \ldots, c_n) \). \( \square \)

The number of non-zero entries of \( A_i \) is the number of the occurrences of the variable \( x_i \). In other words, the function has a linear structure \( \alpha = (c_1, \ldots, c_n) \). If the two following conditions are satisfied:

1. \( \bigoplus_{i=1}^{n} c_i A_i = 0 \),
2. for all \( 1 \leq i \leq n \), \( \alpha A_i \alpha^T = 0 \).
Lemma 8.15 Let \( f(x) \) be a cubic function on \( V_{2n+1} \) with no linear structure. If \( r_3(f(x)) \leq n \), then \( r_2(f(x)) > 0 \).

Proof. (By contradiction) Suppose \( r_2(f(x)) = 0 \). Then

\[
F(x) = f(x_1, \ldots, x_r) \oplus x_{r+1} \varphi_{r+1} \oplus x_{2n+1} \varphi_{2n+1},
\]

where \( r = r_3(F(x)) \leq n \) and \( \varphi_i = \varphi_i(x_1, \ldots, x_r), i = r+1, \ldots, 2n+1 \), which are linear functions on \( V_r \). Since \( r \leq n \), there exist \( c_{r+1}, \ldots, c_{2n+1} \in GF(2) \), not all zero, with

\[
c_{r+1} \varphi_{r+1} \oplus \cdots \oplus c_{2n+1} \varphi_{2n+1} = 0.
\]

Without loss of generality, assume \( c_{2n+1} = 1 \). The nonsingular linear transformation

\[
\begin{aligned}
x_i &\rightarrow x_i, & 1 \leq i \leq r \text{ or } i = 2n + 1, \\
x_i &\rightarrow x_i \oplus c_i x_{2n+1}, & r + 1 \leq i \leq 2n,
\end{aligned}
\]

changes \( F(x_1, \ldots, x_{2n+1}) \) into \( G(x_1, \ldots, x_{2n}) \). The vector \((0, \ldots, 0, 1)\) is linear structure of \( G(x_1, \ldots, x_{2n}) \). From Lemma 8.9 we have that \( F(x_1, \ldots, x_{2n+1}) \) has a linear structure. This contradicts the assumption and proves the lemma. \( \square \)

Corollary 8.5 Let \( F(x) \) be a cubic Boolean function on \( V_{2n+1} \) with no linear structure. If \( r_2(F(x)) = 0 \), then \( r_3(F(x)) > n \).

When highly non-linear cubic homogeneous Boolean functions be constructed, only the case \( r_3(f(x)) > n \) and \( r_2(f(x)) = 0 \) be considered.

Set \( E = \{(i, j, k) | 1 < i, j, k < r < n\} \) and \( S = \{(i, j) | 1 < i, j < n\} \). Let

\[
F(x) = \bigoplus_{(i, j, k) \in E} x_i x_j x_k \oplus \bigoplus_{(i, j) \in S} x_i x_j.
\]

There is

\[
F(x) = x^*_1 C x^T(1) \oplus x Q x^T
\]

where

\[
x = (x_1, x_2), \quad x(1) = (x_1, \ldots, x_r), \quad x(2) = (x_{r+1}, \ldots, x_n),
\]

\[
x^*_1 = (x_1 x_2, \ldots, x_1 x_r, \ldots, x_{r-1} x_r),
\]

\[
C^T = B^{(3,r)}_1(f(x)),
\]

\[
f = \bigoplus_{(i, j, k) \in E} x_i x_j x_k,
\]

\[
Q = (q_{ij})_{1 \leq i, j \leq n},
\]

\[
q_{ij} = \begin{cases} 
1, & \text{if } (i, j) \in S \text{ and } i > j, \\
0, & \text{otherwise}
\end{cases}
\]

(8.76)
Theorem 8.12 Let \( F(x) = f(x) \oplus g(x) \) where

\[
\begin{align*}
  f(x) &= \bigoplus_{(i,j,k) \in E} x_i x_j x_k, \quad r = r_3(f(x)), \quad 1 \leq i, j, k \leq r \leq n, \\
  g(x) &= \bigoplus_{(i,j) \in S} x_i x_j, \quad 1 \leq j \leq r, \quad j < i \leq n.
\end{align*}
\]

(8.77)

\( F(x) \) is equivalent (\( \cong \)) to a cubic homogeneous Boolean function iff there exists a non-singular \( n \times n \) matrix \( T \) and a constant vector \( \alpha = (\alpha_1, \cdots, \alpha_n) \) such that:

\[
\left( T(1)^* C \oplus TQ \oplus R \right) T(1)^T = \left( T(1)^* C \oplus TQ \oplus R \right)^T,
\]

(8.78)

where \( C^T = B_{1,2}^{(3,r)}(f(x)) \), \( T = (t_1, \cdots, t_r) \) with \( t_i, 1 \leq i \leq n \), are column vectors of \( n \) coordinates, \( T(1) = (t_1, \cdots, t_r) \), \( T(2) = (t_{r+1}, \cdots, t_n) \), and

\[
Q = (q_{ij}) \\
q_{ij} = \begin{cases} 
1, & (i, j) \in S \text{ and } i > j \\
0, & \text{otherwise}
\end{cases} \quad 1 \leq i \leq n, \quad 1 \leq j \leq r
\]

\[
R = \bigoplus_{(j, k) \in E_1} a_j t_k, \cdots, \bigoplus_{(j, k) \in E_{r-1}} a_j t_k, 0
\]

(8.79)

Proof. Let \( (\alpha, \beta, c) \in G_n \). Then

\[
(\alpha, \beta, c)(F(x)) = F(xT \oplus \alpha) \oplus (\beta, x) \oplus c,
\]

where

\[
\begin{align*}
F(xT \oplus \alpha) &= f(xT \oplus \alpha) \oplus g(xT \oplus \alpha), \\
f(xT \oplus \alpha) &= \bigoplus_{(i,j,k) \in E} (x_i \oplus a_i)(x_j \oplus a_j)(x_k \oplus a_k) \\
&= \bigoplus_{(i,j,k) \in E} \{ x_i x_j x_k \oplus a_k x_i x_j \oplus a_j x_i x_k \oplus a_i x_j x_k \} \oplus \varphi_1(x) \\
&= \bigoplus_{(i,j,k) \in E} x_i x_j x_k \oplus xRT_{(1)}^T x^T \oplus \varphi_1(x) \\
&= H(x) \oplus xT(1)^* C T(1)^T x^T \oplus xRT_{(1)}^T x^T \oplus \varphi(x),
\end{align*}
\]

(8.80)

(8.81)

where \( H \) is a cubic homogeneous function, and \( \varphi_1(x) \) is an affine function.

\[
g(xT \oplus \alpha) = (xT \oplus \alpha)Q(xT(1) \oplus \alpha) = xTQT_{(1)}^T x^T \oplus \varphi_2(x),
\]

where \( \varphi_2(x) \) is an affine function, and \( \alpha(1) = (\alpha_1, \cdots, \alpha_r) \). Now

\[
(\alpha, \beta, c)(F(x)) = H(x) \oplus x(T(1)^* C \oplus TQ \oplus R) T(1)^T x^T \oplus \varphi_3(x),
\]

(8.82)
8.5. Homogeneous Boolean functions with high nonlinearity on $V_{2n+1}$

where $\varphi_3(x)$ is an affine function. $(\alpha, \beta, c)(F(x))$ is a cubic homogeneous function if and only if $x(T_{(1)}^* C \oplus TQ \oplus R)T_{(1)}^T x^T$ is an affine function. From lemma 8.1 that $(T_{(1)}^* C \oplus TQ \oplus R)T_{(1)}^T$ is a symmetric matrix and Equation (8.78) holds. \hfill \square

Note that

$$TQ = (\bigoplus_{1 \leq i \leq n} q_{i_1} t_i, \ldots, \bigoplus_{1 \leq i \leq n} q_{i_r} t_i). \quad (8.83)$$

Since $T$ is a nonsingular $n \times n$ matrix, there exists an $n \times r$ matrix $W = (w_{ij})$ that

$$T_{(1)}^* C = \left(\bigoplus_{(j,k) \in E_1} t_j \ast t_k, \ldots, \bigoplus_{(j,k) \in E_r} t_j \ast t_k\right) = TW = \left(\bigoplus_{1 \leq i \leq n} w_{i_1} t_i, \ldots, \bigoplus_{1 \leq i \leq n} w_{i_r} t_i\right). \quad (8.84)$$

The right hand side of equation (8.83) and (8.84) are likely to be used to check if $T$ satisfies equation (8.78).

**Theorem 8.13** There exist cubic homogeneous function on $V_{2n+1}$ without linear structure and their non-linearity $\geq 2^{2^n} - 2^n$ for $n \geq 2, n \neq 4$.

**Proof.** On $V_5$, let $F(x) = x_1 x_2 x_3 \oplus x_1 x_4 \oplus x_2 x_5$. $F(x)$ has no linear structure, and its non-linearity $N_F = 12$, $r = r_3(F(x)) = 3$. Take $\alpha = 0$ and

$$T = (t_1, t_2, t_3, t_4, t_5) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$ 

Compute

$$T_{(1)}^* C = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = (t_4, t_5, 0),$$

$$TQ = T \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = (t_4, t_5, 0),$$
and (8.78) holds.

On $V_7$, let $f(x) = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_4 \oplus x_2x_5 \oplus x_2x_7 \oplus x_3x_7$. It is easy to check $f(x)$ has no linear structure and $N_f = 56$. $r = r_3(f(x)) = 6$. Take $\alpha = (0, 0, 1, 0, 0, 0, 0)$ and

$$T = (t_1, \cdots, t_7) = \left(\begin{array}{cccccccc}
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 1 & 1 & 1 & 1
\end{array}\right).$$

Then

$$T(t_1, t_7) = \left(\begin{array}{cccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0
\end{array}\right) = (0, t_1 \oplus t_5 \oplus t_7, t_3 \oplus t_7, t_1 \oplus t_6, 0, 0)$$

and

$$TQ = (t_4, t_5 \oplus t_7, t_7, 0, 0, 0), \quad R = (t_2, 0, 0, t_6, 0, 0).$$

Now

$$(T(t_1)C \oplus TQ \oplus R)T_{(1)}^T = (t_2 \oplus t_4)t_1^T \oplus t_1(t_2 \oplus t_4)^T \oplus t_3t_3^T.$$

and it is a symmetric matrix. In this case $F(xT \oplus \alpha) \oplus x(t_3 \oplus t_7)$ is a cubic homogeneous function with $N_F = N_f = 56$ and has no linear structure.

For any $m \geq 3$, $m \neq 4$, from theorem 8.8, that there exist cubic homogeneous bent functions on $V_{2m}$. For any $n > 4$, let $\ell = 2$ or $3$ such that $m = n - \ell \geq 3 \neq 4$, and $F(z) = f(x) \oplus g(y)$ where $f(x)$ is a cubic homogeneous function on $V_{2\ell+1}$ with $N_f \geq 2^{2\ell} - 2^\ell$, and $g(y)$ is a cubic homogeneous bent function on $V_{2(n-\ell)}$, $z = (x, y), x \in V_{2\ell+1}, y \in V_{2(n-\ell)}$. From Theorem 8.10, Corollary 8.2 and Theorem 8.1, homogeneous functions with $N_F \geq 2^n - 2^n$ and have no linear structure are obtained. \(\Box\)

In the following section the transformation matrix solutions for each of the remaining seven inequivalent cases on $V_7$, and results for $V_n$, $n$ odd, $n \geq 11$ are given. The properties of these solutions are discussed.
8.5.2 Cubic homogeneous functions on $V_5$

Let

$$f(x) = x_{i_1}x_{i_2}x_{i_3} \oplus x_{i_1}x_{i_4} \oplus x_{i_2}x_{i_5},$$  \hspace{1cm} (8.85)

where $\{i_1, i_2, i_3, i_4, i_5\} = \{1, 2, 3, 4, 5\}$. Assume the following linear transformation $T$:

$$x_{i_1} \rightarrow x_{i_1} \oplus x_{i_5}, \quad x_{i_2} \rightarrow x_{i_2} \oplus x_{i_4}, \quad x_{i_3} \rightarrow x_{i_3} \oplus x_{i_4} \oplus x_{i_5},$$

$$x_{i_4} \rightarrow x_{i_4}, \quad x_{i_5} \rightarrow x_{i_5}. \hspace{1cm} (8.86)$$

Clearly, matrix $T$ is nonsingular and $f(xT) = \bigoplus_{1 \leq u,v,w \leq 5} x_ux_vx_w \oplus x_{i_1}x_{i_3}x_{i_5} \oplus x_{i_2}x_{i_3}x_{i_4}$ is a cubic homogeneous function with non-linearity $N_f = 12$.

There are 60 different functions of the form (8.85). They are equivalent under permutations of $(1, 2, 3, 4, 5)$. There are 15 different cubic homogeneous Boolean functions (see Appendix A) obtained from the functions of the form (8.85) under the action of $T$ as defined by (8.86). They are equivalent under enumeration of $(1, 2, 3, 4, 5)$.

8.5.3 Cubic homogeneous functions on $V_7$

The author found a lots of cubic homogeneous Boolean functions without linear structures and nonlinearity equal 56 on $V_7$ (see some results in Appendix B).

Case 1: Let

$$f(x) = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1(x_3 \oplus x_7) \oplus x_2(x_6 \oplus x_7) \oplus x_5x_7 \oplus x_6x_7. \hspace{1cm} (8.87)$$

Set $T = (t_1, \cdots, t_7)$ and $TQ = (t_3 \oplus t_7, t_6 \oplus t_7, 0, 0, t_7, t_7)$. Take $\alpha = (0, 1, 0, 0, 1, 1, 0)$, then $R = (t_3, t_4, t_5, 0, 0)$. Let

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

Now

$$\left( T_{(1)}^T C \oplus TQ \oplus R \right) T_{(1)}^T$$

$$= \left( 0, t_5, t_4 \oplus t_6, t_3 \oplus t_4 \oplus t_5 \oplus t_6, t_2 \oplus t_4 \oplus t_5 \oplus t_6, t_3 \oplus t_4 \oplus t_5 \oplus t_6 \right) T_{(1)}^T$$

$$= \left( t_5t_2^T \oplus t_2t_5^T \right) \oplus \left( t_4 \oplus t_6 \right) t_3^T \oplus \left( t_4 \oplus t_6 \right)^T \oplus \left( t_4 \oplus t_5 \oplus t_6 \right) \left( t_4 \oplus t_5 \oplus t_6 \right)^T,$$
is a symmetric matrix. In this case \( f(x\oplus \alpha) \oplus x(t_2 \oplus t_5 \oplus t_7) \oplus 1 \) is a cubic homogeneous Boolean function with \( N_f = 56 \).

**Case 2:** Let

\[
\begin{align*}
f(x) = x_1x_2x_3 &\oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_5x_6 \oplus x_1x_3 \\
&\oplus x_1x_5 \oplus x_2x_4 \oplus x_2x_5 \oplus x_2x_7 \oplus x_6x_7.
\end{align*}
\]

Take \( \alpha = 0 \) and

\[
T = \begin{pmatrix}
1 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1
\end{pmatrix}.
\]

One can get

\[
(T_{(1)}C \oplus TQ \oplus R) T_{(1)}^T = (t_1 \oplus t_6, 0, 0, 0, t_6, t_1 \oplus t_5) T_{(1)}^T \\
= t_1t_1^T \oplus t_6 (t_1 \oplus t_5) T^T \oplus (t_1 \oplus t_5) t_6^T,
\]

and it is a symmetric matrix. Thus \( f(x^T) \oplus xt_1 \) is a homogeneous function as desired.

**Case 3:** Let

\[
\begin{align*}
f(x) = x_1x_2x_3 &\oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_5x_6 \\
&\oplus x_1x_5 \oplus x_1x_7 \oplus x_2x_6 \oplus x_3x_7 \oplus x_4x_5.
\end{align*}
\]

Take \( \alpha = 0 \) and

\[
T = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 & 0
\end{pmatrix}.
\]
Then
\[
\begin{aligned}
(T_{(1)}^* C \oplus TQ \oplus R) T_{(1)}^T &= (0, 0, 0, t_6, t_6, t_4 \oplus t_5) T_{(1)}^* \\
&= t_6 (t_4 \oplus t_5)^T \oplus (t_4 \oplus t_5) t_6^T,
\end{aligned}
\]
is a symmetric matrix. Thus \(f(xT)\) is a homogeneous functions as desired.

**Case 4:** Let
\[
\begin{aligned}
f(x) &= x_1 x_2 x_3 \oplus x_2 x_4 x_5 \oplus x_3 x_4 x_6 \oplus x_1 x_5 x_6 \oplus x_1 x_3 \oplus x_1 x_4 \oplus \\
x_2 x_3 \oplus x_2 x_4 \oplus x_2 x_7 \oplus x_5 x_7.
\end{aligned}
\]
Take \(\alpha = (0, 0, 0, 1, 0, 1, 0)\) and
\[
T = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 0
\end{pmatrix}.
\]
Then
\[
\begin{aligned}
(T_{(1)}^* C \oplus TQ \oplus R) T_{(1)}^T &= (0, 0, t_3, t_6, 0, t_4) \\
&= t_3 t_3^T \oplus t_6 t_4^T \oplus t_4 t_6^T,
\end{aligned}
\]
is a symmetric matrix. Thus \(f(xT \oplus \alpha) \oplus x(t_1 \oplus t_2)\) is an homogeneous function as desired.

**Case 5:** Let
\[
\begin{aligned}
f(x) &= x_1 x_2 x_3 \oplus x_2 x_4 x_5 \oplus x_3 x_4 x_6 \oplus x_1 x_5 x_6 \oplus x_1 x_2 \oplus x_1 x_6 \oplus \\
x_1 x_7 \oplus x_2 x_7 \oplus x_3 x_5 \oplus x_4 x_7 \oplus x_6 x_7.
\end{aligned}
\]
Take \(\alpha = (0, 1, 0, 0, 1, 0, 0)\) and
\[
T = \begin{pmatrix}
1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 1 & 0
\end{pmatrix}.
\]
Then

\[
\left( T^*_l C \oplus TQ \oplus R \right)^T T^{(1)}_l = (t_1 \oplus t_2 \oplus t_3 \oplus t_4 \oplus t_5 \oplus t_6, t_1 \oplus t_3 \oplus t_4 \oplus t_5 \oplus t_6, t_1 \oplus t_2 \oplus t_3 \oplus t_4 \oplus t_6, t_1 \oplus t_2 \oplus t_3 \oplus t_4 \oplus t_5 \oplus t_6, t_1 \oplus t_2 \oplus t_3 \oplus t_4 \oplus t_5 \oplus t_6) T^{(1)}^T
\]

\[
= t_1 t_1^T \oplus (t_2 \oplus t_3 \oplus t_4 \oplus t_5 \oplus t_6) t_1^T \oplus t_1 (t_2 \oplus t_3 \oplus t_4 \oplus t_5 \oplus t_6) T \oplus t_3 t_3^T \oplus t_4 t_4^T \oplus (t_2 \oplus t_3 \oplus t_5 \oplus t_6) (t_3 \oplus t_4) T \oplus (t_3 \oplus t_4) (t_2 \oplus t_5 \oplus t_6) T \oplus (t_2 \oplus t_6) T^T \oplus (t_5 \oplus t_6) (t_2 \oplus t_6) T^T,
\]

is a symmetric matrix. Thus \( f(xT \oplus \alpha) \oplus x(t_1 \oplus t_3 \oplus t_4) \) is a cubic homogeneous function as desired.

**Case 6:** Let

\[
f(x) = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_5x_6 \oplus \\
x_1x_2 \oplus x_1x_7 \oplus x_2x_5 \oplus x_3x_5 \oplus x_4x_7 \oplus x_5x_6.
\]

Take \( \alpha = 0 \) and

\[
T = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 0 \\
1 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 \\
\end{pmatrix}.
\]

Then

\[
\left( T^*_l C \oplus TQ \oplus R \right)^T T^{(1)}_l = (0, t_3, t_2, t_6, t_5, t_4) T^{(1)}^T
\]

\[
= t_2 t_2^T \oplus t_3 t_3^T \oplus t_6 t_6^T \oplus t_5 t_5^T \oplus t_4 t_4^T \oplus t_5 t_5^T,
\]

is a symmetric matrix. So \( f(xT) \oplus xt_5 \) is a cubic homogeneous function as desired.

