On linear unequal error protection codes

van Gils, W.J.

Published: 01/01/1982

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

Please check the document version of this publication:

• A submitted manuscript is the author's version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
• The final author version and the galley proof are versions of the publication after peer review.
• The final published version features the final layout of the paper including the volume, issue and page numbers.

Link to publication

Citation for published version (APA):

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal.

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 27. Oct. 2017
On Linear Unequal Error Protection Codes
by W.J. van Gils

EUT-Report 82-WSK-02
June 1982
MASTER'S THESIS

On Linear Unequal Error Protection Codes

by

W.J. van Gils

Supervisor: Prof. dr. J.H. van Lint
Adviser: Dr. ir. H.C.A. van Tilborg

July 1982

Eindhoven University of Technology
Department of Mathematics and Computing Science
ABSTRACT

It is possible for a linear block code to provide more protection against errors for selected message positions than is guaranteed by the minimum distance of the code. Codes having this property are called Linear Unequal Error Protection (LUEP) codes. In this report the optimal encoding of LUEP codes is discussed and bounds on the length of a code that ensures a given unequal error protection are derived. A number of constructions of LUEP codes are given. Cyclic UEP codes together with Majority Logic Decoding of certain classes of these are treated. A list of LUEP codes of minimal length and a list of cyclic UEP codes are included.

AMS Subject Classification: 94B05, 94B60.
In data transmission and processing a desired level of error control is guaranteed by using error-correcting codes. Most block codes considered in the literature have the property that their correcting capabilities are described in terms of the correct reception of the entire message. These codes can successfully be applied in those cases where all positions in a message word require equal protection against errors. However, many applications exist in which some message positions are more important than other ones. For example in transmitting numerical data, errors in the sign or in the high-order digits are more serious than are errors in the low-order digits. As another example consider the transmission of message words from different sources simultaneously in only one codeword, while the different sources have mutually different demands concerning the protection against errors. Accordingly there is an interest in codes which protect some positions in a message word against a larger number of errors than other ones. Such codes are called Unequal Error Protection codes (abbreviated: UEP codes). Masnick and Wolf (1967) introduced the concept of Unequal Error Protection. But, in contrast with what one would expect, they considered error protection of each single position in a codeword. In this report we consider error protection of single positions in the message words, following the formal definitions of Dunning and Robbins (1978).

In Chapter 1 we introduce the concept of Linear Unequal Error Protection codes (LUEP codes) and define a vector, the so-called separation vector, by which the error-correcting capability of a LUEP code is measured. In Section 1.2 we consider a special form of a generator matrix for a LUEP code, the so-called canonical form, introduced by Boyarinov and Katsmaa (1981).

The error-correcting capability of a LUEP code, measured by the separation vector, depends upon the choice of a generator matrix which is used for the encoding of the message set. But fortunately every code has a so-called optimal generator matrix, whose separation vector is componentwise larger than or equal to the separation vector of any other generator matrix of the code. Chapter 2 provides a necessary and sufficient condition for a generator matrix to be optimal. It is also shown that a generator matrix of a code which has the smallest number of nonzero entries is optimal. The results in Chapter 2 are from Dunning and Robbins (1978).
An interesting and basic problem is to find a LUEP code with a given dimension and separation vector such that its length is minimal and hence its information rate is maximal. In Chapter 3 we derive a number of bounds on the length of LUEP codes. For the special case where all message positions are equally protected, some of our bounds reduce to the well-known Singleton, Plotkin, and Griesmer Bounds. Some earlier work on bounds was done by Katsman (1980); he derived Corollary (3.3.14) for the binary case. Our bounds give better results than the bound of Katsman (1980) does (cf. Section 3.4). The Theorems (3.3.2), (3.3.6), the binary version of (3.3.12), the Corollaries (3.3.7), (3.3.8), and formula (35) for linear UEP codes were already reported in van Gils (1981). Appendix A provides a table of all binary LUEP codes with maximal separation vector and length less than or equal to 15.

