# Binary block codes for correcting asymmetric or unidirectional errors



*DOI:*
10.6100/IR393187

*Document status and date:*
Published: 01/01/1993

*Document Version:*
Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

# Binary Block Codes for Correcting Asymmetric or Unidirectional Errors

Gang FANG

# 关于纠正非对称或单一方向误差的二元区组码

方刚 著

# Binary Block Codes for Correcting Asymmetric or Unidirectional Errors

**PROEFSCHRIFT**

ter verkrijging van de graad van doctor aan de Technische Universiteit Eindhoven, op gezag van de Rector Magnificus, prof. dr. J.H. van Lint, voor een commissie aangewezen door het College van Dekanen in het openbaar te verdedigen op maandag 8 maart 1993 om 16.00 uur

door


**Gang FANG**

geboren te Wuhan, China



druk: wibro dissertatiedrukkerij, helmond.

Dit proefschrift is goedgekeurd door de promotoren
prof. dr. J. H. van Lint
en
prof. dr. ir. H. C. A. van Tilborg

*To the memory of my father*

# Contents

# Abstract

The unidirectional failure properties of some recently developed semiconductor large scale integrated non-volatile memories and magnetic recording systems have provided the basis for a new direction of study in coding theory.

Modeling these memories and systems as ideal binary asymmetric channels, the research reported in this dissertation focuses on the characterization and bounds as well as constructions of error correcting block codes used for these channels.

Starting from the notion of asymmetric distance – a metric suitable for ideal binary asymmetric channels, upper and lower bounds on the maximum cardinality of a block code of length $n$ which corrects up to $t$ asymmetric errors are presented. Most of them extend the results which were known before to a larger area with respect to the length $n$ and the error correcting capability $t$, and some of them are improvements of those published in the existing literature.

Considering the same area of length $n$ and error correcting capability $t$ for codes capable of correcting asymmetric errors, the improved upper and lower bounds on maximum cardinalities of block codes capable of correcting up to $t$ unidirectional errors are also established. The observation of the differences between asymmetric error-correcting codes and unidirectional error-correcting codes gives constructions of the latter codes based on the constructions of the former ones by considering some comparable codewords if it is necessary.

The uniqueness of binary block codes of length less than 9 and minimum asymmetric distance 2 is thoroughly investigated. It is shown that up to permutation, the codes of maximum cardinalities for even lengths are unique, and the numbers of the non-isomorphic codes for odd lengths are simultaneously given.

Using the asymmetric distance metric, the notion of the minimum distance from a certain codeword to all other codewords is introduced. Upper bounds on such distance for maximum size codes are provided. For the trivial case and for codes which are unique up to permutation, all such distances are equal to the minimum distance of the code. This also holds

for all maximum size codes of length $n$ and minimum distance 2 when $n$ is not congruent to 1 or 3 modulo 6. For the remaining cases of length $n$, the same conclusion is suggested and it is left as a conjecture.

With the properties of perfect codes for the binary symmetric channel in mind, natural definitions of perfect, weakly perfect and uniformly weakly perfect binary block codes for correcting asymmetric errors are introduced and their properties are studied.

The analysis of the information rate of the weakly perfect codes which are nontrivial shows that the only binary block codes of length $n$ and minimum distance greater than 2, which correspond to a partition of the whole vector space of dimension $n$, are the repetition code for the ideal binary asymmetric channel. Further study of such codes leads to the fact that any weakly perfect code can always be enlarged to a bigger code.

Special attention is paid to the uniformly weakly perfect codes for correcting asymmetric errors. Some properties with respect to the weight distribution of such codes are discussed. As the results, explicit constructions for the uniformly weakly perfect codes which are nontrivial of length less than 15 and of minimum asymmetric distance 2 are presented. A family of uniformly weakly perfect codes is generated by exploiting the Hamming codes.

# Acknowledgements

THE PAST IS FOREVER WITH ME. It is a pleasure to have this opportunity of expressing my sincere appreciation towards those who have, directly or indirectly, contributed to the research for making this dissertation.

First of all, I would like to thank Professor dr. J. H. van Lint, my dissertation adviser, for initiating me into the field of coding theory and for continuously encouraging and supporting me during the course of this study. Special mention is deserved by the second adviser of this dissertation, Professor dr. ir. H. C. A. van Tilborg, with whom I had many useful discussions and whose patient guidance carried me through the rough periods I have worked on this research. In addition I owe a great deal to the Department of Mathematics and Computing Science at Eindhoven University of Technology for the support throughout the graduate study at this university. I see it as an honour to be a member of the discrete mathematics group at this department. I am pleased to acknowledge my indebtedness to all the members of this group for creating such a pleasant and stimulating environment.

I am deeply grateful to Professor dr. A. E. Brouwer, and to Dr. J. H. Weber, Dr. I. S. Honkala, F. W. Sun, Y. Saitoh and T. Etzion, with whom I had many kind and valuable cooperations and suggestions in this research. The interest shown by the regular participants in the weekly seminar on coding theory at the discrete mathematics group is highly appreciated. And I must record my deep obligation to Mr. F. C. Bussemaker for his kind help when making the computer programs.

Cordial thanks are also due to Mrs. J. van Amsterdam for her perseverant care and help during the whole period of my study at Eindhoven University of Technology; to Dr. J. W. Nienhuys, my dear officemate, whose knowledge in many other fields rather than mathematics and specially in Chinese language gave me enjoyable and relaxed time; and to Dr. P. Attwood for his conscientious and patient correction in my English writings when I started making scientific papers in English.

Last but not least, I wish also to express my total gratitude to my entire family for their moral support, faith in me and patience during the whole period of my education.

# About the author

Gang **FANG** (also known as FANG Gang in Chinese) was born on April 13, 1958 in Wuhan, Hubei Province, China. After finishing his middle school education in August 1974 in Wuhan, he spent two years in Chang Bu, Xin Zhou County, Hubei Province. There he received *re-education* from the peasants on farming, which was, at that time in China, the only way that most of pupils had to follow after they graduated from middle schools. Afterwards, he received his undergraduate education in Xi'an Jiaotong University, Xi'an, Shaanxi Province, China, and his B.S. and M.S. degrees in Applied Mathematics from the university in 1979 and 1985 respectively. He was with the Department of Mathematics, Xi'an Jiaotong University from 1979 to 1988, and was engaged as Assistant Lecturer and Lecturer in Mathematics there in 1979 and 1985, respectively. From Oct. 1988 onwards, Gang FANG has been working as Research Assistant in the Department of Mathematics and Computing Science, Eindhoven University of Technology in the Netherlands, and doing research in the field of coding theory under the direction of Professor dr. J. H. van Lint and Professor dr. ir. H. C. A. van Tilborg, which leads to this dissertation.

# Chapter 1

# Introduction

*Coding theory is still a young subject.*

*J. H. van Lint [49]*

## 1.1 Channel models and errors

A digital communication system can be regarded as a block diagram which, in principle, consists of five parts: source, encoder, noisy channel, decoder and sink. The source information is usually composed of binary or decimal digits or alphabetic information in some form. The encoder transforms these messages into signals acceptable to the channel. These signals enter the channel and are perturbed by noise. The output is received by the decoder, which makes a decision concerning which message was sent and then delivers this message to the sink.

Error control coding has shown itself to be a powerful tool in obtaining efficient and reliable transmission of messages over a noisy channel (see e.g. [35] [42]). Throughout this dissertation we restrict ourselves to binary noisy channels. The *binary symmetric channel* (BSC) is a practical and simple model for random errors that occur in a transmitted word with equal probability $p$ of a 1-to-0 error and a 0-to-1 error, as shown in Figure 1.1. Also, the noise is random in the sense that it affects each bit independently in the transmitted word.

The 1-to-0 error and the 0-to-1 error are termed as *1-error* and *0-error* respectively, adopted from Kim and Freiman [31]. If the errors in a word (or vector) are independent of each other and both 1-errors and 0-errors are equally probable, then these errors are said to be *symmetric errors.*

A great deal of research has been devoted to finding efficient schemes by which digital information can be coded for reliable transmission through a binary noisy channel after the appearance of coding theory, whose birth is marked by the fundamental work of Shannon [46] in 1948. Codes for correcting symmetric errors have extensively been studied for use on a BSC. We only mention the book written by MacWilliams and Sloane [36], in which a list of more than 1400 references is included.

In this dissertation, two other channel models will often be considered, namely the *ideal binary asymmetric channel* (IBAC) and the *ideal binary unidirectional channel* (IBUC). The *binary asymmetric channel* (BAC) is modeled in Figure 1.2, with a probability $p$ of a 1-error and a probability $\epsilon$ of a 0-error, where $\epsilon \neq p$, $0 \leq \epsilon, p \leq 1$.

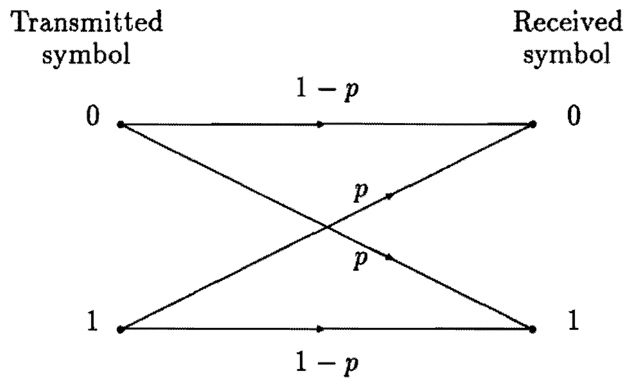


Figure 1.1: The binary symmetric channel (BSC) where $0 \leq p \leq 1/2$.

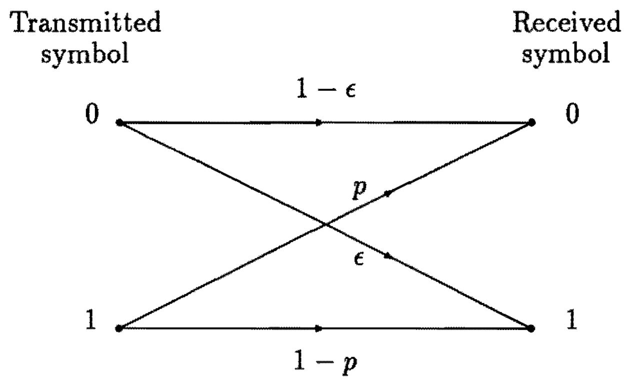


Figure 1.2: The binary asymmetric channel (BAC) where $\epsilon \neq p$, $0 \leq \epsilon, p \leq 1$.

For the special case when $p$ is much greater than $\epsilon$, it is possible to assume $\epsilon$ to be zero. Then we arrive at the model of IBAC, which is often called $Z$-channel too (see Figure 1.3). It is totally error-free for 0's and noisy for 1's. The model of IBUC behaves either like the $Z$-channel or like the inverted $Z$-channel, which is error-free for 1's and noisy only for 0's.

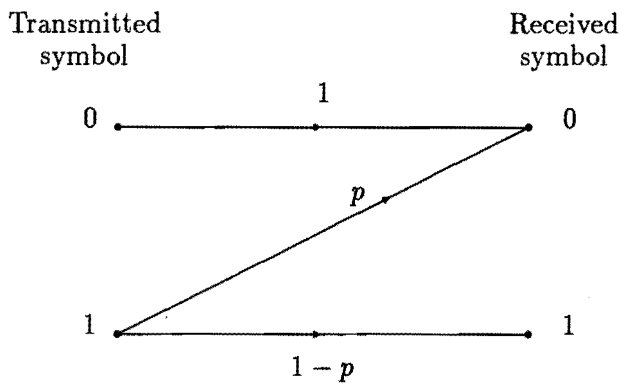


Figure 1.3: The ideal binary asymmetric channel (IBAC or $Z$-channel) where $0 \leq p \leq 1$.

From the foregoing, in an IBAC either 0-errors or 1-errors can occur in the received words but not both. These errors are referred to as *asymmetric errors.* If both 0-errors and 1-errors can occur in the received words, but in any particular received word, all errors are of one type, then these errors are characterized as *unidirectional errors.*

In the last two decades, a lot of attention has been paid to the study of codes which are capable of correcting asymmetric or unidirectional errors. Such codes apply to, for instance, some data storage systems or optical communication [2] [4] [8] - [11] [38] - [41] [44]. For this, the reader is also referred to the references listed in Chapter 7 of [42] and the bibliography of [34]. As an example, we quote a statement from [9] below. After analyzing the failures in the cells of semiconductor large scale integrated (LSI) non-volatile memories and metal-nitride-oxide semiconductor (MNOS) memories, Constantin et al. come to the following conclusion:

> *"The LSI and MNOS memories thus exhibit a unidirectional failure property. Although the rest of the memory system ······ is not dependent on power shutoffs and is subject to symmetric failures, for the overall memory system, the probability of 1 → 0 crossover failure is significantly greater than the 0 → 1 crossover failure."*

The asymmetric or unidirectional failure properties of these memories have provided the basis for a new direction of study in coding theory. In the symmetric error model (BSC), both 0-errors and 1-errors may occur in a received word. In an IBAC, if there are multiple errors, their type is known. A more formal definition of error types with an example will be given at the end of this section.

Let $\mathbf{V_n}$ denote the $n$-dimensional vector-space over $GF(2)$ which is the field containing only two elements 0 and 1, i.e.

$$\mathbf{V_n} = \{(a_1, a_2, \cdots, a_n) | a_i \in \{0,1\}, i = 1, 2, \cdots, n\}.$$

We use the words *vector* or *word* to denote the $n$-tuples from $\mathbf{V_n}$ ($n$ is called the block length or word length). The cardinality of a finite set $A$ is denoted by $|A|$. For any $\mathbf{x} = (x_1, x_2, \cdots, x_n) \in \mathbf{V_n}$ and $\mathbf{y} = (y_1, y_2, \cdots, y_n) \in \mathbf{V_n}$, put

$$N(\mathbf{x}, \mathbf{y}) = |\{i | x_i = 1 \wedge y_i = 0, 1 \leq i \leq n\}|,$$

the number of coordinates of $\mathbf{x}$ and $\mathbf{y}$ with $x_i = 1$ and $y_i = 0$ for $1 \leq i \leq n$. If $N(\mathbf{x}, \mathbf{y}) = 0$, i.e., for all $i$, $x_i = 1$ implies $y_i = 1$, we say that the vector $\mathbf{x}$ *is covered* by the vector $\mathbf{y}$. This can be written as $\mathbf{x} \leq \mathbf{y}$ or $\mathbf{y} \geq \mathbf{x}$. If $\mathbf{x} \not\leq \mathbf{y}$ and $\mathbf{y} \not\leq \mathbf{x}$, the vector $\mathbf{x}$ and the vector $\mathbf{y}$ are said to be *incomparable.* If $\mathbf{x} \leq \mathbf{y}$ or $\mathbf{y} \leq \mathbf{x}$, then we say that they are *comparable.*

**Example 1.1** Let $n = 8$ and

$$\begin{aligned} \mathbf{x} &= (10101011), \\ \mathbf{y} &= (00101011), \\ \mathbf{z} &= (10100000). \end{aligned}$$

Then $N(\mathbf{x}, \mathbf{y}) = 1$ and $N(\mathbf{y}, \mathbf{x}) = 0$, which shows that $\mathbf{x}$ and $\mathbf{y}$ are comparable and $\mathbf{y} \leq \mathbf{x}$. Similarly, $\mathbf{z} \leq \mathbf{x}$. Also, $N(\mathbf{y}, \mathbf{z}) = 3$, $N(\mathbf{z}, \mathbf{y}) = 1$. So $\mathbf{y}$ and $\mathbf{z}$ are incomparable.

**Definition 1.1** *Assume that a vector* $\mathbf{x} \in \mathbf{V_n}$ *is transmitted and a vector* $\mathbf{y} \in \mathbf{V_n}$ *is received.*

1. *We say that* $\mathbf{x}$ *has suffered* $t$ *symmetric or random errors if*

$$N(\mathbf{x}, \mathbf{y}) + N(\mathbf{y}, \mathbf{x}) = t.$$

2. *We say that* $\mathbf{x}$ *has suffered* $t$ *asymmetric errors if*

$$(N(\mathbf{x}, \mathbf{y}) = t) \ \wedge \ (N(\mathbf{y}, \mathbf{x}) = 0).$$

3. *We say that* $\mathbf{x}$ *has suffered* $t$ *unidirectional errors if*

$$(N(\mathbf{x}, \mathbf{y}) = t \ \wedge \ N(\mathbf{y}, \mathbf{x}) = 0) \vee (N(\mathbf{x}, \mathbf{y}) = 0 \ \wedge \ N(\mathbf{y}, \mathbf{x}) = t).$$

**Example 1.2** Let $n = 12$ and

$$\begin{aligned} \mathbf{x} &= (111111000000) \\ \mathbf{y}_1 &= (110000100000) \\ \mathbf{y}_2 &= (111100000000) \\ \mathbf{y}_3 &= (111111000001). \end{aligned}$$

a) When sending $\mathbf{x}$ over a channel which may cause errors of the symmetric type, it is possible to receive $\mathbf{y}_1$ $(t = 5)$, $\mathbf{y}_2$ $(t = 2)$, $\mathbf{y}_3$ $(t = 1)$.

b) When sending $\mathbf{x}$ over a channel which may cause errors of the asymmetric type, it is possible to receive $\mathbf{y}_2$ $(t = 2)$ but impossible to receive $\mathbf{y}_1$ or $\mathbf{y}_3$.

c) When sending $\mathbf{x}$ over a channel which may cause errors of the unidirectional type, it is possible to receive $\mathbf{y}_2$ $(t = 2)$ or $\mathbf{y}_3$ $(t = 1)$ but impossible to receive $\mathbf{y}_1$.

## 1.2 Binary block codes

Codes are designed to detect and/or correct errors in the channels. A code is called a *block code* if the coded information can be divided into blocks of length $n$ $(\geq 1)$. In the binary case, these blocks are the vectors of the vector space $\mathbf{V_n}$, defined in Section 1.1, over the finite field with only two elements 0 and 1, on which the addition and the multiplication are defined by $a + b$ (mod 2) and $ab$ where $a, b \in \{0, 1\}$. For a vector $\mathbf{x} = (x_1, x_2, \cdots, x_n)$ in $\mathbf{V_n}$, $x_i$ is called the $i$th coordinate of $\mathbf{x}$. The *Hamming weight* of $\mathbf{x}$ (also called the *weight* of $\mathbf{x}$), denoted by $w(\mathbf{x})$, is the number of nonzero coordinates of $\mathbf{x}$.

One of the most important parameters of a code is its distance. According to what we have mentioned previously, three different distances between two vectors of $\mathbf{V_n}$ are introduced in this dissertation.

**Definition 1.2** *Let* $\mathbf{a} \in \mathbf{V_n}$ *and* $\mathbf{b} \in \mathbf{V_n}$. *Define*

$$\begin{aligned} d_h(\mathbf{a}, \mathbf{b}) &= N(\mathbf{a}, \mathbf{b}) + N(\mathbf{b}, \mathbf{a}), \\ d_a(\mathbf{a}, \mathbf{b}) &= max\{N(\mathbf{a}, \mathbf{b}), N(\mathbf{b}, \mathbf{a})\}, \end{aligned}$$

*and*

$$d_u(\mathbf{a}, \mathbf{b}) = \begin{cases} d_h(\mathbf{a}, \mathbf{b}), & \text{if } \mathbf{a} \text{ and } \mathbf{b} \text{ are comparable} \\ 2d_a(\mathbf{a}, \mathbf{b}), & \text{otherwise.} \end{cases}$$

$d_h(\mathbf{a}, \mathbf{b})$ is the well known *Hamming distance* between $\mathbf{a}$ and $\mathbf{b}$ which indicates the number of different coordinates in the two vectors. The Hamming distance is utilized for the study of BSC. It is replaced, in the present dissertation, by the *asymmtric distance* $d_a(\mathbf{a}, \mathbf{b})$ or by the *unidirectional* *distance* $d_u(\mathbf{a},\mathbf{b})$ which were introduced by Rao and Chawla [41], Anderson [1] as well as Bose and Rao [4] respectively. An embryonic form of the asymmetric distance and the statement of the error-correcting capability of codes with this distance function can be found in earlier literature, for instance in [52].

It is clear that, for all $\mathbf{a}$, $\mathbf{b} \in \mathbf{V_n}$:

$$d_h(\mathbf{a},\mathbf{b}) \leq d_u(\mathbf{a},\mathbf{b}) \leq 2d_a(\mathbf{a},\mathbf{b})$$

and

$$2d_a(\mathbf{a},\mathbf{b}) = d_h(\mathbf{a},\mathbf{b}) + \mid w(\mathbf{a}) - w(\mathbf{b}) \mid . \tag{1.1}$$

Both the Hamming distance and the asymmetric distance are two legitimate distance functions, or metrics, on $\mathbf{V_n}$. Hence, the name of the asymmetric distance may be confusing since of course the metric is symmetric. In fact, the word "asymmetric" only refers to $Z$-channels. However, the unidirectional distance is not a metric on $\mathbf{V_n}$. This is because it does not satisfy the triangle inequality, as can be seen by taking the vectors in Example 1.1:

$$d_u(\mathbf{y},\mathbf{z}) = 2 \times 3 = 6 > d_u(\mathbf{y},\mathbf{x}) + d_u(\mathbf{x},\mathbf{z}) = 1 + 3 = 4.$$

A binary symmetric error-correcting block code of length $n$ and minimum Hamming distance $d$, indicated by $C_h(n,d)$, is a nonempty proper subset of the vector space $\mathbf{V_n}$ in which any two distinct vectors are at Hamming distance at least $d$ apart and this distance is realized at least once. Similar definitions and notations apply to asymmetric cases (and $C_a(n,d)$) or unidirectional cases (and $C_u(n,d)$) instead of symmetric cases (and $C_h(n,d)$). The vectors in a block code are called *codewords*. The *minimum distance* (often simply called *distance*) of a code is defined as the minimum of the distances between all pairs of codewords. Hence for a $C_f(n,d)$ code $C$, we define

$$d = min\{d_f(\mathbf{a},\mathbf{b}) | \mathbf{a},\mathbf{b} \in C \land \mathbf{a} \neq \mathbf{b}\}$$

where $f$ can be taken as $h$, $u$ and $a$. If $C$ can correct up to $t$ ($t \geq 1$) symmetric errors, we sometimes say that $C$ is a $t$-SyEC code. Similar notations can also be applied in asymmetric cases or unidirectional cases. Hence we have the so-called $t$-AsEC or $t$-UEC codes. In accordance with our notation, we restate the following well known results which give the necessary and sufficient conditions for the error-correcting capability of a block code in terms of the above three distance functions (see e.g. [36], [31] and [4]).

**Theorem 1.1** *Let $C$ be a code of length $n$ and distance $d_f$ ($f = h,a,u$). Then*

*1) $C$ is a t-SyEC code if and only if (iff) $d_h \geq 2t+1$.*

*2) $C$ is a $t$-AsEC code iff $d_a \geq t+1$.*

*3) $C$ is a $t$-UEC code iff $d_u \geq 2t+1$.*

To avoid unnecessary complications in the discussions, we will make two conventions on the codes: the minimum asymmetric distance is always assumed to be greater than or equal to 2 (a code is called *trivial* if its cardinality is less than or equal to 2) and none of the coordinates is identically zero or identically one. It is easy to show that a $C_a(n,d)$ code, if $n < 2d$, contains at most two codewords; therefore, it is a trivial code.

Let $A_i$ denote the number of codewords of weight $i$ in a code $C$ of length $n$, i.e., $A_i = |\{\mathbf{c} \in C \mid w(\mathbf{c}) = i\}|$ for $i = 0, 1, \cdots, n$. The numbers $A_0, A_1, \cdots, A_n$ are termed as the *weight distribution* of $C$. The *weight of* $C$, indicated by $w(C)$, is defined as the sum of the weights of all codewords of $C$. The *rate* of $C$, defined by $(log_2|C|)/n$, is a measure for the efficiency of $C$.

In general, codes should be designed not only with a high rate ('efficiency') but also with a large distance ('reliability', see Theorem 1.1). Regrettably, these are conflicting goals. Very often what we are concerned with in this respect is the following function:

$A_f(n,d)$ : the maximum number of codewords of a $C_f(n,d)$ code

where $f$ stands for $h$, $a$ or $u$. The bounds on $A_h(n,d)$ have been established extensively (see e.g. [36] [5]). In this dissertation, we will discuss the lower and upper bounds on $A_a(n,d)$ and $A_u(n,d)$. We often use the same notation $d$ for both $C_a(n,d)$ codes and $C_u(n,d)$ codes. Usually, this will not lead to confusion. When the best (smallest) known upper bound meets the best (largest) known lower bound, the exact value of $A_a(n,d)$ or $A_u(n,d)$ has been determined. If a $C_f(n,d)$ code $C$ contains $A_f(n,d)$ codewords ($f = h, a, u$), the code $C$ is called *optimal* or we say that $C$ is of maximum *size* (or *cardinality*).

Evidently, any $t$-SyEC code is also a $t$-UEC code, and any $t$-UEC code is also a $t$-AsEC code. This yields

$$A_h(n, 2t+1) \leq A_u(n, 2t+1) \leq A_a(n, t+1) \tag{1.2}$$

for $n > t \geq 1$. Further, it was proved that $A_h(n,3) = A_u(n,3)$ for $n \geq 1$ (see e.g. [57]), namely, a single symmetric error must be unidirectional.

A code in which all the codewords are of the same weight $w$ is called a *constant weight* code of weight $w$. $A(n,d,w)$, which represents the maximum number of binary $n$-tuples of weight $w$ with minimum Hamming distance $\geq d$, is a well known function for constant weight codes. The bounds on $A(n,d,w)$ are well documented in [5]. A *linear code* of length $n$ is a linear subspace of $\mathbf{V_n}$. A $k$-dimensional linear code of length $n$ with minimum Hamming distance $d$ is called a $[n,k,d]$ code.

Two codes are called *equivalent* if they differ only in the order of the coordinates. Thus, equivalent codes have the same parameters, namely the same length, the same number of codewords and the same minimum distance.

Finally, some notations are introduced here for further use. To save space, vectors are sometimes expressed in hexadecimal representation (right justified), that is, we put 0=0000, 1=0001, $\cdots$, 9=1001, A=1010, $\cdots$, F=1111, and usually erase leading zeros. For example, 001010=0A, 10011110=9E, etc.. Bars indicate complements of binary vectors or matrices. The all-one vector and the all-zero vector respectively are abbreviated to $\mathbf{1}$ and $\mathbf{0}$. $\mathbf{a}^l$ denotes the all-$a$ vector of length $l$ ($a = 0, 1$). The Greek letter $\tau$ indicates the transpose of matrices and vectors. For a vector $\mathbf{a} = (a_1, \cdots, a_n) \in \mathbf{V_n}$, $circ(\mathbf{a})$ is used to represent the successive cyclic shifts of the vector $\mathbf{a}$, namely a square matrix of size $n$ by $n$ with top row $\mathbf{a}$. The *support* of $\mathbf{a}$ is the set of indices $i$ with $a_i \neq 0$, and is denoted by $supp(\mathbf{a})$. Sometimes vectors will be identified by their supports.

## 1.3 Motivation of performed research, a brief survey of prior work

The theory of codes for correcting asymmetric or unidirectional errors has been developed less fully than that of codes for correcting symmetric errors; either this is because of the difficulty raised in nonsymmetric channels or because it is a new developing field in coding theory. But, on the other hand, many of the concepts developed for BSC can now be carried over, with slight modifications, to the new model IBAC. The asymmetric distance plays an essential role for codes employed in IBAC. Its relationship with Hamming distance is shown in (1.1). Hence for any $\mathbf{a}$ and $\mathbf{b}$ in $\mathbf{V_n}$, $d_a(\mathbf{a}, \mathbf{b}) \geq \lfloor (d_h(\mathbf{a}, \mathbf{b}) + 1)/2 \rfloor$. Here, $\lfloor r \rfloor$ denotes the largest integer not exceeding the real number $r$. We also use $\lceil r \rceil$ to denote the smallest integer not less than the real number $r$. According to Theorem 1.1, it is easy to see then, that for equivalent error-correcting capability, the Hamming distance imposed on a code for BSC is more restrictive than the asymmetric distance imposed on a code for IBAC.

For instance, a binary code having asymmetric distance 2, is capable of correcting any single 1-error. Since $d_h(\mathbf{a}, \mathbf{b}) \geq 3$ implies $d_a(\mathbf{a}, \mathbf{b}) \geq 2$, any 1-SyEC code is of course a 1-AsEC code. However, it would be inefficient to use single error-correcting codes designed for BSC as codes for IBAC. One should hope, for any given $n$, to come up with a 1-AsEC code of length $n$ having more codewords, i.e., a higher information rate, than the single error-correcting Hamming code of length $n$. And indeed, Kim and Freiman [31] have succeeded in giving a constructive proof of this contention for most length $n$ codes. The superiority of the codes of [31] lies in the fact that they are of larger size (and hence can represent a greater number of different messages) than the optimal symmetric codes of equivalent length which meet the same minimum reliability requirement in IBAC.

Even higher information rates were achieved by Varshamov [55] [53], and generalizations to multiple error-correcting codes for IBAC were also given by Varshamov [54] and McEliece [37] in which they encounter problems that are presently unsolved in number theory.

Constantin and Rao [9] introduced a class of codes suitable for asymmetric channels, which are referred to as *group-theoretic codes*. As their name shows, the development of such codes relies mainly on the theory of Abelian groups, and their structure is evidently inherited from the structure of the Abelian group that generated them. These codes are of minimum asymmetric distance 2 and have been shown to be superior in their information rates over the previously known 1-AsEC codes of Kim-Freiman and Varshamov.

Early in the eighties, some good bounds on $A_a(n, d)$ were derived by Delsarte and Piret [12] as well as by Kløve [33], which are better than those given by Varshamov [51] and Goldbaum [24] previously. An interesting construction method for some 1-AsEC codes was also developed by Delsarte and Piret in their paper using Steiner systems. Further, they constructed 2-AsEC codes by using the Nordstrom-Robinson code which is applied for BSC.

More recent papers on this subject and on unidirectional codes, which were available to me, are [58] – [60], [45] and [14]. In [58] – [60], Weber et al. constructed codes mainly by using a general 'expurgating/puncturing' construction method by means of some good well known symmetric error-correcting codes. Saitoh et al. [45] found some better codes, in the sense that they have higher information rates, due to a good computer search. Some improved results were recently announced in [14], in which three methods were applied by Etzion, namely the partitioning method which is a generalization of a method used to construct constant weight codes (see e.g. [5]), the method of combining codes from a few existing codes, and the method which is called shortening by weights. The codes found in [45] and [14] result in numerous new lower bounds of the size of $t$-AsEC codes and the size of $t$-UEC codes in the area of length $n \leq 23$ and error correcting capability $t \leq 6$.

For later use, we recall the concept of $t$-designs. A *design* $(\Omega, \mathcal{B})$ is a set $\Omega$ (of 'points') together with a collection $\mathcal{B}$ of subsets of $\Omega$ (called 'blocks'). A $t$-$(v, k, \lambda)$ design is a design in which $|\Omega| = v$, $|B| = k$ for any block $B \in \mathcal{B}$ such that any set of $t$ distinct points of $\Omega$ belongs to exactly $\lambda$ blocks. A *Steiner system* $S(t, k, v)$ is a $t$-$(v, k, 1)$ design. A *balanced incomplete block design* is a 2-$(v, k, \lambda)$ design, which is also often denoted by $D(v, b, r, k, \lambda)$

where $b$ indicates the number of blocks in the design and $r$ the number of blocks containing a given point. A *symmetric design* (or square 2-design) is a 2-design with as many blocks as objects. For further background, see [25], [13] or [36].

An ingenious construction method for asymmetric error-correcting codes is shown in [50], in which Van Lint et al. presented a 3-AsEC code of length 14 and size 30. The construction depends on well known block designs. Its description is worth giving here briefly.

Let $C$ be a 3-AsEC code of length 14. Without loss of generality, we may assume that the all-one vector $\mathbf{1}$ and the all-zero vector $\mathbf{0}$ are in $C$. Using Kløve's result [33] with some combinatorial arguments leads to the weight distribution of $C$ satisfying: $A_4 \leq 3$, $A_4 + A_5 + A_6 \leq 12$ and $A_7 \leq 8$.

To construct the required code, let $C$ contain eight codewords of weight 7, i.e., $A_7 = 8$. In so doing, Van Lint et al. had proved that these codewords of weight 7 form a 2-(8,4,3) design. Let $A = circ(1101000)$ be the incidence matrix of a projective plane $\mathcal{P}_A$ of order 2. Then we can take the vector $(\mathbf{1}, \mathbf{0})$ of length 14 together with the rows of the matrix $(A, J-A)$ ($J$ denotes the all-one matrix) as the incidence matrix of the 2-(8,4,3) design formed by the words of weight 7 in $C$. Let $B = circ(0001011)$ be the incidence matrix of another projective plane $\mathcal{P}_B$ of order 2. Since the minimum asymmetric distance of $C$ is 4, and the planes $\mathcal{P}_A$ and $\mathcal{P}_B$ have no lines in common, we can take the rows of the matrix $(B, B)$ as the codewords of weight 6 and the complements of them as the codewords of weight 8 in $C$. Further analysis on the planes $\mathcal{P}_A$ and $\mathcal{P}_B$ provides three words of weight 4 and three words of weight 10 to add to $C$. This gives a 3-AsEC code of length 14 containing 30 codewords.

Traditional coding theory is mainly focussed on codes for correcting and/or detecting errors of the symmetric types. Nevertheless, some codes can now be made for multiple types of error corrections/detections. A code is called $t_1$-SyEC $t_2$-UEC $t_3$-AsEC $d_1$-SyED $d_2$-UED $d_3$-AsED ($0 \leq t_1 \leq t_2 \leq t_3$, $0 \leq d_1 \leq d_2 \leq d_3$, $t_i \leq d_i$) if it can correct up to $t_1$ symmetric errors, up to $t_2$ unidirectional errors, and up to $t_3$ asymmetric errors, as well as detect from $t_1 + 1$ to $d_1$ symmetric errors that are not of the unidirectional type, from $t_2 + 1$ to $d_2$ unidirectional errors that are not of the asymmetric type, and from $t_3 + 1$ to $d_3$ asymmetric errors. The conditions that are necessary and sufficient for a code to be $t_1$-SyEC $t_2$-UEC $t_3$-AsEC $d_1$-SyED $d_2$-UED $d_3$-AsED have been generally derived by Weber [57]. But it seems to be difficult to study these kinds of codes in general. Much research has been done for codes with two different types of error corrections and/or detections [42]. In the present dissertation, we shall restrict ourselves to codes for correcting errors of only one type, namely $t$-AsEC codes and $t$-UEC codes.

The race to develop better and better codes, that started in 1948 as a result of Shannon's theory, is still in progress and this dissertation represents a ticket to this race.

## 1.4 Objectives and research outline

We are basically concerned with bounds and constructions of codes for correcting asymmetric or unidirectional errors, and with studies of properties of codes for correcting asymmetric errors.