**Case 7:** Let

\[
f(x) = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_4x_7 \oplus x_2x_6x_7 \oplus \\
x_1x_5 \oplus x_1x_6 \oplus x_2x_3 \oplus x_3x_7 \oplus x_5x_6.
\]
Take $\alpha = (0, 0, 0, 1, 0, 0, 1)$ and

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

Then

$$(T^*C \oplus TQ \oplus R)T^T = (0, t_3, t_2, t_5 \oplus t_6, t_4 \oplus t_6, t_4 \oplus t_5 \oplus t_6 \oplus t_7, t_6)T^T$$

$$= t_2t_3^T \oplus t_3t_2^T \oplus t_4(t_5 \oplus t_6)^T \oplus (t_5 \oplus t_6)t_4^T \oplus t_5t_6^T \oplus t_6t_5^T \oplus t_6t_7^T \oplus t_7t_6^T,$$

is a symmetric matrix. So $f(xT \oplus \alpha) \oplus x(t_1 \oplus t_3 \oplus t_6)$ is a cubic homogeneous function as desired.

Including the Boolean function on $V_7$ which given in theorem (8.4), there are 8 cubic functions of 7 variables. Every one of them is equivalent to a cubic homogeneous function under the action of $G_7$. But they are not equivalent to each other. There is no generalized construction of the matrix $T$ and the vector $\alpha$ so that $f(xT \oplus \alpha) = H(x) \oplus \varphi(x)$ where $H(x)$ is cubic homogeneous function, and $\varphi(x)$ is an affine function. The search is carried on. The cases just given are positive evidence for such a construction.

8.5.4 On $V_{2n+1}$, $n > 4$

The cubic homogeneous Boolean functions, $f(x)$ on $V_5$ with high non-linearity $N_f = 12$ exist, and cubic homogeneous bent functions, $g(y)$ on $V_6$ are found. From theorem 8.10 and corollary 8.2 one can construct a cubic homogeneous Boolean function $F(z) = f(x) \oplus g(y)$ on $V_{11}$ with high non-linearity $N_F = 2^{10} - 2^5 = 992$.

Example 8.1 Let

$$f(x) = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_3x_4$$

$$\oplus x_1x_3x_5 \oplus x_2x_3x_4 \oplus x_2x_4x_5 \oplus x_3x_4x_5,$$
and
\[ g(y) = y_1 y_2 y_3 \oplus y_1 y_2 y_4 \oplus y_1 y_2 y_5 \oplus y_1 y_3 y_4 \oplus y_1 y_3 y_6 \]
\[ \oplus y_1 y_4 y_5 \oplus y_1 y_4 y_6 \oplus y_1 y_5 y_6 \oplus y_2 y_3 y_5 \oplus y_2 y_3 y_6 \]
\[ \oplus y_2 y_4 y_5 \oplus y_2 y_4 y_6 \oplus y_2 y_5 y_6 \oplus y_3 y_4 y_5 \oplus y_3 y_4 y_6 \oplus y_3 y_5 y_6, \]

then \( F(z) = f(x) \oplus g(y) \) is a cubic homogeneous Boolean function and \( N_F = 992. \)

Using this method, one can construct cubic homogeneous Boolean functions \( F \) on \( V_{2n+1} \) for \( n > 4 \) with high non-linearity \( N_F \geq 2^{2n} - 2^n. \)

### 8.5.5 Properties of matrix transformation

Now consider the transformation matrix properties.

**Lemma 8.16** Let \( T \) be an \( n \times r \) matrix and \( P \) be an \( n \times n \) permutation matrix. Then \( (PT)^* = PT^* \)

**Proof.** Set \( p = (p_{ij}) \), \( T = (t_{ij}) = (t_1, \cdots, t_r) \). Let \( PT = (s_{ij}) = (s_1, \cdots, s_n) \). The conclusion of lemma 8.16 will be easily followed. \( \square \)

**Lemma 8.17** If \( T \) satisfies (8.78) for some cubic functions \( f(x) \), and \( P \) is a permutation. Then \( PT \) satisfies (8.78), too.

**Proof.** Let \( T = (T_1, T_2) \), \( PT = (S_1, S_2) \), where \( T_1 \), \( S_1 \) are \( n \times r \) matrices, \( S_1 = PT_1 \), \( S_2 = PT_2 \). From lemma 8.16 that \( S_1^* = PT_1^* \), and
\[
\bar{R} = \left( \bigoplus_{(j,k) \in E_1} a_j s_k, \cdots, \bigoplus_{(j,k) \in E_r} a_j s_k, 0 \right)
\]
\[
= P \left( \bigoplus_{(j,k) \in E_1} a_j t_k, \cdots, \bigoplus_{(j,k) \in E_r} a_j t_k, 0 \right) = PR,
\]

therefore
\[
(S_1^* C \oplus SQ \oplus \bar{R}) S_1 = P \left( T_1^* C \oplus TQ \oplus \bar{R} \right) T_1^T P^T.
\]

The lemma is proved. \( \square \)
Chapter 9

A Family of $C$-Partitions and $T$-Matrices

This chapter is based on the paper by M. Xia and T. Xia [161]. 40 percent of the results are due to the second author. In this chapter the author gives the definition of $C$-partitions in an abelian group, considers the relation between $C$-partitions, supplementary difference sets and $T$-matrices, and for an abelian group of order $v = q^2$ with $q \equiv 3 (mod 8)$ a prime power, obtains some new constructions for $C$-partitions, $T$-matrices and Hadamard matrices.

9.1 Introduction

It is well known that the $T$-matrices play an important role in the construction of Hadamard matrices. In 1974, R. J. Turyn [146] gave an infinite class of $T$-matrices of order $t = 2^i \cdot 10^j \cdot 26^k + 1$ for $i, j, k \geq 0$. Naturally, one asks if there exist four $T$-matrices of order $t$ for any integer $t \geq 1$? So far there is no essential progress on this problem (see [7], [20], [22], [54], [105], [117], [146], [152]).

In 1984, M.Y. Xia in [152] has proposed the concept of $C$-partitions in an abelian group, and discussed the relationship between the $C$-partitions, supplementary difference sets and $T$-matrices. The purpose was to generalize the concept of $T$-matrices without the circulant restriction. But he did not obtain a systematic result. Now using a result adapted from [159], there exist $C$-partitions in the abelian group of order $q^2$ for every $q \equiv 3 (mod 8)$ a prime power. An infinite class of $T$-matrices and new Hadamard matrices are obtained.

In Section 9.2 the notation and definitions are given. In section 9.3 some necessary preliminaries are showed and the tight relationship between $C$-partitions, SDS and $T$-matrices is discussed. In section 9.4 special SDS are constructed from which $C$-partitions will flow. Consequently a family of $T$-matrices and Hadamard matrices are obtained.
9.2 The definitions

If \( A_1, \ldots, A_8 \) are \( C \)-partitions (see definition 4.7), let \( B_1, \ldots, B_8 \) be obtained from \( A_1, \ldots, A_8 \) by one of the following transformations:

(a) for any fixed \( i, 1 \leq i \leq 4 \), \( B_i = A_{i+4}, B_{i+4} = A_i \), and \( B_j = A_j, B_{j+4} = A_{j+4} \) for \( j \neq i, 1 \leq j \leq 4 \);

(b) for any pair \( (i, j), i \neq j, 1 \leq i, j \leq 4 \), \( B_i = A_j, B_{i+4} = A_{j+4}, B_j = A_i, B_{j+4} = A_{i+4} \), and \( B_k = A_k, B_{k+4} = A_{k+4}, k \neq i, j, 1 \leq k \leq 4 \);

then from definition 4.7 \( B_1, \ldots, B_8 \) are \( C \)-partitions too.

If \( A_1, \ldots, A_8 \) are \( C \)-partitions, by counting the number of terms in the two sides of (iii), it follows that

\[
\sum_{i=1}^{4} (| A_i | - | A_{i+4} |)^2 = v
\]

9.3 The Relationship

This section shows how one can construct \( T \)-matrices from \( C \)-partitions and that \( C \)-partitions are equivalent to supplementary difference sets of some special kind.

**Theorem 9.1** (see [152]) Suppose \( G \) is an abelian group of order \( v \). Then there exist \( C \)-partitions in \( G \) if and only if there are SDS of type \( H \) such that every element of \( G \) appears an even number of times in the system of \( D_1, D_2, D_3, D_4 \).

**Proof.** Suppose \( A_1, \ldots, A_8 \) are \( C \)-partitions, that is, \( A_i \cap A_j = \emptyset \) for \( i \neq j \), \( G = \cup_{i=1}^{8} A_i \) and \( \sum_{i=1}^{8} \Delta A_i = v \theta + \sum_{i=1}^{4} \Delta (A_i, A_{i+4}) \), put

\[
D_1 = A_1 \cup A_2 \cup A_3 \cup A_4, \quad D_2 = A_1 \cup A_2 \cup A_7 \cup A_8
\]
\[
D_3 = A_1 \cup A_3 \cup A_6 \cup A_8, \quad D_4 = A_1 \cup A_4 \cup A_6 \cup A_7
\]

Then

\[
\sum_{i=1}^{4} \Delta D_i = 4 \Delta A_1 + 2 \sum_{i=2}^{8} \Delta A_i - 2 \Delta A_5 + 2 \Delta (A_1, A_2 \cup A_3 \cup A_4 \cup A_6 \cup A_7 \cup A_8) + \Delta (A_2 \cup A_6, A_3 \cup A_4 \cup A_7 \cup A_8) + \Delta (A_3 \cup A_7, A_4 \cup A_8)
\]
\[
= \Delta (A_1, G) - \Delta (A_5, G) + \sum_{i=1}^{8} \Delta A_i - \sum_{i=1}^{4} \Delta (A_i, A_{i+4}) + \Delta G
\]
\[
= v \theta + [2(| A_1 | - | A_5 |)] + v|T|.
\]
9.3. The Relationship

Moreover,

\[ \sum_{i=1}^{4} |D_i| |v| = 2(\sum_{i=1}^{4} |A_i| - |A_5|) + 2 \sum_{i=1}^{8} |A_i| |v| = 2(\sum_{i=1}^{4} |A_i| - |A_5|) + v \]

so, \(D_1, D_2, D_3, D_4\) are SDS of type \(H\).

Obviously, every element of \(G\) arises an even number of times (0 or 2 or 4) in the system of \(D_1, D_2, D_3, D_4\). So \(D_1, D_2, D_3, D_4\) are desired SDS.

Conversely, let \(D_1, D_2, D_3, D_4\) be \(4 - \{v; \sum_{i=1}^{4} |D_i| \mid D_1 \mid, \mid D_2 \mid, \mid D_3 \mid, \mid D_4 \mid, \sum_{i=1}^{8} |A_i| - |A_5| \mid -v\} \) SDS and every element of \(G\) occurs an even number of times in the system of \(D_1, D_2, D_3, D_4\). Put

\[ A_1 = \cap_{i=1}^{4} D_i, \quad A_2 = (D_1 \cap D_2) \setminus A_1, \quad A_3 = (D_1 \cap D_3) \setminus A_1, \quad A_4 = (D_1 \cap D_4) \setminus A_1, \]
\[ A_5 = \cap_{i=1}^{4} \bar{D}_i, \quad A_6 = (D_3 \cap D_4) \setminus A_1, \quad A_7 = (D_2 \cap D_4) \setminus A_1, \quad A_8 = (D_2 \cap D_3) \setminus A_1. \]

For any element \(g\) of \(G\) occurring \(\lambda\) times in the system of \(D_1, D_2, D_3, D_4\), from the hypothesis that \(\lambda\) should be equal to 0 or 2 or 4. If \(\lambda = 0, g \in A_5\), if \(\lambda = 4, g \in A_1\), if \(\lambda = 2, g \in \cup_{i=2}^{4} (A_i \cup A_{i+4})\). So \(\cup_{i=1}^{8} A_i = G\) and \(A_1 \cap A_5 = \phi, (A_1 \cup A_5) \cap (\cup_{i=2}^{4} (A_i \cup A_{i+4})) = \phi\). Moreover, \(A_i \cap A_{i+4} = \phi, i = 2, 3, 4\) and for \(i \neq j, 2 \leq i, j \leq 4, A_i \cap A_j = D_1 \cap D_i \cap D_j \cap \bar{D}_k = \phi, A_i \cap A_{j+4} = D_1 \cap D_i \cap \bar{D}_j \cap D_k = \phi, A_{i+4} \cap A_j = D_1 \cap D_i \cap \bar{D}_j \cap D_k = \phi\), where \(k \neq i, j\).

Obviously,

\[ D_1 = A_1 \cup A_2 \cup A_3 \cup A_4, \quad D_2 = A_1 \cup A_2 \cup A_7 \cup A_8, \]
\[ D_3 = A_1 \cup A_3 \cup A_6 \cup A_8, \quad D_4 = A_1 \cup A_4 \cup A_6 \cup A_7. \]

From

\[ v\theta + \left( \sum_{i=1}^{4} |D_i| |v| \right) T = \sum_{i=1}^{4} \Delta D_i \]
\[ = \Delta(A_1, G) + \sum_{i=1}^{8} \Delta A_i - \sum_{i=1}^{4} \Delta(A_i, A_{i+4}) \]
\[ = (2(\sum_{i=1}^{4} |A_i| - |A_5|) + v) T + \sum_{i=1}^{8} \Delta A_i - \sum_{i=1}^{4} \Delta(A_i, A_{i+4}) \]
\[ = \left( \sum_{i=1}^{4} |D_i| |v| \right) T + \sum_{i=1}^{8} \Delta A_i - \sum_{i=1}^{4} \Delta(A_i, A_{i+4}), \quad (9.1) \]

if follows that

\[ \sum_{i=1}^{8} \Delta A_i = v\theta + \sum_{i=1}^{4} \Delta(A_i, A_{i+4}) \]

This means that \(A_1, \cdots, A_8\) are \(C\)-partitions of \(G\). The proof is completed. \(\square\)
Theorem 9.2 (see [152]) Suppose $G$ is an abelian group of order $v$. Then there exist $C$–partitions in $G$ if and only if there exist SDS of type $H$ such that every element of $G$ arises one or three times in the system of the SDS.

Proof. Suppose $A_1, \ldots, A_8$ are $C$–partitions. Let

$$
D_i^* = A_1 \cup A_6 \cup A_7 \cup A_8, \quad D_i^* = A_2 \cup A_5 \cup A_7 \cup A_8, \\
D_3^* = A_3 \cup A_5 \cup A_6 \cup A_8, \quad D_i^* = A_4 \cup A_5 \cup A_6 \cup A_7.
$$

(9.2)

There is

$$
\sum_{i=1}^{4} \Delta D_i^* = \sum_{i=1}^{4} (\Delta A_i - \Delta (A_i, A_{i+4})) + \Delta (\bigcup_{j=5}^{8} A_j) + \Delta (\bigcup_{j=5,j\neq i+4}^{8} A_j)
$$

$$
= \sum_{i=1}^{4} \Delta A_i - \sum_{i=1}^{4} \Delta (A_i, A_{i+4}) + \Delta (\bigcup_{j=5}^{8} A_j) + \sum_{i=1}^{4} \Delta (\bigcup_{j=5,j\neq i+4}^{8} A_j)
$$

$$
= \sum_{i=1}^{8} \Delta A_i - \sum_{i=5}^{8} \Delta (A_i, A_{i+4}) + \sum_{i=1}^{4} \Delta (\bigcup_{j=1,j\neq i}^{4} A_j)
$$

$$
= v\theta + \lambda T,
$$

where $\lambda = 2 \sum_{i=5}^{8} |A_i| = \sum_{i=1}^{4} |D_i^*| - v$. So $D_1^*, D_2^*, D_3^*$ and $D_4^*$ are SDS of type $H$. Clearly, every element of $G$ occurs one or three times in the system of the SDS.

Conversely, let $D_1^*, D_2^*, D_3^*$ and $D_4^*$ be

$$
4 - \{v; |D_1^*|, |D_2^*|, |D_3^*|, |D_4^*|; \sum_{i=1}^{4} |D_i^*| - v\} \text{ SDS and every element of } G \text{ arises one or three times in the system of the SDS.}
$$

It follows that $\bigcup_{i=1}^{4} D_i^* = G$, $\bigcap_{i=1}^{4} D_i^* = \phi$. Put

$$
A_i = \bigcap_{j=1,j\neq i}^{4} D_j^*, \quad A_{i+4} = \bigcap_{j=1,j\neq i}^{4} D_j^*, \quad i = 1, 2, 3, 4.
$$

For any element $g$ of $G$, if $g$ appears one time in the system of $D_1^*, D_2^*, D_3^*$ and $D_4^*$, then $g \in \bigcup_{i=1}^{4} A_i$, if $g$ appears three times in the system of the SDS, then $g \in \bigcup_{i=1}^{4} A_{i+4}$, so $G = \bigcup_{i=1}^{8} A_i$. Now for $i \neq j$, $1 \leq i, j \leq 4$,

$$
A_i \cap A_j = \bigcap_{k=1}^{4} \tilde{D}_k^* = G \\setminus \left( \bigcup_{k=1}^{4} D_k^* \right) = \phi, \quad A_{i+4} \cap A_{j+4} = \bigcap_{k=1}^{4} D_k^* = \phi,
$$

and

$$
A_i \cap A_{j+4} \subset \tilde{D}_k^* D_k^* = \phi, \quad 1 \leq k \leq 4, \quad k \neq i, j.
$$

Finally, it is easy to know that (9.2) holds and

$$
v\theta + \left( \sum_{i=1}^{4} |D_i^*| - v \right) T = \sum_{i=1}^{4} \Delta D_i^*
$$

$$
= \sum_{i=1}^{8} \Delta A_i - \sum_{i=5}^{8} \Delta (A_i, A_{i+4}) + 2\left( \sum_{i=5}^{8} |A_i| \right) T,
$$

where $\Delta D_i^*$ is the difference in the number of times an element appears in the $D_i^*$ and $\Delta (A_i, A_{i+4})$ is the difference in the number of times an element appears in $A_i$ and $A_{i+4}$.
9.3. The Relationship

consequently,

$$\sum_{i=1}^{8} \Delta A_i - \sum_{i=1}^{4} \Delta (A_i, A_{i+4}) = v\theta. \quad (9.3)$$

The proof is completed. □

**Theorem 9.3** (see [152]) Suppose $G$ is an abelian group of order $v$. If there exist $C$-partitions in $G$, there are $T$-matrices of order $v$.

**Proof.** Let $A_1, \ldots, A_8$ be $C$-partitions in $G$. Put the elements of $G$ in any order: $g_1, \ldots, g_v$. Set

$$T_i = (t_{jk}^{(i)})_{1 \leq j, k \leq v}, \quad t_{jk}^{(i)} = \begin{cases} 
1, & \text{if } g_k \otimes g_j \in A_i, \\
-1, & \text{if } g_k \otimes g_j \in A_{i+4}, \quad 1 \leq i \leq 4, \\
0, & \text{otherwise,}
\end{cases}$$

From the definition of $T_i$, $1 \leq i \leq 4$, it is easy to know that $T_iT_j = T_jT_i$, $i \neq j$, $1 \leq i, j \leq 4$. Because $A_i \cap A_j = \phi$ when $i \neq j$ and $\bigcup_{i=1}^{8} A_i = G$, then $\sum_{i=1}^{4} | t_{jk}^{(i)} | = 1$, $1 \leq j, k \leq v$. From (9.3) it follows that $\sum_{i=1}^{4} T_iT_i^T = vI$. Conditions (1), (3) and (4) in definition 4.8 are satisfied. Let

$$R = (r_{ij})_{1 \leq i, j \leq v}, \quad r_{ij} = \begin{cases} 
1, & \text{if } g_i \oplus g_j = 0; \\
0, & \text{otherwise.}
\end{cases}$$

$R$ is monomial matrix and $R^T = R$, $R^2 = I$. It is easy to verify that

$$(T_iR)^T = T_iR, i = 1, 2, 3, 4.$$  

Condition (2) in Definition 4.8 is satisfied too. So $T_1$, $T_2$, $T_3$ and $T_4$ are desired $T$-matrices. □

From theorem 9.1 and theorem 9.3, if in an abelian group $G$ of order $v$ there exist $D_1$, $D_2$, $D_3$ and $D_4$ which are SDS of type $H$ and every element of $G$ appears an even number of times in the system of $D_1$, $D_2$, $D_3$ and $D_4$, then there exist $T$-matrices $T_1$, $T_2$, $T_3$ and $T_4$ of order $v$.