In Chapter 4 we construct a number of LUEP codes. Section 4.1 provides some infinite families of LUEP codes which have minimal length and maximal separation vector. Section 4.2 contains a number of constructions which build LUEP codes from (LUEP) codes of smaller length, such as the direct sum and direct product construction, the \(|u|u+v| \) construction, and concatenation.

Chapter 5 deals with cyclic UEP codes. In Section 5.1 we give an optimal generator matrix for a cyclic UEP code and observe how its error-correcting capability depends on the weight distribution of its cyclic subcodes. In Section 5.2 we consider classes of cyclic UEP codes which can be decoded by Majority Logic Decoding Methods. Earlier results (Theorem (5.2.1) and (5.2.8)) on cyclic UEP codes were obtained by Dyn'kin and Togonidze (1976). Appendix B provides a table of all binary cyclic UEP codes of length less than or equal to 39.
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ABSTRACT</strong></td>
<td>i</td>
</tr>
<tr>
<td><strong>PREFACE</strong></td>
<td>ii</td>
</tr>
<tr>
<td><strong>CONTENTS</strong></td>
<td>iv</td>
</tr>
<tr>
<td><strong>LIST OF SYMBOLS</strong></td>
<td>vi</td>
</tr>
<tr>
<td><strong>1. INTRODUCTION</strong></td>
<td></td>
</tr>
<tr>
<td>1.1 Definition of Linear Unequal Error Protection Codes</td>
<td>1</td>
</tr>
<tr>
<td>1.2 The canonical form of a generator matrix</td>
<td>3</td>
</tr>
<tr>
<td>1.3 Notes</td>
<td>5</td>
</tr>
<tr>
<td><strong>2. OPTIMAL ENCODING OF LINEAR UNEQUAL ERROR PROTECTION CODES</strong></td>
<td></td>
</tr>
<tr>
<td>2.1 A necessary and sufficient condition for a generator matrix to be optimal</td>
<td>6</td>
</tr>
<tr>
<td>2.2 Minimal weight generator matrices</td>
<td>8</td>
</tr>
<tr>
<td>2.3 Notes</td>
<td>9</td>
</tr>
<tr>
<td><strong>3. BOUNDS ON THE LENGTH OF LINEAR UNEQUAL ERROR PROTECTION CODES</strong></td>
<td></td>
</tr>
<tr>
<td>3.1 Definitions and properties</td>
<td>10</td>
</tr>
<tr>
<td>3.2 Upper bounds</td>
<td>11</td>
</tr>
<tr>
<td>3.3 Lower bounds</td>
<td>12</td>
</tr>
<tr>
<td>3.4 Notes</td>
<td>17</td>
</tr>
<tr>
<td><strong>4. CONSTRUCTIONS OF LINEAR UNEQUAL ERROR PROTECTION CODES</strong></td>
<td></td>
</tr>
<tr>
<td>4.1 Certain families of codes</td>
<td>19</td>
</tr>
<tr>
<td>4.2 Combining codes</td>
<td>23</td>
</tr>
<tr>
<td>4.3 Notes</td>
<td>29</td>
</tr>
<tr>
<td><strong>5. CYCLIC UNEQUAL ERROR PROTECTION CODES</strong></td>
<td></td>
</tr>
<tr>
<td>5.1 The separation vector of a cyclic UEP code</td>
<td>30</td>
</tr>
<tr>
<td>5.2 Majority Logic Decoding of cyclic UEP codes</td>
<td>33</td>
</tr>
<tr>
<td>5.3 Notes</td>
<td>46</td>
</tr>
</tbody>
</table>
APPENDIX A: BINARY OPTIMAL LINEAR UEP CODES OF LENGTH LESS THAN OR EQUAL TO 15  

APPENDIX B: A TABLE OF ALL BINARY CYCLIC UEP CODES OF LENGTH LESS THAN OR EQUAL TO 39  

REFERENCES  

INDEX
LIST OF SYMBOLS

\( \mathbb{F}_q \), \( GF(q) \) : the finite field (Galois field) of \( q \) elements.

