Maximal partial packings of Z_2^n with perfect codes

Master of Science Thesis in Mathematics at KTH, Stockholm, Sweden

Thomas Westerbäck
thomas.westerback@mora.se
December, 2005

Abstract

A maximal partial Hamming packing of Z_2^n is defined by us to be a family $\mathcal{S}$ of mutually disjoint translates of Hamming codes of length n, such that any translate of any Hamming code of length n intersects at least one of the translates of Hamming codes in $\mathcal{S}$. The number of translates of Hamming codes in $\mathcal{S}$ is the packing number, and a partial Hamming packing is strictly partial if the family $\mathcal{S}$ does not constitute a partition of Z_2^n.

A simple and useful condition describing when two translates of Hamming codes are disjunct or not disjunct is proved. This condition depends on the dual codes of the corresponding Hamming codes. Partly by using this condition, it is shown that the packing number p, for any maximal strictly partial Hamming packing of Z_2^n, $n = 2^m - 1$, satisfies $m + 1 \leq p \leq n - 1$.

It is also proved that for any n equal to $2^m - 1$, $m \geq 4$, there exist maximal strictly partial Hamming packings of Z_2^n with packing numbers $n-10, n-9, n-8, \ldots, n-1$. This implies that the upper bound is tight for any $n = 2^m - 1$, $m \geq 4$.

All packing numbers for maximal strictly partial Hamming packings of Z_2^n, $n = 7$ and 15, are given by a computer search. In the case $n = 7$ the packing number is 5, and in the case $n = 15$ the possible packing numbers are $5, 6, 7, \ldots, 13$ and 14.

(Supervised by Olof Heden, Department of Mathematics, KTH.)

Contents

1 Introduction

In this section we give a brief introduction of the concepts and methodology used in this Master of Science Thesis. The concepts that are introduced here will be explained with more details in later sections.

1.1 Coding theory

Coding theory is concerned with how to encode, decode and transfer information from one place to another in an efficient and accurate manner. The study of coding theory began in the 1940's with works of Golay, Hamming and Shannon.

A subarea of coding theory is the theory of error correcting codes. The theory of error correcting codes has been developed for many different applications. For example, error correcting codes are used in CD-players and in the Voyager spacecraft which have sent pictures of Jupiter and Saturn to Earth.

A *perfect e-error correcting binary code* of length n, is a subset C of Z_2^n, such that for every $\bar{x} \in Z_2^n$ there is a unique $\bar{c} \in C$, satisfying that the number of positions for which $\bar{x}$ and $\bar{c}$ differ is less than or equal to e. In this thesis we will study perfect 1-error correcting binary codes, which we simply will call *perfect codes*. A linear perfect code is called a *Hamming code*, i.e. a perfect code C is a Hamming code if $\bar{c}, \bar{c}' \in C$ implies that $\bar{c} + \bar{c}' \in C$.

It is well known, (as will be explained in Section 2), that if C is a perfect 1-error correcting binary code of length n, then $n = 2^m - 1$ for some integer m. Hence the possible lengths for perfect codes are $1, 3, 7, 15, 31, \ldots$. There is a general construction for all Hamming codes of every possible lengths, (this construction is given in Section 2). However, there only exist non linear perfect codes of length $n \geq 15$ and there is no general construction for all of them. There are many different constructions on perfect codes, see e.g. [14].

Perfect codes are fascinating. Although the basic structure of a perfect code is simple, it is a finite set of elements that satisfies a conceptual simple condition, there are many relations within each perfect code and with other perfect codes. For example, there is no known classification of perfect codes of length $n \geq 15$. Further, from [9], the number of different perfect codes of length $n \geq 15$, is greater than

$$2^{2^{\frac{n+1}{2}-\log_2(n+1)}} \cdot 3^{2^{\frac{n-3}{4}}} \cdot 2^{2^{\frac{n+5}{4}-\log_2(n+1)}}.$$

The number of atoms in the observable universe is estimated to be about 10^{80}, which is much less than the number of different perfect codes of length 31 which is, by the equation above, at least 10^{682}.

The properties in the paragraph above show that it is hard to order, enumerate and classify perfect codes. There are many interesting problems concerning perfect codes that still remain open.

1.2 Methodology and disposition

The main subject of our investigations in this thesis is the packing number of maximal strictly partial Hamming packings.

A *partial Hamming packing* of Z_2^n is a family $\mathcal{S}$ of mutually disjoint translates of, not necessarily different, Hamming codes in Z_2^n. Further, a partial Hamming packing of Z_2^n is *strictly partial* and *maximal* if the following conditions are satisfied:

(i) *The union of the sets in the corresponding family $\mathcal{S}$ is a strict subset of Z_2^n.*

(ii) *There does not exist any translate of any Hamming code of length n which is disjunct to the union of the sets in the corresponding family $\mathcal{S}$.*

The *packing number* of a partial packing is the number p of translates of Hamming codes in the partial packing.

To our knowledge there have not been any studies on maximal strictly partial Hamming packings so far. However, in other areas of mathematics, similar objects have been studied. For example, maximal partial spreads in $P(3, q)$. A maximal partial spread in $P(3, q)$ is a set S of mutually skew lines in the projective 3-dimensional geometry, such that any line in this geometry intersects at least one of the lines in S. That study started by Mesner in 1967 and has continued since then, [10]. Further, there have been studies on partitions of Z_2^n with translates of Hamming codes and translates of any perfect codes, which may be seen as full partial Hamming packings respectively full partial packings. For example, in [12], by using a computer study, Phelps gives all inequivalent partitions of Z_2^7 with perfect codes. (All perfect codes of Z_2^7 are translates of Hamming codes. Two partitions are equivalent if we can obtain one of the partitions from the other by a permutation of the coordinate set of Z_2^7 and the addition of one element $\bar{x} \in Z_2^7$.) These partitions are significant for one of the more important constructions of perfect codes, namely the Phelps construction, see e.g. [11].

In this study we will use both theoretical and computer based methods. The main results of the study are:

- Corollary 3 of Section 5, that gives a necessary and sufficient condition for when a set of translates of Hamming codes is a partial Hamming packing.

- Corollary 4 and Corollary 6 of Section 6, that gives a lower and an upper bound for the packing numbers of maximal strictly partial Hamming packings.

- Theorem 9 and Theorem 10 in Section 7, which give, by use of a computer search, the packing numbers that exist for maximal strictly partial Hamming packings of Z_2^7 and Z_2^{15}.

- Corollary 7 of Section 7, which gives an existence result for some packing numbers of maximal strictly partial Hamming packings of Z_2^n, $n \geq 15$.

As mention before, even though perfect codes are conceptually easy to handle, there are many different relations between perfect codes and there are many different perfect

codes. These properties may cause problems when dealing with perfect codes in practice. For example, the number of different translates of Hamming codes of length 31 equals

$$32 \cdot \frac{31!}{31 \cdot 30 \cdot 28 \cdot 24 \cdot 16} \approx 3 \cdot 10^{30},$$

(see Proposition 5 of section 2). Suppose we could execute one of these translates every clock cycle on a 5 GHz personal computer. Then it would take approximate $2 \cdot 10^{13}$ years to execute all of the translates. This shows that the computer search we are using in this study for maximal strictly partial Hamming packings of Z_2^n, $n = 7, 15$, is impossible to perform when n is greater than or equal to 31.

This thesis is organized in the following way. Section 2 contains some basic facts concerning coding theory in general and perfect codes in particular. This will introduce the casual reader to the subject, and give the necessary basic knowledge needed for later sections. In Section 3 and 4 we give some results concerning more specific topics that we will use when we prove the main results in this thesis. The main results will be given in Section 5, 6 and 7. In Section 8, we summarize the results we have obtained and list some open problems.

(As this is a Master of Science Thesis we also include some elementary proofs, that are normally not included in regular research reports in mathematics.)

2 Preliminaries and notation

In this section we shall give some basic definitions, results and notation concerning coding theory in general and perfect codes in particular.

The results in this section are well known and covered in many books about error-correcting codes. For a general introduction to coding theory see for example [13].

2.1 Binary codes

A *binary code* is a subset of Z_2^n,

$$Z_2^n = \underbrace{Z_2 \times Z_2 \times \ldots \times Z_2}_{n} \ ,$$

where Z_2 is the finite field with two elements. These elements will be denoted by 0 and 1. Note, that by a *code*, C, we will always mean a binary code.

Following are some definitions and notation concerning the elements of Z_2^n. By a *word* we mean an element $\bar{x} = (x_1, x_2, \ldots, x_n) \in Z_2^n$. The number n is called the *length* of the word. Addition and scalar multiplication will be defined by

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

and

$$\lambda(a_1, a_2, \ldots, a_n) = (\lambda a_1, \lambda a_2, \ldots, \lambda a_n).$$

Hence, with the addition and scalar multiplication above, Z_2^n is a vector space.

The *dot product* of two words $\bar{a}, \bar{b} \in Z_2^n$ is defined by,

$$\bar{a} \cdot \bar{b} \equiv a_1 b_1 + a_2 b_2 + \ldots + a_n b_n \pmod 2.$$

This dot product will be used to define orthogonality and dual codes.

Example. Consider the words $\bar{a} = (101)$, $\bar{b} = (001)$ in Z_2^3. Then

$$\bar{a} + \bar{b} = (100)$$

and

$$\bar{a} \cdot \bar{b} \equiv 1 \cdot 0 + 0 \cdot 0 + 1 \cdot 1 \equiv 1 \pmod 2.$$

A code C is *linear*, if for any $\bar{x}, \bar{x}' \in C$, the word $(\bar{x} + \bar{x}') \in C$. This means that C is linear if and only if C is a subspace of the vector space Z_2^n.

Example. Let C be the code $\{(000), (110)(001)(111)\}$ and C' the code $\{(110)(001)(111)\}$. Then C is a linear code and C' is a non linear code, as for example $(110)+(110) = (000) \notin C'$.

There are some frequently used words that will have a special notation. Let, for $i = 1, 2, \ldots, n$, $\bar{e}_i$ be the word in Z_2^n with a 1 in the position i and with 0:s in the remaining coordinate positions. Also, let $\bar{e}_0 = \bar{0} = (00\ldots0)$ and $\bar{1} = (11\ldots1)$.

Further, to every word $\bar{x} = (x_1, x_2, \ldots, x_n) \in Z_2^n$, we associate a word that is denoted as $\bar{x}^*$,

$$\bar{x}^* = (x_0^*, x_1^*, x_2^*, \ldots, x_n^*) = (0, x_1, x_2, \ldots, x_n).$$

Example. Consider the words $\bar{e}_0$, $\bar{e}_2$ and $\bar{1}$ in Z_2^3. Then

$$\bar{e}_0 = (000), \quad \bar{e}_2 = (010), \quad \bar{1} = (111) \quad \textit{and} \quad \bar{e}_2^* = (0010).$$

For any integer n, let

$$[n] = \{1, 2, \ldots, n\} \quad \text{and} \quad [n]^* = \{0, 1, 2, \ldots, n\}.$$

When considering the distance between two words, different definitions of distances may be used in general. However, here we will only consider the Hamming distance. By $d(\bar{x}, \bar{x}')$ we denote the *Hamming distance* between the words $\bar{x}, \bar{x}' \in Z_2^n$,

$$d(\bar{x}, \bar{x}') = \mid \{i \in [n] \mid x_i \neq x_i'\} \mid .$$

The *support* of any word $\bar{x} \in Z_2^n$, $supp(\bar{x})$, is defined to be the set

$$supp(\bar{x}) = \{i \in [n] \mid x_i = 1\},$$

and the *weight*, $w(\bar{x})$, to be the integer

$$w(\bar{x}) = \mid supp(\bar{x}) \mid .$$

An *e-sphere* with center $\bar{x}$, where e is an integer and $\bar{x} \in Z_2^n$, is the set

$$S_e(\bar{x}) = \{\bar{c} \in Z_2^n \mid \ d(\bar{x}, \bar{c}) \leq e\}.$$

Example. Consider the words $\bar{a} = (101)$, $\bar{b} = (001)$ in Z_2^3. Then

$$d(\bar{a}, \bar{b}) = 1,\ supp(\bar{a}) = \{1, 3\},\ w(\bar{a}) = 2 \text{ and } S_1(\bar{a}) = \{(101), (001), (111), (100)\}.$$

2.2 Perfect 1-error correcting binary codes

As mention in the introduction, coding theory is concerned with how to encode, decode and transfer information from one place to another in an efficient and accurate manner. When information is transmitted, disturbance on the transmission channel may cause the received information to differ from the originally transmitted information. When this happens we need to be able to detect and correct the errors.

With an e-error correcting code we are able to detect and correct e or less errors in a code word. For example, if we have a 1-error correcting code we are able to detect and correct one error in a code word, i.e. if one of the 0:s of a transmitted code word has been changed to 1 or if one of the 1:s have been changed to 0.

A code C is an *e-error correcting* code, if

$$\bar{c}, \bar{c}' \in C \text{ and } \bar{c} \neq \bar{c}' \quad \Rightarrow \quad S_e(\bar{c}) \cap S_e(\bar{c}') = \emptyset.$$

Example. If the messages that will be sent over a channel is, *yes* or *no*, then we can encode the messages with the code $C = \{(000), (111)\}$, where $yes = (000)$ and $no = (111)$. The code C is a 1-error correcting code.

Now suppose the message that will be sent is *yes*, i.e. (000), but the word that the receiver gets is (010), then a 1-error has occurred. Because there is only one unique code word in C at a distance less than or equal to 1 from (010), the receiver should correct the received word to (000). (We assume that the probability of errors are small, thus the probability for multiple errors are much smaller.)

We are now ready to define the main object of this thesis, perfect 1-error correcting binary codes. A *perfect 1-error correcting binary code* of length n is a subset C of Z_2^n satisfying the following condition:

For every word $\bar{x} \in Z_2^n$ there is a unique word $\bar{c} \in C$, such that $d(\bar{x}, \bar{c}) \leq 1$.

By a *perfect code* we will always mean a perfect 1-error correcting binary code. Note that by the definition above of perfect codes we may conclude that a subset C of Z_2^n is a perfect code if and only if

$$\dot{\bigcup_{\bar{c} \in C}} S_1(\bar{c}) = Z_2^n. \tag{1}$$

(The notation $\dot{\cup}$ means here that all the sets in the union are mutually disjoint. For example, all the sets $S_1(\bar{c})$, $\bar{c} \in C$ above, constitute a partition of Z_2^n.)

A perfect code C, such that $\bar{0} \in C$, is sometimes called a *normal perfect code*. This terminology will be used in this thesis.

A rather simple method for constructing all linear perfect codes was given in a paper from 1950 by Hamming, see [4]. Hence, a perfect code that is linear is called a *Hamming code*. For example, the code $C = \{(000), (111)\}$ is a Hamming code. Below we explain the method that Hamming invented.

Construction. Consider the space Z_2^n, $n = 2^m - 1$. Let the matrix H consist of m rows and n columns, such that the n columns consist of all non zero words of Z_2^m. Then the set

$$C = \{\bar{c} = (c_1, c_2, \ldots, c_n) \in Z_2^n \mid H\bar{c}^T = \bar{0}^T\}, \tag{2}$$

is a Hamming code of length n. To see this we note the following: Due to the fact that each word in $Z_2^m \setminus \{\bar{0}\}$ is equal to a unique column of the matrix H above, we may observe that for any word $\bar{x} \in Z_2^n \setminus C$ there is a unique $i \in [n]$ such that $H\bar{x}^T = H\bar{e}_i^T$. This implies that

$$H\bar{x}^T = H\bar{e}_i^T \quad \Leftrightarrow \quad H(\bar{x} + \bar{e}_i)^T = \bar{0}^T \quad \Leftrightarrow \quad \bar{x} + \bar{e}_i \in C.$$

Hence for all $\bar{x} \in Z_2^n$ there is a unique $\bar{c} \in C$ such that $d(\bar{c}, \bar{x}) \leq 1$. Consequently C is a perfect code.

