Constructions and an existence result of uniquely decodable codepairs for the two-access binary adder channel

TECHNISCHE HOGESCHOOL EINDHOVEN
NEDERLAND
ONDERAFDELING DER WISKUNDE
EN INFORMATICA

EINDHOVEN UNIVERSITY OF TECHNOLOGY
THE NETHERLANDS
DEPARTMENT OF MATHEMATICS
AND COMPUTING SCIENCE

Constructions and an existence result of uniquely decodable codepairs for the two-access binary adder channel

by

Paul A.B.M. Coebergh van den Braak

AMS Subjectclassification 94 A 15

EUT. - Report 83-WSK-01

January 1983

CONTENTS · page

Chapter 0. Introduction.

0.1. Abstract.

In this report we examine the encoding problem for the two access binary adder channel. In this Chapter we state the problem and mention the most important known results. In Chapter 1 we deduce lower and upper bounds for $|C_2|$ where C_1 is fixed and (C_1,C_2) is uniquely decodable. In Chapters 2,3,4 and 5 explicit constructions for uniquely decodable codepairs are given. Results are given in Chapter 6. For a summary we refer to Chapter 7.

0.2. The problem.

Consider the following communication system:

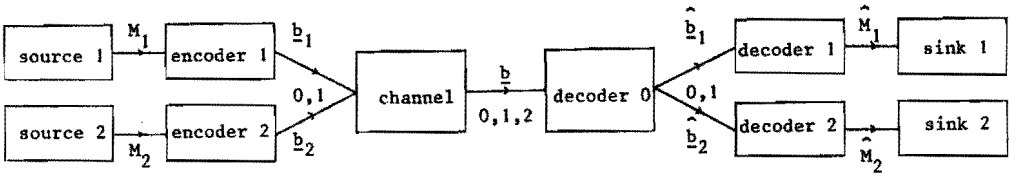


fig.1.

Two users wish to send one-way information over the channel. Their messages M_1, M_2 are encoded in sequences $\underline{b}_1$ resp. $\underline{b}_2$ of zeros and ones, which enter the channel simultaneously. (We assume that $\underline{b}_1$ and $\underline{b}_2$ have the same length.) These sequences are transformed by the channel in one sequence $\underline{b}$ of zeros, ones and twos which is the real sum of $\underline{b}_1$ and $\underline{b}_2$, possibly disturbed by noise. (Below we give a more detailed description of the channel.) From the output sequence $\underline{b}$ the first decoder makes estimates $\hat{\underline{b}}_1$ resp. $\hat{\underline{b}}_2$ of the original zero-one sequences $\underline{b}_1$ resp. $\underline{b}_2$. These estimates should of course be decoded again to obtain estimates $\hat{M}_1$ and $\hat{M}_2$ of the original messages. (Remark: in the literature

it is customary to take decoders 0,1,2 together as one decoder.)

The first important question is in what way the output sequence $\underline{b}$ is determined by the input sequences $\underline{b}_1$ and $\underline{b}_2$.We assume that the channel is in full bit synchronisation,which means that two input bits b_1 and b_2 enter the channel at the same time.Now suppose both b_1 and b_2 may be disturbed by an error after which the resulting symbols are simply added.Then,denoting real addition by + and <u>mod</u> 2 addition by $\oplus$,we have

$$b = (b_1 \oplus e_1) + (b_2 \oplus e_2) \ , \quad b_1,b_2,e_1,e_2 \in \{0,1\} \ ,$$
$$P(e_i=1) = 1-P(e_i=0) = p_i \ , \ 0 \le p_i \le \tfrac{1}{2} \ , \ i=1,2.$$

This model becomes <u>symmetric</u> by choosing $p_1=p_2=:p$, $0 \le p \le \frac{1}{2}$ .We say that p is the probability of making "one error".Now the channel is described by the following:

b		0	1	2
b_1	b_2			
0	0	$(1-p)^2$	$2p(1-p)$	p^2
0	1	$p(1-p)$	$(1-p)^2+p^2$	$p(1-p)$
1	0	$p(1-p)$	$(1-p)^2+p^2$	$p(1-p)$
1	1	p^2	$2p(1-p)$	$(1-p)^2$

table 1.

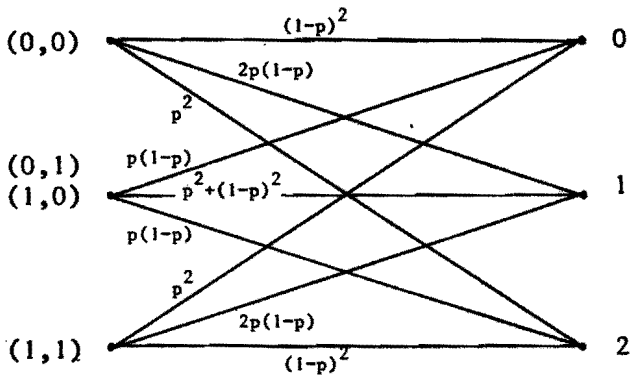


fig.2.

Above we see the transition probabilities between input and output symbols. For instance, $P(b=2|b_1=b_2=0) = p^2$.

Now our problem is to find encoding strategies for encoders 1,2 such that the average probability of $(\hat{\underline{b}}_1,\hat{\underline{b}}_2)$ being equal to $(\underline{b}_1,\underline{b}_2)$ is as large as possible. (Here we assume that all possible pairs (M_1,M_2) of messages are equaly likely.) It will be clear to the reader that for any encoding strategy we should have in mind a decoding strategy for decoder 0.However,we will not deal with the problem how to realise this in practice.

0.3.Restrictions to the problem.

From now on we restrict ourselves to the case that the channel is deterministic or noiseless - that is, p=0.This simplifies our model to:

b_1 \ b_2	0	1
0	0	1
1	1	2

table 2.

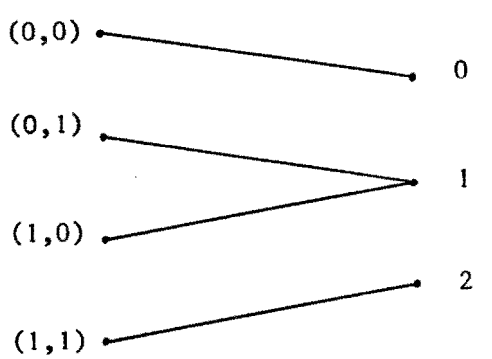


fig.3.

This model is easily described by $b = b_1+b_2$.

Moreover,we shall only use block codes for encoders 1,2.So any encoding strategy consists of a codepair (C_1,C_2) where $C_1 \subset \mathbb{F}_2^n$, $C_2 \subset \mathbb{F}_2^n$ for some $n \in \mathbb{N}$ .For each block transmission encoder i receives one out of $|C_i|$ different messages, selects the corresponding codeword in C_i and sends this into the channel.(i=1, 2.)We assume that we have block synchronisation - that is,the block transmissions for both encoders are at the same time.So a pair of codewords $\underline{c}_1 \in C_1$, $\underline{c}_2 \in C_2$ leaves the channel as a block $\underline{c}_1+\underline{c}_2 \in \{0,1,2\}^n$.

Finally,we will not accept ambiguity at all.So we require that for any $\underline{v} \in \{ \underline{c}_1+\underline{c}_2 \mid \underline{c}_1 \in C_1 \wedge \underline{c}_2 \in C_2 \}$ there is a unique pair $(\underline{c}_1,\underline{c}_2) \in C_1 \times C_2$ such that $\underline{v} = \underline{c}_1 + \underline{c}_2$.

Now we can clarify our point of view with respect to decoder 0.It is clear that if the codepair (C_1,C_2) has the above property it will always be possible (though possibly very laborious) to find the unique pair $(\underline{c}_1,\underline{c}_2)$ which adds up to the given outputvector.This guarantees communication without ambiguity.

0.4.Some definitions and some known results.

As in §0.2. we shall denote real addition by + and mod 2 addition by $\oplus$. For any $n \in \mathbb{N}$, $C \subset \mathbb{F}_2^n$, $D \subset \mathbb{F}_2^n$ we call (C,D) a codepair.We say that the codepair (C,D) is uniquely decodable if

$$(1) \qquad \forall_{\underline{c},\underline{c}' \in C} \forall_{\underline{d},\underline{d}' \in D} [\underline{c}+\underline{d} = \underline{c}'+\underline{d}' \Rightarrow (\underline{c}=\underline{c}' \wedge \underline{d}=\underline{d}')]$$

For any codepair (C,D) of length n let

$$(2) \qquad R_1 := \frac{1}{n} \ {}^2\log |C| \ , \quad R_2 := \frac{1}{n} \ {}^2\log |D| \ .$$

(R_1,R_2) is called the ratepair belonging to (C,D) .A decoding strategy for (C,D) is a mapping

$$(3) \qquad \phi : \{ \underline{c}+\underline{d} \mid \underline{c} \in C \wedge \underline{d} \in D \} \to C \times D \ .$$

Let the corresponding error probability be given by

$$(4) \qquad P_e(C,D,\phi) := \frac{1}{|C| \cdot |D|} |\{ (\underline{c},\underline{d}) \in C \times D \mid \phi(\underline{c}+\underline{d}) \neq (\underline{c},\underline{d}) \}| \ .$$

We call a ratepair ε-achievable if it belongs to a codepair (C,D) for which a decoding strategy ϕ exists such that $P_e(C,D,\phi) \leq \varepsilon$.

Now consider the set $\{(R_1,R_2) \mid \forall_{\varepsilon>0}: (R_1,R_2)$ is ε-achievable.$\}$ .The closure of the convex hull of this set is called the capacity region for the noiseless two-access binary adder channel.Roughly speeking,the capacity region is the set of ratepairs (R_1,R_2) for which it is possible to send information with arbitrarily small error probability from source i to sink i with information rate R_i ,for i=1,2 simultaneously.It has been proved in [1] that the capacity region for our noiseless channel is given by

(5) $\qquad 0 \le R_1 \le 1 \ , \ 0 \le R_2 \le 1 \ , \ R_1+R_2 \le 1\frac{1}{2} \ .$

This region is depicted in fig.4..

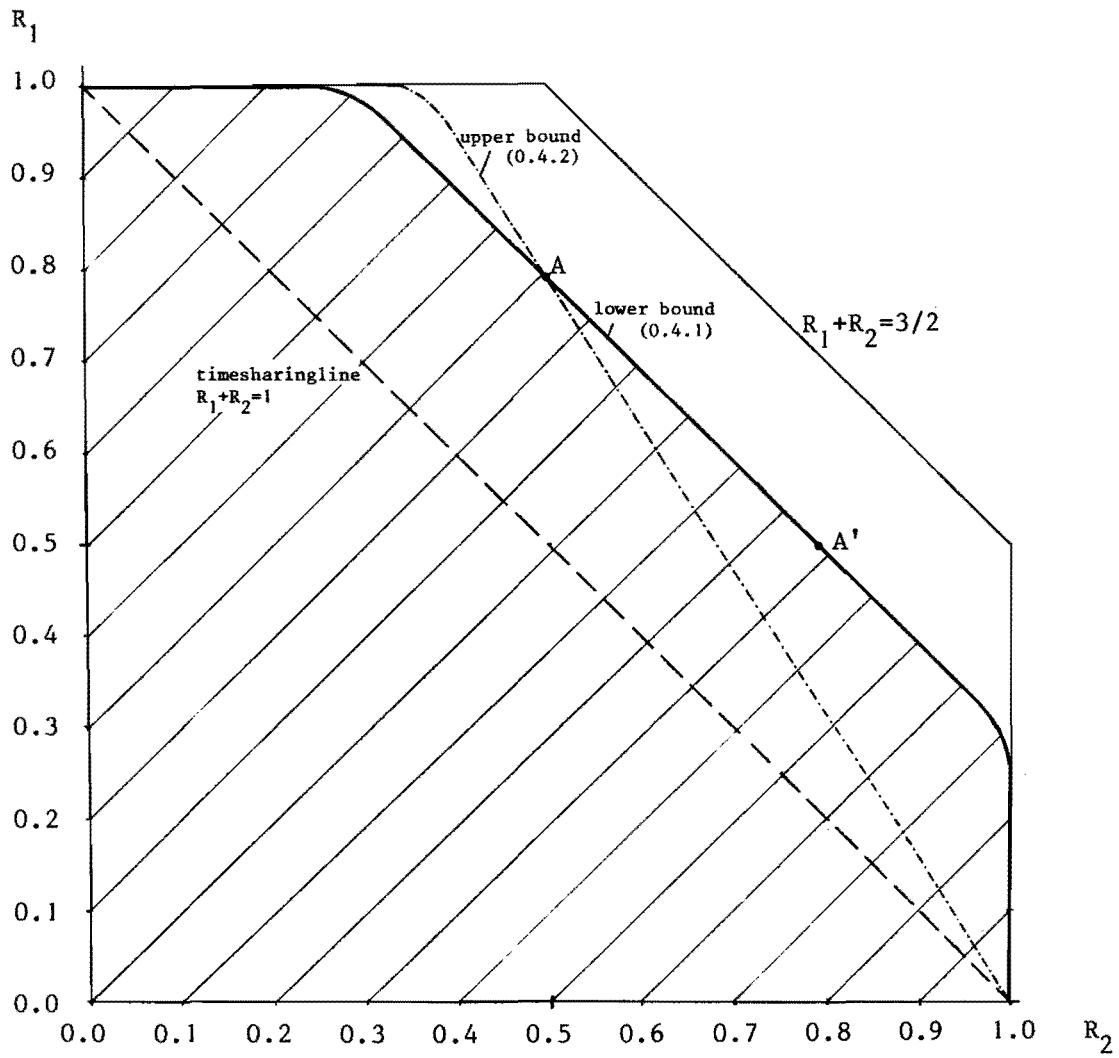


fig.4.

Note that the capacity region does not need to be equal to the set of ratepairs belonging to uniquely decodable codepairs,since this is the set V_{ud} := $\{(R_1,R_2) | (R_1,R_2)$ is 0-achievable.$\}$ .Of course V_{ud} is a subset of the capacity region.However,it has not been exactly determined yet.The best known lower bound up to now is given by:

0.4.1.Theorem. (Wei,Kasami,Lin,Yamamura,[5].) Let $0 \leq R_1 \leq \frac{1}{2}$.There is a uniquely decodable codepair (C,D) with ratepair (R_1,R_2) such that C is a linear code and

$$(6) \qquad R_2 \geq \begin{cases} 1 - o(1) & \text{if } 0 \leq R_1 < 1/4 \\ \frac{1}{2}(1 + H(2R_1) - o(1)) & \text{if } 1/4 \leq R_1 < 1/3 \\ \frac{1}{2}{}^2\log 6 - R_1 - o(1) & \text{if } 1/3 \leq R_1 \leq 1/2 \end{cases}$$

Here, $H(x) = -x\,{}^2\log x - (1-x)\,{}^2\log(1-x)$, $0 < x < 1$, and $o(1)$ is vanishingly small if the block length n tends to infinity.

This gives us the bold line segment from (0,1) to A in fig.4..By interchanging the role of C and D we obtain the line segment from A' to (1,0).

Now we introduce the notion of timesharing.Suppose we have u.d. codepairs (C,D) and (C',D') of length n resp. n' with ratepairs (R_1,R_2) resp. (R_1',R_2'). Let m and m' be nonnegative integers and M:=m+m'.Now for every M block transmissions the first m pairs of input words are taken from (C,D) and the last m' pairs are taken from (C',D').This technique yields communication without ambiguity,while the new information rates are given by

$$(7) \qquad R_i = \frac{m.n.R_i + m'.n'.R_i'}{m.n + m'.n'} \quad , \; i = 1,2 \; .$$

Hence the point (R_1,R_2) is on the line segment from (R_1,R_2) to (R_1',R_2').So,for any point P on this line segment,we can construct a uniquely decodable code-pair with a ratepair arbitrarily close to P by a suitable choice of m and m'.

Since we may apply timesharing of the codes reaching the points A resp. A' , (0.4.1) and the above imply that there exists a uniquely decodable codepair for each point on the bold line in fig.4. (and hence for each point in the shaded area.).Another interesting result is given by:

0.4.2.Theorem. (Kasami and Lin,[3].)Let C be a [n,k] systematic code of rate $R_1 = k/n$ .Then the maximum rate R_2 of any code D of length n such that (C,D) be uniquely decodable satisfies

$$(8) \qquad R_2 \leq \begin{cases} 1 & \text{if } 0 \leq R_1 < 1/3 \\ R_1 + (1-R_1)H(R_1/(1-R_1)) + o(1) & \text{if } 1/3 \leq R_1 < 2/5 \\ (1-R_1)^2 \log 3 & \text{if } 2/5 \leq R_1 \leq 1 \end{cases}$$

Here $H(x)$ and $o(1)$ are as in (0.4.1).

The upper bound obtained from the above Theorem is given by the dotted line in fig.4..

0.4.3.Remarks. (i) The reader may have the idea that (0.4.1) and (0.4.2) are contradictory.However,this is not the case.We note that the line segment A-A'-(1,0) is obtained from (0.4.1) by interchanging the role of C and D and by the use of timesharing,which implies that we may no longer conclude that these points are obtainable by uniquely decodable codepairs (C,D) where C is a linear code.

(ii) As a matter of fact it follows from (0.4.1) and (0.4.2) that the maximum

rate R_2^{max} such that a uniquely decodable codepair (C,D) exists where C is a linear code of rate $R_1 = k/n$, $\frac{1}{2} \leq R_1 < 1$,is given by $R_2^{max} = (1-R_1)\ {}^2\log 3$, which is the dotted line segment A-(1,0) in fig.4..Indeed,these points are obtainable by timesharing the codepair (C,D) reaching the point A and the codepair ($C' = \mathbb{F}_2^n$,$D' = \{0\}$) reaching the point (1,0).(Note that the concatenation of two linear codes is again linear,which guarantees that we obtain a linear code C by timesharing the codes C and C'.)

(iii) We can of course recover the symmetry between R_1 and R_2 in (0.4.2) by considering uniquely decodable codepairs "for which one of the two codes is systematic".In order to obtain a convex area one has to consider uniquely decodable codepairs obtained by timesharing two codepairs each of which contains at least one systematic code.

(iv) Note that (0.4.1) only states the existence of certain codepairs.The proof is not provided with explicit construction methods.The same holds for (5).

(v) The point A = $(\frac{1}{2},\frac{1}{2}\ {}^2\log 3)$ is obtained by the uniquely decodable codepair (C = {00,11},D = {00,01,10}) of length 2.(Note that C is linear.)Interchanging of C and D gives us the point A'.Hence,using timesharing,we can reach any point on the line segment A-A' by a uniquely decodable code which is explicitely known.

Chapter 1.Conditions on (C,D) for being uniquely decodable.Upper and lower bounds on |D| for fixed C such that (C,D) is uniquely decodable.

1.1.Abstract.

In this Chapter we will derive conditions on codepairs (C,D) which are equivalent to the condition that (C,D) is u.d..(From now on we shall use u.d. as an abbreviation of "uniquely decodable".)The necessity of these conditions has bee shown by van Tilborg ([4]).The conditions enable us to have a closer look at the graph-theoretic approach to the encoding problem proposed by Wei,Kasami, Lin and Yamamura in [5].This approach consists of the association of a certain graph G_C on 2^n points to any code $C \subset \mathbb{F}_2^n$,with the property that any coclique in G_C corresponds in a unique way to a code D (of the same size) such that (C,D) is u.d..

Results of van Tilborg ([4]) are equivalent to the observation that certain cliques exist in G_C .From this van Tilborg derived an upper bound on |D| such that (C,D) be u.d. in terms of the Krawtchouk expansion of the annihilator polynomial of C.(For definitions see [7].)

Using a well-known graph-theoretic result due to Turán we find a lower bound on the maximum size of D such that (C,D) be uniquely decodable in terms of the distance enumerator of C.Subsequently,an increase of this lower bound is obtained by a closer examination of the number of edges in G_C .

1.2.Conditions.

1.2.1.Lemma.Let $n \in \mathbb{N}$, $\underline{c},\underline{c}',\underline{d},\underline{d}' \in \mathbb{F}_2^n$ .Then we have

(9) $\quad \underline{c} + \underline{d} = \underline{c}' + \underline{d}' \quad \Leftrightarrow \quad \exists_{\underline{u} \in \mathbb{F}_2^n} \; [(\forall_i : u_i = 1 \Rightarrow c_i = c_i') \wedge \underline{d}' = \underline{c} \oplus \underline{u} \wedge \underline{d} = \underline{c}' \oplus \underline{u}]$

Proof. (i) Let $\underline{u}$ satisfy the right hand side conditions.We have

$$c_i + d_i = c_i + (c_i' \oplus u_i)$$
$$c_i' + d_i' = c_i' + (c_i \oplus u_i)$$

If $u_i = 1$ these are equal since $c_i = c_i'$ in this case.If $u_i = 0$ these are equal since $c_i' \oplus u_i = c_i'$, $c_i \oplus u_i = c_i$ in this case.

(ii) Let $\underline{c} + \underline{d} = \underline{c}' + \underline{d}'$. W.l.o.g. we have

$$\underline{c} = 0\text{---}0,0\text{---}0,0\text{---}0,1\text{---}1,1\text{---}1,1\text{---}1$$
$$\underline{d} = 0\text{---}0,1\text{---}1,1\text{---}1,0\text{---}0,0\text{---}0,1\text{---}1$$
$$\underline{c} + \underline{d} = 0\text{---}0,1\text{---}1,1\text{---}1,1\text{---}1,1\text{---}1,2\text{---}2 \tag{10}$$
$$\underline{c}' = 0\text{---}0,0\text{---}0,1\text{---}1,0\text{---}0,1\text{---}1,1\text{---}1$$
$$\underline{d}' = 0\text{---}0,1\text{---}1,0\text{---}0,1\text{---}1,0\text{---}0,1\text{---}1$$

Now let $\underline{u} := \underline{c} \oplus \underline{d}'$ .From the above it is clear that $\underline{u} = \underline{c}' \oplus \underline{d}$,and moreover

$$u_i = \begin{cases} 1 \text{ if } c_i \oplus d_i = 1 \text{ and } c_i = c_i' \\ 0 \text{ otherwise.} \end{cases}$$

From these we have $u_i = 1 \Rightarrow c_i = c_i'$ and $\underline{d}' = \underline{u} \oplus \underline{c}$, $\underline{d} = \underline{u} \oplus \underline{c}'$. □

The following result is similar.

1.2.2.Lemma.Let $n \in \mathbb{N}$, $\underline{c},\underline{c}',\underline{d},\underline{d}' \in \mathbb{F}_2^n$ .Then we have

$$\underline{c} + \underline{d} = \underline{c}' + \underline{d}' \iff \exists_{\underline{u} \in \mathbb{F}_2^n} [(\forall_i : u_i = 0 \Rightarrow c_i = c_i') \wedge \underline{d} = \underline{c} \oplus \underline{u} \wedge \underline{d}' = \underline{c}' \oplus \underline{u}] \tag{11}$$

Proof. (i) Let $\underline{u}$ satisfy the right hand side conditions.We have

$$c_i + d_i = c_i + (c_i \oplus u_i)$$
$$c_i' + d_i' = c_i' + (c_i' \oplus u_i)$$

If $u_i = 0$ these are $2c_i$ resp. $2c_i'$ .Hence they are equal since $c_i = c_i'$ in this case.If $u_i = 1$ it is clear that both are equal to one.

(ii) Let $\underline{c} + \underline{d} = \underline{c}' + \underline{d}'$ .Again we have (10) w.l.o.g..Hence for $\underline{u} := \underline{c} \oplus \underline{d}$ we have $\underline{u} = \underline{c}' \oplus \underline{d}'$ and moreover

$$u_i = \begin{cases} 1 \text{ if } c_i + d_i = 1 \\ 0 \text{ otherwise.} \end{cases}$$

From these it follows that $\underline{d} = \underline{u} \oplus \underline{c}$, $\underline{d}' = \underline{u} \oplus \underline{c}'$ .Furthermore

$$u_i = 0 \Rightarrow c_i + d_i \in \{0,2\} \text{ .Note that}$$
$$c_i + d_i = 0 \Rightarrow c_i = d_i = c_i' = d_i' = 0 \text{ ,and}$$
$$c_i + d_i = 2 \Rightarrow c_i = d_i = c_i' = d_i' = 1.$$

Hence $u_i = 0 \Rightarrow c_i = c_i'$. □

1.2.3.Remark. Note that the $\Leftarrow$ parts ((i) in proofs) of the preceding Lemmas are due to van Tilborg ([4]).

Now for convenience we introduce the notion of covering.For $n \in \mathbb{N}$, $\underline{u},\underline{v} \in \mathbb{F}_2^n$ define

(12) $$\underline{u} \sqsubset \underline{v} :\Leftrightarrow \forall_i [\, u_i = 1 \Rightarrow v_i = 1 \,]$$

We say that $\underline{v}$ covers $\underline{u}$ .From now on we shall denote the all-one vector $(1,1,\ldots,1)$ by $\underline{1}$ .From Lemmas (1.2.1),(1.2.2) we easily obtain the following theorem:

1.2.4.Theorem. Let $n \in \mathbb{N}$, $C \subset \mathbb{F}_2^n$, $D \subset \mathbb{F}_2^n$ .Then the following three propositions are equivalent:

(i) (C,D) is uniquely decodable.

(ii) $\forall_{\underline{c},\underline{c}'\in C|\underline{c}\neq\underline{c}'} \forall_{\underline{u}\sqsubset \underline{c}\oplus\underline{c}'\oplus\underline{1}}$ [at most one of $\underline{c}\oplus\underline{u}$, $\underline{c}'\oplus\underline{u}$ is in D.]

(iii) $\forall_{\underline{c},\underline{c}'\in C|\underline{c}\neq\underline{c}'} \forall_{\underline{u}\mid \underline{c}\oplus\underline{c}'\sqsubset\underline{u}}$ [at most one of $\underline{c}\oplus\underline{u}$, $\underline{c}'\oplus\underline{u}$ is in D.]

Proof. (i)⇔(ii).Note that $\underline{u}\sqsubset \underline{c}\oplus\underline{c}'\oplus\underline{1}$ is equivalent to $u_i=1 \Rightarrow c_i=c_i'$ and that (C,D) is not u.d. iff the LHS of (1.2.1) is satisfied for some $\underline{c},\underline{c}'\in C$, $\underline{d},\underline{d}'\in D$, $\underline{c}\neq\underline{c}'$.Apply Lemma (1.2.1).

(i)⇔(iii). $\underline{c}\oplus\underline{c}'\sqsubset\underline{u}$ is equivalent to $u_i=0 \Rightarrow c_i=c_i'$ .Apply Lemma (1.2.2). □

1.3.Introduction of a graph $G_C = (V_C, E_C)$.

In this section we will associate a graph to the code C such that any coclique in the graph corresponds in a unique way to a code D of the same size with the property that (C,D) is uniquely decodable.First we give a brief introduction to graphs.

A graph $G = (V,E)$ consists of a set V of vertices and a set $E\subset P_2(V)$ of edges.Here $P_2(V)$ denotes the set of all subsets of V containing two elements. We say that $v_1, v_2 \in V$ are connected by an edge if $\{v_1, v_2\} \in E$.
A clique in G is a subset $A\subset V$ such that $P_2(A)\subset E$,that is,any two vertices in A are connected by an edge.A coclique in G is a subset $B\subset V$ such that $P_2(B)\cap E = \emptyset$,that is,any two vertices in B are not connected by an edge.A well-known result in graph theory is

1.3.1.Theorem.(Turán,[6]) Let $G = (V,E)$ be a graph.Let M_G be the maximum number such that there is a coclique in G of size M_G .Then

$$(13) \qquad M_G \geq \frac{|V|^2}{|V| + 2|E|}$$

Now we introduce our graph G_C .

1.3.2.Definition.Let $n\in\mathbb{N}$, $C\subset\mathbb{F}_2^n$ .The graph $G_C = (V_C, E_C)$ is defined by

$$V_C := \mathbb{F}_2^n$$

$$E_C := \bigcup_{\underline{c}\in C} \bigcup_{\underline{c}'\in C\setminus\{\underline{c}\}} \bigcup_{\underline{u}\sqsubset \underline{c}\oplus\underline{c}'\oplus\underline{1}} \{\{\underline{c}\oplus\underline{u}, \underline{c}'\oplus\underline{u}\}\} \tag{14}$$

1.3.3.Remark.Note that each edge is added to E_C at least twice in (1.3.2), since the pairs $(\underline{c},\underline{c}')$ and $(\underline{c}',\underline{c})$ contribute exactly the same set of edges.

1.3.4.Example. Take n=2 , C = { 01,10,11 }.We get:

$\underline{c}$	$\underline{c}'$	$\underline{c}\oplus\underline{c}'\oplus\underline{1}$	$\underline{u}$	edge
01	10	00	00	{01,10}
	11	01	00	{01,11}
			01	{00,10}
10	01	00	00	{10,01}
	11	10	00	{10,11}
			10	{00,01}
11	01	01	00	{11,01}
			01	{10,00}
	10	10	00	{11,10}
			10	{01,00}

table 3.

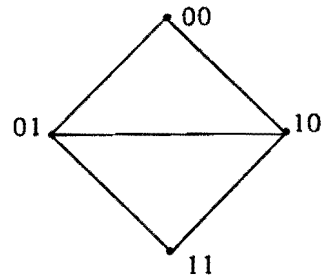


fig.5. Picture of G_C

Now if we compare the definition of our graph G_C with Theorem (1.2.4) we see that two vertices of the graph,say $\underline{d},\underline{d}'\in\mathbb{F}_2^n = V_C$,are connected by an edge iff the occurence of both $\underline{d}$ and $\underline{d}'$ in a code $D\subset\mathbb{F}_2^n$ would imply that (C,D) is not uniquely decodable.Hence if we choose a code D corresponding to a coclique in

G_C ,we have a u.d. codepair (C,D).We state this as follows:

1.3.5.Theorem.Let $n\in\mathbb{N}$, $C\subset\mathbb{F}_2^n$, G_C as in (1.3.2).Let $D\subset\mathbb{F}_2^n$ be any code.Then (C,D) is uniquely decodable if and only if D is a coclique in G_C .

Proof.(cf.(1.3.4).) (i) Suppose D is not a coclique in G_C .Obviously we have a pair $\{\underline{d},\underline{d}'\}\subset D$ such that $\{\underline{d},\underline{d}'\}\in E_C$ .According to the definition of E_C ,there are vectors $\underline{c},\underline{c}'\in C$, $\underline{c}\neq\underline{c}'$, $\underline{u}\in\mathbb{F}_2^n$ satisfying

(*) $\quad \underline{u} \sqsubset \underline{c} \oplus \underline{c}' \oplus \underline{1}$

(**) $\quad$ w.l.o.g. $\underline{d} = \underline{c} \oplus \underline{u}$, $\underline{d}' = \underline{c}' \oplus \underline{u}$.

Hence (1.2.4 (ii)) is violated and it follows from Theorem (1.2.4) that (C,D) is not uniquely decodable.

(ii) Suppose D is a coclique in G_C .According to the definition of E_C ,it is clear that (1.2.4 (ii)) holds.Now Theorem (1.2.4) implies that (C,D) is u.d..□

1.3.6.Remark.There is a strong relationship between the above and van Tilborg's results in [4].We shall give a rough explanation of this claim.Let $n\in\mathbb{N}$, $C\subset\mathbb{F}_2^n$. For any $\underline{v},\underline{w}\in\mathbb{F}_2^n$ such that $\underline{w} \sqsubset \underline{v}$ define

(15) $\quad C(\underline{v},\underline{w}) := \{ \underline{c} \in C \mid \forall_i: v_i = 1 \Rightarrow c_i = w_i \}$

$C(\underline{v},\underline{w})$ consists of all words in C which agree with a fixed vector $\underline{w}$ on those coordinates for which $v_i=1$.

Now ([4],Lemma 6) is more or less equivalent to the proposition that for any $\underline{v} \in\mathbb{F}_2^n$, $\underline{w} \sqsubset \underline{v}$, $\underline{u} \sqsubset \underline{v}$ the set

(16) $\{ \underline{c} \oplus \underline{u} \mid \underline{c} \in C(\underline{v},\underline{w}) \}$

is a clique in G_C .Similarly,([4],Lemma 7) is more or less equivalent to the proposition that

(17) $\{ \underline{c} \oplus \underline{u}' \mid \underline{c} \in C(\underline{v},\underline{w}) \}$

is a clique in G_C for any $\underline{v} \in \mathbb{F}_2^n$, $\underline{w} \sqsubset \underline{v}$, $\underline{u}' \oplus \underline{1} \sqsubset \underline{v}$ .Note that,writing $\underline{u}' = \underline{u} \oplus \underline{1}$ in (17),we get the same set of cliques in both cases!(The fact that in [4] Lemmas 6,7 not at all look the same is a consequence of the fact that $\underline{c} + \underline{d} = \underline{c}' + \underline{d}' \Leftrightarrow \underline{c} + (\underline{d}' \oplus \underline{1}) = \underline{c}' + (\underline{d} \oplus \underline{1})$,which is easy to check. (cf.(2.3.1).) A consequence of the above is that it is sufficient to consider all cliques obtained from (16),(17) with $w_H(\underline{u}) \leq \lfloor \frac{1}{2}n \rfloor$, $w_H(\underline{u}') \leq \lfloor \frac{1}{2}n \rfloor$,where w_H denotes Hamming weight.)

In the following we will not make use of the above.However,we mention that the observations in [4] lead to the following theorem:

1.3.7.Theorem.(van Tilborg,[4].)Let $n \in \mathbb{N}$, $C \subset \mathbb{F}_2^n$ .Let α_i ,$0 \leq i \leq r$,be the Krawtchouk coefficients of the annihilator polynomial $\alpha(x)$ of a code C.(See Sloane & Mc.Williams,[7].)Then,for any $D \subset \mathbb{F}_2^n$ such that (C,D) is u.d. we have

(18) $$|D| \leq \sum_{k=0}^{r} \max\{0,\alpha_k\}.\binom{n}{k}.2^{\min\{k,n-k\}}$$

Moreover,a method for constructing D is proposed in [4].In the above terminology this method leans upon the idea that,in order to pick the maximum number of vertices with no two in the same clique (i.e. a coclique),one should avoid vertices occuring in more than one clique.This method turns out to be quite successfull.

1.4. Calculation of $|E_C|$. Lower bounds on $|D|$.

Now we turn back to our graph G_C. In order to enable ourselves to apply Theorem (1.3.1) we should count the number of edges in the graph. The following theorem gives an upperbound.

1.4.1. Theorem. Let $n \in \mathbb{N}$, $C \subset \mathbb{F}_2^n$, $G_C = (V_C, E_C)$ as in (1.3.2). Then

$$|E_C| \leq 2^{n-1} . |C| . \sum_{i=1}^{n} A_i \, 2^{-i} \quad \text{, where} \tag{19}$$

$$A_i := \frac{1}{|C|} \, | \{ (\underline{c}, \underline{c}') \in C^2 \mid d_H(\underline{c}, \underline{c}') = i \} | \tag{20}$$

Here d_H denotes Hamming distance and (A_i) is the distance distribution of C.