Bounds on the maximum cardinality of codes for correcting less than 5 asymmetric/unidirectional errors have been studied by several authors, as mentioned in Section 1.3, and they have been tabulated for codes of length $\leq 23$. The first goal in this research is to give better bounds on the maximum cardinality of codes for correcting $t$ or fewer asymmetric/unidirectional errors with $5 \leq t \leq 8$, and to extend the existing tables of bounds to codes of length $\leq 27$.

The study for perfect codes and weakly perfect codes which are capable of correcting asymmetric errors is the second goal. According to the definitions of such codes, there are many questions one can conceivably address with respect to those codes. However, in this dissertation we are mainly concerned with the following two questions:

1. Which notion of $t$-asymmetric-error-correcting perfect codes of length $n$ corresponds to a partition of the binary $n$-dimensional vector space?

2. Does a nontrivial asymmetric-error-correcting perfect (weakly perfect or uniformly weakly perfect) code exist that reaches the highest information rate among all codes of the same length with the same error-correcting capability?

We will present the answers to the above two questions.

The investigations on uniqueness of optimal block codes for correcting single asymmetric errors and on properties of uniformly weakly perfect codes are additional interests in this research.

This dissertation is organized as follows.

In Chapter 2 some basic results are given in preparation for obtaining bounds on the maximum sizes of codes for correcting asymmetric errors, which will be used in the following two chapters. It will be seen that most of these results can be applied to codes for correcting unidirectional errors.

Chapter 3 is devoted to bounds on the maximum size of binary block $t$-AsEC codes of length $\leq 27$ with $5 \leq t \leq 8$. The improved upper bounds are based on analyses of finding better solutions in a set of linear inequalities on the weight distribution derived from Theorem 1 of [33] (generalizing the result of Delsarte and Piret [12]) and subject to Theorem 2 of [59]. Using further combinatorial arguments, stronger relations on the weight distribution of such codes have been found. Since it is difficult to explain these arguments in general, they will be demonstrated in each concrete case. Lower bounds follow virtually from the constructions of codes. Some constructions described in this dissertation depend on the well known 2-designs or good constant weight codes, and some are based on known codes with smaller lengths and lesser distances. Trial-and-error is also used to construct some special codes according to the restrictions on their weight distributions. All the resulting codes have either a nicer description or better parameters. Furthermore, some improved bounds on maximum cardinalities of 4-AsEC codes of length $\leq 23$ are presented. Since the corresponding codes have not been found yet, their maximum sizes were taken from the literature. One miscellaneous result included in this chapter is the new upper bound on the maximum size of 1-AsEC codes of length 10.

Along the same lines, we develop bounds on the maximum size of binary block $t$-UEC codes of length $\leq 27$ with $5 \leq t \leq 8$ in Chapter 4. On the construction side, most of the unidirectional error-correcting codes were obtained by modifying the asymmetric error-correcting codes, found in Chapter 3, with the same length and the same error correcting capability.

Chapter 5 deals with uniqueness of optimal 1-AsEC codes of length less than 9. It is shown that up to permutation, the optimal $C_a(n,2)$ codes for $n$ = 2,4,6 and 8 are unique, and there exist exactly four non-isomorphic $C_a(3,2)$ codes containing 2 codewords, four non-isomorphic $C_a(5,2)$ codes with 6 codewords and twelve non-isomorphic $C_a(7,2)$ codes with 18 codewords.

A different direction taken in the dissertation points to codes with some *'perfect'* conditions, treated in Chapter 6. For the asymmetric distance metric, the notion of the minimum distance $r(\mathbf{c})$ from a certain codeword $\mathbf{c}$ to all other codewords is introduced. We then present the bounds on $r(\mathbf{c})$ for all codewords of an optimal code. After introducing the definition of perfect codes, weakly perfect codes and uniformly weakly perfect codes, some properties of such codes are discussed. Consequently, the two questions stated above on such codes are answered. As a special interest, uniformly weakly perfect codes are considered at the end of this chapter.

In Appendix **A**, five tables are given. The bounds obtained in Chapter 3 lead to Table A.3, and those revealed in Chapter 4 are summarized in Table A.5. All the updated best bounds on the maximum size of codes of length $\leq 23$ and error correcting capability $\leq 4$ respectively are listed in Tables A.1, A.2 and A.4 for the sake of completeness. Finally, Appendix **B** shows how to reconstruct the codes mentioned in Chapters 3 and 4.

# Chapter 2

# General results

## 2.1 Some combinatorial bounds

Since the techniques used in this dissertation will improve on previous methods, it will be necessary to quote some of the existing results.

**Theorem 2.1** *Let $C$ be a $C_a(n,d)$ code for $n \geq d \geq 2$. Then the weight distribution of $C$ satisfies*

$$\sum_{j=w-s}^{w} A^l(s, 2d, w-j)A_j \leq A^u(n+s, 2d, w)$$

*where $A^u(n,d,w)$ and $A^l(n,d,w)$ denote any upper resp. lower bound on $A(n,d,w)$, $w = 0, 1, \cdots, n$ and $s = 0, \cdots, w$.*

Theorem 2.1 is due to Kløve [33]. Since any $t$-UEC code is also a $t$-AsEC code, Theorem 2.1 holds for $C_u(n,d)$ codes as well. Tables of bounds on $A(n,d,w)$ can be found in [5] and [6]. Sometimes the upper bounds on $A_a(n,d)$ obtained with Theorem 2.1 can be improved by using additional combinatorial arguments. We cite the following theorem.

**Theorem 2.2** *Let $C$ be a $C_a(n,d)$ code. Let $l$ and $i$ be integers such that $0 < l \leq i \leq n$. Define*

$$\begin{aligned} D &= \textstyle\sum_{j=i-l}^{i} A_j, \\ E &= \textstyle\sum_{j=i-l}^{i} jA_j, \\ q &= \lfloor E/n \rfloor, \\ r &= E - nq, \\ S_k &= \textstyle\sum_{j=i-l}^{k+i-l-1} A_j, \quad \textit{for } k = 1, 2, \cdots, l, \\ S &= \textstyle\sum_{j=1}^{l} S_j(S_j - 1). \end{aligned}$$

*Then*

$$nq(q-1) + 2rq + S \leq D(D-1)(i-d). \tag{2.1}$$

Theorem 2.2 is from Weber et al. [59]. Note that (2.1) always holds no matter whether $i \geq d$ or not. Obviously, Theorem 2.2 also holds for $C_u(n,d)$ codes. The non-existence of a code can be derived from the constraints on the weight distribution by using Theorem 2.2. The key to this is to contradict (2.1) by choosing suitable integers $i$ and $l$ when a code is assumed with a certain weight distribution. However, in practice, it has been found that Theorem 2.2 is useful only when $i$ and $l$ are taken to be relatively small, since (2.1) holds when $i$ and $l$ are large. How we use Theorem 2.2 to sharpen the upper bounds on the maximum size of codes will be shown in the following chapter.

The next theorem provides a concatenation technique for constructing $C_a(n,d)$ or $C_u(n,d)$ codes using known codes of smaller length and distance.

**Theorem 2.3** *For $m \geq 1$ and $1 \leq d_i \leq n_i$, $i = 1, \cdots, m$,*

$$min\{A_f(n_i, d_i) | i = 1, \cdots, m\} \leq A_f(n,d)$$

*where $n = \sum_{i=1}^{m} n_i$, $d = \sum_{i=1}^{m} d_i$ and $f = a, u$.*

*Proof:* When $m = 1$, the assertion is obviously true. Suppose that $m = 2$. Let $C_1$ be a $C_f(n_1, d_1)$ code of size $\nu = A_f(n_1, d_1)$, and $C_2$ a $C_f(n_2, d_2)$ code of size $\mu = A_f(n_2, d_2)$. Without loss of generality, we may assume that $\nu \leq \mu$. Put the elements of $C_i$ $i = 1, 2$ in order of non-decreasing weight. So $C_1 = \{\mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_\nu\}$ with $w(\mathbf{a}_1) \leq w(\mathbf{a}_2) \leq \cdots \leq w(\mathbf{a}_\nu)$, and $C_2 = \{\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_\mu\}$ with $w(\mathbf{b}_1) \leq w(\mathbf{b}_2) \leq \cdots \leq w(\mathbf{b}_\mu)$. Now the code $C_3$ consisting of the $\nu$ words $(\mathbf{a}_i, \mathbf{b}_i)$ $1 \leq i \leq \nu$, is a $C_f(n_1+n_2, d_1+d_2)$ code of cardinality $\nu$. This proves that $A_f(n_1 + n_2, d_1 + d_2) \geq \nu$. The theorem follows by induction. □

Theorem 2.3 is usually applied by using the two following corollaries.

**Corollary 2.1** *For any integer $r \geq 1$ and $f = a, u$*

$$A_f(n,d) \leq A_f(rn, rd).$$

*Proof:* Apply Theorem 2.3 repeatedly with $C_1 = C_2$. □

**Corollary 2.2** *For each $0 \leq s \leq n$ and $0 \leq t \leq d$,*

$$min\{A_f(s,t), A_f(n-s, d-t)\} \leq A_f(n,d)$$

*where $f$ stands for $a$ or $u$.*

*Proof:* This is the case $m = 2$ in Theorem 2.3. □

The next three theorems give the exact value of $A_a(n,d)$ when $d$ is large.

**Theorem 2.4** *Let $\lfloor n/2 \rfloor < d \leq n$. Then $A_a(n,d) = 2$.*

*Proof:* If on the contrary $C$ is a $C_a(n,d)$ code with $\lfloor n/2 \rfloor < d$ and $|C| = 3$, then, without loss of generality, the three words $\mathbf{1}$, $\mathbf{0}$ and $\mathbf{1}^a\mathbf{0}^b$ may be assumed to be the codewords of $C$ where $a \geq d$ and $b \geq d$. This implies that $n = a + b \geq 2d > n$, which is not possible. □

**Theorem 2.5** *Let $n$ be even. Then $A_a(n, n/2) = 4$.*

*Proof:* It even takes little effort to prove that such a code is unique and consists of $\mathbf{0}, \mathbf{1}$ and two complementary words of weight $n/2$. □

**Theorem 2.6** *Let $n$ be odd. Then*

$$A_a(n, \lfloor n/2 \rfloor) = \begin{cases} 8 & \text{if } n = 3; \\ 6 & \text{if } n = 5; \\ 4 & \text{if } n \geq 7. \end{cases}$$

*Proof:* The conclusion is obviously true for the case of $n = 3$, since $A_a(n,d) = A_a(3,1) = |\mathbf{V_3}| = 2^3 = 8$. Also, it is easy to show that any optimal $C_a(5,2)$ code has size 6 (see Theorem 5.1 in Chapter 5), i.e., $A_a(5,2) = 6$. Finally, when $n \geq 7$, we may write $n = 2d+1$ since $n$ is an odd number. From Theorem 2.5 and the fact that $A_a(n,d)$ is non-decreasing in $n$, it follows that $4 = A_a(n-1,d) \leq A_a(n,d)$. On the other hand, it can be readily shown that

$$\sum_{i=0}^{d-1} A_i \leq 1, \qquad \sum_{i=n-d+1}^{n} A_i \leq 1 \quad \text{and} \quad A_d + A_{d+1} \leq 2.$$

Therefore, $A_a(n,d) \leq 4$, which yields that $A_a(n,d) = 4$. □

The well known *Singleton bound* is used for estimating the function $A_h(n,d)$. Applying the same techniques (see e.g. [49]) to $C_a(n,d)$ codes, we can obtain the following similar result for the function $A_a(n,d)$.

**Theorem 2.7** *For $n \geq 2d$, $A_a(n,d) \leq 2^{n-2d+2}$.*

*Proof:* It is easy to see that $A_a(n,d) \leq 2A_a(n-1,d)$. Using the inequality $n-2d$ times and then using Theorem 2.5, one will arrive at $A_a(n,d) \leq 2^{n-2d}A_a(2d,d) = 2^{n-2d+2}$. □

**Theorem 2.8** *Let $C$ be a $C_a(n,d)$ code with weight distribution $A_0, A_1, \cdots, A_n$. Let $s$ and $i$ be integers such that $0 \leq s \leq i \leq n$. Define*

$$T = \sum_{j=i-s}^{i} A_j A'(s, 2d, i-j) \tag{2.2}$$

*Then*

$$T \leq \left\lfloor \frac{d(n+s)}{(d-i)(n+s)+i^2} \right\rfloor, \quad \text{if } i^2 \geq (i-d)(n+s). \tag{2.3}$$

*Proof:* Choose a subcode $C_1$ of $C$ such that $C_1 = \{\mathbf{c} \in C \mid i-s \leq w(\mathbf{c}) \leq i\}$. For $i-s \leq j \leq i$, let $T_j$ be a constant weight code of length $s$, minimum Hamming distance $2d$, constant weight $i-j$, containing $A'(s, 2d, i-j)$ words. Put

$$X = \bigcup_{j=i-s}^{i} \{(\mathbf{c}, \mathbf{x}) \mid \mathbf{c} \in C_1 \wedge w(\mathbf{c}) = j \wedge \mathbf{x} \in T_j\}.$$

Then $X$ is a code of length $n+s$, minimum Hamming distance $2d$ and constant weight $i$, containing $T$ words. We list the code $X$ as a $T$ by $n+s$ matrix and let $P$ be the sum of the inner products between all ordered pairs of distinct rows of $X$. Since any two different codewords in $X$ are of Hamming distance at least $2d$, and of the same weight $i$, their inner product is at most $i-d$. This leads to $P \leq T(T-1)(i-d)$.

On the other hand, if we take $y_j$ as the number of 1's in the $j$th column for $j = 1, 2, \cdots, n+s$, then the sum $\sum_{j=1}^{n+s} y_j$ is the total number of 1's in $X$ which equals $iT$. Hence, from the *Cauchy-Schwartz* inequality, it follows

$$\begin{aligned} P &= \sum_{j=1}^{n+s} y_j(y_j - 1) = \sum_{j=1}^{n+s} y_j^2 - \sum_{j=1}^{n+s} y_j \\ &\geq \frac{1}{n+s}\left(\sum_{j=1}^{n+s} y_j\right)^2 - \sum_{j=1}^{n+s} y_j = \frac{i^2T^2}{n+s} - iT. \end{aligned}$$

Therefore,

$$T(T-1)(i-d) \geq P \geq \frac{i^2T^2}{n+s} - iT.$$

This is equivalent to (2.3). □

**Corollary 2.3** *Let $C$ be a $C_a(n,d)$ code with weight distribution $A_0, A_1, \cdots, A_n$. Let $s$ and $i$ be integers such that $0 \leq s \leq i \leq n$, and $T$ be defined as in (2.2). Then*

$$(n+s)q(q-1) + 2rq \leq T(T-1)(i-d)$$

*where $q = \lfloor iT/(n+s) \rfloor$ and $r = iT - (n+s)q$.*

*Proof:* It is known [59] that the minimum of $\sum_{j=1}^{n+s} z_j^2$ subject to $\sum_{j=1}^{n+s} z_j = (n+s)q + r$ and the $z_j$'s being nonnegative integers, is attained when $z_1 = z_2 = \cdots = z_r = q+1$ and $z_{r+1} = z_{r+2} = \cdots = z_{n+s} = q$. Hence, from the proof of Theorem 2.8, it follows that

$$\begin{aligned} T(T-1)(i-d) &\geq \sum_{j=1}^{n+s} y_j^2 - \sum_{j=1}^{n+s} y_j \\ &\geq (r(q+1)^2 + (n+s-r)q^2) - ((n+s)q + r) \\ &= (n+s)q(q-1) + 2rq. \end{aligned}$$

This completes the proof. □

For larger values of $n$ and $d$, (2.3) in Theorem 2.8 is possibly more useful than Theorem 2.1 since it does not require any knowledge of $A(n,d,w)$ and is easy to compute for large values of $n$ if the condition shown in (2.3) is satisfied. As an example of applications of Theorem 2.8, we show

**Theorem 2.9** *$A_a(3d,d) \leq 13$ if $d \not\equiv 0$ (mod 3); $A_a(3d,d) \leq 14$ if $d \equiv 0$ (mod 3).*

*Proof:* Let $C$ be a $C_a(3d,d)$ code with weight distribution $A_0, A_1, \cdots, A_{3d}$. Without loss of generality, we may assume that $A_0 = A_{3d} = 1$. First, suppose that $d \not\equiv 0$ (mod 3). So $r = \lfloor d/3 \rfloor < d/3$. Consider $A_d, \cdots, A_{2d}$. From Theorem 2.1, it follows that

$$A_d + \ldots + A_{d+r} \leq A(3d+r, 2d, d+r) = A(3d+r, 2d, 2d). \tag{2.4}$$

Since $A(n,d,w) \geq 4$ iff $n \geq max\{3d-2w, d+2w/3, w+d/2\}$ (see e.g. [5]), (2.4) results in $A_d + \cdots + A_{d+r} \leq 3$. By symmetry, one also has $A_{2d-r} + \cdots + A_{2d} \leq 3$. It now suffices to prove that $g = A_{d+r+1} + \cdots + A_{2d-r-1} \leq 5$. This is guaranteed by Theorem 2.8:

$$g \leq \frac{d(3d+d-2r-2)}{(d-2d+r+1)(4d-2r-2)+(2d-r-1)^2} = 2d/(r+1) < 6.$$

Therefore, $|C| \leq 1+3+5+3+1 = 13$. This implies that $A_a(3d,d) \leq 13$ if $d \not\equiv 0$ (mod 3). Similarly, when $3 \mid d$, one has that $A_d + \cdots + A_{d-d/3-1} \leq 3$ and $A_{d+d/3} + \cdots + A_{2d-d/3} \leq 6$. Hence, $A_a(3d,d) \leq 14$ if $3 \mid d$. □

## 2.2 Some results related to code constructions

If the largest known lower bound on $A_a(n,d)$ is less than the least known upper bound, then it is possible to find a larger code to increase the lower bound, or to lower the upper bound, or both. For all options, investigation with the constraints on the weight distribution should be helpful in view of the constructions of codes. In this respect, the concept of $t$-designs provides tools for us. The following result is due to Van Lint et al. [50].

**Theorem 2.10** *Let $M$ be a (0,1)-matrix of size $v$ by $n$ with row sums $\geq r$. Suppose the inner product of any two distinct rows of $M$ is $\leq \lambda$ with*

$$\lambda \leq \frac{r}{v-1}\left(\frac{vr}{n}-1\right).$$

*Then $M$ is the incidence matrix of a 2-design $D(v,n,r,k,\lambda)$ with $k = (vr)/n$.*

The proof of Theorem 2.10 is an interesting application of the *Cauchy-Schwartz* inequality. It will be seen in Chapter 3 that Theorem 2.10 is also useful in improving the upper bounds obtained by Theorem 2.1.

Note that for a $C_f(n,d)$ $(f = a,u)$ code, the inner product of any two distinct codewords of weight $i$ $(i \geq d)$ is certainly less than or equal to $i-d$. Thus, as a consequence of Theorem 2.10, one corollary is given by

**Corollary 2.4** *Let $C$ be a $C_f(n,d)$ code $(f = a,u)$, and $A_i$ the number of codewords of $C$ of weight $i$. If*

$$i - d \leq \frac{i}{A_i - 1}\left(\frac{iA_i}{n} - 1\right),$$

*then the codewords of $C$ of weight $i$ form the incidence matrix of a 2-design $D(A_i, n, i, k, i-d)$ with $k = (iA_i)/n$.*

*Proof:* Replace $v$ by $A_i$, $r$ by $i$ and $\lambda$ by $i-d$ in Theorem 2.10. □

The following theorem will allow us sometimes to add some codewords to an already constructed asymmetric error-correcting code.

**Theorem 2.11** *Let $C$ be a $C_a(n,d)$ code containing* $\mathbf{0}$ *and* $\mathbf{1}$, *and let* $\mathbf{b} \in \mathbf{V_n}$ *such that* $d \leq w(\mathbf{b}) \leq w(\mathbf{a})$ *for all nonzero codewords* $\mathbf{a} \in C$. *Then both* $\mathbf{b}$ *and its complement* $\overline{\mathbf{b}}$ *can be added to $C$ iff for any nonzero codeword* $\mathbf{a} \in C$ *with* $\mathbf{a} \neq \mathbf{b}$, *the inner product between* $\mathbf{a}$ *and* $\mathbf{b}$ *satisfies* $<\mathbf{a},\mathbf{b}> \leq w(\mathbf{a}) - d$ *and*

$$<\mathbf{a},\mathbf{b}> \geq \begin{cases} w(\mathbf{a}) + w(\mathbf{b}) + d - n, & \text{if } n \geq w(\mathbf{a}) + w(\mathbf{b}) \\ d, & \text{otherwise.} \end{cases}$$

*Proof:* "$\Longrightarrow$" Suppose that both $\mathbf{b}$ and $\overline{\mathbf{b}}$ can be added to $C$. Let $\mathbf{a}$ be any nonzero codeword of $C$ different from $\mathbf{b}$. From (1.1) and $w(\mathbf{b}) \leq w(\mathbf{a})$, it follows that

$$\begin{aligned} 2d &\leq 2d_a(\mathbf{a},\mathbf{b}) = d_h(\mathbf{a},\mathbf{b}) + \mid w(\mathbf{a}) - w(\mathbf{b}) \mid \\ &= d_h(\mathbf{a},\mathbf{b}) + w(\mathbf{a}) - w(\mathbf{b}) \\ &= w(\mathbf{a}) + w(\mathbf{b}) - 2 <\mathbf{a},\mathbf{b}> + w(\mathbf{a}) - w(\mathbf{b}) \\ &= 2w(\mathbf{a}) - 2 <\mathbf{a},\mathbf{b}>. \end{aligned}$$

So $<\mathbf{a},\mathbf{b}> \leq w(\mathbf{a}) - d$. On the other hand, by replacing $\mathbf{b}$ by $\overline{\mathbf{b}}$ in (1.1), we find

$$\begin{aligned} 2d &\leq 2d_a(\mathbf{a},\overline{\mathbf{b}}) = d_h(\mathbf{a},\overline{\mathbf{b}}) + \mid w(\mathbf{a}) - w(\overline{\mathbf{b}}) \mid \\ &= d_h(\mathbf{a},\overline{\mathbf{b}}) + \mid w(\mathbf{a}) + w(\mathbf{b}) - n \mid. \end{aligned}$$

Hence, if $n \geq w(\mathbf{a}) + w(\mathbf{b})$ one has

$$\begin{aligned} 2d &\leq d_h(\mathbf{a},\overline{\mathbf{b}}) - w(\mathbf{a}) - w(\mathbf{b}) + n \\ &= w(\mathbf{a}) + w(\overline{\mathbf{b}}) - 2 <\mathbf{a},\overline{\mathbf{b}}> - w(\mathbf{a}) - w(\mathbf{b}) + n \\ &= w(\mathbf{a}) + n - w(\mathbf{b}) - 2(w(\mathbf{a}) - <\mathbf{a},\mathbf{b}>) + w(\mathbf{a}) + w(\mathbf{b}) - n \\ &= 2 <\mathbf{a},\mathbf{b}> + 2n - 2w(\mathbf{a}) - 2w(\mathbf{b}), \end{aligned}$$

while otherwise

$$\begin{aligned} 2d &\le d_h(\mathbf{a},\overline{\mathbf{b}}) + w(\mathbf{a}) + w(\mathbf{b}) - n \\ &= w(\mathbf{a}) + w(\overline{\mathbf{b}}) - 2 < \mathbf{a},\overline{\mathbf{b}} > + w(\mathbf{a}) + w(\mathbf{b}) - n \\ &= w(\mathbf{a}) + n - w(\mathbf{b}) - 2(w(\mathbf{a}) - < \mathbf{a},\mathbf{b} >) + w(\mathbf{a}) + w(\mathbf{b}) - n \\ &= 2 < \mathbf{a},\mathbf{b} > . \end{aligned}$$

"$\Longleftarrow$" Let $\mathbf{a}$ be a nonzero codeword of $C$ and $\mathbf{a} \ne \mathbf{b}$ such that $< \mathbf{a},\mathbf{b} > \le w(\mathbf{a}) - d$. Suppose that $\mathbf{b} \in C$ and $\overline{\mathbf{b}} \notin C$. Assuming that

$$< \mathbf{a},\mathbf{b} > \ge \begin{cases} w(\mathbf{a}) + w(\mathbf{b}) + d - n, & \text{if } n \ge w(\mathbf{a}) + w(\mathbf{b}) \\ d, & \text{otherwise.} \end{cases}$$

one can reverse the arguments above and obtain $d \le d_a(\mathbf{a},\overline{\mathbf{b}})$ (independent of $n \ge w(\mathbf{a}) + w(\mathbf{b})$ or not). Moreover, since $\mathbf{1} \in C$, $n - w(\mathbf{a}) \ge d$, also

$$d_a(\overline{\mathbf{b}},\mathbf{0}) = n - w(\mathbf{b}) \ge n - w(\mathbf{a}) \ge d.$$

Therefore also $\overline{\mathbf{b}}$ can be added to $C$.

If both $\mathbf{b} \notin C$ and $\overline{\mathbf{b}} \notin C$, then the inequalities satisfied by the inner product between $\mathbf{a}$ and $\mathbf{b}$ guarantee that $d \le d_a(\mathbf{a},\mathbf{b})$ and $d \le d_a(\mathbf{a},\overline{\mathbf{b}})$. Furthermore, we have

$$\begin{aligned} d_a(\mathbf{b},\mathbf{0}) &= w(\mathbf{b}) \ge d, \\ d_a(\overline{\mathbf{b}},\mathbf{0}) &= n - w(\mathbf{b}) \ge n - w(\mathbf{a}) \ge d, \\ d_a(\mathbf{b},\overline{\mathbf{b}}) &= max\{w(\mathbf{b}), n - w(\mathbf{b})\} \ge w(\mathbf{b}) \ge d. \end{aligned}$$

Together these inequalities imply that both $\mathbf{b}$ and $\overline{\mathbf{b}}$ can be added to $C$. □

A corollary to Theorem 2.11 is the following.

**Corollary 2.5** *Let $M$ be the $v \times n$ incidence matrix of a 2-design $D(v,n,r,k,\lambda)$. If $n \ge 3r - 2\lambda$ and $r \le n/2$, then all the rows of $M$ and the complement of them together form a binary asymmetric error-correcting code of length $n$ and distance $r - \lambda$.*

*Proof:* By definition each row of $M$ has weight $r$ and the inner product of each pair of distinct rows equals $\lambda$. Since $n \ge 3r - 2\lambda$, every pair of distinct rows $\mathbf{a}$ and $\mathbf{b}$ of $M$ satisfies $\lambda = < \mathbf{a},\mathbf{b} > \ge r + r + (r - \lambda) - n$. Let $d = r - \lambda$, then

$$w(\mathbf{a}) - d = < \mathbf{a},\mathbf{b} > \ge w(\mathbf{a}) + w(\mathbf{b}) + d - n.$$

Also, $r \le n/2$ implies that $n \ge w(\mathbf{a}) + w(\mathbf{b})$. Therefore the assertion follows from Theorem 2.11 immediately. □

Now we are ready to establish the bounds for $C_a(n,d)$ and $C_u(n,d)$ codes with which the following two chapters will be concerned.

# Chapter 3

# Bounds and constructions for codes capable of correcting asymmetric errors

## 3.1 Bounds and constructions for 5-AsEC codes

This section is devoted to the bounds on $A_a(n,6)$ for length $n \leq 27$. From Theorems 2.4, 2.5 and 2.6, it is only necessary to consider $C_a(n,6)$ codes for $n \geq 14$. All proofs in this section consist of two parts: an upper bound on the cardinality of such a code is derived and an actual construction is given. Because of the lengths of the proofs and their similarities, we shall only give the complete proofs of some of the theorems. For the other cases only some information is given. The interested reader can find the complete proofs in [17].

Throughout this chapter, it will be assumed that any $C_a(n,d)$ code contains the all-one vector $\mathbf{1}$ and the all-zero vector $\mathbf{0}$. That assumption is valid without loss of generality, according to Kløve [33]. It follows that $A_i = A_{n-i} = 0$ for $i = 1, 2, \cdots, d-1$.

**Theorem 3.1** $A_a(14,6) = 4$.

*Proof:* Let $C$ be an optimal $C_a(14,6)$ code. From Theorem 2.1 ($s$=2, $w$=8) it follows that $A_6 + A_7 + A_8 \leq 2$. Hence

$$|C| = A_a(14,6) = \sum_{i=0}^{14} A_i \leq 1 + 2 + 1 = 4.$$

On the other hand, one can even construct a $C_a(14,7)$ code: take $\mathbf{0}$, $\mathbf{1}$ and two complementary words of weight 7. □

**Theorem 3.2** $A_a(15,6) = 6$.

*Proof:* Let $C$ be an optimal $C_a(15,6)$ code. From Theorem 2.1 ($s$=1, $w$=7,9), it follows that $A_6 + A_7 \leq 2$ and $A_8 + A_9 \leq 2$. So

$$|C| = A_a(15,6) = \sum_{i=0}^{15} A_i \leq 1 + 2 + 2 + 1 = 6.$$

On the other hand, a $C_a(15,6)$ code of size 6 can be obtained by applying Corollary 2.1 with $r = 3$ to a $C_a(5,2)$ code of size 6. □

**Theorem 3.3** $A_a(16,6) = 7$.

*Proof:* Let $C$ be an optimal $C_a(16,6)$ code. From Theorem 2.1 ($s$=2, $w$=8; $s$=1, $w$=10), it follows that $A_6 + A_7 + A_8 \leq 3$ and $A_9 + A_{10} \leq 2$. Hence

$$|C| = A_a(16,6) = \sum_{i=0}^{16} A_i \leq 1 + 3 + 2 + 1 = 7.$$

On the other hand, a code with this cardinality can be found by applying Corollary 2.1 with $r = 2$ to a $C_a(8,3)$ code of size 7 (which can be found in [12]). □

**Theorem 3.4** $A_a(17,6) = 8$.

*Proof:* Let $C$ be an optimal $C_a(17,6)$ code. From Theorem 2.1 ($s$=2, $w$=8,11), it follows that $A_6 + A_7 + A_8 \leq 3$ and $A_9 + A_{10} + A_{11} \leq 3$, which leads to

$$|C| = A_a(17,6) = \sum_{i=0}^{17} A_i \leq 1 + 3 + 3 + 1 = 8.$$

A code of this size is given by 00000, 1F800, 007E0, 1861E, 071DC, 13CF3, 0CB6F and 1FFFF. □

**Theorem 3.5** $A_a(18,6) = 12$.

*Proof:* Let $C$ be an optimal $C_a(18,6)$ code. From Theorem 2.1 ($s$=1, $w$=7,12; $s$=2, $w$=10), it follows that $A_6 + A_7 \leq 3$, $A_8 + A_9 + A_{10} \leq 6$ and $A_{11} + A_{12} \leq 3$. So

$$|C| = A_a(18,6) = \sum_{i=0}^{18} A_i \leq 1 + 3 + 6 + 3 + 1 = 14.$$

Next, we shall lower this upper bound to 12.

(a) Suppose that $|C|$=14. Then $A_6 + A_7 = 3$ and $A_8 + A_9 + A_{10} = 6$. From Theorem 2.1 ($s$=1, $w$=10), it follows that $A_9 + A_{10} \leq 4$. This means that $A_8$ must be greater than or equal to two. Obviously, the pair $(A_6, A_7)$ only has four possible values: (3,0),(0,3),(1,2) and (2,1). However, it is easy to see that $A_6 = 3$ or $A_7 = 3$ implies $A_8 = 0$, and that $A_7 = 2$ will lead to $A_8 \leq 1$. Since the triple $(A_6, A_7, A_8)$ cannot be (2,1,2) or (1,2,2), according to Theorem 2.2 ($i$=8, $l$=2) and Theorem 2.1 ($s$=1, $w$=8), we get a contradiction with the assumptions. So $A_6 + A_7 = 3$ implies that $A_8 + A_9 + A_{10} \leq 5$.

(b) Similarly, for reasons of symmetry, the assumption $A_{11} + A_{12} = 3$ implies that $A_8 + A_9 + A_{10} \leq 5$.

(c) Suppose that $A_6 + A_7 = 3$, $A_{11} + A_{12} = 3$ and $A_8 + A_9 + A_{10} = 5$. Then, from Theorem 2.1 ($s$=1, $w$=10), it follows that $A_9 + A_{10} \leq 4$. Hence $A_8 \geq 1$. But $A_8$ must be less than 2, as shown in (a). So $A_8 = 1$. Therefore, by symmetry, $A_{10} = 1$ and thus $A_9 = 3$. This is not possible by Theorem 2.2 ($i$=10, $l$=2).

It follows from (a) to (c) that

$$|C| = A_a(18,6) = \sum_{i=0}^{18} A_i \leq 1 + 10 + 1 = 12.$$

The existence of a $C_a(18,6)$ code of size 12 follows from Corollary 2.1 applied with $r = 3$ to an optimal $C_a(6,2)$ code (of size 12). □

The next cases will involve deeper analysis of the weight structures of these codes. Only in the first case this more detailed analysis will be demonstrated. For the other cases we refer the reader to [17].

**Theorem 3.6** $A_a(19,6) = 16$.

*Proof:* Let $C$ be an optimal $C_a(19,6)$ code. From Theorem 2 ($s$=2, $w$=8,13; $s$=1, $w$=10), it follows that $A_6 + A_7 + A_8 \leq 5$, $A_9 + A_{10} \leq 6$ and $A_{11} + A_{12} + A_{13} \leq 5$. These inequalities yield

$$|C| = A_a(19,6) = \sum_{i=0}^{19} A_i \leq 1 + 5 + 6 + 5 + 1 = 18.$$

A further analysis on the weight distribution of $C$ shows that the upper bound on $|C|$ is 16 rather than 18.

(a) Let $C'$ be a $C_a(19,6)$ code satisfying $A_9 + A_{10} = 6$. We extend these six words with an overall parity check symbol. Without loss of generality, they may be listed as in Figure 3.1.

$$6\left\{\begin{array}{|c|c|}\hline 0 & \\ \vdots & \text{Codewords of } C' \text{ of weight } 10 \\ 0 & \\ \hline 1 & \\ \vdots & \text{Codewords of } C' \text{ of weight } 9 \\ 1 & \\ \hline \end{array}\right.$$

Figure 3.1: The six extended codewords in the proof of Theorem 3.6.

From Theorem 2.10 ($r$=10, $v$=6, $n$=20, $\lambda \leq 4$), it follows that Figure 3.1 will form the incidence matrix of a 2-design $D(6, 20, 10, 3, 4)$.