\( \mathbb{F}_q[x] \) : the ring of polynomials in \( x \) over \( \mathbb{F}_q \).

\( \mathbb{F}_q[x]/(x^n-1) \) : the residue class ring \( \mathbb{F}_q[x] \) modulo \( (x^n-1) \).

\( n \) : the wordlength of a code.

\( k \) : the dimension of a code.

\( d \) : the minimum distance of a code.

\( s \) : the separation vector of a code.

\( wt(c) \) : the Hamming weight of the vector \( c \).

\( wt[C] \) : \( \min \{ wt(c) \mid c \in C \} \).

\( WT(C) \) : \( \{ wt(c) \mid c \in C \} \).

\( C(\rho) \) : \( \{ c \in C \mid wt(c) \leq \rho \} \).

\( G \) : the generator matrix of a code.

\( G_{i*} \) : the \( i \)th row of the matrix \( G \).

\( G_{*j} \) : the \( j \)th column of the matrix \( G \).

\( R(G) \) : the set of rows of the matrix \( G \).

\( R(G)(\rho) \) : \( \{ X \in R(G) \mid C(\rho) < X \} \).

\( s(G) \) : the separation vector of a code.

\( <X> \) : the linear span of the set \( X \).

\([n,k,d]\) : a linear code of wordlength \( n \), dimension \( k \), and minimum distance \( d \).

\([n,k,s]\) : a linear code of wordlength \( n \), dimension \( k \), and separation vector \( s \).

\( n_1(s) \) : cf. page 10.

\( n_q(s) \) : cf. page 10.

\( M_i \) : a minimal ideal in \( \mathbb{F}_q[x]/(x^n-1) \).

\( M_{ij} \) : a generator matrix of \( M_i \).

\( C_i[x] \) : the cyclotomic coset modulo \( n \) containing \( i \).

\( x \) : the largest integer less than or equal to \( x \).

\( \lfloor x \rfloor \) : the smallest integer larger than or equal to \( x \).

\( a \mid b \) : \( a \) is a divisor of \( b \).

\( I_k \) : the \( k \) by \( k \) unit matrix.
1. INTRODUCTION

In this chapter we give an introduction to the concept of Linear Unequal Error Protection Codes. The reader is assumed to be familiar with the basic principles of linear algebra, finite fields, and error-correcting codes. For an extensive treatment we refer to MacWilliams and Sloane (1978) and van Lint (1982). In Section 1.1 we define "Unequal Error Protection" and in Section 1.2 we derive a special form of the generator matrix for a linear UEP code, the so-called canonical form.

1.1 Definition of Linear Unequal Error Protection Codes

Let $q$ be a prime power and let $\mathbb{F}_q = \text{GF}(q)$ be the Galois field of order $q$. A linear $[n,k]$ code $C$ of length $n$ and dimension $k$ over $\mathbb{F}_q$ is a $k$-dimensional linear subspace of $\mathbb{F}_q^n$. A generator matrix $G$ of this code is a $k \times n$ matrix whose rows form a basis of $C$. The bijection from $\mathbb{F}_q^k$ onto $C$ which maps any element $m \in \mathbb{F}_q^k$ of the message set onto a codeword $c = mG$ is called an encoding of $C$ by means of the generator matrix $G$. For $x \in \mathbb{F}_q^n$, $\text{wt}(x)$ denotes the (Hamming) weight of $x$, i.e. the number of nonzero components in $x$.

Dunning and Robbins (1978) have introduced the following formal definition.