Proof. From the definition of E_C and (1.3.3) we have (note that the number of vectors $\underline{u}$ s.t. $\underline{u} \sqsubset \underline{c} \oplus \underline{c}' \oplus \underline{1}$ is $2^{n-d_H(\underline{c},\underline{c}')}$) that

$$|E_C| \leq \tfrac{1}{2} \sum_{\underline{c} \in C} \sum_{\underline{c}' \in C \setminus \{\underline{c}\}} 2^{n-d_H(\underline{c},\underline{c}')} = \tfrac{1}{2} \sum_{i=1}^{n} \sum_{(\underline{c},\underline{c}') \in C^2 \mid d_H(\underline{c},\underline{c}')=i} 2^{n-i} = \tag{21}$$

$$\tfrac{1}{2} \sum_{i=1}^{n} |C| . A_i \, 2^{n-i} = 2^{n-1} . |C| . \sum_{i=1}^{n} A_i \, 2^{-i} \, . \qquad \square$$

1.4.2. Example. Take n and C as in (1.3.4). Note that $A_1 = 4/3$, $A_2 = 2/3$. So (1.4.1) implies that $|E_C| \leq 2.3.(\frac{1}{2}.\frac{4}{3} + \frac{1}{4}.\frac{2}{3}) = 5$. Note that, in this example, (1.4.1) gives the exact value. This follows from the fact that each edge is counted exactly twice as we can verify in table 3.

Now application of Theorems (1.3.1), (1.3.5) and (1.4.1) leads to the following theorem.

1.4.3.Theorem.Let $n\in\mathbb{N}$,$C\subset\mathbb{F}_2^n$ .Let A_i $(i=0,\ldots,n)$ be the distance enumerator of C.(cf. (20).) Then there is a code $D\subset\mathbb{F}_2^n$ such that (C,D) is u.d. and

$$(22)\qquad |D| \geq \frac{2^n}{1 + |C|.\sum_{i=1}^{n} A_i\, 2^{-i}} \quad .$$

Proof.Apply (1.3.1),(1.3.5) and (1.4.1). □

1.4.4.Corollary.Let C be a binary code of length n with minimum distance at least d.Then there is a code $D\subset\mathbb{F}_2^n$ such that (C,D) is u.d. and

$$(23)\qquad |D| \geq \frac{2^n}{1 + 2^{-d}.|C|.(|C|-1)} \quad .$$

Proof.It is well-known that for any code C : $\sum_{i=1}^{n} A_i = |C|-1$ .Note that the definition of d implies that $A_1 = A_2 = \ldots = A_{d-1} = 0$ .So $\sum_{i=1}^{n} A_i\, 2^{-i} = \sum_{i=d}^{n} A_i\, 2^{-i} \leq 2^{-d} \sum_{i=d}^{n} A_i = 2^{-d}(|C|-1)$,which,together with (1.4.3),proves the statement. □

1.4.5.Remark.Note that (1.4.3),(1.4.4) only state the existence of a code D of specified size.The proof of (1.3.1) is not provided with an explicit construction method for a coclique which is big enough.Consequently,(1.4.3),(1.4.4) are nonconstructive.

We will illustrate (1.4.3) and (1.4.4) with some examples.First we state a result which can easily be obtained from (1.4.4) and the following well-known theorem:

1.4.6.Theorem.(Gilbert-Varshamov lower bound,[7]).Suppose $0 \le \delta < \frac{1}{2}$ .Then there exists an infinite sequence of $[n,k,d]$ binary linear codes with $d/n \ge \delta$ and rate $R = k/n$ satisfying $R \ge 1-H(d/n)$,for all n.($H(x)$ as in (0.4.1).)

1.4.7.Theorem.Let $H(x) := -x\,^2\log x - (1-x)\,^2\log(1-x)$ .Define ξ by $0 \le \xi < \frac{1}{4}$, $1-H(2\xi) = \xi$.(so $=0.1412...$) Let $0 \le R_1 \le 1$ s.t. $1-2R_1+H^{\leftarrow}(1-R_1) \ge 0$.(So, $0 \le R_1 \le 0.54744...$ .Here $0 \le H^{\leftarrow}(x) \le \frac{1}{2}$.)Then for arbitrarily large n there is a uniquely decodable codepair (C,D) ,where C is a linear code of rate $R_1-o(1)$ such that

$$(24) \qquad R_2 \ge \begin{cases} 1 - o(1) & \text{if } 0 \le R_1 \le \xi \\ 1 - 2R_1 + H^{\leftarrow}(1-R_1) - o(1) & \text{if } \xi < R_1 \end{cases} .$$

Here $o(1)$ is vanishingly small if n tends to infinity.

Proof.First note that the existence of an $[n,k,d]$ linear code implies the existence of $[n,\ell,d]$ linear codes for all $\ell \le k$ .Now let $0 \le R_1 \le \xi$ .This implies $1 - H(2R_1) \ge R_1$ .From (1.4.6) we can find a linear code C' of minimum distance $\lceil 2nR_1 \rceil$ of dimension $k \ge n(1-H(2R_1)) \ge nR_1$ .Now the above observation implies that there is a linear code C of the same minimum distance with rate $R_1 - o(1)$. Application of (1.4.4) leads to the conclusion that there is a code D s.t. (C,D) is u.d. and

$$(25) \qquad |D| \ge \frac{2^n}{1 + 2^{-2nR_1}.(2^{nR_1})^2} = 2^{n-1} ,$$

which implies $R_2 \ge 1 - \frac{1}{n}$.

Next,let $\xi < R_1$ .Define $\delta := H^{\leftarrow}(1-R_1)$ and find a linear code C of length n , minimum distance $\lceil \delta n \rceil$ and dimension $\lfloor n(1-H(\delta)) \rfloor = n(R_1 - o(1))$ .The existence

of C is guaranteed by (1.4.6) and its rate is $R_1 - o(1)$ .Application of (1.4.4) leads to the conclusion that there is a code D such that (C,D) is u.d. and

$$(26) \qquad |D| \geq \frac{2^n}{1 + 2^{-\delta n}.(2^{nR_1})^2} \overset{(*)}{\geq} \frac{2^n}{2.2^{n(2R_1-\delta)}} = 2^{n[1-2R_1+H^{\leftarrow}(1-R_1)]-1},$$

which implies that $R_2 \geq 1 - 2R_1 + H^{\leftarrow}(1-R_1) - o(1)$ .Note that (*) follows from $2R_1 \geq \delta$,which is a consequence from the fact that $R_1 > \xi$. □

1.4.8.Remarks. (i) Note that (1.4.7) is not only non-constructive w.r.t. D but also w.r.t. C.

(ii) Moreover (1.4.7) is much weaker than (0.4.1) as we can see in fig.6..

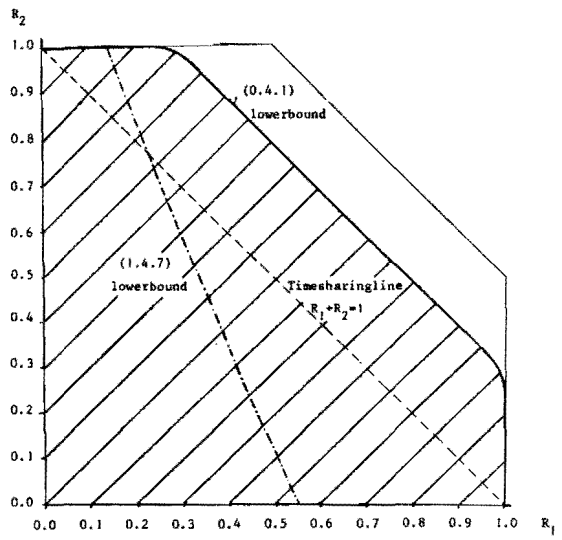


fig.6.

1.4.9.Examples on (1.4.3) and (1.4.4). (i) For the code from (1.3.4) we have d = 1 in (1.4.4).This leads to $|D| \geq \lceil 4/(1+\frac{1}{2}.3.2) \rceil = 1$,while (1.4.3) states that $|D| \geq \lceil 4/(1+3.(\frac{1}{2}.\frac{4}{3} + \frac{1}{4}.\frac{2}{3})) \rceil = \lceil \frac{8}{7} \rceil = 2$ .This illustrates that (1.4.4) is weaker than (1.4.3).Note that (1.4.3) is sharp in this case.

(ii) n = 5 , C = {0,3,12,30,27,21} .Here C is given in binary notation,which means that we denote any vector $\underline{c} = (c_1,c_2,\ldots,c_n)$ by the number $\sum_{i=1}^{n} c_i\, 2^{n-i}$.

(From now on we shall use this notation for codes with relatively big n.)We have $A_0 = 1$, $A_1 = A_5 = 0$, $A_2 = A_3 = A_4 = 10/6$.(1.4.4) gives $|D| \geq 4$; (1.4.3) gives $|D| \geq 6$; (1.3.7) gives $|D| \leq 17$ .It can be shown that the maximum size of D such that (C,D) be u.d. is 15 .For example,take D = {6,7,9, 10,13,14,15,16,18,21,22,24,25,26,29} .Note that the ratepair belonging to (C,D) is (0.51699,0.78138) which is above the lower bound obtained from (0.4.1) since $R_1+R_2 = 1.29837 > \frac{1}{2}\,{}^2\log 6$.

(iii) n = 5 , C = {0,3,12,31,26,21} .Here we have $A_0 = 1$, $A_1 = 0$, $A_2 = 8/6$, $A_3 = 16/6$, $A_4 = 4/6$, $A_5 = 2/6$.(1.4.4) gives $|D| \geq 4$; (1.4.3) gives $|D| \geq 7$ and (1.3.7) gives $|D| \leq 17$ .In [4] it is shown that the maximum size of D such that (C,D) be u.d. is 15 ,and all codes D which achieve this bound are given. The same ratepair as in (ii) is obtained.

(iv) In the following table parameters [n,k,d] are listed for which the existence of BCH (and hence linear) codes is known.We have $R_1 = k/n$ .Application of (1.4.4) gives the lower bound on R_2 .Note that in this case the linear code C of the pair (C,D) is explicitely known,which is not the case in (0.4.1) !

n	k	d	R_1	$R_2 \geq$	$R_1+R_2 \geq$
31	6	15	0.19355	0.99460	1.18815
32	6	16	0.18750	0.99731	1.18481
63	10	27	0.15873	0.99982	1.15855
64	10	28	0.15625	0.99991	1.15616
127	22	47	0.17323	0.99866	1.17189
128	22	48	0.17188	0.99931	1.17119
127	15	55	0.11811	$1-4.10^{-10}$	1.11811
128	15	56	0.11719	$1-2.10^{-10}$	1.11719
255	37	91	0.14510	$1-5.10^{-8}$	1.14510
256	37	92	0.14453	$1-2\frac{1}{2}.10^{-8}$	1.14453

table 4.

1.5. A closer look at $|E_C|$ increases the bound.

As observed in (1.3.3), in the definition of E_C each edge is added to E_C at least twice. In this section we shall have an investigation of the exact number of times any edge is added. The following lemma shows under which circumstances any edge may be added more than twice.

1.5.1. Lemma. Let $n \in \mathbb{N}$, $C \subset \mathbb{F}_2^n$. Let $\underline{c}_1, \underline{c}_1', \underline{c}_2, \underline{c}_2' \in C$. For $\underline{c}, \underline{c}' \in C$ define

$$E(\underline{c},\underline{c}') := \bigcup_{\underline{u} \sqsubset \underline{c} \oplus \underline{c}' \oplus \underline{1}} \{ \{ \underline{c} \oplus \underline{u} , \underline{c}' \oplus \underline{u} \} \} \quad . \tag{27}$$

(This is the set of edges contributed to E_C by the pair $(\underline{c},\underline{c}') \in C^2$.) Then we have

(i) Either $E(\underline{c}_1,\underline{c}_1')$ and $E(\underline{c}_2,\underline{c}_2')$ are disjoint or they coincide.

(ii) $E(\underline{c}_1,\underline{c}_1') = E(\underline{c}_2,\underline{c}_2') \Leftrightarrow \{ \underline{c}_2 , \underline{c}_2' \} \in E(\underline{c}_1,\underline{c}_1')$.

Proof. First note that both sides in (ii) are false if $E(\underline{c}_1,\underline{c}_1') \cap E(\underline{c}_2,\underline{c}_2') = \emptyset$ since $\{\underline{c}_2,\underline{c}_2'\} \in E(\underline{c}_2,\underline{c}_2')$. (I)

Now assume $E(\underline{c}_1,\underline{c}_1') \cap E(\underline{c}_2,\underline{c}_2') \neq \emptyset$. (II)

Note that $U_i := \{\underline{u} \in \mathbb{F}_2^n \mid \underline{u} \sqsubset \underline{c}_i \oplus \underline{c}_i' \oplus \underline{1} \}$ is a subspace in $\mathbb{F}_2^n$. By assumption, we have $\underline{u}_1 \in U_1$, $\underline{u}_2 \in U_2$ such that $\{\underline{c}_1 \oplus \underline{u}_1, \underline{c}_1' \oplus \underline{u}_1\} = \{\underline{c}_2 \oplus \underline{u}_2, \underline{c}_2' \oplus \underline{u}_2\}$ (*).

Adding the two vectors in each of these sets we obtain $\underline{c}_1 \oplus \underline{c}_1' = \underline{c}_2 \oplus \underline{c}_2'$. Hence from the definition of U_i we have $U_1 = U_2$ (**).

So, in particular, $\underline{u}_1 \oplus \underline{u}_2 \in U_1$. Hence, adding $\underline{u}_2$ to the vectors on both sides in (*) we find that $\{\underline{c}_2,\underline{c}_2'\} = \{\underline{c}_1 \oplus (\underline{u}_1 \oplus \underline{u}_2), \underline{c}_1' \oplus (\underline{u}_1 \oplus \underline{u}_2)\} \in E(\underline{c}_1,\underline{c}_1')$. This proves the RHS of (ii). Now we show that assumption (II) also implies the LHS of (ii). Note that this proves (i)! Indeed, take any edge $\{\underline{c}_2 \oplus \underline{v}, \underline{c}_2' \oplus \underline{v}\} \in E(\underline{c}_2,\underline{c}_2')$. Here

$\underline{v} \in U_2$ .Using the RHS of (ii) we find a $\underline{u} \in U_1$ such that $\{\underline{c}_2 \oplus \underline{v}, \underline{c}_2' \oplus \underline{v}\} = \{(\underline{c}_1 \oplus \underline{u}) \oplus \underline{v}, (\underline{c}_1' \oplus \underline{u}) \oplus \underline{v}\}$ .Hence this edge is in $E(\underline{c}_1, \underline{c}_1')$ since we conclude from (**) that $\underline{u} \oplus \underline{v} \in U_1$ .This shows that $E(\underline{c}_2, \underline{c}_2') \subset E(\underline{c}_1, \underline{c}_1')$ .Interchanging the role of $(\underline{c}_1, \underline{c}_1')$ and $(\underline{c}_2, \underline{c}_2')$ we find that the LHS of (ii) is satisfied.
Now we conclude (ii) from the fact that either both sides are false (case(I)) or both are true (case(II)). □

1.5.2.Example.Let $n=5$, $C = \{\underline{c}_1, \underline{c}_1', \underline{c}_2, \underline{c}_2'\}$ as below.We have $\underline{c}_2 = \underline{c}_1 \oplus \underline{w}$, $\underline{c}_2' = \underline{c}_1' \oplus \underline{w}$, $\underline{w} \in U_1$.(that is, $\underline{w} \sqsubset \underline{c}_1 \oplus \underline{c}_1' \oplus \underline{1}$).Note that we do not consider all edges in E_C .

		$\underline{u}$	edge		
$\underline{c}_1$	0 1 1 0 1	0 0 0 0 0	{0 1 1 0 1 , 1 0 0 0 1}	a	$E(\underline{c}_1, \underline{c}_1')$
$\underline{c}_1'$	1 0 0 0 1	0 0 0 0 1	{0 1 1 0 0 , 1 0 0 0 0}	b	
		0 0 0 1 0	{0 1 1 1 1 , 1 0 0 1 1}	c	
$\underline{w}$	0 0 0 1 0	0 0 0 1 1	{0 1 1 1 0 , 1 0 0 1 0}	d	
$\underline{c}_2$	0 1 1 1 1	0 0 0 0 0	{0 1 1 1 1 , 1 0 0 1 1}	c	$E(\underline{c}_2, \underline{c}_2')$
$\underline{c}_2'$	1 0 0 1 1	0 0 0 0 1	{0 1 1 1 0 , 1 0 0 1 0}	d	
		0 0 0 1 0	{0 1 1 0 1 , 1 0 0 0 1}	a	
		0 0 0 1 1	{0 1 1 0 0 , 1 0 0 0 0}	b	

table 5.

1.5.3.Remark.Note that $\{\underline{c}, \underline{c}'\} \in E(\underline{c}, \underline{c}')$ implies (according to (1.5.1(ii))) that $E(\underline{c}, \underline{c}') = E(\underline{c}', \underline{c})$ as mentioned in (1.3.3).

Now we state the main result of this section.

1.5.4.Theorem.Let $n \in \mathbb{N}$, $C \subset \mathbb{F}_2^n$, $G_C = (V_C, E_C)$ as in (1.3.2).For $\underline{c}, \underline{c}' \in C$ define (cf. (27) and §1.3.)

(28) $$N_C(\underline{c},\underline{c}') := |\, E(\underline{c},\underline{c}') \cap P_2(C) \,| \,.$$

That is, the number of edges in $E(\underline{c},\underline{c}')$ being a 2-subset of C. Then

(29) $$|E_C| = \tfrac{1}{2} \sum_{\underline{c}\in C} \sum_{\underline{c}'\in C\setminus\{\underline{c}\}} \frac{2^{n-d_H(\underline{c},\underline{c}')}}{N_C(\underline{c},\underline{c}')} \,.$$

Proof. It is clear that $2N_C(\underline{c},\underline{c}')$ equals the number of ordered pairs $(\underline{c}_2,\underline{c}_2')$ such that $\{\underline{c}_2,\underline{c}_2'\} \in E(\underline{c},\underline{c}')$. According to (1.5.1) this implies that any edge in $E(\underline{c},\underline{c}')$ is added to E_C exactly $2N_C(\underline{c},\underline{c}')$ times in (1.3.2). So, dividing by this number, we count each edge exactly once in (29). □

The following lemma may be usefull for calculating the numbers $N_C(\underline{c},\underline{c}')$ in practice.

1.5.5. Lemma. Let $n\in\mathbb{N}$, $C\subset\mathbb{F}_2^n$, $N_C(\underline{c},\underline{c}')$ as in (28) for $\underline{c},\underline{c}'\in C$. Then we have

(30) $$N_C(\underline{c},\underline{c}') = |\{\underline{v} \sqsubset \underline{c}\oplus\underline{c}'\oplus\underline{1} \mid \underline{c}\oplus\underline{v} \in C \wedge \underline{c}'\oplus\underline{v} \in C\}|$$
$$|\{\underline{u} \in \mathbb{F}_2^n \mid \underline{c}\oplus\underline{c}' \sqsubset \underline{u} \wedge \underline{c}\oplus\underline{u} \in C \wedge \underline{c}'\oplus\underline{u} \in C\}| \,.$$

Proof. The first equation is immediate from (28) and (27). Now define $\underline{u} := \underline{v}\oplus\underline{c}\oplus\underline{c}'$ (and hence $\underline{v} = \underline{u}\oplus\underline{c}\oplus\underline{c}'$). We have $\{\underline{c}\oplus\underline{u},\underline{c}'\oplus\underline{u}\} = \{\underline{c}\oplus\underline{v},\underline{c}'\oplus\underline{v}\}$. Hence if one of these is a subset of C so is the other. Moreover we have $\underline{c}\oplus\underline{c}' \sqsubset \underline{u} \Leftrightarrow \underline{v} \sqsubset \underline{c}\oplus\underline{c}'\oplus\underline{1}$ (*). Indeed, suppose $\underline{c}\oplus\underline{c}' \sqsubset \underline{u}$, then for any coordinate i such that $v_i=1$ we cannot have $c_i\neq c_i'$, $u_i=0$. Hence $v_i=1$ implies $c_i=c_i'$. Conversely, assuming $\underline{v} \sqsubset \underline{c}\oplus\underline{c}'\oplus\underline{1}$, we have that $c_i\neq c_i'$ implies $v_i=0$, which yields $u_i=1$. This proves (*).
So there is a unique correspondence between the vectors $\underline{u}$ and the vectors $\underline{v}$ in (30), which proves the second equation. □

As a consequence of Theorem (1.5.4) we have:

1.5.6.Theorem.Let $n\in\mathbb{N}$, $C\subset\mathbb{F}_2^n$ .For $\underline{c},\underline{c}'\in C$ let $N_C(\underline{c},\underline{c}')$ be as in (28).Then there is a code $D\subset\mathbb{F}_2^n$ such that (C,D) is uniquely decodable and

$$(31)\qquad |D| \geq \frac{2^n}{1 + \sum_{(\underline{c},\underline{c}')\in C^2 \mid \underline{c}\neq\underline{c}'} 2^{-d_H(\underline{c},\underline{c}')}/N_C(\underline{c},\underline{c}')} \quad .$$

Proof.Application of (1.3.1),(1.3.5) and (1.5.4). □

1.5.7.Examples. (i) In (1.3.4) we have $N_C(\underline{c},\underline{c}') = 1$ for all $\underline{c}\neq\underline{c}'$ .So in this case (1.4.1) and (1.4.3) give the same results as (1.5.4) resp. (1.5.6).

(ii) Let $C = \{ \underline{c}_1,\underline{c}_1',\underline{c}_2,\underline{c}_2' \}$ as in (1.5.2) .We have,as one can easily verify:

$\underline{c}$	$\underline{c}'$	$d_H(\underline{c},\underline{c}')=d_H(\underline{c}',\underline{c})$	$N_C(\underline{c},\underline{c}')=N_C(\underline{c}',\underline{c})$
$\underline{c}_1$	$\underline{c}_1'$	3	2
	$\underline{c}_2$	1	2
	$\underline{c}_2'$	4	1
$\underline{c}_1'$	$\underline{c}_2$	4	1
	$\underline{c}_2'$	1	2
$\underline{c}_2$	$\underline{c}_2'$	3	2

$A_0 = 1$

$A_1 = A_3 = A_4 = 1$

$A_2 = A_5 = 0$

table 6.

Now (1.4.1) and (1.4.3) state that $|E_C| \leq 44$, $|D| \geq 9$,but from (1.5.4) and (1.5.6) we obtain $|E_C| = 24$, $|D| \geq 13$.

1.5.8.Remark.In order to apply (1.5.6) we should be able to calculate the num-

bers $N_C(\underline{c},\underline{c}')$ .Unless C is a very structured code this seems to be very difficult.However,since for any C , $\underline{c},\underline{c}' \in C$ we have $N_C(\underline{c},\underline{c}') \geq 1$,we might use (1.5.6) already if we only know some of the numbers $N_C(\underline{c},\underline{c}')$ .The case of interest is of course that we know these numbers for pairs $(\underline{c},\underline{c}')$ with relatively small Hamming distance,since these give the greatest terms in (31).

Of course we can enumerate the numbers $N_C(\underline{c},\underline{c}')$ for any code C using the computer.However,this will only be possible in practice if $|C|$ is relatively small, since there are $\binom{|C|}{2}$ numbers to be calculated.

In the following section we show that,if C is a linear code,the calculation of $N_C(\underline{c},\underline{c}')$ is less laborious.

1.6.For linear codes the bound is more easily to be calculated.

In this section we make use of the fact that,if C is a linear code,for any $\underline{c} \in C$, $\underline{v} \in \mathbb{F}_2^n$:

(32) $\qquad \underline{c} \oplus \underline{v} \in C \Leftrightarrow \underline{v} \in C$.

The main consequence of this is the following:

1.6.1.Lemma.Let $n \in \mathbb{N}$, $C \subset \mathbb{F}_2^n$ a linear code.For $\underline{c},\underline{c}' \in C$ let $N_C(\underline{c},\underline{c}')$ be as in (28).Define

(33) $\qquad L_C(\underline{c}) := |\{ \underline{v} \in C \mid \underline{v} \sqsubset \underline{c} \oplus \underline{1} \}|$.

Then for $\underline{c},\underline{c}' \in C$, $\underline{c} \neq \underline{c}'$ we have $N_C(\underline{c},\underline{c}') = L_C(\underline{c} \oplus \underline{c}')$.

Proof.This follows immediate from Lemma (1.5.5) and (32). □

1.6.2.Remark.Note that the set on the RHS in (33) is a linear subcode of C (determined by $\underline{c}$) since it consists of all codewords $\underline{v}\in C$ satisfying the extra (possibly dependent) parity checks $v_i=0$ for all i such that $c_i\neq c_i'$ .So $L_C(\underline{c})$ is a power of 2 .According to the second equation in (30) it is clear that we also have the equality $L_C(\underline{c}) = |\{ \underline{u}\in C \mid \underline{c} \sqsubset \underline{u} \}|$.

Now for linear codes (1.5.4) takes the form

1.6.3.Theorem.Let $n\in\mathbb{N}$, $C\subset\mathbb{F}_2^n$ a linear code, $G_C = (V_C ,E_C)$ as in (1.3.2).For $\underline{c}\in C$ define $L_C(\underline{c})$ as in (33).Then

$$|E_C| = \tfrac{1}{2}|C| \sum_{\underline{c}\in C\setminus\{\underline{0}\}} \frac{2^{n-w_H(\underline{c})}}{L_C(\underline{c})} \quad . \tag{34}$$

Proof.Note that,from (1.6.1) and (32):

$$\sum_{\underline{c}\in C}\sum_{\underline{c}'\in C\setminus\{\underline{c}\}} \frac{2^{n-d_H(\underline{c},\underline{c}')}}{N_C(\underline{c},\underline{c}')} = \sum_{\underline{c}\in C}\sum_{\underline{c}'\in C\setminus\{\underline{c}\}} \frac{2^{n-w_H(\underline{c}\oplus\underline{c}')}}{L_C(\underline{c}\oplus\underline{c}')} = \tag{35}$$

$$|C|\cdot \sum_{\underline{y}\in C\setminus\{\underline{0}\}} \frac{2^{n-w_H(\underline{y})}}{L_C(\underline{y})} \text{ and apply (1.5.4).}$$

□

From the above we obtain:

1.6.4.Theorem.Let $n\in\mathbb{N}$, $k\in\mathbb{N}$, $C\subset\mathbb{F}_2^n$ a linear code of dimension k.Let for $\underline{c}\in C$ $L_C(\underline{c})$ be as in (33).Then there is a code $D\subset\mathbb{F}_2^n$ such that (C,D) is u.d. and

$$|D| \geq \frac{2^n}{1 + 2^k \sum_{\underline{c}\in C\setminus\{\underline{0}\}} 2^{-w_H(\underline{c})}/L_C(\underline{c})} \quad . \tag{36}$$

Proof. Application of (1.3.1),(1.3.5) and (1.6.3). □

1.6.5. Remark. Note that, in order to apply (1.6.4), we only need to calculate $|C|-1$ different numbers.

1.6.6. Examples. (i) (cf.[7].) Let $n=24$, $C = G_{24}$, that is, the well-known binary Golay code. Here $k=12$. In the following table the several parameters of interest are listed.

# $\underline{c}$	$w_H(\underline{c})$	$w_H(\underline{u})$	$\#_{\underline{u}\in G_{24}}(\underline{c} \sqsubset \underline{u})$	$L_C(\underline{c})$ (cf.(1.6.2).)
$A_8 = 759$	8	8	1	
		12	0	
		16	30 (*)	
		24	1	32
$A_{12}=2576$	12	12	1	
		16	0	
		24	1	2
$A_{16}= 759$	16	16	1	
		24	1	2
$A_{24}= 1$	24	24	1	1

table 7.

Krawtchouk expansion of the annihilator polynomial :

$$\alpha(x) = P_0(x) + P_1(x) + P_2(x) + P_3(x) + \frac{1}{6} P_4(x)$$

We have $R_1 = \frac{1}{2}$. Moreover we obtain

from (1.3.7): $R_2 \leq 0.6450$, $|D| \leq 45.681$,

from (1.4.1),(1.4.3): $R_2 \geq 0.4229$, $|D| \geq 1.137$, $|E_C| \leq 123.878.246.400$,

from (1.6.3),(1.6.4): $R_2 \geq 0.5531$, $|D| \geq 9.915$, $|E_C| = 14.186.973.184$.

We remark that (*) is obtained from the following:

(a) The words of weight 16 are the complements of those of weight 8 ,and

(b) the words of weight 8 form a $S(5,8,24)$ of which all intersection numbers are known.

(ii) Consider the codes from (1.4.9(iv)) again.The ones of odd length are cyclic,which enables us to obtain an increase of the bound for R_2 by using (1.6.4).Assume the code length n is a prime.Then it follows that the period of each codeword is n or one,the latter only being possible for the words $\underline{0}$ and $\underline{1}$. Hence if $2^k \equiv 2 \bmod n$ we know that $\{\underline{0},\underline{1}\}\subset C$,from which it follows that

$$L_C(\underline{c}) \geq 2 \quad \text{if} \quad \underline{c} \neq \underline{1} \quad \text{,and}$$

$$A_i = A_{n-i} \quad \text{if } 0 \leq i \leq n \quad .$$

Since $d \leq i \leq n-d \Rightarrow 2^i + 2^{n-i} \leq 2^d + 2^{n-d}$ we obtain from (1.6.3):

$$|E_C| = \tfrac{1}{2}|C| \sum_{\underline{c}\in C\setminus\{\underline{0}\}} \frac{2^{n-w_H(\underline{c})}}{L_C(\underline{c})} \leq 2^{k-1}\left(\frac{2^k-2}{2}\left(\frac{2^{n-d}}{2}+\frac{2^d}{2}\right)+2^{n-n}\right) =$$

$$= 2^{k-1}\left((2^{k-1}-1)(2^{n-d-1}+2^{d-1})+1\right) \quad .$$

Now application of (1.3.1) and (1.3.5) gives the following lower bounds on R_2 :

n	k	d	R_1	$R_2 \geq$	$R_1+R_2 \geq$
31	6	15	0.19355	0.99793	1.19148
127	22	47	0.17323	0.99965	1.17288

table 8.

(The other codes from table 4 do not satisfy the conditions mentioned above.) Note that for the code of length 31 both the weight enumerator and the numbers $L_C(\underline{c})$ are determined by the above,namely $A_0 = A_{31} = 1$,$A_{15} = A_{16} = 31$,

$L_C(\underline{c}) = 2$ if $w_H(\underline{c}) \in \{15,16\}$ and $L_C(\underline{1}) = 1$.

1.6.7.Remark.All lower bounds on $|D|$ given in this chapter depend on (1.3.1). In fact,Turán's Theorem is some stronger.It states:

Let $G = (V,E)$ be a graph.Denote the number of vertices by v and the number of edges by e .Then the maximum number of vertices occuring in any coclique of G is at least M_G,where $M_G = \min\{m \in \mathbb{N} \mid e \geq \lfloor \frac{v}{m} \rfloor . v - \binom{\lfloor v/m \rfloor + 1}{2} . m \}$.

Now all results from this Chapter may be restated according to the above. However,the lower bounds on $|D|$ obtained in this way cannot easily be given as simple explicit expressions.As far as the examples given in this chapter are concerned,the only case for which the increase of the bound is of interest is the code of length 31 from the preceding example.Using the results from (1.6.6(ii)) a further increase of 10^{-3} is obtained for the lower bound on R_2. This gives us the parameters $n=31$, $k=6$, $d=15$, $R_1=0.19355$, $R_2 \geq 0.99893$ and $R_1+R_2 \geq 1.19248$.

Chapter 2.Explicit constructions.

2.1,Abstract.

In this Chapter we will give an explicit construction method for uniquely decodable codepairs for our channel.It will be shown by examples that this method enables us to reach new ratepairs.Here "new" should be understood in the sense that the ratepair belonging to the constructed codepair is outside the convex hull of the set of all ratepairs belonging to codepairs known before.

Section 2.2. gives an explanation of the idea.In section 2.3. we present a simplified version of our construction,which can be obtained from the general result by a certain choice of the parameters.In section 2.4. the general result is presented.

2.2.A brief introduction.

This section gives a description of the idea which is developed more general and more precisely in the following sections.The reader should realize that, for later use,the terminology in the rest of this Chapter is slightly different from the following.

If one is looking for u.d. codepairs one finds that it is much easier to construct "almost u.d." codepairs.That is,the condition for being u.d. is violated only in a few specified cases.To be more precise,suppose that we have a codepair (C,D) (not u.d.) such that we can split C and D in two parts,say $C=C^{(0)} \cup C^{(1)}$, $D=D^{(0)} \cup D^{(1)}$ with the property that

$$(37)\qquad \forall_{\underline{c},\underline{c}'\in C\,|\,\underline{c}\neq\underline{c}'}\ \forall_{\underline{d},\underline{d}'\in D}\ [\ \underline{c}+\underline{d}=\underline{c}'+\underline{d}'\ \Rightarrow\ (\text{either } (\underline{c},\underline{d})\in C^{(0)}\times D^{(1)}\ \wedge\ (\underline{c}',\underline{d}')\in C^{(1)}\times D^{(0)}\ \text{ or }\ (\underline{c}',\underline{d}')\in C^{(0)}\times D^{(1)}\ \wedge\ (\underline{c},\underline{d})\in C^{(1)}\times D^{(0)}.)\ ]$$

For instance, split $C=\{00,11\}$ into $C^{(0)}=\{00\}$ and $C^{(1)}=\{11\}$, and $D=\mathbb{F}_2^2$ into $D^{(0)}=\{00\}$ and $D^{(1)}=\{01,10,11\}$.

Now suppose we send one extra bit for each block transmission in the following way. Each word from C is followed by a zero and each word from $D^{(i)}$ is followed by the symbol i $(i=0,1)$. So in fact we use the codepair $(\bar{C},\bar{D}=\bar{D}^{(0)}\cup\bar{D}^{(1)})$ where $\bar{C}=\{\,\underline{c}|0\mid \underline{c}\in C\,\}$ and $\bar{D}^{(i)}=\{\,\underline{d}|i\mid \underline{d}\in D^{(i)}\,\}$ $(i=0,1)$. We claim that the codepair $(\bar{C},\bar{D})$ is uniquely decodable. Indeed, suppose two different pairs $(\underline{c},\underline{d})$ and $(\underline{c}',\underline{d}')$ produce the same outputvector $\underline{c}+\underline{d}$. It follows from (37) that the new added symbols produce a 0 at the receiving end for one of these pairs and a 1 for the other.

However, the above srategy of labeling the codewords is not successfull, since we have introduced an increase of the block length which results in a decrease of the rates.