Note that the rows in the matrix H above are linear independent.

Example. Take

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

Then

$$C = \{(c_1, c_2, \ldots, c_7) \mid \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_7 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}\}.$$

Thus we get the Hamming code

$$C = \{(0000000), (1110000), (1001100), \ldots, (0110011), (0001111), (1111111)\}.$$

A matrix H is called a *parity-check matrix* for a code C of length n, if the rows in H are linear independent and C consists precisely of all words $\bar{c} \in Z_2^n$ such that $H\bar{c}^T = \bar{0}^T$. Hence, the matrix H in the construction (2) is a parity-check matrix to the corresponding perfect code C.

A straightforward result on parity-check matrices is the following proposition:

Proposition 1. *Consider two different parity-check matrices H and H', the corresponding codes C and C' respectively are the same if and only if the linear span of the rows in each matrix are the same.*

Consider any two subsets $A, B \in Z_2^n$, then

$$A + B = \{\bar{a} + \bar{b} \mid \bar{a} \in A, \bar{b} \in B\}.$$

(Note that $A + B$ is not a multiset.)

A translate of a perfect code C of length n is any set

$$C + \bar{x} = \{\bar{c} + \bar{x} \mid \bar{c} \in C\},$$

where $\bar{x}$ is a fixed word of Z_2^n.

Note that a translate of a perfect code is also a perfect code, as will be proved in Corollary 2 on page 8. Further, from the definition of perfect codes we get that for any perfect code C, $\mid S_1(\bar{0}) \cap C \mid = 1$. These properties imply that any perfect code of any length n is a translate, $C + \bar{e}_i$, where $i \in \{0, 1, \ldots, n\}$ and C is a normal perfect code of length n.

Also, by trivial verifications we get that any translate, $C + \bar{x}$, of a Hamming code C of length n is equal to one of the following sets

$$C + \bar{e}_i = \{\bar{c} + \bar{e}_i \mid \bar{c} \in C\}, \quad i = 0, 1, \ldots, n.$$

Example. Consider the Hamming code $C = \{(000), (111)\}$ of length 3. There are four translates of C, namely:

$$\begin{aligned} C + \bar{e}_1 &= \{(100), (011)\}, \\ C + \bar{e}_2 &= \{(010), (101)\}, \\ C + \bar{e}_3 &= \{(001), (110)\}, \\ C + \bar{e}_0 &= \{(000), (111)\} = C. \end{aligned}$$

2.3 Partial packings

In coding theory there is a well known upper bound for the number of words in any e-error correcting codes. This bound is called the *sphere packing bound* and it states that for any e-error correcting code A of length n

$$\mid A \mid \quad \leq \quad \frac{2^n}{1 + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{e}},$$

see for example [13]. The number of words in any perfect code attains this upper bound. This property will be stated as condition (i) in the theorem below.

Theorem 1. *Let C be a subset of Z_2^n. Then C is a perfect code of length n if and only if both of the following conditions are satisfied:*

$$\begin{array}{lll} (i) & \mid C \mid \; = 2^n/(1+n), & \\ (ii) & \bar{c}, \bar{c}' \in C \text{ and } \bar{c} \neq \bar{c}' & \Rightarrow \quad S_1(\bar{c}) \cap S_1(\bar{c}') = \emptyset. \end{array}$$

Proof. From (1) on page 5, C is a perfect code of length n if and only if

$$\dot{\bigcup_{\bar{c}\in C}} S_1(\bar{c}) = Z_2^n.$$

This is equivalent to

$$S_1(\bar{c}) \cap S_1(\bar{c}') = \emptyset \quad if \quad \bar{c}, \bar{c}' \in C, \bar{c} \neq \bar{c}'$$

and

$$2^n = \mid Z_2^n \mid = \sum_{\bar{c}\in C} \mid S_1(\bar{c}) \mid = \mid C \mid \cdot \mid S_1(\bar{0}) \mid = \mid C \mid \cdot (1 + \binom{n}{1}).$$

The next corollary is an immediate consequence of Theorem 1.

Corollary 1. *If C is any perfect code of length n, then $n = 2^m - 1$ for some integer $m \geq 1$ and $\mid C \mid = 2^{n-m}$.*

The next corollary is also a well known result.

Corollary 2. *Any translate of any perfect code is a perfect code.*

Proof. Let C be any perfect code of length n. Then

$$\mid C + \bar{x} \mid = \mid C \mid = 2^n/(n+1), \quad \bar{x} \in Z_2^n.$$

If there exist any two words $(\bar{c}+\bar{x}), (\bar{c}'+\bar{x}) \in (C+\bar{x})$, $\bar{c} \neq \bar{c}'$, and any word $\bar{x}' \in Z_2^n$ such that $\bar{x}' \in S_1(\bar{c}+\bar{x}) \cap S_1(\bar{c}'+x)$, then $(\bar{x}'+\bar{x}) \in S_1(\bar{c}) \cap S_1(\bar{c}')$, which is a contradiction. Hence by Theorem 1 the corollary is proved.

Now we define the main topic of this thesis, partial packings. A *partial packing of Z_2^n with translates of perfect codes*, is a family of mutually disjoint translates of perfect codes of length n. By a *partial packing* we will always mean a partial packing with translates of perfect codes and by a *partial Hamming packing* we will always mean a partial packing with translates of Hamming codes. Note that a partial Hamming packing is also a partial packing.

We will write $PP(C_0, C_1, \ldots, C_k; \pi; n)$ for the following partial packing of Z_2^n,

$$(C_0 + \bar{e}_{\pi(0)}) \quad \dot{\cup} \quad (C_1 + \bar{e}_{\pi(1)}) \quad \dot{\cup} \quad \ldots \quad \dot{\cup} \quad (C_k + \bar{e}_{\pi(k)}), \tag{3}$$

where $C_0, C_1, \ldots, C_k$ are normal perfect codes of length n and π is a permutation of the set $\{0, 1, 2, \ldots, n\}$.

Further, if the perfect codes $C_0, C_1, \ldots, C_k$ in (3) are Hamming codes, then we have a partial Hamming packing of Z_2^n which we may denote by $PHP(C_0, C_1, \ldots, C_k; \pi; n)$.

Note that the perfect codes $C_0, C_1, \ldots, C_k$ in (3) do not need to be distinct.

Example. Let C_0, C_1 and C_2 be the Hamming code $\{(000),(111)\}$. Also let π be the permutation of $\{0,1,2,3\}$ where $\pi(0)=1$, $\pi(1)=3$, $\pi(2)=0$ and $\pi(3)=2$. Then

$$\begin{aligned}(C_0+\bar{e}_{\pi(0)}) &= \{(100),(011)\},\\ (C_1+\bar{e}_{\pi(1)}) &= \{(001),(110)\},\\ (C_2+\bar{e}_{\pi(2)}) &= \{(000),(111)\}.\end{aligned}$$

Thus, we get a partial Hamming packing, $PHP(C_0,C_1,C_2;\pi;3)$, and consequently a partial packing, $PP(C_0,C_1,C_2;\pi;3)$, such that these packings equal

$$\{(100),(011)\}\ \dot{\cup}\ \{(001),(110)\}\ \dot{\cup}\ \{(000),(111)\}.$$

The number of translates of perfect codes in a partial packing is called the *packing number*. Hence, the packing number of a $PP(C_0,C_1,\ldots,C_k;\pi;n)$ equals $k+1$.

By Corollary 1, we may conclude that for any partial packing of Z_2^n, $n=2^m-1$, with packing number p the number of words in the partial packing equals $p\cdot 2^{n-m}$. Consequently, the packing number for any partial packing of Z_2^n is less than or equal to $n+1$, with equality if and only if the partial packing is a partition of Z_2^n.

A $PP(C_0,C_1,\ldots,C_k;\pi;n)$ is a *maximal partial packing*, if for any perfect code C of length n and any $j\in\{0,1,2,\ldots,n\}$

$$\Big(\dot{\bigcup}_{i=0}^{k}(C_i+\bar{e}_{\pi(i)})\Big)\cap(C+\bar{e}_j)\neq\emptyset. \tag{4}$$

Further, a $PHP(C_0,C_1,\ldots,C_k;\pi;n)$, is a *maximal partial Hamming packing* if condition (4) above is satisfied for any Hamming code C of length n and any $j\in\{0,1,2,\ldots,n\}$.

Example. If C is a perfect code of length n, then to any word $\bar{x}\in Z_2^n$ there is a unique word $\bar{c}\in C$ such that $d(\bar{x},\bar{c})\leq 1$. This implies that

$$C\ \dot{\cup}\ (C+\bar{e}_1)\ \dot{\cup}\ (C+\bar{e}_2)\ \dot{\cup}\ \ldots\ \dot{\cup}\ (C+\bar{e}_n)=Z_2^n.$$

Thus, for any perfect code of length n and any permutation π of $\{0,1,\ldots,n\}$ we get a maximal $PP(C_0,C_1,\ldots,C_n;\pi;n)$ if $C=C_0=C_1=\ldots=C_n$.

Note that a maximal partial Hamming packing does not need to be a maximal partial packing.

A *maximal strictly* $PP(C_0,C_1,\ldots,C_k;\pi;n)$ is a maximal partial packing with a packing number less than $(n+1)$, i.e.

$$(C_0+\bar{e}_{\pi(0)})\ \dot{\cup}\ (C_1+\bar{e}_{\pi(1)})\ \dot{\cup}\ \ldots\ \dot{\cup}\ (C_k+\bar{e}_{\pi(k)})\subsetneqq Z_2^n.$$

Also, a *maximal strictly* $PHP(C_0,C_1,\ldots,C_k;\pi;n)$ is a maximal partial Hamming packing with packing number less than $(n+1)$.

2.4 Rank, kernel and dual code

The set of all linear combinations of the words in a code C is denoted by $< C >$. This set is called the *linear span* of C. Further, the *rank* of a code C, denoted by $rank(C)$, is the dimension of the linear span $< C >$. A *full rank* code is a code C of length n with $rank(C) = n$.

The *kernel* of a code C of length n is the set of periods, i.e.

$$ker(C) = \{\bar{p} \in Z_2^n \mid \bar{p} + \bar{c} \in C \quad \forall \bar{c} \in C\}.$$

This set is a subspace of Z_2^n. Also, C is a linear code if and only if $ker(C) = C$.

The set of words of Z_2^n orthogonal to all words in a linear code C of length n, denoted by $C^\perp$, is the *dual code* of C, i.e.

$$C^\perp = \{\bar{x} \in Z_2^n \mid \bar{x} \cdot \bar{c} \equiv 0 \pmod 2 \quad \forall \bar{c} \in C\}.$$

It is straightforward to show, that $C^\perp$ is also a linear code and that for any linear codes A, B of length n

$$(A \cap B)^\perp \quad = \quad A^\perp + B^\perp \tag{5}$$

and

$$A^\perp = (A^\perp)^\perp. \tag{6}$$

Example. Let $C = \{(1100), (0010)\}$, then

$$\begin{array}{lcl} < C > & = & \{(0000), (1100), (0010), (1110)\}, \\ < C >^\perp & = & \{(0000), (0001), (1100), (1101)\}, \\ ker(C) & = & \{(0000), (1110)\}, \\ rank(C) & = & 2. \end{array}$$

By the construction (2) on page 6, we get a Hamming code of length $n = 2^m - 1$, by using a parity-check matrix with m independent rows. The generated subspace of the rows in this parity-check matrix is the dual of the associated Hamming code. Hence, if we have a Hamming code C of length n, then

$$C = \{\bar{c} \in Z_2^n \mid \bar{x} \cdot \bar{c} \quad \forall \bar{x} \in C^\perp\}.$$

The proposition below is a well known result in coding theory, see for example [13].

Proposition 2. *For any linear code A of length n*

$$dim(A) = n - dim(A^\perp).$$

By Corollary 1 on page 8, we get that for any perfect code C of length $n = 2^m - 1$,

$$rank(C) \geq \log_2(2^{n-m}) = n - m, \tag{7}$$

where $rank(C) = n - m$ if and only if C is a Hamming code. Thus, by Proposition 2 above, for any perfect code C of length $n = 2^m - 1$,

$$dim(< C >^{\perp}) \quad \leq \quad m, \tag{8}$$

where $dim(C) = m$ if and only if C is a Hamming code.

The next proposition is a consequence of some elementary results concerning vector spaces and we will use this proposition frequently in Section 5.

Proposition 3. *Let A and B be any linear codes of length n. Then*

$$dim(A \cap B) = n - dim(A^{\perp}) - dim(B^{\perp}) + dim(A^{\perp} \cap B^{\perp}).$$

Proof. An elementary result in linear algebra, that may be proved by a straightforward verification, states that for any subspaces V and W of a vector space,

$$dim(V + W) + dim(V \cap W) = dim(V) + dim(W).$$

This implies, by (5), that

$$dim((A \cap B)^{\perp}) + dim(A^{\perp} \cap B^{\perp}) = dim(A^{\perp}) + dim(B^{\perp}).$$

The proposition now follows from Proposition 2.

3 Simplex codes and the associated extended fundamental partition to a simplex code

In [8], Hergert shows that if C is a perfect code, then $< C >^{\perp}$ is a simplex code. To any simplex code we may associate a special partition that will be called the extended fundamental partition. The concepts of simplex code and extended fundamental partition will be used frequently. We will in this section give the basic facts about these subjects.

We define a *simplex code* D to be a subspace of Z_2^n, $n = 2^m - 1$, such that

$$\bar{d} \in D \setminus \{\bar{0}\} \quad \Rightarrow \quad w(\bar{d}) = \frac{n+1}{2}.$$

Note that any subspace of a simplex code is also a simplex code.

Example. The space spanned by the two words of length seven in the matrix below is a simplex code,

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

In [1], the term fundamental partition $I_0, I_1, \ldots, I_t$ of $\{1, 2, \ldots, n\}$ is defined for any simplex code D of length $n = 2^m - 1$, when $1 \leq dim(D) \leq m - 1$. The existence of these extended partitions for simplex codes is also a result of [2]. By Lemma 1 below, we extend this definition to a partition of $\{0, 1, \ldots, n\}$ such that it works for any simplex code of length $n = 2^m - 1$, with dimension less than or equal to m. This extended partition will be called the *extended fundamental partition* and will be denoted by $I_0^*, I_1^*, \ldots, I_t^*$.

The lemma below is a straightforward result from e.g. [1] or [2].

Lemma 1. *To any simplex code D of length $n = 2^m - 1$ and $0 \leq dim(D) \leq m$, there is a partition of the set $\{0, 1, \ldots, n\}$,*

$$I_0^* \dot{\cup} I_1^* \dot{\cup} \ldots \dot{\cup} I_t^* = \{0, 1, \ldots, n\},$$

where $t = 2^{dim(D)} - 1$, such that the following conditions are satisfied:

$$\begin{array}{lllll} (i) & \mid I_0^* \mid & = \mid I_1^* \mid & = \ldots = \mid I_t^* \mid & = (n+1)/2^{dim(D)}, \\ (ii) & \bar{d} \in D & \Rightarrow & I_0^* \cap supp(\bar{d}) = \emptyset, & \\ (iii) & \bar{d} \in D & \Rightarrow & \text{either } I_i^* \subseteq supp(\bar{d}) \text{ or } I_i^* \cap supp(\bar{d}) = \emptyset, & i = 1, 2, \ldots, t. \end{array}$$

Another result concerning the extended fundamental partition to a simplex code is the following property, which is also a straightforward result from e.g. [1] or [2].