(1.1.1) Definition: For a linear $[n,k]$ code $C$ over the alphabet $\mathbb{F}_q$, the separation vector $s(G) = (s(G)_1, \ldots, s(G)_k)$ of length $k$, with respect to a generator matrix $G$ of $C$, is defined by

$$s(G)_i := \min \{ \text{wt}(mG) : m \in \mathbb{F}_q^k, \ m_i \neq 0 \} \quad (i=1, \ldots, k).$$

This means that for any $\alpha, \beta \in \mathbb{F}_q$, $\alpha \neq \beta$, the sets $\{ mG : m \in \mathbb{F}_q^k, \ m_i = \alpha \}$ and $\{ mG : m \in \mathbb{F}_q^k, \ m_i = \beta \}$ are at distance $s(G)_i$ apart (i=1,\ldots,k). This observation implies the following error-correcting capability of a code when we use it on a q-ary symmetric channel.
(1.1.2) **Theorem:** For a linear \([n,k]\) code \(C\) over \(\mathbb{F}_q\), which uses the matrix \(G\) for its encoding, we can guarantee the correct reception of the \(i^{th}\) digit of the message word if the error pattern has a Hamming weight less than or equal to \(\left\lfloor \frac{(s(G)_i - 1)}{2} \right\rfloor\) by using maximum likelihood decoding.

From Definition (1.1.1) it is immediately clear that the minimum distance of the code equals

\[
d = \min \{ s(G)_i \mid i = 1, \ldots, k \}.
\]

Hence by Theorem (1.1.2) we can guarantee correct reception of the complete message if the error pattern has a weight less than or equal to \(\left\lfloor \frac{(d-1)}{2} \right\rfloor\).

The following definition is an immediate consequence of Theorem (1.1.2).

(1.1.3) **Definition:** If a linear code \(C\) has a generator matrix \(G\) such that the components of the separation vector \(s(G)\) are not mutually equal, then the code \(C\) is called a **Linear Unequal Error Protection** Code (LUEP code).

One can easily decode LUEP codes by using Syndrome Decoding (cf. MacWilliams and Sloane (1978)). This decoding method reaches the correction capability given by Theorem (1.1.2), because of the following fact. For a fixed coset \(R\) of a linear code \(C\), encoded by means of a generator matrix \(G\), let \(U\) be the set of coset leaders of \(R\). For any \(r \in R\), \(r+U\) contains all codewords which are closest to \(r\), i.e. at a distance \(d(r,C)\), the distance between \(r\) and \(C\), from \(r\). If \(i \in \{ 1, \ldots, k \}\) is such that the weight of the elements of \(U\) is less than or equal to \(\left\lfloor \frac{(s(G)_i - 1)}{2} \right\rfloor\), then the \(i^{th}\) digits of the messages corresponding to the elements of \(r+U\) are mutually equal. Hence if \(r\) is the received word, Syndrome Decoding correctly reproduces the \(i^{th}\) digit of the message sent.

In Section 5.2 we treat a Majority Logic Decoding method for certain classes of cyclic UEP codes.
1.2 The canonical form of a generator matrix

By simultaneously permuting the message positions in the message words and the rows of a generator matrix $G$, we may obtain a generator matrix $\bar{G}$ for the code such that $s(\bar{G})$ is nonincreasing, i.e. $s(\bar{G})_i \geq s(\bar{G})_{i+1}$ for $i = 1, \ldots, k-1$. From now on we assume that the message positions and the rows in generator matrices are ordered such that the corresponding separation vectors are nonincreasing.

Boyarinov and Katsman (1981) have introduced a special form of a generator matrix, called a canonical form.

\begin{align*}
\begin{array}{c|c|c|c}
I_{k_1} & 0 & 0 & 0 \\
\hline
G_{2,1} & I_{k_2} & 0 & 0 \\
\hline
G_{z-1,1} & G_{z-1,2} & I_{k_{z-1}} & 0 \\
\hline
G_{z,1} & G_{z,2} & G_{z,z-1} & I_{k_z} \\
\end{array}
\end{align*}

For $k \in \mathbb{N}$ we define a partial order in $\mathbb{R}^k$ by

$$x \preceq y : \iff x_i \leq y_i \text{ for } i = 1, \ldots, k,$$

where $x, y \in \mathbb{R}^k$. We say that $\bar{x}$ is a maximum of the set $A \subset \mathbb{R}^k$ if for all $x \in A$, $x \leq \bar{x}$.