In order to avoid this deficiency we must actually <u>use</u> the extra length for more information. That is, we must define <u>sets</u> of labels, say $U^{(i)}$ and $V^{(i)}$, $i=0,1$ such that each word from $C^{(i)}$ may be followed by any word from $U^{(i)}$ $(i=0,1)$ and similar for $D^{(i)},V^{(i)}$. Here $U^{(i)}$ and $V^{(i)}$ are subsets of $\mathbb{F}_2^m$ for some $m\in\mathbb{N}$. (The strategy described above corresponds to the choice $m=1, U^{(0)}=U^{(1)}=\{0\}$, $V^{(0)}=\{0\}$, $V^{(1)}=\{1\}$.) So we wish to construct a u.d. codepair $(\mathcal{C},\mathcal{D})$ where

$$(38)\qquad \mathcal{C}:=\bigcup_{i=0,1}\{\,\underline{c}|\underline{u}\mid \underline{c}\in C^{(i)}\wedge\underline{u}\in U^{(i)}\,\}\ \text{ and }\ \mathcal{D}:=\bigcup_{i=0,1}\{\,\underline{d}|\underline{v}\mid \underline{d}\in D^{(i)}\wedge\underline{v}\in V^{(i)}\,\}.$$

How do we have to choose $U^{(i)}$ and $V^{(i)}$ such that the trick still works?In the first place $(U^{(k)},V^{(\ell)})$ must be u.d. for $k,\ell\in\{0,1\}$ .Indeed,suppose we can find k and ℓ such that $(U^{(k)},V^{(\ell)})$ is not u.d..Fix any $\underline{c}\in C^{(k)}$, $\underline{d}\in D^{(\ell)}$ and define $C' := \{ \underline{c}|\underline{u} \mid \underline{u}\in U^{(k)} \} \subset C$, $D' := \{ \underline{d}|\underline{v} \mid \underline{v}\in V^{(\ell)} \} \subset \mathcal{D}$ .Now (C',D') is not u.d. and hence the same holds for $(C,\mathcal{D})$.

Next,we must be sure that we can "identify" any pair $(\underline{c},\underline{d})\in(C^{(0)}\times D^{(1)})\cup(C^{(1)}\times D^{(0)})$ by looking at the sum $\underline{u}+\underline{v}$ of the corresponding pair of labels $(\underline{u},\underline{v})$ .So $U^{(i)}$ and $V^{(i)}$ must have the property that

(39) $$\forall_{\underline{u}\in U^{(0)}}\ \forall_{\underline{u}'\in U^{(1)}}\ \forall_{\underline{v}\in V^{(1)}}\ \forall_{\underline{v}'\in V^{(0)}}\ [\ \underline{u}+\underline{v}\neq\underline{u}'+\underline{v}'\ ]\ .$$

Indeed,if (39) were not the case,we could find $(\underline{c},\underline{d})\in C^{(0)}\times D^{(1)}$, $(\underline{c}',\underline{d}')\in C^{(1)}\times D^{(0)}$ and $(\underline{u},\underline{v})\in U^{(0)}\times V^{(1)}$, $(\underline{u}'\underline{v}')\in U^{(1)}\times V^{(0)}$ such that $\underline{c}|\underline{u}+\underline{d}|\underline{v}=\underline{c}'|\underline{u}'+\underline{d}'|\underline{v}'$.

2.2.1.Example.Choose $U^{(0)}=\{000,011,110\}$, $U^{(1)}=\{001,010,111\}$, $V^{(0)}=\{000,010\}$ and $V^{(1)}=\{101\}$ .Note that $(U^{(k)},V^{(\ell)})$ is u.d. for $k,\ell\in\{0,1\}$ and that (39) is satisfied.However,this choice does not give interesting results.

For reasons of convenience we give the following definition (cf.(39)):

2.2.2.Definition.Let C,C',D,D' be binary codes of length n.We say that (C,D) is orthogonal to (C',D') ,denoted by $(C,D)\perp(C',D')$,if

(40) $$\forall_{\underline{c}\in C}\ \forall_{\underline{c}'\in C'}\ \forall_{\underline{d}\in D}\ \forall_{\underline{d}'\in D}\ [\ \underline{c}+\underline{d}\neq\underline{c}'+\underline{d}\ ]\ .$$

2.3.A simple construction.

In the preceding section we have given a vague description of our construction. However,the general result looks entirely different.In this section we first

present a special case which may enable the reader to get some insight in the heart of the matter. In the terminology of §2.2. the construction presented here makes use of a special choice for the $U^{(i)}$, namely $U^{(1)}=\{\underline{u}\oplus\underline{1} \mid \underline{u}\in U^{(0)}\}$. The following simple lemma shows that this is a reasonable choice.

2.3.1.Lemma. Let C and D be binary codes of length n. Then (C,D) is uniquely decodable iff $(C\oplus\underline{1},D)$ is uniquely decodable. Here $C\oplus\underline{1} = \{ \underline{c}\oplus\underline{1} \mid \underline{c}\in C \}$.

Proof. Note that $\underline{c} \oplus \underline{1} = \underline{1} - \underline{c}$ for any $\underline{c}\in\mathbb{F}_2^n$. So for $\underline{c},\underline{c}'\in C$, $\underline{d},\underline{d}'\in D$ we have $\underline{c} + \underline{d} = \underline{c}' + \underline{d}' \Leftrightarrow \underline{1} - \underline{c}' + \underline{d} = \underline{1} - \underline{c} + \underline{d}' \Leftrightarrow (\underline{c}' \oplus \underline{1}) + \underline{d} = (\underline{c} \oplus \underline{1}) + \underline{d}'$. Hence if the condition on (C,D) for being u.d. is violated so is the condition on $(C\oplus\underline{1},D)$ and conversely. □

Now we can describe the construction as follows. (Note again that the terminology is different from §2.2.)

2.3.2.Theorem. Let $n,m\in\mathbb{N}$. Let there be codes $U,V,W \subset \mathbb{F}_2^m$ with the following properties:

(41)
(i) (U,V) and (U,W) are uniquely decodable.
(ii) $(U \oplus \underline{1},W) \perp (U,V)$.

Furthermore, let there be a binary codepair $(C,D\cup F)$ of length n such that there is a partition $C = C^{(0)} \cup C^{(1)}$ with the following properties:

(42)
(i) (C,D) and (C,F) are uniquely decodable.
(ii) $(C^{(i)},D \cup F)$ is uniquely decodable for $i=0,1$.
(iii) $(C^{(0)},F) \perp (C^{(1)},D)$.
(iv) $D \cap F = \emptyset$.

Then the codepair $(\mathcal{C},\mathcal{D})$ is uniquely decodable,where

$$(43)\qquad \begin{aligned} \mathcal{C} &:= (C^{(0)}|U\oplus\underline{1}) \cup (C^{(1)}|U) \quad \text{and} \\ \mathcal{D} &:= (D|W) \cup (F|V) \quad . \end{aligned}$$

Here,for any pair of codes $C_1\subset\mathbb{F}_2^{n_1}$, $C_2\subset\mathbb{F}_2^{n_2}$ $C_1|C_2$ denotes the set $\{\underline{c}_1|\underline{c}_2 \mid \underline{c}_1\in C_1 \wedge \underline{c}_2\in C_2\}$.

Proof.(see also 2.3.3(ii).)Suppose $\underline{c} = \underline{c}_1|\underline{c}_2 \in \mathcal{C}$, $\underline{c}' = \underline{c}_1'|\underline{c}_2' \in \mathcal{C}$, $\underline{d} = \underline{d}_1|\underline{d}_2 \in$ and $\underline{d}' = \underline{d}_1'|\underline{d}_2' \in \mathcal{D}$,such that $\underline{c} + \underline{d} = \underline{c}' + \underline{d}'$.
So,in particular, $\underline{c}_i + \underline{d}_i = \underline{c}_i' + \underline{d}_i'$ for $i=1,2$ $(*)$.
Since $\underline{c}_1,\underline{c}_1'\in C$ and $\underline{d}_1,\underline{d}_1'\in D\cup F$ the conditions (42)(i),(ii),(iii) state that we have

$$\begin{aligned} &\text{either (a) } \underline{c}_1 = \underline{c}_1' \ , \ \underline{d}_1 = \underline{d}_1' \\ &\text{or (b) w.l.o.g. } \underline{c}_1\in C^{(0)} \ , \ \underline{c}_1'\in C^{(1)} \ , \ \underline{d}_1\in D \ , \ \underline{d}_1'\in F \ . \end{aligned}$$

Now assume that (b) is the case.From the construction of $\mathcal{C}$ and $\mathcal{D}$ it then follow that $\underline{c}_2\in U\oplus\underline{1}$, $\underline{c}_2'\in U$, $\underline{d}_2\in W$ and $\underline{d}_2'\in V$ .This contradicts $(*)$ and (41)(ii) .
Hence we have (a) .But now both $(\underline{c}_2,\underline{d}_2)$ and $(\underline{c}_2',\underline{d}_2')$ are chosen from one of the codepairs (U,V) , (U,W) , $(U\oplus\underline{1},V)$ and $(U\oplus\underline{1},W)$ .These are all u.d. from (41)(i and Lemma 2.3.1..So,using $(*)$,we conclude that $\underline{c}_2=\underline{c}_2'$, $\underline{d}_2=\underline{d}_2'$ and hence $\underline{c}=\underline{c}'$, $\underline{d}=\underline{d}'$. [

2.3.3.Remarks. (i) The codepair $(\mathcal{C},\mathcal{D})$ has length $n+m$ and

$$(44)\qquad \begin{aligned} |\mathcal{C}| &= |C|.|U| \quad , \\ |\mathcal{D}| &= |D|.|W| + |F|.|V| \quad . \end{aligned}$$

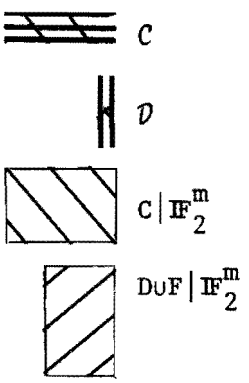
Hence,if (C,F) and (U,V) have ratepairs (R_1,R_2) resp. (R_1',R_2') ,then the ratepai

(R_1,R_2) of $(C,\mathcal{D})$ satisfies

$$(45) \qquad R_1 = \frac{nR_1 + mR_1'}{n+m} \quad , \quad R_2 > \frac{nR_2 + mR_2'}{n+m} \quad .$$

So this point is above the timesharingline between (R_1,R_2) and (R_1',R_2') .(Note that the roles of (V,F) and (W,D) are similar.)

(ii) We may illustrate the situation with a picture.In fig.7. we see all codes depicted in $\mathbb{F}_2^{n+m}\times\mathbb{F}_2^{n+m}$. Note that, if $\underline{c}=\underline{c}_1|\underline{c}_2$, $\underline{c}=\underline{c}_1'|\underline{c}_2'\in C$, $\underline{d}=\underline{d}_1|\underline{d}_2$, $\underline{d}'=\underline{d}_1'|\underline{d}_2'\in\mathcal{D}$ we can have $\underline{c}_1+\underline{d}_1=\underline{c}_1'+\underline{d}_1'$ only if $(\underline{c},\underline{d})$ is in one of the decorated squares and $(\underline{c}',\underline{d}')$ is in the other.However,if this is the case, $\underline{c}_2+\underline{d}_2\neq\underline{c}_2'+\underline{d}_2'$.



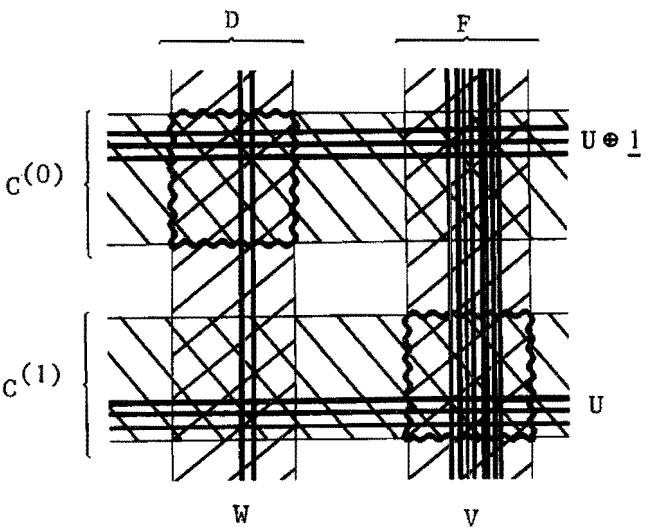


fig.7.

2.3.4.Examples. (i) Let m=3 , n=2 .U={001,011,101} , V={000,001,110,111} , W={000,110} ; C={00,11} , D={11} , F= {00,01,10} ; $C^{(0)}$={00} , $C^{(1)}$={11} . It is not difficult to check that (41) and (42) are satisfied.Now (2.3.2) states that $(C,\mathcal{D})$ is u.d. where C = {00110,00100,00010,11001,11011,11101} and

$\mathcal{D}$ = {11000,11110,00000,00001,00110,00111,01000,
01001,01110,01111,10000,10001,10110,10111} .

(ii) m=5 , n=2 .$C=C^{(0)}\cup C^{(1)}$,D and F are chosen as in (i) .

Let,in binary notation (cf.(1.4.9)(ii))

$U=\{0,3,12,21,27,30\}$, $V=\{6,7,9,10,13,14,15,16,18,21,22,24,25,26,29\}$, $W=\{22\}$. Again,(41) and (42) are satisfied.Now (2.3.2) states the existence of a u.d. codepair $(\mathcal{C},\mathcal{D})$ of length 7 with $|\mathcal{C}| = 12$, $|\mathcal{D}| = 46$.This yields the ratepair $R_1 = 0.51214$, $R_2 = 0.78908$ and $R_1 + R_2 = 1.30122$.Note that we have started with the ratepairs of (C,F) resp. (U,V) for which $R_1+R_2=1.29248$ resp. $R_1'+R_2'=1.29837$.

2.4.A more general construction method.

In this section,the idea of splitting the codes C and D (where (C,D) is not u.d.) as described in §2.2. is extended to the case that we may split C and D in more parts.As we shall see from the examples this enables us to obtain even better results than in the preceding section.We describe the construction as follows,where C and D do not have a similar role as in §2.2..

2.4.1.Theorem.Let $n,m \in \mathbb{N}$ .Let there be binary codes $U^{(i)},V^{(i)}$ $(i=0,1,2),W^{(i)}$ $(i=0,1)$ of length m with the following properties:

(46)
- (i) All codepairs $(U^{(i)},V^{(j)})$ $(i,j=0,1,2)$ and $(U^{(i)},W^{(j)})$ $(i=0,1,2$ and $j=0,1)$ are uniquely decodable.
- (ii) $(U^{(i)},V^{(j)}) \perp (U^{(j)},W^{(i)})$ for $\{i,j\} = \{0,1\}$.
- (iii) $(U^{(0)},W^{(1)}) \perp (U^{(1)},W^{(0)})$.

Furthermore,let there be given a binary codepair $(B\cup C,D\cup E\cup F)$ of length n such that there are partitions $C=C^{(0)}\cup C^{(1)}$, $D=D^{(0)}\cup D^{(1)}$, $F=F^{(0)}\cup F^{(1)}$ with the following properties:

(47)
(i) $(B \cup C, E \cup F)$ is uniquely decodable.
(ii) $(B \cup C^{(i)}, D \cup E \cup F)$ is uniquely decodable for $i=0,1$.
(iii) $(B \cup C, D^{(i)} \cup E \cup F^{(i)})$ is uniquely decodable for $i=0,1$.
(iv) $(C^{(0)},D^{(0)}) \perp (C^{(1)},D^{(1)})$.
(v) $(C^{(i)},D^{(i)}) \perp (C^{(j)},F^{(j)})$ for $\{i,j\} = \{0,1\}$.
(vi) $B \cap C = \phi$, $D \cap E = \phi$, $D \cap F = \phi$, $E \cap F = \phi$.

Then the codepair $(\mathcal{C},\mathcal{D})$ of length $n+m$ is uniquely decodable, where

(48)
$$\mathcal{C} := (C^{(0)}|U^{(0)}) \cup (C^{(1)}|U^{(1)}) \cup (B|U^{(2)}) \quad \text{and}$$
$$\mathcal{D} := (F^{(0)}|V^{(0)}) \cup (F^{(1)}|V^{(1)}) \cup (E|V^{(2)}) \cup (D^{(0)}|W^{(0)}) \cup (D^{(1)}|W^{(1)}).$$

Proof. Let $\underline{c} = \underline{c}_1|\underline{c}_2$ and $\underline{c}' = \underline{c}_1'|\underline{c}_2'$ be in $\mathcal{C}$, and $\underline{d} = \underline{d}_1|\underline{d}_2$, $\underline{d}' = \underline{d}_1'|\underline{d}_2'$ be in $\mathcal{D}$. Assume $\underline{c} + \underline{d} = \underline{c}' + \underline{d}'$. It follows that

$$\underline{c}_1 + \underline{d}_1 = \underline{c}_1' + \underline{d}_1' \ , \ \underline{c}_2 + \underline{d}_2 = \underline{c}_2' + \underline{d}_2' \qquad (*) \ .$$

First we show that

$$(\underline{c}_1 = \underline{c}_1' \wedge \underline{d}_1 = \underline{d}_1') \Leftrightarrow (\underline{c} = \underline{c}' \wedge \underline{d} = \underline{d}') \qquad (**) \ .$$

For, suppose the LHS in (**) holds. From (47)(vi) it then follows that we have either $\underline{c}_1,\underline{c}_1' \in B$ or $\underline{c}_1,\underline{c}_1' \in C^{(i)}$ for some $i \in \{0,1\}$. Similarly we have either $\underline{d}_1,\underline{d}_1' \in E$ or $\underline{d}_1,\underline{d}_1' \in D^{(i)}$ or $\underline{d}_1,\underline{d}_1' \in F^{(i)}$ for some $i \in \{0,1\}$.
But now it follows from the construction of $\mathcal{C}$ and $\mathcal{D}$ that $\underline{c}_2,\underline{c}_2' \in U^{(i)}$ for some $i \in \{0,1,2\}$, and either $\underline{d}_2,\underline{d}_2' \in V^{(i)}$ for some $i \in \{0,1,2\}$ or $\underline{d}_2,\underline{d}_2' \in W^{(i)}$ for some $i \in \{0,1\}$. From this, (*) and (46)(i) it is clear that $\underline{c}_2=\underline{c}_2'$, $\underline{d}_2=\underline{d}_2'$. This proves (**) .

Now consider the following cases:

(a) $\underline{c}_1,\underline{c}_1' \in B \cup C^{(i)}$ for $i=0$ or $i=1$.

Since $\underline{d}_1, \underline{d}_1' \in D \cup E \cup F$ we see from (*) and (47)(ii) that $\underline{c}_1 = \underline{c}_1'$ and $\underline{d}_1 = \underline{d}_1'$ .Now (**) implies that $\underline{c} = \underline{c}'$ and $\underline{d} = \underline{d}'$.

(b) $\underline{d}_1, \underline{d}_1' \in E \cup F$.

Since $\underline{c}_1, \underline{c}_1' \in B \cup C$ we see from (*) and (47)(i) that $\underline{c}_1 = \underline{c}_1'$ and $\underline{d}_1 = \underline{d}_1'$ .So,again from (**),it follows that $\underline{c} = \underline{c}'$ and $\underline{d} = \underline{d}'$.

(c) $\underline{d}_1, \underline{d}_1' \in D^{(i)} \cup E \cup F^{(i)}$ for i=0 or i=1 .

As in (b),using (47)(iii), we find that $\underline{c} = \underline{c}'$ and $\underline{d} = \underline{d}'$.

We note that (a) implies that we are done unless $\underline{c}_1 \in C^{(i)}$ and $\underline{c}_1' \in C^{(j)}$ for $\{i,j\} = \{0,1\}$ .So from now on we assume (w.l.o.g.) that $\underline{c}_1 \in C^{(0)}$, $\underline{c}_1' \in C^{(1)}$.

It follows from (48) that $\underline{c}_2 \in U^{(0)}$ and $\underline{c}_2' \in U^{(1)}$.

Note that (47)(iv) implies that we cannot have $\underline{d}_1 \in D^{(0)}$, $\underline{d}_1' \in D^{(1)}$.Similarly (47)(v) implies that we cannot have $\underline{d}_1 \in D^{(0)}$, $\underline{d}_1' \in F^{(1)}$ or $\underline{d}_1 \in F^{(0)}$, $\underline{d}_1' \in D^{(1)}$.

Hence,according to (b) and (c),the only cases remaining to check are:

(d) $\underline{d}_1 \in D^{(1)}$, $\underline{d}_1' \in D^{(0)}$ .From (48) we have $\underline{d}_2 \in W^{(1)}$, $\underline{d}_2' \in W^{(0)}$,which is impossible by (46)(iii) and (*) .

(e) $\underline{d}_1 \in D^{(1)}$, $\underline{d}_1' \in F^{(0)}$ .Again from (48) we have $\underline{d}_2 \in W^{(1)}$, $\underline{d}_2' \in V^{(0)}$ .This is impossible by (46)(ii) and (*) .

(f) $\underline{d}_1 \in F^{(1)}$, $\underline{d}_1' \in D^{(0)}$.(48) implies that $\underline{d}_2 \in V^{(1)}$, $\underline{d}_2' \in W^{(0)}$ .This is impossible by (46)(ii) and (*) .

Hence,since the above covers all cases, $(C,\mathcal{D})$ is u.d.. □

2.4.2.Remarks.(examples will be given in (2.4.4).)

(i) We have made a codepair $(C,\mathcal{D})$ of length n+m with

$$(49) \qquad |C| = |C^{(0)}|.|U^{(0)}| + |C^{(1)}|.|U^{(1)}| + |B|.|U^{(2)}|$$

$$(49) \qquad |\mathcal{D}| = |F^{(0)}|.|V^{(0)}| + |F^{(1)}|.|V^{(1)}| + |E|.|V^{(2)}|$$
$$|D^{(0)}|.|W^{(0)}| + |D^{(1)}|.|W^{(1)}| \quad .$$

This may,as in (2.3.3.(i)),enable us to reach ratepairs lying above the time-sharingline between the ratepairs of the best codes with which we start the construction.

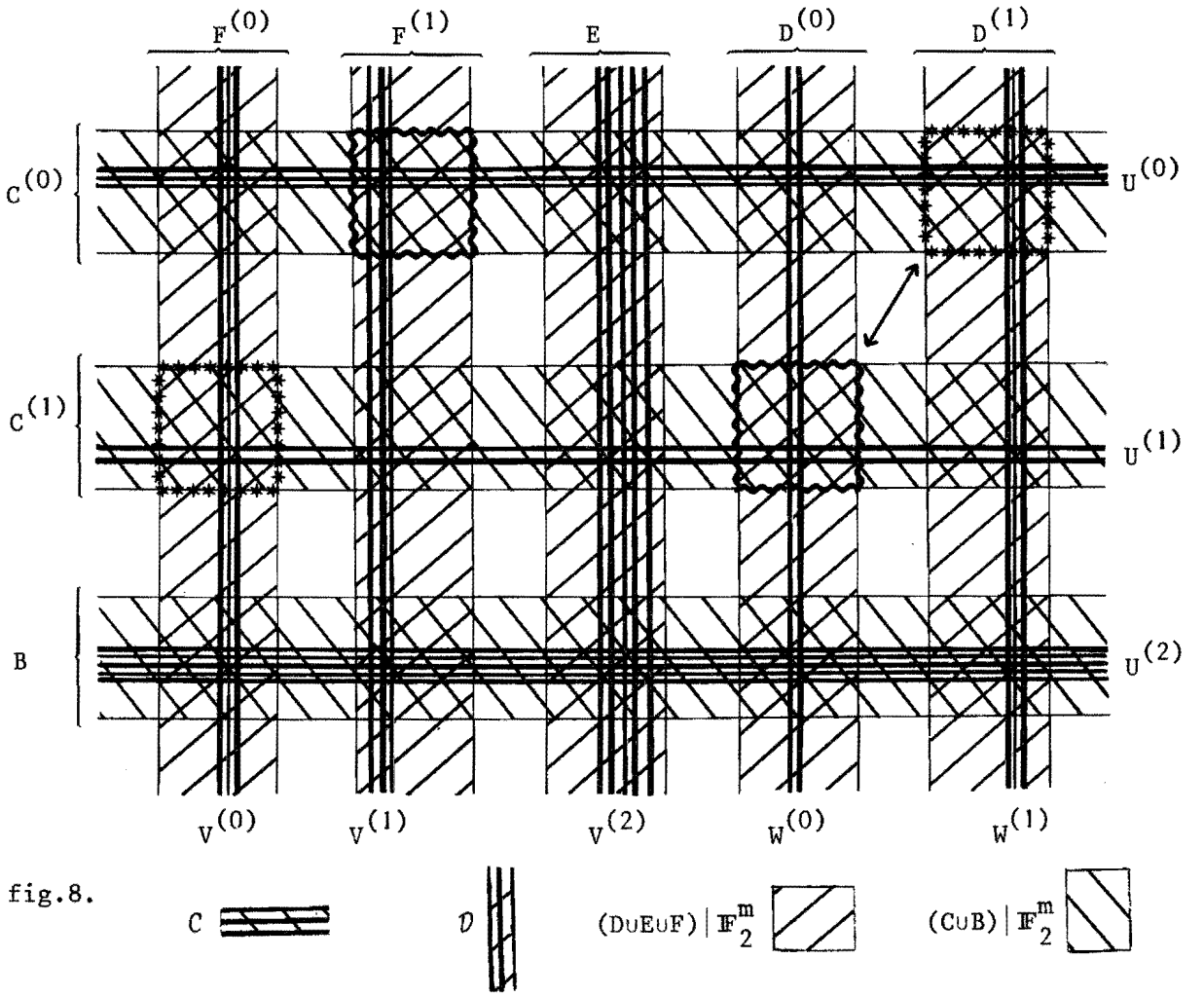


fig.8.

C $\mathcal{D}$ (DuEuF)|$\mathbb{F}_2^m$ (CuB)|$\mathbb{F}_2^m$

(ii) Again the idea may be clarified by a picture.In fig.8. all codes are depicted in $\mathbb{F}_2^{n+m} \times \mathbb{F}_2^{n+m}$ .Note that,if $\underline{c}=\underline{c}_1|\underline{c}_2$, $\underline{c}'=\underline{c}_1'|\underline{c}_2' \in C$, $\underline{d}=\underline{d}_1|\underline{d}_2$, $\underline{d}'=\underline{d}_1'|\underline{d}_2'$ in $\mathcal{D}$ we can have $\underline{c}_1+\underline{d}_1 = \underline{c}_1'+\underline{d}_1'$ only if:

-either $(\underline{c},\underline{d})$ is in one of the squares marked with ***** and $(\underline{c}',\underline{d}')$ is in the other,or

- $(\underline{c},\underline{d})$ is in one of the squares marked with ~~~~ and $(\underline{c}',\underline{d}')$ is in the other,or

- $(\underline{c},\underline{d})$ is in one of the decorated squares between which there is an arrow and $(\underline{c}',\underline{d}')$ is in the other.

However,in all of these cases we have $\underline{c}_2+\underline{d}_2 \neq \underline{c}_2'+\underline{d}_2'$.

(iii) Note that (2.3.2) is actually a special case of (2.4.1).Indeed,(2.3.2) follows from (2.4.1) by substitution of: (LHS ≡ (2.4.1),RHS ≡ (2.3.2).)

$U^{(0)} = U \oplus \underline{1}$,$U^{(1)} = U$, $U^{(2)} = \phi$; $V^{(i)} = V$,i=0,1,2 ; $W^{(0)} = \phi$, $W^{(1)} = W$.

$B = \phi$; $C^{(i)} = C^{(i)}$,i=0,1 ; $D^{(0)} = \phi$, $D^{(1)} = D$; $E = \phi$; $F^{(0)} = F$, $F^{(1)} = \phi$.

Of course many other specializations of (2.4.1) are possible.Also,many other generalizations of (2.3.2) are possible.

(iv) One should use (2.4.1) as follows.

In order to find a collection of codes B,C,D,E,F satisfying (47),start with any u.d. codepair (P,Q).Add as many new vectors to Q as possible to obtain a pair (P,R) , $|R| \geq |Q|$.(Remark.Here we arrive at step 1 in the table below which gives an example of the following.)

step	B	$C^{(0)}$	$C^{(1)}$	E	$F^{(0)}$	$F^{(1)}$	$D^{(0)}$	$D^{(1}$
1	P	ϕ	ϕ	R	ϕ	ϕ	ϕ	ϕ
2	{5,10}	{12}	{0}	R\{3}	ϕ	{3}	{15}	ϕ
3	{5,10}	{12}	{0}	R\{3,2}	ϕ	{3,2}	{15,14}	ϕ
4	ϕ	{12,5}	{0,10}	{6,9,12}	ϕ	{3,2,8,11}	{15,14,13}	ϕ
5	ϕ	{12,5}	{0,10}	{6,9}	{12}	{3,2,8,11}	{15,14,13}	{0}

P = {0,5,10,12} , R = {2,3,6,8,9,11,12} (binary notation; n=4.) table 8.

Now for all $\underline{d} \notin R$ the pair $(P, R \cup \{\underline{d}\})$ is not u.d..However,there may be some $\underline{d} \in \mathbb{F}_2^n \setminus R$ such that,with the definition $D^{(0)} := \{\underline{d}\}$, $D^{(1)} := \emptyset$ our codes satisfy (47) after a suitable choice of the partitions $P = B \cup C^{(0)} \cup C^{(1)}$, $R = E \cup F^{(0)} \cup F^{(1)}$ .Proceeding in this way,we add as many vectors to $D^{(0)}$ as possible,adapting the above partitions if necessary.

Next there might be some $\underline{d} \in \mathbb{F}_2^n \setminus R \setminus D^{(0)}$ such that with the definition $D^{(1)} = \{\underline{d}\}$ (47) still holds after,if necessary,adapting of our partitions.Again,add as many new vectors to $D^{(1)}$ as possible.

We note that the construction of a collection of codes $U^{(i)}, V^{(i)}, W^{(i)}$ satifying (46) is much more difficult.One should start with any u.d. codepair $(U^{(2)}, V^{(2)})$.Next find $U^{(0)}, U^{(1)}$ such that $(U^{(i)}, V^{(2)})$ is u.d. for i=0,1.In general these can be chosen as subsets of U resp. $U \oplus 1$ (cf.(2.3.1)).Now for $V^{(i)}$ (i=0,1) one can choose subsets of $V^{(2)}$ .If all these codes are defined reasonable one can find nonempty $W^{(i)}$ such that (46) is satisfied.(In general, $W^{(0)}$ and $W^{(1)}$ will be relatively small codes.)

The following lemma may be usefull.(Remark.the lemma remains true if we replace $\underline{1}$ by any vector $\underline{u}$ .However,this is not the case in (2.3.1).So one will not need this generalization in practice.)

2.4.3.Lemma.Let C_1, C_2, D_1, D_2 be binary codes of length n.Then $(C_1, D_1) \perp (C_2, D_2)$ iff $(C_1 \oplus \underline{1}, D_1 \oplus \underline{1}) \perp (C_2 \oplus \underline{1}, D_2 \oplus \underline{1})$.

Proof.It suffices to prove the "if" part since application of this to the codes on the RHS implies the "only if" part.Now suppose $(C_1 \oplus \underline{1}, D_1 \oplus \underline{1}) \perp (C_2 \oplus \underline{1}, D_2 \oplus \underline{1})$ and assume $\underline{c}_1 \in C_1$, $\underline{c}_2 \in C_2$, $\underline{d}_1 \in D_1$, $\underline{d}_2 \in D_2$.

Since $(\underline{c}_1 \oplus \underline{1}) + (\underline{d}_1 \oplus \underline{1}) \neq (\underline{c}_2 \oplus \underline{1}) + (\underline{d}_2 \oplus \underline{1})$ and $(\underline{c}_i \oplus \underline{1}) + (\underline{d}_i \oplus \underline{1}) = \underline{2} - \underline{c}_i - \underline{d}_i$ for i=1,2 we have $\underline{c}_1 \oplus \underline{d}_1 \neq \underline{c}_2 \oplus \underline{d}_2$. □

2.4.4.Examples.(i) Let $n=2$, $m=5$ .Choose (in binary notation)

$B = \phi$; $C^{(0)} = \{0\}$, $C^{(1)} = \{3\}$; $D^{(0)} = \phi$, $D^{(1)} = \{3\}$; $E = \{1,2\}$;

$F^{(0)} = \{0\}$, $F^{(1)} = \phi$.

$U^{(0)} = \{1,4,10,19,28,31\}$, $U^{(1)} = U^{(0)} \oplus \underline{1} = \{0,3,12,21,27,30\}$, $U^{(2)} = \phi$;

$V^{(0)} = \{6,7,9,10,13,14,15,16,18,21,22,24,25,26\}$, $V^{(1)} = \phi$, $V^{(2)} = V^{(0)} \cup \{29\}$;

$W^{(0)} = \phi$, $W^{(1)} = \{13,22,25\}$.

Now Theorem (2.4.1) gives the construction of a u.d. codepair of length 7 , where $|C| = 12$ and $|\mathcal{D}| = 47$ .This yields the codepair $R_1 = 0.51214$, $R_2 = 0.79351$ and $R_1 + R_2 = 1.30565$.

Note that essentially we have used the same codepairs as in (2.3.4(ii)).

(ii) Let $n=m=5$. Choose $B = \phi$; $C^{(0)} = \{0,3,12\}$, $C^{(1)} = \{21,27,30\}$; $D^{(0)} = \phi$, $D^{(1)} = \{23,26,29\}$; $E = \{6,7,9,10,13,15,16,18,21,22,24,25\}$; $F^{(0)} = \{2,5,8\}$; $F^{(1)} = \phi$. Take $U^{(i)}, V^{(i)}$ and $W^{(i)}$ as above.

Here we obtain a u.d. codepair $(C,\mathcal{D})$ of length 10 with $|C| = 36$, $|\mathcal{D}| = 231$. This gives us the ratepair $R_1 = 0.51699$, $R_2 = 0.78517$. $R_1 + R_2 = 1.30217$.

(iii) Let $n=4$, $m=5$ .Take B,C,D,E,F as in step 5 of table 8.Take $U^{(i)}$, $V^{(i)}$ and $W^{(i)}$ as in (i) above,except for $V^{(1)} := V^{(0)} \oplus \underline{1}$, $W^{(0)} := W^{(1)} \oplus \underline{1}$. We get a codepair of length 9 with $|C| = 24$, $|\mathcal{D}| = 112$ .The ratepair obtained in this way is not interesting.However,we see that (since we may as well take $U^{(2)} := U^{(0)}$) codes $U^{(i)}, V^{(i)}, W^{(i)}$ exist satisfying (46) such that none of them is empty.

Chapter 3.Another construction method.

3.1.Abstract.

In this Chapter we describe a construction method which yields families of u.d. codepairs for our channel.In Chapter 6 it will be shown that this method enables us to reach ratepairs outside the convex hull of the set of all ratepairs belonging to codepairs known up to now.In particular,the ratepairs obtained in this way lie above the lower bound obtained from (0.4.1) in the range $0.4 \leq R_1 \leq 0.9$ .The method described in this Chapter is a generalization of van Tilborg's work in [8] .

Section 3.2. gives an explanation of the idea.In section 3.3. we define the "basic codes" C,D and E needed for our construction.Moreover we prove the first important result.Section 3.4. gives the general construction method for a u.d. codepair (C,D) .This method shall be worked out for a special case in Chapter 4.