Let $D_1$, $D_2$, $D_3$ and $D_4$ be SDS of type $H$ in an abelian group $G$ of order $v$, that is,

$$\sum_{i=1}^{4} \Delta D_i = v\theta + \lambda T, \quad \text{and} \quad \lambda = \sum_{i=1}^{4} | D_i | - v.$$  

If $\Delta(D_1, D_2) + \Delta(D_3, D_4) = \lambda T$, write

$$(D_1, D_2, D_3, D_4) \in H_1(v);$$
9.3. The Relationship

if $\bigodot D_i = D_i, i = 1, 2, 3, 4$, write

$$(D_1, D_2, D_3, D_4) \in W_0(v).$$

if $\bigodot D_i = D_i, i = 1, 2, 3, 4$ and $\Delta(D_i, D_j) + \Delta(D_k, D_l) = \lambda T, \{i, j, k, l\} = \{1, 2, 3, 4\}$, write

$$(D_1, D_2, D_3, D_4) \in W_2(v).$$

It is well known that

(a) if $W_2(v) \neq \phi$, $v$ must be a complete square and $W_2(v) \neq \phi$ for $v = 9^rN^4$ where $r = 0$ or $1$, $N$ is an integer (see [18], [155], [160], [157], [159] for details).

(b) if $H_1(v) \neq \phi$, $v$ must be the sum of two squares and $H_1(v) \neq \phi$ for $v \in S_1 \cup S_2 \cup S_3 \cup S_4$ (see [157], [156]) where

$$S_1 = \{5, 13, 17, 25, 37, 41, 61\},$$
$$S_2 = \{p^{2r} : p \equiv 5(mod 8) \text{ a prime}\},$$
$$S_3 = \{9^rN^4 : r = 0, 1 \text{ and } N \text{ is an integer}\},$$
$$S_4 = \{v_1v_2 : v_1 \in S_1 \cup S_2 \text{ and } v_2 \in S_3\}.$$

(c) $W_0(v) \neq \phi$ for $v \in S_3 \cup S_5 \cup S_6$ (see [117], [155], [154]) where

$$S_5 = \{v : 2v - 1 \equiv 1(mod 4) \text{ is a prime power}\},$$
$$S_6 = \{q^2 : q \equiv 1(mod 4) \text{ is a prime power}\}.$$

**Theorem 9.4** If there exist $T$-matrices of order $t$ and SDS of type $H$, say $D_1, D_2, D_3$ and $D_4$ in an abelian group $G$ of order $v$, such that $D_1 \bigodot D_3 = D_3 \bigodot D_1$ and $D_2 \bigodot D_4 = D_4 \bigodot D_2$, then there exists an Hadamard matrix of order $4tv$.

**Proof.** Let $T_1, T_2, T_3$ and $T_4$ be $T$-matrices of order $t$, $B_1, B_2, B_3$ and $B_4$ are the $\pm 1$ incidence matrices (type 1) of $D_1, D_2, D_3$ and $D_4$, respectively. From the hypotheses, it follows that

$$B_1B_3^T = B_3B_1^T, \quad B_2B_4^T = B_4B_2^T,$$

$$\sum_{i=1}^{4} T_iT_i^T = tI_t, \quad \sum_{i=1}^{4} B_iB_i^T = 4vI_v.$$

Put

$$W_1 = T_1 \times B_1 + T_2 \times B_2 + T_3 \times B_3 + T_4 \times B_4,$$
$$W_2 = T_1 \times B_2^T - T_2 \times B_1^T + T_3 \times B_4^T - T_4 \times B_3^T,$$
$$W_3 = T_1 \times B_3 - T_2 \times B_4 - T_3 \times B_1 + T_4 \times B_2,$$
$$W_4 = T_1 \times B_4^T + T_2 \times B_3^T - T_3 \times B_2^T - T_4 \times B_1^T.$$
where $\times$ denotes the Kronecker product. It is easy to see that $W_1, W_2, W_3$ and $W_4$ are $\pm 1$ matrices, and

$$
\sum_{i=1}^{4} W_i W_i^T = \left(\sum_{i=1}^{4} T_i T_i^T \right) \times \left(\sum_{i=1}^{4} B_i B_i^T \right) + \\
(T_1 T_3^T - T_3 T_1^T - T_2 T_4^T + T_4 T_2^T) \times (B_1 B_3^T - B_3 B_1^T - B_2 B_4^T + B_4 B_2^T) \nonumber \\
= 4tv I_{tv}.
$$

Therefore a Goethals–Seidel (or Wallis–Whiteman) type construction applies, and an Hadamard matrix of order $4tv$ can be formed.

Corollary 9.1 If there exist $T$–matrices of order $t$, then there exists an Hadamard matrix of order $4t3^r$ for every integer $r \geq 0$(see [88], [152]).

Corollary 9.2 If there exist $T$–matrices of order $t$, then there exists an Hadamard matrix of order $4tv$ for every $v$ such that $W_0(v) \neq \phi$.

Theorem 9.5 If there exist $T$–matrices of order $t$ and $H_1(v) \neq \phi$, then there exists an Hadamard matrix of order $4tv$.

Proof. Let $T_1, T_2, T_3$ and $T_4$ be $T$–matrices of order $t$ and $(D_1, D_2, D_3, D_4) \in H_1(v)$. Let $B_1, B_2, B_3$ and $B_4$ be $\pm 1$ incidence matrices (type 1) of $D_1, D_2, D_3$ and $D_4$, respectively. Put

$$
W_1 = T_1 \times B_1 + T_2 \times B_2 + T_3 \times B_3 + T_4 \times B_4, \\
W_2 = T_1 \times B_2 + T_2 \times B_1 + T_3 \times B_4 + T_4 \times B_3, \\
W_3 = T_1 \times B_3^T + T_2 \times B_4^T - T_3 \times B_1^T - T_4 \times B_2^T, \\
W_4 = T_1 \times B_4^T + T_2 \times B_3^T - T_3 \times B_2^T - T_4 \times B_1^T.
$$

It is easy to verify that

$$
\sum_{i=1}^{4} W_i W_i^T = 4tv I_{tv}.
$$

Applying again Goethals–Seidel (or Wallis–Whiteman) type construction, there exists an Hadamard matrix of order $4tv$. \hfill \square

### 9.4 Constructing $C$–partitions

Suppose that $v = q^2$, $q = 4m + 3$ is a prime power, $g$ is a generator of the multiplicative group of $GF(v)$. Let

$$
E_i = \{g^{8(m+1)j+i} : j = 0, \ldots, 2m\}, \quad i = 0, 1, \ldots, 8m + 7,
$$

9.4. Constructing $C-$partitions

There is

$$T^* = \sum_{i=0}^{4m+3} T_i, \quad T = \theta + T^*.$$  

Define

$$E_i = E_j \quad \text{as} \quad i \equiv j (\text{mod} \ 8m + 8),$$

$$S_i = S_j \quad \text{as} \quad i \equiv j (\text{mod} \ 4m + 4),$$

$$T_i = T_j \quad \text{as} \quad i \equiv j (\text{mod} \ 4m + 4).$$

Then

$$gS_i = S_{i+1}, \quad gT_i = T_{i+1}, \quad i = 0, 1, \ldots, 4m + 3,$$

$$gE_i = E_{i+1}, \quad i = 0, 1, \ldots, 8m + 7,$$

$$gT^* = T^*, \quad gT = T, \quad g\theta = \theta.$$  

Denote

$$\Phi_0 = \triangle E_0, \quad \Phi_i = \triangle (E_0, E_i), \quad i = 0, 1, \ldots, 8m + 7,$$

and define

$$\phi_i = \phi_j \quad \text{as} \quad i \equiv j (\text{mod} \ 8m + 8).$$

Then

$$\triangle E_i = g^i \phi_0, \quad i = 0, 1, \ldots, 8m + 7,$$

$$\triangle (E_i, E_j) = g^i \phi_{j-i} = g^i \phi_{i-j} \quad \text{for} \quad i \neq j,$$

in particular,

$$\phi_i = g^i \phi_{-i} = g^i \phi_{8m + 8 - i}, \quad i = 1, \ldots, 8m + 7.$$  

From [159] it is known

**Lemma 9.1** If $q = 4m + 3$ is a prime power, $v = q^2$, then following equations hold:

(a) \ \Phi_0 = (2m + 1)\theta + mT_0,

(b) \ \Phi_{4m+4} = (2m + 1)T_0,

(c) \ \Phi_i + \Phi_{i+4m+4} = T^* - T_0 - T_i, \quad i = 1, \ldots, 4m + 3.$$

For $0 \leq t \leq 2m + 1$, put

$$D = \bigcup_{i=0}^{2t} E_{a_i} \cup \bigcup_{j=1}^{2m+1-t} S_{b_j}, \quad (9.4)$$

(If $t = 2m + 1$ the term $\bigcup_{j=1}^{\theta} S_{b_j}$ would be vanished) where $a_i, b_j$ satisfy

$$| \{ a_i (\text{mod} \ 4m + 4) : i = 0, \ldots, 2t \} \cup \{ b_j : j = 1, \ldots, 2m + 1 - t \} | = 2m + 2 + t, \quad (9.5)$$
that is, \(a_i \neq a_j (\text{mod } 4m + 4)\) for \(i \neq j\) and \(a_i \neq b_j (\text{mod } 4m + 4)\), \(i = 0, \ldots, 2t, j = 1, \ldots, 2m + 1 - t\).

**Lemma 9.2** Suppose \(D\) is given as in (9.4) and \(a_i, b_i\) satisfy (9.5), then

\[
\Delta D = 2(2m + 1)(2m + 1 - t)\theta + (4m^2 + 4m + 1 - t^2)T^* + (t - 2m - 1)\sum_{i=0}^{2t} T_{a_i} + \Delta(U_{i=0}^t E_{a_i}).
\]  

(9.6)

For proof see [159] for details.

The expression (9.6) is dependent on the set of \(a_i\)'s only, but the set of \(b_j\)'s has nothing to do with it.

In the following suppose \(m = 2r\), that is, \(g = 8r + 3\) is a prime power and denote

\[
F_i = \bigcup_{j=0}^{2r} E_{8j+i}, \quad i = 0, \ldots, 7,
\]

\[
G_i = \sum_{d \in F_i \cup F_{i+4}} d, \quad i = 0, 1, 2, 3.
\]

**Theorem 9.6** If \(q = 8r + 3\) is a prime power, there exist \(C\)-partitions in \(GF(q^2)\).

**Proof.** Let \(I = \{0, 1, \ldots, 2r\}\). \(I_0, I_1, I_2\) and \(I_3\) are subsets of \(I\) and \(|I_i| = r\), and let \(I_i = I \setminus I_i, i = 0, 1, 2, 3\). Take

\[
D_1 = \bigcup_{j \in I_1} S_{8j+1} \cup F_0 \cup F_3 \cup F_6,
\]

\[
D_2 = \bigcup_{j \in I_0} S_{8j} \cup \bigcup_{j \in I_2} S_{8j+2} \cup \bigcup_{j \in I_3} S_{8j+3} \cup F_1,
\]

\[
D_3 = \bigcup_{j \in I_3} S_{8j+3} \cup F_0 \cup F_2 \cup F_5,
\]

\[
D_4 = \bigcup_{j \in I_0} S_{8j} \cup \bigcup_{j \in I_1} S_{8j+1} \cup \bigcup_{j \in I_2} S_{8j+2} \cup F_3.
\]

From (9.6) there are

\[
\Delta D_1 = 2r(4r + 1)\theta + (7r^2 + 2r)T^* - r(G_0 + G_2 + G_3) + \Delta(F_0 \cup F_3 \cup F_6),
\]

\[
\Delta D_2 = 2(4r + 1)(3r + 1)\theta + ((4r + 1)^2 - r^2)T^* - (3r + 1)G_1 + \Delta F_1,
\]

\[
\Delta D_3 = 2(4r + 1)\theta + (7r^2 + 2r)T^* - r(G_0 + G_1 + G_2) + \Delta(F_0 \cup F_2 \cup F_5),
\]

\[
\Delta D_4 = 2(4r + 1)(3r + 1)\theta + ((4r + 1)^2 - r^2)T^* - (3r + 1)G_3 + \Delta F_3,
\]

and

\[
\sum_{i=1}^{4} \Delta D_i = 4(4r + 1)^2\theta + 2(22r^2 + 9r + 1)T^* - (2r + 1)(G_1 + G_3).
\]
9.4. Constructing C−partitions

\[+2(1 + g + g^2 + g^3)\Delta F_0 + \Delta(F_0, F_3) + \Delta(F_0, F_5)\]
\[+g^2\Delta(F_0, F_3) + g^3\Delta(F_0, F_3) + \Delta(F_0, F_2 \cup F_6)\]
\[= 4(4r + 1)^2\theta + 2(22r^2 + 9r + 1)T^* - (2r + 1)(G_1 + G_3)\]
\[+ \sum_{i=0}^{3} g^i(2\Delta F_0 + \Delta(F_0, F_3)) + \Delta(F_0, F_2 \cup F_6). \]  

(9.7)

Write \( \Delta F_0 = (2r + 1)(4r + 1)\theta + \sum_{i=0}^{3} \alpha_i G_i \). Counting the number of terms on the two sides in the equation above, there are

\[(2r + 1)^2(4r + 1)^2 = (2r + 1)(4r + 1) + 2(2r + 1)(4r + 1)\sum_{i=0}^{3} \alpha_i,\]

and

\[\sum_{i=0}^{3} \alpha_i = \frac{1}{2}((2r + 1)(4r + 1) - 1).\]

So,

\[2 \sum_{i=0}^{3} g^i \Delta F_0 = 8(2r + 1)(4r + 1)\theta + ((2r + 1)(4r + 1) - 1)T^*. \]  

(9.8)

Similarly, one can prove that

\[(1 + g + g^2 + g^3)\Delta(F_0, F_3) = (2r + 1)(4r + 1)T^*.\]  

(9.9)

Now

\[\Delta(F_0, F_2 \cup F_6) = \sum_{i=0}^{2r} \sum_{j=0}^{2r} \Delta(E_{8i}, E_{8j+2} \cup E_{8j+8r+6})\]
\[= \sum_{i=0}^{2r} g^{8i} \sum_{j=0}^{2r} (\Phi_{8(j-i)+2} + \Phi_{8(j-i)+8r+6})\]
\[= \sum_{i=0}^{2r} g^{8i} \sum_{j=0}^{2r} (T^* - T_0 - T_{8(j-i)+2})\]
\[= (2r + 1)^2T^* - (2r + 1)\sum_{i=0}^{2r} (T_{8i} + T_{8i+2})\]
\[= (2r + 1)^2T^* - (2r + 1)(G_0 + G_2). \]  

(9.10)

From (9.7)−(9.10) there is

\[\sum_{i=1}^{4} \Delta D_i = 4(8r + 3)(4r + 1)\theta + (64r^2 + 32r + 3)T^*\]
\[= q^2\theta + q(q - 2)T.\]
Thus, $D_1$, $D_2$, $D_3$ and $D_4$ are SDS of type $H$. Noting that

$$\bigcup_{j \in I_1} S_{8j+1} \cup \bigcup_{j \in I_1} S_{8j+1} = F_1 \cup F_5,$$
$$\bigcup_{j \in I_2} S_{8j+2} \cup \bigcup_{j \in I_2} S_{8j+2} = F_2 \cup F_6,$$

so, every element of $G$ appears an even number of times in the system of $D_1$, $D_2$, $D_3$ and $D_4$. By theorem 9.1 there exist $C-$partitions in $G$. The theorem is proved. □

From example, let $r = 0$, now $I = \{0\}$, $I_i = \emptyset$, $i = 0, 1, 2, 3$, and $F_i = \{g^i\}$, $i = 0, 1, \ldots, 7$. In this case

$$D_1 = \{g^0, g^3, g^6\}, \quad D_2 = \{g, g^2, g^6\},$$
$$D_3 = \{g^0, g^2, g^5\}, \quad D_4 = \{g, g^3, g^5\},$$

and in $GF(9)$ there exists $C-$partitions $A_1, \ldots, A_8$ as follows:

$$A_1 = \phi, \quad A_2 = \{g^6\}, \quad A_3 = \{g^0\}, \quad A_4 = \{g^3\},$$
$$A_5 = \{0, g^4, g^7\}, \quad A_6 = \{g^5\}, \quad A_7 = \{g\}, \quad A_8 = \{g^2\}.$$

From theorem 9.6 the following result is true.

**Corollary 9.3** Let $p \equiv 3(\text{mod } 8)$ be a prime. If $W_0(p) \neq \phi$ and there exist $C-$partitions in $GF(p)$, there exist Hadamard matrices of order $4p^r$ for any integer $r \geq 0$.

**Proof.** Firstly, $W_2(p^{4r}) \neq \phi$ for every integer $r \geq 0$. By the hypotheses of the corollary, there exist Hadamard matrices of order $4p^{4r}$ and $4p^{4r+1}$ for every integer $r \geq 0$. From theorem 9.6 and $W_0(p) \neq \phi$, there exist Hadamard matrices of order $4p^{4r+2}$ and $4p^{4r+3}$ for every integer $r \geq 0$. □

For example, when $p = 3, 11, 19, 43$, the conclusions of corollary 9.3 are valid.
Chapter 10

Regular Hadamard Matrix, Maximum Excess and SBIBD

This chapter is based on the paper by M. Xia, T. Xia and J. Seberry [162]. 50 percent of the results are due to the second author.

In this chapter Hadamard matrix, SBIBD, SDS, DS and T-matrix are discussed. When
\[ k = q_1, q_2, q_4 q_1, q_4 q_2, q_2 q_3 N^2, q_4 q_3 N^2, \]
where \( q_1 \equiv 1 \pmod{4}, q_2 \equiv 3 \pmod{8}, q_3 \equiv 5 \pmod{8}, \) \( q_1, q_2, q_3 \) are prime powers, \( q_4 = 7 \) or \( 23, N = 2^a 3^b r^2, a, b = 0 \) or \( 1, r \) is an arbitrary integer, there exist regular Hadamard matrices of order \( 4k^2, \) and also there exists \( SBIBD(4k^2, 2k^2 + k, k^2 + k). \)

When \( k \in \{ 1, 3, 5, \cdots, 45, 49, \cdots, 69, 73, 75, 81, \cdots, 101, 105, 109, \cdots, 125, 129, 135, 137, 143, \cdots, 149, 153, \cdots, 161, 165, 169, \cdots, 175, 181, \cdots, 189, 193, \cdots, 197, 201, \cdots, 207, 219, 221, 225, 229, 235, 241, 245, 247, 625, 32r, 25 \cdot 32r \}, r > 0, \) there exists \( 4k^2 - Hadamard \) matrix and \( SBIBD(4k^2, 2k^2 + k, k^2 + k) \) (see [59], [116] for details).

In section 10.1 some definition and lemmas are given. In section 10.2 SDS and \( T- \) matrices are used to construct \( SBIBD. \) The author find new results which give many new \( SBIBDs. \)

10.1 Background

The excess of a \( H - matrix \) by \( \sigma(H) \) denoted as following
\[ \sigma(H) = \sum_{1 \leq i, j \leq n} a_{ij}, \quad a_{ij} \text{ is a entry of } H. \]

Let \( \sigma(n) = \max \{ \sigma(H) \} \). The weight of a H-matrix \( H, \) denoted by \( W(H), \) is the number of \( 1 \) in the \( H. \) Denote \( W(n) = \max \{ W(H) \}. \) It is obvious that \( \sigma(H) = 2W(H) - n^2 \) and \( \sigma(n) = 2W(n) - n^2 \) (see [59], [67], [106], [114] for details).

M. R. Best [11] proved that
\[ \sigma(n) \leq n \sqrt{n} \quad (10.1) \]
10.1. Background

Definition 10.1 (Incidence matrix) The incidence matrix $A = (a_{ij})$ of a $(v, k, \lambda) - DS$ $D$ is defined by ordering the elements of the group $G = \{g_i\}, i = 1, \ldots, v,$ and defining

$$a_{ij} = \begin{cases} 1, & g_j \oplus g_i \in D, \\ 0, & \text{otherwise} \end{cases}$$

Lemma 10.1 (J. Seberry [114]) The following conditions are equivalent:

(i) There exists a Hadamard matrix of order $4k^2$ which maximum excess is $8k^3$.

(ii) There exists a regular Hadamard matrix of order $4k^2$.

(iii) There exists SBIBD($4k^2, 2k^2 + k, k^2 + k$).

Some very useful methods to construct Hadamard matrices with maximum excess from Williamson matrices and $T-$matrices are given in [114].

Lemma 10.2 (M. Y. Xia and G. Liu [154]) Let $q$ be a prime power, if $q \equiv 1 (\mod 4)$, there exist $4 - \{q^2; \frac{1}{2}q(q - 1); q(q - 2)\}$ supplementary difference sets.

Lemma 10.3 (M. Y. Xia and G. Liu [158]) Let $q$ be a power of a prime, $q \equiv 3 (\mod 8)$, then there exist $4 - \{q^2; \frac{1}{2}q(q - 1); q(q - 2)\}$ supplementary difference sets.