Any generator matrix $G$ of a code can be transformed into a canonical generator matrix $G_{\text{can}}$ of the code such that $s(G_{\text{can}}) \geq s(G)$ by a number
of elementary transformations on the rows of $G$, i.e. permutation and addition of rows and multiplication of rows by scalars. This is a consequence of the following theorem.

(1.2.2) Theorem: For $k, n \in \mathbb{N}$, $i, j \in \{1, \ldots, k\}$, $i \neq j$, $\alpha \in \mathbb{F}_q \setminus \{0\}$ and a $k$ by $n$ matrix $G$ over $\mathbb{F}_q$ let $G'$ be a $k$ by $n$ matrix obtained by replacing the $i$'th row of $G$ by the sum of the $i$'th row and $\alpha$ times the $j$'th row of $G$.

Then the separation vector $s(G')$ satisfies

$$s(G')_v = s(G)_v \quad \text{for } v \neq j$$

(4)

$$s(G')_j \geq s(G)_j \quad \text{if } s(G)_j = s(G)_i$$

(5)

$$s(G')_j \geq s(G)_j \quad \text{if } s(G)_j > s(G)_i$$

(6)

$$s(G')_j = s(G)_i \quad \text{if } s(G)_j < s(G)_i$$

(7)

Proof: For a set $X \in \mathbb{F}_q^n$, $\langle X \rangle$ denotes the linear span of $X$ and $\text{wt}[X]$ is the minimum weight in $X$, i.e. $\min \{ \text{wt}(x) \mid x \in X \}$. For a matrix $A$, $R(A)$ denotes the set of rows of $A$ and $A_i$ denotes the $i$'th row of $A$.

For $v \neq i,j$ we have $s(G')_v := \text{wt}[G' + \langle R(G') \setminus \{G' \} \rangle] = \text{wt}[G_{v*} + \{\beta(G_i^* + \alpha G_j^*) \mid \beta \in \mathbb{F}_q \} + \langle R(G) \setminus \{G_i^*, G_j^* \} \rangle] = \text{wt}[G_{v*} + \{\beta G_i^* \mid \beta \in \mathbb{F}_q \} + \langle R(G) \setminus \{G_i^*, G_j^* \} \rangle] = \text{wt}[G_{v*} + \langle R(G) \setminus \{G_i^*, G_j^* \} \rangle] = s(G)_v$.

$$s(G')_i := \text{wt}[G_{i*} + \langle R(G') \setminus \{G' \} \rangle] = \text{wt}[G_i^* + \alpha G_j^* + \langle R(G) \setminus \{G_i^* \} \rangle] = \text{wt}[G_i^* + \langle R(G) \setminus \{G_i^* \} \rangle] = s(G)_i$$

$$s(G')_j := \text{wt}[G_{j*} + \langle R(G') \setminus \{G' \} \rangle] = \text{wt}[G_j^* + \{\beta(G_i^* + \alpha G_j^*) \mid \beta \in \mathbb{F}_q \} + \langle R(G) \setminus \{G_i^*, G_j^* \} \rangle] = s(G)_j$$

For $s(G)_j < s(G)_i$ we have that $\text{wt}[G_j^* + \langle R(G) \setminus \{G_i^*, G_j^* \} \rangle] = s(G)_j$, $\text{wt}[G_j^* + \{\beta(G_i^* + \alpha G_j^*) \mid \beta \in \mathbb{F}_q \setminus \{0\} \} + \langle R(G) \setminus \{G_i^*, G_j^* \} \rangle] \geq s(G)_i$ and hence $s(G')_j = s(G)_j$, i.e. formula (5).

In a similar way we obtain formula (6) and (7).