3.2.A brief introduction.

Below we explain the idea behind the construction given in this Chapter.The reader should realize that the general method is much more complicated.As a consequence the terminology in the rest of this Chapter is slightly different from the following.

We turn back to our "almost u.d." codepair mentioned in §2.2..That is,we can split $C=C^{(0)} \cup C^{(1)}$ and $D=D^{(0)} \cup D^{(1)}$ such that we have

$$(37) \qquad \forall_{\underline{c},\underline{c}' \in C \mid \underline{c} \neq \underline{c}'} \; \forall_{\underline{d},\underline{d}' \in D} \; [\, \underline{c}+\underline{d} = \underline{c}'+\underline{d}' \Rightarrow (\text{either } (\underline{c},\underline{d}) \in C^{(0)} \times D^{(1)} \wedge (\underline{c}',\underline{d}') \in C^{(1)} \times D^{(0)} \text{ or } (\underline{c}',\underline{d}') \in C^{(0)} \times D^{(1)} \wedge (\underline{c},\underline{d}) \in C^{(1)} \times D^{(0)}.) \,]$$

Now let us fix any outputvector $\underline{h} = \underline{c} + \underline{d}$ where $\underline{c} \in C$, $\underline{d} \in D$ .It is clear from (37) that (if we only know $\underline{h}$) we can determine which of the following is the case:

$$
\begin{aligned}
&\text{(a) } \underline{c} \in C^{(0)} \wedge \underline{d} \in D^{(0)} \\
(50) \qquad &\text{(b) } \underline{c} \in C^{(0)} \wedge \underline{d} \in D^{(1)} \text{ or } \underline{c} \in C^{(1)} \wedge \underline{d} \in D^{(0)} \\
&\text{(c) } \underline{c} \in C^{(1)} \wedge \underline{d} \in D^{(1)}
\end{aligned}
$$

It is clear that we need some side-information if (b) is the case.In Chapter 2 we have seen that this side-information can be added by concatenation of the words from $C^{(i)}$ resp. $D^{(i)}$ with the words from carefully chosen codes $U^{(i)}$ resp. $V^{(i)}$ .As mentioned in (2.4.2(iv)) it is hard to find such codes $U^{(i)}, V^{(i)}$.

The method presented in this Chapter uses the properties of the pair (C,D) in an entirely different way.That is,the side-information is added differently. However,we shall need one more restriction.We require that for each codeword $\underline{d}$ in $D^{(i)}$ there is exactly one $\underline{d}' \in D^{(1-i)}$ such that $\underline{c},\underline{c}' \in C$ exist satisfying $\underline{c} + \underline{d} = \underline{c}' + \underline{d}'$ .In other words,we assume that there is a bijective mapping $\phi: D^{(0)} \to D^{(1)}$ such that

$$
(51) \qquad \forall_{\underline{d} \in D^{(0)}} \forall_{\underline{d}' \in D^{(1)}} [(\exists_{\underline{c},\underline{c}' \in C} : \underline{c} + \underline{d} = \underline{c}' + \underline{d}') \Leftrightarrow \underline{d}' = \phi(\underline{d})]
$$

For example choose $C^{(0)} = \{000,010,100\}$, $C^{(1)} = \{001,011,101\}$; $D^{(0)} = \{000,110\}$ and $D^{(1)} = \{001,111\}$ .Here $\phi(000) = 001$ and $\phi(110) = 111$.

Now fix $s \in \mathbb{N}$ and $\underline{d} \in (D^{(0)})^s$ .We wish to find out for what vectors $\underline{d}' \in D^s$ there exist $\underline{c},\underline{c}' \in C^s$ such that $\underline{c} + \underline{d} = \underline{c}' + \underline{d}'$ .Let us partition $\underline{d} = (\underline{d}_1, \ldots, \underline{d}_s)$ s.t. $\underline{d}_i \in D^{(0)}$ for $i = 1,2,\ldots,s$ .Partition $\underline{c},\underline{c}',\underline{d}'$ in a similar way.It is clear that $\underline{c} + \underline{d} = \underline{c}' + \underline{d}'$ implies that $\underline{c}_i + \underline{d}_i = \underline{c}_i' + \underline{d}_i'$ for all i .So (51) and

(37) imply that $\underline{d}'_i \in \{\underline{d}_i, \phi(\underline{d}_i)\}$ for each i .

Hence $\underline{d}'$ must be in the set $A(\underline{d}) := \{ \underline{e} = (\underline{e}_1,\ldots,\underline{e}_s) \in D^s \mid \forall_i : \underline{e}_i \in \{\underline{d}_i, \phi(\underline{d}_i)\} \}$. This set consists of all 2^s vectors obtained from $\underline{d}$ by replacing $\underline{d}_i$ by $\phi(\underline{d}_i)$ for some of the indices $i \in \{1,2,\ldots,s\}$.

In a similar way as above one can show that for all $\underline{d},\underline{d}' \in D^s$ we have

$$(52) \qquad \exists_{\underline{c},\underline{c}' \in C^s} [\, \underline{c} + \underline{d} = \underline{c}' + \underline{d}' \,] \;\Leftrightarrow\; \exists_{\underline{y} \in (D^{(0)})^s} [\, \underline{d} \in A(\underline{y}) \wedge \underline{d}' \in A(\underline{y}) \,] \quad .$$

Hence for any $\mathcal{D} \subset D^s$ we have that $(C^s,\mathcal{D})$ is u.d. if and only if $|\mathcal{D} \cap A(\underline{y})| \leq 1$ for all $\underline{y} \in (D^{(0)})^s$ (*).

However, the ratepairs belonging to such codepairs are equal (or even worse) to the ratepair belonging to the u.d. codepair $(C,D^{(0)})$. So we have not found anything interesting yet.

Now we turn back to (50). Let $\underline{c} \in C^{(k)}$, $\underline{d} \in D^{(\ell)}$. Then we have

$$(53) \qquad k+\ell = \begin{cases} 0 & \text{in case (50a) : } k=0 \text{ , } \ell=0 \\ 1 & \text{in case (50b) : } k=0 \text{ , } \ell=1 \text{ or } k=1 \text{ , } \ell=0 \\ 2 & \text{in case (50c) : } k=1 \text{ , } \ell=1 \end{cases}$$

So (since we can determine from $\underline{h} = \underline{c} + \underline{d}$ which of these is the case) the upper indices behave just like the bits in our channel! Now the idea is, to choose the respective rows of upper indices from a u.d. codepair. That is, choose a u.d. codepair (P,Q) of length s and define $(C,\mathcal{D})$ as follows. C consists of all words $\underline{c} = (\underline{c}_1,\ldots,\underline{c}_s) \in C^s$ for which the binary vector $(p_1,\ldots,p_s)$ of upper indices s.t. $\underline{c}_i \in C^{(p_i)}$ $(i = 1,\ldots,s)$ agrees whith some codeword in P. $\mathcal{D}$ is defined in a similar way using Q. More precisely, for any $\underline{c} \in C^s$, $\underline{d} \in D^s$ define $\underline{p} = \zeta(\underline{c})$ and $\underline{q} = \zeta(\underline{d})$ of length s by

$$(54)\qquad \begin{aligned} p_i = 0 \quad &\text{if} \quad \underline{c}_i \in C^{(0)} \ , \ p_i = 1 \quad \text{if} \quad \underline{c}_i \in C^{(1)} \ , \\ q_i = 0 \quad &\text{if} \quad \underline{d}_i \in D^{(0)} \ , \ q_i = 1 \quad \text{if} \quad \underline{d}_i \in D^{(1)} \ . \end{aligned}$$

Now define the codepair $(C,\mathcal{D})$ by

$$(55)\qquad \begin{aligned} C &:= \{ \ \underline{c} \in C^s \mid \zeta(\underline{c}) \in P \ \} \ , \\ \mathcal{D} &:= \{ \ \underline{d} \in D^s \mid \zeta(\underline{d}) \in Q \ \} \ . \end{aligned}$$

We claim that $(C,\mathcal{D})$ is u.d..Indeed,suppose $\underline{c} + \underline{d} = \underline{c}' + \underline{d}'$ for $\underline{c},\underline{c}' \in C$, $\underline{d},\underline{d}' \in \mathcal{D}$. From (50) and (53) we have $\zeta(\underline{c}) + \zeta(\underline{d}) = \zeta(\underline{c}') + \zeta(\underline{d}')$.Hence it follows from the construction of $(C,\mathcal{D})$ that $\zeta(\underline{d}) = \zeta(\underline{d}')$ .But (52) implies that $\underline{d}$ and $\underline{d}'$ are in the same set $A(\underline{y})$ for some $\underline{y} \in (D^{(0)})^s$ .Since for each $\underline{q} \in Q$ there is exactly one $\underline{d} \in A(\underline{y})$ s.t. $\zeta(\underline{d}) = \underline{q}$ it is clear that $\underline{d} = \underline{d}'$ .So indeed $(C,\mathcal{D})$ is u.d..

We note that the choice $P = \mathbb{F}_2^s$, $Q = \{\underline{0}\}$ gives us a codepair $(C^s,\mathcal{D})$ as in (*). The ratepair equals that of $(C,D^{(0)})$.Since (P,Q) is a "bad" codepair we may expect that other choices give better results.

3.3.A concept for basic codes.Some observations.

As mentioned before,the construction presented in this Chapter is much more complicated then the idea described above.The main difference is that there is one more code involved (namely E) .The concept for the codes C,D and E needed for our method is given below.In the rest of this Chapter we shall assume that C,D and E satisfy all properties mentioned in (56).

Assume we have a binary codepair $(C,D \cup E)$ of length n such that there are partitions $C = C^{(0)} \cup C^{(1)}$, $D = D^{(0)} \cup D^{(1)}$ with the following properties :

(i) $(C,D^{(i)} \cup E)$ is uniquely decodable for $i = 0,1$.

(ii) $(C^{(i)},D \cup E)$ is uniquely decodable for $i = 0,1$.

(iii) $(C^{(0)},D^{(0)}) \perp (C^{(1)},D^{(1)})$.

(56) (iv) There is a bijective mapping $\phi: D^{(0)} \to D^{(1)}$ such that

$$\forall_{\underline{d} \in D^{(0)}} \forall_{\underline{d}' \in D^{(1)}} [(\exists_{\underline{c},\underline{c}' \in C}: \underline{c} + \underline{d} = \underline{c}' + \underline{d}') \Leftrightarrow \underline{d}' = \phi(\underline{d})] .$$

(v) $D \cap E = \emptyset$, $C^{(0)} \neq \emptyset$, $C^{(1)} \neq \emptyset$, $D^{(0)} \neq \emptyset$.

3.3.1.Examples. (i) Choose $C^{(0)} = D^{(0)} = \{\underline{0}\}$, $C^{(1)} = D^{(1)} = \{\underline{1}\}$, $E = \mathbb{F}_2^n \setminus \{\underline{0},\underline{1}\}$ .Here $\phi(\underline{0}) = \underline{1}$.

(ii) Choose $n = 4$, $C^{(0)} = \{0000,0011\}$, $C^{(1)} = \{1100,1111\}$, $D^{(0)} = \{0000,0001, 0010\}$, $D^{(1)} = \{1100,1101,1110\}$, $E = \{0100,0101,0110,1000,1001,1010\}$ .Here $\phi(0000) = 1100$, $\phi(0001) = 1101$, $\phi(0010) = 1110$.

To clarify the idea all codes are depicted in $\mathbb{F}_2^n \times \mathbb{F}_2^n$ in fig.9.Note that if $\underline{c},\underline{c}' \in C$, $\underline{d},\underline{d}' \in D \cup E$ we can only have $\underline{c} + \underline{d} = \underline{c}' + \underline{d}'$ if $(\underline{c},\underline{d})$ is in one of the decorated rectangles and $(\underline{c}',\underline{d}')$ is in the other.Moreover,either $\underline{d}' = \phi(\underline{d})$ or $\underline{d} = \phi(\underline{d}')$.

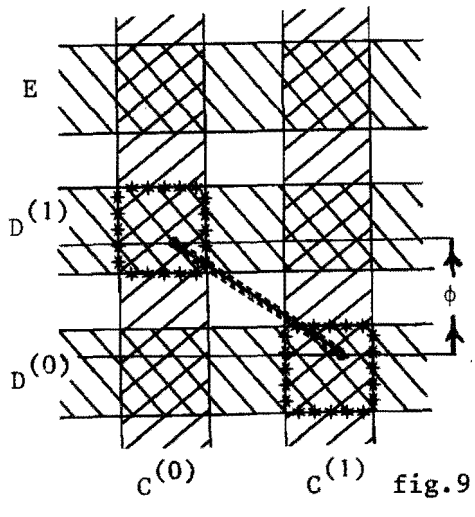


fig.9.

Now for any $s \in \mathbb{N}$, $C \subset C^s$ we may choose $\mathcal{D} := (D^{(0)} \cup E)^s$ to obtain a u.d. codepair $(C,\mathcal{D})$ ((56)(i)).However,lots of other choices for $\mathcal{D}$ give a u.d. codepair, as we will see in (3.3.4).First we need the following definition.

3.3.2.Definition.Let C,D and E be as in (56).For any $\underline{y} = (\underline{y}_1,\ldots,\underline{y}_s) \in (D^{(0)} \cup E)^s$

we define

$$(57)\qquad \begin{aligned} W(\underline{y}) &:= \{\, i \in \{1,2,\ldots,s\} \mid \underline{y}_i \in E \,\}\ \text{, and} \\ A(\underline{y}) &:= \{\, \underline{d} = (\underline{d}_1,\ldots,\underline{d}_s) \in (D \cup E)^s \mid \forall_{i \in W(\underline{y})} : \underline{d}_i = \underline{y}_i \ \wedge \\ &\qquad\qquad \forall_{i \notin W(\underline{y})} : \underline{d}_i \in \{\underline{y}_i, \phi(\underline{y}_i)\} \,\}. \end{aligned}$$

The following lemma is the analogue of (52).

3.3.3.Lemma.Let C,D and E be as in (56).Let $s \in \mathbb{N}$, $C \subset C^s$. Fix $\underline{d},\underline{d}' \in (D \cup E)^s$ .Then the existence of $\underline{c},\underline{c}' \in C$ such that $\underline{c} + \underline{d} = \underline{c}' + \underline{d}'$ implies the existence of a vector $\underline{y} \in (D^{(0)} \cup E)^s$ such that $\underline{d} \in A(\underline{y}) \wedge \underline{d}' \in A(\underline{y})$.

Proof.Assume that $\underline{c},\underline{c}' \in C$, $\underline{d},\underline{d}' \in (D \cup E)^s$ and $\underline{c} + \underline{d} = \underline{c}' + \underline{d}'$ .Partition $\underline{c} = (\underline{c}_1,\ldots,\underline{c}_s)$ and partition $\underline{c}',\underline{d},\underline{d}'$ in a similar way.It is clear that ,for $i = 1,2,\ldots,s$: $\underline{c}_i + \underline{d}_i = \underline{c}_i' + \underline{d}_i'$ (*) .

Now consider the following cases:

(a) $\underline{c}_i,\underline{c}_i' \in C^{(j)}$ for $j = 0$ or $j = 1$ .It follows from (*) and (56)(ii) that we have $\underline{c}_i = \underline{c}_i'$ and $\underline{d}_i = \underline{d}_i'$.

(b) $\underline{c}_i \in C^{(0)}$ and $\underline{c}_i' \in C^{(1)}$ .It follows from (*) and (56)(i),(iii) that we have $\underline{d}_i \in D^{(1)}$ and $\underline{d}_i' \in D^{(0)}$.Now (56)(iv) implies that $\underline{d}_i = \phi(\underline{d}_i')$.

(c) $\underline{c}_i \in C^{(1)}$ and $\underline{c}_i' \in C^{(0)}$.As in (ii) we find $\underline{d}_i \in D^{(0)}$, $\underline{d}_i' \in D^{(1)}$ and $\underline{d}_i' = \phi(\underline{d}_i)$.

The above covers all cases.Now define $\underline{y} := (\underline{y}_1,\ldots,\underline{y}_s)$ where

$$\underline{y}_i := \begin{cases} \underline{d}_i \text{ if (a) is the case and } \underline{d}_i \in D^{(0)} \text{ ,or (c) is the case,} \\ \underline{d}_i' \text{ if (a) is the case and } \underline{d}_i \in D^{(1)} \text{ ,or (b) is the case.} \end{cases}$$

Now we have $\underline{y} \in (D^{(0)} \cup E)^s$ and $\{\underline{d},\underline{d}'\} \subset A(\underline{y})$. □

3.3.4.Corollary.Let C,D and E be as in (56).Let $C \subset C^s$ and $\mathcal{D} \subset (D \cup E)^s$ such that $\forall_{\underline{y} \in (D^{(0)} \cup E)^s} [\ |\mathcal{D} \cap A(\underline{y})| \leq 1\ ]$ .Then the codepair $(C,\mathcal{D})$ is u.d..

Note that none of the ratepairs obtained from (3.3.4) "exceeds" that of $(C = C^s, \mathcal{D} = (D^{(0)} \cup E)^s)$. (3.3.4) is the analogue of (*) in §3.2..

3.4.Definition of C.How to construct $\mathcal{D}$.

In this section we introduce the code C.The definition does not make use of a code P which is one of a u.d. codepair (P,Q) (as in §3.2.),but of an arbitrary (binary) code Z of length s.This difference is strongly related to the fact that a code E is used here which does not occur in §3.2..However,in essence the method is similar to that in §3.2..That is,we choose $C \subset C^s$ with such a structure that codes $\mathcal{D} \subset (D \cup E)^s$ exist such that $(C,\mathcal{D})$ is u.d. and $|\mathcal{D}|$ is relatively large. Since $(C, D^{(0)} \cup E)$ is u.d. it depends on the product $\frac{|C|}{|C|^s} \cdot \frac{|\mathcal{D}|}{|D^{(0)} \cup E|^s}$ whether a "new" ratepair is obtained or not.

Below we give the definition of C.Afterwards conditions on $\mathcal{D}$ will be derived such that $(C,\mathcal{D})$ is u.d..Results concerning the size of $\mathcal{D}$ are presented.

3.4.1.Definition.Let C,D and E be as in (56).Let Z be any binary code of length s .We define the code C as follows:

$$(58) \qquad C := \{\ \underline{c} = (\underline{c}_1,\ldots,\underline{c}_s) \in C^s \mid \exists_{\underline{z} \in Z}\ \forall_i : \underline{c}_i \in C^{(z_i)}\ \}\ .$$

3.4.2.Remark.The size of C is easily to compute using the weight enumerator $W_Z(x,y)$ of the code Z,which is defined by

$$(59) \qquad a_i := |\ \{\ \underline{z} \in Z \mid w_H(\underline{z}) = i\ \}\ |\ ,(i = 0,1,\ldots,s)\ ;\ W_Z(x,y) := \sum_{i=0}^{s} a_i\ x^{s-i}\ y^i\ .$$

(Here w_H denotes Hamming weight.)We have

(60) $$|C| = W_Z(|C^{(0)}|, |C^{(1)}|) \quad .$$

The following lemma shows which pairs $\{\underline{d},\underline{d}'\} \subset (D \cup E)^s$ may not be included in $\mathcal{D}$.

3.4.3.Lemma.Let C,D and E be as in (56).Let C be as in (3.4.1).Fix $\underline{y} \in (D^{(0)} \cup E)^s$ Then for any $\underline{d},\underline{d}' \in A(\underline{y})$ the proposition that there are $\underline{c},\underline{c}' \in C$ such that $\underline{c}+\underline{d} = \underline{c}'+\underline{d}'$ is equivalent to

(61) $$\exists_{\underline{z},\underline{z}' \in Z} [((z_i,z_i') = (0,1) \text{ if } (\underline{d}_i,\underline{d}_i') \in D^{(1)} \times D^{(0)}) \wedge ((z_i,z_i') = (1,0) \text{ if } (\underline{d}_i,\underline{d}_i') \in D^{(0)} \times D^{(1)}) \wedge (z_i = z_i' \text{ if } \underline{d}_i = \underline{d}_i')] .$$

(Note that $\underline{d},\underline{d}' \in A(\underline{y})$ implies that for each i one of the three cases in (61) must hold.)

Proof.First assume there are $\underline{c},\underline{c}' \in C$ such that $\underline{c}+\underline{d} = \underline{c}'+\underline{d}'$ .For any i with $\underline{d}_i = \underline{d}_i'$ we must have $\underline{c}_i = \underline{c}_i'$ .Since $C^{(0)} \cap C^{(1)} = \phi$ it follows that $\underline{c}_i,\underline{c}_i' \in C^{(j)}$ for $j = 0$ or $j = 1$.
For any i with $\underline{d}_i \in D^{(0)}$, $\underline{d}_i' \in D^{(1)}$ we must have $\underline{c}_i \in C^{(1)}$, $\underline{c}_i' \in C^{(0)}$ from (56)(ii),(iii).Similarly if $\underline{d}_i \in D^{(1)}$, $\underline{d}_i' \in D^{(0)}$ we have $\underline{c}_i \in C^{(0)}$, $\underline{c}_i' \in C^{(1)}$.
The existence of $\underline{z},\underline{z}' \in Z$ with the desired properties now follows from the definition of C.

Next,assume such $\underline{z},\underline{z}' \in Z$ exist.If $z_i = z_i'$ choose any $\underline{c}_i = \underline{c}_i' \in C^{(z_i)}$ to obtain $\underline{c}_i + \underline{d}_i = \underline{c}_i' + \underline{d}_i'$.
If $(z_i,z_i') = (0,1)$ we have $\underline{d}_i \in D^{(1)}$ and $\underline{d}_i' \in D^{(0)}$ .Since $\underline{d},\underline{d}' \in A(\underline{y})$ we see from (57) that $\underline{d}_i = \phi(\underline{d}_i')$ .It follows from (56)(iv) that there are $\underline{c},\underline{c}' \in C$

such that $\underline{c}+\underline{d}_i = \underline{c}'+\underline{d}_i'$ .Moreover (56)(ii),(iii) imply that $\underline{c} \in C^{(0)}$, $\underline{c}' \in C^{(1)}$.

Define $\underline{c}_i := \underline{c}$ and $\underline{c}_i' := \underline{c}'$.

Similarly,if $(z_i,z_i') = (1,0)$ we can find $\underline{c}_i \in C^{(1)}$, $\underline{c}_i' \in C^{(0)}$ such that $\underline{c}_i+\underline{d}_i = \underline{c}_i'+\underline{d}_i'$ .Now define $\underline{c} := (\underline{c}_1,\ldots,\underline{c}_s)$ and $\underline{c}' := (\underline{c}_1',\ldots\underline{c}_s')$ .It is clear that $\underline{c},\underline{c}' \in C$ and $\underline{c}+\underline{d} = \underline{c}'+\underline{d}'$. □

3.4.4.Example. Let $C^{(0)} = D^{(0)} = \{00\}$, $C^{(1)} = D^{(1)} = \{11\}$, $E = \{01,10\}$.

Here $\phi(00) = 11$.(This is (3.3.1(i)) for $n = 2$.)

Let $s = 4$; $Z =$ 1 0 1 0 / 0 1 0 1 / 1 1 1 1 / 0 0 0 0 $\quad C =$ 11 00 11 00 / 00 11 00 11 / 11 11 11 11 / 00 00 00 00 (Note that C is isomorfic to the concatenation of {0000,1111} with itself.)

Now let us consider the following vectors in $(D^{(0)} \cup E)^4$:

$\underline{y} =$ 01 00 01 00 $\quad \underline{y}' =$ 01 10 00 00

$A(\underline{y})$

$\underline{y}$	01	00	01	00	$\underline{y}'$ 01 10 00 00
$\underline{d}$	01	00	01	11	$\underline{d}'$ 01 10 00 11
$\underline{e}$	01	11	01	00	$\underline{e}'$ 01 10 11 00
$\underline{f}$	01	11	01	11	$\underline{f}'$ 01 10 11 11

$A(\underline{y}')$

Now for any two vectors in $A(\underline{y})$ the existence of $\underline{z},\underline{z}' \in Z$ as in (61) implies $z_1 = z_1'$, $z_3 = z_3'$ .Then the choice of Z implies that either $\underline{z} = \underline{z}'$ or $z_2 = z_4 \neq z_2' = z_4'$ .Hence any subset of $A(\underline{y})$ in which $\underline{y}$ and $\underline{f}$ do not both occur can be added to $\mathcal{D}$.

For any two vectors in $A(\underline{y}')$ the existence of $\underline{z},\underline{z}' \in Z$ as in (61) implies $\underline{z} = \underline{z}'$ .Hence all vectors $\underline{y}',\underline{d}',\underline{e}',\underline{f}'$ can be added to $\mathcal{D}$.

Now let C be defined as in (3.4.1).Then the maximum size of $\mathcal{D} \subset (D \cup E)^s$ such that $(C,\mathcal{D})$ is u.d. depends heavily on the structure of Z.In general it is not

easy to see how "efficient" the choice of $\mathcal{D}$ is,given C.However,in some restricted sense we can say something about this.We need some definitions.

3.4.5.Definitions. (a) Let $C,\mathcal{D}$ and E be binary codes of length n such that $(C,\mathcal{D})$ is uniquely decodable.We call the codepair $(C,\mathcal{D})$ "optimal with respect to E" if

(62) (i) $\mathcal{D} \subset E$

(ii) For all $F \subset E$ such that (C,F) is u.d. we have $|F| \leq |\mathcal{D}|$.

If a codepair $(C,\mathcal{D})$ is optimal with respect to $\mathbb{F}_2^n$ we say that it is optimal.

(b) Let C,D and E be as in (56).Let Z be a binary code of length s . For any $\underline{y} \in (D^{(0)} \cup E)^s$ let

(63) $M_Z(\underline{y})$:= The maximum number of vectors in $A(\underline{y})$ such that for any pair $\underline{d},\underline{d}'$ of them no vectors $\underline{z},\underline{z}'$ exist as in (61).

3.4.6.Remark.Note that the notion of being optimal depends on the choice of the code C.A "bad" choice of C may result in a bad codepair which,however,is optimal.

Now we are able to state the main result of this section.

3.4.7.Theorem.Let C,D and E be as in (56).Let s,Z and C be as in (3.4.1).Then there is a code $\mathcal{D}$ of length $N := sn$ and size

$$(64) \qquad |\mathcal{D}| = \sum_{\underline{y} \in (D^{(0)} \cup E)^s} M_Z(\underline{y}) \quad ,$$

such that $(C,\mathcal{D})$ is u.d. and optimal with respect to $(D \cup E)^s$.

Proof. The existence of $\mathcal{D}$ follows from Lemmas (3.3.3) and (3.4.3) and the definition of $M_Z(\underline{y})$. Now assume we have a code $F \subset (D \cup E)^s$ such that (C,F) is u.d.. For any $\underline{f} \in F$ we can find one vector $\underline{y} \in (D^{(0)} \cup E)^s$ such that $\underline{f} \in A(\underline{y})$. Since the definition of $M_Z(\underline{y})$ and (3.4.3) imply that, for each $\underline{y}$, $|F \cap A(\underline{y})| \leq M_Z(\underline{y})$ it is immediately clear that $|F| \leq \sum_{\underline{y} \in (D^{(0)} \cup E)^s} M_Z(\underline{y}) = |\mathcal{D}|$. □

3.4.8. Remarks. (i) If $D \cup E = \mathbb{F}_2^n$ (like in (3.3.1(i)) it follows that $(C,\mathcal{D})$ is optimal.

(ii) A closer investigation of $M_Z(\underline{y})$ is given in (3.4.10).

(iii) Note that all proofs are "componentwise". Hence it is not difficult to generalize this section to the case that we have codepairs $(C_i, D_i \cup E_i)$ for $i = 1,2,\ldots,s$, for each i satisfying (56). This gives us the following Theorem.

3.4.9. Theorem. Let $s \in \mathbb{N}$, n_i, C_i, D_i and E_i as in (56) for $i = 1,2,\ldots,s$. Let Z be a binary code of length s. Define

$$(65) \qquad C := \{ \underline{c} = (\underline{c}_1,\ldots\underline{c}_s) \in \prod_{i=1}^{s} C_i \mid \exists_{\underline{z} \in Z} \forall_i : \underline{c}_i \in C_i^{(z_i)} \} .$$

For each $\underline{y} = (\underline{y}_1,\ldots,\underline{y}_s) \in \prod_{i=1}^{s} (D_i^{(0)} \cup E_i)$ let $M_Z(\underline{y})$ be as in (63), where

$$(66) \qquad A(\underline{y}) := \{ \underline{d} = (\underline{d}_1,\ldots,\underline{d}_s) \in \prod_{i=1}^{s} (D_i \cup E_i) \mid \forall_{i \mid \underline{y}_i \in E_i} : \underline{d}_i = \underline{y}_i \quad \forall_{i \mid \underline{y}_i \notin E_i} : \underline{d}_i \in \{\underline{y}_i, \phi_i(\underline{y}_i)\} \}.$$

Then there is a code $\mathcal{D}$ of length $N := \sum_{i=1}^{s} n_i$ of size

$$(67) \qquad |\mathcal{D}| = \sum_{\underline{y} \in \prod_{i=1}^{s} (D_i^{(0)} \cup E_i)} M_Z(\underline{y}) \quad ,$$

Such that $(C,\mathcal{D})$ is uniquely decodable and optimal w.r.t. $\prod_{i=1}^{s}(D_i \cup E_i)$.

The proof is left to the reader.

In order to apply Theorems (3.4.7) and (3.4.9) we should be able to enumerate the numbers $M_Z(\underline{y})$ .The following lemma gives an explicit expression.However, calculation of $M_Z(\underline{y})$ according to this expression will be very hard in practice.So the lemma shows us the difficulty of finding these numbers.

3.4.10.Lemma.Let C,D and E be as in (56).Let $s \in \mathbb{N}$, Z a binary code of length s .Fix $\underline{y} \in (D^{(0)} \cup E)^s$ .Let $W(\underline{y})$ and $M_Z(\underline{y})$ be as in (3.3.2) resp. (3.4.5). Define $\underline{v}(\underline{y}) := (v_1,\ldots,v_s)$ by $v_i := 0$ if $\underline{y}_i \in D^{(0)}$, $v_i := 1$ if $\underline{y}_i \in E$ .For each $\underline{u} \sqsubset \underline{v}(\underline{y})$ (cf.(12)) let $Z_{\underline{u}} := \{\underline{z} \in Z \mid \forall_{i \in W(\underline{y})} : z_i = u_i\}$, and let $Z_{(\underline{y},\underline{u})}$ be the code obtained from $Z_{\underline{u}}$ by deleting all coordinates occuring in $W(\underline{y})$. Then

$$(68) \qquad M_Z(\underline{y}) = \max \{ |Q| \mid (Z_{(\underline{y},\underline{u})},Q) \text{ is u.d. for all } \underline{u} \sqsubset \underline{v}(\underline{y}) \} .$$

Proof.We assume w.l.o.g. that $W(\underline{y}) = \{ s-|W(\underline{y})|+1, s-|W(\underline{y})|+2,\ldots,s\}$.

Suppose that $\tilde{Q}$ reaches the maximum in (68).For any $\underline{q} \in \tilde{Q}$ define $\underline{d} = \theta(\underline{q})$ by: $\underline{d} \in A(\underline{y})$ and $\underline{d}_i \in D^{(q_i)}$ for $i = 1,2,\ldots,s-|W(\underline{y})|$ .Now let $\underline{d} = \theta(\underline{q})$, $\underline{d}' = \theta(\underline{q}')$ for $\underline{q},\underline{q}' \in \tilde{Q}$ and assume that $\underline{z},\underline{z}' \in Z$ exist as in (61).
Obviously there is some $\underline{u} \sqsubset \underline{v}(\underline{y})$ such that $z_i = z_i' = u_i$ for $i \in W(\underline{y})$ .So we have $(z_1,\ldots z_{s-\ W(\underline{y})}) \in Z_{(\underline{y},\underline{u})}$ and $(z_1',\ldots,z'_{s-\ W(\underline{y})}) \in Z_{(\underline{y},\underline{u})}$.
Now for each $i \le s-\ W(\underline{y})$ one of the following holds:

$$(69) \qquad \begin{aligned} &(i) \quad q_i = q_i' \wedge \underline{d}_i = \underline{d}_i' \wedge z_i = z_i' \\ &(ii) \quad (q_i,q_i') = (0,1) \wedge (\underline{d}_i,\underline{d}_i') \in D^{(0)} \times D^{(1)} \wedge (z_i,z_i') = (1,0) \\ &(iii) \quad (q_i,q_i') = (1,0) \wedge (\underline{d}_i,\underline{d}_i') \in D^{(1)} \times D^{(0)} \wedge (z_i,z_i') = (0,1) \end{aligned}$$

So for $i \leq s-|W(\underline{y})|$ we have $q_i + z_i = q_i' + z_i'$,contradicting the fact that $(Z_{(\underline{y},\underline{u})},\tilde{Q})$ is uniquely decodable.Hence $\{ \theta(\underline{q}) \mid \underline{q} \in \tilde{Q} \}$ is a set of $|\tilde{Q}|$ vectors in $A(\underline{y})$ such that for no pair of them $\underline{z},\underline{z}'$ exist like in (61).This proves that $M_Z(\underline{y})$ is greater or equal to the RHS of (68).

Next,assume we can find a set V of vectors in $A(\underline{y})$ such that for no pair of them $\underline{z},\underline{z}' \in Z$ exist as in (61),such that $|V|$ exceeds the RHS of (68).For any $\underline{d} \in V$ define $\underline{q} = \zeta(\underline{d})$ by: $q_i = 0$ if $\underline{d}_i \in D^{(0)}$ and $q_i = 1$ if $\underline{d}_i \in D^{(1)}$ (cf. §3.2.).Remark: $\underline{q}$ is a vector of length $s-|W(\underline{y})|$.

Obviously there is at least one vector $\underline{u} \sqsubset \underline{v}(\underline{y})$ s.t. $(Z_{(\underline{y},\underline{u})},\{\zeta(\underline{d}) \mid \underline{d} \in V\})$ is <u>not</u> uniquely decodable.So we can find $\tilde{\underline{z}},\tilde{\underline{z}}' \in Z_{(\underline{y},\underline{u})}$ and $\underline{d},\underline{d}' \in V$ such that $\tilde{\underline{z}} + \zeta(\underline{d}) = \tilde{\underline{z}}' + \zeta(\underline{d}')$ (*) .
Now define $\underline{z},\underline{z}'$ of length s by: $(z_i,z_i') := (\tilde{z}_i,\tilde{z}_i')$ if $i \leq s-|W(\underline{y})|$ and $(z_i,z_i') := (u_i,u_i)$ if $i > s-|W(\underline{y})|$ .Obviously we have $\underline{z},\underline{z}' \in Z$.Moreover,for $i > s-|W(\underline{y})|$ we have $\underline{d}_i = \underline{d}_i'$ and $z_i = z_i'$ .From (*) it is clear that for each $i \leq s\ |W(\underline{y})|$ one of (69) must hold.Hence $\underline{z},\underline{z}'$ satisfy (61) and $M_Z(\underline{y}) < |V|$. □

<u>3.4.11.Remarks.</u> (i) It is clear from (3.4.10) that $M_Z(\underline{y})$ depends only on Z and $W(\underline{y})$.