This implies that every column in Figure 3.1 will contain exactly three ones. Therefore, $A_9 = A_{10} = 3$, which concludes that $A_8 = 0$. Indeed, if the opposite holds, let **b** represent a codeword of weight 8, then, without loss of generality, the word **b** may be assumed in such a way that its first eight coordinates are all ones and the remaining eleven positions are zeros, as listed in the last row of Figure 3.2. Because the distance $\geq 6$, there are at most three ones in the first eight positions for the codewords of weight 9, and four ones in the first eight positions for the codewords of weight 10 respectively. So they may be arranged as in Figure 3.2. There $R_i$ indicates the remaining 11 coordinates of codewords of weight $i$ for $i$=9,10. Counting the number of ones in the first eight coordinates of the six codewords of weight 9 and weight 10 rowwise and columnwise in Figure 3.2 leads to $24 = 8 \times 3 \leq 3 \times 3 + 3 \times 4 = 21$, which is a contradiction.

| | |
|---|---|
| Weight $\leq 4$ | $R_{10}$ |
| Weight $\leq 3$ | $R_9$ |
| 11111111 | $0 \cdots 0$ |

Figure 3.2: Illustration figure when $A_8 \neq 0$ in the proof of Theorem 3.6.

Proceeding in the same way, one has $A_{11} = 0$. On the other hand, Theorem 2.1 ($s$=1, $w$=7,13) shows that $A_6+A_7 \leq 3$ and $A_{12}+A_{13} \leq 3$. So

$$|C'| = \sum_{i=0}^{19} A_i \leq 1 + 3 + 6 + 3 + 1 = 14.$$

This produces that the maximum size of any $C_a(19,6)$ code with $A_9 + A_{10} = 6$ never exceeds 14. Thus we can conclude that

$$|C| = A_a(19,6) = \sum_{i=0}^{19} A_i \leq 1 + 5 + 5 + 5 + 1 = 17.$$

(b) Suppose that $|C| = 17$. This will, from (a), result in $A_6+A_7+A_8 = 5$, $A_9 + A_{10} = 5$ and $A_{11}+A_{12}+A_{13} = 5$. Also, from Theorem 2.1 ($s$=0, $w$=6,7,8,9,10; $s$=1, $w$=7,8,9), it follows that $A_6 \leq 3$, $A_7 \leq 3$, $A_8 \leq 3$, $A_9 \leq 4$, $A_{10} \leq 4$, $A_6 + A_7 \leq 3$, $A_7 + A_8 \leq 5$ and $A_8 + A_9 \leq 5$. Since $A_6 = 3$ or $A_7 = 3$ implies that $A_8 = 0$, the triple $(A_6, A_7, A_8)$ can only have five possible values: (2,1,2), (2,0,3), (1,2,2), (1,1,3), (0,2,3), while the pair $(A_9, A_{10})$ can only have three alternatives: (1,4), (3,2), (2,3). But, by Theorem 2.2 ($i$=10, $l$=2), the triple $(A_8, A_9, A_{10})$ cannot take any of these possible values; consequently, either $A_6 + A_7 + A_8 \leq 4$ or $A_9 + A_{10} \leq 4$, which contradicts the assumption of $|C| = 17$.

Finally, from (a) and (b), it follows that

$$|C| = A_a(19,6) = \sum_{i=0}^{19} A_i \leq 1 + 14 + 1 = 16.$$

From previous analyses, we are now inspired to find how the weight distribution of $C$ can be if $C$ contains 16 codewords. Suppose that $|C| = 16$, then it follows from the statements in (b) that $A_9+A_{10} = 4$, $A_6+A_7+A_8 = 5$ and $A_{11} + A_{12} + A_{13} = 5$ due to symmetry. So the pair $(A_9, A_{10})$ can only take the values $(2,2), (3,1)$ or $(1,3)$. According to symmetry again, we only need to consider two pairs $(2,2)$ and $(3,1)$. From $A_8 + A_9 \leq 5$ and Theorem 2.2 ($i$=9,10, $l$=2), it follows that the triple $(A_7, A_8, A_9)$ cannot be $(1,2,3)$, $(2,2,3)$ or $(2,2,2)$, and the triple $(A_8, A_9, A_{10})$ cannot be $(3,2,2)$. Therefore, the weight distribution of $C$ will be uniquely determined if **1** and **0** are codewords, and it is given by

$$\begin{array}{rlllllllll} & \{ & A_6, & A_7, & A_8, & A_9, & A_{10}, & A_{11}, & A_{12}, & A_{13} \ \} \\ = & \{ & 2, & 1, & 2, & 2, & 2, & 2, & 1, & 2 \ \}. \end{array} \tag{3.1}$$

In Appendix $B$, a $C_a(19,6)$ code which contains 16 codewords and satisfies (3.1) is presented. It is denoted by $C_{19}$. □

**Theorem 3.7** $22 \leq A_a(20,6) \leq 23$.

*Proof:* The standard inequalities of Theorem 2.1 ($s$=2, $w$=8,11,14) yield

$$A_a(20,6) = \sum_{i=0}^{20} A_i \leq 1 + 6 + 12 + 6 + 1 = 26.$$

In [17] it is shown how a more careful analysis of the weight structure results in the upper bound $A_a(20,6) \leq 23$.

A construction of a $C_a(20,6)$ code $C_{20}$ with 22 codewords will now be given. The codewords of weight 9 and 10 depend on a projective plane of order 2. Let $P$ be the $7 \times 7$ circulant with top row (1101000). Then $P$ is the incidence matrix of a projective plane of order 2. So the inner product between any two distinct rows of $P$ is equal to 1. Let $J$ be a 7 by 7 matrix in which all entries are equal to 1. Evidently, the inner product between any two different rows of $J - P$ equals 2. Put

$$M = \begin{pmatrix} P^* & P & J-P \end{pmatrix}$$

where $P^*$ is the punctured version of $P$ by deleting the first column of $P$. To the seven rows of $M$ we add **1**, **0** and the following thirteen

54112, 082$C$7, $A$0878, 07$F$40, 79488, 3$F$983, $DF$624,
$E$2$F$98, 037$EF$, $ACA$3$F$, 5$DCF$9, $F$3976, $BE$7$D$5.

These words form the $C_a(20,6)$ code $C_{20}$ of cardinality 22. □

**Theorem 3.8** $32 \le A_a(21,6) \le 34$.

*Proof:* The standard inequalities of Theorem 2.1 ($s$=2, $w$=8,15; $s$=1, $w$=10,12) yield

$$A_a(21,6) = \sum_{i=0}^{21} A_i \le 1 + 6 + 11 + 11 + 6 + 1 = 36.$$

This upper bound can be further improved to $A_a(21,6) \le 34$ (see [17]).

In the following construction of a $C_a(21,6)$ code of size 32, we again start with 2-designs to construct most of the codewords and then add other words while keeping the distance at 6. Let $C_{21}$ be a $C_a(21,6)$ code satisfying $A_{10}+A_{11} = 12$. Then, Theorem 2.10 shows that all the codewords of weight 10 and weight 11 are nothing but a punctured version obtained by deleting one block from a 2-design $D(12,22,11,6,5)$. Let $A = circ(10000110101)$ and $B = circ(11010001101)$. Set

$$M = \begin{pmatrix} 11111111111 & 00000000000 \\ A & B \end{pmatrix}.$$

Then $M$ is the incidence matrix of a 2-design $D(12,22,11,6,5)$. Let $M_1$ be the matrix obtained by deleting the first column of $M$. The rows of $M_1$ will be the six codewords of weight 10 and the six codewords of weight 11 in $C_{21}$. Consider the five following words of weight 9:

$$M_2 = \begin{pmatrix} 000100111000110101100 \\ 001110100001011000011 \\ 010001001100001101011 \\ 101000100110000110101 \\ 110100010011000011010 \end{pmatrix}.$$

It can easily be checked that the rows of the matrix $M_2$, together with the rows of the matrix $M_1$ of weight 10 form a punctured version of the incidence matrix of a 2-design $D(11,22,10,5,4)$ (by omitting one of the blocks). Each row of $M_2$ satisfies the inequalities in Theorem 2.11 when compared with the rows of $M_1$. So the rows of $M_2$, together with their complements, denoted by the matrix $M_3$, can be added to $C_{21}$ as the codewords of weight 9 and weight 12.

To these 22 words of $C_{21}$ (made from all the rows of $M_i$ for $i = 1,2,3$), the rows of the following matrix can be added

$$M_4 = \begin{pmatrix} 000000001101010010110 \\ 000010010010100100011 \\ 111100000000010100000 \\ 000001100000101011000 \end{pmatrix}$$

as the codewords of weight 6 and weight 7, and the rows of

$$M_5 = \begin{pmatrix} 000000111011111111111 \\ 011111100101010111110 \\ 101111010110101101111 \\ 111101111101111010001 \end{pmatrix}$$

can be added as the codewords of weight 14 and weight 15. Also **1** and **0** can be included. Obviously, $C_{21}$ is now the desired $C_a(21,6)$ code of size 32. □

**Theorem 3.9** $48 \leq A_a(22,6) \leq 60$.

*Proof:* Theorem 2.1 ($s$=0, $w$=11; $s$=1, $w$=10; $s$=2, $w$=8) shows

$$A_a(22,6) = \sum_{i=0}^{22} A_i \leq 1 + 9 + 16 + 12 + 16 + 9 + 1 = 64.$$

A more careful analysis reduces this bound further to $A_a(21,6) \leq 60$ (see [17]). For a construction of a $C_a(22,6)$ code of size 48, we start with the $(n = 23, d = 12, w = 10)$ optimal, constant weight code mentioned in [5]. This code contains 16 codewords in which six begin with 1 and ten with 0. Let $M$ contain these codewords punctured on the first coordinate. It is a $C_a(22,6)$ code with $A_9 = 6$ and $A_{10} = 10$. To $M$, add all the complements of words of $M$ (using Theorem 2.11). Also add **0** and **1** as well as the fourteen following words

$$\begin{array}{lllll} 2FEBC7, & 0BFD7A, & 15779F, & 3C8EFB, & 36F374, \\ 0DA4DA, & 1696A9, & 2A58F8, & 316A8B, & 090D07, \\ 321324, & 028478, & 14508A, & 00A381. & \end{array}$$

This gives a $C_a(22,6)$ code of size 48. It is denoted by $C_{22}$. □

**Theorem 3.10** $66 \leq A_a(23,6) \leq 110$.

*Proof:* Theorem 2.1 ($s$=2, $w$=1; $s$=8, $w$=10; $s$=0, $w$=11) shows

$$A_a(23,6) = \sum_{i=0}^{23} A_i \leq 1 + 10 + 24 + 23 + 23 + 24 + 10 + 1 = 116.$$

This upper bound can be lowered further to $A_a(23,6) \leq 110$ (see [17]). Next, we shall present a $C_a(23,6)$ code containing 66 codewords. Let $M = circ(00101001100110101111000)$. Then, $M$ is the incidence matrix of a symmetric 2-design $D(23,23,11,11,5)$. Thus, the inner product of any two distinct rows of $M$ will equal 5. From Corollary 2.4, it follows that all the rows of $M$ and their complements will form a $C_a(23,6)$ code. Let $C_{23}$ represent the code consisting of these 46 words. To $C_{23}$, we add the following words

$$
\begin{aligned}
\mathbf{a}_1 &= (00000000000000000000000),\\
\mathbf{a}_2 &= (00001100010010000100010),\\
\mathbf{a}_3 &= (00110001000100000010001),\\
\mathbf{a}_4 &= (10100010000000011001100),\\
\mathbf{a}_5 &= (00000000000011110011011),\\
\mathbf{a}_6 &= (00000000011101001100101),\\
\mathbf{a}_7 &= (00000111101000000111000),\\
\mathbf{a}_8 &= (00011010100100101000010),\\
\mathbf{a}_9 &= (01011101000001010000100),\\
\mathbf{a}_{10} &= (11100000111001010000000),
\end{aligned}
$$

and their complements (using Theorem 2.11). It is easy to see that we have obtained now a $C_a(23,6)$ code with 66 codewords, denoted by $C_{23}$. □

**Theorem 3.11** $91 \leq A_a(24,6) \leq 210$.

*Proof:* Theorem 2.1 ($s$=0, $w$=13; $s$=1, $w$=10,12,15; $s$=2, $w$=8,18) guarantees

$$A_a(24,6) = \sum_{i=0}^{24} A_i \leq 2(1+13+39)+70+34 = 210.$$

We are going to construct a $C_a(24,6)$ code of size 91 in which the codewords of weight 11 and weight 12 depend upon a symmetric conference matrix of 26 by 26. In Table 7 of [7], four inequivalent symmetric conference matrices of order 26 are listed. Take the first one and denote it by $A$. By its symmetry, only the upper triangular part of $A$ has to be presented. In octal form, this is

77770000760176014606074414146300606367256126535052461
32544363456166544232643512750770247266314634536156 00

Put $B = \overline{A} + I$ where $\overline{A}$ is the matrix made from the complements of the rows of $A$ and $I$ the identity matrix. Then, all rows of $A$ and $B$ together form a $(n=25, d=12, w=12)$ constant weight code (cf. [47]). Delete the first column of both $A$ and $B$, and add the 39 other words listed in Appendix $B$, plus $\mathbf{1}$ and $\mathbf{0}$. All the words mentioned above form a $C_a(24,6)$ code, indicated by $C_{24}$, of size 91. □

**Theorem 3.12** $124 \leq A_a(25,6) \leq 380$.

*Proof:* From Theorem 2.1 ($s$=0, $w$=10; $s$=1, $w$=7,9,12), it follows that

$$A_a(25,6) = \sum_{i=0}^{25} A_i \leq 2(1+5+28+39+117) = 380.$$

On the other hand, a $C_a(25,6)$ code of size 124 will be constructed below. Honkala [28] constructed a $(n=26, d=12, w=13)$ constant weight code of size 58 in the following way. Let $B$ be the circulant with top row

$$(0\ \ +1\ \ -1\ \ +1\ \ +1\ \ -1\ \ -1\ \ -1\ \ -1\ \ +1\ \ +1\ \ -1\ \ +1).$$

This is a Jacobsthal matrix of order 13. Let $B_1$ and $B_2$ be the 13 by 26 matrices obtained from $B$ by encoding its rows according to the rules $0 \to 01$, $+1 \to 11$, $-1 \to 00$ and rules $0 \to 01$, $+1 \to 00$, $-1 \to 11$ respectively. Also, let $B_3$ be the 32 by 26 matrix made by encoding the codewords of the binary code $(n=13, M=32, d=6)$ in [36] according to rules $0 \to 01$, $1 \to 10$. Put $D = (B_1^T, B_2^T, B_3^T)^T$. Deleting the first column of $D$ will yield the words of weight 12 and weight 13 in a code. Adding the 64 words listed in Appendix $B$ plus **1** and **0** will result in a $C_a(25,6)$ code, called $C_{25}$, of size 124. □

**Theorem 3.13** $173 \leq A_a(26,6) \leq 721.$

*Proof:* It follows from Theorem 2.1 ($s$=0, $w$=6,7,8,13; $s$=1, $w$=8,10,12; $s$=2, $w$=8) and one additional argument (see [17]) that

$$A_a(26,6) = \sum_{i=0}^{26} A_i \leq 2(1+17+75+209)+117 = 721.$$

In Appendix $B$, a $C_a(26,6)$ code of size 173, denoted by $C_{26}$, is presented in which the 58 codewords of weight 13 are the rows of the matrix $D$ defined in the proof of Theorem 3.12. □

**Theorem 3.14** $249 \leq A_a(27,6) \leq 1350.$

*Proof:* It follows from Theorem 2.1 ($s$=1, $w$=7,9,11) that

$$A_a(27,6) = \sum_{i=0}^{27} A_i \leq 2(1+8+46+109+430) = 1350.$$

On the other hand, by omitting the first coordinate from all the codewords of the $(n=28, d=12, w=14)$ constant weight code of cardinality 106 as described in [5], 53 words of weight 13 and 53 words of weight 14 are obtained. To them (together with **1** and **0**), the 141 other words in Appendix $B$ can be added. This gives a $C_a(27,6)$ code, denoted by $C_{27}$, of size 249. □

In this section, the upper bounds on $A_a(n,6)$ for length $n \leq 27$ have been derived. And for each of these lengths, a code has been constructed, that leads to the lower bound of $A_a(n,6)$. All the results produced in this section are listed in the second column of Table A.3 in Appendix $A$. In the next section, we shall present similar results for $A_a(n,7), n \leq 27$.

## 3.2 Bounds and constructions for 6-AsEC codes

From Theorems 2.5 and 2.6, it immediately follows that $A_a(14,7) = 4$ and $A_a(15,7) = 4$. The remaining cases will be shown in detail in the following theorems.

**Theorem 3.15** $A_a(14,7) = A_a(15,7) = A_a(16,7) = A_a(17,7) = 4.$

*Proof:* From Theorem 3.1 it follows that $A_a(14,7) \geq 4$. So it remains to prove that $A_a(17,7) \leq 4$. Let $C$ be an optimal $C_a(17,7)$ code. From Theorem 2.1 ($s$=3, $w$=10), it follows that $A_7 + A_8 + A_9 + A_{10} \leq 2$. So $|C| = A_a(17,7) \leq 1+2+1 = 4$. □

**Theorem 3.16** $A_a(18,7) = 6.$

*Proof:* Applying Theorem 2.1 ($s$=2, $w$=9; $s$=1,$w$=11) to the present case leads to $A_a(18,7) \leq 1+2+2+1 = 6$. A $C_a(18,7)$ code, denoted by $X_{18}$, of size 6 can be constructed by means of Corollary 2.2 with $s$=5 and $t$=2, where $C_5$ is an optimal $C_a(5,2)$ code and $C_{13}$ is the optimal $C_a(13,5)$ code in [59]. □

**Theorem 3.17** $A_a(19,7) = 7.$

*Proof:* Exploiting Theorem 2.1 ($s$=1,$w$=8,10,12) with a minor improvement (see [17]) results in $A_a(19,7) \leq 1+5+1 = 7$. Since $A_a(11,4) = 8$ and $A_a(8,3) = 7$, the assertion follows from Corollary 2.2 by taking $s$=8 and $t$=3. □

**Theorem 3.18** $A_a(20,7) = 9.$

*Proof:* From Theorem 2.1 ($s$=3, $w$=10; $s$=2, $w$=13), it follows that $A_a(20,7) \leq 1+4+3+1 = 9$. A $C_a(20,7)$ code, indicated by $X_{20}$, of size 9 is given by 00000, 038C3, 1C30C, E03F0, FFC00, 325AF, 5BBD6, AD67D, FFFFF. □

**Theorem 3.19** $A_a(21,7) = 12.$

*Proof:* From Theorem 2.1 ($s$=2, $w$=9,14; $s$=1, $w$=11), it follows that $A_a(21,7) \leq 1+3+4+3+1 = 12$. The construction of a $C_a(21,7)$ code of size 12 follows from Corollary 2.2 with $s$=6 and $t$=2 (since $A_a(6,2) = A_a(15,5) = 12$). A $C_a(21,7)$ code, denoted by $X_{21}$, of cardinality 12 is made by juxtaposing an optimal $C_a(6,2)$ code on the optimal $C_a(15,5)$ code in [59], and listed in Appendix $B$. □

From now on we shall not indicate the values of the parameters $s$ and $w$ when using Theorem 2.1. The reader should have no problem finding them.

**Theorem 3.20** $A_a(22,7) = 14$ *and* $19 \leq A_a(23,7) \leq 20.$

*Proof:* The standard inequalities of Theorem 2.1 yield $A_a(22,7) \leq 2(1+4)+6 = 16$ and $A_a(23,7) \leq 2(1+3+7) = 22$. Both can be further reduced (see [17]) to $A_a(22,7) \leq 14$ and $A_a(23,7) \leq 20$ respectively. In Appendix $B$, a $C_a(22,7)$ code, denoted by $X_{22}$, of size 14 can be found, and Saitoh et al. [45] found a $C_a(23,7)$ code of size 19. This completes the proof. □

**Theorem 3.21** $27 \leq A_a(24,7) \leq 30$ *and* $40 \leq A_a(25,7) \leq 46$.

*Proof:* From Theorem 2.1, it follows that $A_a(24,7) \leq 2(1+6+7)+6 = 34$ and $A_a(25,7) \leq 2(1+6+10)+14 = 48$. Further analyses (see [17]) on weight structures lower these bounds to $A_a(24,7) \leq 30$ and $A_a(25,7) \leq 46$.

In order to construct a code of length 24 and distance 7, we start with two 2-designs: $D(8,14,7,4,3)$ and $D(11,11,5,5,2)$, both are taken from Table I.1 in [25]. Erase the last three rows from the incidence matrix of the second design and then juxtapose it to the first design. This yields a $(n=25, d=14, w=12)$ constant weight code of size 8. Deleting the first coordinate from these codewords results in four words of weight 12 and four words of weight 11. To these eight words, nineteen other words (see Appendix $B$) can be added in such a way that they together form a $C_a(24,7)$ code, denoted by $X_{24}$, of size 27.

A $C_a(25,7)$ code, denoted by $X_{25}$, containing 40 codewords is given in Appendix $B$ too. The fourteen codewords of weight 12 and weight 13 in this code are obtained in the following way: take the complements of all the rows of the incidence matrix of the symmetric 2-design $D(27,27,13,13,6)$ from Table I.1 of [25], denoted by $D$, then delete the first coordinate of the words in $D$ and those 13 words starting with 0. In addition, the six codewords of weight 14 are chosen as the complements of the six codewords of weight 11 (using Theorem 2.11). □

**Theorem 3.22** $58 \leq A_a(26,7) \leq 80$ *and* $80 \leq A_a(27,7) \leq 144$.

*Proof:* From Theorem 2.1, it follows that $A_a(26,7) \leq 2(1+7+13+13)+14 = 82$ and $A_a(27,7) \leq 2(1+7+21+43) = 144$. The first bound can be further lowered (see [17]) to $A_a(26,7) \leq 80$.

A $C_a(26,7)$ code, denoted by $X_{26}$, can be constructed in the following way: the 14 codewords of weight 13 and the 13 codewords of weight 14 are obtained from the rows of $D$ as defined in the proof of Theorem 3.21 by deleting the first column. The complements of codewords of weight 14 will give the codewords of weight 12 (using Theorem 2.11), and finally, based on these 40 codewords, the 18 words listed in Appendix $B$ are added. This will be the code $X_{26}$ of size 58.

Take all the rows of $D$ (defined in Theorem 3.21) and their complements (using Corollary 2.4). Based on these 54 words, the 26 other words presented in Appendix $B$ can be added to form the set $X_{27}$. Clearly, $X_{27}$ is a $C_a(27,7)$ code containing 80 codewords. □

All the results produced in this section are summarized in the third column of Table A.3 in Appendix $A$ for an asymmetric distance = 7.

## 3.3 Bounds and constructions for 7-AsEC and 8-AsEC codes

This section explains the lower and upper bounds on $A_a(n,d)$ for $d$=8 and 9, and for $n \leq 27$. Since the constructions for $C_a(n,d)$ codes are trivial if Corollary 2.1 or Corollary 2.2 is used, it is not necessary to present the codewords for every code, we only need to show its upper bound. From Theorems 2.4, 2.5 and 2.6, it follows directly that

$$\begin{array}{ll} A_a(n,8) = 2, & \text{for } n = 8,\cdots,15, \\ A_a(n,9) = 2, & \text{for } n = 9,\cdots,17, \\ A_a(16,8) = 4, & A_a(17,8) = 4, \\ A_a(18,9) = 4, & A_a(19,9) = 4. \end{array}$$

Furthermore, by using Theorem 2.1, with a little effort it can be proved that

$$\begin{array}{l} A_a(18,8) = A_a(19,8) = 4, \\ A_a(20,9) = A_a(21,9) = A_a(22,9) = 4. \end{array}$$

Below we show the remaining cases.

**Theorem 3.23** $A_a(20,8) = A_a(21,8) = 6$.

*Proof:* On one hand, from Theorem 2.1, it follows that $A_a(21,8) \leq 1+2+2+1 = 6$. On the other hand, a $C_a(20,8)$ code containing six codewords can be constructed by applying Corollary 2.1 to an optimal $C_a(10,4)$ code of size 6. □

**Theorem 3.24** $A_a(22,8) = 8$, $A_a(23,8) = 9$ *and* $A_a(24,8) = 12$.

*Proof:* From Theorem 2.1, it follows that $A_a(22,8) \leq 1+3+3+1 = 8$. The lower bound follows from $A_a(11,4)$=8 [59] and Corollary 2.1 with $r = 2$.

Similarly, one can get (see [17]) that $A_a(23,8) \leq 9$ (additional argument with Theorem 2.1) and $A_a(24,8) \leq 12$. The lower bounds respectively follow from the $C_a(23,8)$ code by Honkala [29]:

$$\begin{array}{lll} 11111111 & 11111111 & 1111111 \\ 00000000 & 11111111 & 1111111 \\ 11111111 & 00000000 & 1111111 \\ 00000000 & 00000000 & 0000000 \\ 11000000 & 11100000 & 0111000 \\ 00111000 & 00011000 & 0000111 \\ 10100110 & 10010110 & 1100100 \\ 01010101 & 01001101 & 1010010 \\ 10101011 & 01101011 & 0001001 \end{array} \qquad (3.2)$$

and from $A_a(12,4) = 12$ [59] by applying Corollary 2.1 with $r = 2$. □

**Theorem 3.25** *$13 \le A_a(25,8) \le 14$, $18 \le A_a(26,8) \le 19$ and $23 \le A_a(27,8) \le 26$.*

*Proof:* From Theorem 2.1, it follows that

$$\begin{aligned} A_a(25,8) &\le 1+5+4+5+1 = 16, \\ A_a(26,8) &\le 2(1+4)+5+7 = 22, \\ A_a(27,8) &\le 2(1+6+7) = 28. \end{aligned}$$

In [17] one can find how these upper bounds can be refined to $A_a(25,8) \le 14$, $A_a(26,8) \le 19$ and $A_a(27,8) \le 26$. In Appendix $B$, a $C_a(25,8)$ code containing 13 codewords is presented. It is denoted by $Y_{25}$. Again, in Appendix $B$, a $C_a(27,8)$ code containing 23 codewords and denoted by $Y_{27}$, is shown. The second lower bound immediately follows from $A_a(13,4) = 18$ [59] and Corollary 2.1 with $r = 2$. □

Bounds on $A_a(n,9)$ for $n \le 27$ can be obtained more readily.

**Theorem 3.26** *$A_a(23,9) = 6$, $A_a(24,9) = 7$ and $A_a(25,9) = 8$.*

*Proof:* Theorem 2.1 (see [17]) yields $A_a(23,9) \le 6$, $A_a(24,9) \le 7$ and $A_a(25,9) \le 8$. The lower bounds respectively follow from $A_a(13,5) = A_a(10,4) = 6$ [59] and Corollary 2.2 with $s$=10 and $t$=4, from $A_a(8,3) = 7$ [12] and Corollary 2.1 with $r$=3, and from $A_a(14,5) = A_a(11,4) = 8$ [59] and Corollary 2.2 with $s$=11 and $t$=4. □

**Theorem 3.27** *$A_a(26,9) = 9$ and $A_a(27,9) = 12$.*

*Proof:* Theorem 2.1 with further analyses on weight distributions (see [17]) derives that $A_a(26,9) \le 9$ and $A_a(27,9) \le 12$. On the other hand, it is known that $A_a(20,7) = 9$ (Theorem 3.18) and $A_a(6,2) = 12$. Hence, $A_a(26,9) = 9$ according to Corollary 2.2. Also, since $A_a(15,5) = A_a(12,4) = 12$, it follows from Corollary 2.2 with $s$=12 and $t$=4 that $A_a(27,9) = 12$. □

The results of the bounds on $A_a(n,d)$ in this section can be found in the last two columns of Table A.3 in Appendix $A$. In the next section, some improved bounds on $A_a(n,5)$ for $n \le 23$ are given.

## 3.4 Some improvements on 4-AsEC codes

The exact values of all the bounds on $A_a(n,5)$ for length $n \le 17$ are already known [59]. Here we only consider values of $n$ with $18 \le n \le 23$. However, we want to point out that some optimal $C_a(n,5)$ codes can be constructed by Theorem 2.3. For instance, an optimal $C_a(13,5)$ code can be constructed by concatenating an optimal $C_a(10,4)$ code with $\mathbf{V}_3$; an optimal $C_a(14,5)$ code can be obtained by concatenating an optimal $C_a(11,4)$ code with $\mathbf{V}_3$

again, and an optimal $C_a(15,5)$ code can be formed by concatenating an optimal $C_a(9,3)$ code with an optimal $C_a(6,2)$ code, and so on.

To obtain better lower bounds on $A_a(n,5)$ for $18 \le n \le 23$, the same techniques as used in the previous sections are applied. So one starts with a 2-design $D(v, n+1, r, k, \lambda)$ with $d = r - \lambda$ or with a good constant weight code of size $A^l(n+1, 2d, w)$ where often $w$ will be chosen as $\lceil (n+1)/2 \rceil$, after which some puncturing or shortening techniques are applied, to get a set of legitimate words. Finally, one tries to add as many words as possible.

**Theorem 3.28** $A_a(18,5) \ge 40$.

*Proof:* Take the $(n = 20, d = 10, w = 8)$ optimal constant weight code of size 17 from [5], and shorten this code with respect to the first coordinate, leading to twelve words of length 19, asymmetric distance 5 and constant weight 8. Deleting the first coordinates of these twelve words yields eight words of weight 8 and four words of weight 7 which are at distance 5 apart mutually. Let $Z_{18}$ consist of those twelve words, and let $\mathbf{a}_1$, $\mathbf{a}_2$ and $\mathbf{b}$ be chosen from $Z_{18}$ so that $w(\mathbf{a}_1) = w(\mathbf{a}_2) = 8$ and $w(\mathbf{b}) = 7$. Then, it can be easily shown that $< \mathbf{a}_1, \mathbf{a}_2 >= 3$ and $2 \le< \mathbf{a}_1, \mathbf{b} >\le 3$ which satisfy the inequalities in Theorem 2.11. Hence, the complements of all the words of $Z_{18}$, as well as the following sixteen can be added to $Z_{18}$ while keeping $d_a = 5$:

$$\begin{array}{llllll} 3FFFF, & 1FF56, & 2FFA9, & 323FF, & 09CFF, & 01FA6, \\ 08F59, & 1630F, & 263F0, & 3B056, & 3D0A9, & 39C00, \\ 07300, & 10059, & 200A6, & 00000. & & \end{array}$$

The enlarged set will again be denoted by $Z_{18}$. It is a $C_a(18,5)$ code containing 40 codewords. □

**Theorem 3.29** $A_a(20,5) \le 128$.

*Proof:* From Theorem 2.1 and a result by Böinck (mentioned in [57]), it follows that $A_5+A_6+A_7 \le 15$, $A_8+A_9 \le 39$, $A_{10}+A_{11} \le 44$, $A_{12}+A_{13} \le 21$ and $A_{14}+A_{15} \le 7$. So

$$A_a(20,5) = \sum_{i=0}^{20} A_i \le 1 + 15 + 39 + 44 + 21 + 7 + 1 = 128.$$

By using combinatorial arguments, we obtained a $C_a(20,5)$ code of size 68, that is easy to construct. Start with the incidence matrix $M$ of the symmetric 2-design $D(19,19,9,9,4)$ in Table I.1 of [25], that is the circulant with top row (0100111101010000110) (rows corresponding to blocks), then putting the vector $\mathbf{1}$ of length 20 as the top row together with the matrix $(\mathbf{1}^T M)$ forms a Hadamard matrix of order 20 if all its zeroes are changed into minus ones. Let $Z_{20}$ contain all the rows of such a matrix apart from the first row, then $Z_{20}$ is a constant weight code of length 20, asymmetric distance 5 and constant weight 10. Since the inner product of any two different words in $Z_{20}$ is 5, the size of $Z_{20}$ can be enlarged by adding the complements of all its words to itself according to Corollary 2.5. To the 38 words of $Z_{20}$, the 15 following words are added

$$\begin{array}{llllll} 00000, & 0C007, & 20360, & 9A048, & A2481, & 000FE, \\ 00F0B, & 07151, & 0EAA0, & 19524, & 6380C, & 74182, \\ A9212, & C4644, & D0831. & & & \end{array}$$

Again, adding their complements (using Theorem 2.11) will keep the distance unchanged. One gets the $C_a(20,5)$ code $Z_{20}$ of size 68. Recently, Etzion [14] found a $C_a(20,5)$ code containing 71 words. □

**Theorem 3.30** $104 \leq A_a(21,5) \leq 228$.

*Proof:* It follows from a small improvement to Theorem 2.1 (see [17]) that $A_a(21,5) \leq 2(1+19+21+73) = 228$. A $C_a(21,5)$ code of size 104 can be constructed as follows. Consider the rows of the circulants with top rows: (10010010001111010 1000) and (10100011100110111 0000). Add **1** and **0**, and the 60 words given in Appendix $B$ to obtain the $C_a(21,5)$ code $Z_{21}$ of size 104. □

**Theorem 3.31** $A_a(22,5) \geq 163$ *and* $A_a(23,5) \geq 243$.

*Proof:* Let $Z_{22}$ consist of **1** and **0**, the 98 words presented in Appendix $B$, the rows of the circulants with top rows (000001010110011101111) and (000011111010110001001) with a zero appended to them and the rows of the circulant with top row (000101001111100100011), with a one appended to them. Then $Z_{22}$ is a $C_a(22,5)$ code of cardinality 163.

Take the $(n = 24, d = 10, w = 12)$ constant weight code of size 96 from [5] (Table XI). Deleting the first coordinate will yield forty-eight words of length 23 and weight 11, and forty-eight words of length 23 and weight 12. To these 96 words, **1**, **0** and the 145 words listed in Appendix $B$ can be added. This yields a $C_a(23,5)$ code, denoted by $Z_{23}$, of cardinality 243. □

## 3.5 A new upper bound on $A_a(10,2)$

As a miscellaneous result, an improved upper bound on the maximum size of 1-AsEC codes of length 10 will be given here.

Let $C$ be a 1-AsEC code of length 10 and size $A_a(10,2)$. Also let **0** and **1** be the codewords of $C$. From Theorem 2.1, it follows that the weight distribution of the code $C$ satisfies $A_2 \leq 5$, $A_3 + A_4 \leq 35$, $A_5 \leq 36$, $A_6 + A_7 \leq 35$ and $A_8 \leq 5$. Combining of those inequalities yields

$$|C| = A_a(10,2) \leq 2(1+5+35)+36 = 118.$$

Weber et al. [57] improved this upper bound $A_a(10,2) \leq 117$ using a linear programming approach. A lower bound on $A_a(10,2)$ was taken as the size of the $C_a(10,2)$ code constructed by Delsarte and Piret [12], which shows that $A_a(10,2) \geq 108$. Below we claim

**Theorem 3.32** $111 \leq A_a(10,2) \leq 115$.

The proof of Theorem 3.32 is very tedious and can be found in [17]. The lower bound comes from the construction of such a code due to Etzion [15]. This code has the weight distribution: $A_0 = 1, A_2 = 5, A_3 = 11, A_4 = 22, A_5 = 33, A_6 = 22, A_7 = 11, A_8 = 5$ and $A_{10} = 1$. For the improved upper bound it suffices to show that for a $C_a(10,2)$ code,

1) $A_2 + A_3 + A_4 = 40$ or $A_6 + A_7 + A_8 = 40$ implies that $A_5 \leq 30$;

2) $A_5 = 36$ forces $A_3 + A_4 \leq 30$ and $A_6 + A_7 \leq 30$.

The proof of these two statements is presented in [17].