Proposition 4. *Let $D =< \bar{d}_1, \bar{d}_2, \ldots, \bar{d}_k >$ be a simplex code of length $n = 2^m - 1$ such that $dim(D) \leq m - 1$. Also, let the associated extended fundamental partition of D be denoted by $I_0^*, I_1^*, \ldots, I_t^*$. If $\bar{d} \notin D$ is a word such that $< \bar{d}_1, \bar{d}_2, \ldots, \bar{d}_k, \bar{d} >$ constitutes a simplex code, then for $i = 0, 1, \ldots, t$,*

$$\mid I_i^* \cap supp(\bar{d}) \mid \; = \; \mid I_0^* \mid /2.$$

Note, that if D is a simplex code of length $n = 2^m - 1$, then $0 \leq dim(D) \leq m$. Also note, that if C is a perfect code of length $n = 2^m - 1$, then the dimension of the simplex code $< C >^{\perp}$ equals m if and only if C is a Hamming code.

Example. The simplex code spanned by the two words of length seven in the matrix

$$\begin{pmatrix} 0\,0\,0\,1\,1\,1\,1 \\ 0\,1\,1\,0\,0\,1\,1 \end{pmatrix},$$

has the associated extended fundamental partition

$$I_0^* = \{0, 1\},\ I_1^* = \{2, 3\},\ I_2^* = \{4, 5\} \text{ and } I_3^* = \{6, 7\}.$$

Example. The simplex code spanned by the three words of length seven in the matrix

$$\begin{pmatrix} 1\,1\,1\,1\,0\,0\,0 \\ 1\,1\,0\,0\,1\,1\,0 \\ 1\,0\,1\,0\,1\,0\,1 \end{pmatrix},$$

is the dual of a Hamming code and has the associated extended fundamental partition

$$I_0^* = \{0\},\ I_1^* = \{1\},\ I_2^* = \{2\},\ I_3^* = \{3\},\ I_4^* = \{4\},\ I_5^* = \{5\},\ I_6^* = \{6\} \text{ and } I_7^* = \{7\}.$$

The following proposition is needed for our computer search in Section 7. We use some of the properties of simplex codes to prove it.

Proposition 5. *The number of different Hamming codes of length $n = 2^m - 1$ is*

$$\frac{n!}{(2^m - 2^0) \cdot (2^m - 2^1) \cdot (2^m - 2^2) \cdot \ldots \cdot (2^m - 2^{m-1})}\ .$$

Proof. The number of different parity-check matrices in the construction (2) on page 6, is equal to $n!$, since we have to order n different columns. Further, in general if A is any subspace of Z_2^n, then we may construct a base $\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_k$, $k = dim(A)$, of A by successively choosing

$$\bar{b}_1 \in A \setminus \{\bar{0}\}, \quad \bar{b}_2 \in A \setminus < \bar{b}_1 > \ , \ \ldots \ , \quad \bar{b}_k \in A \setminus < \bar{b}_1, \bar{b}_2, \ldots, \bar{b}_{k-1} > .$$

Thus, by elementary linear algebra, the number of ways to choose a base by the procedure above for a subspace A of Z_2^n equals

$$(2^{dim(A)} - 2^0) \cdot (2^{dim(A)} - 2^1) \cdot (2^{dim(A)} - 2^2) \cdot \ldots \cdot (2^{dim(A)} - 2^{dim(A)-1}). \tag{9}$$

From Hergert [8], we know that the subspace of Z_2^n generated by the rows of any parity-check matrix in the construction (2) is a simplex code. Hence, we may conclude that if $\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_k$ is a base of A, then the matrix

$$\begin{pmatrix} - & \bar{b}_1 & - \\ - & \bar{b}_2 & - \\ & \vdots & \\ - & \bar{b}_k & - \end{pmatrix}$$

is a parity-check matrix of a type that is used in the construction (2). The proposition is now proved.

The next lemma is a key result in the proof of Theorem 11 in Section 7. Observe that in this lemma the words $\bar{x}^{(1)}, \bar{x}^{(2)}, \ldots, \bar{x}^{((n+1)/2)}$ are not necessarily distinct.

Lemma 2. *Suppose D is a simplex code of length $n = 2^m - 1$ and $\bar{d} \in D \setminus \{\bar{0}\}$. Let $supp(\bar{d}) = \{i_1, i_2, \ldots, i_{(n+1)/2}\}$ and let j be a fixed integer in $\{0, 1, \ldots, n\} \setminus supp(\bar{d})$.*

If D' is a linear code of length n, with the property that for each $k = 1, 2, \ldots, (n+1)/2$ there is a word

$$\bar{x}^{(k)} = (x_{1k}, x_{2k}, \ldots, x_{nk}) \in D \cap D' \text{ such that } x^*_{i_k k} \neq x^*_{jk},$$

then $\bar{d} \in D'$

Proof. Suppose $\bar{d} \notin D'$. Then the fact that D' is a linear code implies that

$$< \bar{x}^{(1)}, \bar{x}^{(2)}, \ldots, \bar{x}^{((n+1)/2)} > \subsetneqq < \bar{x}^{(1)}, \bar{x}^{(2)}, \ldots, \bar{x}^{((n+1)/2)}, \bar{d} > \subseteqq D. \qquad (10)$$

Since every subspace of a simplex code is a simplex code we get that the linear code $< \bar{x}^{(1)}, \bar{x}^{(2)}, \ldots, \bar{x}^{((n+1)/2)} >$ is a simplex code with an associated extended fundamental partition $I_0^*, I_1^*, \ldots, I_t^*$. By (10),

$$dim(< \bar{x}^{(1)}, \bar{x}^{(2)}, \ldots, \bar{x}^{((n+1)/2)} >) < dim(D) \leq m.$$

Thus by Proposition 4 on page 12,

$$\mid supp(\bar{d}) \cap I_i^* \mid = \mid I_0^* \mid /2, \qquad i = 0, 1, 2, \ldots, t.$$

Hence there exists an element i_k of $supp(\bar{d})$ and a set I_s^* in the extended fundamental partition $I_0^*, I_1^*, \ldots, I_t^*$, such that $j, i_k \in I_s^*$. This implies that no word $\bar{x}^{(k)} \in D \cap D'$ exists such that

$$x_{i_k k}^* \neq x_{jk}^*,$$

which is a contradiction. The lemma is now proved.

Example. We use the same notation as in the lemma above. Assume that $\bar{d} = (1111000)$, $j = 0$ and D is the simplex code of length 7 generated by the rows in the following matrix:

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

Also, let D' be a linear code of length 7 in which there exist, not necessarily distinct, words $\bar{x}^{(1)}, \bar{x}^{(2)}, \bar{x}^{(3)}, \bar{x}^{(4)} \in D \cap D'$, such that

$$x_{11}^* \neq x_{01}^*, \quad x_{22}^* \neq x_{02}^*, \quad x_{33}^* \neq x_{03}^* \quad \text{and} \quad x_{44}^* \neq x_{04}^*.$$

Then by Lemma 2 above, the word $\bar{d} = (1111000) \in D'$.

4 Fourier coefficients

The technique with Fourier coefficients can be a very useful method when proving results concerning perfect codes. In Section 6 we will use this method to prove Theorem 8.

This section consists of two subsections. In the first subsection the basic definitions and results that we need concerning Fourier coefficients in connection with perfect codes in general are given. In the second subsection some more specific results on Fourier coefficients in connection with Hamming codes are given.

4.1 Fourier coefficients and perfect codes

Most of the material in this subsection is covered in [5] and [6].

We consider a group algebra $\mathbf{R}[x_1, x_2, \ldots, x_n]$. The elements in $\mathbf{R}[x_1, x_2, \ldots, x_n]$ are polynomials in n variables $x_1, x_2, \ldots, x_n$, over the real numbers $\mathbf{R}$. Thus, for any polynomial $r(x_1, x_2, \ldots, x_n)$ of $\mathbf{R}[x_1, x_2, \ldots, x_n]$,

$$r(x_1, x_2, \ldots, x_n) \quad = \quad \sum_{\bar{t} \in Z_2^n} r_{\bar{t}} x_1^{t_1} x_2^{t_2} \ldots x_n^{t_n},$$

where $\bar{t} = (t_1, t_2, \ldots, t_n)$ and $r_{\bar{t}} \in \mathbf{R}$.

The addition of polynomials in $\mathbf{R}[x_1, x_2, \ldots, x_n]$ is defined in the usual way. The multiplication of polynomials is defined by extending the multiplication of monomials to multiplication of polynomials in the usual way. If $(s_1, s_2, \ldots, s_n)$, $(t_1, t_2, \ldots, t_n) \in Z_2^n$, then

$$x_1^{s_1} x_1^{s_2} \ldots x_1^{s_n} \cdot x_1^{t_1} x_1^{t_2} \ldots x_1^{t_n} \quad = \quad x_1^{u_1} x_1^{u_2} \ldots x_1^{u_n},$$

where $u_i \equiv s_i + t_i \pmod 2$ for $i = 1, 2, \ldots, n$.

To connect Z_2^n with the group algebra above we represent any word in Z_2^n as a monomial in $\mathbf{R}[x_1, x_2, \ldots, x_n]$,

$$\bar{t} = (t_1, t_2, \ldots, t_n) \in Z_2^n \quad \longleftrightarrow \quad x_1^{t_1} x_2^{t_2} \ldots x_n^{t_n}.$$

A subset A of Z_2^n is represented by a polynomial $A(\bar{x})$ in $\mathbf{R}[x_1, x_2, \ldots, x_n]$. This polynomial will be

$$A(\bar{x}) \quad = \quad \sum_{\bar{t} \in A} x_1^{t_1} x_2^{t_2} \ldots x_n^{t_n}. \tag{11}$$

Example. Let A be the subset $\{000, 101, 111\}$ of Z_2^3, then

$$A(\bar{x}) \quad = \quad 1 + x_1 x_3 + x_1 x_2 x_3.$$

Now we define the set of polynomials in $\mathbf{R}[x_1, x_2, \ldots, x_n]$ needed in order to define the Fourier coefficient:

$$y_{\bar{t}}(\bar{x}) = \frac{1}{2^n} \prod_{i=1}^{n} (1 - x_i)^{t_i} (1 + x_i)^{1 - t_i},$$

where $\bar{t} = (t_1, t_2, \ldots, t_n)$ and $\bar{x} = (x_1, x_2, \ldots, x_n)$.

Example. If $\bar{t} = (101)$, then $y_{\bar{t}}(\bar{x})$ is equal to

$$\frac{1}{2^3}(1 - x_1)(1 + x_2)(1 - x_3) = \frac{1}{8}(1 - x_1 + x_2 - x_3 - x_1 x_2 + x_1 x_3 - x_2 x_3 + x_1 x_2 x_3).$$

We are now ready to define the Fourier coefficient for any subset of Z_2^n and to state the Propositions 6 - 11. The proofs of the Propositions 6, 7 and 9 - 11 may be found in e.g. [5] or [6].

Proposition 6. *The group algebra* $\mathbf{R}[x_1, x_2, \ldots, x_n]$ *defined above, may be considered as a vector space of dimension* 2^n *over the real numbers. Further, the set of polynomials* $\{y_{\bar{t}}(\bar{x}) \mid \bar{t} \in Z_2^n\}$*, constitutes a base for the vector space* $\mathbf{R}[x_1, x_2, \ldots, x_n]$.

Thus from the proposition above, we get that for any subset C of Z_2^n there is a unique subset of real numbers $A_{\bar{t}}(C)$, $\bar{t} \in Z_2^n$, such that

$$C(\bar{x}) \quad = \quad \sum_{\bar{t} \in Z_2^n} A_{\bar{t}}(C) y_{\bar{t}}(\bar{x}).$$

The coefficients $A_{\bar{t}}(C)$, $\bar{t} \in Z_2^n$ above, are the associated *Fourier coefficients* to the subset C.

Example. From the definition of $y_{\bar{t}}(\bar{x})$, we observe that

$$Z_2^n(\bar{x}) \quad = \quad (1 + x_1)(1 + x_2) \cdot \ldots \cdot (1 + x_n) \quad = \quad 2^n y_{\bar{0}}(\bar{x}). \tag{12}$$

Hence the Fourier coefficients of the set Z_2^n satisfy

$$A_{\bar{t}}(Z_2^n) = \begin{cases} 2^n & \text{if } \bar{t} = \bar{0}, \\ 0 & \text{if } \bar{t} \neq \bar{0}, \end{cases} \qquad \bar{t} \in Z_2^n.$$

Proposition 7. *For any* $\bar{t} \in Z_2^n$ *and any subset* C *of* Z_2^n*, the associated Fourier coefficient* $A_{\bar{t}}(C)$*, may be calculated by using the following formula:*

$$A_{\bar{t}}(C) = \mid \{\bar{c} \in C \mid \bar{c} \cdot \bar{t} = 0\} \mid - \mid \{\bar{c} \in C \mid \bar{c} \cdot \bar{t} = 1\} \mid .$$

The zero word is orthogonal to any word of Z_2^n, i.e. for any $\bar{t} \in Z_2^n$, $\bar{t} \cdot \bar{0} = 0$. Consequently $A_{\bar{t}}(C) \geq - \mid C \mid + 1$ for any subset C of Z_2^n where $\bar{0} \in C$. Further, for any subset C of Z_2^n, a word $\bar{t}$ is in the dual code of the linear span of C if and only if $\bar{t}$ is orthogonal to all words of C. Thus by Proposition 7, the following proposition is true.

Proposition 8. *For any* $\bar{t} \in Z_2^n$ *and any subset* C *of* Z_2^n*, such that* $\bar{0} \in C$*,*

$$- \mid C \mid +1 \quad \leq \quad A_{\bar{t}}(C) \quad \leq \quad \mid C \mid$$

and

$$\bar{t} \in < C >^{\perp} \quad \Longleftrightarrow \quad A_{\bar{t}}(C) \; = \; \mid C \mid .$$

Note that Corollary 1 in Section 2 gives that for any perfect code C of Z_2^n, $n = 2^m - 1$,

$$\mid C \mid \; = 2^{n-m}.$$

Proposition 9. *For any* $\bar{t} \in Z_2^n$ *and any subset* C *of* Z_2^n*, such that* $\bar{0} \in C$*,*

$$A_{\bar{t}}(C + \bar{e}_i) = \begin{cases} A_{\bar{t}}(C) & \textit{if } \; t_i = 0, \\ -A_{\bar{t}}(C) & \textit{if } \; t_i = 1, \end{cases} \qquad i = 1, 2, \ldots, n.$$

Note that for any perfect code C of Z_2^n, $n = 2^m - 1$, the corresponding Fourier coefficient $A_{\bar{0}}(C)$ equals 2^{n-m}.

The next proposition gives a very particular and important result concerning Fourier coefficients and perfect codes.

Proposition 10. *The Fourier coefficients of any perfect code C in Z_2^n satisfy,*

$$A_{\bar{t}}(C) = 0 \quad if \quad w(\bar{t}) \notin \{0, \frac{n+1}{2}\}.$$

Let for any subset C of Z_2^n, the set $\{\bar{t} \in Z_2^n \mid A_{\bar{t}}(C) \neq 0\}$ be denoted by $A(C)$.