(ii) Theoratically, $M_Z(\underline{y})$ can be found using the superposition of the graphs $G_{Z_{(\underline{y},\underline{u})}}$ for all $\underline{u} \sqsubset \underline{v}(\underline{y})$.(cf.Chapter 1.).

<u>3.4.12.Example.</u>Let all codes be as in (3.4.4).Then we have,as one can verify using (3.4.10) : $M_Z(\underline{y}) = 9$ if $W(\underline{y}) = \phi$; 6 if $|W(\underline{y})| = 1$; 4 if $W(\underline{y}) \in \{\{1,2\},\{2,3\},\{3,4\},\{4,1\}\}$; 3 if $W(\underline{y}) \in \{\{1,3\},\{2,4\}\}$; 2 if $|W(\underline{y})| = 3$ and $M_Z(\underline{y}) = 1$ if $|W(\underline{y})| = 4$.

Now (3.4.7) states that the maximum size of $\mathcal{D}$ such that $(C,\mathcal{D})$ is u.d. equals 225 .(Note that there are,in this example, $|E|^W = 2^W$ vectors $\underline{y} \in (D^{(0)} \cup E)^s = \{00,01,10\}^4$ such that $|W(\underline{y})| = W$.) The same result is obtained in [8] using a different approach.

Chapter 4. Evaluation of $M_Z(\underline{y})$ for certain choices of Z.

4.1.Abstract.

In this Chapter we give a detailed description of the codes obtained from (3.4.7) in the case that Z is a code which contains all words whose Hamming weights are divisible by some natural number w .We shall use the codes C,D and E as defined in (56).In section 4.2. we show that,for our special choice of Z, the conditions derived in (3.4.3) can be "translated" into a form which is more manageable.In section 4.3. the value of $M_Z(\underline{y})$ is calculated by straightforward observations using the conditions from §4.2.In section 4.4. explicit expressions for $|C|$ and $|D|$ are given according to (3.4.7).

4.2.Definition of Z .A new version of the conditions from (3.4.3).

In this Chapter we shall make use of the following definitions:

4.2.1.Definitions. Let n,C,D,E and ϕ be as in (56) .For $\underline{y} \in (D^{(0)} \cup E)^s$ let $W(\underline{y})$ and $A(\underline{y})$ be as in (3.3.2) and $M_Z(\underline{y})$ as in (3.4.5)(b) .

Let $s = q.w + r$,where $q,w,r \in \mathbb{N}$, $0 \leq r < w$;define $N := sn$ .For any $\underline{d} = (\underline{d}_1,\ldots,\underline{d}_s) \in (D \cup E)^s$ let

(70) $$w^*(\underline{d}) := |\{ i \in \{1,\ldots,s\} \mid \underline{d}_i \in D^{(1)} \}| \ \underline{\text{mod}}\ w .$$

As in (3.4.1) we define the code C by

(58) $$C := \{ \underline{c} = (\underline{c}_1,\ldots,\underline{c}_s) \in C^s \mid \exists_{\underline{z} \in Z} \forall_i : \underline{c}_i \in C^{(z_i)} \} ,$$

where Z shall be chosen as in (4.2.2).

For any $\underline{y} \in (D^{(0)} \cup E)^s$ and $\underline{d},\underline{d}' \in A(\underline{y})$ define

$$(71) \qquad a_{ij}(\underline{d},\underline{d}') := |\{ k \in \{1,\ldots,s\} \mid \underline{d}_k \in D^{(i)} \wedge \underline{d}'_k \in D^{(j)} \}| \ , (i,j=0,1) \ .$$

Moreover, if $w^*(\underline{d}) = w^*(\underline{d}')$ define $\alpha(\underline{d},\underline{d}')$, $\beta(\underline{d},\underline{d}')$, $\gamma(\underline{d},\underline{d}')$ by

$$(72) \qquad \begin{aligned} \alpha(\underline{d},\underline{d}').w + \gamma(\underline{d},\underline{d}') &:= a_{10}(\underline{d},\underline{d}') \\ \beta(\underline{d},\underline{d}').w + \gamma(\underline{d},\underline{d}') &:= a_{01}(\underline{d},\underline{d}') \end{aligned} \qquad 0 \le \gamma(\underline{d},\underline{d}') < w \ .$$

(This definition is legitimate, since $w^*(\underline{d}) = w^*(\underline{d}')$.)

Moreover the code Z , which is introduced in (3.4.1), shall in the following be defined by:

4.2.2.Definition. Define the binary code Z of length s by

$$(73) \qquad Z := \{ \underline{z} \in \mathbb{F}_2^s \mid w_H(\underline{z}) \equiv 0 \mod w \} \ .$$

Below we derive another form of the conditions from (3.4.3). The reader should realize that we do not intend to enumerate the numbers $M_Z(\underline{y})$ according to (68) for this would be very complicated. As a first result we have the lemma below.

4.2.3.Lemma. Let all definitions be as in (4.2.1), Z as in (4.2.2). Fix $\underline{y} \in (D^{(0)} \cup E)^s$ and let $\underline{d},\underline{d}' \in A(\underline{y})$. Then the existence of $\underline{z},\underline{z}' \in Z$ as in (61) implies $w^*(\underline{d}) = w^*(\underline{d}')$.

Proof. Since only the two vectors $\underline{d}$ and $\underline{d}'$ are involved we shall abbreviate $a_{ij}(\underline{d},\underline{d}')$ to a_{ij} in this proof $(i,j=0,1)$. Assume that for $\underline{d}$ and $\underline{d}'$ there are vectors $\underline{z},\underline{z}' \in Z$ as in (61). Define $x := |\{ k \mid z_k = z'_k = 1 \}|$. It is clear that

$$w_H(\underline{z}) = a_{01} + x \equiv 0 \ \underline{\text{mod}}\ w \quad \text{and} \quad w_H(\underline{z}') = a_{10} + x \equiv 0 \ \underline{\text{mod}}\ w \ .$$

Hence $a_{10}-a_{01} \equiv 0 \ \underline{\text{mod}}\ w$ .Furthermore

$$w^*(\underline{d}) = a_{10} + a_{11} \ \underline{\text{mod}}\ w \quad \text{and} \quad w^*(\underline{d}') = a_{01} + a_{11} \ \underline{\text{mod}}\ w \ ,$$

which implies $w^*(\underline{d}) - w^*(\underline{d}') \equiv a_{10} - a_{01} \equiv 0 \ \underline{\text{mod}}\ w$. □

Now the following lemma gives us the new form of the conditions from (3.4.3).

4.2.4.Lemma.Let all definitions be as in (4.2.1), Z as in (4.2.2).Fix $\underline{y} \in (D^{(0)} \cup E)^s$ and $\underline{d},\underline{d}' \in A(\underline{y})$ such that $w^*(\underline{d}) = w^*(\underline{d}')$ .Then the existence of $\underline{z},\underline{z}' \in Z$ as in (61) is equivalent to:

(74)
$$\begin{aligned} &\text{Either } \gamma(\underline{d},\underline{d}') = 0 \ , \text{or } \alpha(\underline{d},\underline{d}') + \beta(\underline{d},\underline{d}') < q - 1 \ , \\ &\text{or } \alpha(\underline{d},\underline{d}') + \beta(\underline{d},\underline{d}') = q - 1 \quad \text{and } \gamma(\underline{d},\underline{d}') \le r \quad . \end{aligned}$$

Proof.As in the proof of (4.2.3) we shall delete the postscript $(\underline{d},\underline{d}')$ belonging to a_{ij} ,α,β, and γ.
First assume $\underline{z},\underline{z}' \in Z$ exist with the desired properties.Define $x := |\{ k \mid z_k = z'_k = 1 \}|$ as in the proof of (4.2.3).Since $w_H(\underline{z}) = a_{01} + x \equiv 0 \ \underline{\text{mod}}\ w$ it is clear that $x \ge 0$ if $\gamma = 0$,and $x \ge w - \gamma$ if $\gamma \ne 0$.
Hence $s = qw + r \ge a_{10} + a_{01} + x$ gives us either $x = 0$,which implies $\gamma = 0$ (note that $a_{10} + a_{01} \le s$ from their definition),or $w(\alpha + \beta + 1) + \gamma \le qw + r$ .The latter implies $\alpha + \beta \le q - 1$ and,in addition, $\gamma \le r$ if $\alpha + \beta = q - 1$.

Next,assume (74) is satisfied.Define x by: $x := 0$ if $\gamma = 0$ and $x := w - \gamma$ if $\gamma \ne 0$ .We see from the above that (74) implies $a_{01} + a_{10} + x \le s$ .Now assume w.l.o.g. that $\underline{d}_i = \underline{d}'_i$ for $i = 1,2,\ldots,s - a_{01} - a_{10}$ .Define $\underline{z},\underline{z}' \in Z$ as follows:

$$(z_i, z_i') = \begin{cases} (1,1) & \text{if} \quad 1 \le i \le x \\ (0,0) & \text{if} \quad x < i \le s - a_{01} - a_{10} \\ (0,1) & \text{if} \quad \underline{d}_i \in D^{(1)} \wedge \underline{d}_i' \in D^{(0)} \\ (1,0) & \text{if} \quad \underline{d}_i \in D^{(0)} \wedge \underline{d}_i' \in D^{(1)} \end{cases}$$

Since $x \le s - a_{01} - a_{10}$ it is clear that $\underline{z}$ and $\underline{z}'$ are well-defined.Furthermore they satisfy (61) if $\underline{z}, \underline{z}' \in Z$ .We have

$$w_H(\underline{z}) = a_{01} + x = \begin{cases} \beta w + \gamma + w - \gamma \equiv 0 \ \underline{\text{mod}}\ w & \text{if} \quad \gamma \neq 0 \\ \beta w + \gamma \equiv 0 \ \underline{\text{mod}}\ w & \text{if} \quad \gamma = 0 \end{cases}$$

This implies that $\underline{z} \in Z$ .Similarly $\underline{z}' \in Z$. □

In the following section we shall evaluate $M_Z(\underline{y})$ by use of the above Lemmas. We shall first give an example.

4.2.5.Example.For $w = 2$,van Tilborg showed ([8]) that

$$M_Z(\underline{y}) = \begin{cases} 1 & \text{if} \quad |W(\underline{y})| = s \\ 2 & \text{if} \quad 0 < |W(\underline{y})| < s \text{ ,or } |W(\underline{y})| = 0 \text{ and } r = 1 \\ 3 & \text{if} \quad |W(\underline{y})| = 0 \text{ and } r = 0 \end{cases}$$

4.3.Evaluation of $M_Z(\underline{y})$.

In this section we shall have a close investigation of the conditions (74) and the resulting choice of $A(\underline{y}) \cap \mathcal{D}$ for each $\underline{y} \in (D^{(0)} \cup E)^s$ .We remark that (4.2.3),(4.2.4) and the definition of $M_Z(\underline{y})$ imply that,for $\underline{y} \in (D^{(0)} \cup E)^s$ and Z as in (4.2.2):

(75) $M_Z(\underline{y})$ = The maximum number of vectors in $A(\underline{y})$ such that for each pair $\underline{d}, \underline{d}'$ of them one of the following holds:

(a) $w^*(\underline{d}) \neq w^*(\underline{d}')$,or

(b) $\alpha(\underline{d},\underline{d}') + \beta(\underline{d},\underline{d}') = q - 1$ and $\gamma(\underline{d},\underline{d}') > r$,or

(c) $\alpha(\underline{d},\underline{d}') + \beta(\underline{d},\underline{d}') = q$ and $\gamma(\underline{d},\underline{d}') \neq 0$.

It shall be convenient to make use of the following definition:

4.3.1.Definition.Let $\underline{y} \in (D^{(0)} \cup E)^s$,$\underline{d},\underline{d}' \in A(\underline{y})$ .We call the pair $\{\underline{d},\underline{d}'\}$ inadmissible if none of the above three cases (75)(a),(b),(c) is satisfied for $\underline{d}$ and $\underline{d}'$.(Note that the roles of $\underline{d}$ and $\underline{d}'$ in (75) are similar.Moreover $(C,\{\underline{d},\underline{d}'\})$ is uniquely decodable iff $\{\underline{d},\underline{d}'\}$ is not inadmissible.)

The following lemma is a first observation concerning inadmissible pairs.

4.3.2.Lemma.Let all definitions be as in (4.2.1) where $q \geq 2$ and define $\delta := \max\{ r, w - r \}$ .Fix $\underline{y} \in (D^{(0)} \cup E)^s$ .Then

(i) For any triple $\{\underline{e},\underline{e}',\underline{e}''\} \subset A(\underline{y})$ such that $w^*(\underline{e}) = w^*(\underline{e}') = w^*(\underline{e}'')$ there is an inadmissible pair $\{\underline{d},\underline{d}'\} \subset \{\underline{e},\underline{e}',\underline{e}''\}$.

(ii) If $|W(\underline{y})| > \delta - 2$ we have that any pair $\{\underline{d},\underline{d}'\} \subset A(\underline{y})$ such that $w^*(\underline{d}) = w^*(\underline{d}')$ is inadmissible.

Before proving the Lemma we first state the following:

4.3.3.Corollary.Let all definitions be as in (4.2.1) where $q \geq 2$.Let Z be as in (4.2.2) and $\delta := \max\{ r, w - r \}$ .Then for each $\underline{y} \in (D^{(0)} \cup E)^s$ we have

(76)
(i) $M_Z(\underline{y}) \leq 2w$,and
(ii) If $|W(\underline{y})| > \delta - 2$: $M_Z(\underline{y}) = \min\{ w , s - |W(\underline{y})| + 1 \}$.

Proof of Lemma (4.3.2).We shall prove (ii) first.So,assume that $|W(\underline{y})| > \delta - 2$

and fix $\underline{d},\underline{d}' \in A(\underline{y})$ such that $w^*(\underline{d}) = w^*(\underline{d}')$.

Since $|\{ k \mid \underline{d}_k \neq \underline{d}'_k \}| \leq s - |W(\underline{y})| < qw + r - \delta + 2$,we have

$$(77)\quad \begin{array}{ll} (a) & a_{01}(\underline{d},\underline{d}') + a_{10}(\underline{d},\underline{d}') < (q-1)w + 2r + 2 \quad \text{,and} \\ (b) & a_{01}(\underline{d},\underline{d}') + a_{10}(\underline{d},\underline{d}') < qw + 2 \quad . \end{array}$$

Note that the left hand sides in (a) and (b) equal

$$[\ \alpha(\underline{d},\underline{d}') + \beta(\underline{d},\underline{d}')\ ].w + 2\,\gamma(\underline{d},\underline{d}') \quad .$$

Now from (a) we see that $\alpha(\underline{d},\underline{d}') + \beta(\underline{d},\underline{d}') = q-1$ implies $\gamma(\underline{d},\underline{d}') \leq r$.

Similarly,from (b),we have that $\alpha(\underline{d},\underline{d}') + \beta(\underline{d},\underline{d}') = q$ implies $\gamma(\underline{d},\underline{d}') = 0$.

So $\{\underline{d},\underline{d}'\}$ is an inadmissible pair.

Next,in order to prove (i),note that we are done unless $|W(\underline{y})| \leq \delta - 2$ .So assume that this is the case and fix $\{\underline{e},\underline{e}',\underline{e}''\} \subset A(\underline{y})$ such that $w^*(\underline{e}) = w^*(\underline{e}') = w^*(\underline{e}'')$ .Again from the above we are done unless for each pair $\{\underline{d},\underline{d}'\} \subset \{\underline{e},\underline{e}',\underline{e}''\}$ either (77)(a) or (77)(b) is violated.

We define $b_{ijk} := |\{ \ell \mid \underline{e}_\ell \in D^{(i)} \wedge \underline{e}'_\ell \in D^{(j)} \wedge \underline{e}''_\ell \in D^{(k)} \}|$ .Then we have

$$\begin{array}{lll} a_{01}(\underline{e},\underline{e}') = b_{010} + b_{011} & ; & a_{10}(\underline{e},\underline{e}') = b_{100} + b_{101} \quad , \\ a_{01}(\underline{e},\underline{e}'') = b_{001} + b_{011} & ; & a_{10}(\underline{e},\underline{e}'') = b_{100} + b_{110} \quad , \\ a_{01}(\underline{e}',\underline{e}'') = b_{001} + b_{101} & ; & a_{10}(\underline{e}',\underline{e}'') = b_{010} + b_{110} \quad . \end{array}$$

It follows that with the definition

$$t := \sum_{(\underline{d},\underline{d}') \in \{(\underline{e},\underline{e}'),(\underline{e},\underline{e}''),(\underline{e}',\underline{e}'')\}} [\ a_{01}(\underline{d},\underline{d}') + a_{10}(\underline{d},\underline{d}')\ ]$$

we have $t = 2 \sum_{(i,j,k) \notin \{(000),(111)\}} b_{ijk} \leq 2s \quad (*)$.

We will show that for none of the choices of $\{\underline{d},\underline{d}'\} \subset \{\underline{e},\underline{e}',\underline{e}''\}$ (77)(b) is

violated.Consider the following cases:

(I) All of the choices violate (b).It follows that $t \geq 3qw + 6$.

(II) Exactly two of the choices violate (b).From the remark on the preceding page we find that the third choice violates (a).So $t \geq (3q - 1)w + 2r + 6$.

(III) Exactly one of the choices violates (b) and the other two violate (a). Now we have $t \geq (3q - 2)w + 4r + 6$.

Combining these with (*) we find $qw + 6 \leq 2r$ in case (I) ; $(q - 1)w + 6 \leq 0$ in case (II) and $(q - 2)w + 2r + 6 \leq 0$ in case (III).It is clear that none of these hold if $q \geq 2$ .So the only remaining possibility is:

(IV) All choices of $\{\underline{d},\underline{d}'\} \subset \{\underline{e},\underline{e}',\underline{e}''\}$ violate (77)(a),but not (77)(b) .

(IV) implies that $t \geq (3q - 3)w + 6r + 6$ which leads to $4r + 6 \leq (3 - q)w$ .Hence we are done if $q > 2$ .From now on assume that $q = 2$.

The last part of assumption (IV) implies (like in the proof of (ii)) that for each pair $\{\underline{d},\underline{d}'\} \subset \{\underline{e},\underline{e}',\underline{e}''\}$ such that $\alpha(\underline{d},\underline{d}') + \beta(\underline{d},\underline{d}') = q = 2$ we have $\gamma(\underline{d},\underline{d}') = 0$.

Hence (according to (4.3.1)) again we are done,unless for each of the choices for $\{\underline{d},\underline{d}'\}$ we have $\alpha(\underline{d},\underline{d}') + \beta(\underline{d},\underline{d}') = 1$ and $\gamma(\underline{d},\underline{d}') > r$ (**) .

Hence,assuming (**) and relabeling $\underline{e},\underline{e}',\underline{e}''$ if necessary,we have $\alpha(\underline{e},\underline{e}') = 1$, $\beta(\underline{e},\underline{e}') = 0$ .But now $\beta(\underline{e},\underline{e}'') \neq 1$ or else $s = 2w + r \geq b_{100} + b_{101} + b_{001} + b_{011} = a_{10}(\underline{e},\underline{e}') + a_{01}(\underline{e},\underline{e}'') > 2w + 2r$ which is impossible.Similarly, $\alpha(\underline{e}',\underline{e}'') \neq 1$ or else $s = 2w + r \geq b_{100} + b_{101} + b_{010} + b_{110} = a_{10}(\underline{e},\underline{e}') + a_{10}(\underline{e}',\underline{e}'') > 2w + 2r$ .But now we have $\beta(\underline{e}',\underline{e}'') = \alpha(\underline{e},\underline{e}'') = 1$ which implies that $s = 2w + r \geq b_{100} + b_{110} + b_{001} + b_{101} = a_{10}(\underline{e},\underline{e}'') + a_{01}(\underline{e}',\underline{e}'') > 2w + 2r$ .Hence (**) is false which proves (i). □

Now for $q \geq 2$ we see from the preceding Lemma how we can find $M_Z(\underline{y})$ for $\underline{y} \in (D^{(0)} \cup E)^s$, $|W(\underline{y})| \leq \delta - 2$ .We only need to examine the maximum number of

values of w^* such that two vectors $\underline{d},\underline{d}'$ can be added to $\mathcal{D} \cap A(\underline{y})$ satisfying $w^*(\underline{d}) = w^*(\underline{d}') = w^*$ .This number being M ,we have $M_Z(\underline{y}) = 2M + (w - M) = w + M$.(Note $|W(\underline{y})| \leq \delta - 2$ implies that for each $w^* \in \{0,1,\ldots,w-1\}$ there are vectors $\underline{d}$ in $A(\underline{y})$ such that $w^*(\underline{d}) = w^*$.) The lemma below shows that for certain values of w^* only one vector may be added to $\mathcal{D}$.We first need the following definition.

4.3.4.Definition.Let all definitions be as in (4.2.1),where $q \geq 2$ .Define $\delta := \max\{r, w-r\}$ and fix $\underline{y} \in (D^{(0)} \cup E)^s$ such that $|W(\underline{y})| \leq \delta - 2$ .We define the sets $V_1(\underline{y})$, $V_2(\underline{y})$, $B_1(\underline{y})$ and $B_2(\underline{y})$ by

(78)
$$V_1(\underline{y}) := \begin{cases} \phi & \text{if } 2r < w \text{ and } |W(\underline{y})| \geq r-1 \\ \{1,2,\ldots,r-1-|W(\underline{y})|\} & \text{otherwise} \end{cases}$$

$$V_2(\underline{y}) := \begin{cases} \phi & \text{if } 2r \geq w \text{ and } |W(\underline{y})| \geq w-r-1 \\ \{r+1,r+2,\ldots,w-1-|W(\underline{y})|\} & \text{otherwise} \end{cases}$$

(79) $$B_2(\underline{y}) := V_1(\underline{y}) \cup V_2(\underline{y}) \text{ and } B_1(\underline{y}) := \{0,1,\ldots,w-1\} \setminus B_2(\underline{y}) .$$

Remark: $B_2(\underline{y})$ is splitted for later use in Chapter 5.

4.3.5.Lemma.Let all definitions be as in (4.2.1),where $q \geq 2$ .Define $\delta := \max\{r, w-r\}$ and fix $\underline{y} \in (D^{(0)} \cup E)^s$ such that $|W(\underline{y})| \leq \delta - 2$ .Let $B_1(\underline{y})$ be as in (4.3.4).Then each pair $\{\underline{d},\underline{d}'\} \subset A(\underline{y})$ such that $w^*(\underline{d}) = w^*(\underline{d}') \in B_1(\underline{y})$ is inadmissible.

Proof.Fix $\{\underline{d},\underline{d}'\} \subset A(\underline{y})$ such that $w^*(\underline{d}) = w^*(\underline{d}') =: \ell$,and assume that $\{\underline{d},\underline{d}'\}$ is not inadmissible.It is clear that the lemma is proved if we can show that $\ell \in B_2(\underline{y})$ .Define

$$\rho := \begin{cases} 1 & \text{if } 2r \geq w \quad (\text{i.e. } \delta = r) \\ r+1 & \text{if } 2r < w \quad (\text{i.e. } \delta = w-r) \end{cases}$$

In this proof we shall abbreviate $a_{ij}(\underline{d},\underline{d}')$ to a_{ij} and similar for α,β,γ .

We note that

(i) $\sum_{i,j=0,1} a_{ij} = s - |W(\underline{y})|$, $a_{ij} \geq 0$ $(i,j=0,1)$;

(ii) $a_{01} + a_{10} \geq s - \delta + 2$ (this follows from the proof of (4.3.2(ii)) ;

(iii) $\ell \equiv a_{11} + \gamma \pmod{w}$;

(iv) $a_{01} + a_{10} \equiv 2\gamma \pmod{w}$.

Now (i) and (ii) imply that there is some k, $0 \leq k \leq \delta - 2 - |W(\underline{y})|$ such that

(v) $a_{01} + a_{10} = s - \delta + 2 + k = \begin{cases} qw + 2\rho + k & \text{if } 2r \geq w \\ (q-1)w + 2\rho + k & \text{if } 2r < w \end{cases}$, and

(vi) $0 \leq a_{11} \leq \delta - 2 - |W(\underline{y})| - k$.

Now (iv) and (v) imply $2\gamma \equiv a_{01} + a_{10} \equiv 2\rho + k \pmod{w}$ .Hence we have

case w is even : k is even and $\gamma \in \{\rho + \frac{k}{2}, \rho + \frac{k+w}{2} \pmod{w}\}$,

case w is odd : $\gamma = \rho + \frac{k}{2}$ if k is even ,

$\gamma = \rho + \frac{k+w}{2} \pmod{w}$ if k is odd.

(We note that $\rho + \frac{k}{2} < w$.)

(A) Suppose $\gamma = \rho + \frac{k}{2}$. Then from (iii) and (vi) we have that $w^*(\underline{d}) = \ell \in U_1(k)$ where

$$U_1(k) := \{ \rho + \tfrac{k}{2} \pmod{w}, \rho + 1 + \tfrac{k}{2} \pmod{w}, \ldots, \rho + \delta - 2 - |W(\underline{y})| - \tfrac{k}{2} \pmod{w} \} .$$

Note that $k \geq 0 \Rightarrow U_1(k) \subset U_1(0)$ .Hence if $\gamma = \rho + \frac{k}{2}$ for some k we have

(80) $$w^*(\underline{d}) = \ell \in U_1(0) = \begin{cases} \{1,2,\ldots,r-1-|W(\underline{y})|\} = V_1(\underline{y}) & \text{,if } 2r \geq w ; \\ \{r+1,r+2,\ldots,w-1-|W(\underline{y})|\} = V_2(\underline{y}) & \text{,if } 2r < w . \end{cases}$$

(B) From now on we shall assume that $\gamma = \rho + \frac{k+w}{2} \pmod{w}$ for some k .So again from (iii) and (vi) we find that $w^*(\underline{d}) = \ell \in U_2(k)$,where

$$U_2(k) := \{\, \rho + \tfrac{w+k}{2} \underline{\bmod} w\,,\ \rho + 1 + \tfrac{w+k}{2} \underline{\bmod} w\,,\ldots,\rho + \tfrac{w-k}{2} + \delta - 2 - |W(\underline{y})| \underline{\bmod} w \,\}\,.$$

Since $w(\alpha+\beta) \equiv a_{01} + a_{10} - 2\gamma \underline{\bmod} w$,we find from (v)

case $2r \geq w$: $\alpha+\beta = q-1$ (Note that in this case always $\rho + \frac{k+w}{2} < w$)

case $2r < w$: $\alpha+\beta = q-2$ unless $\rho + \frac{k+w}{2} \geq w$,in which case

$\alpha+\beta = q$ .Here $\rho + \frac{k+w}{2} = w$ corresponds to $\gamma = 0$.

Since $\underline{d}$ and $\underline{d}'$ satisfy (75)(b) or (75)(c) we have

case $2r \geq w$: $\gamma = \rho + \frac{k+w}{2} > r$ i.e. $k \geq 2r - w$;

case $2r < w$: $\rho + \frac{k+w}{2} > w$ i.e. $k \geq w - 2r$.

This shows that the condition $0 \leq k \leq \delta - 2 - |W(\underline{y})|$ should be replaced by :

(vii) $2\delta - w \leq k \leq \delta - 2 - |W(\underline{y})|$ (Note that the lower bound has suitable parity.)

Now note that $k > h \Rightarrow U_2(k) \subset U_2(h)$ (*) and consider the following cases:

(81)(a) $|W(\underline{y})| \geq w - \delta - 1 = \begin{cases} w - r - 1 & \text{if } 2r \geq w\,, \\ r - 1 & \text{if } 2r < w\,. \end{cases}$

Now there does not exist a k satisfying (vii).Hence $w^*(\underline{d}) = \ell \in \emptyset$.

(81)(b) $|W(\underline{y})| < w - \delta - 1$.(vii) and (*) imply

$$w^*(\underline{d}) = \ell \in U_2(2\delta - w) = \begin{cases} \{r+1, r+2, \ldots, w - 1 - |W(\underline{y})|\,\} = V_2(\underline{y}), & \text{if } 2r \geq w \\ \{1, 2, \ldots, r - 1 - |W(\underline{y})|\,\} = V_1(\underline{y}) & \text{if } 2r < w \end{cases}$$

Now (80) and (81) prove the lemma. □

Now fix $\underline{y} \in (D^{(0)} \cup E)^s$ such that $|W(\underline{y})| \leq \delta - 2$ .Suppose that for each $\ell \in B_2(\underline{y})$ we can actually construct a pair $\{\underline{d}_\ell, \underline{d}'_\ell\} \subset A(\underline{y})$ s.t. $w^*(\underline{d}_\ell) = w^*(\underline{d}'_\ell) = \ell$ and $\{\underline{d}_\ell, \underline{d}'_\ell\}$ is <u>not</u> inadmissible.Then the number $M_Z(\underline{y})$ is determined,namely $M_Z(\underline{y}) = |B_1(\underline{y})| + 2|B_2(\underline{y})|$.(Note that for $|W(\underline{y})| > \delta - 2$ the number is already

known,cf.(4.3.3).)

In the following lemma we describe the construction of these pairs.The reader should realize that the lemma states much more than we need right now for this construction.The use of this will become clear in Chapter 5.

4.3.6.Lemma.Let all definitions be as in (4.2.1) where $q \geq 2$ .Define $\delta := \max\{r, w-r\}$ and fix $\underline{y} \in (D^{(0)} \cup E)^s$ s.t. $|W(\underline{y})| \leq \delta - 2$ .Let $B_2(\underline{y}) = V_1(\underline{y}) \cup V_2(\underline{y})$ be as in (4.3.4) and define the following numbers:

$$b_{10}(\underline{y}) := 1 \quad ; b_{01}(\underline{y}) := qw+1 \quad ; b_{11}(\ell,\underline{y}) := \ell - 1 \quad \text{for } \ell \in V_1(\underline{y}) \quad ;$$

$$c_{10}(\underline{y}) := r+1 \quad ; c_{01}(\underline{y}) := (q-1)w+r+1 \quad ; c_{11}(k,\underline{y}) := k-r-1 \quad \text{for}$$

(82) $\quad k \in V_2(\underline{y})$,and

$$b_{00}(\ell,\underline{y}) := s - |W(\underline{y})| - b_{11}(\ell,\underline{y}) - b_{10}(\underline{y}) - b_{01}(\underline{y}) \quad , \ell \in V_1(\underline{y}) \ ;$$

$$c_{00}(k,\underline{y}) := s - |W(\underline{y})| - c_{11}(k,\underline{y}) - c_{10}(\underline{y}) - c_{01}(\underline{y}) \quad , k \in V_2(\underline{y}) \ .$$

Then these numbers satisfy the following properties:

(i) For each $\ell \in V_1(\underline{y})$, $k \in V_2(\underline{y})$ there exist vectors $\underline{d},\underline{d}',\underline{e},\underline{e}' \in A(\underline{y})$ s.t.

(83) $\quad a_{10}(\underline{d},\underline{d}') = b_{10}(\underline{y}) \quad ; \quad a_{01}(\underline{d},\underline{d}') = b_{01}(\underline{y}) \quad ,$

(84) $\quad a_{11}(\underline{d},\underline{d}') = b_{11}(\ell,\underline{y}) \ ; \quad a_{00}(\underline{d},\underline{d}') = b_{00}(\ell,\underline{y}) \quad ,$

(85) $\quad a_{10}(\underline{e},\underline{e}') = c_{10}(\underline{y}) \quad ; \quad a_{01}(\underline{e},\underline{e}') = c_{01}(\underline{y}) \quad ,$

(86) $\quad a_{11}(\underline{e},\underline{e}') = c_{11}(k,\underline{y}) \ ; \quad a_{00}(\underline{e},\underline{e}') = c_{00}(k,\underline{y}) \quad .$

(ii) For each pair of vectors $\{\underline{d},\underline{d}'\} \subset A(\underline{y})$ satisfying (83) and (84) resp. $\{\underline{e},\underline{e}'\} \subset A(\underline{y})$ satisfying (85) and (86) we have that $w^*(\underline{d}) = w^*(\underline{d}') = \ell$, $w^*(\underline{e}) = w^*(\underline{e}') = k$,and neither $\{\underline{d},\underline{d}'\}$ nor $\{\underline{e},\underline{e}'\}$ is inadmissible.

(iii) For each choice of $\underline{d},\underline{d}',\underline{e},\underline{e}' \in A(\underline{y})$ such that (83) and (85) are satisfied

we have $w^*(\underline{d}) = w^*(\underline{d}') \in V_1(\underline{y})$ and $w^*(\underline{e}) = w^*(\underline{e}') \in V_2(\underline{y})$ .Moreover,in particular, $w^*(\underline{d}) \neq w^*(\underline{e})$.

(iv) If $\ell \in V_1(\underline{y})$, $\ell \neq r - 1 - |W(\underline{y})|$ then $b_{00}(\ell,\underline{y}) > 0$,and
if $k \in V_2(\underline{y})$, $k \neq w - 1 - |W(\underline{y})|$ then $c_{00}(k,\underline{y}) > 0$.

Before proving the lemma we first state a corollary which gathers the results concerning $M_Z(\underline{y})$.

4.3.7.Corollary.Let all definitions be as in (4.2.1),where $q \geq 2$ .Let Z be as in (4.2.2).Define $\delta := \max\{r, w-r\}$ and fix $\underline{y} \in (D^{(0)} \cup E)^s$ .Then

(i) If $|W(\underline{y})| > \delta - 2$: $M_Z(\underline{y}) = \min\{ w , s - |W(\underline{y})| + 1 \}$;

(ii) If $|W(\underline{y})| \leq \delta - 2$: $M_Z(\underline{y}) = \max\{ w + \delta - 1 - |W(\underline{y})|, 2(w - 1 - |W(\underline{y})|) \}$.

Proof of the corollary. (i) is noted in (4.3.3)(ii) .