# Chapter 4

# Bounds and constructions for codes capable of correcting unidirectional errors

In this chapter, we shall be concerned with bounds on the maximum size of $t$-UEC codes of length $n$ for $5 \leq t \leq 8$, namely, the bounds on $A_u(n, 2t+1)$ for $5 \leq t \leq 8$. It follows from (1.2) that each value $A_u(n, 2t+1)$ is bounded above by the upper bound on $A_a(n, t+1)$, while, the latter has already been produced in the previous chapter; therefore, the emphasis here will be put on the constructions of $t$-UEC codes.

However, the constructions of such codes ($n \leq 27$, $11 \leq 2t+1 \leq 17$) do not require as much effort as in Chapter 3 for $t$-AsEC codes, even though the unidirectional distance seems to be a more complicated feature than the asymmetric distance. It was found that most of the $t$-UEC codes that we constructed would be obtained simply by modifying some comparable pairs of codewords in the corresponding $t$-AsEC codes of the same length. Essentially, if $C$ is a $C_a(n, t+1)$ code in which any pair of codewords is incomparable, then $C$ is certainly a $C_u(n, 2t+1)$ code by the definition.

In addition, if a $C_u(n, 2t+1)$ code $C$ contains $\mathbf{0}$ or $\mathbf{1}$, then the weight distribution of $C$ must satisfy $A_i = 0$, for $i = 1, \cdots, 2t$ or $A_{n-i} = 0$, for $i = 1, \cdots, 2t$. Therefore, it seems that an optimal $C_u(n, d_u)$ code which is nontrivial cannot contain the all-one vector $\mathbf{1}$ or the all-zero vector $\mathbf{0}$. It is worthwhile noting that, for a $t$-UEC code of length $n$, the sum $\sum_{i=0}^{t} A_i \leq 1$, and also the sum $\sum_{i=0}^{t} A_{n-i} \leq 1$, just like any $t$-AsEC code of length $n$. In Appendix $B$, the words which are specifically underlined indicate those which have to be erased when constructing codes for correcting unidirectional errors.

## 4.1 Bounds and constructions for 5-UEC codes

We shall start with $n$=13.

**Theorem 4.1** $A_u(13, 11) = A_u(14, 11) = 4$

*Proof:* It follows from $A_u(13, 11) \leq A_u(14, 11) \leq A_a(14, 6) = 4$ that we only have to construct a $C_u(13, 11)$ code of size 4. The four words are given by 1800, 07E0, 0C1F and 13FF. □

**Theorem 4.2** *$A_u(15, 11) = 4$, $A_u(16, 11) = 6$ and $A_u(17, 11) = 8$.*

*Proof:* It follows from Theorem 2.1 that $A_u(15, 11) \leq 1 + 2 + 2 + 1 = 6$. With some extra effort [17] this upper bound can be lowered to $A_u(15, 11) \leq 4$. A construction of a code of size 4 follows from the previous theorem.

Let $C$ be an optimal $C_u(16, 11)$ code. Then it follows from Theorem 2.1, that $|C| \leq 1 + 3 + 2 + 1 = 7$. In [17] it is shown how this bound can be improved to $A_u(16, 11) \leq 6$. A $C_u(16, 11)$ code of cardinality 6 is given by 0001, FC00, 03F0, E38E, 1C7E and F9FF.

A $C_u(17, 11)$ code of size 8 is given by 00007, 1F800, 007E0, 1861E, 071DC, 0EB33, 15CEB and 1BFDD. So the result follows from $A_u(17, 11) \leq A_a(17, 6) = 8$. □

For the remaining cases, we shall only give the constructions of these codes, since the corresponding upper bounds will be simply those on $A_a(n, d)$. All the $C_k$ ($k = 19, \cdots, 27$) codes mentioned in the following theorem have been defined in Theorem 3.6 to Theorem 3.14 in Section 3.1 respectively.

**Theorem 4.3** *$A_u(18, 11) \geq 10$, $A_u(19, 11) \geq 14$, $A_u(20, 11) \geq 22$, $A_u(21, 11) \geq 30$, $A_u(22, 11) \geq 46$, $A_u(23, 11) \geq 63$, $A_u(24, 11) \geq 86$, $A_u(25, 11) \geq 119$, $A_u(26, 11) \geq 167$ and $A_u(27, 11) \geq 239$.*

*Proof:* Take the 2-AsEC code of length 9, denoted by $C_9$ in [12], and delete **0**, **1** and the two words of weight 6. Now add the two words 00405 and 36FDB. This gives a $C_u(18, 11)$ code of size 10.

Deleting **1** and **0** from the code $C_{19}$ gives a $C_u(19, 11)$ code of size 14.

Erase **1** and **0** from the code $C_{20}$, and add the words 83080 and 7FF2F, giving a $C_u(20, 11)$ code of size 22.

Erase **1** and **0** from the code $C_{21}$ and change the third row of the matrix $M_5$ in the proof of Theorem 3.8 into the vector 17BC6F. This leads to a $C_u(21, 11)$ code of size 30.

Remove **1** and **0** and the five words 2FEBC7, 321324, 028478, 14508A and 00A381 from the code $C_{22}$, and add the following five words: 27BFED, 005AA1, 068470, 22310A and 0100CC. Then a $C_u(22, 11)$ code of size 46 is obtained.

From the code $C_{23}$, delete $\mathbf{1}$, $\mathbf{0}$ and the three words of weight 8 (i.e., $\mathbf{a}_5$, $\mathbf{a}_7$ and $\mathbf{a}_{10}$) and add the following two words of weight 8: 636011 and 681528. Then a $C_u(23,11)$ code of size 63 is obtained.

From the code $C_{24}$, delete $\mathbf{0}$ and $\mathbf{1}$, and the codewords 773FEB, B9DDF7, E35B7E, FAA5EE, 7D753A and BDB9C9, then add the following three vectors: FF99DA, 6F5FF5 and B1BDFF. One gets a $C_u(24,11)$ code of size 86.

From the code $C_{25}$, delete the eleven words $\mathbf{0}$, $\mathbf{1}$, 0BB5FFD, 1EEFEB3, 07FA3F7, 127FD7E, 1B773AB, 1EC0FEF, 12C6240, 1521441 and 0E28200, then add the following six words: 17F7AF9, 0B737BF, 167CD7F, 1EE2BE7, 0122051 and 12840A0. One gets a $C_u(25,11)$ code of size 119.

Delete $\mathbf{0}$ and $\mathbf{1}$ from the code $C_{26}$ and also the following fifteen words: 0F7DBF7, 3BB7DDE, 2DCFC7F, 36FD779, 3F726EF, 375FB9A, 3BC9FAD, 0FF7E2A, 13F8AFE, 287B5FE, 3F65A5D, 1E091E0, 004D601, 008229C and 1821050. Then add the following eleven words: 3FFBBC7, 2BB77FB, 36EFD7D, 13DCFFE, 357FE9B, 0F6FE6E, 38797FD, 3FC5BAD, 3FB1ADA, 008D205 and 00614C0. A $C_u(26,11)$ code of size 167 is constructed.

From the code $C_{27}$, erase the twenty-seven words: $\mathbf{0}$, $\mathbf{1}$, 6F9BBF7, 7BF7E5E, 556FAFF, 78DCFBF, 7EA75FD, 1AEBF77, 1FF59BE, 6DBDEEC, 3A7DAF9, 3D4F5EE, 3DAEE1F, 4DE47F7, 56FACBB, 62EFBCE, 33D6B9B, 35B54FB, 78FE4DC, 7C3A3EB, 7DEBF80, 020B8E1, 09E0502, 41500C9, 0288215, 2C04188 and 0091940. Then add the following seventeen words: 1FF7B3F, 6EEFDED, 52BEFF7, 7D3FAF9, 3DEBC7E, 6DBCFAE, 78CD7DF, 3AFEABA, 3B65BED, 3DA67F3, 5EB5CFC, 747B1EB, 7DEFD80, 0148183, 54D0200, 0424488 and 0809A40. This results in a $C_u(27,11)$ code of size 239. □

## 4.2 Bounds and constructions for 6-UEC codes

It is easy to show that $A_u(13,13) = A_u(14,13) = 2$ and $A_u(15,13) = 4$. Also from (1.2), it follows that $A_u(16,13) = A_u(17,13) = 4$. For the remaining cases, we again only give lower bounds by means of explicit code constructions.

**Theorem 4.4** $A_u(18,13) = 6$ *and* $A_u(19,13) = 7$.

*Proof:* The words 0000F, 3F800, 007F0, 3C78E, 078F7 and 3BF79 give a $C_u(18,13)$ code of size 6, while the upper bound comes from $A_a(18,7) = 6$. The words 00015, 7F000, 00FE0, 70E1E, 3C1E7, 4F799 and 3BF7F form a $C_u(19,13)$ code of size 7, while the upper bound comes from $A_a(19,7) = 7$. □

All the $X_k$ ($k = 20, \cdots, 27$) codes mentioned in the following theorem have been defined in Theorem 3.18 to Theorem 3.22 in Section 3.2.

**Theorem 4.5** *$A_u(20,13) = 9$, $A_u(21,13) \geq 10$, $A_u(22,13) \geq 13$, $A_u(23,13) \geq 19$, $A_u(24,13) \geq 27$, $A_u(25,13) \geq 39$, $A_u(26,13) \geq 58$ and $A_u(27,13) \geq 80$.*

*Proof:* From the optimal $C_a(20,7)$ code $X_{20}$, delete **0** and **1**, and add the two words 40420 and FEDFB to obtain a $C_u(20,13)$ code of size 9. The upper bound follows from (1.2).

Delete **0** and **1** from the code $X_{21}$, to obtain a $C_u(21,13)$ code of size 10.

Delete **0** and **1**, as well as the word 324418 from the code $X_{22}$, and add 3FEEFE and 321418 to give a $C_u(22,13)$ code of size 13.

Saitoh et al. [45] gives the following $C_a(23,7)$ code of size 19: 000000, 00007F, 003F80, 1FC000, 21C387, 22DC38, 3C21D8, 472661, 187A66, 053C9F, 4A85EE, 5B4B19, 14D7F1, 67F942, 2BAAF5, 76663E, 39DD2F, 4E7FCD and 7FFFFF. In this code, erase **0**, **1** and 003F80, and add 202300, 501D82 and 7DFAFA. One gets a $C_u(23,13)$ code of size 19.

In the code $X_{24}$, delete **0**, **1** and the word 4DBBAF, then add B20040, 59BDAF and 3FEFFE to obtain a $C_u(24,13)$ code of size 27.

Remove from the code $X_{25}$ the words **0**, **1**, 0177DAF and 1AFC3CE and add 0001812, 0B34DEF and 0D7FFFB. A $C_u(25,13)$ code of size 39 is obtained.

From the code $X_{26}$, delete **0**, **1**, 0FAAFBF, 24BFFC3 and 0253044 and add 14BFF9F, 3D9BBE1, 2053044, 0200228 and 3FE7FF6. So $A_u(26,13) \geq 58$.

From the code $X_{27}$, delete **0**, **1**, 0AC8013, 2DEFBAD and 7AD6BF6, and add 4AC8012, 5DEF3F4, 7ADEF2E, 6D7DFBF and 2030042. So $A_u(27,13) \geq 80$. □

## 4.3 Bounds and constructions for 7-UEC and 8-UEC codes

It is easy to show that $A_u(i,15) = 2$ for $13 \leq i \leq 16$, and $A_u(17,15) = 4$. Hence, from $A_a(19,8) = 4$, it follows that $A_u(18,15) = A_u(19,15) = 4$. Other trivial bounds are

$$\begin{aligned} A_u(i,17) &= 2, \quad \text{for } i = 13, \cdots, 18; \\ A_u(j,17) &= 4, \quad \text{for } j = 19, \cdots, 22. \end{aligned}$$

We shall now discuss the remaining cases.

**Theorem 4.6** *$A_u(20,15) = 5$.*

*Proof:* Let $C$ be an optimal $C_u(20,15)$ code. From Theorem 2.1, it follows that $A_8 \leq 2$ and $A_9 + A_{10} + A_{11} + A_{12} \leq 2$. But, if $A_8 = 2$, then $A_9 = A_{10} = A_{11} = 0$. On the other hand, $A_8 = 2$ and $A_{12} = 2$ will result in $\sum_{i=0}^{7} A_i = 0$ and $\sum_{i=13}^{20} A_i = 0$. So it follows that $|C| \leq 5$. On the other hand, The words 00018, FF000, 80FF0, 3CF0F and F31F7 form a $C_u(20,17)$ code of size 5. □

**Theorem 4.7** $A_u(21,15) = 6$.

*Proof:* On one hand, the upper bound comes from $A_a(21,8) = 6$, and on the other hand the words 000003, 1FE000, 001FE0, 1E1E1E, 01E1FE and 1FDDE1 form a $C_u(21,15)$ code of size 6. □

**Theorem 4.8** $A_u(22,15) = 7$.

*Proof:* Let $C$ be an optimal $C_u(22,15)$ code. From Theorem 2.1, it follows that $A_8 + A_9 + A_{10} \leq 3$ and $A_{11} + A_{12} + A_{13} + A_{14} \leq 3$. If $A_8 + A_9 + A_{10} = 3$, then the triple $(A_8, A_9, A_{10})$ only has three alternatives: (2,0,1), (1,1,1) and (1,0,2). It can be readily shown that each of those three values will make the sum $\sum_{i=0}^{7} A_i$ equal to zero. Hence $|C| \leq 7$. On the other hand the words 000031, 3FC000, 003FC0, 38383E, 37B7B0, 0F4E5F and 3BFBEF form a $C_u(22,15)$ code of size 7. □

**Theorem 4.9** $A_u(23,15) = 9$.

*Proof:* The upper bound comes from $A_a(23,8) = 9$. On the other hand, in Theorem 3.24, changing $\mathbf{0}$ and $\mathbf{1}$ from the code shown in (3.2) respectively to the following two vectors: $\mathbf{0}^6\mathbf{1}0^8 110^6$ and $\mathbf{1}^{16}01^2 01^2 0$ results in a $C_u(23,15)$ code of size 9. □

**Theorem 4.10** $A_u(24,15) \geq 10$.

*Proof:* Consider the following matrices:

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

$$B_1 = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix},$$

$$B_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}, \quad B_4 = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Then, the rows in

$$\begin{pmatrix} A & A & A & A \\ B_1 & B_2 & B_3 & B_4 \end{pmatrix}$$

form a $C_u(24,15)$ code of size 10. □

**Theorem 4.11** *$A_u(25,15) \geq 13$, $A_u(26,15) \geq 18$ and $A_u(27,15) \geq 23$.*

*Proof:* Delete **0**, **1** and 18DFDF8 from the code $Y_{25}$ (see Theorem 3.25), and add the following three vectors: 0000214, 18DFDF4 and 0F77FFB to show $A_u(25,15) \geq 13$.

Weber et al. (cf. Table VI of [59]) presented an optimal $C_a(13,4)$ code. With the same notation used by Weber, put

$$C = \{(\mathbf{c}_i|\mathbf{c}_i)|i = 2,\cdots,15\} \cup \{(\mathbf{c}_{16}|\mathbf{c}_{17}),(\mathbf{c}_{17}|\mathbf{c}_{16}),\mathbf{a},\mathbf{b}\}$$

in which: $\mathbf{a}$ = 0800C01 and $\mathbf{b}$= 1EBFFFF. Then, $C$ is a $C_u(26,15)$ code of size 18.

Delete **0**, **1** and 6041613 from the code $Y_{27}$ (see Theorem 3.25), and add the following three vectors to it: 2441612, 4800041 and 5F7BFFF. This shows that $A_u(27,15) \geq 23$. □

**Theorem 4.12** *$A_u(23,17) = 6$, $A_u(24,17) = 6$, $A_u(25,17) = 8$, $A_u(26,17) = 9$ and $A_u(27,17) \geq 10$.*

*Proof:* The first fact follows from the bound $A_a(23,9) = 6$ and the $C_u(23,17)$ code consisting of the words: 000007, 7FC000, 003FE0, 7C3E1E, 07C3FB and 7BFDFD.

Let $C$ be an optimal $C_u(24,17)$ code. From Theorem 2.1, it follows that $|C| \leq 7$. This upper bound can be further lowered to $|C| \leq 6$ (see [17]). From $A_u(23,17) = 6$ it now follows that $A_u(24,17) = 6$.

The third statement follows from the bound $A_a(25,9) = 8$ and the $C_u(25,17)$ code consisting of the words: 000000B, 1FF0000, 000FF80, 1C0E07E, 03C1E79, 18FC78D, 07379E7 and 1BFBFFE.

Let $D_1$ consist of the rows (in the same order) of $X_{20}$ after deletion of **0** and **1**, and let $D_2$ be the following matrix

$$D_2 = \begin{pmatrix} 110000 \\ 001100 \\ 000011 \\ 101010 \\ 100101 \\ 011001 \\ 010110 \end{pmatrix}$$

Then all the rows of the matrix $(D_1 \mid D_2)$, together with 0010003 and 3DAFFFE will form a $C_u(26, 17)$ code of size 9. It follows from $A_a(26, 9) = 9$ that $A_u(26, 17) = 9$.

Concatenate $C_{15}$ minus **0** and **1** with two appropriate subcodes of optimal $C_a(6, 2)$ codes to get the $C_u(27, 17)$ code containing 7C00C30, 03E030C, 421E0C3, 3199AAA, 0C75965, 696A659, 36A6596, 4F8DF33, 54FBAAF and 3B573FA. □

All the results presented in this chapter are combined into Table A.5 in Appendix $A$.

# Chapter 5

# Uniqueness of optimal 1-AsEC codes of length less than 9

In this Chapter, it is shown that up to permutation the optimal $C_a(n,2)$ codes for $n$ = 2,4,6 and 8 are unique and there exactly exist four non-isomorphic $C_a(3,2)$ codes containing two codewords, four non-isomorphic $C_a(5,2)$ codes with six codewords and twelve non-isomorphic $C_a(7,2)$ codes with eighteen codewords.

## 5.1 Optimal 1-AsEC codes of length less than 8

From Table A.1 in Appendix $A$, one can find that $A_a(2,2)$=2, $A_a(3,2)$=2, $A_a(4,2)$=4, $A_a(5,2)$=6 and $A_a(6,2) = 12$. With a little effort, one will immediately arrive at the conclusions for the cases of $n = 2,3,4,5$ and 6, which are exhibited in the following Theorems 5.1 and 5.2.

**Theorem 5.1** *Let $a, b \in \{0,1\}$. For $2 \leq n \leq 4$, any optimal $C_a(n,2)$ code is equivalent to one of the following sets: $\{(00),(11)\}$ ($n = 2$), $\{(00a),(11b)\}$ ($n = 3$) and $\{(0000),(1100),(0011),(1111)\}$ ($n = 4$). And any optimal $C_a(5,2)$ code is equivalent to one of the following four matrices:*

$$C_a(5,2)[a,b] \triangleq \begin{pmatrix} 0 & 0 & 0 & 0 & a \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & b \end{pmatrix}.$$

So there are four optimal $C_a(3,2)$ codes and four optimal $C_a(5,2)$ codes which are not equivalent. All permutations which map every word in a code $C$ to a word of $C$ form the *automorphism group* of $C$ which is denoted by $Aut(C)$. Denote the identity by $I$. Then we found

$$Aut(C_a(5,2)[0,0]) = Aut(C_a(5,2)[0,1])\ \{I,(12)(34),(13)(24),(14)(23)\};$$
$$Aut(C_a(5,2)[1,0]) = Aut(C_a(5,2)[1,1])\ \{I,(13)(45),(14)(35),(15)(34)\}.$$

Since $A_a(5,2) = 6$ and the minimum distance is 2, an optimal $C_a(6,2)$ code must satisfy that half of its codewords is made from the rows of a matrix with the form $C_a(5,2)[0,0]$ with a zero appended to them, and the remaining half of the codewords from the rows of a matrix with the form $C_a(5,2)[1,1]$ with a one appended to them. Hence the weight distribution of the code satisfies $A_0 = A_6 = 1, A_2 = A_4 = 3$ and $A_3 = 4$. Thus one can readily show the following theorem.

**Theorem 5.2** *Up to permutation, optimal $C_a(6,2)$ codes look like (the columns are codewords)*

$$\begin{array}{c} 000101100111 \\ 000110010111 \\ 001001011011 \\ 001010101011 \\ 010000111101 \\ 010011001101 \end{array} \tag{5.1}$$

The elements of the automorphism group acting on the rows of (5.1) are the following 24 permutations:

$$\begin{array}{llll} I, & (34)(56), & (35)(46), & (36)(45), \\ (12)(56), & (12)(34), & (12)(3546), & (12)(3645), \\ (13)(24), & (1324)(56), & (135)(246), & (136)(245), \\ (1423)(56), & (14)(23), & (146)(235), & (145)(236), \\ (153)(264), & (154)(263), & (15)(26), & (1526)(34), \\ (163)(254), & (164)(253), & (16)(25), & (1625)(34). \end{array}$$

By means of exhaustive search by computer it was found that there exist exactly twelve non-isomorphic binary 1-AsEC codes of length 7 containing eighteen codewords. They are optimal and are listed in (5.2), (5.3) and (5.4) respectively where $a, b \in \{0,1\}$ (the codewords are the columns).

$$C_1(7,2)[a,b] \triangleq \left( \begin{array}{c} a1111111100000000b \\ 111110000111100000 \\ 111101000100011100 \\ 110010110110011000 \\ 110001101011010010 \\ 101010101001110100 \\ 101001110101000110 \end{array} \right) \tag{5.2}$$

$$C_2(7,2)[a,b] \triangleq \begin{pmatrix} a111111100000000b \\ 11111000011100000 \\ 11100110011001100\,0 \\ 11010101010101010\,0 \\ 11001010101100011\,0 \\ 10011011010000111\,0 \\ 10010110101010110\,0 \end{pmatrix} \tag{5.3}$$

$$C_3(7,2)[a,b] \triangleq \begin{pmatrix} a111111100000000b \\ 11111000011100000 \\ 11100110011001100\,0 \\ 11010101010101010\,0 \\ 11001010101100011\,0 \\ 10011100101010110\,0 \\ 10001111010000111\,0 \end{pmatrix} \tag{5.4}$$

From (5.2), (5.3) and (5.4), it follows that optimal $C_a(7,2)$ codes satisfy $A_2 = 3, A_3 = A_4 = 5$ and $A_5 = 3$. The automorphism groups acting on the rows of (5.2), (5.3) and (5.4) are shown below:

$Aut(C_1(7,2)[a,b]) = \{I\}$, for all a,b $\in \{0,1\}$;
$Aut(C_2(7,2)[0,0]) = Aut(C_2(7,2)[0,1]) = \{I,(14)(23)(57)\}$;
$Aut(C_2(7,2)[1,0]) = Aut(C_2(7,2)[1,1]) = \{I,(27)(35)(46)\}$;
$Aut(C_3(7,2)[0,0]) = Aut(C_3(7,2)[0,1]) = \{I,(12)(36)(47)\}$;
$Aut(C_3(7,2)[1,0]) = Aut(C_3(7,2)[1,1]) = \{I,(27)(34)(56)\}$.

## 5.2 Optimal 1-AsEC codes of length 8

Using the properties of optimal $C_a(7,2)$ codes shown in the previous section, we can prove

**Theorem 5.3** *Up to permutation, optimal $C_a(8,2)$ codes are of the same form.*

*Proof:* Let $C$ be an optimal $C_a(8,2)$ code. Then $|C| = 36$ by Table A.1 in Appendix $A$. Arrange $C$ as a 36 by 8 matrix. Every column of $C$ contains exactly 18 ones and 18 zeros because $A_a(7,2)$ is 18. Further analysis shows that half of the codewords of $C$ is made from the rows of a matrix with the form $C_j(7,2)[0,0]$ appended a zero to them, and the remaining words from the rows of a matrix with the form $C_i(7,2)[1,1]$ appended a one to them where $i,j \in \{1,2,3\}$. This results in $\mathbf{0},\mathbf{1} \in C, A_2 = A_6 = 4, A_3 = A_5 = 8$ and $A_4 = 10$. Without loss of generality, we may assume that

$$\{1,2\},\{3,4\},\{5,6\},\{7,8\} \tag{5.5}$$

are the supports of the codewords of weight 2. Kalbfleisch et al. [30] proved that a maximal (8,3) system has eight triples containing every pair exactly once except the four pairs of (5.5) which do not occur. The eight triples are uniquely determined up to permutation when (5.5) is fixed. They are taken as the codewords of $C$ of weight 3, and are listed below:

$$\begin{array}{llll} \mathbf{3}_1 = \{1,3,7\}, & \mathbf{3}_2 = \{1,4,5\}, & \mathbf{3}_3 = \{1,6,8\}, & \mathbf{3}_4 = \{2,3,6\}, \\ \mathbf{3}_5 = \{2,4,8\}, & \mathbf{3}_6 = \{2,5,7\}, & \mathbf{3}_7 = \{3,5,8\}, & \mathbf{3}_8 = \{4,6,7\}. \end{array} \tag{5.6}$$

Now we consider the ten codewords of weight 4 which form a 10 by 8 submatrix of $C$, denoted by $Q = (q_{ij})$. Because of the special types of the words of weight 3 and weight 4 in (5.2) to (5.4), each column of $Q$ involves exactly five ones and five zeros. Without loss of generality, divide $Q$ into two submatrices: $(\mathbf{1}^T Q_1)$ and $(\mathbf{0}^T Q_2)$ where $Q_1$ and $Q_2$ are two 5 by 7 matrices, and $Q_1$ comes from the codewords of weight 3 in an optimal $C_a(7,2)$ code and $Q_2$ from the codewords of weight 4 in an optimal $C_a(7,2)$ code. Also from (5.2) to (5.4), it follows that in $Q_1$ only one column has three ones and the others all have two ones exactly, and in $Q_2$ only one column has two ones and the others three ones each. Since $\{1,3,7\}, \{1,4,5\}$ and $\{1,6,8\}$ are codewords, the first column of $Q_1$ must have three ones, and so the first column of $Q_2$ must have two ones. With the distance $d_a \geq 2$ in mind, we may, without loss of generality, take the first three columns of $Q$ as follows:

$$\begin{pmatrix} 1111100000 \\ 1110011000 \\ 1001010110 \end{pmatrix}^T \tag{5.7}$$

and we may also assume that $q_{27} = q_{57} = 1$ since $\{1,3,7\}$ is a codeword. Let $\mathbf{4}_i$ $(i = 1,2,\cdots,10)$ denote the rows of $Q$ in the ordered of (5.7) from top to bottom. By using (5.6), one can show that $q_{14} = 1, q_{15} = 1$ or $q_{18} = 1$ for the first row of $Q$. First suppose that $q_{14} = 1$. In the following we shall abbreviate the statement "that the condition $A$ holds implies that the result $B$ holds" by "$A \Longrightarrow B$". Using this notation we get

$$(d_a(\mathbf{3}_6, \mathbf{4}_2) \geq 2 \ \wedge \ d_a(\mathbf{4}_1, \mathbf{4}_2) \geq 2) \Longrightarrow (q_{26} = 1 \ \vee \ q_{28} = 1).$$

However, $q_{28} = 1 \Longrightarrow q_{35} = q_{36} = 1$, which gives rise to

$$\begin{aligned} q_{44} = 1 &\Longrightarrow d_a(\mathbf{4}_1, \mathbf{4}_4) < 2; \\ q_{47} = 1 &\Longrightarrow d_a(\mathbf{3}_1, \mathbf{4}_4) < 2; \\ q_{45} = q_{46} = 1 &\Longrightarrow d_a(\mathbf{4}_3, \mathbf{4}_4) < 2; \\ q_{45} = q_{48} = 1 &\Longrightarrow d_a(\mathbf{3}_7, \mathbf{4}_4) < 2; \\ q_{46} = q_{48} = 1 &\Longrightarrow d_a(\mathbf{3}_3, \mathbf{4}_4) < 2. \end{aligned}$$

This implies that $q_{26} = 1$ and $q_{28} = 0$, hence $q_{35} = q_{38} = 1$. In this case, we find

$$(d_a(\mathbf{4}_1, \mathbf{4}_4) \geq 2 \ \wedge \ d_a(\mathbf{3}_3, \mathbf{4}_4) \geq 2 \ \wedge \ d_a(\mathbf{3}_7, \mathbf{4}_4) \geq 2) \Longrightarrow q_{45} = q_{46} = 1.$$

Proceeding in the same way, we can evaluate the entries: $q_{54} = q_{57} = q_{58} = 1, q_{67} = q_{68} = 1$ and $q_{74} = q_{75} = q_{76} = 1$. Moreover if we ignore the order of $\mathbf{4}_8$ and $\mathbf{4}_9$, then the supports of the last three rows of $Q$ must be $\{3,4,5,7\}, \{3,4,6,8\}$ and $\{5,6,7,8\}$. All the supports of the rows of $Q$ when $q_{14} = 1$ are listed in the first column of (5.8).

| $q_{14} = 1$ | $q_{15} = 1$ | $q_{18} = 1$ |
|---|---|---|
| $\{1,2,3,4\}$ | $\{1,2,3,5\}$ | $\{1,2,3,8\}$ |
| $\{1,2,5,8\}$ | $\{1,2,7,8\}$ | $\{1,2,4,7\}$ |
| $\{1,2,6,7\}$ | $\{1,2,4,6\}$ | $\{1,2,5,6\}$ |
| $\{1,3,5,6\}$ | $\{1,3,4,8\}$ | $\{1,3,4,6\}$ |
| $\{1,4,7,8\}$ | $\{1,5,6,7\}$ | $\{1,5,7,8\}$ |
| $\{2,3,7,8\}$ | $\{2,3,4,7\}$ | $\{2,3,4,5\}$ |
| $\{2,4,5,6\}$ | $\{2,5,6,8\}$ | $\{2,6,7,8\}$ |
| $\{3,4,5,7\}$ | $\{3,4,5,6\}$ | $\{3,4,7,8\}$ |
| $\{3,4,6,8\}$ | $\{3,6,7,8\}$ | $\{3,5,6,7\}$ |
| $\{5,6,7,8\}$ | $\{4,5,7,8\}$ | $\{4,5,6,8\}$ |

(5.8)

Other two different sets of quadruples when $q_{15} = 1$ or $q_{18} = 1$ are derived also and shown in the second and the third columns of (5.8) respectively. Let $D_i$ ($i = 1,2,3$) be the sets consisting of the words in (5.5), (5.6) and the $i$th column of (5.8). Then the permutation (37)(48)(56) acting on the coordinates of $D_2$ changes $D_2$ into $D_1$. On the other hand, $D_2$ can be obtained by permuting the coordinates of $D_3$ with (358)(467). This means that $D_1, D_2$ and $D_3$ are equivalent. Therefore, without loss of generality, we may take the first column of (5.8) as the ten codewords of $C$ of weight 4.

Next we determine the codewords of weight 5. Since $A_6 = 4$ and the length is 8, each column of the submatrix formed by the four codewords of weight 6 has exactly three ones and one zero. It turns out that each column of the submatrix formed by the eight codewords of weight 5, denoted by $F = (f_{ij})$, involves exactly five ones and three zeros. Divide $F$ into $(\mathbf{1}^\tau F_1)$ and $(\mathbf{0}^\tau F_2)$ where $F_1$ and $F_2$ are 5 by 7 and 3 by 7 matrices resp. For the same reason as mentioned for $Q_i$ ($i = 1,2$), one comes to the claim: in $F_1$ only one column contains two ones and the others involve exactly three ones each; in $F_2$ exactly one column is of weight 3 and the remaining columns are of weight 2. Furthermore, the first column of $F_1$ cannot have three ones and the inner product of the first two columns of $F_1$ must be equal to 1. So, without loss of generality, the first three columns of $F$ may be read as below:

$$\begin{pmatrix} 11111000 \\ 11000111 \\ 10110110 \end{pmatrix}^T .$$

Let $\mathbf{5}_i$ $(i = 1, 2, \cdots, 8)$ be the rows of $F$ from top to bottom. Evidently, there are only two possible choices for $\mathbf{5}_1$, namely $\{1,2,3,5,7\}$ or $\{1,2,3,6,8\}$. It is trivial to prove that the second choice is impossible. Thus $\mathbf{5}_1 = \{1,2,3,5,7\}$. In this case, one has that $f_{24} = f_{26} = f_{28} = 1$. Moreover if the order of $\mathbf{5}_3$ and $\mathbf{5}_4$ is ignored, they must be $\{1,3,4,5,8\}$ and $\{1,3,6,7,8\}$. From the properties of $F_1$, It follows that $f_{54} = f_{55} = f_{56} = f_{57} = 1$. Consequently, $\mathbf{5}_6$ and $\mathbf{5}_7$ equal $\{2,3,4,6,7\}$ and $\{2,3,5,6,8\}$ resp. (if we ignore the order of them). It turns out to be $f_{84} = f_{85} = f_{87} = f_{88} = 1$ because of the properties of $F_2$. This uniquely completes the construction of $F$. The rows of $F$ are the following eight 5-tuples:

$$\begin{array}{lll} \{1,2,3,5,7\}, & \{1,2,4,6,8\}, & \{1,3,4,5,8\}, \\ \{1,3,6,7,8\}, & \{1,4,5,6,7\}, & \{2,3,4,6,7\}, \\ \{2,3,5,6,8\}, & \{2,4,5,7,8\}. & \end{array} \tag{5.9}$$

To complete the proof, we need to determine the four codewords of weight 6. This can be done by investigating the complements of (5.9):

$$\begin{array}{llll} \{4,6,8\}, & \{3,5,7\}, & \{2,6,7\}, & \{2,4,5\}, \\ \{2,3,8\}, & \{1,5,8\}, & \{1,4,7\}, & \{1,3,6\}. \end{array} \tag{5.10}$$

Since (5.10) does not contain the four disjoint pairs in (5.5), the complements of (5.5) can be uniquely taken as the required codewords of weight 6. □

The optimal $C_a(8,2)$ code shown in the proof of Theorem 5.3 can be written in the following standard form (the columns are codewords):

$$\begin{array}{c} 111111111111111111000000000000000000 \\ 111111111000000000111111111000000000 \\ 111110000011110000111100001111100000 \\ 111101000010001110100011101111010000 \\ 110010110011001100010011011100101100 \\ 110001101001101001111010001010011100 \\ 101010101000111010100101011100011010 \\ 101001110010100011010101101010101010 \end{array} \tag{5.11}$$

The elements of the automorphism group acting on the rows of (5.11) are

$$\begin{array}{llll} (1324)(5768), & (1423)(5867), & (1526)(3847), & (12)(34)(56)(78), \\ (1625)(3748), & (1728)(3546), & (1827)(3645), & I. \end{array}$$

One can check that if the first row of (5.11) is deleted, then the first 18 punctured words will form the optimal $C_a(7,2)$ code shown in (5.2) with $a = b = 1$, and the remaining 18 punctured words will be equivalent to the optimal $C_a(7,2)$ code of (5.2) with $a = b = 0$. The results in this chapter lead to Table 5.1.

| $n$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| $A_a(n,2)$ | 2 | 2 | 4 | 6 | 12 | 18 | 36 |
| $\sharp$ | 1 | 4 | 1 | 4 | 1 | 12 | 1 |

Figure 5.1: The numbers of non-isomorphic optimal $C_a(n,2)$ codes for $n \leq 8$.