Lemma 10.4 (Y. Q. Chen [18], M. Y. Xia [155]) Let $q = 2^a3^bN^2$, $a, b = 0$ or $1$, $N$ is an arbitrary integer, then there exist $(4q^2, 2q^2 + q^2 + q)$ difference sets and Williamson type matrices (type 1) $A_1, A_2, A_3$ and $A_4$ of order $q^2$ that satisfy

$$\sigma(A_1) = \sigma(A_2) = \sigma(A_3) = q^3, \quad \sigma(A_4) = -q^3,$$

$$A_1^2 + A_2^2 + A_3^2 + A_4^2 = 4q^2I_{q^2},$$

$$A_iA_j + A_kA_l = 0, \quad \{i, j, k, l\} = \{1, 2, 3, 4\}.$$ (10.2)

Lemma 10.5 (M. Y. Xia and T. Xia [156]) Let $q_1$ be a prime power, $q_1 \equiv 5 (\mod 8)$, $q_2 = 2^a3^bN^2$, $a, b = 0$ or $1$, $N$ is an arbitrary integer, then there exist $(1, -1)$ matrices $A_1, A_2, A_3$ and $A_4$ of order $(q_1q_2)^2$ that satisfy:

$$\sigma(A_1) = \sigma(A_2) = \sigma(A_3) = (q_1q_2)^3, \quad \sigma(A_4) = -(q_1q_2)^3,$$

$$A_1A_1^T + A_2A_2^T + A_3A_3^T + A_4A_4^T = 4(q_1q_2)^2I_{(q_1q_2)^2},$$

$$A_1A_2^T + A_2A_1^T + A_3A_4^T + A_4A_3^T = 0.$$ (10.3)

Notation 10.1 Circular or type 1 matrices which satisfy the formula marked by "*", will be called Xia-Xia matrices.
10.2 Construction of SBIBD from SDS

Proposition 10.1 Let \( p \equiv 5(\text{mod } 8) \) be a prime, \( q \equiv 2a_3bN^2 \), \( a, b = 0 \) or \( 1 \), \( N \) be an arbitrary integer, for any integer \( r \geq 1 \), there exists \( (1,-1) \) matrices \( A_1, A_2, A_3 \) and \( A_4 \) of order \( (p^r q)^2 \) that satisfy

\[
\sigma(A_1) = \sigma(A_2) = \sigma(A_3) = (p^r q)^3, \quad \sigma(A_4) = -(p^r q)^3,
\]

\[
\sum_{i=1}^{4} A_i A_i^T = 4(p^r q)^2 I_{(p^r q)^2},
\]

\[
A_1 A_2^T + A_2 A_1^T + A_3 A_4^T + A_4 A_3^T = 0
\]

Proof. When \( q_1 = p^{2r+1} \), then \( q_1 \equiv 5(\text{mod } 8) \), from lemma 10.5, the result is true. When \( q_1 = p^{2r} = (p^r)^2 \), from lemma 10.4 the conclusion is true. This completes the proof. \( \square \)

Remark. By using definition 4.10 it can be said that when \( p \equiv 5(\text{mod } 8) \), \( q = 2a_3bN^2 \), \( a, b = 0 \) or \( 1 \), \( N \) is an arbitrary integer, for any integer \( r \geq 1 \), there exist SDS \( D_1, D_2, D_3 \) and \( D_4 \) of order \( p^{2r} q^2 \) and type \( H_1 \). This means \( H_1(p^{2r} q^2) \neq \emptyset \) wherever such SDS exist for order \( p^{2r} q^2 \).

\[ 10.2 \text{ Construction of SBIBD from SDS} \]

Theorem 10.1 If there exists \( H_4 \)-type SDS on an Abelian group \( G \) of order \( q^2 \), then there exists SBIBD \((4q^2, 2q^2 + q, q^2 + q)\).

Proof. Let \( D_1, D_2, D_3, D_4 \) be \( 4 - \{q^2, \frac{1}{2} q(q-1); q(q-2)\} \) SDS on \( G \), since there is

\[ |D_1| = |D_2| = |D_3| = |D_4| = \frac{1}{2} q(q-1), \sum_{i=1}^{4} \triangle D_i = q^2 \theta + q(q-2)G. \]

Let \( g_1, \cdots, g_{q^2} \) be the arbitrary order of \( G \), set

\[ A_i = (a_{jk}^{(i)})_{1 \leq j, k \leq q^2}, \quad a_{jk}^{(i)} = \begin{cases} -1 & \text{if } g_k \oplus g_j \in D_i, \\ 1 & \text{otherwise}, \end{cases} \]

\[ R = (r_{jk})_{1 \leq j, k \leq q^2}, \quad r_{jk} = \begin{cases} 1 & \text{if } g_j \oplus g_k = 0, \\ 0 & \text{otherwise}. \end{cases} \]

It is obvious that \( A_1, A_2, A_3, A_4 \) are the matrices of type 1. In this case

(i) \( A_i A_j = A_j A_i, i \neq j, i, j = 1, 2, 3, 4, \)

(ii) \( (A_i R)^T = A_i R, i = 1, 2, 3, 4, \)

(iii) \( \sum_{i=1}^{4} A_i A_i^T = 4q^2 I_{q^2}. \)
Since $|D_i| = \frac{1}{2}q(q - 1)$, there exist $\frac{1}{2}q(q + 1)$ ones and $\frac{1}{2}q(q - 1)$ negative ones in each row of $A_i$, $i = 1, 2, 3, 4$, so $\sigma(A_i) = q^3, i = 1, 2, 3, 4$. Set

$$H = \begin{pmatrix}
-A_1 & A_2 & A_3 & A_4 \\
A_2 & A_1 & A_4 & -A_3 \\
A_3 & -A_4 & A_1 & A_2 \\
A_4 & A_3 & -A_2 & A_1
\end{pmatrix}.$$ (10.7)

It is easy to verify that $HH^T = 4q^2I_{4q^2}, \sigma(A_1) = \sigma(A_2) = \sigma(A_3) = \sigma(A_4)$, $i = 1, 2, 3, 4$. So there is

$$\sigma(H) = 2\{\sigma(A_1) + \sigma(A_2) + \sigma(A_3) + \sigma(A_4)\} = 8q^3.$$

From lemma 10.1, $\frac{1}{2}(H + J)$ is a $SBIBD(4q^2, 2q^2 + q, q^2 + q)$. This completes the proof. \(\square\)

**Corollary 10.1** Let $q$ be a prime power, $q \equiv 1(mod 4)$ or $q \equiv 3(mod 8)$. There exists $SBIBD(4q^2, 2q^2 + q, q^2 + q)$.

**Proof.** From lemma 10.2, lemma 10.3 and theorem 10.1 the conclusion is true. \(\square\)

**Remark.** When $q \equiv 1(mod 4)$ is a prime power, there exist Williamson type matrices $A_1, A_2, A_3$ and $A_4$ of order $q^2$, that make the matrix $H$ of (10.7) have maximum excess and the form

$$H = \begin{pmatrix}
-A_1 & A_2 & A_3 & A_4 \\
A_2 & A_1 & A_4 & -A_3 \\
A_3 & -A_4 & A_1 & A_2 \\
A_4 & A_3 & -A_2 & A_1
\end{pmatrix}.$$ (10.8)

**Lemma 10.6** Let $q = 2^a3^bN^2$, $a, b = 0$ or 1, $N$ be arbitrary integer. There exists $SBIBD(4q^2, 2q^2 + q, q^2 + q)$.

**Proof.** From lemma 10.4, there exist $DS$ of type $(4q^2, 2q^2 + q, q^2 + q)$, the $(0, 1)$ incidence matrix $B$ of the $DS$ is an $SBIBD(4q^2, 2q^2 + q, q^2 + q)$. The proof is completed. \(\square\)

**Remark.** From lemma 10.4, there exist Williamson type matrices $A_1, A_2, A_3, A_4$ of order $q^2$ that satisfy (10.2). In this case, the matrix $H$ of order $4q^2$ with maximum excess has the following form

$$H = \begin{pmatrix}
A_1 & A_2 & A_3 & A_4 \\
A_2 & A_1 & A_4 & A_3 \\
A_3 & A_4 & A_1 & A_2 \\
A_4 & A_3 & A_2 & A_1
\end{pmatrix}.$$ (10.9)
10.3. Construction of SBIBD from SDS and $T-$ matrices

or

$$H = \begin{pmatrix}
A_1 & A_2 & A_3 & A_4 \\
A_2 & A_3 & A_4 & A_1 \\
A_3 & A_4 & A_1 & A_2 \\
A_4 & A_1 & A_2 & A_3
\end{pmatrix}. \quad (10.10)$$

**Lemma 10.7** Let $p \equiv 5(\text{mod } 8)$ be a prime, $q = 2^a3^bp^cN^2$, $a, b, c = 0$ or 1, $N$ be an arbitrary integer, then there exists $SBIBD(4q^2, 2q^2 + q, q^2 + q)$.

**Proof.** When $c = 0$, from lemma 10.6, the lemma 10.7 is true. When $c = 1$, from lemma 10.5 that there exist $(1, -1)$ matrices (type 1) $A_1, A_2, A_3$ and $A_4$ of order $q^2$ that satisfy (10.3). Let

$$H = \begin{pmatrix}
A_1 & A_2 & A_3 & A_4 \\
A_2 & A_1 & A_4 & A_3 \\
-A_3^T & -A_4^T & A_1^T & A_2^T \\
-A_4^T & -A_3^T & A_2^T & A_1^T
\end{pmatrix}. \quad (10.11)$$

then $HH^T = 4q^2I_{4q^2}$, $\sigma(H) = 4(\sigma(A_1) + \sigma(A_2)) = 8q^3$. So the matrix $H$ of (10.11) is an Hadamard matrix with maximum excess. In this case, from lemma 10.1 there exists $SBIBD(4q^2, 2q^2 + q, q^2 + q)$. The proof is completed. \qed

**Proposition 10.2** Let $q = 2^{r_1}3^{r_2}p^{r_3}N^2$, $p \equiv 5(\text{mod } 8)$ be a prime, $r_1, r_2, r_3$ be integers and $r_1, r_2, r_3 \geq 0$, $N$ be an arbitrary integer. Then lemma 10.7 still holds.

**Proof.** Let $r_i = 2m_i + a_i$, $0 \leq a_i \leq 1$, $i = 1, 2, 3$, then $q = 2^{a_1}3^{a_2}p^{a_3}(2^{m_1}3^{m_2}p^{m_3}N)^2$. From lemma 10.7 the result is true. \qed

10.3. Construction of SBIBD from SDS and $T-$ matrices

More details of $T-$ matrices are discussed in [20]. This section refer to the paper [161].

**Theorem 10.2** If there exist $4 - \{q^2; \frac{1}{2}q(q - 1); q(q - 2)\}$ SDS $D_1, D_2, D_3, D_4$ of order $q^2$ in an Abelian group $G$, and every entry of $G$ appears an even number of times in $D_1, D_2, D_3, D_4$, then there exist $T-$matrices $T_1, T_2, T_3, T_4$ that satisfy

$$\sigma(T_1) = q^3, \quad \sigma(T_2) = \sigma(T_3) = \sigma(T_4) = 0.$$
Proof. Let

\begin{align*}
E_1 &= G \setminus (D_1 \cup D_2 \cup D_3 \cup D_4), & E_2 &= (D_1 \cap D_2) \setminus E_5, \\
E_3 &= (D_1 \cap D_3) \setminus E_5, & E_4 &= (D_1 \cap D_4) \setminus E_5, \\
E_5 &= D_1 \cap D_2 \cap D_3 \cap D_4, & E_6 &= (D_3 \cap D_4) \setminus E_5, \\
E_7 &= (D_2 \cap D_4) \setminus E_5, & E_8 &= (D_2 \cap D_3) \setminus E_5.
\end{align*}

From [181] there are

\begin{align*}
E_i \cap E_j &= \phi, \ i \neq j, \ 1 \leq i, j \leq 8, \\
G &= \bigcup_{i=1}^{8} E_i, \\
\sum_{i=1}^{8} \Delta E_i &= q^2 \theta + \sum_{i=1}^{4} \Delta (E_i, E_{i+4}),
\end{align*}

and

\begin{align*}
D_1 &= E_5 \cup E_2 \cup E_3 \cup E_4, & D_2 &= E_5 \cup E_2 \cup E_7 \cup E_8 \\
D_3 &= E_5 \cup E_3 \cup E_6 \cup E_8, & D_4 &= E_5 \cup E_4 \cup E_6 \cup E_7.
\end{align*}

Set \(| E_i | = e_i, i = 1, \ldots, 8, \) then

\begin{align*}
| D_1 | = e_2 + e_3 + e_4 + e_5, & \quad | D_2 | = e_2 + e_5 + e_7 + e_8, \\
| D_3 | = e_3 + e_5 + e_6 + e_8, & \quad | D_4 | = e_4 + e_5 + e_6 + e_7.
\end{align*}

Since \(| D_1 | = | D_2 | = | D_3 | = | D_4 | = \frac{1}{2} q(q - 1)\), then

\begin{align*}
e_2 - e_6 = e_3 - e_7 = e_4 - e_8 = 0.
\end{align*}

Since

\begin{align*}
q^2 &= \left| G \right| = \left| \bigcup_{i=1}^{8} E_i \right| = \sum_{i=1}^{8} e_i = e_1 + e_5 + 2(e_2 + e_3 + e_4) \\
&= e_1 - e_5 + 2(e_2 + e_3 + e_4 + e_5) = e_1 - e_5 + q(q - 1),
\end{align*}

then \(e_1 - e_5 = q\). Let \(g_1, \ldots, g_{q^2}\) be an arbitrary order of entries of \(G\), and

\begin{align*}
T_i &= \left( t_{jk}^{(i)} \right)_{1 \leq j, k \leq q^2}, \ t_{jk}^{(i)} = \left\{ \begin{array}{ll}
1 & \text{if } g_k \in E_i, \\
-1 & \text{if } g_k \in E_{i+4}, \ i = 1, 2, 3, 4. \\
0 & \text{otherwise},
\end{array} \right.
\end{align*}

\(T_1, T_2, T_3, T_4\) are \(T\)-matrices of order \(q^2\) and

\begin{align*}
\sigma(T_1) &= q^3, & \sigma(T_2) &= \sigma(T_3) &= \sigma(T_4) &= 0.
\end{align*}

This completes the proof. \(\square\)
Proposition 10.3  Let $q$ be a prime power and $q \equiv 3(\text{mod } 8)$, then there exist $T$-matrices $T_1, T_2, T_3$ and $T_4$ of order $q^2$ that satisfy theorem 10.2.

Theorem 10.3  If there exist $T$-matrices $T_1, T_2, T_3$ and $T_4$ of order $t^2$, and $\sigma(T_1) = t^3$, $\sigma(T_2) = \sigma(T_3) = \sigma(T_4) = 0$, then there exists SBIBD($4k^2, 2k^2 + k, k^2 + k$), $k = tq$, $q \equiv 1(\text{mod } 4)$ be a prime power.

Proof.  When $q \equiv 1(\text{mod } 4)$ be a prime power, from lemma 10.2, there exist $4 - \{q^2, \frac{1}{2}q(q - 1); q(q - 2)\}$ SDS. In this case from theorem 10.1 there exist Williamson type (type 1) matrices $A_1, A_2, A_3$ and $A_4$ of order $q^2$ which satisfy

(i) $A_i = A_i^T$, $A_i A_j = A_j A_i$, $1 \leq i, j \leq 4$, $i \neq j$,

(ii) $\sum_{i=1}^{4} A_i^2 = 4q^2 I_{q^2}$,

(iii) $\sigma(A_1) = \sigma(A_2) = \sigma(A_3) = \sigma(A_4) = q^3$.

Let

\begin{align*}
B_1 &= T_1 \times A_1 + T_2 \times A_2 + T_3 \times A_3 + T_4 \times A_4, \\
B_2 &= T_1 \times A_2 - T_2 \times A_1 + T_3 \times A_4 - T_4 \times A_3, \\
B_3 &= T_1 \times A_3 + T_2 \times A_4 - T_3 \times A_1 - T_4 \times A_2, \\
B_4 &= T_1 \times A_4 - T_2 \times A_3 - T_3 \times A_2 + T_4 \times A_3,
\end{align*}

where $\times$ is kronecker product. It is obvious that $B_i B_j = B_j B_i$, $i \neq j$, $i, j = 1, 2, 3, 4$, and

$$\sum_{i=1}^{4} B_i B_i^T = \left(\sum_{i=1}^{4} T_i T_i^T\right) \times \left(\sum_{i=1}^{4} A_i^2\right) = 4(tq)^2 I_{(tq)^2}.$$  

Since $\sigma(T_i \times A_i) = \sigma(T_i) \sigma(A_i)$, $i = 1, 2, 3, 4$,

$$\sigma(B_1) = \sigma(B_2) = \sigma(B_3) = \sigma(B_4) = (tq)^3.$$  

Let

$$Q = R \times I_{q^2},$$

where $R$ is a monomial matrix of order $t^2$ that satisfies $R = R^T$, $R^2 = I$, and $(T_i R_i)^T = T_i R_i$, $i = 1, 2, 3, 4$. It is easy to show that $Q$ is a permutation matrix and $(B_i Q)^T = B_i Q$, $i = 1, 2, 3, 4$. Let

$$H = \begin{pmatrix}
B_1 & B_2 Q & -B_3 Q & B_4 Q \\
B_2 Q & -B_1 & B_1^T Q & B_3^T Q \\
B_3 Q & B_1^T Q & B_1 & -B_2^T Q \\
-B_4 Q & B_3^T Q & B_2^T Q & B_1
\end{pmatrix}.$$
Then $HH^T = 4k^2I_{4k^2}$, and $\sigma(H) = 2(\sum_{i=1}^4 \sigma(B_i)) = 8k^3$. In this case, the matrix $H$ of order $4k^2$ defined from (10.12), (10.13), (10.14) has the maximum excess. There exist $SBIBD(4k^2, 2k^2 + k, k^2 + k)$, $k = tq$. The proof is complete.

**Proposition 10.4** When $k = q_1q_2$, where $q_1 = 1(mod 4)$, $q_2 = 3(mod 8)$ are prime powers, there exists $SBIBD(4k^2, 2k^2 + k, k^2 + k)$.

**Proof.** From [161], there exist $T$-matrices $T_1, T_2, T_3, T_4$ satisfying theorem 10.3. This completes the proof.

**Theorem 10.4** If

1. there exist $T$-matrices $T_1, T_2, T_3, T_4$ of order $t^2$ that satisfy

   \[ \sigma(T_1) = t^3, \quad \sigma(T_2) = \sigma(T_3) = \sigma(T_4) = 0, \]

2. there exist $(1, -1)$ matrices (type 1) $A_1, A_2, A_3$ and $A_4$ of order $q^2$ that satisfy

   (i) $\sum_{i=1}^4 A_iA_i^T = 4q^2I_{q^2}$,

   (ii) $A_1A_2^T + A_2A_1^T + A_3A_4^T + A_4A_3^T = 0$,

   (iii) $\sigma(A_1) = \sigma(A_2) = \sigma(A_3) = q^3 = -\sigma(A_4)$.

Then there exists $SBIBD(4k^2, 2k^2 + k, k^2 + k)$, $k = tq$.

**Proof.** Let

\[
\begin{align*}
B_1 &= T_1 \times A_1 + T_2 \times A_2 + T_3 \times A_3 + T_4 \times A_4, \\
B_2 &= T_1 \times A_2 + T_2 \times A_1 + T_3 \times A_4 + T_4 \times A_3, \\
B_3 &= T_1 \times A_3^T + T_2 \times A_4^T - T_3 \times A_1T - T_4 \times A_2^T, \\
B_4 &= -T_1 \times A_4^T - T_2 \times A_3^T + T_3 \times A_2^T + T_4 \times A_1^T,
\end{align*}
\]

It is easy to verify that

\[
\sum_{i=1}^4 B_iB_i^T = \left(\sum_{i=1}^4 T_iT_i^T\right) \times \left(\sum_{i=1}^4 A_iA_i^T\right) = 4k^2I_{k^2},
\]

and

\[ \sigma(B_1) = \sigma(B_2) = \sigma(B_3) = \sigma(B_4) = k^3. \]
Set
\[
H = \begin{pmatrix}
B_1 & B_2 R & -B_3 R & B_4 R \\
B_2 R & -B_1 & B_4^T R & B_3^T R \\
B_3 R & B_4^T R & B_1 & -B_2 R \\
-B_4 R & B_3^T R & B_2^T R & B_1
\end{pmatrix},
\]
where \( R = R_1 \times R_2, R_1, R_2 \) are monomial matrices of order \( t^2 \) and \( q^2 \), and \((T_1 R_i)^T = T_i R_1, (A_i R_2)^T = A_i R_2, i = 1, 2, 3, 4 \). In this case \( H H^T = 4k^2 I_{4k^2} \), and \( \sigma(H) = 2 \sum_{i=1}^{4} \sigma(B_i) = 8k^3 \). Then \( H \) is a Hadamard matrix with maximum excess. \( \frac{1}{2}(H + J) \) is a \( SBIBD(4k^2, 2k^2 + k, k^2 + k) \).