Proposition 11. *For any perfect code C of length n,*

$$ker(C) =< A(C) >^{\perp} .$$

4.2 Fourier coefficients and Hamming codes

Proposition 12. *For any $\bar{t} = (t_1, t_2, \ldots, t_n) \in Z_2^n$ and any Hamming code C of length $n = 2^m - 1$,*

$$A_{\bar{t}}(C) = \begin{cases} 2^{n-m} & if \quad \bar{t} \in C^{\perp}, \\ 0 & if \quad \bar{t} \notin C^{\perp}, \end{cases}$$

and

$$A_{\bar{t}}(C + \bar{e}_i) = \begin{cases} 2^{n-m} & if \quad \bar{t} \in C^{\perp} \text{ and } t_i = 0, \\ -2^{n-m} & if \quad \bar{t} \in C^{\perp} \text{ and } t_i = 1, \\ 0 & if \quad \bar{t} \notin C^{\perp}, \end{cases} \qquad i = 1, 2, \ldots, n.$$

Proof. Note that $C = ker(C)$ for any Hamming code C. This implies by (6) on page 10 and Proposition 11, that $C =< \{\bar{t} \in Z_2^n \mid A_{\bar{t}}(C) \neq 0\} >^{\perp} = (C^{\perp})^{\perp}$. We thus get, by Proposition 8 and equation (8) on page 11 that

$$A_t(C) = 2^{n-m} \text{ if } \bar{t} \in C^{\perp} \quad \text{and} \quad A_t(C) = 0 \text{ if } \bar{t} \notin C^{\perp}.$$

The proposition now follows from Proposition 9.

Proposition 13. *If C is a perfect code of length $n = 2^m - 1$, such that*

$$A_{\bar{t}}(C) \in \{0, -2^{n-m}, 2^{n-m}\}$$

for all $\bar{t} \in Z_2^n$, then C is a translate of some Hamming code.

Proof. Without loss of generality we may assume that $\bar{0} \in C$, since by Proposition 9, we get that for any normal perfect code C' of length n and any $\bar{t} \in Z_2^n$

$$A_{\bar{t}}(C' + \bar{e}_i) \in \{-A_{\bar{t}}(C'), A_{\bar{t}}(C')\} \qquad i = 1, 2, \ldots, n\}.$$

We remind that $A(C) = \{\bar{t} \in Z_2^n \mid A_{\bar{t}}(C) \neq 0\}$. Further, equation (6) and Proposition 11 implies that $< A(C) >= ker(C)^{\perp}$.

Most trivially, as $\bar{0} \in C$, the subspace $ker(C)$ of Z_2^n is a subset of C. Now we assume that C is a non linear perfect code. This implies that $dim(ker(C)) \leq n - m - 1$. (In fact one can, as an easy exercise, prove that for any non linear perfect code C of length $n = 2^m - 1$, $dim(ker(C)) \leq n - m - 2$.) Consequently by Proposition 2 in Section 2

$$dim(< A(C) >) = dim(ker(C)^{\perp}) \geq m + 1.$$

Since $dim(< C >^{\perp}) \leq m - 1$ we get by the equation above that there exists a word $\bar{t} \in A(C)$ such that $\bar{t} \notin < C >^{\perp}$. Hence $A_{\bar{t}} \neq 0$ and by Proposition 8 and the fact that $\mid C \mid = 2^{n-m}$,

$$-2^{n-m} + 1 \leq A_{\bar{t}}(C) \leq 2^{n-m} - 1.$$

The proposition now follows from Proposition 12.

5 Disjunct perfect codes

Given two subsets A and B of Z_2^n, the *intersection number* of A and B is defined as

$$\eta(A, B) = \mid A \cap B \mid .$$

In this section we will obtain some results which deal with the question whether two perfect codes are disjunct or not disjunct. The results here will concern both Hamming codes and perfect codes in general.

In the rest of this thesis, even though we denote perfect codes as C_i and C_j where $i \neq j$, C_i and C_j does not necessarily have to be different perfect codes. Further, (since there only exists one normal perfect code of length 1 and one of length 3), we will henceforth only consider perfect codes of length $n \geq 7$.

5.1 Disjunct translates of Hamming codes

The key result in our investigations of maximal partial Hamming packings is Corollary 3 in this subsection. However, we need some more results before we prove that corollary.

The following results will be used in the proof of Lemma 3. For any Hamming code C of length $n = 2^m - 1$ and $i = 1, 2, \ldots, n$

$$< C + \bar{e}_i > \quad = \quad C \,\dot{\cup}\, (C + \bar{e}_i). \tag{13}$$

Hence $dim(< C + \bar{e}_i >) = n - m + 1$, and consequently by Proposition 2 in Section 2, we get that

$$dim(< C + \bar{e}_i >^{\perp}) \quad = \quad m - 1. \tag{14}$$

Let C be any Hamming code of length $n = 2^m - 1$. From the construction (2) on page 6, we also get that for any set of base vectors of $C^{\perp}$, there exists for each $i \in \{1, 2, \ldots, n\}$ a base vector $\bar{d}^{(i)}$ such that the $i : th$ coordinate of $\bar{d}^{(i)}$ equals 1. Define

$$D_i = \{(d_1, d_2, \ldots, d_n) \in C^{\perp} \mid d_i = 0\}, \quad i = 1, 2, \ldots, n.$$

The set D_i is a subspace of $C^{\perp}$ and we may conclude that $C^{\perp} = D_i \,\dot{\cup}\, (\bar{d}^{(i)} + D_i)$. We thus get that

$$\mid \{(d_1, d_2, \ldots, d_n) \in C^{\perp} \mid d_i = 0\} \mid \;=\; \mid \{(d_1, d_2, \ldots, d_n) \in C^{\perp} \mid d_i = 1\} \mid .$$

Hence from equation (14) and the fact that $dim(C^{\perp}) = m$, we get that

$$< C + \bar{e}_i >^{\perp} \quad = \quad \{\bar{x} \in C^{\perp} \mid x_i = 0\}. \tag{15}$$

Lemma 3. *Assume that C_i and C_j are any two Hamming codes of length $n = 2^m - 1$, where $i, j \in \{0, 1, \ldots, n\}$ and $i \neq j$. Then the following conditions are equivalent:*

$$\begin{array}{lllll} (i) & \eta(C_i + \bar{e}_i \ , \ C_j + \bar{e}_j) & \neq & 0, \\ (ii) & \eta(C_i + \bar{e}_i \ , \ C_j + \bar{e}_j) & = & \eta(C_i \cap C_j), \\ (iii) & < C_i + \bar{e}_i >^{\perp} \ \cap \ C_j^{\perp} & = & C_i^{\perp} \ \cap \ < C_j + \bar{e}_j >^{\perp} . \end{array}$$

Proof. The proof will be divided into two main cases. The first case deals with when $j = 0$. In the second case both i and j are non zero.

First we state some results that will be used in the proof of the first case. Let C and C' be any two Hamming codes of length n, not necessarily different, and let $i = 1, 2, \ldots, n$. By Proposition 3 of Section 2,

$$dim(< C + \bar{e}_i > \cap C') = n - dim(< C + \bar{e}_i >^{\perp}) - dim(C'^{\perp}) + dim(< C + \bar{e}_i >^{\perp} \cap C'^{\perp})$$

and

$$n \;=\; dim(C \cap C') \;+\; dim(C^{\perp}) \;+\; dim(C'^{\perp}) \;-\; dim(C^{\perp} \cap C'^{\perp}).$$

We know that $dim(C^{\perp}) = dim(C'^{\perp}) = m$ and $dim(< C + e_i >^{\perp}) = m - 1$, hence from the equations above we get that

$$dim(< C + \bar{e}_i > \cap C') = 1 + dim(C \cap C') - dim(C^{\perp} \cap C'^{\perp}) + dim(< C + \bar{e}_i >^{\perp} \cap C'^{\perp}). \tag{16}$$

Also, from equation (13), we may conclude that

$$< C + \bar{e}_i > \cap C' \;=\; (C \cap C') \;\;\dot{\cup}\;\; ((C + \bar{e}_i) \cap C').$$

Hence,

$$\eta(C + \bar{e}_i \ , \ C') \;=\; 2^{dim(< C + \bar{e}_i > \cap C')} \;-\; 2^{dim(C \cap C')}. \tag{17}$$

Case 1, $i \in \{1, 2, \ldots, n\}$ and $j = 0$: Assume

$$< C_i + \bar{e}_i >^{\perp} \ \cap \ C_0^{\perp} \ = \ C_i^{\perp} \ \cap \ C_0^{\perp}.$$

Then, by combining the equations (16) and (17), we get

$$\eta(C_i + \bar{e}_i \ , \ C_0) \ = \ 2^{dim(C_i \cap C_0)+1} \ - \ 2^{dim(C_i \cap C_0)} \ = \ \eta(C_i \ , \ C_0).$$

Now we assume that

$$< C_i + \bar{e}_i >^{\perp} \ \cap \ C_0^{\perp} \ \neq \ C_i^{\perp} \ \cap \ C_0^{\perp}.$$

Then, due to the fact that $< C_i + \bar{e}_i >^{\perp} \subsetneqq C_i^{\perp}$ and $dim(< C_i + \bar{e}_i >^{\perp}) = dim(C_i^{\perp}) - 1$, we may conclude that

$$dim(< C_i + \bar{e}_i >^{\perp} \cap C_0^{\perp}) = dim(C_i^{\perp} \cap C_0^{\perp}) - 1.$$

Thus by combining the equations (16) and (17),

$$\eta(C_i + \bar{e}_i \ , \ C_0) \ = \ 2^{dim(C_i \cap C_0)} \ - \ 2^{dim(C_i \cap C_0)} \ = \ 0.$$

We have now proved that in the case $j = 0$, the conditions $(i), (ii)$ and (iii) are equivalent.

Case 2, $i, j \in \{1, 2, \ldots, n\}$ where $i \neq j$: To prove the lemma in case 2, we divide this case into the following four different subcases:

(2.1) $$C_i^{\perp} \cap C_j^{\perp} \ = \ < C_i + \bar{e}_i >^{\perp} \cap C_j^{\perp} \ = \ C_i^{\perp} \cap < C_j + \bar{e}_j >^{\perp} .$$

(2.2) $$\begin{array}{rcl} C_i^{\perp} \cap C_j^{\perp} & = & < C_i + \bar{e}_i >^{\perp} \cap C_j^{\perp}, \\ C_i^{\perp} \cap C_j^{\perp} & \neq & C_i^{\perp} \cap < C_j + \bar{e}_j >^{\perp} . \end{array}$$

(2.3) $$\begin{array}{rcl} C_i^{\perp} \cap C_j^{\perp} & \neq & < C_i + \bar{e}_i >^{\perp} \cap C_j^{\perp}, \\ < C_i + \bar{e}_i >^{\perp} \cap C_j^{\perp} & = & C_i^{\perp} \cap < C_j + \bar{e}_j >^{\perp} . \end{array}$$

(2.4) $$\begin{array}{rcl} C_i^{\perp} \cap C_j^{\perp} & \neq & < C_i + \bar{e}_i >^{\perp} \cap C_j^{\perp}, \\ C_i^{\perp} \cap C_j^{\perp} & \neq & C_i^{\perp} \cap < C_j + \bar{e}_j >^{\perp}, \\ < C_i + \bar{e}_i >^{\perp} \cap C_j^{\perp} & \neq & C_i^{\perp} \cap < C_j + \bar{e}_j >^{\perp} . \end{array}$$

For any Hamming code C, the dual code of any translate of C is a subspace of the dual code of C. Thus we get the following implication

$$\begin{array}{c} < C_i + \bar{e}_i >^{\perp} \cap C_j^{\perp} = C_i^{\perp} \cap < C_j + \bar{e}_j >^{\perp} \ \Rightarrow \\ < C_i + \bar{e}_i >^{\perp} \cap < C_j + \bar{e}_j >^{\perp} = < C_i + \bar{e}_i >^{\perp} \cap C_j^{\perp} = C_i^{\perp} \cap < C_j + \bar{e}_j >^{\perp} . \end{array}$$

By the implication above, and due to the facts that for any Hamming code C of length n, $dim(C^{\perp}) = dim(< C + \bar{e}_i >^{\perp}) + 1$ and $< C + \bar{e}_i >^{\perp} \subsetneqq C^{\perp}$ for $i = 1, 2, \ldots, n$, we get

the following relations in the four subcases.

$$\begin{array}{lll} (2.1)\ dim(< C_i+\bar{e}_i >^{\perp} \cap < C_j+\bar{e}_j >^{\perp}) & = & dim(C_i^{\perp} \cap C_j^{\perp}). \\ (2.2)\ dim(< C_i+\bar{e}_i >^{\perp} \cap < C_j+\bar{e}_j >^{\perp}) & = & dim(C_i^{\perp} \cap C_j^{\perp}) - 1. \\ (2.3)\ dim(< C_i+\bar{e}_i >^{\perp} \cap < C_j+\bar{e}_j >^{\perp}) & = & dim(C_i^{\perp} \cap C_j^{\perp}) - 1. \\ (2.4)\ dim(< C_i+\bar{e}_i >^{\perp} \cap < C_j+\bar{e}_j >^{\perp}) & = & dim(C_i^{\perp} \cap C_j^{\perp}) - 2. \end{array}$$

With the same argument used to prove equation (16), we get that

$$\begin{array}{c} dim(< C_i+\bar{e}_i > \cap < C_j+\bar{e}_j >) = \\ 2 + dim(C_i \cap C_j) - dim(C_i^{\perp} \cap C_j^{\perp}) + dim(< C_i+\bar{e}_i >^{\perp} \cap < C_j+\bar{e}_j >^{\perp}). \end{array} \tag{18}$$

From (13) we may conclude that

$$< C_i+\bar{e}_i > \cap < C_j+\bar{e}_j >= (C_i \cap C_j) \dot{\cup} ((C_i+\bar{e}_i) \cap C_j) \dot{\cup} (C_i \cap (C_j+\bar{e}_j)) \dot{\cup} ((C_i+\bar{e}_i) \cap (C_j+\bar{e}_j)).$$

Hence,

$$\eta(C_i+\bar{e}_i, C_j+\bar{e}_j) = 2^{dim(<C_i+\bar{e}_i> \cap <C_j+\bar{e}_j>)} - \eta(C_i, C_j) - \eta(C_i+\bar{e}_i, C_j) - \eta(C_i, C_j+\bar{e}_j). \tag{19}$$

Now, by combining (18) and (19) in the four subcases (2.1), (2.2), (2.3) and (2.4) we get the following relations:

$$\begin{array}{llll} (2.1) & \eta(C_i+\bar{e}_i\ , C_j+\bar{e}_j) = \eta(C_i, C_j) & \text{and} & < C_i+\bar{e}_i >^{\perp} \cap C_j^{\perp} = C_i^{\perp} \cap < C_j+\bar{e}_j >^{\perp}. \\ (2.2) & \eta(C_i+\bar{e}_i\ , C_j+\bar{e}_j) = 0 & \text{and} & < C_i+\bar{e}_i >^{\perp} \cap C_j^{\perp} \neq C_i^{\perp} \cap < C_j+\bar{e}_j >^{\perp}. \\ (2.3) & \eta(C_i+\bar{e}_i\ , C_j+\bar{e}_j) = \eta(C_i, C_j) & \text{and} & < C_i+\bar{e}_i >^{\perp} \cap C_j^{\perp} = C_i^{\perp} \cap < C_j+\bar{e}_j >^{\perp}. \\ (2.4) & \eta(C_i+\bar{e}_i\ , C_j+\bar{e}_j) = 0 & \text{and} & < C_i+\bar{e}_i >^{\perp} \cap C_j^{\perp} \neq C_i^{\perp} \cap < C_j+\bar{e}_j >^{\perp}. \end{array}$$

The lemma is proved.

Note that in the lemma above and in the theorem below and its corollary, the Hamming codes C_i and C_j, $i \neq j$, are not necessarily distinct.