# Chapter 6

# Weakly perfect codes for correcting asymmetric errors

## 6.1 Introduction

Perfect codes for correcting symmetric errors have received a lot of attention since the celebrated Hamming codes were discovered for the binary symmetric channel (BSC) in 1950, two years after Shannon [46] published the foundation of information theory that was the impetus to the research on error-correcting codes. An excellent exposition on the existence of nontrivial perfect codes was given by Van Lint [48] (including many references). For additional results on perfect codes, one is also referred to [49] and [36]. For later comparisons, we indicate two main properties of binary perfect codes for BSC below:

- A binary perfect block code of length $n$ and minimum Hamming distance $2t+1$ (capable of correcting up to $t$ symmetric errors) corresponds to a partition of $\mathbf{V_n}$. This partition consists of a collection of spheres all with the same radius $t$ centered around the codewords. That is to say, all such packing spheres are mutually disjoint and together cover the whole space. So a perfect code can correct all (symmetric) errors of weight $\leq t$, but none of weight greater than $t$.

- A binary perfect block code has the highest information rate (or maximum size) among all codes of the same length and error-correcting capability. Therefore, in this sense it can be said that the whole vector space is packed optimally by a perfect code.

The study of perfect codes used for BSC has been generalized in several directions which are mentioned in the comments of Chapter 7 of [49]. Though in the last two decades, a lot of attention has been paid to the study of codes which are capable of correcting asymmetric errors as mentioned in

Chapter 1, no literature, as far as we know, discusses perfect asymmetric-error-correcting codes, and the definition of such codes has not even been given yet. Most of previous works on $t$-AsEC codes have had very little impact on the material presented in this chapter.

For decoding of a code, one should realize that through a binary asymmetric channel, a possibly received word, say $\mathbf{y}$, only comes from the codewords covering it. The strategy of a maximum likelihood decoder is of course to decode the received word $\mathbf{y}$ to one of the codewords of lowest weight covering $\mathbf{y}$. Therefore in view of sphere packing, the set to be packed in asymmetric cases is, in general, not the whole vector space anymore as in symmetric cases. It will consist of all possibly received words that can be obtained from all codewords by introducing asymmetric errors. In fact, in asymmetric cases the set to be packed is the whole vector space if and only if the all-one vector is a codeword (when only 1-errors are considered). Generally, this set will depend on the specific code. A partition of this set by using the packing spheres defined in (6.2) for a given code generates some condition of *perfect packing* and *weakly perfect packing.*

The study of perfect codes and weakly perfect codes which are capable of correcting asymmetric errors is the main goal of this chapter, which warrants additional investigation on AsEC codes at a fundamental level. We shall first be concerned with the same two properties, as stated above for perfect codes used for BSC, for $C_a(n,d)$ codes. In other words, we shall answer the two questions raised in Section 1.4.

Below, we define perfect, weakly perfect and uniformly weakly perfect binary block codes for correcting asymmetric errors. The following notions will be used throughout the present chapter.

**Definition 6.1** *Let $C$ be a $C_a(n,d_a)$ code. For any codeword $\mathbf{c} \in C$, $r(\mathbf{c})$ will be used to denote the asymmetric distance to the nearest codeword to $\mathbf{c}$, namely*

$$r(\mathbf{c}) = min\{d_a(\mathbf{x},\mathbf{c}) | \mathbf{c} \neq \mathbf{x} \wedge \mathbf{x} \in C\} = d_a(\mathbf{c}, C \backslash \{\mathbf{c}\}) \qquad (6.1)$$

Evidently, $r(\mathbf{c}) \geq d_a$ for any codeword $\mathbf{c}$ in Definition 6.1. The idea behind Definition 6.1 is that for a $C_a(n,d_a)$ code $C$, there may exist a codeword $\mathbf{c} \in C$ such that $r(\mathbf{c}) > d_a$, which means that the word $\mathbf{c}$ can be protected against more errors than other codewords $\mathbf{x}$ with $r(\mathbf{x}) = d_a$. Codes with this property do exist. For instance, in a 1-AsEC linear code of maximum dimension and length $n$ ($n \neq 2,4$), any nonzero codeword will have a weight greater than the minimum asymmetric distance of the code [57]. Therefore at least $r(\mathbf{0})$ is larger than the minimum asymmetric distance of the code.

The *sphere* with radius $t$ and center $\mathbf{c}$ is defined by

$$S_a(\mathbf{c},t) = \{\mathbf{x} \in \mathbf{V_n} \mid d_a(\mathbf{c},\mathbf{x}) \leq t \ \wedge \ \mathbf{c} \geq \mathbf{x}\}. \tag{6.2}$$

In other words, $S_a(\mathbf{c},t)$ consists of all vectors that can be obtained from $\mathbf{c}$ by introducing up to $t$ 1-errors. Therefore, the cardinality of the sphere $S_a(\mathbf{c},t)$ equals

$$\mid S_a(\mathbf{c},t) \mid = \sum_{i=0}^{t} \binom{w(\mathbf{c})}{i}.$$

Unlike in Hamming space, this number relies not only on the radius $t$ but also on the weight of the word $\mathbf{c}$.

**Definition 6.2** *Let $C$ be a $C_a(n,d_a)$ code. Also, let $E$ denote the set of all possibly received words, i.e. $E = \{\mathbf{x} \in \mathbf{V_n} \mid \exists_{\mathbf{c}\in C}[\mathbf{c} \geq \mathbf{x}]\}$. The code $C$ is called a* weakly perfect *code, for short $WP$ code, if*

$$E = \bigcup_{\mathbf{c}\in C} S_a(\mathbf{c}, r(\mathbf{c})-1). \tag{6.3}$$

*In particular, if all $r(\mathbf{c})$ are equal to $d_a$ in (6.3), then $C$ is called a* uniformly weakly perfect *code, for short, $UWP$ code. If $E = \mathbf{V_n}$ in (6.3), then $C$ is called a* perfect *code.*

Obviously, $\mid C \mid \leq \mid E \mid \leq \mid \mathbf{V_n} \mid = 2^n$, and $E = \mathbf{V_n}$ if and only if $\mathbf{1} \in C$. From Definition 6.2, it follows that any $UWP$ $C_a(n,d_a)$ code is also a $WP$ $C_a(n,d_a)$ code. The definition given for perfect $C_a(n,d_a)$ codes is consistent with that given for the perfect codes used for BSC. Define:

$W_a(n,d_a)$ : the maximum number of codewords in a $WP$ $C_a(n,d_a)$ code;

$U_a(n,d_a)$ : the maximum number of codewords in a $UWP$ $C_a(n,d_a)$ code.

Of course

$$U_a(n,d_a) \leq W_a(n,d_a) \leq A_a(n,d_a). \tag{6.4}$$

To illustrate the existence of $WP$ $C_a(n,d_a)$ codes, we present some examples.

**Example 6.1** Let $C$ be the repetition code of length $n$. Then $E = \mathbf{V_n}$, $S_a(\mathbf{0},n-1) = \{\mathbf{0}\}$ and $S_a(\mathbf{1},n-1) = \mathbf{V_n}\backslash\{\mathbf{0}\}$. Hence the condition stated in (6.3) is satisfied, and $C$ is a perfect code.

**Example 6.2** Let $C$ consist of the three words: 00000, 11000 and 00111. Then, $C$ is a nontrivial $WP$ $C_a(5,2)$ code and $r(00111) = 3$, whereas $r(\mathbf{0}) = r(11000) = 2$.

**Example 6.3** Let $C$ be the code obtained from the optimal $C_a(6,2)$ code in (5.1) by deleting the all-one vector $\mathbf{1}$. Then, it can be checked that $C$ is a nontrivial $UWP$ code of size 11 by Definition 6.2. From Theorem 5.2, (6.4) and Theorem 6.8 (see Section 6.3), it follows that $U_a(6,2) = W_a(6,2) = 11$. This code is unique up to permutation.

Theorem 2.3 shows that concatenating two $C_a(n,d_a)$ codes gives a $C_a(2n,2d_a)$ code. However, concatenating two weakly perfect codes does not necessarily result in a weakly perfect code. For instance, concatenating the code $C$ in Example 6.3 with itself does not yield a $WP$ $C_a(12,4)$ code.

If $C$ is a $WP$ $C_a(n,d_a)$ code, then the code obtained by deleting one of the largest weight codewords of $C$ will be a $WP$ code of length $n$ as well. The proof is easy. Let $\mathbf{x}$ be one of the largest weight codewords of $C$, and $C' = C\backslash\{\mathbf{x}\}$. Also, let $r(\mathbf{c}) = d_a(\mathbf{c}, C\backslash\{\mathbf{c}\})$ and $r'(\mathbf{c}) = d_a(\mathbf{c}, C'\backslash\{\mathbf{c}\})$ for any $\mathbf{c} \in C'$. Then $r(\mathbf{c}) \leq r'(\mathbf{c})$ for any $\mathbf{c} \in C'$. Let $E'$ denote the set consisting of all possibly received words corresponding to $C'$, i.e. $E' = \{\mathbf{y} \in \mathbf{V_n} | \exists_{\mathbf{c}\in C'}[\mathbf{c} \geq \mathbf{y}]\}$. Now we need to show that $E' \subseteq \bigcup_{\mathbf{c}\in C'} S_a(\mathbf{c}, r'(\mathbf{c}) - 1)$. Let $\mathbf{z} \in E'$. Since $C$ is a $WP$ code and $E' \subseteq E$, one has

$$\mathbf{z} \in \bigcup_{\mathbf{c}\in C'} S_a(\mathbf{c}, r(\mathbf{c}) - 1) \cup S_a(\mathbf{x}, r(\mathbf{x}) - 1).$$

Note that $d_a(\mathbf{z},\mathbf{x}) \geq r(\mathbf{x})$. So $\mathbf{z} \notin S_a(\mathbf{x}, r(\mathbf{x}) - 1)$. Hence

$$\mathbf{z} \in \bigcup_{\mathbf{c}\in C'} S_a(\mathbf{c}, r(\mathbf{c}) - 1) \subseteq \bigcup_{\mathbf{c}\in C'} S_a(\mathbf{c}, r'(\mathbf{c}) - 1).$$

Thus $C'$ is a $WP$ code of length $n$ (but possibly with a larger minimum distance than $d_a$).

**Example 6.4** Let $C$ be the code defined in Example 6.3. The set $\{\mathbf{x} \mid (\mathbf{x}, 1) \in C\}$ gives a $UWP$ $C_a(5,2)$ code of size 5 by Definition 6.2. From Theorem 5.1, (6.4) and Theorem 6.8 (see Section 6.3), it follows that $U_a(5,2) = W_a(5,2) = 5$.

**Example 6.5** For any integer number $w$ $(0 \leq w < n)$, the set of all words of length $n$ and weight at most $w$ together with the all-one vector $\mathbf{1}$ is a perfect $C_a(n,1)$ code.

The *probability of error*, or the *word error rate*, $P_{err}$, for a particular decoding rule is the probability that the decoder produces a wrong codeword. Assume that $\mathbf{c}_1, \mathbf{c}_2, \cdots, \mathbf{c}_M$ are codewords of a code $C$ which are used with equal probability, then the probability of incorrect decoding of a received word is

$$P_{err}(C) = \frac{1}{M}\sum_{i=1}^{M} P_i \tag{6.5}$$

where $P_i$ is the probability of making an incorrect decision given that $\mathbf{c}_i$ is transmitted for $i = 1, 2, \cdots, M$.

For a $C_a(n, d_a)$ code $C$, our decoding rules are based on two assumptions. First of all, it is assumed that all codewords are transmitted equally likely during communication. Furthermore, the decoding strategy is that if $\mathbf{x}$ is received, then $\mathbf{x}$ is decoded into a codeword $\mathbf{c}$ where $\mathbf{c} \geq \mathbf{x}$ and $w(\mathbf{c}) = min\{w(\mathbf{y}) | \mathbf{y} \in C \wedge \mathbf{y} \geq \mathbf{x}\}$. This decoding rule results in *maximum-likelihood-decoding.*

Section 6.2 will present some basic results derived from the above definitions which will be needed to prove the main conclusions, which will be presented in Section 6.3. It is shown that any perfect code defined in Definition 6.2 has a trivial form. To be more precise, it must be the repetition code. This answers the first question listed in Section 1.4. It follows that any asymmetric error-correcting code for which all the Goldbaum inequalities [24] are sharp must have a trivial form too. Further analysis shows that any weakly perfect code which is nontrivial can always be enlarged to a bigger code of the same length and distance, which answers the second question in Section1.4. A general look on $UWP$ $C_a(n, d_a)$ codes is given in Section 6.4. In Section 6.5, we discuss $UWP$ codes of length $\leq 15$ capable of correcting single errors. Some explicit constructions of codes are given.

## 6.2 Some results related to $C_a(n, d_a)$ codes

In this section we shall derive several results regarding $C_a(n, d_a)$ codes that are interesting in their own right but are also necessary for deriving the results in the next section.

**Lemma 6.1** *Let $C$ be a $C_a(n, d_a)$ code. Then the following properties hold:*

1. *if $C$ is nontrivial, then $r(\mathbf{c}) \leq n - d_a$ for any codeword $\mathbf{c} \in C$.*

2. *for any two different codewords $\mathbf{c}_1$ and $\mathbf{c}_2$,*

$$S_a(\mathbf{c}_1, r(\mathbf{c}_1) - 1) \cap S_a(\mathbf{c}_2, r(\mathbf{c}_2) - 1) = \emptyset.$$

*Proof:* The proof of the first assertion is straightforward and omitted. In order to prove the second assertion, take $r = max\{r(\mathbf{c}_1), r(\mathbf{c}_2)\}$. Since $d_a(\mathbf{c}_1, \mathbf{c}_2) \geq r$, without loss of generality, we may assume that $N(\mathbf{c}_1, \mathbf{c}_2) \geq r$. If there exists a vector $\mathbf{x}$ such that $\mathbf{x} \in S_a(\mathbf{c}_1, r(\mathbf{c}_1) - 1) \cap S_a(\mathbf{c}_2, r(\mathbf{c}_2) - 1)$, then from (6.2) one has that $\mathbf{x} \leq \mathbf{c}_1$, $\mathbf{x} \leq \mathbf{c}_2$ and $N(\mathbf{c}_1, \mathbf{x}) \leq r(\mathbf{c}_1) - 1$. This implies that

$$r - 1 \geq r(\mathbf{c}_1) - 1 \geq N(\mathbf{c}_1, \mathbf{x}) \geq N(\mathbf{c}_1, \mathbf{c}_2) \geq r,$$

which is a contradiction. □

Theorem 1.1 shows that $C_a(n,d_a)$ codes can correct up to $d_a-1$ asymmetric errors. However, possibly there exists a codeword $\mathbf{c}$ such that $r(\mathbf{c}) > d_a$. It follows that the minimum distance criterion of judging capabilities of correcting errors of codes can be generalized. This motivates us to introduce the *average error-correcting capability* of a code. The *average error-correcting capability* of a $C_a(n,d_a)$ code $C$ is defined:

$$\overline{r}(C) = \frac{1}{|C|}\sum_{\mathbf{c}\in C}(r(\mathbf{c})-1). \tag{6.6}$$

For the average error-correcting capability of the code $C$, one remark needs to be given here, namely if $\mathbf{c}$ is a codeword of $C$ of weight less than $d_a$, then the error-correcting capability of $\mathbf{c}$ may be referred as any number which is greater than $w(\mathbf{c})$. Hence in the sense of error-correcting capability, $r(\mathbf{c})$ does not give an appropriate measure, nor does $\overline{r}(C)$. However, this will not give much additional scope in the error-correcting capability of the code $C$, so we still adopt the definition in (6.6) as the average error-correcting capability of $C$. Another thing which should be noticed is that sometimes a codeword $\mathbf{c}$ may correct more than $r(\mathbf{c})-1$ errors. The following Theorem 6.1 shows that if a $C_a(n,d_a)$ code does not contain the all-one vector $\mathbf{1}$, then changing a maximal weight codeword into $\mathbf{1}$ may increase the average error-correcting capability of such code.

**Theorem 6.1** *Let $C$ be a $C_a(n,d_a)$ code with average error-correcting capability $\overline{r}(C)$, and $\mathbf{x}$ be a maximum weight codeword of $C$. If $\mathbf{x}\neq\mathbf{1}$, then the code $C'=(C\backslash\{\mathbf{x}\})\cup\{\mathbf{1}\}$ has average error-correcting capability $\overline{r}(C')\geq\overline{r}(C)$.*

*Proof:* Without loss of generality, let $C$ contain $M$ codewords: $\{\mathbf{c}_1,\cdots,\mathbf{c}_M\}$ with $w(\mathbf{c}_i)\leq w(\mathbf{c}_j)$ for $i\leq j$ and $i,j=1,2,\cdots,M$ ($\mathbf{x}=\mathbf{c}_M$). Let $C'=\{\mathbf{c}_1,\cdots,\mathbf{c}_{M-1},\mathbf{1}\}$. From (6.1), it is clear that $d_a(\mathbf{c}_i,\mathbf{c}_M)\leq d_a(\mathbf{c}_i,\mathbf{1})$ for all $i\leq M-1$. This implies the assertion. □

**Lemma 6.2** *If $C$ is a $C_a(n,d_a)$ code with the property: $w(C)\leq w(C')$ for any $C_a(n,d_a)$ code $C'$ with $|C'|=|C|$, then $r(\mathbf{c})=d_a$ for any $\mathbf{c}\in C$.*

*Proof:* Without loss of generality, we may assume that $C$ consists of the $M$ codewords: $\mathbf{c}_1,\cdots,\mathbf{c}_M$ with nondecreasing weight order, i.e., $w(\mathbf{c}_i)\leq w(\mathbf{c}_j)$ for $1\leq i<j\leq M$. Since $C$ is of minimum weight, the codeword $\mathbf{c}_1$ must be the all-zero vector $\mathbf{0}$. If $r(\mathbf{c}_1)\geq d_a+1$, then any $1\to 0$ change in $\mathbf{c}_2$ can be introduced such that the resulting code is still a $C_a(n,d_a)$ code, which contradicts the assumption on the weight of $C$. Similarly, if $r(\mathbf{c})\geq d_a+1$ for $\mathbf{c}\neq\mathbf{c}_1$, then introducing any $1\to 0$ change in $\mathbf{c}$ will give the same contradiction. □

**Theorem 6.2** *A $C_a(n,d_a)$ code $C$ can always be transformed into another $C_a(n,d_a)$ code $C'$ so that $r(\mathbf{c})=d_a$ for any codeword $\mathbf{c}$ of $C'$.*

*Proof:* Without loss of generality, we may assume that $\mathbf{0} \in C$. The same argument used in the proof of Lemma 6.2 can be applied here. Note that the weight of $C$ is finite. Therefore, the process of making $1 \to 0$ changes must terminate in a finite number of steps. □

Theorem 6.2 admits the following heuristic interpretation. Given a $C_a(n, d_a)$ code $C$. From Lemma 6.1, it follows that all the packing spheres centered at the codewords of $C$ are disjoint in the space $\mathbf{V_n}$. If there is $r(\mathbf{c})$ which is greater than $d_a$, then the corresponding center $\mathbf{c}$ can be replaced by a word $\mathbf{y}$ so that $S_a(\mathbf{y}, d_a - 1)$ is a proper subset of $S_a(\mathbf{c}, r(\mathbf{c}) - 1)$, keeping it disjoint from the other packing spheres. Thus, by this technique, all the packing spheres with larger radii ($\geq d_a$) can be reduced to smaller packing spheres that are still disjoint.

Theorem 6.2 also shows that any $C_a(n, d_a)$ code of maximum size can be assumed to satisfy that for any codeword, it has distance $d_a$ to the set of all other codewords. An interesting question is whether this condition is necessary for any nontrivial $C_a(n, d_a)$ code of maximum size. From Theorem 6.2, it follows that the answer is positive for codes which are unique up to permutation. But, in general, it is not true. Two counterexamples are shown below.

**Example 6.6** The four words: 0000000, 1110000, 0001110 and 1111111 form an optimal $C_a(7, 3)$ code. However, the minimum distance from the codeword $\mathbf{1}$ to the other three codewords is 4 which is greater than the minimum distance of the code.

For Example 6.6, one has that $A_a(6, 3) = A_a(7, 3) = 4$ (see Table A.1 in Appendix $A$). In the following, we shall give another example which shows that $C_a(n, d_a)$ codes of size $A_a(n, d_a)$ exist so that at least one codeword is of minimum distance greater than $d_a$ to all other codewords, even though the relation $A_a(n - 1, d_a) < A_a(n, d_a)$ holds.

**Example 6.7** The $C_a(17, 6)$ code consisting of the following eight words:

00000000000000000
11111100000000000
00000011111100000
11000011000011110
00111000111011100
10011110010110011
01100101101101011
11111111111111111

is optimal. From Table A.3 in Appendix $A$, it follows that $A_a(16, 6) = 7 < A_a(17, 6) = 8$. However, the minimum asymmetric distance from the codeword $\mathbf{1}$ to the other codewords is 7.

**Lemma 6.3** *Let $C$ be a $C_a(n, d_a)$ code. If $w(\mathbf{c}) < r(\mathbf{c})$ for a certain $\mathbf{c} \in C$, then $\mathbf{c}$ is of minimum weight in $C$, i.e, $w(\mathbf{c}) < min\{w(\mathbf{x}) | \mathbf{x} \in C \wedge \mathbf{x} \neq \mathbf{c}\}$.*

*Proof:* Suppose that there is a codeword $\mathbf{x}$ in $C$ such that $w(\mathbf{x}) \leq w(\mathbf{c})$. Then $d_a(\mathbf{x}, \mathbf{c}) \leq w(\mathbf{c}) < r(\mathbf{c})$, which contradicts the definition of $r(\mathbf{c})$. □

**Lemma 6.4** *For an optimal $C_a(n, d_a)$ code $C$, $r(\mathbf{c}) \leq 2d_a - 1$ for any codeword $\mathbf{c} \in C$.*

*Proof:* Suppose that there exists a codeword $\mathbf{c}$ such that $r(\mathbf{c}) \geq 2d_a$. Let $\mathbf{y}$ be any word with distance $d_a$ from $\mathbf{c}$. Since $C$ is of maximum size, $\mathbf{y}$ cannot be added to $C$ as a codeword without affecting the minimum distance $d_a$. Hence, $\mathbf{y}$ has distance $\leq d_a - 1$ to a codeword in $C$, say $\mathbf{x}$. From the triangle inequality, we get the following contradiction:

$$2d_a \leq d_a(\mathbf{x}, \mathbf{c}) \leq d_a(\mathbf{x}, \mathbf{y}) + d_a(\mathbf{y}, \mathbf{c}) \leq d_a - 1 + d_a = 2d_a - 1.$$

□

From Examples 6.6 and 6.7, it follows that for an optimal $C_a(n, d_a)$ code, the bound $2d_a - 1$ shown in Lemma 6.4 certainly is not tight but also cannot be replaced by $d_a$. The following theorem strengthens this bound.

**Theorem 6.3** *Let $C$ be an optimal $C_a(n, d_a)$ code. If $n \leq 2d_a$, then $r(c) = d_a$ for any codeword $\mathbf{c}$ of $C$. If $n > 2d_a$ and $\mathbf{c} \in C$, then*

$$r(\mathbf{c}) < \begin{cases} 2d_a - w(\mathbf{c}), & for \;\; 0 \leq w(\mathbf{c}) < d_a; \\ 3d_a/2, & for \;\; d_a \leq w(\mathbf{c}) \leq n - d_a; \\ 2d_a - n + w(\mathbf{c}), & for \;\; n - d_a < w(\mathbf{c}) \leq n. \end{cases}$$

*Proof:* When $n < 2d_a$, $C$ is the repetition code. So the assertion holds. If $n = 2d_a$, the following four words: $\mathbf{0}^{d_a}\mathbf{0}^{d_a}$, $\mathbf{1}^{d_a}\mathbf{0}^{d_a}$, $\mathbf{0}^{d_a}\mathbf{1}^{d_a}$ and $\mathbf{1}^{d_a}\mathbf{1}^{d_a}$ form an optimal $C_a(2d_a, d_a)$ code, which is unique up to permutation. Hence, $r(\mathbf{c}) = d_a$ for any $\mathbf{c} \in C$. Let $n > 2d_a$ and $\mathbf{c} \in C$. Without loss of generality, we may assume that $\mathbf{c} = \mathbf{1}^w\mathbf{0}^{n-w}$ where $w$ is the weight of the codeword $\mathbf{c}$. Since $C$ is optimal, it must contain a unique codeword which has weight less than $d_a$. Suppose that $\mathbf{c}$ is such codeword. Because $n - w \geq d_a$ and $r(\mathbf{c}) < 2d_a$ (using Lemma 6.4), we can put

$$\mathbf{a} = \mathbf{1}^w\mathbf{1}^{r(\mathbf{c})-d_a}\mathbf{0}^{n-w-(r(\mathbf{c})-d_a)}.$$

From the triangle inequality, the asymmetric distance from $\mathbf{a}$ to any codeword other than $\mathbf{c}$ must be at least $d_a$. Moreover, the weight of the word $\mathbf{a}$ must be less than $d_a$, otherwise a $C_a(n, d_a)$ code with larger size can be obtained by replacing $\mathbf{c}$ with $\mathbf{a}$ and $\mathbf{0}$ (if $\mathbf{c} = \mathbf{0}$, then one can simply add $\mathbf{a}$ into $C$), which contradicts the assumption on the size of $C$. Therefore $w(\mathbf{a}) = w + r(\mathbf{c}) - d_a < d_a$. This means that $r(\mathbf{c}) < 2d_a - w(\mathbf{c})$. Similarly, one can prove that for the unique highest weight codeword $\mathbf{c}$

$(n - d_a < w(\mathbf{c}) \leq n)$, $r(\mathbf{c}) < 2d_a - n + w(\mathbf{c})$. For any other codeword $\mathbf{c}$, by using Lemma 6.3, $w(\mathbf{c}) \geq r(\mathbf{c})$. Put

$$\begin{aligned} \mathbf{a} &= 1^w 1^{r(\mathbf{c})-d_a} 0^{n-w-(r(\mathbf{c})-d_a)} \\ \mathbf{b} &= 0^{r(\mathbf{c})-d_a} 1^{w-(r(\mathbf{c})-d_a)} 0^{n-w}. \end{aligned}$$

Hence from the triangle inequality, it follows that for any $\mathbf{c}' \in C$ and $\mathbf{c}' \neq \mathbf{c}$,

$$d_a(\mathbf{a}, \mathbf{c}') \geq d_a(\mathbf{c}', \mathbf{c}) - d_a(\mathbf{c}, \mathbf{a}) \geq r(\mathbf{c}) - (r(\mathbf{c}) - d_a) = d_a.$$

Similarly, $d_a(\mathbf{b}, \mathbf{c}') \geq d_a$. Thus, the asymmetric distance between $\mathbf{a}$ and $\mathbf{b}$ must be less than $d_a$. Indeed, if this is not the case, replacing $\mathbf{c}$ by $\mathbf{a}$ and $\mathbf{b}$ in $C$ will result in a $C_a(n, d_a)$ code of larger size, which is not possible. Therefore $d_a(\mathbf{a}, \mathbf{b}) = 2(r(\mathbf{c}) - d_a) < d_a$. This leads to $r(\mathbf{c}) < 3d_a/2$. □

Theorem 6.3 tells us that in an optimal $C_a(n, d_a)$ code there are at most two codewords at asymmetric distance greater than or equal to $3d_a/2$ to all other codewords. Specifically, one has that $r(\mathbf{0}) < 2d_a$ and $r(\mathbf{1}) < 2d_a$ if $\mathbf{0}$ and $\mathbf{1}$ are these codewords. Furthermore, applying Theorem 6.3 to the case $d_a = 2$ presents some interesting results. In fact, if $C$ is an optimal $C_a(n, 2)$ code with $1 \leq w(\mathbf{c}) \leq n - 1$ for all $\mathbf{c} \in C$, then from Theorem 6.3, it follows that $r(\mathbf{c}) = 2$ for all $\mathbf{c} \in C$. Though, in general all $r(\mathbf{c})$ are not necessary equal to $d_a$ for a nontrivial $C_a(n, d_a)$ code of maximum size, it is at least necessary for many optimal $C_a(n, d_a)$ codes, as shown in the following theorem.

**Theorem 6.4** *Let $C$ be an optimal $C_a(n, 2)$ code. If $n \not\equiv 1$ or $3$ (mod 6), then $r(\mathbf{c}) = 2$ for all $\mathbf{c} \in C$.*

*Proof:* Without loss of generality, the all-zero vector $\mathbf{0}$ may be assumed to be a codeword. By Theorem 6.3 and for reasons of symmetry, we only need to prove that $r(\mathbf{0}) = 2$. Assume $r(\mathbf{0}) > 2$. Then from Theorem 6.3 it follows that $r(\mathbf{0}) = 3$. This means that apart from the all-zero vector $\mathbf{0}$, all the other codewords of $C$ have weight at least three. If the length $n$ is not congruent to 1 or 3 modulo 6, then the set of codewords of $C$ of weight 3 cannot form a Steiner triple system [32]. Hence, there exists at least one word of weight 2 which has asymmetric distance greater than or equal to 2 to all codewords of weight 3 and trivially is at distance greater than or equal to 2 to all codewords of weight greater than 3 as well as to $\mathbf{0}$. So this word of weight 2 can be added to $C$ without decreasing the minimum distance, which contradicts the assumption that the code $C$ is optimal. □

The question whether any optimal $C_a(n, 2)$ code $C$ must satisfy that $r(\mathbf{c}) = 2$ for any $\mathbf{c} \in C$ is still open. From the proof of Theorem 6.4, one only needs to prove that no optimal $C_a(n, 2)$ code exists that contains $\mathbf{0}$, and in which the codewords of weight 3 form a Steiner triple system $S(2, 3, n)$. At the present, we could only check this for $n = 7$ and one case for $n = 9$ (based on the known results). Therefore, we are left with

**Conjecture:** Any optimal $C_a(n,2)$ code $C$ satisfies $r(\mathbf{c}) = 2$ for all $\mathbf{c} \in C$.

We shall now investigate the significance of taking the all-one vector $\mathbf{1}$ as a codeword in a $C_a(n,d_a)$ code (this will come back when $WP$ $C_a(n,d_a)$ codes will be discussed in the next section). It is well known (Kløve's observation) that the all-one vector $\mathbf{1}$ and the all-zero vector $\mathbf{0}$ may always be assumed to be codewords in a $C_a(n,d_a)$ code. This is useful in code constructions as shown in Chapter 3. However, for a fixed length $n$ and distance $d_a$, two or more $C_a(n,d_a)$ codes may exist, all of maximum size but not equivalent to each other. In this case, their performance cannot be judged by simply comparing their average error-correcting capabilities and their information rates, since both parameters may be equal. For example, with the same notations as used in Theorem 5.1, we let $C_1 = C_a(5,2)[0,1]$ and $C_2 = C_a(5,2)[0,0]$. Then $|C_1| = |C_2| = A_a(5,2) = 6$. So they have the same information rate. Also, for both codes the minimum distance from a certain codeword to all other codewords is 2 by Theorem 6.4. Hence they have the same average error-correcting capability. To distinguish their performance we shall study their respective probabilities of erroneous decoding.

When error probability is taken into account, one arrives at the following question: let $C$ be an optimal $C_a(n,d_a)$ code without the word $\mathbf{1}$ and let $C' = (C\backslash\{\mathbf{f}\}) \cup \{\mathbf{1}\}$ where $\mathbf{f}$ is one of the maximal weight codewords of $C$, does the inequality $P_{err}(C') \leq P_{err}(C)$ hold ? This question was essentially solved by Weber [56] (unpublished), which shows that if $\mathbf{f}$ is a codeword of $C$ of weight $w(\mathbf{f}) = n-j$ $(1 \leq j \leq d_a-1)$, then $P_{err}(C') \leq P_{err}(C)$. Therefore, for the above two codes $C_1$ and $C_2$, we have that $P_{err}(C_1) \leq P_{err}(C_2)$. In fact, one can show that $P_{err}(C_1) < P_{err}(C_2)$. Thus, $C_1$ can be said to be better than $C_2$ in the sense that it has a lower error probability. Below, a slightly more general result than that obtained by Weber will be presented in Theorem 6.5 for which the proof is essentially due to Weber.

For the decoding of a $C_a(n,d_a)$ code $C$, it is known that a received word $\mathbf{y}$ only comes from the codewords covering it. In other words, the received set $E$ depends on the specific code $C$, which is not the case for the BSC where any word in $\mathbf{V_n}$ can be a possibly received word. The strategy of a maximum likelihood decoder is of course to decode the received word $\mathbf{y}$ to one of the codewords of lowest weight covering $\mathbf{y}$. This fact is stated in Lemma 6.5. We denote the probability of receiving $\mathbf{y}$ given that $\mathbf{x}$ is transmitted as $P(\mathbf{y}|\mathbf{x})$.