**Proposition 10.5** Let \( k = 2a_1^3 a_2^2 p_1^{a_3} p_2^{a_4} N^2, \) \( a_1, a_2, a_3, a_4 = 0 \) or \( 1, p_1 = 5(mod 8), p_2 = 3(mod 8) \) are primes and \( N \) be an arbitrary integer, then there exist \( SBIBD(4k^2, 2k^2 + k, k^2 + k) \).

**Proof.** When \( a_4 = 0 \), from lemma 10.7, the result is true. When \( a_4 = 1 \), set \( t = p_2, q = 2a_1^3 a_2^2 p_1^{a_3} N^2 \). From lemma 10.5, proposition 10.3 and theorem 10.4, the conclusion is correct.

**Remark.** Let \( k = 2a_1^3 a_2^2 p_1^{a_3} p_2^{a_4} N^2, \) \( a_1, a_2, a_3, a_4 \geq 0, p_1 \equiv 5(mod 8), p_2 \equiv 3(mod 8) \), then proposition 10.5 is still true.

Let \( a_i = 2s_i + r_i, \) where \( s_i \geq 0, 0 \leq r_i \leq 1, i = 1, 2, 3, 4 \). Then \( k = 2r_1^3 r_2^2 p_1^{a_3} p_2^{a_4} (2s_1^3 p_1^{a_3} p_2^{a_4} N^2)^2 \) satisfies the condition of proposition 10.5.

**Proposition 10.6** If \( q \equiv 1(mod 4) \) is a prime power, there exist \( SBIBD(4(7q)^2, 2(7q)^2 + 7q, (7q)^2 + 7q) \).

**Proposition 10.7** When \( p_2^{a_4} \) in proposition 10.5 is replaced by \( 7 \), the conclusion of proposition 10.5 is still true.

**Proof.** Let \( g = x \oplus 2 \) be a generator of \( GF(7^2) \), set
\[
F_i = \{ g^{16j+i}(mod x^2 \oplus 1, mod 7) : j = 0, 1, 2 \}, i = 0, 1, \ldots, 15.
\]

\[
E_1 = \{0\} \cup F_{11} \cup F_{12} \cup F_{15}, \quad E_2 = F_0 \cup F_{13}, \quad E_3 = F_5 \cup F_6, \quad E_4 = F_4 \cup F_{14},
\]
\[
E_5 = F_{10}, \quad E_6 = F_1 \cup F_2, \quad E_7 = F_7 \cup F_8, \quad E_8 = F_5 \cup F_9.
\]
It is easy to verify that
\[
\sum_{i=1}^{8} \Delta E_i = 49\theta + \sum_{i=1}^{4} \Delta(E_i, E_{i+4}).
\]
Without loss of generality, let \( g_1, \ldots, g_{49} \) be an arbitrary order on \( GF(7^2) \), set

\[
T_i = \left( t_{jk}^{(i)} \right)_{1 \leq j, k \leq 49}, \quad t_{jk}^{(i)} = \begin{cases} 
1, & \text{if } g_k \oplus g_j \in E_i, \\
-1, & \text{if } g_k \oplus g_j \in E_{i+4}, \quad i = 1, 2, 3, 4. \\
0, & \text{otherwise}.
\end{cases}
\]

The matrices \( T_1, T_2, T_3, T_4 \) are \( T \)-matrices of order 49, and

\[
\sigma(T_1) = 7^3, \quad \sigma(T_2) = \sigma(T_3) = \sigma(T_4) = 0.
\]

From theorem 10.3 and theorem 10.4, the proposition 10.6 and 10.7 are all true. This completes the proof. \( \square \)

From proposition 10.7 that for any integer \( r \geq 1 \), there exist \( SBIBD(4 \cdot 7^r, 2 \cdot 7^r + 7^r, 7^r \cdot 7^r + 7^r) \). When \( r \) is even, \( q = 7^r = 1(mod 4) \), from lemma 10.7 that the conclusion is true. When \( r \) is odd, then \( 7^{r-1} = 1(mod 4) \). In this case let \( q = 7^{r-1} \), from proposition 10.6, the conclusion is true.

From proposition 10.7, the conclusion that for any integer \( a, b \geq 1, p = 5(mod 8) \) a prime, from proposition 10.7, there exists \( SBIBD(4(7^apb)^2, 2(7^apb)^2 + 7^apb, (7^apb)^2 + 7^apb) \). From proposition 10.7, the conclusion that for \( a, b, c \geq 0, p = 5(mod 8) \) a prime, there exists \( SBIBD(4(3^apb^c)^2, 2(3^apb^c)^2 + 3^apb^c, (3^apb^c)^2 + 3^apb^c) \) is true.

**Lemma 10.8** There exist \( 4 - \{23^2, 23 \cdot 11, 23 \cdot 21\} \) SDS of order 232.

**Proof.** Let \( g = x + 2 \) be a generator on \( GF(23)^2 \). Set

\[
E_i = \{ g^{48j+i}(mod x^2 + 1, mod 23) : j = 0, 1, \ldots, 10 \}, \quad i = 0, 5, \ldots, 47.
\]

Put

\[
\begin{align*}
A_1 &= \{0\} \cup E_9 \cup E_{12} \cup E_{13} \cup E_{28} \cup E_{41} \cup E_{44} \cup E_{45}, \\
A_2 &= E_0 \cup E_{16} \cup E_{17} \cup E_{29} \cup E_{32} \cup E_{33}, \\
A_3 &= E_2 \cup E_4 \cup E_{18} \cup E_{20} \cup E_{34} \cup E_{36}, \\
A_4 &= E_3 \cup E_8 \cup E_{19} \cup E_{24} \cup E_{35} \cup E_{40}, \\
A_5 &= E_1 \cup E_5 \cup E_6 \cup E_{22} \cup E_{38}, \\
A_6 &= E_{10} \cup E_{21} \cup E_{25} \cup E_{26} \cup E_{37} \cup E_{42}, \\
A_7 &= E_7 \cup E_{11} \cup E_{23} \cup E_{27} \cup E_{39} \cup E_{43}, \\
A_8 &= E_{14} \cup E_{15} \cup E_{30} \cup E_{31} \cup E_{46} \cup E_{47}.
\end{align*}
\] (10.15)

Let \( g_1, \ldots, g_{23^2} \) be an arbitrary order on \( GF(23)^2 \). Set matrix

\[
T_i = \left( t_{jk}^{(i)} \right)_{1 \leq j, k \leq 23^2}, \quad t_{jk}^{(i)} = \begin{cases} 
1, & \text{if } g_k \oplus g_j \in A_i, \\
-1, & \text{if } g_k \oplus g_j \in A_{i+4}, \quad i = 1, 2, 3, 4, \\
0, & \text{otherwise}.
\end{cases}
\] (10.16)
10.3. Construction of SBIBD from SDS and T-matrices

Then $T_1, T_2, T_3$ and $T_4$ defined in (10.16) are $T$-matrices of order $23^2$ and

$$\sigma(T_1) = 23^3, \quad \sigma(T_2) = \sigma(T_3) = \sigma(T_4) = 0.$$  

In this case the set $\{A_i\}_{i=1}^{8}$ defined in (10.15) is a $C-$Partitions (see [161] for details). The sets

$$D_1 = A_5 \cup A_2 \cup A_3 \cup A_4, \quad D_2 = A_5 \cup A_2 \cup A_7 \cup A_8,$$

$$D_3 = A_5 \cup A_3 \cup A_6 \cup A_8, \quad D_4 = A_5 \cup A_4 \cup A_6 \cup A_7.$$  

are $4 - \{23^2; 23 \cdot 11; 23 \cdot 21\}$ SDS. This completes the proof. 

Proposition 10.8 There exists SBIBD($4 \cdot 23^2; 2 \cdot 23^2 + 23, 23^2 + 23$).

From theorem 10.1 proposition 10.8 is easily proved.

Proposition 10.9 When $7$ in proposition 10.6 be replaced by $23$, there exists SBIBD($4 \cdot (23q)^2, 2 \cdot (23q)^2 + 23q, (23q)^2 + 23q$).

Proposition 10.10 There exists SBIBD($4 \cdot 23^{2r}, 2 \cdot 23^{2r} + 23^r, 23^{2r} + 23^r$).

Proof. For any integer $r \geq 1$, when $r$ is even, $q = 23^r \equiv 1(mod 4)$, from proposition 10.6, there exists SBIBD($4 \cdot 23^{2r}, 2 \cdot 23^{2r} + 23^r, 23^{2r} + 23^r$). When $r$ is odd, then $q = 23^{r-1} \equiv 1(mod 4)$, in this case the conclusion is true.

Remark. For any integer $a, b \geq 1, p \equiv 5(mod 8)$ be a prime, there exists SBIBD($4 \cdot (23^a p^b)^2, 2 \cdot (23^a p^b)^2 + 23^a p^b, (23^a p^b)^2 + 23^a p^b$).

For any $a, b, c \geq 0, p \equiv 5(mod 8)$ a prime, there exists SBIBD($4 \cdot (3^a 23^b p^c)^2, 2 \cdot (3^a 23^b p^c)^2 + 3^a 23^b p^c, (3^a 23^b p^c)^2 + 3^a 23^b p^c$).
Chapter 11

Some Infinite families of Orthogonal Design

This chapter is base on the paper by J. Seberry and T. Xia [127]. 70 percent of the results due to the second author. In section 11.2, 11.3 some methods inspired by Kharaghani are generalized to obtain infinite family of orthogonal design in 8 variables. In section 11.4 some new orthogonal designs are given by using $T-$matrices and Williamson-type matrices.

11.1 Background

An orthogonal design of order $n$ and type $(s_1, s_2, \ldots, s_u)$ denoted by $OD(n; s_1, s_2, \ldots, s_u)$ in the variables $x_1, x_2, \ldots, x_m$, is a matrix $A$ of order $n$ with entries in the set $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ satisfies

$$AA^T = \sum_{i=1}^{u} (s_i x_i^2) I_n,$$

where $I_n$ is the identity matrix of order $n$.

A pair of matrices $A, B$ is said to be amicable (anti-amicable) if $AB^T - BA^T = 0$ ($AB^T + BA^T = 0$). Following [58] a set $\{A_1, A_2, \ldots, A_{2n}\}$ of square real matrices is said to be amicable if

$$\sum_{i=1}^{n} \left( A_{\sigma(2i-1)} A_{\sigma(2i)}^T - A_{\sigma(2i)} A_{\sigma(2i-1)}^T \right) = 0 \quad (11.1)$$

for some permutation $\sigma$ of the set $\{1, 2, \ldots, 2n\}$. For simplicity, always take $\sigma(i) = i$ unless otherwise specified. So

$$\sum_{i=1}^{n} \left( A_{2i-1} A_{2i}^T - A_{2i} A_{2i-1}^T \right) = 0. \quad (11.2)$$

Clearly a set of mutually amicable matrices is amicable, but the converse is not true in general. Throughout the paper $R_n$ denotes the back diagonal identity matrix of order $n$, $I_n$ denotes the identity matrix of order $n$. 

131
Let $A_i, i = 1, 2, 3, 4$ be circulant matrices of order $n$ with entries in $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ satisfying
\[
\sum_{i=1}^{4} A_i A_i^T = \sum_{i=1}^{u} (s_i x_i^2) I_n.
\]
Then the Goethals-Seidel array
\[
G = \begin{pmatrix}
A_1 & A_2 R_n & A_3 R_n & A_4 R_n \\
-A_2 R_n & A_1 & A_4^T R_n & -A_3^T R_n \\
-A_3 R_n & -A_4^T R_n & A_1 & A_2^T R_n \\
-A_4 R_n & A_3^T R_n & A_2^T R_n & A_1
\end{pmatrix}
\tag{11.3}
\]
is an $OD(4n; s_1, s_2, \ldots, s_u)$. See page 107 of [36] for details.

A set of matrices $\{A_1, A_2, \ldots, A_n\}$ of order $m$ with entries in $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ is said to satisfy an additive property of type $(s_1, s_2, \ldots, s_u)$ if
\[
\sum_{i=1}^{n} A_i A_i^T = \sum_{i=1}^{u} (s_i x_i^2) I_m.
\tag{11.4}
\]

Let $\{A_i\}_{i=1}^{5}$ be an amicable set of circulant matrices (or group developed or type 1) of type $(s_1, s_2, \ldots, s_u)$ and order $t$. Denote these by $8 - AS(t; s_1, \ldots, s_u, Z_t)$ or $8 - AS(t; s_1, \ldots, s_u; G)$ for group developed or type 1. In all cases, the group $G$ of the matrix is such that the extension by Seberry and Whiteman [113] of the group from circulant to type 1 allows the same extension to $R$. Then the Kharaghani array [58]
\[
H = \begin{pmatrix}
A_1 & A_2 & A_4 R_n & A_3 R_n & A_6 R_n & A_5 R_n & A_8 R_n & A_7 R_n \\
-A_2 & A_1 & A_3 R_n & -A_4 R_n & A_5 R_n & -A_6 R_n & A_7 R_n & -A_8 R_n \\
-A_4 R_n & -A_3 R_n & A_1 & A_2 & -A_8^T R_n & A_7^T R_n & A_6^T R_n & -A_5^T R_n \\
-A_3 R_n & A_4 R_n & -A_2 & A_1 & A_6^T R_n & A_5^T R_n & -A_8^T R_n & A_7^T R_n \\
-A_6 R_n & -A_5 R_n & A_7^T R_n & -A_8^T R_n & A_1 & A_2 & -A_4 R_n & A_3 R_n \\
-A_5 R_n & A_6 R_n & -A_7^T R_n & -A_8^T R_n & -A_2 & A_1 & A_4^T R_n & A_3^T R_n \\
-A_8 R_n & -A_7 R_n & -A_6^T R_n & A_5^T R_n & A_7^T R_n & -A_4 R_n & A_3 R_n & A_2 \\
-A_7 R_n & A_8 R_n & A_6^T R_n & A_5^T R_n & -A_3^T R_n & -A_4^T R_n & -A_2 & A_1
\end{pmatrix}
\tag{11.5}
\]
is an $OD(8m; s_1, s_2, \ldots, s_u)$.

The Kharaghani array has been used in a number of papers [48, 58, 47, 49, 50, 64, 65, 66] to obtain infinitely many families of orthogonal designs. Research has yet to be initiated to explore the algebraic restrictions imposed an amicable set by the required constraint.

A set $\{A_i\}_{i=1}^{4}$, of circulant matrices, is said to be a short amicable set of length $m$ and type $(u_1, u_2, u_3, u_4)$ if (11.2) and (11.4) are satisfied for $n = 4$ and $u \leq 4$. The set
11.2 Construction of \( OD(8(n + r + s); 2, 2, 2, 2k, 2k, 2k), r \geq 1, s \geq n \)

\( \{A_i\}_{i=1}^4 \), of matrices of order \( m \), is said to be a short amicable set of order \( m \) and type \((u_1, u_2, u_3, u_4)\) if (11.2) and (11.4) are satisfied for \( n = 4 \) and \( u \leq 4 \). Short amicable sets on the same group can be used in either the Goethals-Seidel array or the short Kharaghani array

\[
\begin{pmatrix}
  A & B & CR & DR \\
  -B & A & DR & -CR \\
  -CR & -DR & A & B \\
  -DR & CR & -B & A
\end{pmatrix}
\]

to form an \( OD(4m; u_1, u_2, u_3, u_4) \).

11.2 Construction of \( OD(8(n + r + s); 2, 2, 2, 2k, 2k, 2k), r \geq 1, s \geq n \)

**Theorem 11.1** Let \( X, Y \) be two circulant matrices of order \( n \) and \( XX^T + YY^T = kI_n \). Set

\[
K_1 = I_{n+r+s}, \quad K_2 = \text{circ}(0_r, X, 0_s), \quad K_3 = \text{circ}(0_r, 0_s, Y),
\]

be matrices of order \( n + r + s \), where \( 0_r \) be \( r \) zeros and \( 0_s \) denote \( s \) zeros. Let \( a, b, c, d, e, f, g, h \) be commuting variables. Then there exist a set \( \{A_i\}_{i=1}^8 \) as following

\[
\begin{align*}
A_1 &= aK_1 + fK_2 + eK_3, & A_2 &= cK_1 + hK_2 + gK_3, \\
A_3 &= aK_1 - fK_2 - eK_3, & A_4 &= cK_1 - hK_2 - gK_3, \\
A_5 &= dK_1 + gK_2 - hK_3, & A_6 &= bK_1 + eK_2 - fK_3, \\
A_7 &= dK_1 - gK_2 + hK_3, & A_8 &= bK_1 - eK_2 + fK_3.
\end{align*}
\]

that satisfies amicable property

\[
\sum_{i=1}^4 (A_{2i-1}A_{2i}^T - A_{2i}A_{2i-1}^T) = 0,
\]

and the additive property

\[
\sum_{i=1}^8 (A_iA_i^T) = 2(a^2 + b^2 + c^2 + d^2)I_{n+r+s} + 2k(e^2 + f^2 + g^2 + h^2)I_{n+r+s}.
\]

**Proof.** It is easy to establish the set \( \{A_i\}_{i=1}^8 \) defined in (11.7) satisfies the amicable property (11.8).

Suppose \( X = \text{circ}(a_0, \cdots, a_{n-1}) \), \( Y = \text{circ}(b_0, \cdots, b_{n-1}) \), then

\[
\text{Hall}(X) = \sum_{i=0}^{n-1} a_i x^i, \quad \text{Hall}(X^T) = \sum_{i=0}^{n-1} a_i x^{n-i},
\]
11.2. Construction of $OD(8(n+r+s); 2, 2, 2, 2k, 2k, 2k, 2k, 2k), r \geq 1, s \geq n$

$$\text{Hall}(Y) = \sum_{i=0}^{n-1} b_i x^i, \quad \text{Hall}(Y^T) = \sum_{i=0}^{n-1} b_i x^{n-i}.\$$

Since $XX^T + YY^T = kI_n$, then

$$\text{Hall}(XX^T + YY^T) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (a_i a_j + b_i b_j) x^{i-j} = k.$$

From the definitions of $K_1$, $K_2$, $K_3$, the Hall polynomials are

$$\text{Hall}(K_1) = \text{Hall}(K_1^T) = 1, \quad \text{Hall}(K_2) = \sum_{i=0}^{n-1} a_i x^{n-s}, \quad \text{Hall}(K_2^T) = \sum_{i=0}^{n-1} a_i x^{s-i},$$

$$\text{Hall}(K_3) = \sum_{i=0}^{n-1} b_i x^{n-s}, \quad \text{Hall}(K_3^T) = \sum_{i=0}^{n-1} b_i x^{n-i}.$$

So

$$\text{Hall}(K_2K_2^T + K_3K_3^T) = x^{n+r+s} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (a_i a_j + b_i b_j) x^{i-j} = k.$$

In this case there is

$$K_1K_1^T = I_{n+r+s}, \quad K_2K_2^T + K_3K_3^T = kI_{n+r+s},$$

so, the additive property of the set defined in (11.7) is

$$\sum_{i=1}^{8} (A_i A_i^T) = 2(a^2 + b^2 + c^2 + d^2)K_1K_1^T + 2e^2(K_2K_2^T + K_3K_3^T)$$

$$+ 2f^2(K_2^T K_2 + K_3^T K_3) + 2g^2(K_2K_2^T + K_3K_3^T) + 2h^2(K_2^T K_2 + K_3K_3^T)$$

$$= 2(a^2 + b^2 + c^2 + d^2)I_{n+r+s} + 2k(e^2 + f^2 + g^2 + h^2)I_{n+r+s}. \quad (11.10)$$

This completes the proof. \qed

**Theorem 11.2** If there exist two circulant matrices $X$ and $Y$ of order $n$, that $XX^T + YY^T = kI_n$, there exists $OD(8(n+r+s); 2, 2, 2, 2k, 2k, 2k, 2k, 2k)$, where $r \geq 1, s \geq n$.

**Proof.** Let the $K_1$, $K_2$ and $K_3$ be given by (11.6) and the set $\{A_i\}_{i=1}^{8}$ be given by (11.7). From theorem 11.1, the set $\{A_i\}_{i=1}^{8}$ satisfies the amicable property (11.8) and the additive property (11.9). The Kharaghani Array (11.5) is an $OD(8(n+r+s); 2, 2, 2, 2k, 2k, 2k, 2k, 2k)$. This completes the proof. \qed

**Corollary 11.1** There exists an $OD(8(n+r+s); 2, 2, 2, 2k, 2k, 2k, 2k, 2k)$, where $r \geq 1$, $s \geq n$, $k = 2n - 1 \equiv 1 (mod 4)$ is a prime power.
11.3. Construction of $OD(8n; 1, 1, 1, 1, \frac{1}{2}k, \frac{1}{2}k, \frac{1}{2}k, \frac{1}{2}k)$

**Proof.** Under the hypothesis of Corollary 11.1, from Theorem 5.4 there exist two circulant and symmetric matrices $X$ and $Y$ of order $n$, such that $XX + YY = kI_n$. The conclusion is followed by Theorem 11.2.