Theorem 2. *Let C_i and C_j be any two Hamming codes of length n, and i, j two different elements of the set $\{0, 1, \ldots, n\}$. Then $\eta(C_i+e_i, C_j+e_j) = 0$ if and only if there exists a word $\bar{x} \in C_i^{\perp} \cap C_j^{\perp}$ such that $x_i^* \neq x_j^*$.*

Proof. From (15) on page 19, for any Hamming code C of length n,

$$< C+\bar{e}_k >^{\perp} = \{\bar{x} \in C^{\perp} \mid x_k^* = 0\}, \quad k = 0, 1, \ldots, n.$$

Thus we get that

$$< C_i+e_i >^{\perp} \cap C_j^{\perp} = \{\bar{x} \in C_i^{\perp} \cap C_j^{\perp} \mid x_i^* = 0\}$$

and

$$C_i^{\perp} \cap < C_j+e_j >^{\perp} = \{\bar{x} \in C_i^{\perp} \cap C_j^{\perp} \mid x_j^* = 0\}.$$

This implies that there exists a word $\bar{x} \in C_i^{\perp} \cap C_j^{\perp}$ such that

$$x_i^* \neq x_j^* \quad \Longleftrightarrow \quad < C_i + e_i >^{\perp} \cap C_j^{\perp} \neq C_i^{\perp} \cap < C_j + e_j >^{\perp} .$$

The theorem now follows from Lemma 3.

An immediate consequence of Theorem 2 is Corollary 3 below. This corollary is fundamental for our investigations of partial Hamming packings.

The following definition will be used in the corollary below. For any family of normal perfect codes $C_0, C_1, \ldots, C_k$ of length n, where $k \leq n$, and any permutation π of $\{0, 1, \ldots, n\}$ let the set S_{ij} be defined for each pair $i, j \in \{0, 1, \ldots, k\}$, $i \neq j$, as

$$S_{ij} \;=\; \{\bar{x} \in < C_i >^{\perp} \cap < C_j >^{\perp} |\; x^*_{\pi(i)} \neq x^*_{\pi(j)}\}. \tag{20}$$

Corollary 3. *Consider any family $\mathcal{S}$ of Hamming codes $C_0, C_1, \ldots, C_k$ of length n, $k \leq n$, and any permutation π of $\{0, 1, \ldots, n\}$. The family $\mathcal{S}$ and the permutation π constitute a partial Hamming packing, $PHP(C_0, C_1, \ldots, C_k; \pi; n)$, if and only if for each pair $i, j \in \{0, 1, \ldots, k\}$, $i \neq j$, the associated set $S_{ij} \neq \emptyset$.*

5.2 Disjunct translates of perfect codes in general

As mentioned before, in his thesis [8], Hergert shows that if C is a perfect code, then $< C >^{\perp}$ is a simplex code. It would therefore be interesting to know if Theorem 2 is also valid for non linear perfect codes.

In this subsection we will show that the ($\Leftarrow$) - implication of Theorem 2 is true in general for all perfect codes. This will be proved by using Theorem 3 below. We will here also show that the ($\Rightarrow$) - implication of Theorem 2 is not true in general for all perfect codes. This will be proved by an example where we use the construction of Vasil'ev codes [15].

In [7], the following theorem was showed by Heden. We state it for the extended fundamental partition instead of the fundamental partition as in [7].

Theorem 3. *Let L be a simplex code in Z_2^n, $L \supsetneq \{\bar{0}\}$, with an associated extended fundamental partition consisting of the sets $I_0^*, I_1^*, \ldots, I_t^*$.*

If $C_0, C_1, \ldots, C_t$ are any normal perfect codes in Z_2^n satisfying

$$L \;\subseteq\; < C_j >^{\perp}, \qquad j = 0, 1, 2, \ldots, t$$

then the family $\mathcal{S}$ of $n + 1$ perfect codes $C_j + \bar{e}_i$, where $i \in I_j^*$ for $j = 0, 1, \ldots, t$, constitutes a partition of the set Z_2^n.

A special case of the theorem above is when $L = \{\bar{0}, \bar{x}\}$ is a simplex code of dimension one, C_0 and C_1 are normal perfect codes of length n and L is a subspace of $< C_0 >^{\perp} \cap < C_1 >^{\perp}$. The associated extended fundamental partition to L is

$$I_0^* = \{0, 1, \ldots, n\} \setminus supp(\bar{x}) \quad \text{and} \quad I_1^* = supp(\bar{x})$$

In this case, by Theorem 3 above, the family $\mathcal{S}$ of perfect codes,

$$\mathcal{S} = \{C_0 + \bar{e}_i \mid i \in I_0^*\} \dot{\cup} \{C_1 + \bar{e}_i \mid i \in I_1^*\},$$

constitutes a partition of Z_2^n. Hence the ($\Leftarrow$) - implication of Theorem 2 is true for every perfect code. Thus the following theorem is valid.

Theorem 4. *Assume that C_i and C_j are any two normal perfect codes of length n and assume $i, j \in \{0, 1, \ldots, n\}$, where $i \neq j$. If there exists a word $\bar{x} \in < C_i >^{\perp} \cap < C_j >^{\perp}$ such that $x_i^* \neq x_j^*$, then $(C_i + \bar{e}_i) \cap (C_j + \bar{e}_j) = \emptyset$.*

However, the ($\Rightarrow$) - implication of Theorem 2 is not true in general for perfect codes, as will be illustrated by some examples below. In these examples the lengths of the perfect codes will be at least 15.

Let C be any non linear normal perfect code and $I_0^*, I_1^*, \ldots, I_t^*$ be the extended fundamental partition associated with $< C >^{\perp}$. We know from equation (8) on page 11, that the dimension of $< C >^{\perp}$ is smaller than or equal to $m-1$. Thus, by Lemma 1 in Section 2,

$$\mid I_k^* \mid \ \geq \ 2, \qquad k = 0, 1, 2, \ldots, t.$$

Hence, there exist for example in I_0^*, different elements i, j such that $(C+\bar{e}_i) \cap (C+\bar{e}_j) = \emptyset$. However, there does not exist any word $\bar{x} \in < C >^{\perp}$ such that $x_i^* \neq x_j^*$. Therefore the ($\Rightarrow$) - implication of Theorem 2 is not true if we take $C_i = C$ and $C_j = C$.

The ($\Rightarrow$) - implication of Theorem 2 is obviously not true for two disjunct translates of different normal perfect codes of full rank codes. However, this ($\Rightarrow$) - implication is not even true in general when C_i and C_j are different normal perfect codes, where $dim(< C_i >^{\perp}) = dim(< C_j >^{\perp}) = m-1$, as will be shown by the example below. In this example we will use the construction of Vasil'ev from 1962, see [15]. This construction was the first example of a non linear perfect code.

Theorem 5. *(Vasil'ev) For any perfect code C of length n and for any function $\lambda : \ C \rightarrow Z_2$, the following set is a perfect code of length $2n + 1$:*

$$V(C, \lambda) = \{(\bar{x} \mid \bar{x} + \bar{c} \mid \sigma(\bar{x}) + \lambda(\bar{c})) \mid \bar{x} \in Z_2^n, \bar{c} \in C\},$$

where $\sigma(\bar{x}) \equiv x_1 + x_2 + \ldots + x_n \pmod 2$.

Example. We will construct two non linear Vasil'ev codes of length $2n-1$, $V(C_0, \lambda_0)$ and $V(C_i, \lambda_i)$, where i is a fixed integer in the set {1,2,...,n}, such that

$$< V(C_0, \lambda_0) >^{\perp} \cap < V(C_i, \lambda_i) >^{\perp} = \{\bar{0}\}$$

and

$$V(C_0, \lambda_0) \cap (V(C_i, \lambda_i) + \bar{e}_{n+i}) = \emptyset.$$

In [3], Etzion and Vardy proved that for each $m \geq 3$, there exist two Hamming codes C, C' of length $n = 2^m - 1$, such that

$$\eta(C, C') \quad = \quad 2^{n-r} \qquad \text{for} \qquad r = m+1, m+2, \ldots, 2m.$$

Let i be a fixed integer in $i \in \{1, 2, \ldots, n\}$ and let C_0 and C_i denote any two Hamming codes of the length $n = 2^m - 1$, where $m \in \{3, 4, \ldots\}$, such that $\eta(C_0, C_i) = 2^{n-2m}$. Then by Proposition 3 in Section 2, $C_0^{\perp} \cap C_i^{\perp} = \{\bar{0}\}$. This implies that

$$C_0^{\perp} \cap C_i^{\perp} \quad = \quad C_0^{\perp} \cap < C_i + \bar{e}_i >^{\perp},$$

since $\{\bar{0}\} \subseteqq < C_i + \bar{e}_i >^{\perp} \subseteqq C_i^{\perp}$. Thus, by Proposition 3 in Section 2 and Lemma 3,

$$\eta(C_0, C_i + \bar{e}_i) \quad = \quad \eta(C_0, C_i) \quad = \quad 2^{n - dim(C_0^{\perp}) - dim(C_i^{\perp}) + dim(C_0^{\perp} \cap C_i^{\perp})} \quad = \quad 2^{n-2m}. \qquad (21)$$

Now we define the functions $\lambda_0 : C_0 \to Z_2$ and $\lambda_i : C_i \to Z_2$ as follows:

$$\lambda_0(\bar{c}) = \begin{cases} 0 & \text{if} \quad \bar{c} = \bar{0}, \\ 1 & \text{else}, \end{cases}$$

and

$$\lambda_i(\bar{c}) = \begin{cases} 0 & \text{if} \quad \bar{c} = \bar{0}, \\ 0 & \text{if} \quad \bar{c} + \bar{e}_i \in C_0, \\ 1 & \text{else}. \end{cases}$$

Assume that there exist a word $(\bar{x} \mid \bar{x} + \bar{c} \mid \sigma(\bar{x}) + \lambda_0(\bar{c})) \in V(C_0, \lambda_0)$ and a word $(\bar{x}' \mid \bar{x}' + \bar{c}' \mid \sigma(\bar{x}') + \lambda_i(\bar{c}')) \in V(C_i, \lambda_i)$ such that

$$(\bar{x} \mid \bar{x} + \bar{c} \mid \sigma(\bar{x}) + \lambda_0(\bar{c})) \quad = \quad (\bar{x}' \mid \bar{x}' + \bar{c}' \mid \sigma(\bar{x}') + \lambda_i(\bar{c}')) + \bar{e}_{n+i}.$$

Then $\bar{x} = \bar{x}'$ and $\bar{c} = \bar{c}' + \bar{e}_i$. Consequently, as evidently $\bar{c} \neq \bar{0}$ and $\bar{c}' + \bar{e}_i \in C_0$,

$$\sigma(\bar{x}) + \lambda_0(\bar{c}) = \sigma(\bar{x}) + 1 \neq \sigma(\bar{x}) + 0 = \sigma(\bar{x}') + \lambda_i(\bar{c}').$$

This is a contradiction, and we may therefore conclude that

$$V(C_0, \lambda_0) \quad \cap \quad (V(C_i, \lambda_i) + \bar{e}_{n+i}) \quad = \quad \emptyset.$$

Trivially, for any Hamming code C of length $n = 2^m - 1$, the rank of the Vasil'ev code $V(C, \lambda)$ equals $2n + 1 - m$ if and only if λ is a non linear map, see e.g. [1].

By equation (21), we get that the cardinality of the set $\{\bar{c} \in C_i \mid \lambda_i(\bar{c}) = 0\}$ is $2^{n-2m}+1$. This cardinality is not a divisor of $2^n =\mid Z_2^n \mid$. Hence, by elementary linear algebra, the set $\{\bar{c} \in C_i \mid \lambda_i(\bar{c}) = 0\}$ is not a subspace of Z_2^n, and clearly the function λ_i is non linear. Similarly we get that the function λ_0 is also a non linear function.

By [1], if C is a Hamming code of length $n = 2^m - 1$ and $V(C, \lambda)$ is non linear, then $dim(< V(C, \lambda) >) = 2n+1-m$. Hence from Proposition 2 in Section 2, we may conclude that

$$dim(< V(C_0, \lambda_0) >^{\perp}) \quad = \quad dim(< V(C_i, \lambda_i) >^{\perp}) \quad = \quad m.$$

Therefore, by a straightforward verification, we get that the following m-dimensional subspaces of Z_2^{2n+1}, $\{(\bar{c} \mid \bar{c} \mid 0) \mid \bar{c} \in C_0^{\perp}\}$ and $\{(\bar{c}' \mid \bar{c}' \mid 0) \mid \bar{c}' \in C_i^{\perp}\}$, are the dual codes of the Vasil'ev codes $V(C_0, \lambda_0)$ and $V(C_i, \lambda_i)$ respectively. Hence

$$< V(C_0, \lambda_0) >^{\perp} \cap < V(C_i, \lambda_i) >^{\perp} = \{\bar{0}\}.$$

6 Lower and upper bounds for the packing numbers

Although the main focus of this thesis is on partial Hamming packings, some of the results will also concern partial packings in general. The main results in this section are Corollary 4 and Corollary 6 that give a lower respectively an upper bound for the packing numbers of maximal strictly partial Hamming packings. Further, in this section we also give a trivial lower bound and a non trivial upper bound for the packing numbers of maximal strictly partial packings.

6.1 Lower bounds

The lemma below will be used to get a lower bound for the packing numbers of maximal strictly partial Hamming packings.

We remind the definition of S_{ij} in equation (20) on page 22, where we defined S_{ij} for any $PP(C_0, C_1, \ldots, C_k; \pi; n)$ as

$$S_{ij} \;=\; \{\bar{x} \in C_i^{\perp} \cap C_j^{\perp} \mid x^*_{\pi(i)} \neq x^*_{\pi(j)}\}, \qquad i, j \in \{0, 1, \ldots, k\} \quad \text{and} \quad i \neq j.$$

Lemma 4. *Consider any $PP(C_0, C_1, \ldots, C_k; \pi; n)$, where $n = 2^m - 1$. Assume that there exists a simplex code D of length n and an element i of $\{0, 1, \ldots, k\}$, such that*

$$D \cap S_{ij} \neq \emptyset \quad \textit{for} \quad j = \{0, 1, \ldots, i-1, i+1, \ldots, k\}.$$

Let $s = (n+1)/ \mid D \mid$. Then there exists a permutation π' of $\{0, 1, \ldots, n\}$, such that the family of perfect codes

$$C_0 + \bar{e}_{\pi'(0)}, C_1 + \bar{e}_{\pi'(1)}, \ldots, C_k + \bar{e}_{\pi'(k)}, C_i + \bar{e}_{\pi'(k+1)}, \ldots, C_i + \bar{e}_{\pi'(k+s-1)},$$

constitutes a partial packing of Z_2^n, where $\pi'(l) = \pi(l)$ if $l \in \{0, 1, \ldots, k\}$.

Proof. Suppose D is a simplex code of length n and i is an element of the set $\{0, 1, \ldots, k\}$, such that

$$D \cap S_{ij} \neq \emptyset \quad \text{for} \quad j = 0, 1, \ldots, i-1, i+1, \ldots, k.$$

Then by Lemma 1 in Section 3, D has an associated extended fundamental partition $I_0^*, I_1^*, \ldots, I_t^*$, where

$$\mid I_0^* \mid \;=\; \mid I_1^* \mid \;=\; \ldots \;=\; \mid I_t^* \mid \;=\; (n+1)/ \mid D \mid .$$

Hence, for any $j \in \{0, 1, \ldots, k\}$, there exists a unique set $I^*_{r(i)}$ in the extended fundamental partition above, such that

$$\pi(j) \in I^*_{r(i)} \quad \text{if and only if} \quad j = i.$$

We thus get, by Theorem 4 in Section 5, that for each $\mu \in I^*_{r(i)}$ and each $j \in \{0, 1, \ldots, k\} \setminus \{i\}$

$$(C_i + \bar{e}_{\mu}) \cap (C_j + \bar{e}_{\pi(j)}) \;=\; \emptyset.$$

Now, let π' be a permutation of $\{0, 1, \ldots, n\}$ such that

$$\pi'(l) = \begin{cases} \pi(l) & \text{if } \ l \in \{0, 1, \ldots, k\}, \\ \in I^*_{r(i)} \setminus \{\pi(i)\} & \text{if } \ l \in \{k+1, k+2, \ldots, k+s-1\}. \end{cases}$$

Also, let

$$C_{k+1} \ = \ C_{k+2} \ = \ \ldots \ = \ C_{k+s-1} \ = \ C_i.$$

Then we have a partial packing, $PP(C_0, C_1, \ldots, C_{k+s-1}; \pi'; n)$, (note that this partial packing not necessarily is maximal). The lemma is proved.