**Lemma 6.5** *Let $C$ be a $C_a(n,d_a)$ code and let $\mathbf{y}$ be a received word. If $\mathbf{x}_1, \mathbf{x}_2 \in C$ with $\mathbf{x}_i \geq \mathbf{y}$ $(i = 1,2)$ and $w(\mathbf{x}_2) \geq w(\mathbf{x}_1)$, then $P(\mathbf{y}|\mathbf{x}_1) \geq P(\mathbf{y}|\mathbf{x}_2)$.*

**Theorem 6.5** *Let $C$ be a nontrivial $C_a(n,d_a)$ code and let $\mathbf{f}$ be a codeword of $C$ of maximum weight. Then, $P_{err}(C') \leq P_{err}(C)$ where $C' = (C\backslash\{\mathbf{f}\}) \cup \{\mathbf{g}\}$ and $\mathbf{g} \geq \mathbf{f}$.*

*Proof:* Obviously, $C'$ is still an AsEC code of length $n$ and minimum distance at least $d_a$. Without loss of generality, it is sufficient to consider the case: $\mathbf{f} = \mathbf{0}^j\mathbf{1}^{n-j}$ and $\mathbf{g} = \mathbf{0}^{j-1}\mathbf{1}^{n-j+1}$ for a certain $j \geq 1$. Define:

$$A = \{\mathbf{a} \in \mathbf{V_n} \mid \mathbf{f} \geq \mathbf{a} \ \wedge \ \forall_{\mathbf{c}\in C\setminus\{\mathbf{f}\}}[\mathbf{c} \not\geq \mathbf{a}]\}.$$

If $\mathbf{a} \in A$, we denote $\mathbf{a}'$ as the word obtained by changing the $j$th coordinate of $\mathbf{a}$ (which is 0 because $\mathbf{f} \geq \mathbf{a}$) to 1, and further define the set consisting of all such words $\mathbf{a}'$ by $A'$. Without loss of generality, we may assume that only the words of $A$ are decoded into the codeword $\mathbf{f}$ (clearly, if there is more than one codeword of the same maximum weight, then according to the decoding rule, some words other than the words of $A$ might be decoded into $\mathbf{f}$ as well. But the assumption does not change the overall error probability). Let $P\{correct|\mathbf{x}\}$ denote the probability of making the correct decoding decision given that $\mathbf{x}$ is transmitted. According to (6.5) and Lemma 6.5, we only need to consider two probabilities: $P\{correct|\mathbf{f}\}$ and $P\{correct|\mathbf{g}\}$. Note that $A \cap A' = \emptyset$. One obtains

$$\begin{aligned}
P(correct|\mathbf{g}) &\geq \textstyle\sum_{\mathbf{a}\in A} P(\mathbf{a}|\mathbf{g}) + \sum_{\mathbf{a}'\in A'} P(\mathbf{a}'|\mathbf{g}) \\
&= \textstyle\sum_{\mathbf{a}\in A} p^{n-j+1-w(\mathbf{a})}(1-p)^{w(\mathbf{a})} + \\
&\quad \textstyle\sum_{\mathbf{a}'\in A'} p^{n-j+1-w(\mathbf{a}')}(1-p)^{w(\mathbf{a}')} \\
&= (p + (1-p)) \textstyle\sum_{\mathbf{a}\in A} p^{n-j-w(\mathbf{a})}(1-p)^{w(\mathbf{a})} \\
&= \textstyle\sum_{\mathbf{a}\in A} P(\mathbf{a}|\mathbf{f}) = P(correct|\mathbf{f}).
\end{aligned}$$

Thus, $P_{err}(C') \leq P_{err}(C)$ which completes the proof. □

Weber's original result is a particular case of Theorem 6.5 by taking $\mathbf{g} = \mathbf{1}$ and $\mathbf{f}$ a codeword of weight greater than $n - d_a$. From Theorem 6.5 and Theorem 6.1 together with the observation by Kløve, it follows that the all-one vector $\mathbf{1}$ should always be included in a $C_a(n, d_a)$ code. However, in the next section it will be shown that the all-one vector $\mathbf{1}$ cannot be a codeword in any nontrivial $WP$ code for correcting asymmetric errors.

## 6.3 On the rate of weakly perfect codes

In this section, we will present the answers to the two questions stated in Section 1.4. We shall show that any perfect $C_a(n, d_a)$ code must have a trivial form. This implies that for binary asymmetric channels only the repetition code gives rise to a partition of $\mathbf{V_n}$. Furthermore, it will be shown that any nontrivial $WP$ $C_a(n, d_a)$ code of maximum size cannot be optimal, i.e., $W_a(n, d_a) < A_a(n, d_a)$ for nontrivial cases for any $n$ and $d_a$.

**Lemma 6.6** *Let $C$ be a WP $C_a(n, d_a)$ code containing the all-one vector* $\mathbf{1}$. *Then $C$ must be the repetition code.*

*Proof:* Since $\mathbf{1} \in C$, the received set $E$ corresponding to $C$ equals the whole space $\mathbf{V_n}$. From (6.3) in Definition 6.2, it follows that

$$\mathbf{V_n} = \bigcup_{\mathbf{c} \in C} S_a(\mathbf{c}, r(\mathbf{c}) - 1). \tag{6.7}$$

Let $r = r(\mathbf{1})$. Obviously, $r \geq d_a \geq 2$ and the weight distribution of $C$ satisfies $A_{n-1} = A_{n-2} = \cdots = A_{n-r+1} = 0$. Furthermore, one has

$$A_{n-r} = \binom{n}{n-r}. \tag{6.8}$$

Otherwise, there would exist at least one word of weight $n - r$ which does not belong to the right-hand side of (6.7), which is not possible. If $n - r \geq 1$ in (6.8), there must be two different codewords of weight $n - r$ such that they are at asymmetric distance 1 apart, which disagrees with $d_a \geq 2$. So $n - r = 0$, that is, $n = r$. This shows that the code $C$ is the repetition code which is trivial. □

**Theorem 6.6** *A $C_a(n, d_a)$ code $C$ is perfect if and only if $C$ is the repetition code.*

*Proof:* Because any perfect $C_a(n, d_a)$ code contains the all-one vector $\mathbf{1}$, the assertion directly follows from Lemma 6.6 and Example 6.1. □

Instead of applying the sphere packing concept to the whole space $\mathbf{V_n}$, Goldbaum [24] derives an upper bound on the maximum size of an asymmetric error-correcting code which is only based on the constraints on the vectors of length $n$ having a certain weight $i$. He shows that the weight distribution $A_0, A_1, \ldots, A_n$ of a $C_a(n, d_a)$ code satisfies

$$\sum_{j=0}^{d_a - 1} \binom{i+j}{j} A_{i+j} \leq \binom{n}{i} \tag{6.9}$$

for $i = 0, 1, \ldots, n$. According to Lemma 6.6, we can conclude that

**Theorem 6.7** *The only $C_a(n, d_a)$ code ($n \geq d_a \geq 2$) for which all the Goldbaum inequalities (6.9) are sharp is the the repetition code.*

*Proof:* By taking $i = n$ and $i = n - d_a$ respectively in (6.9), one will be in the same situation as described in the proof of Lemma 6.6. So the result is the same as there. □

Theorem 6.6 shows that no nontrivial $C_a(n, d_a)$ code exists such that the union of all packing spheres centered at the codewords covers the whole space $\mathbf{V_n}$. However, in practice, we are only interested in those words which are in the received set $E$ corresponding to $C$ instead of the whole space $\mathbf{V_n}$. In general, the cardinality of $E$ is greater than that of the union

$S$ of all packing spheres centered at the codewords. But for $WP$ codes, both sets are equal, i.e., $E = S$, by Definition 6.2. Therefore, in this case any possibly received word can always be decoded to a unique codeword (maybe incorrectly). Specifically, a $UWP$ $C_a(n, d_a)$ code can correct all errors of weight $\le d_a - 1$, and none of weight greater than or equal to $d_a$. Of course, we expect that the cardinality (or information rate) of a $WP$ code is as large as possible. Thus, one question arises, namely, whether a nontrivial $WP$ $C_a(n, d_a)$ code exists such that it contains $A_a(n, d_a)$ codewords. In the following, we shall show that the answer to this question is negative.

**Theorem 6.8** *If $n \ge 2d_a$, then $W_a(n, d_a) < A_a(n, d_a)$.*

*Proof:* Let $C$ be a $WP$ $C_a(n, d_a)$ code with cardinality $W_a(n, d_a)$ and with $n \ge 2d_a$. Let $A_0, \cdots, A_n$ be the weight distribution of $C$. Note that $\sum_{i=n-d_a+1}^{n} A_i \le 1$. If $\sum_{i=n-d_a+1}^{n} A_i = 0$, then the all-one vector $\mathbf{1}$ can be always added to $C$ such that this enlarged code is still a $C_a(n, d_a)$ code. So the claim is ture in this case. If $A_n = 1$, then from Lemma 6.6 it follows that $C$ is the repetition code. Because $A_a(n, d_a) \ge 4$ when $n \ge 2d_a$, the assertion holds for this trivial case too. Now, suppose that

$$\sum_{i=n-d_a+1}^{n-1} A_i = 1. \qquad (\text{hence } A_n = 0)$$

Then, there will be an index $j$ $(1 \le j \le d_a - 1)$ such that $A_{n-j} = 1$. Let $\mathbf{a}$ represent the codeword of weight $n - j$, and without loss of generality, the word $\mathbf{a}$ may be assumed to be $\mathbf{a} = \mathbf{0}^j \mathbf{1}^{n-j}$. If $|C| = W_a(n, d_a) = A_a(n, d_a)$, then from Theorem 6.3 it follows that $w(\mathbf{a}) - r(\mathbf{a}) \ge n - 2d_a + 1$. Since $n \ge 2d_a$ and $w(\mathbf{a}) = n - j$, one has that $n - j - r(\mathbf{a}) \ge 1$. Define the following three words of length $n$ (note that $2 \le d_a \le r(\mathbf{a})$):

$$\begin{aligned} \mathbf{x}_1 &= \mathbf{0}^j \, \mathbf{1}^{n-j-r(\mathbf{a})-1} \, 100 \, \mathbf{0}^{r(\mathbf{a})-2}, \\ \mathbf{x}_2 &= \mathbf{0}^j \, \mathbf{1}^{n-j-r(\mathbf{a})-1} \, 010 \, \mathbf{0}^{r(\mathbf{a})-2}, \\ \mathbf{x}_3 &= \mathbf{0}^j \, \mathbf{1}^{n-j-r(\mathbf{a})-1} \, 001 \, \mathbf{0}^{r(\mathbf{a})-2}. \end{aligned}$$

Obviously, the above three words are all of weight $n - j - r(\mathbf{a})$. Therefore, none of them can be contained in the sphere $S_a(\mathbf{a}, r(\mathbf{a}) - 1)$. Since $C$ is weakly perfect, every word of weight $n - j - r(\mathbf{a})$ covered by $\mathbf{a}$ must be covered by one of the codewords of $C$ of weight $i$ where $n - j - r(\mathbf{a}) \le i \le n - r(\mathbf{a})$. Note that the minimum asymmetric distance from the codeword $\mathbf{a}$ to the other codewords is $r(\mathbf{a})$ and $\mathbf{a}$ is of the highest weight. With this in mind, one will arrive at the fact that the three words $\mathbf{x}_1$, $\mathbf{x}_2$ and $\mathbf{x}_3$ must be covered uniquely by three different other codewords of $C$ respectively, and these three codewords are necessarily of the following forms respectively:

$$\mathbf{a}_1 = \mathbf{b}_1 \, \mathbf{1}^{n-j-r(\mathbf{a})-1} \, 100 \, \mathbf{0}^{r(\mathbf{a})-2},$$

$$\mathbf{a}_2 = \mathbf{b}_2 \; 1^{n-j-r(\mathbf{a})-1} \; 010 \; 0^{r(\mathbf{a})-2},$$

$$\mathbf{a}_3 = \mathbf{b}_3 \; 1^{n-j-r(\mathbf{a})-1} \; 001 \; 0^{r(\mathbf{a})-2}.$$

where $\mathbf{b}_1$, $\mathbf{b}_2$ and $\mathbf{b}_3$ are of length $j$. However, since $d_a(\mathbf{a}_1, \mathbf{a}_2) \geq d_a$ and the length of $\mathbf{b}_1$ and $\mathbf{b}_2$ is $j \leq d_a - 1$, one must have $w(\mathbf{b}_1) = j = d_a - 1$ and $w(\mathbf{b}_2) = 0$ (or vice versa). Then $w(\mathbf{b}_3)$ must equal zero by $d_a(\mathbf{a}_1, \mathbf{a}_3) \geq d_a$. This results in $d_a(\mathbf{a}_2, \mathbf{a}_3) = 1$ which is a contradiction. Hence, $|C| < A_a(n, d_a)$ if $n \geq 2d_a$. □

Since a $C_a(n, d_a)$ code, if $n < 2d_a$, is trivial, $U_a(n, d_a) = W_a(n, d_a) = A_a(n, d_a) = 2$ when $n < 2d_a$. Hence, Theorem 6.8 states that the rate of a nontrivial $C_a(n, d_a)$ code of maximum size is always greater than that of $WP$ $C_a(n, d_a)$ codes. Two direct corollaries to Theorem 6.8 are

**Corollary 6.1** *If $n \geq 2d_a$, then any nontrivial $WP$ $C_a(n, d_a)$ code cannot contain a codeword of weight greater than $n - d_a$. Therefore, a $WP$ $C_a(n, d_a)$ code with $n \geq 2d_a$ can always be enlarged with the all-one vector* $\mathbf{1}$ *to a bigger $C_a(n, d_a)$ code.*

*Proof:* From Lemma 6.6, we only need to show the assertion in the corollary is true for $A_n = 0$ and $n \geq 2d_a$. Let $C$ be a nontrivial $WP$ $C_a(n, d_a)$ code containing the codeword $\mathbf{a}$ shown in the proof of Theorem 6.8. From Lemma 6.3, it follows that $w(\mathbf{a}) \geq r(\mathbf{a})$. If $w(\mathbf{a}) \geq r(\mathbf{a}) + 1$, the same contradiction stated in the proof of Theorem 6.8 will be obtained. On the other hand, one can readily verify that the relation $w(\mathbf{a}) = r(\mathbf{a})$ will lead to $|C| \leq 2$ which is trivial, which contradicts the assumption that $C$ is nontrivial. □

**Corollary 6.2** *$U_a(n, d_a) < A_a(n, d_a)$ for $n \geq 2d_a$.*

## 6.4 Properties of $UWP$ $C_a(n, d_a)$ codes

From Theorem 6.6, we know that the vector $\mathbf{1}$ cannot be a codeword of a nontrivial $UWP$ $C_a(n, d_a)$ code. How about the vector $\mathbf{0}$? Evidently, $\mathbf{0}$ is always a possibly received word. This means that $\mathbf{0}$ is always an element of $E$. One may think that the all-zero vector $\mathbf{0}$ should always be chosen as a codeword in a $C_a(n, d_a)$ code, since it cannot be distorted by the channel. However, it will be shown that for a $UWP$ $C_a(n, d_a)$ code, whether $\mathbf{0}$ is a codeword or not depends on the length $n$ and the asymmetric distance $d_a$. We start with the following theorem.

**Theorem 6.9** *Let $C$ be a nontrivial $UWP$ $C_a(n, d_a)$ code. Define $r$ by $n \equiv r \pmod{d_a}$ $(0 \leq r \leq d_a - 1)$. Then $A_r = 1$, $A_{d_a} = (n - r)/d_a$ and $A_i = 0$ for $i \neq r$ and $0 \leq i \leq d_a - 1$.*

*Proof:* For $UWP$ $C_a(n, d_a)$ codes, the sum $\sum_{i=0}^{d_a - 1} A_i = 1$ (since $\mathbf{0} \in E$) and $A_{d_a}$ must be greater than zero (consider the weight one vectors in $E$).

Also, that $C$ is nontrivial means that $2 \leq d_a \leq n - d_a$. Therefore, $n = qd_a + r$ with $q \geq 2$ and $0 \leq r \leq d_a - 1$, and $A_j = 1$ for some $j \in \{0, \cdots, d_a - 1\}$. Let $\mathbf{a}$ denote this codeword of weight $j$. Then, without loss of generality, the vector $\mathbf{a}$ and the $A_{d_a}$ codewords of weight $d_a$ may look like

$$\begin{array}{rcllllll}
\mathbf{a} & = & 1\cdots1 & 0\cdots0 & 0\cdots0 & 0\cdots0 & & 0\cdots0 \\
\mathbf{c}_1 & = & 0\cdots0 & 1\cdots1 & 0\cdots0 & 0\cdots0 & & 0\cdots0 \\
\vdots & \vdots & & & \ddots & & & \\
\mathbf{c}_{A_{d_a}} & = & \underbrace{0\cdots0}_{j} & \underbrace{0\cdots0}_{d_a} & 0\cdots0 & \underbrace{1\cdots1}_{d_a} & & \underbrace{0\cdots0}_{(q-A_{d_a})d_a+r-j}
\end{array}$$

If $(q - A_{d_a})d_a + r - j$ is not equal to 0, then any of other codewords of $C$ cannot have ones in the last $(q - A_{d_a})d_a + r - j$ positions, otherwise there would exist a possibly received word of weight 1 which is not contained in the union $\bigcup_{\mathbf{c}\in C} S_a(\mathbf{c}, d_a - 1)$. This violates the assumption that the code $C$ is a $UWP$ code. Therefore, we conclude that $(q - A_{d_a})d_a + r - j = 0$ (note the conventions stated in the paragraph after Theorem 1.1). Since $r - j < d_a$, it follows that $q - A_{d_a} = 0$ and $r = j$, which gives $A_r = 1$ and $A_{d_a} = q = (n - r)/d_a$. Since the minimum distance is $d_a$, $A_i = 0$ for $i \neq r$ and $0 \leq i \leq d_a - 1$. □

Three corollaries to Theorem 6.9 are

**Corollary 6.3** *Under the hypotheses of Theorem 6.9, $n \equiv 0 \pmod{d_a}$ if and only if $\mathbf{0} \in C$, in which case $A_{d_a} = n/d_a$.*

**Corollary 6.4** *Let $C$ be a nontrivial $UWP$ $C_a(n, d_a)$ code, and let $n$ be a prime number. Then $\mathbf{0} \notin C$.*

**Corollary 6.5** *Let $C$ be a nontrivial $UWP$ $C_a(n, d_a)$ code with $n = qd_a + r$ ($0 \leq r \leq d_a - 1$). If $r = 0$ and $d_a(d_a + 1) > n$, then $A_{d_a+1} = 0$. Also, if $r \neq 0$ and $d_a^2 > n$, then $A_{d_a+1} = 0$ as well.*

*Proof:* Suppose that $r = 0$. From Corollary 6.3, it follows that $A_{d_a} = n/d_a$. Hence, in the code $C$ there are $n/d_a$ codewords of weight $d_a$ with disjoint supports $G_i$ ($i = 1, \cdots, A_{d_a}$) that partition the set of $n$ coordinates. Let $\mathbf{c}$ be a codeword of weight $d_a + 1$. Since the minimum distance is $d_a$, $|supp(\mathbf{c}) \cap G_i| \leq 1$ for all $i = 1, \cdots, A_{d_a}$. This yields that $d_a + 1 \leq A_{d_a} = n/d_a$. It follows that $d_a(d_a + 1) \leq n$ if $A_{d_a+1}$ is not equal to zero, which is equivalent to the first assertion. Similarly, if $r \neq 0$, it follows from Theorem 6.9 that $d_a + 1 \leq q + 1$ when $A_{d_a+1} \neq 0$, which leads to the second claim. □

In Example 6.4, it is shown that a $UWP$ code of smaller length can be obtained from a $UWP$ code with a larger length. The following presents a simple construction method the other way around.

**Theorem 6.10** *For $n \geq d_a \geq 1$, $U_a(n, d_a) \leq U_a(n + 1, d_a)$. If $n + 1 \equiv 0 \pmod{d_a}$, then $U_a(n, d_a) + 1 \leq U_a(n + 1, d_a)$.*

*Proof:* Assume that $C$ is a $UWP$ $C_a(n, d_a)$ code with $U_a(n, d_a)$ codewords. From Theorem 6.9, it follows that if $A_r = 1$ for $0 \leq r \leq d_a - 2$, then a $UWP$ $C_a(n+1, d_a)$ code $C_1$ can be obtained by extending $C$ in the following way

$$C_1 = \{(\mathbf{a}, 1)\} \cup \{(\mathbf{c}, 0) \mid \mathbf{c} \neq \mathbf{a} \wedge \mathbf{c} \in C\}$$

where $\mathbf{a}$ is the codeword of $C$ of weight $r$. Moreover, when $r = d_a - 1$, then

$$C_2 = \{\mathbf{0}, (\mathbf{a}, 1)\} \cup \{(\mathbf{c}, 0) \mid \mathbf{c} \neq \mathbf{a} \wedge \mathbf{c} \in C\}$$

is a $UWP$ $C_a(n+1, d_a)$ code. Clearly, $\mid C_1 \mid = \mid C \mid$ and $\mid C_2 \mid = \mid C \mid +1$, which leads to the conclusions of the theorem. □

To obtain bounds on the size of $UWP$ codes, it turns out to be helpful to derive bounds on suitable combinations of the coefficients of the weight enumerator of such a code.

**Theorem 6.11** *A nontrivial $UWP$ $C_a(n, d_a)$ code $C$ with $A_j \neq 0$ for $n - d_a \geq j \geq d_a + 1$ satisfies $\binom{j}{d_a} \leq \sum_{i=j-d_a}^{j-1} A_i$.*

*Proof:* Let $\mathbf{c}$ be a codeword of $C$ such that $w(\mathbf{c}) = j$ and $n - d_a \geq j \geq d_a + 1$. Let $E(\mathbf{c}) = \{\mathbf{e} \mid \mathbf{e} \leq \mathbf{c} \ \wedge \ w(\mathbf{e}) = j - d_a\}$. Thus, for any $\mathbf{e} \in E(\mathbf{c})$, $\mathbf{e} \notin S_a(\mathbf{c}, d_a - 1)$. Since $C$ is a $UWP$ $C_a(n, d_a)$ code, for any $\mathbf{e} \in E(\mathbf{c})$ exactly one codeword of $C$, say $\mathbf{y}$, exists such that $w(\mathbf{y}) \leq j-1$ and $\mathbf{e} \leq \mathbf{y}$. Set

$$\mathcal{Y}(\mathbf{c}) = \{\mathbf{y} \in C \mid w(\mathbf{y}) \leq j - 1 \ \wedge \ \mathbf{e} \leq \mathbf{y} \ \wedge \ \mathbf{e} \in E(\mathbf{c})\}. \tag{6.10}$$

Then, $\binom{j}{d_a} = |E(\mathbf{c})| = \mid \mathcal{Y}(\mathbf{c}) \mid \leq \sum_{i=j-d_a}^{j-1} A_i$. □

**Example 6.8** Let $C$ be a nontrivial $UWP$ $C_a(n, d_a)$ code satisfying $A_{d_a+1} \neq 0$. Then it follows from Theorem 6.11 (taking $j = d_a + 1$), that $\binom{d_a+1}{d_a} \leq \sum_{i=1}^{d_a} A_i$, which implies $d_a + 1 \leq A_{d_a} + 1$. So $A_{d_a} \geq d_a$. Moreover, if $\mathbf{0} \in C$, then $A_{d_a} \geq d_a + 1$. We conclude from Theorem 6.9 that $n \geq d_a(d_a + 1)$, in accordance with Corollary 6.5.

In fact, from (6.10) one can easily see that the number of the codewords of weight $j - d_a$ in the set $\mathcal{Y}(\mathbf{c})$ is less than or equal to $A(j, 2d_a, j - d_a) = \lfloor \frac{j}{d_a} \rfloor$. This yields

**Corollary 6.6** *Under the same assumptions as in Theorem 6.11, one has that $\binom{j}{d_a} - \lfloor \frac{j}{d_a} \rfloor \leq \sum_{i=j-d_a+1}^{j-1} A_i$. In particular, if $d_a = 2$, then $\binom{j}{2} - \lfloor \frac{j}{2} \rfloor \leq A_{j-1}$.*

If $A_j \geq 2$ in Theorem 6.11 and if for the codewords of weight $j$, the inner product between any pair of them is less than $j - d_a$, then Theorem 6.11 can be generalized as follows.

**Theorem 6.12** *If under the assumptions of Theorem 6.11 there are $k$ distinct codewords $\mathbf{c}_1, \cdots, \mathbf{c}_k$ such that $w(\mathbf{c}_i) = j$ for all $i = 1, \cdots, k$, and $< \mathbf{c}_s, \mathbf{c}_t > \leq j - d_a - 1$ for $s \neq t$, and $s, t = 1, \cdots, k$, then $k\binom{j}{d_a} \leq \sum_{i=j-d_a}^{j-1} A_i$.*

*Proof:* For $1 \leq i \leq k$, let $E(\mathbf{c}_i) = \{\mathbf{e} \mid \mathbf{e} \leq \mathbf{c}_i \wedge w(\mathbf{e}) = j - d_a\}$. Since $< \mathbf{c}_s, \mathbf{c}_t > \leq j - d_a - 1$ for $s \neq t$, the sets $E(\mathbf{c}_s)$ and $E(\mathbf{c}_t)$ are disjoint. Also, it is clear that $E(\mathbf{c}_i) \cap S_a(\mathbf{c}_i, d_a - 1) = \emptyset$ for all $i = 1, \cdots, k$. Suppose that there is a vector $\mathbf{x}$ such that $\mathbf{x} \in E(\mathbf{c}_s) \cap S_a(\mathbf{c}_t, d_a - 1)$ where $s \neq t$. Then

$$j - d_a = w(\mathbf{x}) \leq < \mathbf{c}_s, \mathbf{c}_t > \leq j - d_a - 1$$

yields a contradiction. Thus when $s \neq t$, one also has that $E(\mathbf{c}_s) \cap S_a(\mathbf{c}_t, d_a - 1) = \emptyset$. As in the proof of Theorem 6.11, define:

$$\mathcal{Y}(\mathbf{c}_i) = \{\mathbf{x} \in C \mid w(\mathbf{x}) \leq j - 1 \wedge \mathbf{e} \leq \mathbf{x} \wedge \mathbf{e} \in E(\mathbf{c}_i)\}$$

for $i = 1, \cdots, k$. Now we want to prove that $\mathcal{Y}(\mathbf{c}_s)$ and $\mathcal{Y}(\mathbf{c}_t)$ are disjoint when $s \neq t$. Suppose the contrary holds, and let $\mathbf{z} \in \mathcal{Y}(\mathbf{c}_s) \cap \mathcal{Y}(\mathbf{c}_t)$ with $s \neq t$. Then there must exist $\mathbf{a} \in E(\mathbf{c}_s)$ and $\mathbf{b} \in E(\mathbf{c}_t)$ such that $\mathbf{a} \leq \mathbf{z}$ and $\mathbf{b} \leq \mathbf{z}$. The condition $< \mathbf{c}_s, \mathbf{c}_t > \leq j - d_a - 1$ results in $< \mathbf{a}, \mathbf{b} > \leq < \mathbf{c}_s, \mathbf{c}_t > \leq j - d_a - 1$, which leads to

$$\begin{aligned} j - 1 &\geq w(\mathbf{z}) \geq w(\mathbf{a}) + w(\mathbf{b}) - < \mathbf{a}, \mathbf{b} > \\ &\geq 2(j - d_a) - (j - 2d_a - 1) = j + 1. \end{aligned}$$

This is again a contradiction. Therefore, $\mathcal{Y}(\mathbf{c}_s) \cap \mathcal{Y}(\mathbf{c}_t) = \emptyset$ when $s \neq t$. Thus, the required result is obtained

$$\begin{aligned} k\begin{pmatrix} j \\ d_a \end{pmatrix} &= \mid \bigcup_{i=1}^{k} E(\mathbf{c}_i) \mid = \sum_{i=1}^{k} \mid E(\mathbf{c}_i) \mid \\ &= \sum_{i=1}^{k} \mid \mathcal{Y}(\mathbf{c}_i) \mid = \mid \bigcup_{i=1}^{k} \mathcal{Y}(\mathbf{c}_i) \mid \leq \sum_{i=j-d_a}^{j-1} A_i. \end{aligned}$$

□

Theorem 6.11 corresponds to the case $k = 1$ in Theorem 6.12. The following corollary is the corresponding generalization of Corollary 6.6.

**Corollary 6.7** *Under the same hypotheses as in Theorem 6.12, let $S_i$ denote the support of $\mathbf{c}_i$ $(i = 1, \cdots, k)$ and let $m = \mid S_1 \cup \cdots \cup S_k \mid$. Then*

$$k\begin{pmatrix} j \\ d_a \end{pmatrix} - A(m, 2d_a, j - d_a) \leq \sum_{i=j-d_a+1}^{j-1} A_i.$$

*In particular when $d_a = 2$,*

$$k\begin{pmatrix} j \\ 2 \end{pmatrix} - A(m, 4, j - 2) \leq A_{j-1}.$$

**Theorem 6.13** *Let $C$ be a nontrivial UWP $C_a(n, d_a)$ code with $\mathbf{0} \in C$. Then*

$$\binom{i}{j} A_i \leq \left( \sum_{k=d_a}^{j+d_a-1} \binom{k}{j} A_k \right) A(n-j, 2d_a, i-j)$$

*for $i = d_a + 1, \cdots, n - d_a$ and $j = 1, \cdots, i - d_a$.*

*Proof:* Since $\mathbf{0} \in C$, $\sum_{i=1}^{d_a-1} A_i = 0$. Also, from Corollary 6.3, it follows that $A_{d_a} = n/d_a$. Let $\mathbf{c}$ be a codeword of weight $i$ for $d_a + 1 \leq i \leq n - d_a$, and let $\mathbf{e} \leq \mathbf{c}$ be a possibly received word of weight $j$ for $1 \leq j \leq i - d_a$. From the assumption on $C$, it follows that the word $\mathbf{e}$ must be covered by at least one of the codewords of weight $k$ where $j \leq k \leq j + d_a - 1$.

Given the codeword $\mathbf{c}$, there are $\binom{i}{j}$ choices for the word $\mathbf{e}$. On the other hand, the number of words of weight $j$ covered by a codeword of weight $k$ equals $\binom{k}{j}$ for $k = j, \cdots, j + d_a - 1$. In $C$, there are $A_l$ codewords of weight $l$ for $l = i, j, j+1, \cdots, j + d_a - 1$, and every such a $j$-tuple $\mathbf{e}$ from $n$ coordinates can simultaneously occur in no more than $A(n-j, 2d_a, i-j)$ codewords of weight $i$. This gives us the desired estimate

$$\binom{i}{j} A_i \leq \left( \sum_{k=d_a}^{j+d_a-1} \binom{k}{j} A_k \right) A(n-j, 2d_a, i-j)$$

for $i = d_a + 1, \cdots, n - d_a$ and $j = 1, \cdots, i - d_a$. □

**Example 6.9** Take $i = d_a + 1$ and $j = 1$ in Theorem 6.13. Then

$$\begin{aligned} (d_a + 1) A_{d_a+1} &\leq d_a \times A_{d_a} \times A(n-1, 2d_a, d_a) \\ &= d_a \times \tfrac{n}{d_a} \times A(n-1, 2d_a, d_a) \\ &= nA(n-1, 2d_a, d_a) = n \left\lfloor \tfrac{n-1}{d_a} \right\rfloor, \end{aligned}$$

that is

$$A_{d_a+1} \leq \left\lfloor \frac{n}{d_a+1} \left\lfloor \frac{n-1}{d_a} \right\rfloor \right\rfloor.$$

This is the well known expression for constant weight codes.

**Corollary 6.8** *Let $C$ be a nontrivial UWP $C_a(n, 2)$ code with $\mathbf{0} \in C$. Then*

$$\binom{i}{j} A_i \leq (A_j + (j+1) A_{j+1}) A(n-j, 4, i-j)$$

*for $i = 3, \cdots, n-2$ and $j = 1, \cdots, i-2$.*

*Proof:* Apply Theorem 6.13 with $d_a = 2$. □

A similar argument as stated in the proof of Theorem 6.13 can be applied to verify the following claim (the proof is omitted here).

**Theorem 6.14** *Let $C$ be a nontrivial UWP $C_a(n, d_a)$ code with $n = qd_a+r$ $(0 < r < d_a)$. Then*

$$\binom{i}{j} A_i \leq \left( \binom{r}{j} + \sum_{k=d_a}^{j+d_a-1} \binom{k}{j} A_k \right) A(n-j, 2d_a, i-j)$$

*for $i = d_a + 1, \cdots, n - d_a$ and $j = 1, \cdots, i - d_a$.*

## 6.5 Some constructions of $UWP$ $C_a(n, 2)$ codes

In this section attention will be given to the constructions of $UWP$ $C_a(n, 2)$ codes. For later use, we need

**Theorem 6.15** *Let $C$ be a nontrivial $UWP$ $C_a(n, 2)$ code with weight distribution $A_0, A_1, \cdots, A_n$, and let $j = max\{i \mid A_i \neq 0, i = 2, \cdots, n-2\}$. Then $A_i \geq 1$ for $2 \leq i \leq j$.*

*Proof:* Evidently, the set $\{i \mid A_i \neq 0, i = 2, \cdots, n-2\}$ is not empty and $j \geq 2$. Moreover, in $A_2, A_3, \cdots, A_j$, any two consecutive numbers, $A_i$ and $A_{i+1}$ $(i = 1, \cdots, j-1)$, cannot be equal to zero simultaneously. Indeed, suppose the contrary holds, then a possibly received word of weight $i$ would exist. This word can be obtained from a codeword of weight $j$ by introducing $j - i$ $(\geq 2)$ 1-errors, and it does not belong to $\bigcup_{\mathbf{c} \in C} S_a(\mathbf{c}, 1)$. This contradicts the assumption that $C$ is a $UWP$ code.