From this theorem it is immediately clear that we can transform an arbitrary generator matrix $G$ of a code into a canonical generator matrix $G_{\text{can}}$ such that $s(G_{\text{can}}) \geq s(G)$ by applying a sequence of elementary transformations on $G$. This theorem also shows (by formula (7)) that if we want to transform a generator matrix $G$ into a systematic generator matrix $G_{\text{syst}}$, we cannot guarantee that $s(G_{\text{syst}}) \geq s(G)$.
Example: For $q = 2$,

\[
G = \begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
\end{bmatrix}
\] (8)

has separation vector $s(G) = (5,4,4,4,4)$. It is impossible to transform $G$ into a systematic generator matrix $G_{\text{syst}}$ such that $s(G_{\text{syst}}) \geq (5,4,4,4,4)$. Actually, a $5 \times 10$ binary systematic generator matrix with a separation vector of at least $(5,4,4,4,4)$ does not exist (cf. van Gils (1981)).

1.3 Notes

One can generalize Definition (1.1.1) for nonlinear codes. Consider a code $C$ over the alphabet $\mathbb{F}_q$ containing $q^k$ codewords. Let the message set $\mathbb{F}_q^k$ be encoded according to the bijection $\eta$, mapping $\mathbb{F}_q^k$ onto $C$. The separation vector $s(\eta)$ of $C$ with respect to the encoding function $\eta$ is defined by

\[
s(\eta)_i := \min \{ \text{wt}(\eta(m) - \eta(m')) \mid m, m' \in \mathbb{F}_q^k, m_i \neq m_i' \}
\] (9)

for $i = 1, \ldots, k$. Of course Theorem (1.1.2) also holds for nonlinear UEP codes.

Dunning and Robbins (1978) have also considered the Lee Metric. Boyarinov and Katsman (1981') have introduced the canonical form of a generator matrix.
2. OPTIMAL ENCODING OF LINEAR UNEQUAL ERROR PROTECTION CODES

The separation vector defined by formula (1) depends upon the choice of a generator matrix for the code. In this chapter we show that a linear code C has an optimal generator matrix \( G^* \), i.e. \( s(G^*) \geq s(G) \) for all generator matrices G of C. In Section 2.1 we give a necessary and sufficient condition for a generator matrix to be optimal. In Section 2.2 we show that for a linear code a generator matrix with the smallest number of nonzero entries is optimal. The results in this chapter are from Dunning and Robbins (1978).

2.1 A necessary and sufficient condition for a generator matrix to be optimal

(2.1.1) Definition: For a linear code C a generator matrix G is called optimal, whenever \( s(G) \) is the maximum of the set of nonincreasing separation vectors \( s(A) \), where A is a generator matrix of C.

For a linear \([n,k]\) code we define \( \text{WT}(C) := \{ \text{wt}(c) \mid c \in C \} \), i.e. the set of all possible weights of codewords in C. For \( \rho \in \text{WT}(C) \), \( C(\rho) := \{ c \in C \mid \text{wt}(c) \leq \rho \} \) is the set of codewords in C having a weight of at most \( \rho \). For a generator matrix G of C let \( R(G) := \{ G_1^*, \ldots, G_k^* \} \) denote the set of rows of G and let \( R(G)(\rho) := \cap \{ X \subseteq R(G) \mid C(\rho) \subseteq \langle X \rangle \} \) be the smallest subset of \( R(G) \) such that \( C(\rho) \) is contained in its linear span. The relation between \( s(G) \) and \( R(G)(\rho) \) is given in the following lemma.

(2.1.2) Lemma: A generator matrix G of a linear \([n,k]\) code C satisfies

\[
s(G)_i \leq \rho \quad \iff \quad G_i^* \in R(G)(\rho)
\]

for each \( i \in \{1, \ldots, k\} \) and \( \rho \in \text{WT}(C) \).

Proof: Let \( i \in \{1, \ldots, k\} \) and \( \rho \in \text{WT}(C) \). If \( G_i^* \in R(G)(\rho) \) then \( C(\rho) \not\subseteq \langle R(G) \setminus \{ G_i^* \} \rangle \) and hence \( C(\rho) \cap C \setminus \langle R(G) \setminus \{ G_i^* \} \rangle \neq \emptyset \), which implies that
The following theorem provides a necessary and sufficient condition for a generator matrix to be optimal for its rowspace.