(ii) From Lemmas (4.3.5) and (4.3.6) it is clear that for $|W(\underline{y})| \leq \delta - 2$: $M_Z(\underline{y}) = |B_1(\underline{y})| + 2|B_2(\underline{y})| = w + |B_2(\underline{y})|$ .We have

case $2r \geq w$: $|W(\underline{y})| \geq w - r - 1 = w - \delta - 1 \Rightarrow |B_2(\underline{y})| = r - 1 - |W(\underline{y})| = \delta - 1 - |W(\underline{y})|$
$|W(\underline{y})| < w - \delta - 1 \Rightarrow |B_2(\underline{y})| = w - 2 - 2|W(\underline{y})|$

case $2r < w$: $|W(\underline{y})| \geq r - 1 = w - \delta - 1 \Rightarrow |B_2(\underline{y})| = w - r - 1 - |W(\underline{y})| = \delta - 1 - |W(\underline{y})|$
$|W(\underline{y})| < w - \delta - 1 \Rightarrow |B_2(\underline{y})| = w - 2 - 2|W(\underline{y})|$

Now the result follows after a straightforward calculation. □

Proof of lemma (4.3.6).(cf.(4.3.8).) We note that (i) is equivalent to

(87) $b_{10}(\underline{y}) \geq 0$, $b_{01}(\underline{y}) \geq 0$, $c_{10}(\underline{y}) \geq 0$, $c_{01}(\underline{y}) \geq 0$,and

(88) $b_{11}(\ell,\underline{y}) \geq 0$, $b_{00}(\ell,\underline{y}) \geq 0$, $c_{11}(k,\underline{y}) \geq 0$, $c_{00}(k,\underline{y}) \geq 0$ (all ℓ,k),and

$$(89)\qquad \begin{aligned} &b_{10}(\underline{y}) + b_{01}(\underline{y}) + b_{11}(\ell,\underline{y}) + b_{00}(\ell,\underline{y}) + |W(\underline{y})| = s \quad , \ \ell \in V_1(\underline{y}) \\ &c_{10}(\underline{y}) + c_{01}(\underline{y}) + c_{11}(k,\underline{y}) + c_{00}(k,\underline{y}) + |W(\underline{y})| = s \quad , \ k \in V_2(\underline{y}) \quad . \end{aligned}$$

Next note that the first claim in (ii) is equivalent to

$$(90)\qquad \begin{aligned} &b_{10}(\underline{y}) + b_{11}(\ell,\underline{y}) \equiv b_{01}(\underline{y}) + b_{11}(\ell,\underline{y}) \equiv \ell \ \underline{\text{mod}}\ w \quad ,\text{and} \\ &c_{10}(\underline{y}) + c_{11}(k,\underline{y}) \equiv c_{01}(\underline{y}) + c_{11}(k,\underline{y}) \equiv k \ \underline{\text{mod}}\ w \quad . \end{aligned}$$

And,according to definition (4.3.1),the second claim in (ii) is equivalent to

$$(91)\qquad \begin{aligned} &\alpha_b + \beta_b = q \ , \ \gamma_b \neq 0 \quad \text{or} \quad \alpha_b + \beta_b = q-1 \ , \ \gamma_b > r \quad ,\text{and} \\ &\alpha_c + \beta_c = q \ , \ \gamma_c \neq 0 \quad \text{or} \quad \alpha_c + \beta_c = q-1 \ , \ \gamma_c > r \quad ,\text{where} \\ &b_{10}(\underline{y}) =: \alpha_b.w + \gamma_b \ , \ b_{01}(\underline{y}) =: \beta_b.w + \gamma_b \ , \ 0 \leq \gamma_b < w \quad (\text{cf.}(4.2.1)), \\ &\text{and} \ \ \alpha_c \ , \ \beta_c \ , \ \gamma_c \ \ \text{are defined similarly.} \end{aligned}$$

It is clear that (90) and (91) are trivially satisfied,which proves (ii).(Note that $r+1=w$ would imply $2r \geq w$, $|W(\underline{y})| \geq w-r-1$ and hence $V_2(\underline{y}) = \phi$,in which case there is nothing to prove for the numbers c_{ij} .)
Furthermore (87) and (89) are satisfied.Fixing the numbers $b_{10}(\underline{y})$, $b_{01}(\underline{y})$, $c_{10}(\underline{y})$ and $c_{01}(\underline{y})$ we have that $\{ b_{11}(\ell,\underline{y}) \mid \ell \in V_1(\underline{y}) \}$ respectively $\{c_{11}(k,\underline{y}) \mid k \in V_2(\underline{y}) \}$ is exactly the set of numbers for which (88) holds.This proves (i).Moreover,in combination with (ii) it proves also the first claim in (iii).The second part of (iii) is clear since $V_1(\underline{y}) \cap V_2(\underline{y}) = \phi$.
Finally,(iv) is a simple matter of checking. □

4.3.8.Examples.In all examples below we choose C,D and E of length n as follows: $C^{(0)} = D^{(0)} = \{\underline{0}\}$, $C^{(1)} = D^{(1)} = \{\underline{1}\}$, $E = \{\underline{x}\}$ for some fixed vector $\underline{x} \notin \{\underline{0},\underline{1}\}$. The vectors in the examples are subscripted in such a way

that the subscript equals the corresponding value of w* ,for example $w^*(\underline{e}_3)=3$.

(i)	q = 2	$\underline{y} = \underline{0}^{12}$	$b_{10}(\underline{y}) = 1$	$b_{11}(1,\underline{y}) = 0$,	$b_{00}(1,\underline{y}) = 0$
	w = 5		$b_{01}(\underline{y}) = 11$		
	r = 2	$\lvert W(\underline{y})\rvert = 0$	$c_{10}(\underline{y}) = 3$	$c_{11}(3,\underline{y}) = 0$,	$c_{00}(3,\underline{y}) = 1$
	δ = 3	$V_1(\underline{y}) = \{1\}$	$c_{01}(\underline{y}) = 8$	$c_{11}(4,\underline{y}) = 1$,	$c_{00}(4,\underline{y}) = 0$
	s = 12	$V_2(\underline{y}) = \{3,4\}$			

table 9.

We can construct the following vectors,which may all be added to $\mathcal{V}$:

$\underline{d}_1 : \underline{1}|\underline{0}^{11}$ $\quad \underline{e}_3 : \underline{0}|\underline{1}^3|\underline{0}^8$ $\quad \underline{e}_4 : \underline{1}|\underline{1}^3|\underline{0}^8$ (Of course many other choices

$\underline{d}_1' : \underline{0}|\underline{1}^{11}$ $\quad \underline{e}_3' : \underline{0}|\underline{0}^3|\underline{1}^8$ $\quad \underline{e}_4' : \underline{1}|\underline{0}^3|\underline{1}^8$ are possible.)

(ii)	q = 2	$\underline{y} = \underline{x}|\underline{0}^{12}$	$b_{10}(\underline{y}) = 1$	$b_{11}(1,\underline{y}) = 0$,	$b_{00}(1,\underline{y}) = 0$
	w = 5		$b_{01}(\underline{y}) = 11$		
	r = 3	$\lvert W(\underline{y})\rvert = 1$			
	δ = 3	$V_1(\underline{y}) = \{1\}$			
	s = 13	$V_2(\underline{y}) = \phi$			

table 10.

The following vectors can both be added to $\mathcal{V}$: $\underline{d}_1 : \underline{x}|\underline{1}|\underline{0}^{11}$, $\underline{d}' : \underline{x}|\underline{0}|\underline{1}^{11}$.

(iii)	q = 3	$\underline{y} = \underline{x}^2|\underline{0}^{40}$	$b_{10}(\underline{y}) = 1$	$b_{11}(1,\underline{y}) = 0$,	$b_{00}(1,\underline{y}) = 2$
	w = 12		$b_{01}(\underline{y}) = 37$	$b_{11}(2,\underline{y}) = 1$,	$b_{00}(2,\underline{y}) = 1$
	r = 6	$\lvert W(\underline{y})\rvert = 2$		$b_{11}(3,\underline{y}) = 2$,	$b_{00}(3,\underline{y}) = 0$
	δ = 6	$V_1(\underline{y}) = \{1,2,3\}$	$c_{10}(\underline{y}) = 7$	$c_{11}(7,\underline{y}) = 0$,	$c_{00}(7,\underline{y}) = 2$
	s = 42	$V_2(\underline{y}) = \{7,8,9\}$	$c_{01}(\underline{y}) = 31$	$c_{11}(8,\underline{y}) = 1$,	$c_{00}(8,\underline{y}) = 1$
				$c_{11}(9,\underline{y}) = 2$,	$c_{00}(9,\underline{y}) = 0$

table 11.

Construct the following vectors:

$\underline{d}_1 : \underline{x}^2|\underline{0}^2|\underline{1}|\underline{0}^{37}$ $\quad \underline{d}_2 : \underline{x}^2|\underline{0}|\underline{1}|\underline{1}|\underline{0}^{37}$ $\quad \underline{d}_3 : \underline{x}^2|\underline{1}^2|\underline{1}|\underline{0}^{37}$

$\underline{d}_1' : \underline{x}^2|\underline{0}^2|\underline{0}|\underline{1}^{37}$ $\quad \underline{d}_2' : \underline{x}^2|\underline{0}|\underline{1}|\underline{0}|\underline{1}^{37}$ $\quad \underline{d}_3' : \underline{x}^2|\underline{1}^2|\underline{0}|\underline{1}^{37}$

$\underline{e}_7 : \underline{x}^2|\underline{0}^2|\underline{1}^7|\underline{0}^{31}$ $\quad \underline{e}_8 : \underline{x}^2|\underline{0}|\underline{1}|\underline{1}^7|\underline{0}^{31}$ $\quad \underline{e}_9 : \underline{x}^2|\underline{1}^2|\underline{1}^7|\underline{0}^{31}$

$\underline{e}_7' : \underline{x}^2|\underline{0}^2|\underline{0}^7|\underline{1}^{31}$ $\quad \underline{e}_8' : \underline{x}^2|\underline{0}|\underline{1}|\underline{0}^7|\underline{1}^{31}$ $\quad \underline{e}_9' : \underline{x}^2|\underline{1}^2|\underline{0}^7|\underline{1}^{31}$

These can all be added to $\mathcal{D}$.

Remark: in the preceding examples one can of course,in addition,add one vector to $\mathcal{D}$ for each value of w* occuring in $B_1(\underline{y})$.

4.4.Explicit expressions for $|C|$ and $|\mathcal{D}|$.

Below we state the main result of this Chapter:

4.4.1.Theorem. Let $n \in \mathbb{N}$ and let C,D and E be binary codes of length n s.t. there are partitions $C = C^{(0)} \cup C^{(1)}$, $D = D^{(0)} \cup D^{(1)}$ satisfying

(i) $(C, D^{(i)} \cup E)$ is uniquely decodable for $i = 0,1$.

(ii) $(C^{(i)}, D \cup E)$ is uniquely decodable for $i = 0,1$.

(iii) $(C^{(0)}, D^{(0)}) \perp (C^{(1)}, D^{(1)})$.

(56) (iv) There is a bijective mapping $\phi: D^{(0)} \to D^{(1)}$ such that

$$\forall_{\underline{d} \in D^{(0)}} \forall_{\underline{d}' \in D^{(1)}} [(\exists_{\underline{c},\underline{c}' \in C}: \underline{c} + \underline{d} = \underline{c}' + \underline{d}') \Leftrightarrow \underline{d}' = \phi(\underline{d})] .$$

(v) $D \cap E = \phi$, $C^{(0)} \neq \phi$, $C^{(1)} \neq \phi$, $D^{(0)} \neq \phi$.

Let $q, w, r \in \mathbb{N}$ s.t. $0 \leq r < w$, $w \geq 2$, $q \geq 2$ and define $s := qw + r$, $N := sn$;

(73) $$Z := \{ \underline{z} \in \mathbb{F}_2^s \mid w_H(\underline{z}) \equiv 0 \mod w \} ,$$

(58) $$C := \{ \underline{c} = (\underline{c}_1, \ldots, \underline{c}_s) \in C^s \mid \exists_{\underline{z} \in Z} \forall_i : \underline{c}_i \in C^{(z_i)} \} .$$

Let $x := |D^{(0)}| / |D^{(0)} \cup E|$, $y := |C^{(0)}| / |C|$ and $\delta := \max\{ r, w - r \}$ .Then

(i) C is a code of length N and size

(92) $$|C| = \sum_{k=0}^{q} \binom{s}{kw} |C^{(0)}|^{s-kw} . |C^{(1)}|^{kw} = |C|^s . \sum_{k=0}^{q} \binom{s}{kw} y^{s-kw} (1-y)^{kw} .$$

(ii) There is a code $\mathcal{D}$ such that $(C,\mathcal{D})$ is uniquely decodable and optimal w.r.t. $(D \cup E)^s$ of length N and size

$$(93) \qquad |\mathcal{D}| = |D^{(0)} \cup E|^s . \Big(w - \sum_{i=0}^{w-2} \binom{s}{i}(w-i-1)\, x^i (1-x)^{s-i} + \sum_{i=0}^{w-\delta-2} \binom{s}{i}(w-2-2i)\, x^{s-i}(1-x)^i + \sum_{i=w-\delta-1}^{\delta-2} \binom{s}{i}(\delta-1-i)\, x^{s-i}(1-x)^i \Big) .$$

Proof. Relation (92) follows from (60) and the definition of Z.

Application of Theorem (3.4.7), Corollary (4.3.7) and a straightforward calculation, using

$$\sum_{\underline{y} \in (D^{(0)} \cup E)^s} M_Z(\underline{y}) = |D^{(0)} \cup E|^s . w + \sum_{\underline{y} \in (D^{(0)} \cup E)^s} (M_Z(\underline{y}) - w)$$

yields (93). In the second term of (93) we have substituted $i = s - |W(\underline{y})|$ and in the third and fourth terms $i = |W(\underline{y})|$. □

4.4.2. Remarks. (i) The Theorem only states the existence of $\mathcal{D}$. However, it should be clear from this Chapter that we have given an explicit construction for $\mathcal{D}$.

(ii) For $q = 1$ the problem of finding $M_Z(\underline{y})$ is different. It is easy to show that in this case no result like (4.3.2(i)) is obtainable in general for any number of vectors $\underline{e}^{(1)}, \underline{e}^{(2)}, \ldots, \underline{e}^{(t)}$.

A generalization of (4.4.1) according to (3.4.8)(iii) leads to :

4.4.3. Theorem. Let $q, w, r \in \mathbb{N}$ s.t. $0 \le r < w$, $w \ge 2$, $q \ge 2$ and define

$s := qw + r$ .For $i = 1,2,\ldots,s$ let $n_i \in \mathbb{N}$ and let C_i , D_i , E_i be codes as in (56). Let $N := \sum_{i=1}^{s} n_i$ .Define

$$Z := \{ \underline{z} \in \mathbb{F}_2^s \mid w_H(\underline{z}) \equiv 0 \ \underline{\mathrm{mod}}\ w \} \quad \text{and}$$

$$C := \{ \underline{c} = (\underline{c}_1,\ldots,\underline{c}_s) \in \prod_{i=1}^{s} C_i \mid \exists_{\underline{z} \in Z} \ \forall_{i \in \{1,\ldots,s\}} : \ \underline{c}_i \in C_i^{(z_i)} \} \ .$$

For $i = 1,2,\ldots,s$ let $x_i := |D_i^{(0)}| \ / \ |D_i^{(0)} \cup E_i|$ $y_i := |C_i^{(0)}| \ / \ |C_i|$ .Finally let $\delta := \max \{ r, w - r \}$ .Then we have

(i) C is a code of length N and size

$$(94) \qquad |C| = \prod_{i=1}^{s} |C_i| . \sum_{k=0}^{q} \sum_{1 \le i_1 < \ldots < i_{kw} \le s} \ \prod_{i \notin \{i_1,\ldots,i_{kw}\}} y_i \ \prod_{i \in \{i_1,\ldots,i_{kw}\}} (1-y_i)$$

(ii) There is a code $\mathcal{D}$ such that $(C,\mathcal{D})$ is u.d. and optimal w.r.t. $\prod_{i=1}^{s}(D_i \cup E_i)$ of length N and size

$$(95) \qquad |\mathcal{D}| = \prod_{i=1}^{s} |D_i^{(0)} \cup E_i| . (w - T_1 + T_2 + T_3) \ , \text{where}$$

$$T_1 = \sum_{k=0}^{w-2} (w-k-1) \sum_{1 \le i_1 < \ldots < i_k \le s} \ \prod_{i \in \{i_1,\ldots,i_k\}} x_i \ \prod_{i \notin \{i_1,\ldots,i_k\}} (1-x_i) \ ,$$

$$T_2 = \sum_{k=0}^{w-\delta-2} (w-2k-2) \sum_{1 \le i_i < \ldots < i_k \le s} \ \prod_{i \notin \{i_1,\ldots,i_k\}} x_i \ \prod_{i \in \{i_1,\ldots,i_k\}} (1-x_i) \ ,$$

$$T_3 = \sum_{k=w-\delta-1}^{\delta-2} (\delta-1-k) \sum_{1 \le i_1 < \ldots < i_k \le s} \ \prod_{i \notin \{i_1,\ldots,i_k\}} x_i \ \prod_{i \in \{i_1,\ldots,i_k\}} (1-x_i) \ .$$

Here terms with $k < 0$ vanish.The proof is omitted.

Results are presented in Chapter 6.

Chapter 5.The construction yields new basic codes.

5.1.Abstract.

The construction described in Chapters 3 and 4 makes use of the codes C, D and E from (56).In this Chapter we will show that the codepairs $(C,\mathcal{D})$ obtained from the construction can be extended to codepairs $(C, F \cup E)$ satisfying (56) where C, F and E take the place of C,D and E respectively.(We use F in order to avoid ambiguity.)This enables us to "iterate" the construction.As we will see in Chapter 6 we obtain another improvement of the ratepairs in this way.

Section 5.2. gives an explanation of the idea.In section 5.3. we define the codes C, F and E and observe that four of the properties in (56) are satisfied by these codes.In section 5.4. it is shown that the fifth property is also satisfied if we make a special choice for $\mathcal{D}$.Sections 5.5. and 5.6. give explicit constructions for $(C, F \cup E)$ and explicit expressions for the sizes of these codes.

5.2.A brief introduction.

In this section we shall explain the idea which leads to the extension of the pair $(C,\mathcal{D})$ to a codepair $(C, F \cup E)$ satisfying (56).The reader should realize that the following is a simplification of the actual situation.

We turn back again to our "almost u.d." codepair $(C = C^{(0)} \cup C^{(1)}, D = D^{(0)} \cup D^{(1)})$ from sections 3.2. and 4.2..So we assume (C,D) to satisfy

$$(37) \qquad \forall_{\underline{c},\underline{c}' \in C \mid \underline{c} \neq \underline{c}'} \; \forall_{\underline{d},\underline{d}' \in D} \; [\, \underline{c}+\underline{d} = \underline{c}'+\underline{d}' \Rightarrow (\text{either } (\underline{c},\underline{d}) \in C^{(0)} \times D^{(1)} \wedge (\underline{c}',\underline{d}') \in C^{(1)} \times D^{(0)} \text{ or } (\underline{c}',\underline{d}') \in C^{(0)} \times D^{(1)} \wedge (\underline{c},\underline{d}) \in C^{(1)} \times D^{(0)}.) \,] \,,$$

and there is a bijective mapping $\phi: D^{(0)} \to D^{(1)}$ such that

$$(51) \qquad \forall_{\underline{d} \in D^{(0)}} \forall_{\underline{d}' \in D^{(1)}} [(\exists_{\underline{c},\underline{c}' \in C} : \underline{c} + \underline{d} = \underline{c}' + \underline{d}') \Leftrightarrow \underline{d}' = \phi(\underline{d})]$$

As in §4.2. we define

$$(96) \qquad \begin{aligned} C &:= \{ \underline{c} = (\underline{c}_1, .., \underline{c}_s) \in C^s \mid \exists_{\underline{p} \in P} \forall_i : \underline{c}_i \in C^{(p_i)} \} , \\ \mathcal{D} &:= \{ \underline{d} = (\underline{d}_1, .., \underline{d}_s) \in D^s \mid \exists_{\underline{q} \in Q} \forall_i : \underline{d}_i \in D^{(q_i)} \} , \end{aligned}$$

where (P,Q) is a u.d. codepair of length s .Note that it is clear from Lemma (2.3.1) that $(P, Q \oplus \underline{1})$ is u.d..Hence with the definition

$$(97) \qquad \mathcal{D}' := \{ \underline{d} = (\underline{d}_1, .., \underline{d}_s) \in D^s \mid \exists_{\underline{q} \in Q \oplus \underline{1}} \forall_i : \underline{d}_i \in D^{(q_i)} \}$$

we have found another u.d. codepair $(C, \mathcal{D}')$ .Now for simplicity we shall assume that $\forall_{\underline{q} \in Q} : q_s = 0$.

So,for any $\underline{d} = (\underline{d}_1, \ldots, \underline{d}_s) \in \mathcal{D}$, $\underline{d}' = (\underline{d}'_1, \ldots, \underline{d}'_s) \in \mathcal{D}'$ we have that $\underline{d}_s \in D^{(0)}$ and $\underline{d}'_s \in D^{(1)}$.But this and (37) imply that we can only have $\underline{c} + \underline{d}_s = \underline{c}' + \underline{d}'_s$, $\underline{c},\underline{c}'$ in C if $\underline{c} \in C^{(1)}$ and $\underline{c}' \in C^{(0)}$ (*) .

So if we define

$$(98) \qquad C^{(i)} := \{ \underline{c} = (\underline{c}_1, \ldots, \underline{c}_s) \in C \mid \underline{c}_s \in C^{(i)} \} \quad , \; i = 0,1$$

we see that it is proved in (*) that for all $\underline{d} \in \mathcal{D}$, $\underline{d}' \in \mathcal{D}'$:

$$(99) \qquad \forall_{\underline{c} \in C} \forall_{\underline{c}' \in C} [\underline{c} + \underline{d} = \underline{c}' + \underline{d}' \Rightarrow \underline{c} \in C^{(1)} \text{ and } \underline{c}' \in C^{(0)} .]$$

Now suppose that $\underline{c} + \underline{d} = \underline{c}' + \underline{d}'$, where $\underline{c},\underline{c}' \in C$, $\underline{c} \neq \underline{c}'$ and $\underline{d},\underline{d}' \in \mathcal{D} \cup \mathcal{D}'$. Since both $(C,\mathcal{D})$ and $(C,\mathcal{D}')$ are u.d. it is clear that we must have $\underline{d} \in \mathcal{D}$, $\underline{d}' \in \mathcal{D}'$ or the other way around.Combining this with (99) we obtain that for all $\underline{d},\underline{d}' \in \mathcal{D} \cup \mathcal{D}'$:

(100) $\forall_{\underline{c},\underline{c}' \in C \mid \underline{c} \neq \underline{c}'} [\ \underline{c}+\underline{d} = \underline{c}'+\underline{d}' \Rightarrow$ either $(\underline{c},\underline{d}) \in C^{(0)} \times \mathcal{D}' \wedge (\underline{c}',\underline{d}') \in C^{(1)} \times$
or $(\underline{c}',\underline{d}') \in C^{(0)} \times \mathcal{D}' \wedge (\underline{c},\underline{d}) \in C^{(1)} \times \mathcal{D}$

So with the definitions $F^{(0)} := \mathcal{D}$, $F^{(1)} := \mathcal{D}'$, $F := F^{(0)} \cup F^{(1)}$ we have that $(C = C^{(0)} \cup C^{(1)}, F = F^{(0)} \cup F^{(1)})$ is a codepair as in (37) where C and F take the place of C and D respectively.

Of course we do <u>not</u> have (51) so far.In order to prove (51) one should make special requirements on the codepair (P,Q) .In the above terminology it would be sufficient to require that for all $\underline{q} \in Q$ there exists exactly one $\underline{q}' \in Q \oplus \underline{1}$ such that $\underline{p}+\underline{q} = \underline{p}'+\underline{q}'$ for some $\underline{p},\underline{p}' \in P$ .Indeed,in that case the converse is also true and one can easily derive (51).However,we will not deal with this detail here since in the actual situation as described later in this Chapter the requirements are entirely different.

The idea presented above shall be developed more precisely in the following sections for the codepair $(C,\mathcal{D})$ from Chapter 3 ,where we shall make the special choice for Z as described in Chapter 4.So there shall be two extra complication namely the fact that the codes E and $\bar{E}$ are involved and the fact that we wish to prove (51) for the new codepair $(C , F \cup E)$.

5.3.Definitions.A first observation.

In this section we define the codepair $(C , F \cup E)$ based on the pair $(C,\mathcal{D})$ (as described in Chapters 3 and 4) and on certain sets $G(\underline{y}) \subset A(\underline{y}) \cap \mathcal{D}$ which satisfy the properties presented in (5.3.1) below.Next we show that the pair $(C , F \cup E)$ satisfies (56)(i)-(iii),(v) but not necessarily (56)(iv) .We will first give all definitions.

5.3.1.Definitions. In this Chapter we adopt all definitions from (4.2.1) and (4.3.4). Moreover we shall choose Z as in (4.2.2) and define $\delta := \max\{ r , w - r \}$. We assume that $\mathcal{D} \subset (D \cup E)^s$ such that $(C,\mathcal{D})$ is u.d..

Define the mapping ψ on $(D \cup E)^s$ by

$$(101) \qquad \psi((\underline{d}_1,\ldots,\underline{d}_s)) := (\underline{e}_1,\ldots,\underline{e}_s) \quad \text{with} \quad \underline{e}_i = \begin{cases} \underline{d}_i & \text{if } \underline{d}_i \in E \ , \\ \phi(\underline{d}_i) & \text{if } \underline{d}_i \in D^{(0)} \ , \\ \phi^{\leftarrow}(\underline{d}_i) & \text{if } \underline{d}_i \in D^{(1)} \ . \end{cases}$$

For any $V \subset (D \cup E)^s$ we shall denote the set $\{ \psi(\underline{d}) \mid \underline{d} \in V \}$ by $\psi(V)$.

Now for each $\underline{y} \in (D^{(0)} \cup E)^s$ let $G(\underline{y})$ be a subset of $A(\underline{y}) \cap \mathcal{D}$ with the following properties:

$$(G1) \quad \forall_{\underline{d} = (\underline{d}_1,\ldots,\underline{d}_s) \in G(\underline{y})} : \underline{d}_s \in D^{(0)} \ ,$$

$$(102) \qquad (G2) \quad \{w^*(\underline{d}) \mid \underline{d} \in G(\underline{y}) \} = \{ w^*(\underline{e}) \mid \underline{e} \in \psi(G(\underline{y})) \} \ ,$$

(G3) If $|W(\underline{y})| \leq \delta - 2$ and $\underline{d},\underline{d}' \in A(\underline{y}) \cap \mathcal{D}$ such that $w^*(\underline{d}) = w^*(\underline{d}') \in \in B_2(\underline{y})$ then either $\{\underline{d},\underline{d}'\} \cap G(\underline{y}) = \emptyset$ or $\{\underline{d},\underline{d}'\} \subset G(\underline{y})$.

(Remark.Such sets exist since we may choose $G(\underline{y}) = \emptyset$ for each $\underline{y}$ .However,we wish to choose $G(\underline{y})$ as large as possible.)

Now define the codepair $(C , F \cup E)$ as follows:

$$C^{(i)} := \{ \underline{c} = (\underline{c}_1,\ldots,\underline{c}_s) \in C \mid \underline{c}_s \in C^{(i)} \} \ , \ i = 0,1$$

$$(103) \qquad F^{(0)} := \bigcup_{\underline{y} \in (D^{(0)} \cup E)^s} G(\underline{y}) \ ; \ F^{(1)} := \bigcup_{\underline{y} \in (D^{(0)} \cup E)^s} \psi(G(\underline{y})) \ ;$$

$F := F^{(0)} \cup F^{(1)}$ and $E := \mathcal{D} \setminus F^{(0)}$. (Note that $F^{(0)} \subset \mathcal{D}$.)

Now we have the following result.

5.3.2.Lemma.With the above definitions the system $(C, F \cup E)$ satisfies the conditions (56)(i),(ii) and (iii).Moreover if there is a $\underline{y} \in (D^{(0)} \cup E)^s$ s.t. $G(\underline{y}) \neq \emptyset$,(56)(v) holds.The system does not necessarily satisfy (56)(iv).

Remark. C,F and E take the place of C,D and E respectively.

Proof. We first note the following:

(104)

(a) $\underline{d} \in A(\underline{y}) \Leftrightarrow \psi(\underline{d}) \in A(\underline{y})$.

(b) If $\underline{d},\underline{d}' \in A(\underline{y})$ for some $\underline{y}$: $w^*(\underline{d}) = w^*(\underline{d}') \Leftrightarrow w^*(\psi(\underline{d})) = w^*(\psi(\underline{d}'))$

(c) $a_{10}(\underline{d},\underline{d}') = a_{10}(\psi(\underline{d}'),\psi(\underline{d}))$ and $a_{01}(\underline{d},\underline{d}') = a_{01}(\psi(\underline{d}'),\psi(\underline{d}))$.

(d) By (G1) ,for any $\underline{f} = (\underline{f}_1,\ldots,\underline{f}_s) \in F^{(0)}$ we have $\underline{f}_s \in D^{(0)}$. From this and the definitions of ψ and $F^{(1)}$ it follows that for any $\underline{f} = (\underline{f}_1,\ldots,\underline{f}_s) \in F^{(1)}$: $\underline{f}_s \in D^{(1)}$.

$C = C^{(0)} \cup C^{(1)}$ is a partition.Hence we see from the definitions that $C = C^{(0)} \cup C^{(1)}$ is a partition.Similarly,since $D = D^{(0)} \cup D^{(1)}$ is a partition we see from (104)(d) that $F = F^{(0)} \cup F^{(1)}$ also is.

Since $(C,\mathcal{D})$ is u.d. we see that (56)(i) holds for $i = 0$. (*)

Now suppose $\exists_{\underline{c},\underline{c}' \in C} \exists_{\underline{f},\underline{f}' \in F^{(1)} \cup E} [\, \underline{f} \neq \underline{f}' \wedge \underline{c} + \underline{f} = \underline{c}' + \underline{f}' \,]$ .It follows from (*) that $\{\underline{f},\underline{f}'\} \not\subset E$.

Moreover,(3.3.3) implies that $\underline{f},\underline{f}' \in A(\underline{y})$ for some $\underline{y}$,and (4.2.3) implies that $w^*(\underline{f}) = w^*(\underline{f}')$. Hence w.l.o.g. one of the following holds:

(I) $\exists_{\underline{y}} [\, \underline{f} \in A(\underline{y}) \cap E \wedge \underline{f}' \in A(\underline{y}) \cap F^{(1)} \wedge w^*(\underline{f}) = w^*(\underline{f}') \,]$,or

(II) $\exists_{\underline{y}} [\, \underline{f},\underline{f}' \in A(\underline{y}) \cap F^{(1)} \wedge w^*(\underline{f}) = w^*(\underline{f}') \,]$.

Consider case (I).Obviously $\underline{f}' \in \psi(G(\underline{y}))$. So we conclude from (G2) that there is some $\underline{f}'' \in G(\underline{y})$ s.t. $w^*(\underline{f}') = w^*(\underline{f}'')$. It follows that $w^*(\underline{f}) = w^*(\underline{f}'')$. Since $\underline{f} \in E = \mathcal{D} \setminus F^{(0)}$ and $\underline{f}'' \in G(\underline{y}) \subset F^{(0)}$ we have $\underline{f} \neq \underline{f}''$ and,from (G3), $w^*(\underline{f}) \notin B_2(\underline{y})$

if $|W(\underline{y})| \leq \delta - 2$. So (4.3.2(ii)) and (4.3.5) imply that $(C,\{\underline{f},\underline{f}''\})$ is not u.d. contradicting (*) .

Now consider case (II) . Here $\underline{f},\underline{f}' \in \psi(G(\underline{y}))$. Hence there are $\underline{d},\underline{d}' \in G(\underline{y})$ s.t. $\underline{f} = \psi(\underline{d})$ and $\underline{f}' = \psi(\underline{d}')$. Now (104)(b) implies that $w^*(\underline{d}) = w^*(\underline{d}')$ .Application of (104)(c) and (4.2.4) yields $(C,\{\underline{d},\underline{d}'\})$ is u.d. $\Leftrightarrow$ $(C,\{\underline{f},\underline{f}'\})$ is u.d. . Here both sides are correct according to (*) .

The above shows (56)(i) for $i = 1$.

Next consider (56)(ii).Suppose $\exists_{\underline{c},\underline{c}' \in C^{(i)}} \exists_{\underline{f},\underline{f}' \in F \cup E} [\, \underline{c} + \underline{f} = \underline{c}' + \underline{f}' \,]$ for $i = 0$ or $i = 1$.

Since (56)(i) holds for $(C , F \cup E)$ we have that,w.l.o.g. , $\underline{f} \in F^{(0)}$, $\underline{f}' \in F^{(1)}$. So from (104)(d) we find that $\underline{f}_s \neq \underline{f}'_s$ .By assumption we have $\underline{c}_s,\underline{c}'_s \in C^{(i)}$ and $\underline{c}_s + \underline{f}_s = \underline{c}'_s + \underline{f}'_s$ .These propositions disagree with the fact that $(C^{(i)},D \cup E)$ is u.d. ((56)(ii) for $(C,D \cup E)$) .This proves (56)(ii).

Now consider (56)(iii).Assume

$\exists_{\underline{c} \in C^{(0)}} \exists_{\underline{c}' \in C^{(1)}} \exists_{\underline{f} \in F^{(0)}} \exists_{\underline{f}' \in F^{(1)}} [\, \underline{c} + \underline{f} = \underline{c}' + \underline{f}' \,]$.

In particular, $\underline{c}_s + \underline{f}_s = \underline{c}'_s + \underline{f}'_s$ .Here we have $\underline{c}_s \in C^{(0)}$, $\underline{c}'_s \in C^{(1)}$ by assumption and $\underline{f}_s \in D^{(0)}$, $\underline{f}'_s \in D^{(1)}$ from (104)(d).But these propositions disagree with (56)(iii) holding for $(C,D \cup E)$.This proves (56)(iii).

Finally,we have $F^{(0)} \cap E = \phi$; since $q \geq 2$ we have $C^{(0)} \neq \phi$ and $C^{(1)} \neq \phi$ .The restriction $\exists_{\underline{y}} : G(\underline{y}) \neq \phi$ guarantees that $F^{(0)} \neq \phi$ .Now assume $\underline{f} \in F^{(1)} \cap E$. Find $\underline{y}$ in $(D^{(0)} \cup E)^s$ s.t. $\underline{f} \in \psi(G(\underline{y}))$. By (G2) we can find a vector $\underline{e} \in G(\underline{y})$ s.t. $w^*(\underline{e}) = w^*(\underline{f})$ .Since $\underline{f} \in E$ we have $\underline{f} \neq \underline{e}$ .Hence $w^*(\underline{f}) \in B_2(\underline{y})$ or else $(C,F^{(0)} \cup E)$ would not be u.d..Moreover $\underline{f} \notin G(\underline{y})$ from (104)(d).But $\underline{e} \in G(\underline{y})$, $\underline{f} \notin G(\underline{y})$, $w^*(\underline{e}) = w^*(\underline{f}) \in B_2(\underline{y})$ violate (G3).So $F^{(1)} \cap E = \phi$ and the lemma is proved. □

5.3.3.Examples.Below we have $C=\{\underline{0}\}$, $D=\{\underline{1}\}$, $E=\{\underline{x}\}$ of length n as in (4.3.8). Again the subscript of the vectors below equals their w*-value.