Next, we prove that among the numbers $A_2, \cdots, A_j$, none is zero. From Theorem 6.9, it follows that $A_2 \geq 1$. Suppose there is an index $s$ with $3 \leq s \leq j-1$ such that $A_s = 0$. Then both $A_{s-1}$ and $A_{s+1}$ are not equal to zero due to the previous argument. Let $\mathbf{c}$ be a codeword of weight $s+1$. All the possibly received words that can be obtained from $\mathbf{c}$ by introducing two 1-errors make up the set $E_0 = \{\mathbf{x} \in \mathbf{V_n} \mid w(\mathbf{x}) = s-1 \ \wedge \ \mathbf{x} \leq \mathbf{c}\}$, which has cardinality $\binom{s+1}{s-1} = \binom{s+1}{2}$. Since the minimum distance of $C$ is 2, the words in $E_0$ cannot all be codewords of weight $s-1$. So at least one vector of $E_0$ will exist that is not in the set $\bigcup_{\mathbf{c} \in C} S_a(\mathbf{c}, 1)$. This is not possible. Hence, $A_i \geq 1$ for $2 \leq i \leq j$. □

**Theorem 6.16** *Let $C$ be a nontrivial $UWP$ $C_a(n, 2)$ code with even length. Then the number of codewords of weight 3 of $C$, i.e. $A_3$, is less than or equal to $(n^2 - 2n)/6$.*

*Proof:* From Theorem 2.1, it follows that $A_2 + A_3 \leq A(n+1, 2d_a, 3)$. However, it is known that $A(n+1, 2d_a, 3) \leq n(n+1)/6$ (see e.g. [5]). From Corollary 6.3 it follows that $A_2 = n/2$, and therefore, $A_3 \leq n(n+1)/6 - n/2 = (n^2 - 2n)/6$. □

It is known that $A(n+1, 2d_a, 3) \le n(n+1)/6$ with equality if and only if a Steiner system $S(2,3,n+1)$ exists (cf. [5]). When $n+1 \equiv 1 \pmod 6$ or $n+1 \equiv 3 \pmod 6$, Steiner triple systems $S(2,3,n+1)$ do exist [43]. Therefore, if $N$ is the $b \times (n+1)$ incidence matrix of a Steiner triple system $S(2,3,n+1)$ where $b$ represents the number of blocks in such a system, then deleting one of the columns of $N$ leads to an $UWP$ $C_2(n,2)$ code if the all-zero vector $\mathbf{0}$ is added. For the case $n \equiv 4 \pmod 6$, we show

**Theorem 6.17** *Let $C$ be a nontrivial $UWP$ $C_a(n,2)$ code with $n > 4$ and $n \equiv 4$ (mod 6). Then $A_3 \le (n^2 - 2n - 8)/6$.*

*Proof:* From Corollary 6.3, it follows that $\mathbf{0} \in C$ and $A_2 = n/2$. Without loss of generality, let $\{1,2\}$, $\{3,4\}$, $\{5,6\}$, $\{7,8\}$, $\cdots$, $\{n-1,n\}$ be the (supports of the) codewords of weight 2, and assume that $n = 6k+4$ $(k \ge 1)$. In [30], it was shown that the size of a maximal $(n,3)$ system is $(n^2 - 2n - 2)/6$, and for such a system, up to permutation, $3k+3$ pairs $\{1,2\}$, $\{1,3\}$, $\{1,4\}$, $\{5,6\}$, $\{7,8\}$, $\cdots$, $\{n-1,n\}$ do not occur in any triple, while every other pair appears exactly once. Hence, the triple looking like $\{3,4,a\}$ will occur once for a certain $a \in \{2,\cdots,n\}$. Deleting this triple from such a maximal $(n,3)$ system, one gets that $A_3 \le (n^2-2n-2)/6-1 = (n^2-2n-8)/6$. □

**Corollary 6.9** *Let $C$ be a nontrivial $UWP$ $C_a(n,2)$ code. If $n > 4$, $n \equiv 4$ (mod 6), and if $C$ contains the $(n^2 - 2n - 8)/6$ codewords of weight 3 described in the proof of Theorem 6.17, then no codeword of $C$ of weight $i$ $(i \ge 4)$ can cover any of the four pairs $\{1,3\}$, $\{1,4\}$, $\{3,a\}$ and $\{4,a\}$.*

**Theorem 6.18** *Let $C$ be a nontrivial $UWP$ $C_a(n,2)$ code with $n \equiv 0$ or $2$ (mod 6). If $A_3 = (n^2-2n)/6$, then $A_4 \le n(n^2-5n+6)/24$.*

*Proof:* Hanani [27] showed that Steiner quadruple systems $S(3,4,n+2)$ exist for $n+2 \equiv 2$ or $4 \pmod 6$. For such systems, the number of blocks (quadruples) equals $b = n(n+1)(n+2)/24$. Also, Theorem 2.1 shows that $A_2 + A_3 + A_4 \le A(n+2, 2d_a, 4)$. With the same argument as in Theorem 6.16 the assertion follows. □

**Remark 6.1** Theorem 6.18 also provides a construction for $UWP$ $C_a(n,2)$ codes. Using the same notation as in Theorem 6.18, let $A$ be the $b \times (n+2)$ incidence matrix of a Steiner quadruple system $S(3,4,n+2)$. Then, every column of $A$ will contain exactly $r$ ones, where $r$ equals $n(n+1)/6$. Without loss of generality, we may take the matrix $A$ such that the first $r$ rows of $A$ all start with 1 and the remaining $b-r$ rows all begin with 0. If we delete the first column of $A$, then the first $r$ rows will form the incidence matrix of a Steiner triple system $S(2,3,n+1)$ and the inner product between any two distinct columns of $A$ is equal to $n/2$. Therefore, we may further assume that $A$ looks like Figure 6.1, in which $A_{11}$ contains $n/2$ disjoint pairs and $A_{01}$ contains $(n^2-2n)/6$ triples for which every pair from the set $\{1,\cdots,m-2\}$

occurs exactly once, except for those in $A_{11}$. The number of words in $A_{00}$ equals $b-r-(n^2-2n)/6$. So $A_{00}$ yields $n(n^2-5n+6)/24$ words of weight 4. Clearly, the words in these three submatrices ($A_{11}, A_{01}$ and $A_{00}$) together with $\mathbf{0}$ form a $UWP$ $C_a(n,2)$ code of size $1+n(n^2-n+10)/24$.

| | | |
|---|---|---|
| 1 ⋮ 1 | 1 ⋮ 1 | $A_{11}$, rowweight=2 |
| 1 ⋮ 1 | 0 ⋮ 0 | $A_{10}$, rowweight=3 |
| 0 ⋮ 0 | 1 ⋮ 1 | $A_{01}$, rowweight=3 |
| 0 ⋮ 0 | 0 ⋮ 0 | $A_{00}$, rowweight=4 |

Figure 6.1: Illustration figure for Remark 6.1.

A construction of a $UWP$ $C_a(8,2)$ code of size 23. By using Theorem 6.18, we get a nontrivial $UWP$ code, denoted by $C_8$, of length 8 and size 23 that can correct a single error. The code consists of the words listed in (5.5), (5.6) and in the first column of (5.8). It is easy to compute that

$$A_3\binom{3}{2} = \binom{8}{2} - A_2 = 24$$

and

$$\binom{n}{3} - A_3 = 48 \geq A_4\binom{4}{3} = 40.$$

Therefore, there exist eight triples which do not occur in the code $C_8$. They are

$$\begin{array}{c}\{1,3,8\},\{1,4,6\},\{1,5,7\},\{2,3,5\},\\ \{2,4,7\},\{2,6,8\},\{3,6,7\},\{4,5,8\}.\end{array} \tag{6.11}$$

It can be shown that any of the words of weight 5 at distance 2 to all the codewords of $C_8$ must cover one of the triples in (6.11). This shows that none of the words of weight 5 can be added to the code $C_8$, further, none of weight greater than 5 can be added to $C_8$ either according to Theorem 6.15.

A construction of a $UWP$ $C_a(7,2)$ code of size 11. Of course, taking all the codewords starting with 1 in $C_8$ mentioned previously, and then deleting all the first coordinates, results in a $UWP$ $C_a(7,2)$ code of size 9. It can be proved that no other word can be added then. Nevertheless, a $UWP$ $C_a(7,2)$ code $C_7$ of size 11 can be obtained by using the construction method indicated in the proof of Theorem 6.10. This code is

$$C_7 = \{(\mathbf{0},1)\} \cup \{(\mathbf{c},0) | \mathbf{c} \neq \mathbf{0} \wedge \mathbf{c} \in C\}$$

where $C$ is the $UWP$ $C_a(6,2)$ code of maximum size given in Example 6.3.

A construction of a $UWP$ $C_a(10,2)$ code of size 30. Below, we will construct a nontrivial $UWP$ code of length 10 and size 30 for correcting single errors. Best [3] found that there are exactly 11 optimal non–isomorphic binary constant weight codes containing 35 words of length 11, weight 4 and minimum Hamming distance 4. These 11 non-isomorphic codes determine $35 \times 11$ matrices. In [17], it was shown that only three sets consisting of five disjoint words of weight 2, twelve words of weight 3 and twenty-three words of weight 4 can be found by deleting one column from those eleven matrices, and furthermore the three sets are all equivalent. In other words, if a $C_a(10,2)$ code satisfies $A_2 + A_3 + A_4 = 40$, then these 40 codewords are determined uniquely. Without loss of generality, they look like

$$\begin{array}{ll}
\text{weight=2:} & \{1,5\},\{2,7\},\{3,9\},\{4,8\},\{6,10\}; \\[1em]
\text{weight=3:} & \{1,4,10\},\{1,6,7\},\{1,8,9\},\{2,3,6\},\{2,5,9\},\{2,8,10\}, \\
& \{3,5,10\},\{3,7,8\},\{4,5,7\},\{4,6,9\},\{5,6,8\},\{7,9,10\}; \\[1em]
\text{weight=4:} & \underline{\{1,2,3,7\}},\underline{\{1,2,4,9\}},\underline{\{1,2,5,10\}},\underline{\{1,3,4,6\}},\underline{\{1,3,5,8\}}, \\
& \underline{\{1,3,9,10\}},\{1,4,7,8\},\{1,5,7,9\},\{1,6,8,10\},\underline{\{2,3,4,5\}}, \\
& \{2,3,8,9\},\ \underline{\{2,4,6,8\}},\underline{\{2,4,7,10\}},\{2,5,6,7\},\{2,6,9,10\}, \\
& \underline{\{3,4,7,9\}},\underline{\{3,4,8,10\}},\{3,5,6,9\},\{3,6,7,10\},\{4,5,6,10\}, \\
& \{4,5,8,9\},\{5,7,8,10\},\{6,7,8,9\}.
\end{array}$$

Since

$$A_2 + \begin{pmatrix} 3 \\ 2 \end{pmatrix} A_3 = 5 + 3 \times 12 = 41 \quad \text{and} \quad \begin{pmatrix} 10 \\ 2 \end{pmatrix} = 45,$$

only four pairs do not occur in the codewords of weight 2 and weight 3. They are $\{1,2\}$, $\{1,3\}$, $\{2,4\}$ and $\{3,4\}$. According to Corollary 6.9, the above eleven quadruples which are underlined have to be erased. Therefore, the remaining words plus the all-zero vector form a $UWP$ $C_a(10,2)$ code of size 30. We denote it by $C_{10}$.

Now, we show that $A_6 = 0$ for $C_{10}$. Assume that $A_6 \neq 0$. From Theorem 6.15 and Corollary 6.6, it follows that $A_5 \neq 0$ and $A_5 \geq \binom{6}{4} - A(6,4,4) = 15 - 3 = 12$. This results in $A_5 = 12$ because $12\binom{5}{3} = \binom{10}{3} = 120$. It implies that every triple from the set $\{1, \cdots, 10\}$ occurs exactly once in one of the codewords of weight 5, which contradicts the construction of $C_{10}$. Hence, $A_6$ must be zero. Furthermore, one can also prove that $A_5$ equals 0 for $C_{10}$ by checking all the possibilities. Therefore, from Theorem 6.15, it follows that any word of weight greater than 4 cannot be added to the code $C_{10}$.

From the binary Hamming codes, a class of nontrivial $UWP$ $C_a(n,2)$ codes can be derived. This is described by the following theorems.

**Theorem 6.19** *Let $\mathcal{H}_r$ $(r \geq 2)$ denote a binary Hamming code of length $n = 2^r - 1$, i.e., $\mathcal{H}_r$ is a $[2^r - 1, 2^r - 1 - r, 3]$ code. Let $C$ be the union of the following three types of words*

1. *The all-zero vector of length $n - 1 = 2^r - 2$;*
2. *All the words obtained by deleting the first coordinate from each of the codewords of $\mathcal{H}_r$ of weight 3;*
3. *All the words obtained by taking all the codewords of weight 4 in $\mathcal{H}_r$ which begin with 0, and then by omitting the first coordinate from each of them.*

*Then $C$ is a $UWP$ $C_a(n-1,2)$ code of cardinality $(n^3 - 4n^2 + 15n + 12)/24$.*

*Proof:* For $r = 2$ the statement is trivial. So suppose that $r \geq 3$. Let $W_i$ $(i = 0, 1, \cdots, n)$ be the coefficients of weight enumerator of $\mathcal{H}_r$. Since $2^r \equiv 2$ or $4$ $(mod\ 6)$, $2^r - 1 \equiv 1$ or $3$ $(mod\ 6)$. Thus, Steiner triple systems $S(2, 3, 2^r - 1)$ will exist for all $r \geq 3$ [43]. On the other hand, the weight distribution of $\mathcal{H}_r$ satisfies the following recurrence [49]: $W_0 = 1$, $W_1 = 0$, and

$$\binom{i+1}{i} W_{i+1} = \binom{n}{i} - W_i - (n - i + 1)W_{i-1}. \tag{6.12}$$

Therefore, $W_3$ and $W_4$ are related to each other by the following equalities

$$\binom{3}{2} W_3 = \binom{n}{2} \quad \text{and} \quad \binom{4}{3} W_4 = \binom{n}{3} - W_3.$$

They express that every pair involving $1, \cdots, n-1$ or $n$ appears exactly once in the codewords of weight 3, while, every triple from the set $\{1, \cdots, n\}$ occurs exactly once, either in a codeword of weight 3 or in a codeword of weight 4. Thus, all the codewords of weight 3 form a Steiner triple system $S(2, 3, n)$ with $W_3$ blocks, and all the codewords of weight 4 present a 2-design containing $W_4$ blocks. Let $M_1$ and $M_2$ represent the $W_3 \times n$ and $W_4 \times n$ incidence matrices of those two designs respectively. Then every column of $M_1$ contains exactly $3W_3/n = (n-1)/2$ ones, and every column of $M_4$ exactly $4W_4/n = (n-1)(n-3)/6$ ones. So the assertion follows the statements described in Remark 6.1, i.e., $C$ is a $UWP$ $C_a(n-1,2)$ code with size

$$1 + W_3 + \left(W_4 - \frac{(n-1)(n-3)}{6}\right) = \frac{n^3 - 4n^2 + 15n + 12}{24}.$$

This completes the proof. □

Let the codewords in $\mathcal{H}_r$ of weight $i$ form the $W_i \times n$ matrix $M_i$ ($3 \le i \le n-3$). Since the automorphism group of $\mathcal{H}_r$ is doubly-transitive, it follows that all the codewords of weight $i$ in a binary Hamming code, form a 2-design with $W_i$ blocks. From the point of view of Theorem 6.19, the code $C$ constructed in Example 6.3 in Section 6.1 is just a simple example of Theorem 6.19 using the binary [7,4,3] Hamming code. For the $UWP$ code established in Theorem 6.19, we naturally want to know whether any other words can be added to it in order to enlarge its size. The next theorem will provide the answer to that question. Due to Example 6.3, the proof only needs to be given for the case $r \ge 4$.

**Theorem 6.20** *Let the hypotheses of Theorem 6.19 apply. If $n = 15$ (i.e. $r = 4$), then no word of weight greater than 4 can be added to $C$. If $n \ge 31$ (viz. $r \ge 5$), then the number of words of weight 5 that can be added to $C$, while keeping the enlarged code uniformly weakly perfect, is equal to $(n-1)(n-3)(n-7)(n-15)/120$.*

*Proof:* Let $W_i$ ($i = 0, \cdots, n$) be defined as before. Since there are exactly $(n-1)/2$ codewords of weight 3 which start with 1 and since they come from a Steiner triple system $S(2,3,n)$, without loss of generality, those words may look as follows:

$$\{1,2,3\}, \{1,4,5\}, \cdots, \{1, n-1, n\}. \tag{6.13}$$

On the other hand, by (6.12) the number of the codewords in $\mathcal{H}_r$ of weight 4 starting with 1 equals $r_4 = (n-1)(n-3)/6$, and the number of the codewords of weight 5 starting with 1 is $r_5 = 5W_5/n = (n-1)(n-3)(n-7)/24$. The construction of $C$ implies that it contains $W_4 - r_4 = (n-1)(n-3)(n-4)/24$ words originating from the codewords of $\mathcal{H}_r$ of weight 4 starting with 0 by deleting the first coordinates. Also, $W_5 - r_5 = (n-1)(n-3)(n-5)(n-7)/(5 \times 24)$ gives the number of the codewords of weight 5 beginning with 0 in $\mathcal{H}_r$. These are the words that have to be checked to see if some of them can be added to $C$ or not after erasing the first coordinate from each.

Let $\mathbf{c}$ be a codeword of $\mathcal{H}_r$ of weight 4 beginning with 1. Since $\mathcal{H}_r$ is a linear code with minimum Hamming distance 3, $(n-7)/2$ codewords of weight 5 starting with 0 can be obtained by adding $\mathbf{c}$ to each of the $(n-1)/2$ codewords of weight 3 in (6.13). In other words, every codeword of weight 4 starting with 1 corresponds to exactly $(n-7)/2$ codewords of weight 5 starting with 0. This leads to

$$\begin{aligned} W_5 - r_5 &= (n-1)(n-3)(n-5)(n-7)/(5 \times 24) \\ &\geq r_4(n-7)/2 = (n-1)(n-3)(n-7)/12. \end{aligned}$$

Subtracting the right-hand side from the left-hand side in the above inequality results in the difference

$$D = \frac{(n-1)(n-3)(n-7)(n-15)}{120} \geq 0. \tag{6.14}$$

When $n = 15$ $(r = 4)$, one gets $D = 0$, which shows that no other words of weight 5 can be added to $C$. Therefore, in this case, the size of code $C$ cannot be enlarged anymore according to Theorem 6.15. However, when $n \geq 31$ (i.e. $r \geq 5$), $D$ is a positive integer, and these $D$ codewords of weight 5 satisfy the property that each triple occurring in them can be covered by exactly one of the codewords of weight 4 in $C$. That is to say, if we add those $D$ words to $C$, then any possibly received word of weight 3 obtained from them by introducing two 1-errors will be covered exactly by one of the codewords of $C$ of weight 4. This completes the proof. □

**Remark 6.2** The results stated in Theorem 6.20 can also be interpreted geometrically. Since all the nonzero points in a projective geometry $PG(r-1,2)$ form the columns of the parity check matrix of the Hamming code $\mathcal{H}_r$, each line in $PG(r-1,2)$ corresponds to precisely one codeword of $\mathcal{H}_r$ of weight 3. Let $\Omega = \{1, 2, \cdots, 2^r - 1\}$ be the non-zero point set of $PG(r-1,2)$. Each point corresponds to a binary vector of length $r$. Without loss of generality, we may regard $\Omega$ as the parity check matrix of $\mathcal{H}_r$ in the same order. Let $Q = \{p_1, p_2, p_3, p_4, p_5\}$ be a subset of $\Omega$ for which $p_i \neq 1$ $(i = 1, \cdots, 5)$ and $\sum_{i=1}^{5} p_i = \mathbf{0}$. Apparently, $Q$ corresponds to a codeword of $\mathcal{H}_r$ of weight 5 starting with 0. Suppose that there are two points $p_s$ and $p_t$ in $Q$ such that $p_s + p_t = 1$. Then the remaining three points (or a triple) of $Q$ must be covered by a codeword of $\mathcal{H}_r$ of weight 4 starting with 1. Hence, finding the number of codewords of weight 5 which can be added in the code $C$ in Theorem 6.19 is equivalent to finding the number of five-point sets as $Q$ such that any line through a pair of points of $Q$ does not pass through the point 1. The solution to this problem can be found in the next theorem, the proof of which is given at the end of this section.

**Theorem 6.21** *Let $\mathcal{P}$ be a $PG(r-1,2)$ with nonzero point set $\Omega = \{1, 2, \cdots, 2^r - 1\}$ (each point can be regarded as a binary vector of length $r$) and $r \geq 4$. Also let $Q = \{p_1, p_2, p_3, p_4, p_5\} \subseteq \Omega$ with the properties:*

1. *$p_i \neq p_j$ for $i \neq j$ and $i, j = 1, \cdots, 5$;*

2. *$p_i \neq 1$ for $i = 1, \cdots, 5$;*

*3.* $\sum_{i=1}^{5} p_i = \mathbf{0}$ *(when the five points are represented by binary vectors of length r);*

*4. Any line through two distinct points from Q does not pass through the point 1.*

*Then the number of five-point sets defined above as Q equals*

$$\frac{(2^r-16)(2^r-2)(2^r-4)(2^r-8)}{(2^4-1)(2^4-2)(2^4-4)(2^4-8)}168. \tag{6.15}$$

*This number is equal to the number D in (6.14).*

Finding words of weight 6 which can be added to $C$ defined in Theorem 6.19 becomes more difficult. Here we just give an upper bound on the number of such words.

**Theorem 6.22** *Let the hypotheses of Theorem 6.19 apply. Also, let $C$ contain $D$ codewords of weight 5 as defined in (6.14). Then the number of words of weight 6, indicated by $D'$, which can be added to $C$ while keeping $C$ uniformly weakly perfect, is bounded by*

$$D' \le \lfloor (n-4)/2 \rfloor D/15.$$

*Proof:* From Theorems 6.15 and 6.19, it follows that $D'$ must be zero when $n = 15$. For $n \ge 31$, we only need to consider the codewords of $\mathcal{H}_r$ of weight 6 beginning with 0. Since the number of codewords of $\mathcal{H}_r$ of weight 6 starting with 1 equals $r_6 = (6W_6)/n$, the number of codewords of $\mathcal{H}_r$ of weight 6 starting with 0 is $W_6 - r_6$. Let $F$ consist of those $W_6 - r_6$ words, and let $\mathbf{a}$ be a word of $F$ that can be added to $C$ while keeping $C$ uniformly weakly perfect. Then, any quadruple obtained from $\mathbf{a}$ by introducing 2 1-errors cannot be a codeword of $C$ of weight 4, since the code $\mathcal{H}_r$ has the minimum Hamming distance 3. Therefore, such quadruple must be covered by exactly one of the codewords of $C$ of weight 5. The number of quadruples chosen from a word of $F$ is $\binom{6}{4} = 15$. In addition, each quadruple can simultaneously occur in no more than $A(n-4,4,2) = \lfloor (n-4)/2 \rfloor$ words of $F$. This gives us the following estimate

$$\binom{6}{4} D' \le D \times \lfloor (n-4)/2 \rfloor.$$

Hence, the statement follows. □

Table 6.1 shows the sizes of the nontrivial $UWP$ $C_a(n,2)$ codes which are constructed in this chapter with length $n$ in the region $1 \le n \le 15$. The entries are marked as follows:

a) Examples 6.3 and 6.4 shown in Section 6.1.

b) Code being able to be constructed by using Theorem 6.10.

c) Code being able to be constructed by using Theorem 6.18;

d) Code obtained by taking $r = 4$ in Theorem 6.19.

e) Code constructed in Section 6.5.

f) Trivial.

| $n$ | $U_a(n,2)$ | $n$ | $U_a(n,2)$ |
|---|---|---|---|
| 2 | $2^f$ | 9 | $23^b$ |
| 3 | $2^f$ | 10 | $30^e$ |
| 4 | $3^f$ | 11 | $30^b$ |
| 5 | $5^a$ | 12 | $72^c$ |
| 6 | $11^a$ | 13 | $72^b$ |
| 7 | $11^b$ | 14 | $113^d$ |
| 8 | $23^e$ | 15 | $113^b$ |

Table 6.1: Lower bounds on $U_a(n,2)$ for $1 \le n \le 15$.

*The proof of Theorem 6.21.* It will be presented in three steps corresponding to the cases $r = 4$, $r = 5$ and $r \ge 6$.

(a) If $r = 4$, then $\mathcal{P}$ is a projective geometry $PG(3,2)$ with as point set the binary expressions of the elements of $\Omega = \{1, \cdots, 15\}$. Without loss of generality, we may regard $\Omega$ as the parity check matrix of $\mathcal{H}_4$ in the same order. Suppose that $B$ is a five-point set which satisfies the conditions 1), 2) and 3) of the set $Q$ defined in Theorem 6.21. Clearly, $B$ corresponds to a codeword of $\mathcal{H}_4$ of weight 5 starting with 0. It is obvious that any three points of $B$ cannot be on one line, otherwise the remaining two points of $B$ would be the same, which is not possible. Hence, the five points of $B$ determine ten different lines in $\mathcal{P}$. Each of these lines must pass through exactly one of the points of the set $\overline{B} = \Omega \backslash B$. However, no pair of these lines has a point of $\overline{B}$ in common since none of points in $B$ is zero. That is to say, there must be two points of $B$ which, when joined, form a line incident with the point 1. Thus, the number of five-point sets defined as $Q$ equals zero. So the assertion is true for the case $r = 4$.

(b) If $r = 5$, then $\mathcal{P}$ is a projective geometry $PG(4,2)$ with 31 nonzero points. So $\mathcal{P}$ has 31 different hyperplanes which are all $PG(3,2)$. Each hyperplane contains 15 nonzero points. Each nonzero point of $\mathcal{P}$ must be contained in exactly 15 hyperplanes. Specifically, the point 1 is contained in 15 hyperplanes. As observed in case (a) previously, in those 15 hyperplanes containing the point 1, no such a five-point set $Q$ as defined in the theorem exists. Therefore, we only need to consider the remaining $(31 - 15) =$

16 hyperplanes which don't include the point 1. Since in a hyperplane $PG(3,2)$, there are 168 different five-point sets which satisfy the condition 1) and 3) in the theorem (using (6.12)), the number of five-point sets as $Q$ is equal to $16 \times 168$ which is in accordance with (6.15).

(c) When $r \geq 6$, the number of $PG(3,2)$'s contained in $PG(r-1,2)$ (see Appendix $B$ of [36]) is

$$X = \frac{(2^r-1)(2^r-2)(2^r-4)(2^r-8)}{(2^4-1)(2^4-2)(2^4-4)(2^4-8)}.$$

Let $\mathcal{A}$ be a hyperplane $PG(r-2,2)$ which does not contain the point 1, and let $\mathcal{B}$ be a $PG(3,2)$ which contains the point 1. We want to show that the intersection of $\mathcal{A}$ and $\mathcal{B}$ is a projective plane of order 2, i.e., $PG(2,2)$. Since

$$dim(\mathcal{A}) + dim(\mathcal{B}) = dim(\mathcal{A}+\mathcal{B}) + dim(\mathcal{A}\cap\mathcal{B})$$

and since the whole space $PG(r-1,2)$ has dimension $r$, we find that

$$\begin{aligned} 4 &= dim(\mathcal{B}) \geq dim(\mathcal{A}\cap\mathcal{B}) = dim(\mathcal{A}) + dim(\mathcal{B}) - dim(\mathcal{A}+\mathcal{B}) \\ &= r-1+4-dim(\mathcal{A}+\mathcal{B}) \geq r-1+4-r = 3. \end{aligned}$$

If $dim(\mathcal{A}\cap\mathcal{B}) = 4$, then $\mathcal{B} \subseteq \mathcal{A}$. This contradicts the assumptions of $\mathcal{A}$ and $\mathcal{B}$. Hence, $dim(\mathcal{A}\cap\mathcal{B}) = 3$. Thus, $\mathcal{A}\cap\mathcal{B}$ is a $PG(2,2)$. In $PG(r-1,2)$, the number of $PG(3,2)$'s containing the point 1 is equal to the number of $PG(2,2)$'s in a hyperplane $PG(r-2,2)$ which does not contain the point 1. The later number equals

$$Y = \frac{(2^{r-1}-1)(2^{r-1}-2)(2^{r-1}-4)}{(2^3-1)(2^3-2)(2^3-4)}.$$

Therefore, the number of five-point sets as defined in the theorem is

$$168(X-Y) = 168\frac{(2^r-16)(2^r-2)(2^r-4)(2^r-8)}{(2^4-1)(2^4-2)(2^4-4)(2^4-8)}$$

which equals the number $D$ in (6.14) after replacing $2^r-1$ with $n$.

# Bibliography


[1] Anderson, D. A.: *Design of self-checking digital networks using coding techniques,* Univ. of Illinois, Urbana, CSL Rep. R-527, Oct. 1971.

[2] Anderson, D. A., Metze. G.: *Design of totally self-checking check circuits for m-out-of-n codes,* IEEE Trans. Comput., C-**22**, 263-269, March 1973.

[3] Best, M. R.: $A(11,4,4) = 35$ *or some new optimal constant weight codes,* ZN 71/77 February, CWI report, Amsterdam.

[4] Bose, B., Rao, T. R. N.: *Theory of unidirectional error correcting/detecting codes,* IEEE Trans. Comput., C-**31**, 521-530, June 1982.

[5] Brouwer, A. E., Shearer, J. B., Sloane, N. J. A., Smith, W. D.: *A new table of constant weight codes,* IEEE Trans. Inform. Theory, IT-**36**, 1334-1380, November 1990.

[6] Brouwer, A. E.: *Private communication.*

[7] Bussemaker, F. C., Mathon, R. A., Seidel, J. J.: *Tables of two-graphs,* T.H.-Report 79-WSK-05, Eindhoven University of Technology, October 1979.

[8] Cohen, L., Green, R., Smith, K., Seely, J. L.: *Single-transistor cell makes room for more memory on an MOS chip,* Electronics **44** (1971): 69-75.

[9] Constantin, S. D., Rao, T. R. N.: *On the theory of binary asymmetric error correcting codes,* Information and Contr. **40**, 20-36, 1979.

[10] Cook, R. W., Sisson, W. H., Storey, T. F., Toy, W. N.: *Design of self-checking microprogram control,* IEEE Trans. Comput., C-**22**, 255-262, March 1973.

[11] Cricchi, J. R., Blake, F. C., Fitzpatrick, M. D.: *The brain source protected MNOS memory endurance,* IEEE International Electron Services Meeting, Washington, D.C. 1973, sects. 3-5.

[12] Delsarte, P., Piret, P.: *Bounds and constructions for binary asymmetric error-correcting codes,* IEEE Trans. Inf. Theory, IT-**27**, 125-128, Jan. 1981; correction, **36**(4), 954, July 1990.

[13] Driessen, L. H. M. E.: *t-DESIGNS,* $t \geq 3$. Master thesis, Dept. of Math. and Compt. Sci., Eindhoven University of Technology, The Netherlands, April 1978.

[14] Etzion, T.: *New lower bounds for asymmetric and unidirectional codes,* IEEE Trans. Inform. Theory, **37**, 1696-1704, Nov.1991.

[15] Etzion, T.: Private communication.

[16] Fang, G., Van Tilborg, H. C. A.: *Some new results on binary asymmetric error-correcting codes,* Proc. of IEEE Inter. Symposium on Infor. Theory, Budapest, Hungary, p.143, June 1991.

[17] —: *New tables of AsEC and UEC codes,* Report 91-WSK-02, Eindhoven University of Technology, The Netherlands, August 1991.

[18] —: *Bounds and Constructions of Asymmetric or Unidirectional Error-Correcting Codes,* Applicable Algebra in Engineering, Communication and Computing, **3**(4), 269-300, Dec. 1992.

[19] Fang, G., Van Tilborg, H. C. A., Sun, F. W.: *Weakly perfect binary block codes for correcting asymmetric errors,* Proc. of Inter. Symposium on Communications, Tainan, Taiwan, 57-60, Dec. 1991.

[20] —: *On uniformly weakly perfect codes for correcting asymmetric errors; Some bounds and constructions,* to appear in The Collection of Papers Dedicated to the Memory of David Gevorkian, Armenia.

[21] Fang, G., Van Tilborg, H. C. A., Sun, F. W., Honkala, I. S.: *Some Features of Binary Block Codes for Correcting Asymmetric Errors,* to appear in Lecture Notes in Computer Science Series of Springer Verlag, Proceedings of AAECC 10, May 1993.

[22] Fang, G., Honkala, I. S.: *On Perfectness of Binary Block Codes for Correcting Asymmetric Errors,* Submitted to Ars Combinatoria.

[23] Fort Jr, M. K., Hedlund, G. A.: *Minimal coverings of pairs by triples,* Pacific J. Math., **8**, 709-719, 1958.

[24] Goldbaum, I. Y.: *Estimate for the number of signals in codes correcting nonsymmetric errors,* (in Russian), Automat. Telemekh., **32**, 94-97, 1971 (English translation: Automat. Rem. Control, **32**, 1783-1785, 1971).

[25] Hall Jr., M.: *Combinatorial Theory*, New York: John Wiley, 1986.

[26] Hamming, R. W.: *Error Detecting and Error Correcting Codes,* Bell System Technical Journal, **29**, 147-160, 1950.

[27] Hanani, H.: *On quadruple systems,* Canad. J. Math., **12**, 145-157, 1960.

[28] Honkala, I. S.: *Some lower bounds for constant weight codes*, Discrete Appl. Math., **18**, 95-98, 1987.

[29] —: Private communication.

[30] Kalbleisch, J. G., Stanton, R. G.: *Maximal and minimal coverings of $(k-1)$-tuples by $k$-tuples,* Pacific J. Math., **26**, 131-140, 1968.

[31] Kim, W. H., Freiman, C. V.: *Single error correcting codes for asymmetric channels,* IRE Tran. Information Theory IT-**5**, 62-66, June 1959.

[32] Kirkman, T. P.: *On a problem in combinations,* Cambridge and Dublin Math. J., **2**, 191-204, 1847.

[33] Kløve, T.: *Upper bounds on codes correcting asymmetric errors,* IEEE Trans. Inform. Theory, IT-**27**, 128-131, Jan. 1981

[34] —: *Error correcting codes for the asymmetric channel,* Rep. 18-09-07-81, Dept. Mathematics, University of Bergen, Norway, July 1981.

[35] Lin, S., Costello Jr., D. J.: *Error control coding: fundamentals and applications*, Englewood Cliffs, NJ: Prentice-Hall, 1983.

[36] Macwilliams, F. J., Sloane, N. J. A.: *The Theory of Error-Correcting Codes,* Amsterdam: North-Holland, 1979.

[37] McEliece, R. J.: *A comment on 'A class of codes for asymmetric channels and a problem from the additive theory of numbers'*, IEEE Trans. Infor. Theory, IT-**19**(1), p. 137, Jan. 1973.

[38] McEliece, R. J., Rodemich, E. R.: *The Constantin-Rao construction for binary asymmetric error-correcting codes,* Information and Contr. **44**, 187-196, 1980.

[39] Parhami, B., Avizienis, A.: Detection of storage errors in mass memories using low-cost arithmetic error codes, IEEE Trans. Comput., C-**27**(4), 302-308, April 1978.

[40] Pradhan, D. K.: *A new class of error-correcting / detecting codes for fault-tolerant computer application,* IEEE Trans. Comput., C-**29**, 471-481, June 1980.

[41] Rao, T. R. N., Chawla, A. S.: *Asymmetric error codes for some LSI semiconductor memories,* In Proc. Annu. Southeastern Symp. on Syst. Theory, 170-171, Mar. 1975.

[42] Rao, T. R. N., Fujiwara, E.: *Error-control coding for computer systems.* Prentice Hall Series in Computer Engineering, Prentice Hall, 1989.

[43] Reiss, M.: *Uber eine Steinersche Combinatorische Aufgabe welche im 45sten Bande dieses Journals, Seite 181, estellt worden ist,* Crelle's Journal, **56**, 326-344, 1859.

[44] Sahni, R. W.: *Reliability of integration circuits,* Proc. of IEEE Inter. Computer Group Conf., 213-219, Washington, D.C., June 1970.

[45] Saitoh, Y., Yamaguchi, K., Imai, H.: *Some new binary codes correcting asymmetric / unidirectional errors,* IEEE Trans. Inform. Theory, IT-**36**, 645-647, May 1990.

[46] Shannon, C. E.: *A Mathematical Theory of Communication,* Bell System Technical Journal, **27**, 379-423, 623-656, 1948. Reprinted in *The Mathematical Theory of Communication,* by C. E. Shannon and W. Weaver, University of Illinois Press, Urbana, 1949.

[47] Sloane, N. J. A., Seidel, J. J.: *A new family of nonlinear codes obtained from conference matrices,* Ann. NY Acad. Sci., **175** Article 1, 363-365, 1970.

[48] Van Lint, J. H.: *A Survey of Perfect Codes,* Rocky Mountain J. Math., **5**, 199-224, 1975.

[49] —: *Introduction to Coding Theory.* Graduate Texts in Mathematics, **86**, New York: Springer-verlag, 1982.

[50] Van Lint, J. H., Weber, J, H.: *Some combinatorial codes for the binary asymmetric channel,* preprint.

[51] Varshamov. R. R.: *Estimate of the number of signals in codes with correction of nonsymmetric errors,* (in Russian), Automat. Telemekh., **25**, 1628-1629, 1964 (English translation: Automat. Rem. Control, **25**, 1468-1469, 1964).

[52] —: *Some features of linear codes that correct asymmetric errors* (in Russian), Doklady Akad. Nauk. SSSR, **157**(3), 546-548, July 1964 (English translation: Soviet Physics-Doklady, **9**, 538-540, Jan. 1965).

[53] —: *On the theory of asymmetric codes* (in Russian), Doklady Akad. Nauk. SSSR, **164**(4), 757-760, Oct. 1965 (English translation: Soviet Physics-Doklady **10**, 901-903, April 1966).

[54] ——: *A class of codes for asymmetric channels and a problem from the additive theory of numbers*, IEEE Tran. Infor. Theory, IT-**19**(1), 92-95, Jan. 1973.