(2.1.3) **Theorem:** A generator matrix $G$ of a linear $[n,k]$ code $C$ is optimal if and only if for any $\rho \in \text{WT}(C)$ a subset $X \subset R(G)$ of the rows of $G$ exists such that $<C(\rho)> = <X>$.

**Proof:**

**Sufficiency:** Suppose a generator matrix $G$ of $C$ satisfies the condition in the theorem. Assume that $G$ is not optimal, i.e. a generator matrix $A$ exists such that $s(G) < s(A)$ and set $\rho := s(A)-1$. Since $s(A) \geq \ldots \geq s(A) > \rho$, we have $C(\rho) < A(i+1)^* \ldots , A_k^*$ and thus also $C(\rho) < A(i+1)^* \ldots , A_k^*$. On the other hand we have that $\rho = s(G) \geq \ldots \geq s(G)$, which by Lemma (2.1.2) implies that $G_1^*, \ldots , G_k^* \in R(G)(\rho)$. Combining these observations with the fact that $C(\rho) = <R(G)(\rho)>$ we obtain $<G_1^*, \ldots , G_k^*> < R(G)(\rho) = <A(i+1)^* \ldots , A_k^*>$, which is a contradiction. Hence our assumption was wrong and so $G$ is optimal.

**Necessity:** Suppose $G$ is an optimal generator matrix for the code $C$. Let $\rho \in \text{WT}(C)$ and let $A$ be a generator matrix of $C$ such that $<C(\rho)> = <A(k-p+1)^* \ldots , A_k^*>$, where $p := \text{dim}<C(\rho)>$. By Definition (1.1.1) we have that $s(A) \geq \ldots \geq s(A)_{k-p} > \rho$ and hence $s(G)_{k-p} > s(G)_{1} \geq \ldots \geq s(G)_{k-p} > \rho$, since $G$ is optimal. Again applying Lemma (2.1.2) yields that $R(G)(\rho) \subset \{G(k-p+1)^* \ldots , G_k^*\}$ and hence $C(\rho) = <G(k-p+1)^* \ldots , G_k^*>$, since $<C(\rho)> = <R(G)(\rho)>$ and $\text{dim}<G(k-p+1)^* \ldots , G_k^*> = p$.

(2.1.4) **Corollary:** Any linear code has an optimal generator matrix.

Hence the following definition makes sense.

(2.1.5) **Definition:** The separation vector of a linear code is defined as the separation vector of an optimal generator matrix of the code.

We shall use the notation $[n,k,s]$ for a linear code of length $n$, dimension $k$, and separation vector $s$. For $i = 1, \ldots , k$, $\lfloor (s_i - 1)/2 \rfloor$ is called
the protection level of the \( i \)th message position.

2.2 Minimal weight generator matrices

Optimal generator matrices which are easy to compute, given the rowspace, are the so-called minimal weight generator matrices.

(2.2.1) Definition: For a linear \([n,k]\) code \( C \) over \( \mathbb{F}_q \), a generator matrix \( G \) is called a minimal weight generator matrix if

\[
\sum_{i=1}^{k} \text{wt}(G_{i*})
\]

is a minimum of the set

\[
\{ \sum_{i=1}^{k} \text{wt}(A_{i*}) \mid A \text{ is a generator matrix of } C \}.
\]

We shall show that a minimal weight generator matrix is optimal. First we show that it is easy to compute the separation vector of these matrices.

(2.2.2) Lemma: If \( G \) is a minimal weight generator matrix of a \( k \)-dimensional code, then

\[
\text{wt}(G_{i*}) = s(G)_i
\]

for \( i = 1, \ldots, k \).

Proof: Let \( G \) be a generator matrix of a \( k \)-dimensional code such that \( \text{wt}(G_{i*}) \neq s(G)_i \) for some \( i \in \{1, \ldots, k\} \). Since \( s(G)_i \leq \text{wt}(G_{i*}) \) we have the strict inequality \( s(G)_i < \text{wt}(G_{i*}) \).