Theorem 6. *Consider any $PHP(C_0, C_1, \ldots, C_k; \pi; n)$, where $n = 2^m - 1$ and $0 \leq k \leq m-1$. Let $t = 2^{m-k} - 1$. Then for any $i \in \{0, 1, \ldots, k\}$ there exist elements $q_1^{(i)}, q_2^{(i)}, \ldots, q_t^{(i)}$ of $\{0, 1, \ldots, n\}$, such that the family of translates of Hamming codes*

$$C_0 + \bar{e}_{\pi(0)}, C_1 + \bar{e}_{\pi(1)}, \ldots, C_k + \bar{e}_{\pi(k)}, C_i + \bar{e}_{q_1^{(i)}}, \ldots, C_i + \bar{e}_{q_t^{(i)}},$$

constitutes a partial Hamming packing of Z_2^n.

Proof. Since the family of all translates of a Hamming code constitutes a partial Hamming packing of Z_2^n, the theorem is immediately true when $k = 0$.

Consider any $PHP(C_0, C_1, \ldots, C_k; \pi; n)$, where $n = 2^m - 1$ and $1 \leq k \leq m - 1$. (We remind from equation (20) on page 22, that the set S_{ij} is defined for each pair $i, j \in \{0, 1, \ldots, k\}$, $i \neq j$, as

$$S_{ij} \ = \ \{\bar{x} \in C_i^{\perp} \cap C_j^{\perp} \mid x^*_{\pi(i)} \neq x^*_{\pi(j)}\}.)$$

Then, by Corollary 3 in Section 5, each of the sets S_{ij}, $i, j \in \{0, 1, \ldots, k\}$ and $i \neq j$, are non empty. Now, for $i = 0, 1, \ldots, k$, take any set

$$D_i \ = \ < \bar{x}_0, \bar{x}_1, \ldots, \bar{x}_{i-1}, \bar{x}_{i+1}, \ldots, \bar{x}_k >, \qquad \bar{x}_j \in S_{ij}, \ j \in \{0, 1, \ldots, k\} \setminus \{i\}.$$

The set D_i is a subspace of $C_i^{\perp}$ and consequently a simplex code. Further, for $i = 0, 1, \ldots, k$,

$$D_i \cap S_{ij} \ \neq \ \emptyset, \qquad j = 0, 1, \ldots, i-1, i+1, \ldots, k.$$

Hence, the theorem now follows from Lemma 4.

The corollary below gives a lower bound for the packing numbers of maximal strictly partial Hamming packings.

Corollary 4. *The packing number p of any maximal strictly partial Hamming packing of Z_2^n, $n = 2^m - 1$, satisfies*

$$p \ \geq \ m + 1.$$

Proof. For any $PHP(C_0, C_1, \ldots, C_k; \pi; n)$ with $k < m$, Theorem 6 implies that the partial Hamming packing is not maximal, since $2^{m-k} - 1 \geq 1$.

For the packing numbers of maximal strictly partial packings in general we have not found any non trivial lower bound. Note that if C is any perfect code, then the sets of words in two different translates of C are disjunct. Clearly, a trivial and immediate lower bound for the packing numbers of maximal strictly partial packings of any Z_2^n, $n = 2^m - 1$, is two.

6.2 Upper bounds

The following theorem is a consequence of the definition of perfect codes and we will use this theorem to give an upper bound for the packing numbers of maximal strictly partial Hamming packings and maximal strictly partial packings.

Theorem 7. *For any partial packing, $PP(C_0, C_1, \ldots, C_{n-1}; \pi; n)$, the set*

$$C \quad = \quad Z_2^n \setminus \bigcup_{i=0}^{n-1} (C_i + \bar{e}_{\pi(i)})$$

is a perfect code.

Proof. Take any word $\bar{x} \in Z_2^n$. By the definition of a perfect code, see page 5, there exists for each $i = 0, 1, \ldots, n-1$ a unique word $\bar{x}_i \in C_i + \bar{e}_{\pi(i)}$ such that $\bar{x}_i \in S_1(\bar{x})$. Since the sets $C_0 + \bar{e}_{\pi(0)}, C_1 + \bar{e}_{\pi(1)}, \ldots, C_{n-1} + \bar{e}_{\pi(n-1)}$ are mutually disjoint, we get that the words $\bar{x}_0, \bar{x}_1, \ldots, \bar{x}_{n-1}$ are distinct. Hence

$$| \, C \cap S_1(\bar{x}) \, | \quad = \quad | \, S_1(\bar{x}) - \{\bar{x}_0, \bar{x}_1, \ldots, \bar{x}_{n-1}\} \, | \quad = \quad n + 1 - n \quad = \quad 1.$$

This implies that there exists a unique word $\bar{c} \in C$ such that $\bar{c} \in S_1(\bar{x})$. Consequently, by the definition of a perfect code, the set C is a perfect code.

An immediate consequence of the theorem above is the following corollary that gives a non trivial upper bound for the packing numbers of maximal strictly partial packings.

Corollary 5. *The packing number p of any maximal strictly partial packing of Z_2^n, satisfies*

$$p \quad \leq \quad n - 1.$$

Proof. We remind that the packing number for any maximal strictly partial packing of length n is smaller than $n + 1$. By Theorem 7, any $PHP(C_0, C_1, \ldots, C_k; \pi; n)$ with the packing number equal to n is not maximal.

However, we can prove that the same upper bound is true for the packing numbers of maximal strictly partial Hamming packings. This is a consequence of the following theorem.

Theorem 8. *For any partial Hamming packing, $PHP(C_0, C_1, \ldots, C_{n-1}; \pi; n)$, where $n = 2^m - 1$, the set*

$$C \quad = \quad Z_2^n \setminus \bigcup_{i=0}^{n-1} (C_i + \bar{e}_{\pi(i)})$$

is a translate of some Hamming code.

Proof. By Theorem 7, C is a perfect code. Now we will prove that C is a translate of some Hamming code by using the technique with Fourier coefficients.

If A and B are two disjunct subsets of Z_2^n represented by the polynomials $A(\bar{x})$ respectively $B(\bar{x})$ in the group algebra $\mathbf{R}[x_1, x_2, \ldots, x_n]$, see (11) on page 15, then the set $A \dot{\cup} B$ may be represented by

$$(A \dot{\cup} B)(\bar{x}) \quad = \quad A(\bar{x}) + B(\bar{x}).$$

Hence from the fact that the perfect codes

$$C_0 + \bar{e}_{\pi(0)}, C_1 + \bar{e}_{\pi(1)}, \ldots, C_{n-1} + \bar{e}_{\pi(n-1)}$$

constitute a partial packing of Z_2^n, we may conclude that

$$Z_2^n(\bar{x}) \quad = \quad C(\bar{x}) + (C_0 + \bar{e}_{\pi(0)})(\bar{x}) + (C_1 + \bar{e}_{\pi(1)})(\bar{x}) + \ldots + (C_{n-1} + \bar{e}_{\pi(n-1)})(\bar{x}). \quad (22)$$

Further, from Proposition 12 in Section 4, for any $\bar{t} \in Z_2^n$

$$A_{\bar{t}}(C_i + \bar{e}_{\pi(i)}) = \begin{cases} 2^{n-m} \cdot (-1)^{(\bar{t} \, \cdot \, \bar{e}_{\pi(i)})} & \text{if} \quad \bar{t} \in C^{\perp}, \\ 0 & \text{if} \quad \bar{t} \notin C^{\perp}, \end{cases} \qquad i = 0, 1, \ldots, n-1.$$

Hence for $i = 0, 1, \ldots, n-1$,

$$(C_i + \bar{e}_{\pi(i)})(\bar{x}) = 2^{n-m} \sum_{\bar{t} \in C_i^{\perp}} (-1)^{(\bar{t} \, \cdot \, \bar{e}_{\pi(i)})} \cdot y_{\bar{t}}(\bar{x}). \quad (23)$$

From equation (12) on page 16, we get that $Z_2^n(\bar{x}) = 2^n y_{\bar{0}}(\bar{x})$. Further, by Proposition 7 and 9 in Section 4, $\mid A_{\bar{t}}(C) \mid \leq 2^{n-m}$.

Thus, by combining the results in the paragraph above, equation (22) and equation (23), we may conclude that

$$A_{\bar{t}}(C) \neq 0 \quad \Rightarrow \quad \mid A_{\bar{t}}(C) \mid = 2^{n-m}, \qquad \bar{t} \in Z_2^n.$$

The theorem now follows from Proposition 13 in Section 4.

The corollary below gives an upper bound for the packing numbers of maximal strictly partial Hamming packings.

Corollary 6. *The packing number p of any maximal strictly partial Hamming packing of Z_2^n, satisfies*

$$p \quad \leq \quad n - 1.$$

Proof. We remind that the packing number for any maximal strictly partial Hamming packing of length n is smaller than $n + 1$. By Theorem 8, any $PHP(C_0, C_1, \ldots, C_k; \pi; n)$ with the packing number equal to n is not maximal.

7 Maximal strictly partial Hamming packings

In this section we give some existence results for the packing numbers of maximal strictly partial Hamming packings of Z_2^n. The section is divided into two subsections.

In the first subsection the results will consider maximal strictly partial Hamming packings of Z_2^7 and Z_2^{15}. For these cases, by use of a computer, we give a complete solution for the spectrum of the packing numbers.

In the second subsection we give a more general result that consider maximal strictly partial Hamming packings of Z_2^n, where $n \geq 15$. However, our result does not give a complete solution on the spectrum of the packing numbers.

Note that by Corollary 4 and Corollary 6 in Section 6, we get that the packing number p for any maximal strictly partial Hamming packing of Z_2^n, $n = 2^m - 1$, satisfies

$$m + 1 \leq p \leq n - 1. \tag{24}$$

7.1 A computer search for maximal strictly partial Hamming packings of Z_2^7 and Z_2^{15}

The maximal strictly partial Hamming packings we get by the computer search are given in Appendix A. Further, we should remark that although the programming we use for our computer search has been carefully tested it is still possible that errors may have occurred. However, due to our tests, *we* are convinced that the results are true.

In the programming every Hamming code is represented by a parity-check matrix, see construction (2) on page 6. One problem with the programming was how to enumerate these matrices such that each Hamming code is represented just one time. (In fact, every Hamming code of length 7 can be represented by $7 \cdot 6 \cdot 4 = 168$ different parity-check matrices and every Hamming code of length 15 can be represented by $15 \cdot 14 \cdot 12 \cdot 8 = 20160$ different parity-check matrices, see equation (9) on page 13.)

7.1.1 Maximal strictly partial Hamming packings of Z_2^7

By Proposition 5 in Section 3, there are 30 Hamming codes of length 7. To enumerate these Hamming codes we will divide the corresponding set of dual codes into two classes: class $A1$ and class $A2$. Each dual code is represented by a parity-check matrix of the corresponding Hamming code. This representation is described and discussed below.

Parity-check matrices. The matrices in the classes $A1$ and $A2$ are all parity-check matrices of respective type which satisfy the construction (2) on page 6, i.e. the seven columns of the matrix consist of all non zero words of Z_2^3. Below, $- = 0$ or 1.

$$\text{Class } A1: \quad \begin{pmatrix} 0 & 0 & 1 & - & - & - & - \\ 0 & 1 & 0 & - & - & - & - \\ 1 & 0 & 0 & - & - & - & - \end{pmatrix}$$

$$\text{Class } A2: \quad \begin{pmatrix} 0 & 0 & 0 & 1 & - & - & - \\ 0 & 1 & 1 & 0 & - & - & - \\ 1 & 0 & 1 & 0 & - & - & - \end{pmatrix}$$

We will now show that with the matrices above we may enumerate all Hamming codes of length 7 in a unique way. Hence, we have to prove that the matrices in $A1$ and $A2$ generate different subspaces of Z_2^7 and that the number of matrices in $A1$ and $A2$ is 30.

Since the words $(0,0,1)$, $(0,1,0)$ and $(1,0,0)$ are independent, we get that there exists only one word of each type $(0,0,1,-,-,-,-)$, $(0,1,0,-,-,-,-)$ and $(1,0,0,-,-,-,-)$ in any subspace generated by the rows of a matrix in the class $A1$. Consequently, if H and H' are different matrices in $A1$, then at least one of the words $(0,0,1,-,-,-,-)$, $(0,1,0,-,-,-,-)$ and $(1,0,0,-,-,-,-)$ in the subspace generated by the rows of H is not contained in the subspace that the rows of H' generates. We thus get that all the subspaces generated by the matrices in $A1$ are different.

With the same arguments as in the paragraph above, we get that all the subspaces generated by the matrices in the class $A2$ are different, since the words $(0,0,-,1)$, $(0,1,-,0)$ and $(1,0,-,0)$ are independent.

There exists only one word of type $(0,0,0,-,-,-,-)$ in the subspace generated by any matrix in the class $A1$. As the words $(0,0,1)$, $(0,1,0)$ and $(1,0,0)$ are independent, this word must be the zero word, $(0,0,0,0,0,0,0)$. Hence, the word of type $(0,0,0,1,-,-,-)$ that exists in the subspace generated by any matrix in $A2$ is not a member of the subspace generated by any matrix in $A1$. This implies that the generated subspaces of the matrix in $A1$ and the generated subspaces of the matrix in $A2$ are different. Consequently, all the generated subspaces of the matrices in $A1$ and $A2$ are different.

The number of matrices in $A1$ plus the number of matrices in $A2$ equals $4! + 3! = 30$.

Algorithm. The algorithm computes, maximal strictly partial Hamming packings, $PHP(C_0, C_1, \ldots, C_k; id; 7)$, with packing number 4, 5 or 6 if such exist. The permutation id is the identity permutation, i.e. $id(i) = i$ for $i = 0, 1, \ldots, 7$.

If $PHP(C_0, C_1, \ldots, C_k; \pi; n)$ is maximal and strictly partial, then for any $\bar{x} \in Z_2^n$ and any permutation π' of the coordinate set we get a new set of mutually disjoint Hamming translates,

$$\dot{\cup}_{i=0}^{k} \pi'(C_i + \bar{x} + \bar{e}_{\pi(i)}).$$

This set of Hamming translates is also a maximal strictly partial Hamming packing. From equation (24), we get that the only possible packing numbers for maximal strictly partial Hamming packings of Z_2^7 are 4, 5 and 6. Hence, by the computation of the algorithm we get the set of possible packing numbers of maximal strictly partial Hamming packings of Z_2^7.