[55] Varshamov, R. R., Tenengol'ts, G. M.: *Correction code for single asymmetric errors*, Avtomatika Telemekhanika, **26**(2), 288-292, Feb. 1965.

[56] Weber, J. H.: *Private communication.*

[57] ——: *Bounds and constructions for binary block codes correcting asymmetric or unidirectional errors*, the Ph. D. dissertation, Dept. of Electrical Engineering of Delft University of Technology, The Netherlands, 1989.

[58] Weber, J. H., de Vroedt, C., Boekee, D. E.: *New upper bounds on the size of codes correcting asymmetric errors*, IEEE Trans. Inform. Theory, IT-**33**, 434-437, May 1987.

[59] ——: *Bounds and constructions for binary codes of length less than 24 and asymmetric distance less than 6*, IEEE Trans. Inform. Theory, IT-**34**, 1321-1331, September 1988.

[60] ——: *Bounds and constructions for codes correcting unidirectional errors*, IEEE Trans. Inform. Theory, IT-**35**, 797-810, July 1989.

# Appendix A

# Tables of bounds on $A_a(n,d)$ and $A_u(n,d)$

Five tables are presented in this appendix. Tables A.1, A.2 and A.4 give the previously known lower and upper bounds on maximum sizes of asymmetric/unidirectional error-correcting codes for length $\leq 23$ and error correcting capability $\leq 4$. They are summarized here for the sake of completeness. Tables A.3 and A.5 extend Tables A.1, A.2 and A.4 to code lengths up to 27 and error correcting capabilities up to 8, making use of the results obtained in Chapters 3 and 4. All the lower bounds are constructive. All bounds, except the upper bounds in Table A.3, have been indexed by letters, explained below. All the bounds which can be derived from Theorems 2.4, 2.5 or 2.6 are presented without index. All the upper bounds in Table A.3 follow from the results shown in Chapter 3. They are new and unmarked. Since $A_h(n,3) = A_u(n,3)$ for $n \geq 1$, the bounds on $A_u(n,3)$ have not been included here, but they can be found in [36] and [5].

Lower bounds:

- a: Codes mentioned or obtained by Weber et al. [59] and [60].
- b: Codes obtained by Saitoh et al. [45].
- c: Codes obtained by Etzion [14].
- e: Codes obtained by Delsarte and Piret [12].
- f: Codes obtained in Section 3.1.
- g: Codes obtained in Section 3.2.
- h: Codes obtained in Section 3.3.
- i: Codes obtained in Section 3.4.
- j: Codes obtained in Chapter 4.
- v: Codes obtained by Honkala [29].

z: Codes obtained by Etzion [15].

<u>Upper bounds:</u>

k: $A_h(n, 2t+1) \leq A_u(n, 2t+1) \leq A_a(n, t+1)$ for $1 \leq t \leq n$. (see (1.2) in Section 1.2). For example, from Table II of [5], we can find $4096 \leq A_h(23, 7)$. So $4096 \leq A_a(23, 4)$ ($t$=3). Also, from Table A.3 of this dissertation, we can find $A_a(18, 6) = 12$, this leads to $A_u(18, 11) \leq 12$ ($t$=5).

l: Section 3.5.

m: Van Lint et al. [50].

p: Weber et al. [58], [59] or [60], by asymmetric/unidirectional integer linear programming and combinatorial arguments.

q: Delsarte and Piret [12], by integer linear programming.

r: from Section 3.4.

s: from Chapter 4.

| $n$ | $d = 2$ | $d = 3$ |
|---|---|---|
| 4 | 4 | 2 |
| 5 | $^{a}6^{q}$ | 2 |
| 6 | $^{a}12^{q}$ | 4 |
| 7 | $^{e}18^{q}$ | 4 |
| 8 | $^{e}36^{q}$ | $^{e}7^{q}$ |
| 9 | $^{e}62^{p}$ | $^{e}12^{q}$ |
| 10 | $^{z}111 - 115^{l}$ | $^{e}18^{q}$ |
| 11 | $^{c}180 - 210^{q}$ | $^{e}30 - 32^{q}$ |
| 12 | $^{c}336 - 410^{q}$ | $^{a}54 - 63^{q}$ |
| 13 | $^{c}652 - 786^{q}$ | $^{e}98 - 114^{q}$ |
| 14 | $^{c}1228 - 1500^{q}$ | $^{e}186 - 218^{q}$ |
| 15 | $^{c}2240 - 2828^{q}$ | $^{a}266 - 398^{q}$ |
| 16 | $^{c}4280 - 5430^{p}$ | $^{c}386 - 739^{p}$ |
| 17 | $^{c}8280 - 10374^{p}$ | $^{c}738 - 1279^{q}$ |
| 18 | $^{c}15762 - 19898^{p}$ | $^{c}1347 - 2380^{p}$ |
| 19 | $^{c}29236 - 38008^{p}$ | $^{c}2404 - 4242^{p}$ |
| 20 | $^{c}56144 - 73174^{p}$ | $^{c}3650 - 8069^{p}$ |
| 21 | $^{c}107212 - 140798^{p}$ | $^{c}5834 - 14374^{p}$ |
| 22 | $^{c}198336 - 271953^{p}$ | $^{c}8616 - 26679^{p}$ |
| 23 | $^{c}353512 - 523586^{p}$ | $^{c}16450 - 50200^{p}$ |

Table A.1: Bounds on $A_a(n, d)$ for $4 \leq n \leq 23$ and $d = 2, 3$.

| $n$ | $d=4$ | $d=5$ |
|---|---|---|
| 4 | 2 | 1 |
| 5 | 2 | 2 |
| 6 | 2 | 2 |
| 7 | 2 | 2 |
| 8 | 4 | 2 |
| 9 | 4 | 2 |
| 10 | $^{a}6^{q}$ | 4 |
| 11 | $^{a}8^{q}$ | 4 |
| 12 | $^{e}12^{q}$ | $^{a}4^{q}$ |
| 13 | $^{a}18^{q}$ | $^{a}6^{q}$ |
| 14 | $^{a}30-32^{m}$ | $^{a}8^{q}$ |
| 15 | $^{a}44-50^{p}$ | $^{a}12^{q}$ |
| 16 | $^{c}72-90^{p}$ | $^{a}16^{p}$ |
| 17 | $^{c}130-168^{p}$ | $^{a}26^{p}$ |
| 18 | $^{c}238-320^{p}$ | $^{i}40-44^{p}$ |
| 19 | $^{c}458-616^{p}$ | $^{c}54-74^{p}$ |
| 20 | $^{a}860-1144^{p}$ | $^{c}71-128^{r}$ |
| 21 | $^{a}1628-2134^{p}$ | $^{i}104-228^{r}$ |
| 22 | $^{a}3072-4116^{p}$ | $^{i}163-423^{p}$ |
| 23 | $^{k}4096-7346^{p}$ | $^{i}243-754^{p}$ |

Table A.2: Bounds on $A_a(n,d)$ for $4 \le n \le 23$ and $d = 4, 5$.

| $n$ | $d=6$ | $d=7$ | $d=8$ | $d=9$ |
|---|---|---|---|---|
| 8 | 2 | 2 | 2 | 1 |
| 9 | 2 | 2 | 2 | 2 |
| 10 | 2 | 2 | 2 | 2 |
| 11 | 2 | 2 | 2 | 2 |
| 12 | 4 | 2 | 2 | 2 |
| 13 | 4 | 2 | 2 | 2 |
| 14 | [b,f]4 | 4 | 2 | 2 |
| 15 | [b,f]6 | 4 | 2 | 2 |
| 16 | [b,f]7 | [b,g]4 | 4 | 2 |
| 17 | [b,f]8 | [b,g]4 | [h]4 | 2 |
| 18 | [b,f]12 | [b,g]6 | [h]4 | 4 |
| 19 | [f]16 | [b,g]7 | [h]4 | [h]4 |
| 20 | [f]22-23 | [b,g]9 | [h]6 | [h]4 |
| 21 | [f]32-34 | [b,g]12 | [h]6 | [h]4 |
| 22 | [f]48-60 | [b,g]14 | [h]8 | [h]4 |
| 23 | [f]66-110 | [b]19-20 | [v]9 | [h]6 |
| 24 | [f]91-210 | [g]27-30 | [h]12 | [h]7 |
| 25 | [f]124-380 | [g]40-46 | [h]13-14 | [h]8 |
| 26 | [f]173-721 | [g]58-80 | [h]18-19 | [h]9 |
| 27 | [f]249-1350 | [g]80-144 | [h]23-26 | [h]12 |

Table A.3: Bounds on $A_a(n,d)$ for $8 \leq n \leq 27$ and $6 \leq d \leq 9$.

| $n$ | $d=5$ | $d=7$ | $d=9$ |
|---|---|---|---|
| 4 | 2 | 1 | 1 |
| 5 | 2 | 2 | 1 |
| 6 | 2 | 2 | 2 |
| 7 | $^{a}4^{p}$ | 2 | 2 |
| 8 | $^{a}6^{p}$ | $^{a}4^{p}$ | 2 |
| 9 | $^{a}10^{p}$ | $^{a}4^{p}$ | 2 |
| 10 | $^{a}16-18^{k}$ | $^{a}4^{p}$ | 2 |
| 11 | $^{a}26-32^{k}$ | $^{a}7^{p}$ | $^{a}4^{p}$ |
| 12 | $^{a}52-61^{p}$ | $^{a}10^{p}$ | $^{a}4^{k}$ |
| 13 | $^{a}92-114^{k}$ | $^{c}16-18^{k}$ | $^{a}6^{k}$ |
| 14 | $^{a}184-218^{k}$ | $^{b}24-32^{k}$ | $^{a}8^{k}$ |
| 15 | $^{a}256-340^{p}$ | $^{b}42-50^{k}$ | $^{a}10-12^{k}$ |
| 16 | $^{c}384-680^{p}$ | $^{b}62-90^{k}$ | $^{c}14-16^{k}$ |
| 17 | $^{c}736-1277^{p}$ | $^{c}114-168^{k}$ | $^{c}24-26^{k}$ |
| 18 | $^{c}1344-2374^{p}$ | $^{c}201-320^{k}$ | $^{c}37-44^{k}$ |
| 19 | $^{c}2080-4096^{p}$ | $^{a}376-616^{k}$ | $^{c}51-74^{k}$ |
| 20 | $^{c}3423-6942^{p}$ | $^{a}737-1142^{p}$ | $^{c}69-133^{k}$ |
| 21 | $^{c}4672-13774^{p}$ | $^{a}1474-2134^{k}$ | $^{c}102-229^{k}$ |
| 22 | $^{c}8544-24106^{p}$ | $^{a}2588-4114^{p}$ | $^{c}154-423^{k}$ |
| 23 | $^{k}16384-48212^{p}$ | $^{k}4096-7346^{k}$ | $^{c}229-745^{k}$ |

Table A.4: Bounds on $A_u(n,d)$ for $4 \leq n \leq 23$ and $d = 5, 7, 9$.

| $n$ | $d=11$ | $d=13$ | $d=15$ | $d=17$ |
|---|---|---|---|---|
| 8 | 2 | 2 | 1 | 1 |
| 9 | 2 | 2 | 2 | 1 |
| 10 | 2 | 2 | 2 | 2 |
| 11 | 2 | 2 | 2 | 2 |
| 12 | 2 | 2 | 2 | 2 |
| 13 | ${}^{j}4^{k}$ | 2 | 2 | 2 |
| 14 | ${}^{b,j}4^{k}$ | 2 | 2 | 2 |
| 15 | ${}^{b,j}4^{s}$ | 4 | 2 | 2 |
| 16 | ${}^{j}6^{s}$ | ${}^{b,j}4^{k}$ | 2 | 2 |
| 17 | ${}^{j}8^{k}$ | ${}^{b,j}4^{k}$ | ${}^{j}4^{k}$ | 2 |
| 18 | ${}^{b,j}10-12^{k}$ | ${}^{j}6^{k}$ | ${}^{j}4^{k}$ | 2 |
| 19 | ${}^{j}14-16^{k}$ | ${}^{j}7^{k}$ | ${}^{j}4^{k}$ | ${}^{j}4^{k}$ |
| 20 | ${}^{j}22-23^{k}$ | ${}^{j}9^{k}$ | ${}^{j}5^{s}$ | ${}^{j}4^{k}$ |
| 21 | ${}^{j}30-34^{k}$ | ${}^{j}10-12^{k}$ | ${}^{j}6^{k}$ | ${}^{j}4^{k}$ |
| 22 | ${}^{j}46-60^{k}$ | ${}^{j}13-14^{k}$ | ${}^{j}7^{s}$ | ${}^{j}4^{k}$ |
| 23 | ${}^{j}63-110^{k}$ | ${}^{j}19-20^{k}$ | ${}^{j}9^{k}$ | ${}^{j}6^{k}$ |
| 24 | ${}^{j}86-210^{k}$ | ${}^{j}27-30^{k}$ | ${}^{j}10-12^{k}$ | ${}^{j}6^{s}$ |
| 25 | ${}^{j}119-380^{k}$ | ${}^{j}39-46^{k}$ | ${}^{j}13-14^{k}$ | ${}^{j}8^{k}$ |
| 26 | ${}^{j}167-721^{k}$ | ${}^{j}58-80^{k}$ | ${}^{j}18-19^{k}$ | ${}^{j}9^{k}$ |
| 27 | ${}^{j}239-1350^{k}$ | ${}^{j}80-144^{k}$ | ${}^{j}23-26^{k}$ | ${}^{j}10-12^{k}$ |

Table A.5: Bounds on $A_u(n,d)$ for $8 \leq n \leq 27$ and $d = 11, 13, 15, 17$.

# Appendix B

# Some codes mentioned in Chapters 3 and 4

## B.1 Codes mentioned in Section 3.1

$C_{19}$ consists of the following codewords:

00000, 7E000, 01F80, 4107C, 30C63, 0C31B, 2AAD4, 165AC, 79D18, 75287, 6E762, 1B0FB, 64CFD, 5FBCC, 33F37, 7FFFF.

The 39 other codewords for $C_{24}$:

773FEB, B9DDF7, 5DEB5F, AEF3BB, C7F4DD, DBFF21, DC1EBF, E35B7E, FAA5EE, 7D753A, 7FA2B5, BDB9C9, BF6E46, C5AFF2, 28FEFC, 33CF9B, 0F976F, 1679F7, 06F460, 1187A4, 124B58, 2C00FC, 4429A3, 481653, 4BA814, 71502A, 80CC0F, 8D5A80, B8A142, F60205, 1A9089, 230CC2, 25C111, 812269, 821136, D06490, 08C222, 343800, 40054C.

The 64 other codewords for $C_{25}$:

0BB5FFD, 1EEFEB3, 07FA3F7, 127FD7E, 1F9F6CE, 19F9E57, 1B773AB, 1D2EFF8, 1EC0FEF, 1FDD9B4, 08FB9F9, 0F3CA9F, 0FD6C73, 0FEBF0A, 11EE4EF, 1587B3F, 16F57D2, 1733DCD, 1ABE735, 024EFBB, 02F7A4F, 053977B, 056F9D6, 05F4FA5, 0992FDE, 0B8D3E7, 0E5B6D5, 0FA74BC, 13BBAB2, 17DE368, 1B61B7C, 1C79CAE, 1E8DD59, 0019F26, 006AC78, 00763A1, 00865D6, 008DAC9, 032721A, 03A08A7, 0AEC10C, 0C75842, 0D09195, 0E90278, 171AA80, 1C42613, 015314C, 02D1491, 04BA00B, 05046AC, 05E0B10, 06481E2, 0B06D01, 181C065, 18219A8, 0603834, 0988432, 1030296, 12C6240, 1521441, 001C918, 004122B, 0840CC4, 0E28200.

$C_{26}$ comprises **0**, **1** and all the rows of $D$ given in the proof of Theorem 3.12, as well as the 113 following:

0F7DBF7, 3BB7DDE, 2DCFC7F, 36FD779, 3F726EF, 0FFADD9, 15BF1EF, 375FB9A, 3ABFA37 3BC9FAD, 3CE6FF2, 0FF7E2A, 13F8AFE, 1E8377F,

21F5FC7, 262CFBF, 279F6F4, 287B5FE, 391EF6B, 3BCE1D7, 3F65A5D, 0DABABD, 0EDCB4F, 1457FEC, 1736CD7, 17CEF31, 19FF358, 1B5D43F, 1B639EB, 27F213F, 36DB4CB, 3DBBD06, 3DEC4EC, 3E1D9F1, 00DF9B7, 037E6E9, 0535B7B, 06E72DE, 0779F94, 078ADEE, 0B9BE53, 0EB55AD, 182DEF6, 18F2E8F, 1DC5D9A, 1E3A3BA, 2B147DE, 2BE6B64, 2DD93E2, 2E6F703, 2EC0EF9, 316AD5D, 32B7C78, 32B8767, 33AD88F, 35436B7, 0005FBA, 007B2A3, 00BCA74, 01639CC, 0189567, 038E2CA, 05B281B, 05E4685, 0628759, 0693CA4, 0A4EC45, 0E75016, 19564B0, 1AC190B, 1C28C2E, 1C9614C, 22F05C2, 274C922, 2B19891, 2E07229, 30AA1B8, 3249634, 00D50D9, 040E197, 0450B2D, 09248E3, 093D508, 094065E, 0AA2326, 0CCBA10, 1331245, 1382D50, 1E091E0, 2423472, 3088E83, 354A049, 3864311, 00E6C28, 0C126C1, 1053506, 1368092, 150581C, 1694023, 20180EE, 2191330, 2F88404, 0244174, 04A8942, 11005A9, 1A18A08, 2030C15, 2207882, 004D601, 008229C, 0D42022, 1821050, 2414108.

The 141 other codewords for $C_{27}$:

6F9BBF7, 7BF7E5E, 37F9FCB, 556FAFF, 78DCFBF, 7EA75FD, 1AEBF77, 1FF59BE, 37DF6B5, 5F5AFDC, 6B7E17F, 6DBDEEC, 6E77F93, 3A7DAF9, 3D4F5EE, 3DAEE1F, 4DE47F7, 56FACBB, 5BB378F, 5FDF847, 62EFBCE, 670DF7B, 69D3DF9, 17F676C, 1E9DFA3, 2C97B7E, 333BDBC, 33D6B9B, 35B54FB, 366CDD7, 47F92DD, 4E6F63E, 593DF56, 5B8F3F8, 61FEE63, 6BAD8B7, 78FE4DC, 7C3A3EB, 7D51E2F, 7DEBF80, 7EC2AF5, 7FD8572, 01AABFF, 02557FF, 057FD0F, 06FF9F0, 0BB7E39, 0DDCEDA, 174BEE9, 19F95E5, 1C72FB6, 1CE72CF, 1F1E0BF, 1F81D5F, 279B7C6, 2AEB59B, 2B4EF74, 2EF886F, 35ED336, 3F73351, 4B79BAA, 4E3EEC5, 51C7CF6, 58DBB1D, 5D6C979, 67D4DA5, 6D0779D, 6F22CFA, 723785F, 728E72F, 72E1F78, 000A5BF, 0015ACF, 0027F70, 00FB309, 01D8DE0, 02F4075, 0338B16, 036E0CA, 03C3626 05B10BA, 0C52C5A, 0D64391, 0DAA845, 14CC346, 1611D91, 183F406, 1AA86D0, 1B0C839, 1CC78A0, 2AC090F, 2E92330, 352060F, 3B45540, 4260EA9, 4E09076, 57142E0, 5991215, 64864D4, 650BB80, 716A430, 72B3840, 78181CA, 018D453, 068EE08, 0D4948C, 1478823, 1B221A4, 1C01369, 204CAB4, 211315C, 2136C81, 22A5382, 405552A, 44E1914, 50AC08D, 5242253, 6E28501, 7880E22, 003866C, 020B8E1, 0616107, 1180B98, 1A71018, 24C0439, 2760A40, 28200D7, 28DE040, 0013692, 09E0502, 0D10834, 1045C05, 128406A, 142A150, 41500C9, 4826221, 600A80E, 0288215, 2C04188, 6301420, 0091940.

## B.2 Codes mentioned in Sections 3.2 and 3.3

$X_{22}$ is made from the following fourteen codewords:

3FFFFF, 0DDFA7, 3E33DD, 15AD7C, 22EAF3, 1B44CF, 04771B, 3FF800, 3C07E0, 038F06, 0078EC, 324418, 0D2043, 000000.

The 19 other codewords for $X_{24}$:

000000, 0C800F, 4015B0, 017C45, 82CAA2, 992318, 2E1274, 70A0E9, 004FFF, 1EF03B, CF1CE8, 75965E, BAAEB4, EBC167, F56999, 4DBBAF, 97D7F1, EA7E5B, FFFFFF.

The 26 other codewords for $X_{25}$:

1FFFFFF, 1B9BF3E, 17DDCD3, 0177DAF, 06AB7F9, 1AFC3CE, 1D4EB75, 187B0F3, 14B0F76, 13076DE, 0FB6A91, 0F6D722, 0EDBC4C, 0784F0C, 0B4F089, 0CF8921, 104956E, 10928DD, 11243B3, 0027C25, 009B382, 0274258, 1F00843, 05084B8, 1844184, 0000000.

The 18 other codewords for $X_{26}$:

3FFFFFF, 0FAAFBF, 0E553FF, 237FE3C, 24BFFC3, 13E9DD5, 15EE26F, 19D6DBA, 0065A1E, 009D4C3, 011AB70, 01C01AD, 0E0241B, 1C25160, 3268680, 0253044, 05A8802, 0000000.

The 26 other codewords for $X_{27}$:

0000000, 5005221, 012A684, 0AC8013, 0C04D48, 00138BA, 0167143, 1244B94, 1518865, 16A140E, 24D2650, 2989328, 2A344A1, 0C1E7FF, 2AE9D77, 3B7FEC0, 3FB531E, 4FC7CBA, 51E4FCF, 56BBBA3, 7FD80ED, 1773E7F, 2DEFBAD, 63BF5DB, 7AD6BF6, 7FFFFFF.

$Y_{25}$ consists of the following thirteen codewords:

0000000, 03E0141, 10158A8, 043A272, 0703C0F, 00F8F8C, 18C407F, 1FFF000, 1F00FF0, 1C333CF, 1FE8E2F, 18DFDF8, 1FFFFFF.

$Y_{27}$ comprises the following 23 codewords:

7FFFFFF, 3FEDD2E, 6A96EFE, 55F0B7D, 716FE93, 1EDB6A5, 2F355D9, 18DF95A, 072EBE6, 386466F, 4D88C9F, 7313137, 7FFC000, 7C03FC0, 03E3E38, 00B95E3, 045639D, 170584B, 2918A74, 18E2886, 0A0E528, 6041613, 0000000.

## B.3 Codes mentioned in Section 3.4

The 60 other codewords for $Z_{21}$:

001834, 110209, 02A051, 085340, 0C20A8, 120186, 00056D, 000ADA, 00B684, 013903, 01C1B0, 064223, 0AC80C, 0D8442, 161418, 007D6B, 00FAD6, 04B5B5, 0B03EB, 0D607D, 0FAD60, 15AC0F, 1607D6, 1AD607, 1F5AC0, 01D7EC, 02CD9F, 033E75, 052BBE, 06F23B, 0B74DA, 0C9B4F, 12BFA2, 13EB49,

17C876, 191F99, 1A63B5, 1E84ED, 05E7D3, 0759F9, 09F8AF, 0CBEF8, 0E676E, 1392DF, 145EB7, 18AD77, 1DF31C, 1F3587, 07BD5E, 0AFFC5, 0BCE7B, 17EEAC, 197BF2, 1E68DF, 1ED5BA, 0377BF, 1DF4F5, 1F3F69, 1F8BB7, 14FB7F.

The 98 other codewords for $Z_{22}$:

004630, 028109, 181082, 002D06, 0504C1, 209064, 344808, 0422AC, 095A04, 0C8930, 12F400, 130078, 224093, 382141, 0B61A0, 141A13, 144564, 18861C, 251129, 25E014, 2988C2, 2E1450, 330702, 006CD8, 00B34A, 0114B6, 01AE21, 020BC5, 02C82E, 007715, 04F0A3, 06C259, 090373, 1285B1, 133289, 18498B, 1D9045, 20989D, 21444F, 2E2807, 325861, 096AEB, 0D9B36, 0EA6A7, 13533B, 14D4CF, 1A99D5, 1B366C, 24B575, 26CD9A, 2A6753, 2BA92D, 2D5D49, 3525AB, 01F7E6, 03BD5B, 06CB6F, 075DB5, 0DB2DD, 0E17FA, 0F6E1E, 103EBF, 1AF9AA, 1DC1F3, 1E7A71, 33978D, 34BBC3, 355AEC, 36E6D4, 386DE5, 3974DA, 3E9C2E, 0BE7B9, 136BD7, 1B9EE3, 1CF717, 1D396F, 1FCDCC, 227F7C, 25D67B, 27A1FE, 288FDF, 2FF893, 37EF22, 0CFCFE, 2DEB75, 2F37C7, 32F5F3, 373BB9, 39D3BE, 3AFACD, 3B4C7F, 179F7E, 1E6FEB, 35EE9F, 3FF52D, FF2F7, 2BFFDA.

The 145 other codewords for $Z_{23}$:

3FFC3F, 4FEFDD, 1BD7FB, 677B7B, 73EEF6, 79BF4F, 7C65FF, 7EDBB5, 1EAAFF, 24FFE7, 3A7FDC, 4D9FBE, 5FFD61, 67B4FD, 6BE3AF, 7F5657, 1E5DAF, 357CFA, 3B2F73, 3DB39B, 3FC57C, 3FEE85, 4BFB56, 4D7AED, 53AD9F, 55C3F7, 57376E, 62DE3F, 6E9DD3, 7B9BE8, 0177BF, 07EC77, 0B9ECF, 0EF1DD, 0F4BFA, 17DF19, 18FF6A, 1DB6F4, 27B9AE, 2E3EB9, 32A7ED, 356B4F, 36DAD6, 39C8BF, 595DD5, 5AF693, 5B6E3C, 5CB937, 61BAF3, 64BF5C, 67E7C2, 6B117F, 6DF40F, 7771B1, 7A3CE6, 7C867B, 09AB7D, 16AFB2, 1B65CB, 2C6D97, 2D5F64, 3A971E, 426ADF, 42D5F6, 4FA5A5, 57586B, 5CD2AE, 61CD5B, 6AFB21, 7356D8, 750EB5, 7D2D2A, 047365, 072C4D, 0E6CB0, 11D43A, 1AA6C2, 26C29A, 291D43, 29A435, 308E6C, 30E589, 353486, 429AA6, 543A91, 59611C, 6589B0, 6A4750, 00365B, 00AD96, 01538E, 0168E3, 02D0D5, 02EB48, 031939, 0B0A56, 0CCC0B, 0D9690, 0E02AD, 0E9162, 1C49C4, 24453C, 374A01, 3898A1, 3A2113, 518607, 5330C8, 568C50, 5C6222, 61D260, 6401CB, 663421, 682878, 00C333, 0307C1, 03CC24, 04A4E8, 083F20, 104E98, 15F100, 1700B2, 198059, 1A140E, 245852, 4D1805, 501354, 60620D, 69A082, 728128, 02B803, 203198, 21062A, 2A4061, 2C8304, 312844, 4004B5, 406542, 465280, 04088E, 0B2410, 141441, 58C800, 007024, 0082D0, 410109.

# Notation

$\mathbf{V_n}$ — $n$-dimentional vector space over $GF(2)$.

$|A|$ — the cardinality of a finite set $A$.

$N(\mathbf{x},\mathbf{y}) = |\{\ i \mid x_i = 1\ \wedge\ y_i = 0,\ 0 \le i \le n\ \}|$.

$d_h(\mathbf{x},\mathbf{y})$ — the Hamming distance of $\mathbf{x}$ and $\mathbf{y}$.

$d_a(\mathbf{x},\mathbf{y})$ — the asymmetric distance of $\mathbf{x}$ and $\mathbf{y}$.

$d_u(\mathbf{a},\mathbf{b})$ — the unidirectional distance of $\mathbf{x}$ and $\mathbf{y}$.

$w(\mathbf{x})$ — the weight of $\mathbf{x}$.

$w(C)$ — the weight of the code $C$.

$C_a(n,d)$ — AsEC codes of length $n$ and asymmetric distance $d$.

$C_u(n,d)$ — UEC codes of length $n$ and unidirectional distance $d$.

$C_h(n,d)$ — SyEC codes of length $n$ and Hamming distance $d$.

$A_f(n,d)$ — the maximum number of codewords of a $C_f(n,d)$ code ($f = a,u,h$).

$A(n,d,w)$ — the maximum number of binary vectors of length $n$, Hamming distance at least $d$ apart and constant weight $w$.

$circ(\mathbf{x})$ — $n \times n$ circulant with top row $\mathbf{x}$.

$supp(\mathbf{x})$ — the support of $\mathbf{x}$.

$\lfloor r \rfloor$ — the largest integer not exceeding the real number $r$.

$\lceil r \rceil$ — the smallest integer not less than the real number $r$.

$[n,k,d]$ — linear SyEC code of length $n$, dimention $k$ and Hamming distance $d$.

$a \mid b$ — $a$ divides $b$ exactly ( $a,b$ integers).

$<\mathbf{x},\mathbf{y}> = \sum_{i=1}^{n} x_i y_i$ — the inner product of $\mathbf{x}$ and $\mathbf{y}$.

$Aut(C)$ — the automorphism group of $C$.

$r(\mathbf{c})$ — the minimum asymmetric distance from the codeword $\mathbf{c}$ to all other codewords.

$S_a(\mathbf{c},t)$ — the sphere with radius $t$ and center $\mathbf{c}$ for AsEC codes.

$W_a(n,d)$ — the maximum number of codewords in a $WP$ $C_a(n,d)$ code.

$U_a(n,d)$ — the maximum number of codewords in a $UWP$ $C_a(n,d)$ code.

$\overline{r}(C)$ — the average error-correcting capability of a $C_a(n,d)$ code $C$.

# STATEMENTS

*attached to the dissertation*

**Binary Block Codes for Correcting Asymmetric or Unidirectional Errors**

Gang FANG

*March 8, 1993, Eindhoven University of Technology*

1. In 1942, K. Menger first introduced the concept of probabilistic metric spaces (for short, $PM$ spaces) in his paper (*Statistical metrics*, Proc. Nat. Acad. Sci. USA, **28**, pp. 535-537, 1942). The so called probabilistic metric of two points (say $p$ and $q$) in a nonempty set means that the distance of $p$ and $q$ does not correspond to a real number (as usual) but to a distribution function, denoted by $F_{pq}(x)$. For a given $x$, $F_{pq}(x)$ gives the probability that the distance between $p$ and $q$ is less than $x$. There is no doubt that the probabilistic metric is more reasonable, in terms of the standpoint of practical life of human beings, than the normal metric. In our routine life, an expression providing a certain uncertainty often does give an accurate concept.

   — *Fang, G.: Topological structures of PM spaces, Tech. Report, 85-113, Xi'an Jiaotong University, 1985*

2. Let $(S_1, \mathcal{F}_1, \tau)$ and $(S_2, \mathcal{F}_2, \tau)$ be two $PM$ spaces where $\tau$ is continuous. Then the so called $M$-product space $(S_1 \times S_2, \mathcal{F}_1 M \mathcal{F}_2, \tau)$ is also a $PM$ space which satisfies that $S_1 \times S_2$ is separable (complete, compact) if and only if both $S_1$ and $S_2$ are separable (complete, compact).

   — *Fang, G., Zhang, W. X.: Properties of M-product spaces of PM spaces, Journal of Xi'an Jiaotong University,* **20***(4), 87-90, Aug. 1986*

3. A code $C$ is called $s$-$WP$ code if the equality (6.3) in the dissertation holds when $r(\mathbf{c})$ is replaced by $s_L(\mathbf{c})$ for all $\mathbf{c} \in C$, where the number $s_L(\mathbf{c})$ for any $\mathbf{c} \in C$ is defined in

   — *Fang, G., Honkala, I. S.: On Perfectness of Binary Block Codes for Correcting Asymmetric Errors, Proc. of IEEE Inter. Symp. on IT, San Antonio, Texas, USA, January 1993*

   Distinctively, the weakly perfect codes defined in the dissertation are termed as $r$-$WP$ codes. It can be shown that the class of $r$-$WP$ codes is a subset of the class of $s$-$WP$ codes.

4. Theorem 6.6, Theorem 6.8 and Corollary 6.1 in the dissertation are also true to $s$-WP codes.

5. Let $Z(n,s,t)$ be the maximum number of codewords in a $t$-AsEC/$s$-AsED ($s \geq t$) code of length $n$. Then

$$Z(n,s,t) \geq max\{ \sum_{w \equiv i} A(n, 2t+2, w) \mid 0 \leq i \leq s \}$$

where the sum is taken over all integers $w$ congruent to $i$ modulo $(s+1)$. Particularly, the equality holds when $t=0$ and $i = \lfloor n/2 \rfloor$.

6. Given $j \geq 1$, $m \geq j+1$, $n \geq 2m+1$ and $q = \lfloor j/2 \rfloor$. Then

$$\binom{n-j}{m} \geq 2 \sum_{k=0}^{q} \prod_{t=0}^{k} \frac{n-j-t}{m-t}.$$

7. Let $F$ be a $t$-antichain in $\{0,1\}^n$. For $i = 0, 1, \cdots t$ and $\mathbf{f} \in F$, define

$$E_i(\mathbf{f}) = \{ \mathbf{x} \in \{0,1\}^n \mid |\mathbf{x}| = |\mathbf{f}| + t - 2i \wedge d_h(\mathbf{x}, \mathbf{f}) \leq t \}.$$

Then for each $i$ with $0 \leq i \leq t$, $E_i(F) = \bigcup_{\mathbf{f} \in F} E_i(\mathbf{f})$ is an antichain, and

$$\sum_{\mathbf{f} \in F} |E_i(\mathbf{f})|(|\mathbf{f}| + t - 2i)!(n - |\mathbf{f}| - t + 2i)! \leq n!.$$

— *Zhang, Z., Xia, X. G.: LYM Inequalities for t-antichains, Submitted to Discrete Mathematics*

8. In history, Western mathematics entered into China two times. The first entry started at the end of the 16th century and ended at the beginning of the 18th century by the feudalistic closed door policy of Chinese government at that time. This *closed door* was broken down by Western guns and cannons in the Opium Wars in 1840 (cf. *Chinese Mathematics: A Concise History*, by Li Yan and Du Shiran, translated by J. N. Crossley and A. W. -C. Lun, Clarendon press, Oxford, 1987). Besides abacus calculation, which has been preserved and is still widely used today in everyday life in China, all the rest of the ancient mathematics of China blended into the stream of the development of world mathematics. Nowadays the development of science and technology is extremely rapid, and it is clear that there must be no future for any country under a closed door policy.

9. The Netherlands is an internationally-oriented country because of her typical circumstances. China had, has and will have a lot of connections with the Netherlands in economy. However early in this century, also there was a Dutchman who played an important role on the political stage of Chinese history.