**Remark.** The necessary but not sufficient conditions exist such that $X$ and $Y$ in the theorem 11.1 and 11.2 is that $k$ is the sum of two squares (see Koukouvinos and Seberry [63], Horton and Seberry [52] for details).

When $r = 1, s = n$, there exists $OD(8(2n + 1); 2, 2, 2, 2k, 2k, 2k, 2k, 2k)$. When $r = s = n$, there exists $OD(8(3n); 2, 2, 2, 2k, 2k, 2k, 2k, 2k)$.

**Example 11.1** Let $X = (1, 1), Y = (1, -1)$. Set $r = 1, s = t = 2$. Then

$$K_1 = \text{circ}(1, 0, 0, 0, 0, 0, 0, 0),$$

$$K_2 = \text{circ}(0, 1, 0, 0, 1, -1, 0, 0),$$

$$K_3 = \text{circ}(0, 0, 0, 0, 0, 0, 0, 1),$$

and $K_1 K_1^T = I_9, K_2 K_2^T + K_3 K_3^T = 8I_9$. The matrices $\{A_i\}_{i=1}^8$ are following

$$A_1 = \text{circ}(a, b, e, b, -b, -e, e), \quad A_2 = \text{circ}(c, h, g, -g, h, -h, -g, g),$$

$$A_3 = \text{circ}(a, -f, -e, b, e, b, -b, -e, e), \quad A_4 = \text{circ}(c, -h, -g, -g, h, -h, g, g),$$

$$A_5 = \text{circ}(d, g, -h, g, -g, h, -h, h), \quad A_6 = \text{circ}(b, e, f, -f, -e, -f, e, f),$$

$$A_7 = \text{circ}(d, -g, g, h, -g, g, h, -h), \quad A_8 = \text{circ}(b, -e, f, f, -e, e, f, -f).$$

Then the Kharaghani array of (11.5) is $OD(72; 2, 2, 2, 2, 16, 16, 16, 16)$.

### 11.3 Construction of $OD(8n; 1, 1, 1, 1, \frac{1}{2}k, \frac{1}{2}k, \frac{1}{2}k, \frac{1}{2}k)$

**Theorem 11.3** Let $x_1, x_2$ be skew matrices and $x_3, x_4$ be symmetric matrices of order $n$, $\sum_{i=1}^4 x_i x_i^T = kI_n$. Set

$$K_1 = I_n, \quad K_2 = \frac{1}{2}(x_1 + x_2), \quad K_3 = \frac{1}{2}(x_1 - x_2),$$

$$K_4 = \frac{1}{2}(x_3 + x_4), \quad K_5 = \frac{1}{2}(x_3 - x_4). \quad (11.11)$$

Then the set $\{A_i\}_{i=1}^8$ as following

$$A_1 = aK_1 + eK_2 + fK_3, \quad A_2 = gK_4 + hK_5,$$

$$A_3 = dK_1 + hK_2 - gK_3, \quad A_4 = fK_4 - eK_5,$$

$$A_5 = hK_4 - gK_5, \quad A_6 = bK_1 + fK_2 - eK_3,$$

$$A_7 = eK_4 + fK_5, \quad A_8 = cK_1 + gK_2 + hK_3, \quad (11.12)$$

satisfies the amicable property (11.8) and additive property (11.9).
11.3. Construction of $OD(8n; 1, 1, 1, 1, \frac{1}{2}k, \frac{1}{2}k, \frac{1}{2}k, \frac{1}{2}k)$

**Proof.** From the supposition of the theorem 11.3 there is

$$x_1^T = -x_1, \quad x_2^T = -x_2, \quad x_3^T = x_3, \quad x_4^T = x_4.$$ 

In this case,

$$K_2^T = -K_2, \quad K_3^T = -K_3, \quad K_4^T = K_4, \quad K_5^T = K_5.$$ 

From the definition (11.12) that

$$\sum_{i=1}^{4} (A_{2i-1}A_{2i}^T - A_{2i}A_{2i-1}^T)$$

$$= agK_1K_4^T + ahK_1K_5^T + dfK_1K_4^T - deK_1K_5^T + bhK_4K_1^T$$

$$- bgK_5K_1^T + ceK_4K_1^T + cfK_5K_1^T - agK_4K_1^T - ahK_5K_1^T$$

$$- dfK_4K_1^T + deK_5K_1^T - bhK_1K_4^T + bgK_1K_5^T - ceK_1K_4^T$$

$$- cfK_1K_5^T$$

$$= agK_4 + ahK_5 + dfK_4 - deK_5 + bhK_4 - bgK_5 + ceK_4 + cfK_5$$

$$- agK_4 - ahK_5 - dfK_4 + deK_5 - bhK_4 + bgK_5 - ceK_4 - cfK_5$$

$$= 0$$

and

$$\sum_{i=1}^{8} A_iA_i^T$$

$$= aeK_1K_2^T + afK_1K_3^T + aeK_2K_1^T + afK_3K_1^T + dhK_1K_2^T$$

$$- dgK_3K_1^T + dhK_2K_1^T - dgK_3K_1^T + bhK_1K_2^T + beK_3K_1^T$$

$$+ bfK_2K_1^T - beK_3K_1^T + cgK_1K_2^T + chK_1K_3^T + cgK_2K_1^T$$

$$+ chK_3K_1^T + dfK_2K_1^T + eK_2K_2^T + g^2K_3K_3^T + a^2K_1K_1^T$$

$$+ e^2K_2K_2^T + f^2K_3K_3^T + g^2K_4K_4^T + h^2K_5K_5^T + f^2K_4K_4^T$$

$$+ e^2K_3K_5^T + h^2K_4K_4^T + g^2K_5K_5^T + b^2K_1K_1^T + f^2K_2K_2^T$$

$$+ e^2K_3K_3^T + e^2K_4K_4^T + f^2K_5K_5^T + c^2K_1K_1^T + g^2K_2K_2^T + h^2K_3K_3^T$$

$$= (a^2 + b^2 + c^2 + d^2)K_1K_1^T + (e^2 + f^2 + g^2 + h^2)(K_2K_2^T + K_3K_3^T + K_4K_4^T + K_5K_5^T)$$

$$= (a^2 + b^2 + c^2 + d^2)I_n + \frac{1}{2}(e^2 + f^2 + g^2 + h^2)(x_1x_1^T + x_2x_2^T + x_3x_3^T + x_4x_4^T)$$

$$= (a^2 + b^2 + c^2 + d^2)I_n + \frac{1}{2}(e^2 + f^2 + g^2 + h^2)kI_n.$$ 

This completes the proof. \[\Box\]

**Theorem 11.4** Suppose skew matrices $x_1, x_2$ and symmetric matrices $x_3, x_4$ of order $n$ satisfying $\sum_{i=1}^{4} x_ix_i^T = kI_n$. Then there exist $OD(8n; 1, 1, 1, 1, \frac{1}{2}k, \frac{1}{2}k, \frac{1}{2}k, \frac{1}{2}k)$. 
Proof. From theorem 11.3 there exist $K_1, K_2, K_3, K_4$ and $K_5$ as defined in (11.11) and set $\{A_i\}_{i=1}^8$ as (11.12) satisfying amicable property (11.8) and additive property (11.9). Then using the (11.12) in the Kharaghani array (11.5) gives the $OD(8n; 1,1,1,1, \frac{1}{2}k, \frac{1}{2}k, \frac{1}{2}k, \frac{1}{2}k)$ as required. The proof is completed. □

11.4 Construction of Orthogonal Designs from $T-$matrices and Williamson-type matrices

Lemma 11.1 If there exist $n \times n$ $T-$matrices $T_1, T_2, T_3$ and $T_4$, then there exists $OD(4n; n,n,n,n)$.

Proof. Let $T_1, T_2, T_3, T_4$ be $T-$matrices of order $n$, then

$$T_i T_j = T_j T_i, \quad \sum_{i=1}^4 T_i T_i^T = n I_n.$$ 

Choose the set $\{A_i\}_{i=1}^4$ such that

$$A_1 = a T_1 + b T_2 + c T_3 + d T_4, \quad A_2 = -b T_1 + a T_2 + d T_3 - c T_4,$$

$$A_3 = -c T_1 - d T_2 + a T_3 + b T_4, \quad A_4 = -d T_1 + c T_2 - b T_3 + a T_4. \quad (11.13)$$

It is easy to verify the set defined in (11.13) satisfies the additive property, such that

$$\sum_{i=1}^4 A_i A_i^T = (a^2 + b^2 + c^2 + d^2) \sum_{i=1}^4 T_i T_i^T = n(a^2 + b^2 + c^2 + d^2) I_n,$$

and amicable property, such that

$$A_1 A_2^T - A_2 A_1^T + A_3 A_4^T - A_4 A_3^T = 0.$$

The the Goethals-Seidel array (11.3) is an $OD(4n; n,n,n,n)$. □

Theorem 11.5 Let $q$ be a prime power, $q \equiv 3(mod 8)$, then there exists an $OD(4q^2; q^2, q^2, q^2, q^2).$

Proof. From lemma 11.1 and Proposition 10.3 one can easily get the conclusion of the theorem 11.5. □

From Lemma 11.1, Proposition 10.7, the proof of Proposition 10.7 and Lemma 10.8 one can easily get

Proposition 11.1 There exists $OD(4 \cdot 49; 49, 49, 49, 49)$.

Proposition 11.2 There exists an $OD(4 \cdot 23^2; 23^2, 23^2, 23^2, 23^2)$. 
Appendix A

Results on cubic homogeneous functions on $V_5$ with nonlinearity equal $12$

\begin{align*}
f_1 &= x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_2x_3x_4 \\
&\quad \oplus x_2x_4x_5 \oplus x_3x_4x_5 \\
f_2 &= x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_2x_3x_5 \\
&\quad \oplus x_2x_4x_5 \oplus x_3x_4x_5 \\
f_3 &= x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_2x_3x_4 \\
&\quad \oplus x_2x_3x_5 \oplus x_3x_4x_5 \\
f_4 &= x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_3x_4 \oplus x_1x_4x_5 \oplus x_2x_3x_5 \\
&\quad \oplus x_2x_4x_5 \oplus x_3x_4x_5 \\
f_5 &= x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_3x_4 \oplus x_1x_4x_5 \oplus x_2x_3x_4 \\
&\quad \oplus x_2x_3x_5 \oplus x_3x_4x_5 \\
f_6 &= x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_3x_5 \oplus x_1x_4x_5 \oplus x_2x_3x_4 \\
&\quad \oplus x_2x_4x_5 \oplus x_3x_4x_5 \\
f_7 &= x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_1x_4x_5 \oplus x_2x_3x_4 \\
&\quad \oplus x_2x_3x_5 \oplus x_3x_4x_5 \\
f_8 &= x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_1x_4x_5 \oplus x_2x_3x_5 \\
&\quad \oplus x_2x_4x_5 \oplus x_3x_4x_5 \\
f_9 &= x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_5 \oplus x_1x_4x_5 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \\
&\quad \oplus x_2x_4x_5 \oplus x_3x_4x_5 \\
f_{10} &= x_1x_2x_3 \oplus x_1x_2x_5 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_1x_4x_5 \oplus x_2x_3x_4 \\
&\quad \oplus x_2x_3x_5 \oplus x_2x_4x_5 \\
f_{11} &= x_1x_2x_3 \oplus x_1x_2x_5 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_1x_4x_5 \oplus x_2x_3x_4 \\
&\quad \oplus x_2x_4x_5 \oplus x_3x_4x_5 
\end{align*}
$$f_{12} = x_1 x_2 x_3 \oplus x_1 x_2 x_5 \oplus x_1 x_3 x_4 \oplus x_1 x_4 x_5 \oplus x_2 x_3 x_4 \oplus x_2 x_3 x_5 \oplus x_2 x_4 x_5 \oplus x_3 x_4 x_5$$

$$f_{13} = x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_3 x_4 \oplus x_1 x_3 x_5 \oplus x_1 x_4 x_5 \oplus x_2 x_3 x_4 \oplus x_2 x_3 x_5 \oplus x_2 x_4 x_5$$

$$f_{14} = x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_3 x_4 \oplus x_1 x_3 x_5 \oplus x_1 x_4 x_5 \oplus x_2 x_3 x_4 \oplus x_2 x_3 x_5 \oplus x_3 x_4 x_5$$

$$f_{15} = x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_3 x_4 \oplus x_1 x_3 x_5 \oplus x_2 x_3 x_4 \oplus x_2 x_3 x_5 \oplus x_2 x_4 x_5 \oplus x_3 x_4 x_5$$
Appendix B

Some results on cubic homogeneous functions on $V_7$ with nonlinearity equal 56

(I) Cubic homogeneous Boolean functions on $V_7$ with 20 terms

\begin{align*}
f_1 &= x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_4 \\
& \quad \oplus x_1x_3x_5 \oplus x_1x_3x_6 \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_2x_3x_4 \\
& \quad \oplus x_2x_3x_5 \oplus x_2x_4x_5 \oplus x_2x_5x_6 \oplus x_2x_6x_7 \oplus x_3x_4x_6 \oplus x_3x_5x_6 \\
& \quad \oplus x_3x_5x_7 \oplus x_4x_5x_6 \\
f_2 &= x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_4 \\
& \quad \oplus x_1x_3x_5 \oplus x_1x_3x_6 \oplus x_1x_3x_7 \oplus x_1x_4x_6 \oplus x_1x_6x_7 \oplus x_2x_3x_4 \\
& \quad \oplus x_2x_3x_6 \oplus x_2x_4x_5 \oplus x_2x_4x_7 \oplus x_2x_6x_7 \oplus x_3x_4x_5 \oplus x_3x_4x_7 \\
& \quad \oplus x_3x_6x_7 \oplus x_4x_6x_7 \\
f_3 &= x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_4 \\
& \quad \oplus x_1x_3x_5 \oplus x_1x_3x_6 \oplus x_1x_3x_7 \oplus x_1x_4x_6 \oplus x_1x_4x_7 \oplus x_2x_3x_4 \\
& \quad \oplus x_2x_3x_5 \oplus x_2x_4x_5 \oplus x_2x_5x_6 \oplus x_2x_6x_7 \oplus x_3x_4x_6 \oplus x_3x_5x_6 \\
& \quad \oplus x_4x_5x_6 \oplus x_4x_5x_7 \\
f_4 &= x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_4 \\
& \quad \oplus x_1x_3x_5 \oplus x_1x_3x_6 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_6x_7 \oplus x_2x_3x_5 \\
& \quad \oplus x_2x_3x_7 \oplus x_2x_4x_5 \oplus x_2x_5x_7 \oplus x_3x_4x_6 \oplus x_3x_5x_7 \oplus x_4x_5x_7 \\
& \quad \oplus x_4x_6x_7 \oplus x_5x_6x_7 \\
f_5 &= x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_4 \\
& \quad \oplus x_1x_3x_5 \oplus x_1x_3x_6 \oplus x_1x_4x_7 \oplus x_1x_6x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \\
& \quad \oplus x_2x_4x_6 \oplus x_2x_4x_7 \oplus x_2x_5x_6 \oplus x_3x_4x_5 \oplus x_3x_4x_6 \oplus x_3x_4x_7 \\
& \quad \oplus x_3x_5x_6 \oplus x_4x_5x_6
\end{align*}
\[
f_6 = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4x_7 \oplus x_1x_5x_7 \oplus x_1x_6x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3x_6 \oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_4x_7 \oplus x_3x_5x_6 \oplus x_3x_5x_7 \oplus x_3x_6x_7 \oplus x_3x_7x_6 \oplus x_4x_5x_6 \oplus x_4x_5x_7 \oplus x_4x_6x_7 \oplus x_5x_6x_7
\]

\[
f_7 = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4x_7 \oplus x_1x_5x_6 \oplus x_1x_5x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3x_6 \oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_4x_7 \oplus x_3x_5x_6 \oplus x_3x_5x_7 \oplus x_3x_6x_6 \oplus x_3x_6x_7 \oplus x_3x_7x_6 \oplus x_4x_5x_7 \oplus x_4x_6x_7 \oplus x_5x_6x_7
\]

\[
f_8 = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4x_7 \oplus x_1x_5x_6 \oplus x_1x_5x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3x_6 \oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_4x_7 \oplus x_3x_5x_6 \oplus x_3x_5x_7 \oplus x_3x_6x_6 \oplus x_3x_6x_7 \oplus x_3x_7x_6 \oplus x_4x_5x_7 \oplus x_4x_6x_7 \oplus x_5x_6x_7
\]

\[
f_9 = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4x_7 \oplus x_1x_5x_6 \oplus x_1x_5x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3x_6 \oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_4x_7 \oplus x_3x_5x_6 \oplus x_3x_5x_7 \oplus x_3x_6x_6 \oplus x_3x_6x_7 \oplus x_3x_7x_6 \oplus x_4x_5x_7 \oplus x_4x_6x_7 \oplus x_5x_6x_7
\]

\[
f_{10} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4x_7 \oplus x_1x_5x_6 \oplus x_1x_5x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3x_6 \oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_4x_7 \oplus x_3x_5x_6 \oplus x_3x_5x_7 \oplus x_3x_6x_6 \oplus x_3x_6x_7 \oplus x_3x_7x_6 \oplus x_4x_5x_7 \oplus x_4x_6x_7 \oplus x_5x_6x_7
\]

\[
f_{11} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_5 \oplus x_1x_3x_6 \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4x_7 \oplus x_1x_5x_6 \oplus x_1x_5x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3x_6 \oplus x_2x_4x_7 \oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_4x_7 \oplus x_3x_5x_6 \oplus x_3x_5x_7 \oplus x_3x_6x_7 \oplus x_4x_5x_7 \oplus x_4x_6x_7 \oplus x_5x_6x_7
\]

\[
f_{12} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_5 \oplus x_1x_3x_6 \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4x_7 \oplus x_1x_5x_6 \oplus x_1x_5x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3x_6 \oplus x_2x_4x_7 \oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_4x_7 \oplus x_3x_5x_7 \oplus x_3x_6x_7 \oplus x_4x_5x_7 \oplus x_4x_6x_7 \oplus x_5x_6x_7
\]

\[
f_{13} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_5 \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4x_7 \oplus x_1x_6x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_6 \oplus x_2x_4x_6 \oplus x_2x_4x_7 \oplus x_2x_6x_7 \oplus x_3x_4x_6 \oplus x_3x_4x_7\]
\[ f_{14} = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_2 x_5 + x_1 x_2 x_6 + x_1 x_2 x_7 + x_1 x_3 x_5 \]
\[ + x_1 x_3 x_7 + x_1 x_4 x_5 + x_1 x_4 x_6 + x_1 x_4 x_7 + x_1 x_5 x_7 + x_2 x_3 x_4 \]
\[ + x_2 x_3 x_6 + x_2 x_4 x_6 + x_2 x_4 x_7 + x_2 x_6 x_7 + x_3 x_4 x_6 + x_3 x_4 x_7 \]
\[ + x_3 x_6 x_7 + x_4 x_5 x_6 \]

\[ f_{15} = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_2 x_5 + x_1 x_2 x_6 + x_1 x_2 x_7 + x_1 x_3 x_5 \]
\[ + x_1 x_3 x_7 + x_1 x_4 x_5 + x_1 x_4 x_6 + x_1 x_4 x_7 + x_1 x_5 x_7 + x_2 x_3 x_4 \]
\[ + x_2 x_3 x_6 + x_2 x_4 x_6 + x_2 x_4 x_7 + x_2 x_6 x_7 + x_3 x_5 x_6 + x_3 x_5 x_7 \]
\[ + x_3 x_6 x_7 + x_4 x_5 x_6 \]

\[ f_{16} = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_2 x_5 + x_1 x_2 x_6 + x_1 x_2 x_7 + x_1 x_3 x_5 \]
\[ + x_1 x_3 x_7 + x_1 x_4 x_5 + x_1 x_4 x_6 + x_1 x_4 x_7 + x_1 x_5 x_7 + x_2 x_3 x_4 \]
\[ + x_2 x_3 x_6 + x_2 x_4 x_5 + x_2 x_4 x_6 + x_2 x_4 x_7 + x_2 x_5 x_6 + x_3 x_5 x_7 \]
\[ + x_3 x_6 x_7 + x_4 x_5 x_6 \]