$\mathcal{H}$ = family of all Hamming codes of Z_2^7
$\mathcal{A}$ = family of maximal strictly partial Hamming packings of Z_2^7

id = identity permutation of $\{0, 1, \ldots, 7\}$
W = set of words of length 7
$disjunct$ = boolean

$\mathcal{A} = \{\}$
for k = 3,4,5 **do**
  for$_1$ each (k + 1)-multiset $\{C_0, C_1, \ldots, C_k\}$ of $\mathcal{H}$ **do**
    $W = \{\}$
    $disjunct =$ **true**
    for$_2$ $i = 0, 1, \ldots, k$ **do**
      if $W \cap (C_i + \bar{e}_i) = \emptyset$ **then**
        $W = W \cup (C_i + \bar{e}_i)$
      else
        $disjunct =$ **false**
        break for$_2$
      end
    end
    if $disjunct =$ **true then**
      for$_3$ i = k + 1,k + 2, ...,7 **do**
        for each C of $\mathcal{H}$ **do**
          if $W \cap (C + \bar{e}_i) \neq \emptyset$ **then**
            $disjunct =$ **false**
            break for$_3$
          end
        end
      end
      if $disjunct =$ **true then**
        $\mathcal{A} = \mathcal{A} \cup PHP(C_0, C_1, \ldots, C_k; id; 7)$
        break for$_1$
      end
    end
  end
end
output $\mathcal{A}$

The results from the computation of the algorithm above are stated in the appendix. By these results we get the following theorem.

Theorem 9. *The only integer p for which there exists a maximal strictly partial Hamming packing of Z_2^7 with packing number p is the integer $p = 5$.*

7.1.2 Maximal strictly partial Hamming packings of Z_2^{15}

By Proposition 5 in Section 3, there are 64864800 different Hamming codes of length 15. To enumerate these Hamming codes we will use, as in the case of length 7, a set of parity-check matrices given by classes $B1, B2, \ldots, B9$, discussed below.

Parity-check matrices. The matrices in the classes $B1, B2, \ldots, B9$ are all parity-check matrices of respective type which satisfy the construction (2) on page 6, i.e. the 15 columns of the matrix consist of all non zero words of Z_2^4. Below, $- = 0$ or 1.

$$\text{Class } B1: \quad \begin{pmatrix} 0&0&0&1&-&-&-&-&-&-&-&-&-&-&- \\ 0&0&1&0&-&-&-&-&-&-&-&-&-&-&- \\ 0&1&0&0&-&-&-&-&-&-&-&-&-&-&- \\ 1&0&0&0&-&-&-&-&-&-&-&-&-&-&- \end{pmatrix}$$

$$\text{Class } B2: \quad \begin{pmatrix} 0&0&0&0&1&-&-&-&-&-&-&-&-&-&- \\ 0&0&1&-&0&-&-&-&-&-&-&-&-&-&- \\ 0&1&0&-&0&-&-&-&-&-&-&-&-&-&- \\ 1&0&0&-&0&-&-&-&-&-&-&-&-&-&- \end{pmatrix}$$

$$\text{Class } B3: \quad \begin{pmatrix} 0&0&0&0&0&1&-&-&-&-&-&-&-&-&- \\ 0&0&1&-&-&0&-&-&-&-&-&-&-&-&- \\ 0&1&0&-&-&0&-&-&-&-&-&-&-&-&- \\ 1&0&0&-&-&0&-&-&-&-&-&-&-&-&- \end{pmatrix}$$

$$\text{Class } B4: \quad \begin{pmatrix} 0&0&0&0&0&0&1&-&-&-&-&-&-&-&- \\ 0&0&1&-&-&-&0&-&-&-&-&-&-&-&- \\ 0&1&0&-&-&-&0&-&-&-&-&-&-&-&- \\ 1&0&0&-&-&-&0&-&-&-&-&-&-&-&- \end{pmatrix}$$

$$\text{Class } B5: \quad \begin{pmatrix} 0&0&0&0&0&0&0&1&-&-&-&-&-&-&- \\ 0&0&1&-&-&-&-&0&-&-&-&-&-&-&- \\ 0&1&0&-&-&-&-&0&-&-&-&-&-&-&- \\ 1&0&0&-&-&-&-&0&-&-&-&-&-&-&- \end{pmatrix}$$

$$\text{Class } B6: \quad \begin{pmatrix} 0&0&0&0&1&-&-&-&-&-&-&-&-&-&- \\ 0&0&0&1&0&-&-&-&-&-&-&-&-&-&- \\ 0&1&1&0&0&-&-&-&-&-&-&-&-&-&- \\ 1&0&1&0&0&-&-&-&-&-&-&-&-&-&- \end{pmatrix}$$

$$\text{Class } B7: \quad \begin{pmatrix} 0&0&0&0&0&1&-&-&-&-&-&-&-&-&- \\ 0&0&0&1&-&0&-&-&-&-&-&-&-&-&- \\ 0&1&1&0&-&0&-&-&-&-&-&-&-&-&- \\ 1&0&1&0&-&0&-&-&-&-&-&-&-&-&- \end{pmatrix}$$

$$\text{Class } B8: \quad \begin{pmatrix} 0&0&0&0&0&0&1&-&-&-&-&-&-&-&- \\ 0&0&0&1&-&-&0&-&-&-&-&-&-&-&- \\ 0&1&1&0&-&-&0&-&-&-&-&-&-&-&- \\ 1&0&1&0&-&-&0&-&-&-&-&-&-&-&- \end{pmatrix}$$

$$\text{Class } B9: \quad \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & - & - & - & - & - & - & - \\ 0 & 0 & 0 & 1 & - & - & - & 0 & - & - & - & - & - & - & - \\ 0 & 1 & 1 & 0 & - & - & - & 0 & - & - & - & - & - & - & - \\ 1 & 0 & 1 & 0 & - & - & - & 0 & - & - & - & - & - & - & - \end{pmatrix}$$

With similar methods as used for Hamming codes of length 7, we will show that the parity-check matrices above enumerate all Hamming codes of length 15 in a unique way. Therefore we have to prove that the matrices in $B1, B2, \ldots, B9$ generate different subspaces of Z_2^{15} and that the number of matrices in $B1, B2, \ldots, B9$ is 64864800.

With the same arguments, as on page 30, where we proved that the subspaces generated by the matrices in $A1$ are different, we may prove that the subspaces generated by the matrices in $B1, B2, \ldots, B9$ respectively, are different.

On page 30, we proved that the subspaces generated by the matrices in $A1$ are different from those subspaces generated by the matrices in $A2$. With the same arguments as in that proof, we may prove that the subspaces generated of the matrices in $B1, B2, \ldots, B5$ are different and that the subspaces generated by the matrices in $B6, B7, \ldots, B9$ are different.

Finally, we get that none of the words of type $(0, 0, 1, -, -, -, -, -, -, -, -, -, -, -, -)$ are members of any of the subspaces generated by the matrices of $B6, B7, \ldots, B9$. This implies that the subspaces generated by the matrices in $B1, B2, \ldots, B5$ are different to those subspaces generated by the matrices in $B6, B7, \ldots, B9$. Consequently, all of the subspaces generated by the matrices in $B1, B2, \ldots, B9$ are different.

Further, the total number of matrices in $B1, B2, \ldots, B9$ equals

$$11! + 4 \cdot 10! + 4 \cdot 3 \cdot 9! + 4 \cdot 3 \cdot 2 \cdot 8! + 4! \cdot 7! + 10! + 3 \cdot 9! + 3 \cdot 2 \cdot 8! + 3! \cdot 7! = 64864800.$$

Algorithm. The algorithm computes a maximal partial Hamming packing of Z_2^{15}. Note that from equation (24) on page 29, we get that the only possible packing numbers for maximal strictly partial Hamming packings of Z_2^{15} are $5, 6, 7, \ldots, 14$.

$\mathcal{H}$ = family of all Hamming codes of Z_2^{15}
$\mathcal{B}$ = family of Hamming codes
W = set of words
π = permutation of $\{0, 1, \ldots, 15\}$
p = packing number

$\mathcal{B} = \{\}$
$W = \{\}$
$p = 0$
for i = 0,1,...,15 **do**
    for$_1$ each C of $\mathcal{H}$ enumerated in random order **do**

```
        if W ∩ (C + ē_i) = ∅ then
            W = W ∪ (C + ē_i)
            C_p = C
            B = B ∪ C_p
            π(p) = i
            p = p + 1
            break for_1
        end
    end
end
output B and π
```

Some results from the computations of the algorithm above are given in the appendix. By these results and equation (24), we get the following theorem.

Theorem 10. *The only integers p for which there exist a maximal strictly partial Hamming packing of Z_2^{15} with packing number p are $p = 5, 6, 7, \ldots, 14$.*

7.2 A general construction of some maximal strictly partial Hamming packings

Theorem 11. *If there exists a maximal partial Hamming packing of $Z_2^{n'}$, $n' = 2^m - 1$, with packing number $n' + 1 - r$, then there exists a maximal partial Hamming packing of Z_2^n, $n = 2^{m+1} - 1$, with packing number $n + 1 - r$.*

Proof. Assume that we have a maximal $PHP(C'_0, C'_1, \ldots, C'_k; \pi'; n')$, $n' = 2^m - 1$, with packing number $n' + 1 - r$, i.e. $k = n' - r$. Also, let $H'_0, H'_1, \ldots, H'_k$ denote corresponding parity-check matrices of the Hamming codes $C'_0, C'_1, \ldots, C'_k$.

Now, by using the maximal partial Hamming packing above, we construct a maximal partial Hamming packing of Z_2^n, $n = 2^{m+1} - 1$, with packing number $n + 1 - r$.

Take any Hamming code C' of length n' and denote a corresponding parity-check matrix by H'. Denote by $C, C_0, C_1, \ldots, C_k$ the Hamming codes of length n which corresponds to the following parity-check matrices,

$$H = \left[\begin{array}{c|c|c} 0\ldots0 & 1 & 1\ldots1 \\ \hline H' & \mathbf{0} & H' \end{array}\right]$$

and

$$H_i = \left[\begin{array}{c|c|c} 0\ldots0 & 1 & 1\ldots1 \\ \hline H'_i & \mathbf{0} & H'_i \end{array}\right], \quad i = 0, 1, \ldots, k.$$

Note that $n' + 1 = (n + 1)/2$. Clearly, the $(n + 1)/2$ translates of the Hamming code C,

$$(C + \bar{e}_{n'+1}), (C + \bar{e}_{n'+2}), \ldots, (C + \bar{e}_n),$$

are mutually disjoint.

We remind that π' is the permutation given by the maximal $PHP(C'_0, C'_1 \ldots, C'_k; \pi', n')$. By Corollary 3 in Section 5, for each pair $i, j \in \{0, 1, \ldots, k\}$, $i \neq j$, there exists a word $\bar{y}^{(ij)} \in C_i'^{\perp} \cap C_j'^{\perp}$, such that $y^{(ij)*}_{\pi'(i)} \neq y^{(ij)*}_{\pi'(j)}$. This implies that for each pair $i, j \in \{0, 1, \ldots, k\}$, $i \neq j$, there exists a word $\bar{x}^{(ij)} = \bar{y}^{(ij)} 0 \bar{y}^{(ij)} \in C_i^{\perp} \cap C_j^{\perp}$ such that $x^{(ij)*}_{\pi'(i)} \neq x^{(ij)*}_{\pi'(j)}$. Hence, by using Corollary 3 again, we get that the translates of Hamming codes,

$$(C_0 + \bar{e}_{\pi'(0)}), (C_1 + \bar{e}_{\pi'(1)}), \ldots, (C_k + \bar{e}_{\pi'(k)}),$$

are mutually disjoint.

Further, for each pair i, j, where $i \in \{0, 1, \ldots, k\}$ and $j \in \{n' + 1, n' + 2, \ldots, n\}$, we get the following facts:

$$\begin{array}{ll} (i) & \bar{x} = (0 \ldots 0 1 \ldots 1) \in C_i^{\perp} \cap C^{\perp}, \\ (ii) & x^*_{\pi(i)} = 0 \text{ and } x^*_j = 1. \end{array}$$

This implies, by Theorem 2 in Section 5, that $(C_i + \bar{e}_{\pi(i)}) \cap (C + \bar{e}_j) = \emptyset$.

Let $\mathcal{S}$ denote the family of the following translates of Hamming codes:

$$C_0 + \bar{e}_{\pi'(0)}, C_1 + \bar{e}_{\pi'(1)}, \ldots, C_k + \bar{e}_{\pi'(k)}, C + \bar{e}_{n'+1}, C + \bar{e}_{n'+2}, \ldots, C + \bar{e}_n.$$

The codes in this family are mutually disjoint. Consequently, the family $\mathcal{S}$ constitutes a partial Hamming packing with packing number $n + 1 - r$.

Now, assume there exists a translate $D + \bar{e}_j$ of some Hamming code D of length n, such that $D + \bar{e}_j$ and the codes in the family $\mathcal{S}$ are disjunct. Then,

$$j \in \{0, 1, \ldots, n'\} \setminus \{\pi'(0), \pi'(1), \ldots, \pi'(k)\}.$$

By Lemma 2 in Section 3, we get that the word $\bar{0}\bar{1} \in D^{\perp}$. Also, by Corollary 3 in Section 5, we get that there exist some words $\bar{d}^{(0)}, \bar{d}^{(1)}, \ldots, \bar{d}^{(k)} \in D^{\perp}$, such that

$$\bar{d}^{(i)} \in C_i^{\perp} \quad \text{and} \quad d^{(i)*}_{\pi'(i)} \neq d^{(i)*}_j, \qquad i = 0, 1, \ldots, k. \tag{25}$$

Let A be the set of words of length n', that we get by removing the last $n' + 1$ coordinates in each word of $D^{\perp}$, i.e.

$$A \;=\; \{\bar{x} = (x_1, x_2, \ldots, x_{n'}) \in Z_2^{n'} \mid (x_1, x_2, \ldots, x_{n'}, x_{n'+1}, \ldots, x_n) \in D^{\perp}\}.$$

Since $\bar{0}\bar{1} \in D^{\perp}$, we may conclude from Proposition 4 in Section 3, that A is a simplex code of dimension m. Consequently A is the dual code of a Hamming code of length n'. Let us denote this Hamming code by D'. From (25), we get that there are some words $\bar{y}^{(0)}, \bar{y}^{(1)}, \ldots, \bar{y}^{(k)} \in D'^{\perp} = A$, such that for $i = 0, 1, \ldots, k$,

$$\bar{y}^{(i)} \in C_i'^{\perp} \quad \text{and} \quad y^{(i)*}_{\pi'(i)} \neq y^{(i)*}_j.$$

Hence, by Theorem 2 in Section 5,

$$(C'_i + \bar{e}_{\pi'(i)}) \cap (D' + \bar{e}_j) = \emptyset, \quad i = 1, 2, \ldots, k.$$

This is a contradiction, since $PP(C'_0, C'_1, \ldots, C'_k; \pi'; n')$ is maximal. The theorem is now proved.

Corollary 7. *For any $n = 2^m - 1$, $m \geq 4$, there exist maximal strictly partial Hamming packings of Z_2^n with a packing number p equal to $n-10, n-9, \ldots, n-1$.*

Proof. By Theorem 10, the corollary is true for $m = 4$. Thus from Theorem 11, by induction the theorem is true.

Note that the corollary above and Corollary 6 in Section 6, gives that the upper bound, $p \leq n-1$, for the packing numbers p of maximal strictly partial Hamming packings of Z_2^n, $n \geq 15$, is tight.

8 Conclusions

In this section the results are summarized and problems for further study are suggested.

8.1 Results

The main results of this thesis are the following:

- We have given a condition when translates of Hamming codes are mutually disjoint or not mutually disjoint, which are related to the corresponding dual codes.
- Non trivial lower and upper bounds for the packing numbers of maximal strictly partial Hamming packings have been given.
- A non trivial upper bound for the packing numbers of maximal strictly partial packings with perfect codes has been given.
- By a computer search we have found all possible packing numbers for maximal strictly partial Hamming packings of Z_2^7 and Z_2^{15}.
- Finally we have proved a general result for the existence of some packing numbers of maximal strictly partial Hamming packings of Z_2^n, $n \geq 15$. We have thereby verified that the upper bound is tight for Z_2^n, $n \geq 15$.