(i) $q = 3$ $\underline{y} = \underline{x}^2|\underline{0}^{40}$ (These parameters are the same as in (4.3.8(iii)).)
$w = 12$
$r = 6$ $|W(\underline{y})| = 2$ Suppose $A(\underline{y}) \cap \mathcal{D} = \bigcup_{i=1}^{7} A_i$,where
$\delta = 6$
$s = 42$
$A_1 = \{\underline{d}_1, \underline{d}_1', \underline{d}_3, \underline{d}_3'\}$, $A_2 = \{\underline{d}_2, \underline{d}_2'\}$, $A_3 = \{\underline{e}_7, \underline{e}_7', \underline{e}_9, \underline{e}_9'\}$,
$A_4 = \{\underline{e}_8, \underline{e}_8'\}$, $A_5 = \{\underline{f}_0, \underline{f}_4\}$, $A_6 = \{\underline{f}_5, \underline{f}_{11}\}$, $A_7 = \{\underline{f}_6, \underline{f}_{10}\}$

Here $\underline{d}_i, \underline{d}_i', \underline{e}_i, \underline{e}_i'$ are as in (4.3.8(iii)) and the other vectors are given by:

$\underline{f}_0 : \underline{x}^2|\underline{1}^{36}|\underline{0}^4$ $\underline{f}_5 : \underline{x}^2|\underline{1}^5|\underline{0}^{35}$ $\underline{f}_6 : \underline{x}^2|\underline{1}^6|\underline{0}^{34}$
$\underline{f}_4 : \underline{x}^2|\underline{1}^{40}$ $\underline{f}_{11} : \underline{x}^2|\underline{0}^{29}|\underline{1}^{11}$ $\underline{f}_{10} : \underline{x}^2|\underline{1}^{10}|\underline{0}^{30}$

Note that (by (G2) and (G3)) $G(\underline{y})$ must be the union of some of the A_i.Of these only A_7 can be included by (G1) . So with this choice we have $G(\underline{y}) \subset \{\phi, \{\underline{f}_6, \underline{f}_{10}\}\}$.

(ii) Now suppose that $A(\underline{y}) \cap \mathcal{D}$ consists of the following vectors: (parameters as above)

$\underline{d}_1 : x^2|\underline{1}|\underline{0}^{37}|\underline{0}^2$ $\underline{d}_2 : \underline{x}^2|\underline{1}|\underline{0}^{37}|\underline{1}|\underline{0}$ $\underline{d}_3 : \underline{x}^2|\underline{1}|\underline{0}^{37}|\underline{1}^2$
$\underline{d}_1' : x^2|\underline{0}|\underline{1}^{37}|\underline{0}^2$ $\underline{d}_2' : \underline{x}^2|\underline{0}|\underline{1}^{37}|\underline{1}|\underline{0}$ $\underline{d}_3' : \underline{x}^2|\underline{0}|\underline{1}^{37}|\underline{1}^2$

$\underline{e}_7 : x^2|\underline{1}^7|\underline{0}^{31}|\underline{0}^2$ $\underline{e}_8 : \underline{x}^2|\underline{1}^7|\underline{0}^{31}|\underline{1}|\underline{0}$ $\underline{e}_9 : \underline{x}^2|\underline{1}^7|\underline{0}^{31}|\underline{1}^2$
$\underline{e}_7' : x^2|\underline{0}^7|\underline{1}^{31}|\underline{0}^2$ $\underline{e}_8' : \underline{x}^2|\underline{0}^7|\underline{1}^{31}|\underline{1}|\underline{0}$ $\underline{e}_9' : \underline{x}^2|\underline{0}^7|\underline{1}^{31}|\underline{1}^2$

$\underline{f}_0 : x^2|\underline{0}^{40}$ $\underline{f}_5 : \underline{x}^2|\underline{1}^5|\underline{0}^{35}$ $\underline{f}_6 : \underline{x}^2|\underline{1}^6|\underline{0}^{34}$
$\underline{f}_4 : x^2|\underline{1}^4|\underline{0}^{36}$ $\underline{f}_{11} : \underline{x}^2|\underline{1}^{11}|\underline{0}^{29}$ $\underline{f}_{10} : \underline{x}^2|\underline{1}^{10}|\underline{0}^{30}$

Now we may take $G(\underline{y}) = \{\underline{d}_2, \underline{d}_2', \underline{e}_8, \underline{e}_8', \underline{f}_0, \underline{f}_4, \underline{f}_5, \underline{f}_6, \underline{f}_{10}, \underline{f}_{11}\}$,while none of the remaining 8 vectors can be included.

(iii) If,in (i), we define $\underline{y}' = \underline{0}^{40}|\underline{x}^2$ we see that $G(\underline{y}') = \phi$ whatever $A(\underline{y}') \cap \mathcal{D}$ may be.

5.4.We need more to prove the failing property.

In this section we show that (56)(iv) is satisfied if we make special requirements on the code $\mathcal{D}$.These requirements,which are given in (5.4.4),do not affect the size but only the structure of $\mathcal{D}$.We shall need two more lemmas.

5.4.1.Lemma.Let all definitions be as in (5.3.1).Moreover,assume that $(C,\mathcal{D})$ is optimal w.r.t. $(D \cup E)^s$. Then we have for all $\underline{y} \in (D^{(0)} \cup E)^s$ s.t. $|W(\underline{y})| \leq \delta - 2$

(i) If $k \in B_1(\underline{y}) \cap \{ w^*(\underline{d}) \mid \underline{d} \in G(\underline{y}) \}$ there is exactly one vector $\underline{d} \in \psi(G(\underline{y}))$ such that $w^*(\underline{d}) = k$.

(ii) If $k \in B_2(\underline{y}) \cap \{ w^*(\underline{d}) \mid \underline{d} \in G(\underline{y}) \}$ there are exactly two vectors $\underline{d},\underline{d}' \in \psi(G(\underline{y}))$ such that $w^*(\underline{d}) = w^*(\underline{d}') = k$.

Proof.Fix $\underline{y} \in (D^{(0)} \cup E)^s$ such that $|W(\underline{y})| \leq \delta - 2$ .Define the mapping χ on $\{0,1,\ldots,w-1\}$ by:

$$\chi(k) := (s - |W(\underline{y})| - k) \bmod w .$$

Note that

(a) $\chi(w^*(\underline{d})) = w^*(\psi(\underline{d}))$ for $\underline{d} \in A(\underline{y})$

(b) $\chi(k) = \chi(\ell) \Leftrightarrow k = \ell$

Now let $k \in B_2(\underline{y}) \cap \{ w^*(\underline{d}) \mid \underline{d} \in G(\underline{y}) \}$ .Since $(C,\mathcal{D})$ is optimal w.r.t. $(D \cup E)^s$ there are exactly two vectors $\underline{e},\underline{e}' \in A(\underline{y}) \cap \mathcal{D}$ s.t. $w^*(\underline{e}) = w^*(\underline{e}') = k$ .Moreover, from (G3) we have that $\underline{e},\underline{e}' \in G(\underline{y})$ .Now (a) and (b) imply that there are exactly two vectors $\psi(\underline{e})$, $\psi(\underline{e}') \in \psi(G(\underline{y}))$ s.t. $\chi(k) = w^*(\psi(\underline{e})) = w^*(\psi(\underline{e}'))$ .Now note that $(C,F^{(1)})$ is u.d. by (5.3.2).Hence it follows from the above that

(c) $\chi(k) \in B_2(\underline{y}) \cap \{ w^*(\underline{d}) \mid \underline{d} \in \psi(G(\underline{y})) \} \overset{(G2)}{=} B_2(\underline{y}) \cap \{ w^*(\underline{d}) \mid \underline{d} \in G(\underline{y}) \}$.

But (b) and (c) imply (using a simple counting argument) that also $\chi^{\leftarrow}(k) \in B_2(\underline{y}) \cap \{ w^*(\underline{d}) \mid \underline{d} \in G(\underline{y}) \}$ .Hence we can find exactly two vectors $\underline{f},\underline{f}' \in G(\underline{y})$ such that $w^*(\underline{f}) = w^*(\underline{f}') = \chi^{\leftarrow}(k)$ .Now with $\underline{d} := \psi(\underline{f})$, $\underline{d}' := \psi(\underline{f}')$ we have exactly two vectors $\underline{d},\underline{d}' \in \psi(G(\underline{y}))$ for which $w^*(\underline{d}) = w^*(\underline{d}') = \chi(\chi^{\leftarrow}(k)) = k$ .This proves (ii).

In a similar way we may obtain (i).However,this also follows immediately from (G2) , the fact that $(C,F^{(1)})$ is u.d.,and (4.3.5). □

We shall need the following definition.

5.4.2.Definition.For any $\underline{d},\underline{d}' \in (D \cup E)^s$ let $V_{ij}(\underline{d},\underline{d}')$ be defined by

(105) $$V_{ij}(\underline{d},\underline{d}') := \{ k \in \{1,2,\ldots,s\} \mid \underline{d}_k \in D^{(i)} \wedge \underline{d}'_k \in D^{(j)} \} \ , \ i,j = 0,1 \ .$$

5.4.3.Lemma.Let all definitions be as in (5.3.1) and $V_{ij}(\underline{d},\underline{d}')$ as above.Fix $\underline{y} \in (D^{(0)} \cup E)^s$ and assume that the vectors $\underline{e},\underline{e}',\underline{f},\underline{f}' \in A(\underline{y})$ satisfy

(i) $w^*(\underline{e}) = w^*(\underline{e}') = w^*(\underline{f}) = w^*(\underline{f}')$,

(ii) $(C,\{\underline{e},\underline{f}\})$ is u.d. and $(C,\{\underline{e}',\underline{f}'\})$ is u.d. ,

(iii) $V_{10}(\underline{e},\underline{f}) = V_{10}(\underline{e}',\underline{f}')$ and $V_{01}(\underline{e},\underline{f}) = V_{01}(\underline{e}',\underline{f}')$.

Then $(C,\{\underline{e},\underline{f}'\})$ is u.d..

Proof.W.l.o.g. we may assume that $W(\underline{y}) = \{ s - |W(\underline{y})| + 1, s - |W(\underline{y})| + 2, \ldots, s \}$. For any $\underline{d} = (\underline{d}_1,\ldots,\underline{d}_s) \in W(\underline{y})$ define $\underline{q} = \zeta(\underline{d})$ of length $s - |W(\underline{y})|$ by : $q_i := 0$ if $\underline{d}_i \in D^{(0)}$, $q_i := 1$ if $\underline{d}_i \in D^{(1)}$ .Then we have,w.l.o.g. ,

$$\begin{array}{lll}
\zeta(\underline{e}) &= 0\text{---}0,1\text{---}1,1\text{---}1,1\text{---}1,0\text{---}0,0\text{---}0 & a_{10} = a_{10}(\underline{e},\underline{f}) \\
\zeta(\underline{f}) &= 1\text{---}1,0\text{---}0,1\text{---}1,1\text{---}1,0\text{---}0,0\text{---}0 & \\
\zeta(\underline{e}') &= 0\text{---}0,1\text{---}1,1\text{---}1,0\text{---}0,1\text{---}1,0\text{---}0 & a_{01} = a_{01}(\underline{e},\underline{f}) \\
\zeta(\underline{f}') &= 1\text{---}1,0\text{---}0,1\text{---}1,0\text{---}0,1\text{---}1,0\text{---}0 & \\
& \ a_{01} \ \ a_{10} \quad a \quad b \quad c \quad d &
\end{array}$$

We shall abbreviate $\alpha(\underline{e},\underline{f})$ to α and similar for $\beta(\underline{e},\underline{f})$ and $\gamma(\underline{e},\underline{f})$.

It follows from the above that

$$a_{10}(\underline{e},\underline{f}') = a_{10}(\underline{e},\underline{f}) + b = \alpha w + \gamma + b \quad ,$$
$$a_{01}(\underline{e},\underline{f}') = a_{01}(\underline{e},\underline{f}) + c = \beta w + \gamma + c \quad .$$

Since $\{\underline{e},\underline{f}\}$ is <u>not</u> inadmissible we have either $\alpha + \beta = q$, $\gamma \neq 0$ (*)

or $\alpha + \beta = q - 1$, $\gamma > r$ (**) .(cf.(4.3.1).)

From the above,if (*) is the case,it is trivial that the vectors $\underline{e}$ and $\underline{f}'$ satisfy (75)(c) .

Now consider (**).It is clear that $b + c \leq (qw + r) - (\alpha + \beta)w - 2\gamma$ .That is, $b + c \leq w + r - 2\gamma < w$.

Since (i) implies $b \equiv c \ \underline{\text{mod}}\ w$ it follows that $b = c \leq \frac{w+r}{2} - \gamma$.

Hence we obtain

$$\begin{aligned} a_{10}(\underline{e},\underline{f}') &= \alpha w + \gamma' \\ a_{01}(\underline{e},\underline{f}') &= \beta w + \gamma' \end{aligned} \qquad \gamma \leq \gamma' = b + \gamma \leq \frac{w+r}{2} < w \quad .$$

So these numbers satisfy (75)(b).Hence $\{\underline{e},\underline{f}'\}$ is <u>not</u> inadmissible. □

Below we introduce the notion of a "normalized" codepair $(C,\mathcal{D})$ .It shall be shown afterwards that,with the definitions from (5.3.1),a normalized pair $(C,\mathcal{D})$ yields a codepair for which all properties in (56) are satisfied.However,though the requirements below are sufficient for this,the reader should realize that they are not necessary.

<u>5.4.4.Definition.</u>Let $(C,\mathcal{D})$ be a codepair as described in Theorem (4.4.1).We call $(C,\mathcal{D})$ <u>normalized</u> if for all $\underline{y} \in (D^{(0)} \cup E)^s$ such that $|W(\underline{y})| \leq \delta - 2$, $B_2(\underline{y}) = V_1(\underline{y}) \cup V_2(\underline{y})$ as in (4.3.4),the following holds for <u>each</u> pair of vectors

$\underline{d},\underline{d}' \in A(\underline{y}) \cap \mathcal{D}$ s.t. $w^*(\underline{d}) = w^*(\underline{d}') \in B_2(\underline{y})$:

(i) $$\{a_{10}(\underline{d},\underline{d}'),a_{01}(\underline{d},\underline{d}')\} = \{b_{10}(\underline{y}),b_{01}(\underline{y})\} \quad \text{if} \quad w^*(\underline{d}) \in V_1(\underline{y})$$
$$\{a_{10}(\underline{d},\underline{d}'),a_{01}(\underline{d},\underline{d}')\} = \{c_{10}(\underline{y}),c_{01}(\underline{y})\} \quad \text{if} \quad w^*(\underline{d}) \in V_2(\underline{y})$$

where $b_{ij}(\underline{y})$, $c_{ij}(\underline{y})$ are the numbers from (4.3.6) ,and

(ii) The set $\{V_{10}(\underline{d},\underline{d}'),V_{01}(\underline{d},\underline{d}')\}$ is uniquely determined by the value of t such that $w^*(\underline{d}) \in V_t(\underline{y})$, $t \in \{1,2\}$.

5.4.5.Remark.Note that (i) can easily be satisfied by constructing $\mathcal{D}$ according to (4.3.6).Moreover, (i) implies that we can actually construct $\mathcal{D}$ in such a way that (ii) holds.

5.4.6.Example.Let us examine how we should construct $A(\underline{y}) \cap \mathcal{D}$ in the example from (5.3.3).

We may for $\underline{f}_i$ ($i \in \{0,4,5,6,10,11\}$) take any vector such that $w^*(\underline{f}_i) = i$.

Though for instance $\underline{d}_1$: $\underline{x}^2|\underline{0}^2|\underline{1}^{13}|\underline{0}^{25}$ and $\underline{d}_1'$: $\underline{x}^2|\underline{0}^2|\underline{0}^{13}|\underline{1}^{25}$ would do in $A(\underline{y}) \cap \mathcal{D}$ as a pair for which $w^*(\underline{d}_1) = w^*(\underline{d}_1') = 1$,they cannot be included in $\mathcal{D}$ if $(C,\mathcal{D})$ is normalized since this choice violates (5.4.4(i)).

Moreover,we cannot include $\underline{d}_1,\underline{d}_1'$ as in (5.3.3(i)) and $\underline{d}_2,\underline{d}_2'$ as in (5.3.3(ii)) simultaneously,for this would violate (5.4.4(ii)).

However,we may for instance make any of the four choices obtained by taking all $\underline{d}_i,\underline{d}_i'$ either as in (5.3.3(i)) or as in (5.3.3(ii)),and all $\underline{e}_i,\underline{e}_i'$ either as in (5.3.3(i)) or as in (5.3.3(ii)).

Now we state the main result of this section.

5.4.7.Theorem.Let all definitions be as in (5.3.1).Let $(C,\mathcal{D})$ be u.d. and optimal w.r.t. $(D \cup E)^s$ and assume that $(C,\mathcal{D})$ is normalized.Moreover let there be a $\underline{y} \in (D^{(0)} \cup E)^s$ such that $G(\underline{y}) \neq \emptyset$ .Then the system $(C,F \cup E)$ satisfies (56).

Proof.From (5.3.2) the only property left to prove is (56)(v).Note that

(106) $\quad V_{10}(\underline{d},\underline{d}') = V_{10}(\psi(\underline{d}'),\psi(\underline{d}))$ and $V_{01}(\underline{d},\underline{d}') = V_{01}(\psi(\underline{d}'),\psi(\underline{d}))$.

(cf.(104)(c).)We shall first show

(107) $\quad \forall_{\underline{f} \in F^{(0)}} \exists!_{\underline{f}' \in F^{(1)}} [\exists_{\underline{c},\underline{c}' \in C} : \underline{c} + \underline{f} = \underline{c}' + \underline{f}']$.

First fix $\underline{f} \in G(\underline{y})$ with $|W(\underline{y})| > \delta - 2$. Assume that $\underline{c} + \underline{f} = \underline{c}' + \underline{f}'$ for some $\underline{f}' \in F^{(1)}$, $\underline{c},\underline{c}' \in C$ .From (3.3.3) it is clear that $\underline{f}' \in \psi(G(\underline{y}))$.Note that (G2) implies that $w^*(\underline{e}) = w^*(\underline{f})$ for some $\underline{e} \in \psi(G(\underline{y}))$. Moreover (4.3.2(ii)) and the fact that $(C,F^{(1)})$ is u.d. show that this $\underline{e}$ is unique.It follows from (4.2.3) that we must have $\underline{f}' = \underline{e}$ .Indeed $\underline{c} + \underline{f} = \underline{c}' + \underline{e}$ for some $\underline{c},\underline{c}' \in C$.

Next,assume $\underline{f} \in G(\underline{y})$ with $|W(\underline{y})| \leq \delta - 2$ such that $w^*(\underline{f}) \in B_1(\underline{y})$. Proceeding like above,using (5.4.1(i)) and (4.3.5),we find the unique $\underline{f}' \in F^{(1)}$ such that $\underline{c} + \underline{f} = \underline{c}' + \underline{f}'$ for some $\underline{c},\underline{c}' \in C$.

Finally let $\underline{f} \in G(\underline{y})$, $|W(\underline{y})| \leq \delta - 2$, $w^*(\underline{f}) \in B_2(\underline{y})$ .From (G3) we see that we can find some $\underline{e} \in G(\underline{y})$, $\underline{e} \neq \underline{f}$, such that $w^*(\underline{e}) = w^*(\underline{f})$.

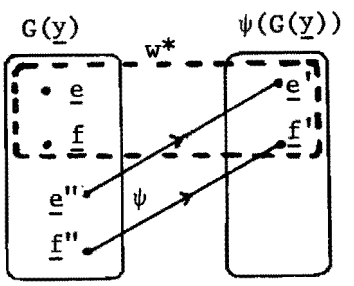


fig.10.

It follows from (5.4.1(ii)) that there are exactly two different vectors $\underline{e}',\underline{f}' \in \psi(G(\underline{y}))$ s.t. $w^*(\underline{e}') = w^*(\underline{f}') = w^*(\underline{f})$ .As above,these are the only candidates for a vector $\underline{d} \in F^{(1)}$ s.t. $\exists_{\underline{c},\underline{c}' \in C} : \underline{c} + \underline{f} = \underline{c}' + \underline{d}$.

Now find $\underline{e}'',\underline{f}'' \in G(\underline{y})$ such that $\underline{e}' = \psi(\underline{e}'')$ and $\underline{f}' = \psi(\underline{f}'')$.

Since $\underline{e},\underline{f},\underline{e}'',\underline{f}'' \in \mathcal{D}$ it follows from (5.4.4(i)) that

(108)
$$\text{either} \quad \{a_{10}(\underline{e},\underline{f}),a_{01}(\underline{e},\underline{f})\} = \{b_{10}(\underline{y}),b_{01}(\underline{y})\} \qquad (a)$$
$$\text{or} \quad \{a_{10}(\underline{e},\underline{f}),a_{01}(\underline{e},\underline{f})\} = \{c_{10}(\underline{y}),c_{01}(\underline{y})\} \qquad (b)$$

and

(109)
$$\text{either} \quad \{a_{10}(\underline{e}'',\underline{f}''),a_{01}(\underline{e}'',\underline{f}'')\} = \{b_{10}(\underline{y}),b_{01}(\underline{y})\} \qquad (c)$$
$$\text{or} \quad \{a_{10}(\underline{e}'',\underline{f}''),a_{01}(\underline{e}'',\underline{f}'')\} = \{c_{10}(\underline{y}),c_{01}(\underline{y})\} \qquad (d)$$

From (106) we have

(110) $$V_{10}(\underline{e}'',\underline{f}'') = V_{10}(\underline{f}',\underline{e}') \quad \text{and} \quad V_{01}(\underline{e}'',\underline{f}'') = V_{01}(\underline{f}',\underline{e}') \ .$$

Hence (109) holds for $(\underline{e}',\underline{f}')$ as well,and since $w^*(\underline{e}) = w^*(\underline{f}) = w^*(\underline{e}') = w^*(\underline{f}')$ we see from (4.3.6(iii)) that in (108),(109) we have either (a) and (c) or (b) and (d).Hence,again from (4.3.6(iii)) we find that either $\{w^*(\underline{e}),w^*(\underline{e}'')\} \subset V_1(\underline{y})$ or $\{w^*(\underline{e}),w^*(\underline{e}'')\} \subset V_2(\underline{y})$ .So from (5.4.4(ii)) we have

$$\{V_{10}(\underline{e},\underline{f}),V_{01}(\underline{e},\underline{f})\} = \{V_{10}(\underline{e}'',\underline{f}''),V_{01}(\underline{e}'',\underline{f}'')\} \ .$$

Hence,using (110) we may assume w.l.o.g. that

$$V_{10}(\underline{e},\underline{f}) = V_{10}(\underline{e}',\underline{f}') \quad \text{and} \quad V_{01}(\underline{e},\underline{f}) = V_{01}(\underline{e}',\underline{f}') \ .$$

So we have (5.4.3(i),(iii)),and since $\{\underline{e},\underline{f}\} \subset F^{(0)}$ and $\{\underline{e}',\underline{f}'\} \subset F^{(1)}$ also (5.4.3(ii)) is satisfied.Now application of that Lemma shows that $(C,\{\underline{e},\underline{f}'\})$ and $(C,\{\underline{e}',\underline{f}\})$ are u.d..Since $(C,\{\underline{e},\underline{f}\})$ is u.d. as well it follows from (4.3.2(i)) (for the triple $\{\underline{e},\underline{f},\underline{f}'\}$) that $\exists_{\underline{c},\underline{c}' \in C} : \underline{c}+\underline{f} = \underline{c}'+\underline{f}'$.
As mentioned before, $\underline{e}'$ and $\underline{f}'$ are the only candidates for a vector $\underline{d} \in F^{(1)}$ s.t. $(C,\{\underline{f},\underline{d}\})$ is <u>not</u> u.d..So the above shows that $\underline{f}'$ is the unique vector with this property.

This proves (107).The only proposition left to prove is

(111) $\quad \forall_{\underline{f}' \in F^{(1)}} \exists!_{\underline{f} \in F^{(0)}} [\, \exists_{\underline{c},\underline{c}' \in C} : \underline{c}+\underline{f} = \underline{c}'+\underline{f}' \,]$.

The proof of (111) is omitted,since it can be obtained from that of (107) by interchanging $F^{(0)}$ and $F^{(1)}$ resp. $G(\underline{y})$ and $\psi(G(\underline{y}))$ and adapting of some details. (In the case that $\underline{e},\underline{f} \in \psi(G(\underline{y}))$, $w^*(\underline{e}) = w^*(\underline{f})$ choose $\underline{e}',\underline{f}',\underline{e}'',\underline{f}'' \in G(\underline{y})$ such that $w^*(\underline{e}') = w^*(\underline{f}') = w^*(\underline{e}) = w^*(\underline{f})$, $\psi(\underline{e}'') = \underline{e}$, $\psi(\underline{f}'') = \underline{f}$ and proceed like above, interchanging $\underline{e}$ and $\underline{e}'$ resp. $\underline{f}$ and $\underline{f}'$.) □

5.4.8.Remark.As Theorems (3.4.7) and (4.4.1) we can generalize Theorem (5.4.7) according to (3.4.8(iii)).We will not present the generalization,which is straightforward,but only that of the more specified analogue of (5.4.7) in §5.6..

5.5.Explicit construction of $(C,F \cup E)$.

In this section we describe explicit constructions for

(i) a code $\mathcal{D}$ such that $(C,\mathcal{D})$ is normalized,and

(ii) a set $G(\underline{y})$ satisfying (G1),(G2),(G3) for each $\underline{y} \in (D^{(0)} \cup E)^s$.

With the definitions from (5.3.1) we then have an explicit construction for $(C,F \cup E)$ satisfying (56).

A look at the expression for $|\mathcal{D}|$ in Theorem (4.4.1) shows that it is desirable to choose x as large as possible - that is,in our case,to choose $|F^{(0)}|$ as large as possible.Below we construct a code $\mathcal{D}$ which is a good choice from this point of vieuw - that is, $|G(\underline{y})|$ can be taken relatively large.

5.5.1.Lemma.Let all definitions be as in (5.3.1).Then there exists a code $\mathcal{D}$ s.t. $(C,\mathcal{D})$ is uniquely decodable,optimal with respect to $(D \cup E)^s$ and normalized s.t.

for each $\underline{y} \in (D^{(0)} \cup E)^s$ with $s \notin W(\underline{y})$ (that is, $\underline{y}_s \in D^{(0)}$) the following holds:

(i) If $\underline{d} \in A(\underline{y}) \cap \mathcal{D}$, $|W(\underline{y})| > \delta - 2$ and $w^*(\underline{d}) < s - |W(\underline{y})|$ then $\underline{d}_s \in D^{(0)}$.

(ii) If $\underline{d} \in A(\underline{y}) \cap \mathcal{D}$, $|W(\underline{y})| \leq \delta - 2$ and $w^*(\underline{d}) \in B_1(\underline{y})$ then $\underline{d}_s \in D^{(0)}$.

(iii) If $\underline{d},\underline{d}' \in A(\underline{y}) \cap \mathcal{D}$, $|W(\underline{y})| \leq \delta - 2$, $w^*(\underline{d}) = w^*(\underline{d}') \in B_2(\underline{y})$ and $a_{00}(\underline{d},\underline{d}') > 0$ then $\underline{d}_s \in D^{(0)}$ and $\underline{d}'_s \in D^{(0)}$.

Proof. Fix $\underline{y} \in (D^{(0)} \cup E)^s$. We construct $A(\underline{y}) \cap \mathcal{D}$ explicitly. Let $\pi(1) < \pi(2) < \ldots$ $\ldots < \pi(s - |W(\underline{y})|)$ denote the indices which are not in $W(\underline{y})$.

(A) If $|W(\underline{y})| > \delta - 2$ let $A(\underline{y}) \cap \mathcal{D} := \{ \underline{d}^{(k)} \mid 0 \leq k \leq \min\{ w-1 , s - |W(\underline{y})| \} \}$, where $\underline{d}^{(k)} = (\underline{d}_1^{(k)}, \ldots, \underline{d}_s^{(k)})$ is defined by

$$\underline{d}^{(k)} \in A(\underline{y}) \ , \ \underline{d}^{(k)}_{\pi(i)} \in D^{(1)} \ \text{ for } \ i \leq k \ , \ \underline{d}^{(k)}_{\pi(i)} \in D^{(0)} \ \text{ for } \ k < i \leq s - |W(\underline{y})|.$$

(B) If $|W(\underline{y})| \leq \delta - 2$ let

$$A(\underline{y}) \cap \mathcal{D} := \{ \underline{d}^{(k)} \mid k \in B_1(\underline{y}) \} \cup \{ \underline{e}^{(k)} \mid k \in V_1(\underline{y}) \} \cup \{ \underline{f}^{(k)} \mid k \in V_1(\underline{y}) \}$$
$$\cup \{ \underline{u}^{(k)} \mid k \in V_2(\underline{y}) \} \cup \{ \underline{v}^{(k)} \mid k \in V_2(\underline{y}) \}$$

where $\underline{d}^{(k)}$ is as in (A) and $\underline{e}^{(k)},\underline{f}^{(k)},\underline{u}^{(k)},\underline{v}^{(k)}$ are defined by : $\underline{e}^{(k)},\underline{f}^{(k)}$, $\underline{u}^{(k)},\underline{v}^{(k)}$ are all in $A(\underline{y})$ and, with the numbers from (4.3.6) :

$$(\underline{e}^{(k)}_{\pi(i)},\underline{f}^{(k)}_{\pi(i)}) \in \begin{cases} D^{(1)} \times D^{(0)} & \text{for } \ 1 \leq i \leq b_{10}(\underline{y}) \\ D^{(0)} \times D^{(1)} & \text{for } \ b_{10}(\underline{y}) < i \leq b_{10}(\underline{y}) + b_{01}(\underline{y}) \\ D^{(1)} \times D^{(1)} & \text{for } \ b_{10}(\underline{y}) + b_{01}(\underline{y}) < i \leq b_{10}(\underline{y}) + b_{01}(\underline{y}) \\ & \qquad + b_{11}(k,\underline{y}) \\ D^{(0)} \times D^{(0)} & \text{for } \ b_{10}(\underline{y}) + b_{01}(\underline{y}) + b_{11}(\underline{y}) < i \leq s - |W(\underline{y})| \end{cases}$$

$(\underline{u}^{(k)}_{\pi(i)},\underline{v}^{(k)}_{\pi(i)})$ is defined in the same way where $b_{ij}(\underline{y})$ and $b_{11}(k,\underline{y})$ should be

replaced by $c_{ij}(\underline{y})$, $c_{11}(k,\underline{y})$ respectively.

From (4.3.6) and (5.4.4) it is immediately clear that $(C,\mathcal{D})$ is u.d.,optimal w.r.t. $(D \cup E)^s$ and normalized.Now note that $s \notin W(\underline{y})$ implies $\pi(s - |W(\underline{y})|) = s$. So (iii) is trivial.Moreover,(i) and (ii) follow immediately from the fact that, for all k , $w^*(\underline{d}^{(k)}) = k$.(Note that $w^*(\underline{d}) < s - |W(\underline{y})|$ for $\underline{d} \in A(\underline{y})$ in case (ii).) □

5.5.2.Example.In (5.3.3(ii)) we have constructed $A(\underline{y}) \cap \mathcal{D}$ as above.

The next step is to define the sets $G(\underline{y})$ and to prove that (G1),(G2),(G3) are satisfied.

5.5.3.Definition.Let $\mathcal{D}$ be a code as described in (5.5.1).For any $\underline{y} \in (D^{(0)} \cup E)^s$ such that $s \in W(\underline{y})$ define $G(\underline{y}) := \phi$,and for any $\underline{y}$ such that $s \notin W(\underline{y})$ define $G(\underline{y})$ as follows:

(112)
$$\text{(i)}\quad G(\underline{y}) := \{\underline{d} \in A(\underline{y}) \cap \mathcal{D} \mid 0 < w^*(\underline{d}) < s - |W(\underline{y})|\} \text{ if } |W(\underline{y})| > s - w \ ,$$
$$\text{(ii)}\quad G(\underline{y}) := A(\underline{y}) \cap \mathcal{D} \text{ if } \delta - 2 < |W(\underline{y})| \leq s - w \ ,$$
$$\text{(iii)}\quad G(\underline{y}) := \{\underline{d} \in A(\underline{y}) \cap \mathcal{D} \mid w^*(\underline{d}) \in B_1(\underline{y})\} \cup \{\underline{d} \in A(\underline{y}) \cap \mathcal{D} \mid 1 < w^*(\underline{d}) < r - 1 - |W(\underline{y})|\} \cup \{\underline{d} \in A(\underline{y}) \cap \mathcal{D} \mid r + 1 < w^*(\underline{d}) < w - 1 - |W(\underline{y})|\} \text{ otherwise .}$$

5.5.4.Lemma.Let all definitions be as in (5.3.1) where $\mathcal{D}$ is a code as in (5.5.1). Let the sets $G(\underline{y})$ be as above.Then these sets satisfy (G1),(G2) and (G3).

Proof.If $s \in W(\underline{y})$ the result is trivial since $G(\underline{y}) = \phi$ .Assume that $s \notin W(\underline{y})$.

First consider the case $|W(\underline{y})| > s - w$.

(G1) is immediate from (5.5.1(i)) and (G3) is empty.Since in this case

$w^*(\psi(\underline{d})) = s - |W(\underline{y})| - w^*(\underline{d})$ we have $\{w^*(\underline{d}) \mid \underline{d} \in G(\underline{y})\} = \{i \mid 0 < i < s - |W(\underline{y})|\}$ $= \{s - |W(\underline{y})| - i \mid 0 < i < s - |W(\underline{y})|\} = \{w^*(\underline{e}) \mid \underline{e} \in \psi(G(\underline{y}))\}$ .This is (G2).

Now consider the case that $\delta - 2 < |W(\underline{y})| \leq s - w$ .Note that $|W(\underline{y})| \leq s - w$ implies $w^*(\underline{d}) < s - |W(\underline{y})|$ for $\underline{d} \in A(\underline{y})$. This and (5.5.1(i)) prove (G1).Again,(G3) is empty.Now note that,in this case, $w^*(\psi(\underline{d})) = (s - |W(\underline{y})| - w^*(\underline{d})) \underline{\bmod} w$ .Hence $\{w^*(\underline{d}) \mid \underline{d} \in G(\underline{y})\} = \{i \mid 0 \leq i < w\} = \{(s - |W(\underline{y})| - i) \underline{\bmod} w \mid 0 \leq i < w\} =$ $= \{w^*(\underline{d}) \mid \underline{d} \in \psi(G(\underline{y}))\}$ .This is (G2).

Finally consider the case that $|W(\underline{y})| \leq \delta - 2$.

From (5.5.1(ii)) we have that $w^*(\underline{d}) \in B_1(\underline{y}) \Rightarrow \underline{d}_s \in D^{(0)}$. Moreover,(5.5.1(iii)) and (4.3.6(iv)) imply that if $\underline{d} \in G(\underline{y})$, $w^*(\underline{d}) \in B_2(\underline{y})$ we have $\underline{d}_s \in D^{(0)}$. This proves (G1) . Now (G3) is immediate from the definition of $G(\underline{y})$.