\[ f_{17} = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_2 x_5 + x_1 x_2 x_6 + x_1 x_2 x_7 + x_1 x_3 x_5 \]
\[ + x_1 x_3 x_7 + x_1 x_4 x_5 + x_1 x_4 x_6 + x_1 x_4 x_7 + x_1 x_5 x_7 + x_2 x_3 x_4 \]
\[ + x_2 x_3 x_6 + x_2 x_4 x_5 + x_2 x_4 x_6 + x_2 x_4 x_7 + x_2 x_5 x_6 + x_3 x_5 x_7 \]
\[ + x_3 x_6 x_7 + x_4 x_5 x_6 \]

\[ f_{18} = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_2 x_5 + x_1 x_2 x_6 + x_1 x_2 x_7 + x_1 x_3 x_5 \]
\[ + x_1 x_3 x_7 + x_1 x_4 x_5 + x_1 x_4 x_6 + x_1 x_4 x_7 + x_1 x_5 x_7 + x_2 x_3 x_4 \]
\[ + x_2 x_3 x_6 + x_2 x_4 x_5 + x_2 x_4 x_6 + x_2 x_4 x_7 + x_2 x_5 x_6 + x_3 x_5 x_7 \]
\[ + x_3 x_6 x_7 + x_4 x_5 x_6 \]

\[ f_{19} = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_2 x_5 + x_1 x_2 x_6 + x_1 x_2 x_7 + x_1 x_3 x_5 \]
\[ + x_1 x_3 x_7 + x_1 x_4 x_5 + x_1 x_4 x_6 + x_1 x_4 x_7 + x_1 x_5 x_7 + x_2 x_3 x_4 \]
\[ + x_2 x_3 x_6 + x_2 x_4 x_5 + x_2 x_4 x_6 + x_2 x_4 x_7 + x_2 x_5 x_6 + x_3 x_5 x_7 \]
\[ + x_3 x_6 x_7 + x_4 x_5 x_6 \]

\[ f_{20} = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_2 x_5 + x_1 x_2 x_6 + x_1 x_2 x_7 + x_1 x_3 x_5 \]
\[ + x_1 x_3 x_7 + x_1 x_4 x_5 + x_1 x_4 x_6 + x_1 x_4 x_7 + x_1 x_5 x_7 + x_2 x_3 x_4 \]
\[ + x_2 x_3 x_6 + x_2 x_4 x_5 + x_2 x_4 x_6 + x_2 x_4 x_7 + x_2 x_5 x_6 + x_3 x_5 x_7 \]
\[ + x_3 x_6 x_7 + x_4 x_5 x_6 \]

\[ f_{21} = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_2 x_5 + x_1 x_2 x_6 + x_1 x_2 x_7 + x_1 x_3 x_5 \]
\[ + x_1 x_3 x_7 + x_1 x_4 x_5 + x_1 x_4 x_6 + x_1 x_4 x_7 + x_1 x_5 x_7 + x_2 x_3 x_7 \]
\[ f_{22} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_5 \]
\[ \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4x_7 \oplus x_1x_6x_7 \oplus x_2x_3x_7 \]
\[ \oplus x_2x_4x_6 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \oplus x_3x_4x_5 \oplus x_3x_5x_7 \oplus x_3x_6x_7 \]
\[ \oplus x_4x_5x_7 \oplus x_4x_6x_7 \]

\[ f_{23} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_5 \]
\[ \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4x_7 \oplus x_1x_6x_7 \oplus x_2x_4x_5 \]
\[ \oplus x_2x_4x_6 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \oplus x_3x_4x_5 \oplus x_3x_5x_6 \oplus x_3x_6x_7 \]
\[ \oplus x_4x_5x_6 \oplus x_4x_6x_7 \]

\[ f_{24} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_5 \]
\[ \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4x_7 \oplus x_1x_6x_7 \oplus x_2x_4x_6 \]
\[ \oplus x_2x_4x_7 \oplus x_2x_5x_6 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \oplus x_3x_4x_5 \oplus x_3x_5x_6 \]
\[ \oplus x_3x_6x_7 \oplus x_4x_5x_6 \]

\[ f_{25} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_5 \]
\[ \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4x_7 \oplus x_1x_6x_7 \oplus x_2x_4x_6 \]
\[ \oplus x_2x_4x_7 \oplus x_2x_5x_6 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \oplus x_3x_4x_5 \oplus x_3x_5x_6 \]
\[ \oplus x_3x_6x_7 \oplus x_4x_5x_6 \]

\[ f_{26} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_5 \]
\[ \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \]
\[ \oplus x_2x_3x_6 \oplus x_2x_4x_6 \oplus x_2x_5x_6 \oplus x_3x_4x_5 \oplus x_3x_4x_6 \oplus x_4x_5x_6 \]
\[ \oplus x_4x_6x_7 \oplus x_5x_6x_7 \]

\[ f_{27} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_5 \]
\[ \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \]
\[ \oplus x_2x_3x_7 \oplus x_2x_4x_5 \oplus x_2x_5x_6 \oplus x_2x_5x_7 \oplus x_3x_4x_5 \oplus x_3x_4x_7 \]
\[ \oplus x_4x_5x_7 \oplus x_5x_6x_7 \]

\[ f_{28} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_5 \]
\[ \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \]
\[ \oplus x_2x_3x_7 \oplus x_2x_4x_5 \oplus x_2x_5x_6 \oplus x_2x_5x_7 \oplus x_3x_4x_7 \oplus x_3x_5x_7 \]
\[ \oplus x_4x_5x_6 \oplus x_4x_5x_7 \]

\[ f_{29} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_5 \]
\[ f_{30} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_5 \]

\[ f_1 = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_5 \]

\[ f_2 = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_5 \]

\[ f_3 = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_5 \]

\[ f_4 = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_5 \]

\[ f_5 = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_5 \]

\[ f_6 = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_5 \]

(II) Cubic homogeneous Boolean functions on $V_7$ with 22 terms
\( f_7 = x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_2x_6 + x_1x_2x_7 + x_1x_3x_6 \\
+ x_1x_3x_7 + x_1x_4x_5 + x_1x_5x_6 + x_1x_5x_7 + x_2x_3x_4 + x_2x_3x_6 \\
+ x_2x_4x_5 + x_2x_4x_7 + x_2x_5x_6 + x_2x_6x_7 + x_3x_4x_5 + x_3x_5x_6 \\
+ x_3x_5x_7 + x_3x_6x_7 + x_4x_5x_6 + x_5x_6x_7 \\
+ x_5x_7 = x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_2x_6 + x_1x_2x_7 + x_1x_3x_6 \\
+ x_1x_3x_7 + x_1x_4x_5 + x_1x_5x_6 + x_1x_5x_7 + x_2x_3x_4 + x_2x_3x_6 \\
+ x_2x_4x_5 + x_2x_4x_7 + x_2x_5x_6 + x_2x_6x_7 + x_3x_4x_5 + x_3x_5x_6 \\
+ x_3x_5x_7 + x_3x_6x_7 + x_4x_5x_6 + x_5x_6x_7 \\
+ x_6 = x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_2x_6 + x_1x_2x_7 + x_1x_3x_6 \\
+ x_1x_3x_7 + x_1x_4x_5 + x_1x_5x_6 + x_1x_5x_7 + x_2x_3x_4 + x_2x_3x_6 \\
+ x_2x_4x_5 + x_2x_4x_7 + x_2x_5x_6 + x_2x_6x_7 + x_3x_4x_5 + x_3x_5x_6 \\
+ x_3x_5x_7 + x_3x_6x_7 + x_4x_5x_6 + x_5x_6x_7 \\
+ x_6 = x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_2x_6 + x_1x_2x_7 + x_1x_3x_6 \\
+ x_1x_3x_7 + x_1x_4x_5 + x_1x_5x_6 + x_1x_5x_7 + x_2x_3x_4 + x_2x_3x_6 \\
+ x_2x_4x_5 + x_2x_4x_7 + x_2x_5x_6 + x_2x_6x_7 + x_3x_4x_5 + x_3x_5x_6 \\
+ x_3x_5x_7 + x_3x_6x_7 + x_4x_5x_6 + x_5x_6x_7 \\
+ x_6 = x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_2x_6 + x_1x_2x_7 + x_1x_3x_6 \\
+ x_1x_3x_7 + x_1x_4x_5 + x_1x_5x_6 + x_1x_5x_7 + x_2x_3x_4 + x_2x_3x_6 \\
+ x_2x_4x_5 + x_2x_4x_7 + x_2x_5x_6 + x_2x_6x_7 + x_3x_4x_5 + x_3x_5x_6 \\
+ x_3x_5x_7 + x_3x_6x_7 + x_4x_5x_6 + x_5x_6x_7 

f_8 = x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_2x_6 + x_1x_2x_7 + x_1x_3x_6 \\
+ x_1x_3x_7 + x_1x_4x_5 + x_1x_5x_6 + x_1x_5x_7 + x_2x_3x_4 + x_2x_3x_6 \\
+ x_2x_4x_5 + x_2x_4x_7 + x_2x_5x_6 + x_2x_6x_7 + x_3x_4x_5 + x_3x_5x_6 \\
+ x_3x_5x_7 + x_3x_6x_7 + x_4x_5x_6 + x_5x_6x_7 

f_9 = x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_2x_6 + x_1x_2x_7 + x_1x_3x_6 \\
+ x_1x_3x_7 + x_1x_4x_5 + x_1x_5x_6 + x_1x_5x_7 + x_2x_3x_4 + x_2x_3x_6 \\
+ x_2x_4x_5 + x_2x_4x_7 + x_2x_5x_6 + x_2x_6x_7 + x_3x_4x_5 + x_3x_5x_6 \\
+ x_3x_5x_7 + x_3x_6x_7 + x_4x_5x_6 + x_5x_6x_7 

f_10 = x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_2x_6 + x_1x_2x_7 + x_1x_3x_6 \\
+ x_1x_3x_7 + x_1x_4x_5 + x_1x_5x_6 + x_1x_5x_7 + x_2x_3x_4 + x_2x_3x_6 \\
+ x_2x_4x_5 + x_2x_4x_7 + x_2x_5x_6 + x_2x_6x_7 + x_3x_4x_5 + x_3x_5x_6 \\
+ x_3x_5x_7 + x_3x_6x_7 + x_4x_5x_6 + x_5x_6x_7 

f_11 = x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_2x_6 + x_1x_2x_7 + x_1x_3x_6 \\
+ x_1x_3x_7 + x_1x_4x_5 + x_1x_5x_6 + x_1x_5x_7 + x_2x_3x_4 + x_2x_3x_6 \\
+ x_2x_4x_5 + x_2x_4x_7 + x_2x_5x_6 + x_2x_6x_7 + x_3x_4x_5 + x_3x_5x_6 \\
+ x_3x_5x_7 + x_3x_6x_7 + x_4x_5x_6 + x_5x_6x_7 

f_12 = x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_2x_6 + x_1x_2x_7 + x_1x_3x_6 \\
+ x_1x_3x_7 + x_1x_4x_5 + x_1x_5x_6 + x_1x_5x_7 + x_2x_3x_4 + x_2x_3x_6 \\
+ x_2x_4x_5 + x_2x_4x_7 + x_2x_5x_6 + x_2x_6x_7 + x_3x_4x_5 + x_3x_5x_6 \\
+ x_3x_5x_7 + x_3x_6x_7 + x_4x_5x_6 + x_5x_6x_7 

f_13 = x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_2x_6 + x_1x_2x_7 + x_1x_3x_6 \\
+ x_1x_3x_7 + x_1x_4x_5 + x_1x_4x_6 + x_1x_4x_7 + x_1x_6x_7 + x_2x_3x_4 \\
+ x_2x_3x_5 + x_2x_3x_6 + x_2x_4x_5 + x_2x_5x_6 + x_2x_6x_7 + x_3x_4x_5 \\
+ x_3x_6x_7 + x_4x_5x_6 + x_4x_5x_7 + x_4x_6x_7 \)
\[ f_{14} = x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_6 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_5 \]
\[ \oplus x_1 x_3 x_7 \oplus x_1 x_4 x_5 \oplus x_1 x_4 x_7 \oplus x_1 x_5 x_7 \oplus x_1 x_6 x_7 \oplus x_2 x_3 x_6 \]
\[ \oplus x_2 x_3 x_7 \oplus x_2 x_5 x_6 \oplus x_2 x_5 x_7 \oplus x_2 x_6 x_7 \oplus x_3 x_4 x_5 \oplus x_3 x_4 x_6 \]
\[ \oplus x_3 x_4 x_7 \oplus x_3 x_5 x_7 \oplus x_4 x_5 x_6 \oplus x_4 x_6 x_7 \]

\[ f_{15} = x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_6 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_5 \]
\[ \oplus x_1 x_4 x_5 \oplus x_1 x_4 x_7 \oplus x_1 x_5 x_6 \oplus x_1 x_5 x_7 \oplus x_2 x_3 x_5 \oplus x_2 x_3 x_6 \]
\[ \oplus x_2 x_3 x_7 \oplus x_2 x_5 x_7 \oplus x_2 x_6 x_7 \oplus x_3 x_4 x_5 \oplus x_3 x_4 x_6 \oplus x_3 x_5 x_6 \]
\[ \oplus x_3 x_6 x_7 \oplus x_4 x_5 x_7 \oplus x_4 x_6 x_7 \oplus x_5 x_6 x_7 \]

\[ f_{16} = x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_6 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_6 \]
\[ \oplus x_1 x_3 x_7 \oplus x_1 x_4 x_5 \oplus x_1 x_5 x_6 \oplus x_1 x_5 x_7 \oplus x_2 x_3 x_4 \oplus x_2 x_3 x_6 \]
\[ \oplus x_2 x_4 x_5 \oplus x_2 x_4 x_7 \oplus x_2 x_5 x_6 \oplus x_2 x_6 x_7 \oplus x_3 x_4 x_5 \oplus x_3 x_5 x_6 \]
\[ \oplus x_3 x_5 x_7 \oplus x_3 x_6 x_7 \oplus x_4 x_5 x_6 \oplus x_5 x_6 x_7 \]

\[ f_{17} = x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_6 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_6 \]
\[ \oplus x_1 x_3 x_7 \oplus x_1 x_4 x_5 \oplus x_1 x_5 x_6 \oplus x_1 x_5 x_7 \oplus x_2 x_3 x_4 \oplus x_2 x_3 x_6 \]
\[ \oplus x_2 x_4 x_5 \oplus x_2 x_4 x_7 \oplus x_2 x_5 x_6 \oplus x_2 x_6 x_7 \oplus x_3 x_4 x_5 \oplus x_3 x_5 x_6 \]
\[ \oplus x_4 x_5 x_6 \oplus x_4 x_5 x_7 \oplus x_4 x_6 x_7 \oplus x_5 x_6 x_7 \]

\[ f_{18} = x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_6 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_6 \]
\[ \oplus x_1 x_3 x_7 \oplus x_1 x_4 x_5 \oplus x_1 x_5 x_6 \oplus x_1 x_5 x_7 \oplus x_2 x_3 x_4 \oplus x_2 x_3 x_6 \]
\[ \oplus x_2 x_4 x_5 \oplus x_2 x_4 x_7 \oplus x_2 x_5 x_6 \oplus x_2 x_6 x_7 \oplus x_3 x_4 x_5 \oplus x_3 x_5 x_6 \]
\[ \oplus x_4 x_5 x_6 \oplus x_4 x_5 x_7 \oplus x_4 x_6 x_7 \oplus x_5 x_6 x_7 \]

\[ f_{19} = x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_6 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_6 \]
\[ \oplus x_1 x_3 x_7 \oplus x_1 x_4 x_5 \oplus x_1 x_5 x_6 \oplus x_1 x_5 x_7 \oplus x_2 x_3 x_4 \oplus x_2 x_3 x_6 \]
\[ \oplus x_2 x_4 x_5 \oplus x_2 x_4 x_7 \oplus x_2 x_5 x_6 \oplus x_2 x_6 x_7 \oplus x_3 x_4 x_5 \oplus x_3 x_5 x_6 \]
\[ \oplus x_3 x_5 x_7 \oplus x_3 x_6 x_7 \oplus x_4 x_5 x_7 \oplus x_5 x_6 x_7 \]

\[ f_{20} = x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_6 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_6 \]
\[ \oplus x_1 x_3 x_7 \oplus x_1 x_4 x_5 \oplus x_1 x_5 x_6 \oplus x_1 x_5 x_7 \oplus x_2 x_3 x_4 \oplus x_2 x_3 x_6 \]
\[ \oplus x_2 x_4 x_5 \oplus x_2 x_4 x_7 \oplus x_2 x_5 x_6 \oplus x_2 x_6 x_7 \oplus x_3 x_4 x_6 \oplus x_3 x_4 x_7 \oplus x_3 x_5 x_7 \]
\[ \oplus x_4 x_5 x_6 \oplus x_4 x_5 x_7 \oplus x_4 x_6 x_7 \oplus x_5 x_6 x_7 \]

\[ f_{21} = x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_6 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_6 \]
\[ \oplus x_1 x_3 x_7 \oplus x_1 x_4 x_5 \oplus x_1 x_5 x_6 \oplus x_1 x_5 x_7 \oplus x_2 x_3 x_4 \oplus x_2 x_3 x_7 \]
\[ \oplus x_2 x_4 x_5 \oplus x_2 x_4 x_6 \oplus x_2 x_5 x_7 \oplus x_2 x_6 x_7 \oplus x_3 x_4 x_5 \oplus x_3 x_5 x_6 \]
\[ f_{22} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_6 \]
\[ \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_5x_6 \oplus x_1x_5x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_7 \]
\[ \oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \oplus x_3x_4x_5 \oplus x_3x_5x_7 \]
\[ \oplus x_4x_5x_6 \oplus x_4x_5x_7 \oplus x_4x_6x_7 \oplus x_5x_6x_7 \]

\[ f_{23} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_6 \]
\[ \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_5x_6 \oplus x_1x_5x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_7 \]
\[ \oplus x_2x_4x_7 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \oplus x_3x_4x_6 \oplus x_3x_4x_7 \oplus x_3x_5x_6 \]
\[ \oplus x_3x_5x_7 \oplus x_3x_6x_7 \oplus x_4x_5x_6 \oplus x_5x_6x_7 \]

\[ f_{24} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_6 \]
\[ \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_5x_6 \oplus x_1x_5x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_7 \]
\[ \oplus x_2x_4x_7 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \oplus x_3x_4x_6 \oplus x_3x_4x_7 \oplus x_3x_5x_6 \]
\[ \oplus x_4x_5x_6 \oplus x_4x_5x_7 \oplus x_4x_6x_7 \oplus x_5x_6x_7 \]

\[ f_{25} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_6 \]
\[ \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_5x_6 \oplus x_1x_5x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_6 \]
\[ \oplus x_2x_4x_5 \oplus x_2x_4x_7 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \oplus x_3x_4x_5 \oplus x_3x_5x_7 \]
\[ \oplus x_3x_5x_7 \oplus x_3x_6x_7 \oplus x_4x_5x_7 \oplus x_5x_6x_7 \]

\[ f_{26} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_6 \]
\[ \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_5x_6 \oplus x_1x_5x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_6 \]
\[ \oplus x_2x_4x_5 \oplus x_2x_4x_7 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \oplus x_3x_4x_5 \oplus x_3x_5x_7 \]
\[ \oplus x_3x_5x_7 \oplus x_3x_6x_7 \oplus x_4x_5x_7 \oplus x_5x_6x_7 \]

\[ f_{27} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_6 \]
\[ \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_5x_6 \oplus x_1x_5x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_6 \]
\[ \oplus x_2x_4x_5 \oplus x_2x_4x_7 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \oplus x_3x_4x_5 \oplus x_3x_5x_7 \]
\[ \oplus x_3x_5x_7 \oplus x_3x_6x_7 \oplus x_4x_5x_6 \oplus x_5x_6x_7 \]

\[ f_{28} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_6 \]
\[ \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_5x_6 \oplus x_1x_5x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_7 \]
\[ \oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_5x_6 \oplus x_2x_5x_7 \oplus x_3x_4x_5 \oplus x_3x_5x_6 \]
\[ \oplus x_3x_5x_7 \oplus x_3x_6x_7 \oplus x_4x_5x_6 \oplus x_5x_6x_7 \]

\[ f_{29} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_6 \]
\[ \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_5x_6 \oplus x_1x_5x_7 \oplus x_2x_3x_5 \oplus x_2x_3x_7 \]
Cubic homogeneous Boolean functions on $V_7$ with 24 terms