8.2 Further study

In this subsection we list some open problems which have connections with the investigations of this thesis:

- Which are the packing numbers for maximal strictly partial Hamming packings of Z_2^n, $n \geq 15$? From the results in this paper we know that the packing numbers for maximal strictly partial Hamming packings of Z_2^{15}, are the integers from the lower bound to the upper bound that we have proved. Is this result also true when n is greater than 15?

- Is it possible to find a general construction for some maximal strictly partial Hamming packings, without using the computer? The general result of this study is proved by using the result of the computer search on maximal strictly partial Hamming packings of Z_2^{15}.
- In this thesis we give a trivial lower bound and a non trivial upper bound for the packing numbers of maximal strictly partial packings with perfect codes in general. One problem to consider for further investigation, would be to see if these bounds could be improved, especially the lower bound.
- It would also be interesting to know which packing numbers exist for maximal strictly partial packings with perfect codes in general and for different classes of perfect codes, e.g. for Vasil'ev codes constructed from Hamming codes.
- Finally, we believe that some of the results in this study may be used in the investigation of other areas concerning perfect codes. We especially believe that Lemma 3 and Theorem 2 in section 5 may be used in studies of similar areas such as intersection numbers of perfect codes or partitions of Z_2^n into perfect codes.

Acknowledgements

I would like to express my sincere apprecation and gratitude to my supervisor Olof Heden for guidence and encouragement during the work on this thesis. It has been a privilege to have you as a superviser.

I would also like to thank Helena Henriksson and Gisela Almeida for proofreading the text.

References

[1] S.V. Avgustinovich, O. Heden, and F.I. Solov'eva, *The classification of some perfect codes*, Designs, Codes and Cryptography, 31 (3) (2004), pp. 313-318.

[2] A. Bonisoli, *Every equidistant linear code is a sequence of dual Hamming codes*, Ars Combinatoria, 18 (1984), pp. 181-186.

[3] T. Etzion and A. Vardy, *On Perfect Codes and Tilings: Problems and Solutions*, SIAM J. Discrete Math. 11 (2) (1998), pp. 205-223.

[4] R.W. Hamming, *Error detecting and error correcting codes*, Bell System Technical Journal, 29 (1950), pp. 147-160.

[5] O. Heden, *On the reconstruction of perfect codes*, Discrete Mathematics, 256 (2002), pp. 479-485.

[6] O. Heden, *Six lectures on perfect codes*, unpublished lecture notes, Perugia (Italy), May 30 - June 9 2005.

[7] O. Heden, *On tilings with different perfect codes*, submitted.

[8] F. Hergert, *Algebraiche Methoden fur nichtlineare Codes*, Thesis, Darmstadt 1985.

[9] D.S. Krotov, *Lower bounds on the number of m-quasigroups of order 4 and the number of perfect binary codes*, Discrete Analysis and Operation Research, 1(7)2 (2000), pp. 47-53.

[10] D. Mesner, *Sets of disjoint lines in P(3,q)*, Canad. J. Math, 19 (1967), pp. 273-280.

[11] K.T. Phelps, *A general product construction for error correcting codes*, SIAM Journal of Algebra and Discrete Methods, 5 (1984), pp. 224-228.

[12] K.T. Phelps, *An enumeration of 1-perfect binary codes*, Australian Journal of Combinatorics, 21 (2000), pp. 287-298.

[13] N.J.A. Sloane and F.J. MacWilliams, *The Theory of error-correcting codes*, North-Holland, 1977.

[14] F.I. Solov'eva, *On Perfect Codes and Related Topics*, Com^{2}Mac Lecture Note Series 13, Pohang 2004.

[15] Y.L. Vasil'ev, *On nongroup close-packed codes,* Problems of Cybernetics, 8 (1962), pp. 375-378.

A Appendix

This appendix contains two tables with maximal strictly partial Hamming packings of Z_2^7 with packing number 5 and of Z_2^{15} with packing numbers $5, 6, 7, \ldots, 14$. These maximal strictly partial Hamming packings were given by the computer searches described in Section 7.

In the tables below, a maximal strictly $PHP(C_0, C_1, \ldots, C_k; \pi; n)$ is represented by its packing number, Hamming codes $C_0, C_1, \ldots, C_k$ and corresponding words $\bar{e}_{\pi(0)}, \bar{e}_{\pi(1)}, \ldots, \bar{e}_{\pi(k)}$ that describe the translations. A Hamming code is represented by a corresponding parity-check matrix. A parity-check matrix will here be denoted by the integers that correspond to the binary numbers that each columns in the matrix represent. For example the matrix

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

will be denoted as

$$(1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7) \ .$$

Table 1. *Maximal strictly partial Hamming packings of* Z_2^7.

Packing number	Hamming codes	Translate words
5	(1 2 4 7 3 5 6)	$\bar{e}_0$
	(1 2 4 3 5 7 6)	$\bar{e}_1$
	(1 2 4 6 7 5 3)	$\bar{e}_2$
	(1 2 4 5 3 6 7)	$\bar{e}_3$
	(1 2 4 7 5 6 3)	$\bar{e}_4$

Table 2. *Maximal strictly partial Hamming packings of* Z_2^{15}.

Packing number	Hamming codes	Translate words
5	(1 2 4 8 15 7 9 14 10 13 6 12 5 11 3)	$\bar{e}_0$
	(1 2 4 7 8 3 13 14 9 5 6 11 10 12 15)	$\bar{e}_1$
	(1 2 4 8 10 13 5 7 15 11 3 6 9 14 12)	$\bar{e}_2$
	(1 2 4 8 7 10 11 9 15 5 14 12 13 3 6)	$\bar{e}_3$
	(1 2 4 5 8 13 10 7 14 9 15 11 6 12 3)	$\bar{e}_4$

6	(1 2 4 8 3 14 15 10 13 11 12 5 7 9 6)	$\bar{e}_0$
	(1 2 4 8 13 12 7 14 3 5 6 9 11 15 10)	$\bar{e}_1$
	(1 2 4 8 5 3 9 6 10 11 7 14 12 15 13)	$\bar{e}_2$
	(1 2 4 8 9 3 5 7 10 14 6 15 13 11 12)	$\bar{e}_3$
	(1 2 4 8 3 14 10 13 15 11 9 5 7 12 6)	$\bar{e}_4$
	(1 2 4 7 8 3 5 9 11 10 6 14 12 15 13)	$\bar{e}_5$
7	(1 2 4 8 3 15 9 7 13 6 12 11 10 5 14)	$\bar{e}_0$
	(1 2 4 8 3 15 5 13 14 9 12 7 6 10 11)	$\bar{e}_1$
	(1 2 4 8 5 14 9 6 3 15 10 11 12 13 7)	$\bar{e}_2$
	(1 2 4 8 11 5 12 13 15 3 6 14 7 10 9)	$\bar{e}_3$
	(1 2 4 6 3 8 9 14 13 15 7 11 10 5 12)	$\bar{e}_4$
	(1 2 4 8 15 5 9 13 3 14 10 11 6 7 12)	$\bar{e}_5$
	(1 2 4 8 3 15 5 13 14 9 12 7 6 10 11)	$\bar{e}_{15}$
8	(1 2 4 8 14 6 10 13 15 11 5 7 12 3 9)	$\bar{e}_0$
	(1 2 3 4 6 8 15 5 7 9 11 10 13 14 12)	$\bar{e}_1$
	(1 2 4 7 8 3 15 14 6 13 5 11 10 9 12)	$\bar{e}_2$
	(1 2 4 8 11 3 15 5 10 9 13 7 6 14 12)	$\bar{e}_3$
	(1 2 4 3 8 11 12 6 9 10 5 7 13 14 15)	$\bar{e}_4$
	(1 2 3 4 8 5 12 11 7 10 6 9 14 13 15)	$\bar{e}_5$
	(1 2 4 8 13 12 9 7 5 15 6 14 11 3 10)	$\bar{e}_6$
	(1 2 3 4 6 8 15 5 7 9 11 10 13 14 12)	$\bar{e}_{15}$
9	(1 2 4 8 9 5 14 11 13 3 10 12 6 7 15)	$\bar{e}_0$
	(1 2 4 6 8 12 13 10 3 5 9 11 15 7 14)	$\bar{e}_1$
	(1 2 4 8 7 10 5 11 3 12 14 13 6 9 15)	$\bar{e}_2$
	(1 2 4 7 8 14 13 3 11 15 9 10 6 5 12)	$\bar{e}_3$
	(1 2 4 7 8 5 12 9 10 14 3 11 6 15 13)	$\bar{e}_4$
	(1 2 3 4 8 13 10 7 11 12 9 14 5 6 15)	$\bar{e}_5$
	(1 2 4 7 8 5 12 9 10 14 3 11 6 15 13)	$\bar{e}_7$
	(1 2 4 8 9 5 14 11 13 3 10 12 6 7 15)	$\bar{e}_{11}$
	(1 2 4 8 7 10 5 11 3 12 14 13 6 9 15)	$\bar{e}_{12}$
10	(1 2 4 8 11 6 13 10 12 9 7 5 14 3 15)	$\bar{e}_0$
	(1 2 4 8 9 15 13 12 10 11 5 7 3 14 6)	$\bar{e}_1$
	(1 2 4 8 6 15 5 3 12 13 10 9 11 7 14)	$\bar{e}_2$
	(1 2 4 7 8 3 5 14 15 13 11 9 10 6 12)	$\bar{e}_3$
	(1 2 4 8 9 3 10 15 14 12 5 7 11 6 13)	$\bar{e}_4$
	(1 2 4 7 8 5 14 6 12 13 11 9 10 3 15)	$\bar{e}_6$
	(1 2 4 7 8 5 14 6 12 13 11 9 10 3 15)	$\bar{e}_7$
	(1 2 4 8 6 15 5 3 12 13 10 9 11 7 14)	$\bar{e}_8$
	(1 2 4 8 3 14 7 6 10 11 15 13 12 5 9)	$\bar{e}_{12}$
	(1 2 4 8 9 15 13 12 10 11 5 7 3 14 6)	$\bar{e}_{14}$

11	(1 2 4 8 11 3 10 9 15 6 13 14 5 7 12)	$\bar{e}_0$
	(1 2 4 6 8 12 9 3 5 11 7 13 10 14 15)	$\bar{e}_1$
	(1 2 4 8 3 15 10 13 7 6 5 14 9 11 12)	$\bar{e}_2$
	(1 2 4 5 8 13 9 10 7 3 14 6 11 12 15)	$\bar{e}_3$
	(1 2 4 8 11 3 10 9 15 6 13 14 5 7 12)	$\bar{e}_4$
	(1 2 4 5 8 12 7 14 9 6 11 3 10 13 15)	$\bar{e}_5$
	(1 2 4 8 6 10 15 13 7 3 5 11 12 14 9)	$\bar{e}_6$
	(1 2 4 6 8 12 9 3 5 11 7 13 10 14 15)	$\bar{e}_8$
	(1 2 4 5 8 12 7 14 9 6 11 3 10 13 15)	$\bar{e}_{10}$
	(1 2 4 8 11 15 10 6 7 13 14 5 9 3 12)	$\bar{e}_{11}$
	(1 2 4 8 11 3 10 9 7 14 13 6 5 15 12)	$\bar{e}_{15}$
12	(1 2 4 8 14 15 10 9 3 7 5 12 6 11 13)	$\bar{e}_0$
	(1 2 4 3 5 7 8 15 13 9 6 10 11 14 12)	$\bar{e}_1$
	(1 2 4 6 8 5 3 11 12 7 9 14 10 13 15)	$\bar{e}_2$
	(1 2 4 8 15 7 13 9 11 14 5 12 6 3 10)	$\bar{e}_3$
	(1 2 4 8 11 9 3 10 12 7 6 15 5 14 13)	$\bar{e}_4$
	(1 2 4 5 3 8 10 14 9 7 15 11 12 6 13)	$\bar{e}_5$
	(1 2 4 8 14 15 13 9 10 7 5 12 6 11 3)	$\bar{e}_6$
	(1 2 4 8 15 7 13 9 11 14 5 12 6 3 10)	$\bar{e}_7$
	(1 2 4 3 5 7 8 15 13 9 6 10 11 14 12)	$\bar{e}_8$
	(1 2 4 8 9 11 13 10 14 7 6 15 5 12 3)	$\bar{e}_{13}$
	(1 2 4 5 8 3 6 14 10 7 15 11 12 13 9)	$\bar{e}_{14}$
	(1 2 4 8 12 14 13 10 3 7 6 15 5 9 11)	$\bar{e}_{15}$
13	(1 2 4 8 3 15 7 14 6 10 9 12 11 13 5)	$\bar{e}_0$
	(1 2 4 8 14 15 10 7 12 9 3 5 6 13 11)	$\bar{e}_1$
	(1 2 4 8 15 14 6 7 10 3 5 9 11 12 13)	$\bar{e}_2$
	(1 2 4 8 12 15 5 6 3 10 14 9 11 13 7)	$\bar{e}_3$
	(1 2 4 5 8 9 7 15 12 10 14 6 13 11 3)	$\bar{e}_4$
	(1 2 4 8 3 14 10 7 6 15 5 9 11 12 13)	$\bar{e}_5$
	(1 2 4 8 14 15 7 10 9 12 6 5 11 13 3)	$\bar{e}_7$
	(1 2 4 8 14 15 10 7 12 9 3 5 6 13 11)	$\bar{e}_9$
	(1 2 4 5 8 9 7 15 12 10 14 6 13 11 3)	$\bar{e}_{11}$
	(1 2 4 8 14 15 7 5 6 12 9 10 11 13 3)	$\bar{e}_{12}$
	(1 2 4 8 14 15 7 12 10 9 5 3 11 13 6)	$\bar{e}_{13}$
	(1 2 4 8 3 15 7 14 6 10 9 12 11 13 5)	$\bar{e}_{14}$
	(1 2 4 8 14 15 7 3 10 6 5 12 11 13 9)	$\bar{e}_{15}$

14	(1 2 4 3 7 8 11 14 6 5 12 15 13 9 10)	$\bar{e}_0$
	(1 2 4 8 15 14 11 6 13 3 7 9 5 10 12)	$\bar{e}_1$
	(1 2 4 8 3 10 6 7 9 11 14 12 5 15 13)	$\bar{e}_2$
	(1 2 4 8 6 7 3 13 12 9 14 11 5 10 15)	$\bar{e}_3$
	(1 2 4 8 3 9 7 6 13 12 11 10 5 14 15)	$\bar{e}_4$
	(1 2 4 3 7 8 11 14 6 5 12 15 13 9 10)	$\bar{e}_6$
	(1 2 4 8 3 11 6 7 9 10 14 13 5 15 12)	$\bar{e}_7$
	(1 2 4 8 7 9 3 6 13 12 15 14 5 10 11)	$\bar{e}_9$
	(1 2 4 8 3 9 7 6 13 12 11 10 5 14 15)	$\bar{e}_{10}$
	(1 2 4 8 6 7 3 13 12 9 14 11 5 10 15)	$\bar{e}_{11}$
	(1 2 4 8 15 14 11 6 13 3 7 9 5 10 12)	$\bar{e}_{12}$
	(1 2 4 8 6 9 3 7 12 13 14 15 5 10 11)	$\bar{e}_{13}$
	(1 2 4 8 7 12 3 6 13 9 15 11 5 10 14)	$\bar{e}_{14}$
	(1 2 4 8 6 13 3 7 12 9 14 11 5 10 15)	$\bar{e}_{15}$