Note again that $w^*(\psi(\underline{d})) = (s - |W(\underline{y})| - w^*(\underline{d})) \underline{\bmod} w$,and that

$B_1(\underline{y}) = \{(s - |W(\underline{y})| - i) \underline{\bmod} w \mid i \in B_1(\underline{y})\}$;

$\{i \mid 1 < i < r - 1 - |W(\underline{y})|\} = \{(s - |W(\underline{y})| - i) \underline{\bmod} w \mid 1 < i < r - 1 - |W(\underline{y})|\}$;

$\{i \mid r + 1 < i < w - 1 - |W(\underline{y})|\} = \{(s - |W(\underline{y})| - i) \underline{\bmod} w \mid r + 1 < i < w - 1 - |W(\underline{y})|\}$,

which are easy to check.Since the union of the left hand sides above equals $\{w^*(\underline{d}) \mid d \in G(\underline{y})\}$ and the union of the right hand sides equals $\{w^*(\underline{d}) \mid \underline{d} \in \psi(G(\underline{y}))\}$ we have (G2) and the lemma is proved. □

5.5.5.Example.In (5.3.3(ii)) we have not only constructed $\mathcal{D}$ as in (5.5.1) (as mentioned before in (5.5.2)) but we have also chosen $G(\underline{y}) = G(\underline{y})$ according to (5.5.3).

5.6.Explicit expressions for $|C^{(i)}|$, $|F^{(i)}|$ and $|E|$.

Below we enumerate the sizes of the codes $C^{(i)}$, $F^{(i)}$ and E as constructed in

the preceding sections. The sizes of $C^{(i)}$ and $F^{(0)} \cup E$ are already known. The only work left is the calculation of $|F^{(0)}| = \sum_{\underline{y} \in (D^{(0)} \cup E)^s} |G(\underline{y})|$. The following lemma gives an explicit expression for $|G(\underline{y})|$. Finally, in (5.6.2) we state the entire result of this Chapter.

5.6.1. Lemma. Let $G(\underline{y})$ be constructed as in (5.5.3) for all $\underline{y} \in (D^{(0)} \cup E)^s$. Then the size of $G(\underline{y})$ is as follows:

(113) (i) If $s \in W(\underline{y})$: $|G(\underline{y})| = 0$.

(ii) If $s \notin W(\underline{y})$:

(a) $|G(\underline{y})| = s - |W(\underline{y})| - 1$ if $s - w < |W(\underline{y})|$,

(b) $|G(\underline{y})| = w$ if $\delta - 2 < |W(\underline{y})| \leq s - w$,

(c) $|G(\underline{y})| = \max \{w - \delta + 1 + |W(\underline{y})|, w + \delta - 5 - |W(\underline{y})|\}$

if $w - \delta - 2 < |W(\underline{y})| \leq \delta - 2$,

(d) $|G(\underline{y})| = 2.\max \{1 + |W(\underline{y})|, \delta - 2, w - 5 - |W(\underline{y})|\}$

if $|W(\underline{y})| \leq w - \delta - 2$.

Proof. The cases (i), (ii)(a) and (ii)(b) are immediate from (5.5.3). Note that it follows from (5.5.3(iii)) that

$|G(\underline{y})| = |B_1(\underline{y})| + 2.\max \{ |V_1(\underline{y})| - 2 , 0\} + 2.\max \{ |V_2(\underline{y})| - 2 , 0\}$. From this we obtain equations (ii)(c), (d) by a straightforward calculation. □

5.6.2. Theorem. Let $n \in \mathbb{N}$ and let C, D and E be binary codes of length n s.t. there are partitions $C = C^{(0)} \cup C^{(1)}$, $D = D^{(0)} \cup D^{(1)}$ satisfying

(56) (i) $(C, D^{(i)} \cup E)$ is uniquely decodable for $i = 0, 1$.

(ii) $(C^{(i)}, D \cup E)$ is uniquely decodable for $i = 0,1$.

(iii) $(C^{(0)}, D^{(0)}) \perp (C^{(1)}, D^{(1)})$.

(56) (iv) There is a bijective mapping $\phi: D^{(0)} \to D^{(1)}$ such that

$$\forall_{\underline{d} \in D^{(0)}} \forall_{\underline{d}' \in D^{(1)}} [(\exists_{\underline{c},\underline{c}' \in C}: \underline{c} + \underline{d} = \underline{c}' + \underline{d}') \Leftrightarrow \underline{d}' = \phi(\underline{d})] .$$

(v) $D \cap E = \phi$, $C^{(0)} \neq \phi$, $C^{(1)} \neq \phi$, $D^{(0)} \neq \phi$.

Let $q, w, r \in \mathbb{N}$ s.t. $0 \leq r < w$, $w \geq 2$, $q \geq 2$ and define $s := qw + r$, $N := sn$;

(73) $Z := \{ \underline{z} \in \mathbb{F}_2^s \mid w_H(\underline{z}) \equiv 0 \mod w \}$, $C = C^{(0)} \cup C^{(1)}$,where

(114) $C^{(j)} := \{ \underline{c} = (\underline{c}_1, \ldots, \underline{c}_s) \in C^s \mid \exists_{\underline{z} \in Z | z_s = j} \forall_i : \underline{c}_i \in C^{(z_i)} \}$, $j = 0,1$;

Let $x := |D^{(0)}| / |D^{(0)} \cup E|$, $y := |C^{(0)}| / |C|$ and $\delta := \max\{ r, w - r \}$ .Then

(i) C is a code of length N and

$$(115) \quad |C^{(0)}| = |C|^s . \sum_{k=0}^{q} \binom{s-1}{kw} y^{s-kw} (1-y)^{kw} ,$$

$$|C^{(1)}| = |C|^s . \sum_{k=1}^{q} \binom{s-1}{kw-1} y^{s-kw} (1-y)^{kw} .$$

(ii) There are codes $F = F^{(0)} \cup F^{(1)}$, E of length N such that C, F and E satisfy the above properties (56)(i) $\div$ (v) ,where C, F and E take the place of C, D and E respectively.Moreover, $(C, F \cup E)$ is optimal w.r.t. $(D \cup E)^s$ and

$$(116) \quad |F^{(0)}| + |E| = |D^{(0)} \cup E|^s . \Big(w - \sum_{i=0}^{w-2} \binom{s}{i} (w-i-1) x^i (1-x)^{s-i} +$$

$$+ \sum_{i=0}^{w-\delta-2} \binom{s}{i} (w-2i-2) x^{s-i} (1-x)^i +$$

$$+ \sum_{i=w-\delta-1}^{\delta-2} \binom{s}{i} (\delta-1-i) x^{s-i} (1-x)^i \Big) ,$$

$$(117)\qquad |F^{(0)}| = |F^{(1)}| = |D^{(0)} \cup E|^s \cdot \Big(xw - \sum_{i=1}^{w-1} \binom{s-1}{i-1}(w-i+1)\, x^i\, (1-x)^{s-i} +$$

$$+ \sum_{i=0}^{w-\delta-2} \binom{s-1}{i} \cdot \max\{2+2i-w, 2\delta-4-w, w-2i-10\} \cdot x^{s-i}\, (1-x)^i +$$

$$+ \sum_{i=w-\delta-1}^{\delta-2} \binom{s-1}{i} \cdot \max\{i+1-\delta, \delta-i-5\} \cdot x^{s-i}\, (1-x)^i \Big) \quad .$$

Proof. Application of Theorems (4.4.1), (5.4.7) and Lemmas (5.5.1), (5.5.4) and (5.6.1). The size of $F^{(0)} \cup E$ equals the expression for $|\mathcal{D}|$ in (4.4.1) which follows immediately from the definitions in (5.3.1). The sizes of $C^{(i)}$ and $F^{(i)}$ are found by staightforward calculation. Note that

$$(118)\qquad |F^{(0)}| = \sum_{\underline{y} \in (D^{(0)} \cup E)^s} |G(\underline{y})| = \sum_{\underline{y} \in (D^{(0)} \cup E)^{s-1} \times D^{(0)}} |G(\underline{y})| =$$

$$= |D^{(0)} \cup E|^{s-1} \cdot |D^{(0)}| \cdot w + \sum_{\underline{y} \in (D^{(0)} \cup E)^{s-1} \times D^{(0)}} (|G(\underline{y})| - w) \quad . \qquad \square$$

5.6.3. Remark. As in (4.4.1) we do have an explicit construction from Chapters 4 and 5 though the Theorem only states the existence of F and E.

A generalization of the preceding Theorem according to (3.4.8(iii)) leads to

5.6.4. Theorem. Let $q, w, r \in \mathbb{N}$ such that $0 \le r < w$, $q \ge 2$, $w \ge 2$. Let $s := qw + r$. For $i = 1, 2, \ldots, s$ let $n_i \in \mathbb{N}$ and let C_i, D_i, E_i be binary codes of length n_i satisfying (56). Define $N := \sum_{i=1}^{s} n_i$.

Let $Z := \{\underline{z} \in \mathbb{F}_2^s \mid w_H(\underline{z}) \equiv 0 \bmod w\}$, $C = C^{(0)} \cup C^{(1)}$ where

$$C^{(j)} := \{(\underline{c}_1, \ldots, \underline{c}_s) \in \prod_{i=1}^{s} C_i \mid \exists_{\underline{z} \in Z \mid z_s = j} \ \forall_i : \underline{c}_i \in C_i^{(z_i)}\} \quad , j = 0, 1 \ .$$

Let $x_i := |D_i^{(0)}|/|D_i^{(0)} \cup E_i|$, $y_i := |C_i^{(0)}|/|C_i|$, $\delta := \{\max r, w-r\}$ .Then

(i) C is a code of length N and

$$(119) \qquad |C^{(0)}| = \prod_{i=1}^{s} |C_i| . \sum_{k=0}^{q} \sum_{1\le i_1<\ldots<i_{kw}<s} \prod_{i\notin\{i_1,\ldots,i_{kw}\}} y_i \prod_{i\in\{i_1,\ldots,i_{kw}\}} (1-y_i)$$

$$|C^{(1)}| = \prod_{i=1}^{s} |C_i| . \sum_{k=1}^{q} \sum_{1\le i_1<\ldots<i_{kw}=s} \prod_{i\notin\{i_1,\ldots,i_{kw}\}} y_i \prod_{i\in\{i_1,\ldots,i_{kw}\}} (1-y_i)$$

(ii) There exist codes $F = F^{(0)} \cup F^{(1)}$, E of length N as described in (5.3.1) where $|F^{(0)} \cup E|$ equals the size of $\mathcal{D}$ given in (4.4.3) and

$$(120) \qquad |F^{(0)}| = |F^{(1)}| = \prod_{i=1}^{s} |D_i^{(0)} \cup E_i| . (xw - T_1 + T_2 + T_3) \quad \text{,where}$$

$$T_1 = \sum_{k=1}^{w-1} \sum_{1\le i_1<\ldots<i_k=s} (w-k+1) \prod_{i\in\{i_1,\ldots,i_k\}} x_i \prod_{i\notin\{i_1,\ldots,i_k\}} (1-x_i) \quad ,$$

$$T_2 = \sum_{k=0}^{w-\delta-2} \sum_{1\le i_1<\ldots<i_k<s} \max\{2+2k-w, 2\delta-4-w, w-2k-10\} \prod_{i\notin\{i_1,\ldots,i_k\}} x_i \prod_{i\in\{i_1,\ldots,i_k\}} (1-x_i)$$

$$T_3 = \sum_{k=w-\delta-1}^{\delta-2} \sum_{1\le i_1<\ldots<i_k<s} \max\{k+1-\delta, \delta-k-5\} \prod_{i\notin\{i_1,\ldots,i_k\}} x_i \prod_{i\in\{i_1,\ldots,i_k\}} (1-x_i)$$

Here terms with $k<0$ vanish. The proof is omitted.

Results are presented in Chapter 6.

Chapter 6.Numerical results.

6.1.Ratepairs obtained from the constructions in Chapters 2,4 and 5 .

In this section we give a survey of the results obtained from (4.4.3) with or without the use of (5.6.4).

In table 12 we list the results obtained from (4.4.3) by making use of the following systems of basic codes :

$C_i^{(0)} = D_i^{(0)} = \{\underline{0}\}$; $C_i^{(1)} = D_i^{(1)} = \{\underline{1}\}$; $E = \mathbb{F}_2^{n_i} \setminus \{\underline{0},\underline{1}\}$ of length n_i .

Here we shall choose $n_i = m_1$ for $1 \le i \le s_1$, $(s_1 \le s)$

$n_i = m_2$ for $s_1 < i \le s$. Let $s_2 := s - s_1$.

The parameters q , w , r , s_1 , s_2 , m_1 , m_2 and the codelength $N = s_1 m_1 + s_2 m_2$ are listed in the table.The first column gives a lable to which we shall refer in §6.2..The last three columns give the ratepair belonging to the codepair.

We note that the codes in table 12 are found by a computer search of which the best results are selected."Best" should be understood in the sense that only those ratepairs are listed which are on the border of the covex hull of the set of all enumerated ratepairs.

Finally we note that the codes marked with * are from van Tilborg ([8]).These are the only ones for which $s_1 < s$. This choice was made as a result of maximum rate analysis in [8].

nr.	q	w	r	s_1	m_1	s_2	m_2	N	R_1	R_2	R_1+R_2	
a1	5	2	1	10	9	1	10	100	0.10000	0.99999	1.09999	*
a2	5	2	0	9	8	1	9	81	0.11111	0.99998	1.11109	*
a3	4	2	1	8	7	1	8	64	0.12500	0.99992	1.12492	*
a4	4	2	0	7	6	1	7	49	0.14286	0.99968	1.14254	*
a5	4	3	0	12	5	0	-	60	0.17360	0.99860	1.17219	
a6	4	3	1	13	5	0	-	65	0.17562	0.99848	1.17410	
a7	7	3	2	23	5	0	-	115	0.18622	0.99749	1.18370	
a8	3	3	2	11	4	0	-	44	0.21399	0.99404	1.20803	
a9	4	3	0	12	4	0	-	48	0.21699	0.99357	1.21056	
a10	4	3	1	13	4	0	-	52	0.21952	0.99312	1.21264	
a11	6	3	0	18	4	0	-	72	0.22799	0.99112	1.21910	
a12	3	3	2	11	3	0	-	33	0.28533	0.97213	1.25746	
a13	4	3	0	12	3	0	-	36	0.28933	0.97038	1.25971	
a14	4	3	1	13	3	0	-	39	0.29270	0.96876	1.26145	
a15	5	3	2	17	3	0	-	51	0.30226	0.96334	1.26559	
a16	6	3	1	19	3	0	-	57	0.30553	0.96115	1.26667	
a17	2	7	0	14	2	0	-	28	0.41949	0.87994	1.29943	
a18	2	8	0	16	2	0	-	32	0.42662	0.87442	1.30105	
a19	2	9	0	18	2	0	-	36	0.43248	0.86959	1.30207	
a20	2	10	0	20	2	0	-	40	0.43738	0.86533	1.30271	
a21	2	11	0	22	2	0	-	44	0.44155	0.86156	1.30311	
a22	2	12	0	24	2	0	-	48	0.44514	0.85820	1.30334	

table 12.

In table 13 we list the results obtained from (4.4.1) by making use of the inner code system as described in (5.6.4).Here,for the construction of the inner code system $(C, F \cup E)$ we make use of the systems

$C_i^{(0)} = D_i^{(0)} = \{\underline{0}\}$; $C_i^{(1)} = D_i^{(1)} = \{\underline{1}\}$; $E = \mathbb{F}_2^{n_i} \setminus \{\underline{0},\underline{1}\}$ of length n_i .Here we choose $n_i = m$ if $i < s$ and $n_s = 2$.

	Inner code					Outer code						
nr.	q	w	r	m	x	Q	W	R	N	R_1	R_2	R_1+R_2
b1	4	3	0	5	0.079	2	3	0	342	0.17823	0.99844	1.17667
b2	4	3	1	4	0.155	2	3	0	300	0.22317	0.99268	1.21585
b3	2	5	0	3	0.168	2	3	0	174	0.26662	0.97899	1.24561
b4	3	3	2	3	0.228	2	5	0	320	0.28796	0.97166	1.25962
b5	4	3	0	3	0.240	2	5	0	350	0.29185	0.96981	1.26165
b6	6	3	0	3	0.288	2	8	0	848	0.30695	0.96074	1.26769
b7	2	6	0	2	0.262	2	5	0	240	0.40224	0.89375	1.29599
b8	2	7	0	2	0.268	2	8	0	448	0.41425	0.88527	1.29951
b9	2	8	0	2	0.273	2	8	0	512	0.42204	0.87913	1.30116
b10	2	10	0	2	0.281	2	10	0	800	0.43425	0.86873	1.30298
b11	2	12	0	2	0.287	2	14	0	1344	0.44310	0.86056	1.30366

table 13.

We note that the choice $n_s > 2$ would result in a small value of the ratio $x := |F^{(0)}| / |F^{(0)} \cup E|$ .This yields a bad ratepair.

The parameters m , q , w and r are listed in the table,and so is the ratio x. The length of the inner code system equals $n = (s-1)m + 2 = (qw + r - 1)m + 2$.

The construction of the outer codepair is based on the inner code system and parameters Q , W and R which are listed in the table .The codelength N equals $Sn = (QW + R)n$.

In the same sense as above only the best codepairs from a computer search are listed.As we shall see in the next section most of the codes from table 13 are actually the best codes known up to now.However,as a consequence of the huge codelengths the increase of the rates when compared with the rates in table 12 is relatively small.So,from a practical point of view ,these codes are not very interesting.

6.2.A survey of the best ratepairs obtained up to now in comparison with the best known earlier results.

In table 14 below we list the best known earlier results for which we refer to van Tilborg ([4] and [8]).

In table 15 the best known results up to now are listed.Again,"best known" means that these points lie on the border of the convex hull of the set of all obtainable ratepairs.With a_i or b_i we refer to the codes in the tables 12 and 13 . The codepair marked with * is obtained by timesharing its neighbours and is,up to now,of all uniquely decodable codepairs for which $R_1 + R_2 \geq \frac{1}{2}\log_2 6$ the one with lowest R_1 .This means that the corresponding ratepair is the point where our results meet the lower bound obtained from (0.4.1) , as we see in fig.11..The code marked with ** is the one obtained from (2.4.4(i)).

Fig.11. is a diagram in which all points and bounds of interest are plotted.

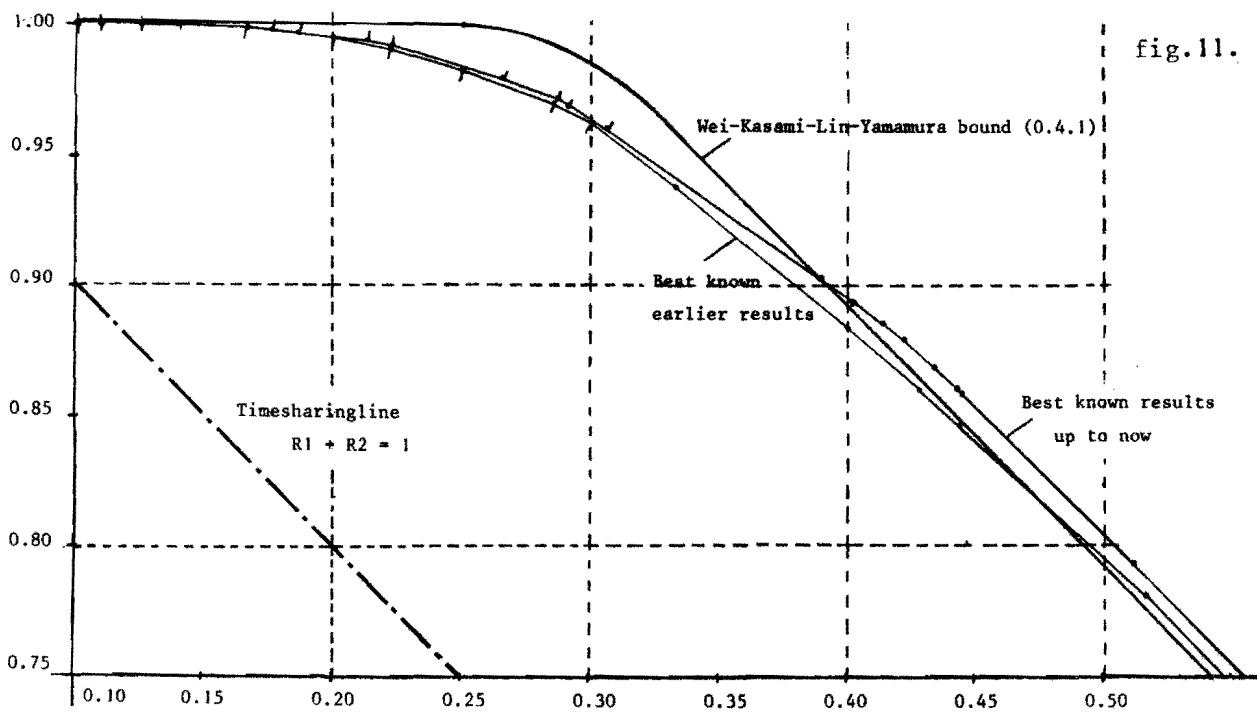


fig.11.

R_1	R_2	R_1+R_2
0.10000	0.99999	1.09999
0.11111	0.99998	1.11109
0.12500	0.99992	1.12492
0.14286	0.99968	1.14254
0.16667	0.99876	1.16543
0.20000	0.99539	1.19539
0.22222	0.99196	1.21418
0.25000	0.98308	1.23308
0.28571	0.97061	1.25632
0.30000	0.96367	1.26367
0.33333	0.93839	1.27172
0.40000	0.88412	1.28412
0.42857	0.86085	1.28942
0.44444	0.84699	1.29143
0.51699	0.78138	1.29837

table 14.
best known earlier results

nr.	R_1	R_2	R_1+R_2
a1	0.10000	0.99999	1.09999
a2	0.11111	0.99998	1.11109
a3	0.12500	0.99992	1.12492
a4	0.14286	0.99968	1.14254
b1	0.17823	0.99844	1.17667
a7	0.18622	0.99749	1.18370
a8	0.21399	0.99404	1.20803
b2	0.22317	0.99268	1.21585
b3	0.26662	0.97899	1.24561
b4	0.28796	0.97166	1.25962
b5	0.29185	0.96981	1.26165
b6	0.30695	0.96074	1.26769
*	0.39043	0.90206	1.29248 = $\frac{1}{2}\,{}^{2}\log 6$
b7	0.40224	0.89375	1.29599
b8	0.41425	0.88527	1.29951
b9	0.42204	0.87913	1.30116
b10	0.43425	0.86873	1.30298
b11	0.44310	0.86056	1.30366
a22	0.44514	0.85820	1.30334
**	0.51214	0.79351	1.30565

table 15.
best known results up to now

Chapter 7.Summary of results.

Below we give a survey of the main issues in this report.

This report contributes to the knowledge of uniquely decodable codepairs for the two-access binary adder channel.This subject can be divided into the following components :

(a) The existence problem : For which pairs of informationrates do there exist pairs of block codes which guarantee unmistakeable transmission for both users simultaneously?

(b) The construction problem : If the existence of such a codepair with specified ratepair is guaranteed,how should we construct these codes?

Neither of these problems has been solved yet.However,in this report we present interesting results concerning both of them.

Chapter 0 gives a description of the channel and the surrounding communication system.We simplify the model with some special assumptions.Moreover a survey of the most important known results is included.

Chapter 1 is concerned with the existence problem.We restrict ourselves to the following question : Let us fix any code C . What is the maximum size of a code D of the same length if we want (C,D) to be uniquely decodable?
For any fixed code C of length n we show the following.We can define a set of pairs $\{\underline{u},\underline{v}\}$, $\underline{u},\underline{v} \in \mathbb{F}_2^n$ called inadmissible pairs such that (C,D) is uniquely decodable iff no inadmissible pairs occur in D . The problem of finding a code D in which no inadmissible pair occurs is equivalent to the problem of finding a coclique in a graph.Using a Theorem concerning the size of a maximal coclique in a graph we obtain a lower bound on the maximal size of D such that (C,D) is

uniquely decodable.The main results are stated in (1.4.3) , (1.5.6) and (1.6.4). We note that these results are weaker than earlier bounds in the sense that the ratepairs obtained in this way fall below them.However,the results are stronger in the sense that in our case one of the two codes is known, cf. (1.4.9(iv)).

The remaining Chapters are concerned with the construction problem.(Note that the construction of a good codepair is also an existence proof!)

Chapter 2 describes an explicit construction method.This method makes use of certain codepairs which are "almost uniquely decodable" and of collections of uniquely decodable codepairs satisfying certain properties of orthogonality.By concatenating these codepairs in a particular way we obtain good (i.e. with high rates) uniquely decodable codepairs.For an explanation of the idea we refer to §2.2..The main results are stated in (2.3.2) and (2.4.1).

In Chapter 3 we describe a general construction method which yields families of uniquely decodable codepairs.Again we make use of "almost uniquely decodable" codepairs.These codepairs are introduced as systems of basic codes. (The concept is different from that in Chapter 2.)Carefull choices of subsets of the s-fold concatenation of the basic codes with themselves yield uniquely decodable codepairs.We refer to §3.2. for an introduction.The main results are stated in (3.4.7) and (3.4.9).

Chapter 4 gives a detailed description of a big collection of codepairs obtained from Chapter 3 by a certain choice of the parameters.A lot af calculations where needed enumerate the sizes of these codes.The main results are stated in (4.4.1) and (4.4.3).The best ratepairs obtained in this way are given in §6.2 and §6.3..

In Chapter 5 it is shown that the codepairs examined in Chapter 4 can be extended in such a way that new systems of basic codes are obtained.So,starting with any

system of basic codes we may generate a sequence of such systems using the construction from Chapter 3 . From each system we obtain a uniquely decodable codepair which gives a better ratepair than its antecessor.However,the gain vanishes very fast with the increase of the block length.For an explanation of the idea we refer to §5.2..The main results are stated in (5.6.2) and (5.6.4).

Finally,in Chapter 6 we give a survey of the best results obtained from the constructions in Chapters 2,4 and 5 in comparison with the best known earlier results.

On the following pages we include a list of important notations.

LIST OF NOTATIONS

		page of first introduction
General		
$+$	addition in $\mathbb{R}$	2
$\oplus$	addition in $\mathbb{F}_2$ (addition mod 2)	2
$\underline{1}$	all-one vector $(1,1,\ldots,1)$ of suitable length	11
$\underline{u} \sqsubset \underline{v}$	$\forall_i : u_i = 1 \Rightarrow v_i = 1$ ($\underline{v}$ covers $\underline{u}$)	11
$(A_i)_{i=0}^n$	distance distribution of a code	16
$(a_i)_{i=0}^n$	weight distribution of a code	49
$P_2(V)$	(V a set) $\{U \subset V \mid \lvert U\rvert = 2\}$	12
$U \mid V$	(U and V codes) $\{\underline{u}\mid\underline{v} \mid \underline{u} \in U \wedge \underline{v} \in V\}$	34
$U \oplus v$	(U a code, $\underline{v}$ a binary vector) $\{\underline{u} \oplus \underline{v} \mid \underline{u} \in U\}$	33
$(C,D) \perp (C',D')$	$\forall_{c\in C}\, \forall_{c'\in C'}\, \forall_{d\in D}\, \forall_{d'\in D'} : \underline{c}+\underline{d} \neq \underline{c}'+\underline{d}'$	32
Chapter 1		
$G_C = (V_C, E_C)$	graph associated to the code C. Vertices : binary vectors of length n. Edges : inadmissible pairs.	13
$E(\underline{c},\underline{c}')$	subset of E_C contributed by the pair $(\underline{c},\underline{c}') \in C^2$	21
$N_C(\underline{c},\underline{c}')$	$\lvert E_C(\underline{c},\underline{c}') \cap P_2(C)\rvert$	23
$L_C(\underline{c})$	(For linear code C) $\lvert\{\underline{v} \in C \mid \underline{v} \sqsubset \underline{c} \oplus \underline{1}\}\rvert$	25
Chapter 3		
ϕ	mapping : $D^{(0)} \to D^{(1)}$ s.t. for $\underline{d} \in D^{(0)}$, $\underline{d}' \in D^{(1)}$: $(\exists_{\underline{c},\underline{c}'\in C} : \underline{c}+\underline{d} = \underline{c}'+\underline{d}') \Leftrightarrow \underline{d}' = \phi(\underline{d})$	47
$W(\underline{y})$	$\{ i \in \{1,2,\ldots,s\} \mid \underline{y}_i \in E \}$	48
$A(\underline{y})$	$\{\underline{d} = (\underline{d}_1,\ldots,\underline{d}_s) \in (D \cup E)^s \mid \forall_{i\in W(\underline{y})} : \underline{d}_i = \underline{y}_i \wedge \forall_{i\notin W(\underline{y})} : \underline{d}_i \in \{\underline{y}_i, \phi(\underline{y}_i)\}\}$	48

C	$\{\underline{c} = (\underline{c}_1,\ldots,\underline{c}_s) \in C^s \mid \exists_{\underline{z}\in Z}\ \forall_i : \underline{c}_i \in C^{(z_i)}\}$	49
$M_Z(\underline{y})$	max. number of vectors in $A(\underline{y})$ such that no pair of them is inadmissible	52
$(C,\mathcal{D})$ optimal w.r.t. E	(For u.d. codepairs only) $\mathcal{D} \subset E$ and : $F \subset E$ and (C,F) is u.d. $\Rightarrow$ $\lvert F\rvert \le \lvert E\rvert$	52

Chapter 4 (see also Ch. 3)

$s = qw + r$	$0 \le r < w \quad N = sn$	57
δ	$\max\{r, w-r\}$	
$w^*(\underline{d})$	$\lvert\{i \in \{1,\ldots,s\} \mid \underline{d}_i \in D^{(1)}\}\rvert$ mod w	57
$V_{ij}(\underline{d},\underline{d}')$	$\{k \in \{1,\ldots,s\} \mid \underline{d}_k \in D^{(i)} \wedge \underline{d}'_k \in D^{(j)}\}$	82
$a_{ij}(\underline{d},\underline{d}')$	$\lvert V_{ij}(\underline{d},\underline{d}')\rvert$	58
$\alpha(\underline{d},\underline{d}')$, $\beta(\underline{d},\underline{d}')$	(only if $w^*(\underline{d}) = w^*(\underline{d}')$) $0 \le \gamma(\underline{d},\underline{d}') < w$	
$\gamma(\underline{d},\underline{d}')$	$\alpha(\underline{d},\underline{d}')w+\gamma(\underline{d},\underline{d}') = a_{10}(\underline{d},\underline{d}')$; similar for β with a_{01}	58
Z	$\{\underline{z} \in \mathbb{F}_2^s \mid w_H(\underline{z}) \equiv 0 \bmod w\}$	58
$\{\underline{d},\underline{d}'\}$ inadmissible		61
$V_1(\underline{y})$	$\{1,\ldots,r-1-\lvert W(\underline{y})\rvert\}$ unless $\lvert W(\underline{y})\rvert \ge r-1$;then ϕ	
$V_2(\underline{y})$	$\{r+1,\ldots,w-1-\lvert W(\underline{y})\rvert\}$ unless $\lvert W(\underline{y})\rvert \ge w-r-1$;then ϕ	64
$B_1(\underline{y})$, $B_2(\underline{y})$	$B_2(\underline{y}) = V_1(\underline{y}) \cup V_2(\underline{y})$ and $B_1(\underline{y}) = \{0,\ldots,w-1\} \setminus B_2(\underline{y})$	64
$b_{ij}(\underline{y})$, $b_{ii}(\ell,\underline{y})$		
$c_{ij}(\underline{y})$, $c_{ii}(k,\underline{y})$	numbers of importance for the construction of a code	67

Chapter 5 (see also Chs. 3 and 4)

ψ	$\psi(\underline{d}_1,\ldots,\underline{d}_s) = (\underline{e}_1,\ldots,\underline{e}_s)$; $\underline{e}_i=\underline{d}_i$ if $\underline{d}_i \in E$; $\underline{e}_i=\phi(\underline{d}_i)$ if $\underline{d}_i \in D^{(0)}$; $\underline{e}_i=\phi^{\leftarrow}(\underline{d}_i)$ if $\underline{d}_i \in D^{(1)}$	77

$\psi(V)$	$\{\psi(\underline{d}) \mid \underline{d} \in V\}$	77
$G(\underline{y})$	subset of $A(\underline{y}) \cap \mathcal{D}$ satisfying properties (G1)$\div$(G3)	77
$C^{(i)}$	$\{\underline{c} = (\underline{c}_1, \ldots, \underline{c}_s) \in C \mid \underline{c}_s \in C^{(i)}\}$	77
$F^{(i)}$, E	$F^{(0)} = \cup_{\underline{y}} G(\underline{y})$, $F^{(1)} = \cup_{\underline{y}} \psi(G(\underline{y}))$, $E = \mathcal{D} \setminus F^{(0)}$	77
$(C,\mathcal{D})$ <u>normalized</u>	(only for codepairs as in (4.4.1))	83

REFERENCES

[1] H.H.J. Liao , "Multiple access channels" , Ph.D. dissertation,Dept. Electrical Engineering , Univ. Hawaii , Honolulu , HI , 1972

[2] N.T. Gaarder and J.K. Wolf , "The capacity region of a multiple-access discrete memoryless channel can increase with feedback" , IEEE Trans. Inform. Theory , vol. IT-21 , pp. 100 - 102 , jan. 1975

[3] T. Kasami and S. Lin , "Bounds on the achievable rates of block coding for a memoryless multiple-access channel" , IEEE Trans. Inform. Theory, vol. IT-24 , pp. 187 - 197 , march 1978

[4] Henk C.A. van Tilborg , "Upperbounds on $|C_2|$ for a uniquely decodable codepair (C_1,C_2) for a two-access binary adder channel" , to appear in IEEE Trans. Inform. Theory.

[5] T. Kasami , S. Lin , V.K. Wei , S. Yamamura , "Graph theoretic approaches to the code construction for the two-user multiple-access binary adder channel" , to appear , Bell laboratories Technical Memorandum 81 - 11217 , 1981

[6] P. Turán , "Egy gráfelmeleti Szélsőértékfeladatról" , Mat.ès Fizikai Lopok, 48 (1941) ,436 - 452 ;see also "On the theory of graphs" , colloq. Math. , 3 (1954) , 19 - 30 , or J. Dénes , "Latin squares and codes" , Proc. Int. Symp. Information Theory , Cachan , France , juli 1977

[7] F.J.A. Mc. Williams and N.J.A. Sloane , "The theory of error-correcting codes" , North-Holland Math. Library , vol.16 , 1977

[8] Henk C.A. van Tilborg , "An explicit construction of a family of codes for a two-access binary adder channel" , (private communication)

[9] S. Lin , T. Kasami and S. Yamamura , "Existence of δ-decodable codes for the two-user multiple-access channel" , IBM J.Res.Dev. , vol. 24 , pp. 486 - 495 , 1980

[10] T. Kasami and S. Lin , "Decoding of linear δ-decodable codes for a multiple-access channel" , IEEE Trans. Inform. Theory , vol. IT-24 , pp. 633 - 635 , 1978

[11] T. Kasami and S. Lin , "Coding for a multiple-access channel" , IEEE Trans. Inform. Theory , vol. IT-22 , pp. 129 - 137 , 1976

[12] R. Ahlswede , "Multi-way communication channels" , Proc. 2nd Inter. Symp. Inform. Theory , Tsahkadsor , Armenian S.S.R. , (1971) , pp. 23 - 52 , Publishing House of the Hungarian Academy of Science , 1973

[13] L. Lovász , "On the Shannon capacity of a graph" , IEEE Trans. Inform. Theory , vol. IT-25 , pp. 1 - 7 , 1979