\[ f_1 = x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_6 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_4 \]
\[ \oplus x_1 x_3 x_5 \oplus x_1 x_3 x_6 \oplus x_1 x_3 x_7 \oplus x_1 x_4 x_5 \oplus x_1 x_4 x_6 \oplus x_2 x_3 x_5 \]
\[ \oplus x_2 x_4 x_5 \oplus x_2 x_4 x_6 \oplus x_2 x_5 x_7 \oplus x_2 x_6 x_7 \oplus x_3 x_5 x_6 \]
\[ \oplus x_3 x_5 x_7 \oplus x_3 x_6 x_7 \oplus x_4 x_5 x_6 \oplus x_4 x_5 x_7 \oplus x_5 x_6 x_7 \]

\[ f_2 = x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_6 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_4 \]
\[ \oplus x_1 x_3 x_5 \oplus x_1 x_3 x_6 \oplus x_1 x_3 x_7 \oplus x_1 x_4 x_5 \oplus x_1 x_4 x_6 \oplus x_2 x_3 x_5 \]
\[ \oplus x_2 x_4 x_5 \oplus x_2 x_4 x_6 \oplus x_2 x_5 x_7 \oplus x_2 x_6 x_7 \oplus x_3 x_4 x_6 \]
\[ \oplus x_3 x_5 x_7 \oplus x_3 x_6 x_7 \oplus x_4 x_5 x_6 \oplus x_4 x_5 x_7 \oplus x_5 x_6 x_7 \]

\[ f_3 = x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_6 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_4 \]
\[ \oplus x_1 x_3 x_5 \oplus x_1 x_3 x_6 \oplus x_1 x_4 x_5 \oplus x_1 x_4 x_6 \oplus x_1 x_4 x_7 \oplus x_2 x_3 x_5 \]
\[ \oplus x_2 x_3 x_6 \oplus x_2 x_4 x_5 \oplus x_2 x_4 x_6 \oplus x_2 x_5 x_7 \oplus x_2 x_6 x_7 \oplus x_3 x_4 x_6 \]
\[ \oplus x_3 x_4 x_7 \oplus x_3 x_5 x_6 \oplus x_3 x_6 x_7 \oplus x_4 x_5 x_6 \oplus x_4 x_5 x_7 \oplus x_5 x_6 x_7 \]

\[ f_4 = x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_6 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_4 \]
\[ \oplus x_1 x_3 x_5 \oplus x_1 x_3 x_6 \oplus x_1 x_4 x_5 \oplus x_1 x_4 x_6 \oplus x_1 x_4 x_7 \oplus x_2 x_3 x_5 \]
\[ \oplus x_2 x_3 x_6 \oplus x_2 x_4 x_5 \oplus x_2 x_4 x_6 \oplus x_2 x_5 x_7 \oplus x_2 x_6 x_7 \oplus x_3 x_4 x_6 \]
\[ \oplus x_3 x_4 x_7 \oplus x_3 x_5 x_6 \oplus x_3 x_6 x_7 \oplus x_4 x_5 x_6 \oplus x_4 x_5 x_7 \oplus x_5 x_6 x_7 \]

\[ f_5 = x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_6 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_4 \]
\[ \oplus x_1 x_3 x_5 \oplus x_1 x_3 x_6 \oplus x_1 x_4 x_5 \oplus x_1 x_4 x_6 \oplus x_1 x_4 x_7 \oplus x_2 x_3 x_6 \]
\[ \oplus x_2 x_3 x_7 \oplus x_2 x_4 x_5 \oplus x_2 x_4 x_6 \oplus x_2 x_5 x_7 \oplus x_3 x_4 x_5 \]
\[ \oplus x_3 x_4 x_6 \oplus x_3 x_5 x_6 \oplus x_3 x_5 x_7 \oplus x_4 x_5 x_7 \oplus x_4 x_6 x_7 \]

\[ f_6 = x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_6 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_4 \]
\[ \oplus x_1 x_3 x_5 \oplus x_1 x_3 x_6 \oplus x_1 x_4 x_5 \oplus x_1 x_4 x_6 \oplus x_1 x_4 x_7 \oplus x_2 x_3 x_5 \]
\begin{align*}
  f_7 &= x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_6 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_4 \\
  &\quad \oplus x_1 x_3 x_6 \oplus x_1 x_3 x_7 \oplus x_1 x_4 x_5 \oplus x_1 x_4 x_6 \oplus x_1 x_4 x_7 \oplus x_2 x_3 x_5 \\
  &\quad \oplus x_2 x_3 x_7 \oplus x_2 x_4 x_6 \oplus x_2 x_4 x_7 \oplus x_2 x_5 x_6 \oplus x_2 x_5 x_7 \oplus x_3 x_4 x_5 \\
  &\quad \oplus x_3 x_4 x_6 \oplus x_3 x_4 x_7 \oplus x_3 x_5 x_6 \oplus x_4 x_5 x_6 \oplus x_4 x_5 x_7 \oplus x_5 x_6 x_7 \\
  f_8 &= x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_6 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_4 \\
  &\quad \oplus x_1 x_3 x_6 \oplus x_1 x_3 x_7 \oplus x_1 x_4 x_5 \oplus x_1 x_4 x_6 \oplus x_1 x_4 x_7 \oplus x_2 x_3 x_4 \\
  &\quad \oplus x_2 x_3 x_5 \oplus x_2 x_3 x_6 \oplus x_2 x_3 x_7 \oplus x_2 x_4 x_5 \oplus x_2 x_4 x_6 \oplus x_3 x_4 x_7 \\
  &\quad \oplus x_3 x_5 x_6 \oplus x_3 x_5 x_7 \oplus x_4 x_5 x_6 \oplus x_4 x_5 x_7 \oplus x_5 x_6 x_7 \\
  f_9 &= x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_6 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_5 \\
  &\quad \oplus x_1 x_3 x_7 \oplus x_1 x_4 x_6 \oplus x_1 x_5 x_6 \oplus x_1 x_6 x_7 \oplus x_2 x_3 x_4 \oplus x_2 x_3 x_5 \\
  &\quad \oplus x_2 x_3 x_7 \oplus x_2 x_4 x_5 \oplus x_2 x_4 x_6 \oplus x_2 x_5 x_6 \oplus x_2 x_6 x_7 \oplus x_3 x_4 x_5 \\
  &\quad \oplus x_3 x_4 x_6 \oplus x_3 x_5 x_6 \oplus x_3 x_5 x_7 \oplus x_3 x_6 x_7 \oplus x_4 x_5 x_7 \oplus x_5 x_6 x_7 \\
  f_{10} &= x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_6 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_5 \\
  &\quad \oplus x_1 x_3 x_7 \oplus x_1 x_4 x_6 \oplus x_1 x_5 x_6 \oplus x_1 x_6 x_7 \oplus x_2 x_3 x_4 \oplus x_2 x_3 x_5 \\
  &\quad \oplus x_2 x_3 x_7 \oplus x_2 x_4 x_5 \oplus x_2 x_4 x_6 \oplus x_2 x_5 x_6 \oplus x_2 x_6 x_7 \oplus x_3 x_4 x_5 \\
  &\quad \oplus x_3 x_4 x_6 \oplus x_3 x_5 x_6 \oplus x_3 x_5 x_7 \oplus x_3 x_6 x_7 \oplus x_4 x_5 x_7 \oplus x_5 x_6 x_7 \\
  f_{11} &= x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_6 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_5 \\
  &\quad \oplus x_1 x_3 x_6 \oplus x_1 x_3 x_7 \oplus x_1 x_4 x_5 \oplus x_1 x_4 x_6 \oplus x_1 x_5 x_6 \oplus x_1 x_6 x_7 \\
  &\quad \oplus x_2 x_3 x_4 \oplus x_2 x_3 x_6 \oplus x_2 x_3 x_7 \oplus x_2 x_4 x_5 \oplus x_2 x_4 x_6 \oplus x_2 x_5 x_7 \\
  &\quad \oplus x_2 x_6 x_7 \oplus x_3 x_4 x_5 \oplus x_3 x_4 x_7 \oplus x_3 x_5 x_6 \oplus x_3 x_5 x_7 \oplus x_4 x_5 x_6 \\
  &\quad \oplus x_4 x_5 x_7 \oplus x_5 x_6 x_7 \\
  f_{12} &= x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_4 \oplus x_1 x_3 x_5 \\
  &\quad \oplus x_1 x_3 x_6 \oplus x_1 x_3 x_7 \oplus x_1 x_4 x_5 \oplus x_1 x_4 x_6 \oplus x_1 x_5 x_6 \oplus x_2 x_3 x_4 \\
  &\quad \oplus x_2 x_3 x_5 \oplus x_2 x_3 x_6 \oplus x_2 x_3 x_7 \oplus x_2 x_4 x_6 \oplus x_2 x_4 x_7 \oplus x_2 x_5 x_6 \\
  &\quad \oplus x_3 x_4 x_5 \oplus x_3 x_4 x_7 \oplus x_3 x_5 x_6 \oplus x_3 x_5 x_7 \oplus x_4 x_5 x_6 \oplus x_4 x_5 x_7 \\
  f_{13} &= x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_4 \oplus x_1 x_3 x_6 \\
  &\quad \oplus x_1 x_4 x_5 \oplus x_1 x_5 x_6 \oplus x_2 x_3 x_4 \oplus x_2 x_3 x_5 \oplus x_2 x_3 x_6 \oplus x_2 x_4 x_5 \\
  &\quad \oplus x_2 x_4 x_6 \oplus x_2 x_4 x_7 \oplus x_2 x_5 x_7 \oplus x_2 x_6 x_7 \oplus x_3 x_4 x_6 \oplus x_3 x_4 x_7 \\
  &\quad \oplus x_3 x_5 x_6 \oplus x_3 x_5 x_7 \oplus x_3 x_6 x_7 \oplus x_4 x_5 x_6 \oplus x_4 x_5 x_7 \oplus x_5 x_6 x_7 \\
  f_{14} &= x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_4 \oplus x_1 x_3 x_6
\[ f_{15} = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_2 x_5 + x_1 x_2 x_7 + x_1 x_3 x_4 + x_1 x_3 x_6 + x_2 x_3 x_4 + x_2 x_3 x_5 + x_2 x_3 x_6 + x_2 x_3 x_7 + x_2 x_4 x_5 + x_2 x_4 x_6 + x_2 x_4 x_7 + x_2 x_5 x_6 + x_2 x_5 x_7 + x_3 x_4 x_5 + x_3 x_4 x_6 + x_3 x_4 x_7 + x_3 x_5 x_6 + x_3 x_5 x_7 + x_3 x_6 x_7 + x_4 x_5 x_6 + x_4 x_5 x_7 + x_4 x_6 x_7 + x_5 x_6 x_7 \]

\[ f_{16} = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_2 x_5 + x_1 x_2 x_7 + x_1 x_3 x_4 + x_1 x_3 x_6 + x_2 x_3 x_4 + x_2 x_3 x_5 + x_2 x_3 x_6 + x_2 x_3 x_7 + x_2 x_4 x_5 + x_2 x_4 x_6 + x_2 x_4 x_7 + x_2 x_5 x_6 + x_2 x_5 x_7 + x_3 x_4 x_5 + x_3 x_4 x_6 + x_3 x_4 x_7 + x_3 x_5 x_6 + x_3 x_5 x_7 + x_3 x_6 x_7 + x_4 x_5 x_6 + x_4 x_5 x_7 + x_4 x_6 x_7 + x_5 x_6 x_7 \]

\[ f_{17} = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_2 x_5 + x_1 x_2 x_7 + x_1 x_3 x_4 + x_1 x_3 x_6 + x_2 x_3 x_4 + x_2 x_3 x_5 + x_2 x_3 x_6 + x_2 x_3 x_7 + x_2 x_4 x_5 + x_2 x_4 x_6 + x_2 x_4 x_7 + x_2 x_5 x_6 + x_2 x_5 x_7 + x_3 x_4 x_5 + x_3 x_4 x_6 + x_3 x_4 x_7 + x_3 x_5 x_6 + x_3 x_5 x_7 + x_3 x_6 x_7 + x_4 x_5 x_6 + x_4 x_5 x_7 + x_4 x_6 x_7 + x_5 x_6 x_7 \]

\[ f_{18} = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_2 x_5 + x_1 x_2 x_7 + x_1 x_3 x_4 + x_1 x_3 x_6 + x_2 x_3 x_4 + x_2 x_3 x_5 + x_2 x_3 x_6 + x_2 x_3 x_7 + x_2 x_4 x_5 + x_2 x_4 x_6 + x_2 x_4 x_7 + x_2 x_5 x_6 + x_2 x_5 x_7 + x_3 x_4 x_5 + x_3 x_4 x_6 + x_3 x_4 x_7 + x_3 x_5 x_6 + x_3 x_5 x_7 + x_3 x_6 x_7 + x_4 x_5 x_6 + x_4 x_5 x_7 + x_4 x_6 x_7 + x_5 x_6 x_7 \]

\[ f_{19} = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_2 x_5 + x_1 x_2 x_7 + x_1 x_3 x_4 + x_1 x_3 x_6 + x_2 x_3 x_4 + x_2 x_3 x_5 + x_2 x_3 x_6 + x_2 x_3 x_7 + x_2 x_4 x_5 + x_2 x_4 x_6 + x_2 x_4 x_7 + x_2 x_5 x_6 + x_2 x_5 x_7 + x_3 x_4 x_5 + x_3 x_4 x_6 + x_3 x_4 x_7 + x_3 x_5 x_6 + x_3 x_5 x_7 + x_3 x_6 x_7 + x_4 x_5 x_6 + x_4 x_5 x_7 + x_4 x_6 x_7 + x_5 x_6 x_7 \]

\[ f_{20} = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_2 x_5 + x_1 x_2 x_7 + x_1 x_3 x_4 + x_1 x_3 x_6 + x_2 x_3 x_4 + x_2 x_3 x_5 + x_2 x_3 x_6 + x_2 x_3 x_7 + x_2 x_4 x_5 + x_2 x_4 x_6 + x_2 x_4 x_7 + x_2 x_5 x_6 + x_2 x_5 x_7 + x_3 x_4 x_5 + x_3 x_4 x_6 + x_3 x_4 x_7 + x_3 x_5 x_6 + x_3 x_5 x_7 + x_3 x_6 x_7 + x_4 x_5 x_6 + x_4 x_5 x_7 + x_4 x_6 x_7 + x_5 x_6 x_7 \]

\[ f_{21} = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_2 x_5 + x_1 x_2 x_7 + x_1 x_3 x_4 + x_1 x_3 x_6 + x_2 x_3 x_4 + x_2 x_3 x_5 + x_2 x_3 x_6 + x_2 x_3 x_7 + x_2 x_4 x_5 + x_2 x_4 x_6 + x_2 x_4 x_7 + x_2 x_5 x_6 + x_2 x_5 x_7 + x_3 x_4 x_5 + x_3 x_4 x_6 + x_3 x_4 x_7 + x_3 x_5 x_6 + x_3 x_5 x_7 + x_3 x_6 x_7 + x_4 x_5 x_6 + x_4 x_5 x_7 + x_4 x_6 x_7 + x_5 x_6 x_7 \]
\[
f_{22} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_7 \oplus x_1x_3x_4 \oplus x_1x_3x_6
\]
\[
\oplus x_1x_4x_5 \oplus x_1x_5x_7 \oplus x_1x_6x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_4x_6 \\
\oplus x_2x_4x_7 \oplus x_2x_5x_6 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \oplus x_3x_4x_5 \oplus x_3x_4x_6 \\
\oplus x_3x_4x_7 \oplus x_3x_5x_6 \oplus x_3x_5x_7 \oplus x_4x_5x_6 \oplus x_4x_5x_7 \oplus x_5x_6x_7
\]

\[
f_{23} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_7 \oplus x_1x_3x_4 \oplus x_1x_3x_6 \\
\oplus x_1x_4x_5 \oplus x_1x_5x_7 \oplus x_1x_6x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3x_7 \\
\oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_4x_7 \oplus x_2x_5x_6 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \\
\oplus x_3x_4x_5 \oplus x_3x_5x_6 \oplus x_3x_5x_7 \oplus x_4x_5x_6 \oplus x_4x_5x_7 \oplus x_5x_6x_7
\]

\[
f_{24} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_7 \oplus x_1x_3x_4 \oplus x_1x_3x_6 \\
\oplus x_1x_4x_5 \oplus x_1x_5x_7 \oplus x_1x_6x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3x_7 \\
\oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_4x_7 \oplus x_2x_5x_6 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \\
\oplus x_3x_4x_5 \oplus x_3x_5x_6 \oplus x_3x_5x_7 \oplus x_4x_5x_6 \oplus x_4x_5x_7 \oplus x_5x_6x_7
\]

\[
f_{25} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_7 \oplus x_1x_3x_4 \oplus x_1x_3x_6 \\
\oplus x_1x_4x_5 \oplus x_1x_5x_7 \oplus x_1x_6x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3x_7 \\
\oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_4x_7 \oplus x_2x_5x_6 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \\
\oplus x_3x_4x_5 \oplus x_3x_5x_6 \oplus x_3x_5x_7 \oplus x_4x_5x_6 \oplus x_4x_5x_7 \oplus x_5x_6x_7
\]

\[
f_{26} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_7 \oplus x_1x_3x_4 \oplus x_1x_3x_6 \\
\oplus x_1x_4x_5 \oplus x_1x_5x_7 \oplus x_1x_6x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3x_7 \\
\oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_4x_7 \oplus x_2x_5x_6 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \\
\oplus x_3x_4x_5 \oplus x_3x_5x_6 \oplus x_3x_5x_7 \oplus x_4x_5x_6 \oplus x_4x_5x_7 \oplus x_5x_6x_7
\]

\[
f_{27} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_7 \oplus x_1x_3x_4 \oplus x_1x_3x_6 \\
\oplus x_1x_4x_5 \oplus x_1x_5x_7 \oplus x_1x_6x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3x_7 \\
\oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_4x_7 \oplus x_2x_5x_6 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \\
\oplus x_3x_4x_5 \oplus x_3x_5x_6 \oplus x_3x_5x_7 \oplus x_4x_5x_6 \oplus x_4x_5x_7 \oplus x_4x_6x_7
\]

\[
f_{28} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_7 \oplus x_1x_3x_4 \oplus x_1x_3x_6 \\
\oplus x_1x_4x_5 \oplus x_1x_5x_7 \oplus x_1x_6x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3x_7 \\
\oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_4x_7 \oplus x_2x_5x_6 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \\
\oplus x_3x_4x_5 \oplus x_3x_5x_6 \oplus x_3x_5x_7 \oplus x_4x_5x_6 \oplus x_4x_5x_7 \oplus x_5x_6x_7
\]

\[
f_{29} = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_7 \oplus x_1x_3x_4 \oplus x_1x_3x_6 \\
\oplus x_1x_4x_5 \oplus x_1x_5x_7 \oplus x_1x_6x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_3x_7 \\
\oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_4x_7 \oplus x_2x_5x_6 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \\
\oplus x_3x_4x_5 \oplus x_3x_4x_6 \oplus x_3x_5x_7 \oplus x_4x_5x_6 \oplus x_4x_5x_7 \oplus x_3x_4x_6
\]
\[
\begin{align*}
    f_{30} &= x_1 x_2 x_3 \oplus x_1 x_2 x_4 \oplus x_1 x_2 x_5 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_4 \oplus x_1 x_3 x_6 \\
    &\quad \oplus x_1 x_4 x_5 \oplus x_1 x_5 x_7 \oplus x_2 x_3 x_4 \oplus x_2 x_3 x_5 \oplus x_2 x_3 x_7 \oplus x_2 x_4 x_6 \\
    &\quad \oplus x_2 x_4 x_7 \oplus x_2 x_5 x_6 \oplus x_2 x_5 x_7 \oplus x_2 x_6 x_7 \oplus x_3 x_4 x_5 \oplus x_3 x_4 x_6 \\
    &\quad \oplus x_3 x_4 x_7 \oplus x_3 x_5 x_6 \oplus x_3 x_5 x_7 \oplus x_4 x_5 x_6 \oplus x_4 x_5 x_7 \oplus x_5 x_6 x_7
\end{align*}
\]


[114] J. Seberry, $SBIBD(4k^2, 2k^2 + k, k^2 + k)$ and Hadamard matrices of order $4k^2$ with maximal excess are equivalent, *Graphs and Combinatorics*, vol. 5, 1989, pp. 373-383.


[116] J. Seberry, Existence of $SBIBD(4k^2, 2k^2 \pm k, k^2 \pm k)$ and Hadamard matrices with maximal excess, *Australasian Journal of Combinatorics*, vol. 4, pp. 87-91, 1991.


[139] J. J. Sylvester, Thoughts on inverse orthogonal matrices, simultaneous sign-successions and tesselated pavements in two or more colors with application to Newton's rule, ornamental title work and the theory of numbers, *Phil. Mag.*, vol. 34, pp. 461-475, 1867.