Let \( v \in C \setminus \langle R(G) \setminus \{G_{i*}\} \rangle \) be such that \( \text{wt}(v) = s(G)_i \). Then we have that

\[
\sum_{j=1}^{k} \text{wt}(G_{j*}) > \sum_{j=1, j \neq i}^{k} \text{wt}(G_{j*}) + \text{wt}(v).
\]

\( G_{1*}, \ldots, G_{(i-1)*}, v, G_{(i+1)*}, \ldots, G_{k*} \) are linearly independent and so they form the rows of a generator matrix for \( C \). Hence \( G \) is not a minimal weight generator matrix. This proves the lemma.

\[\square\]
(2.2.3) **Lemma:** A minimal weight generator matrix \( G \) of a \( k \)-dimensional linear code \( C \) satisfies

\[
\langle C(p) \rangle = \langle \{ G_{i*} \mid i \in \{1, \ldots, k\} \mid \text{wt}(G_{i*}) \leq p \} \rangle
\]

for any \( p \in \text{WT}(C) \).

**Proof:** That LHS \( \supset \) RHS is trivial. On the other hand let \( c \in C(p) \). The message \( m \) such that \( c = mG \) satisfies \( m_j = 0 \) for all \( j \) satisfying \( s(G)_j > p \), which by Lemma (2.2.2) is equivalent to \( \text{wt}(G_{j*}) > p \). Hence \( c \in \text{RHS} \). The RHS of formula (12) is a linear space, so \( \langle C(p) \rangle \subset \text{RHS} \).

(2.2.4) **Theorem:** A minimal weight generator matrix is optimal.

**Proof:** Combine Theorem (2.1.3) and the Lemmas (2.2.2) and (2.2.3).

Besides a proper permutation of the rows any minimal weight generator matrix of a \( k \)-dimensional linear code \( C \) can be constructed by the following algorithm.

1. Set \( i := k \).
2. Choose \( v \in C \setminus \langle G_{(i+1)*}, \ldots, G_k* \rangle \) such that
   \[
   \text{wt}(v) = \text{wt} [C \setminus \langle G_{(i+1)*}, \ldots, G_k* \rangle ].
   \]
3. Set \( G_{i*} := v \).
4. If \( i > 1 \) then decrease \( i \) by 1 and go to step 2, otherwise stop.

2.3 **Notes**

The results of this chapter are from Dunning and Robbins (1978). They also show that a linear code has an optimal encoding (linear or nonlinear) and that no nonlinear encoding is better, i.e. has a larger separation vector, than an optimal linear encoding. They also give an example of a nonlinear code which has no optimal encoding.

If we replace the Hamming metric by the Lee metric, all lemmas and theorems in this chapter remain valid (cf. Dunning and Robbins (1978)).
3. BOUNDS ON THE LENGTH OF LINEAR UNEQUAL ERROR PROTECTION CODES

A basic problem is to find linear UEP codes with a given dimension and separation vector such that their length is minimal and hence their information rate is maximal. In Section 3.1 we give two formal definitions of functions we want to consider together with their properties. In Section 3.2 resp. 3.3 we give upper resp. lower bounds for these functions. Appendix A gives function values for binary LUEP codes of length less than or equal to 15.

3.1 Definitions and properties

(3.1.1) Definition: For any \( k \in \mathbb{N}, s \in \mathbb{N}^k \) and prime power \( q \) we define

\[
q(s) \quad \text{as the length of the shortest linear code over } F_q \text{ of dimension } k \text{ with a separation vector of at least } s.
\]

and

\[
q^{ex}(s) \quad \text{as the length of the shortest linear code over } F_q \text{ of dimension } k \text{ with separation vector (exactly) } s.
\]

An \([q(s), k, s]\) code is called length-optimal. It is called optimal, if an \([q(s), k, t]\) with \( t \geq s, t \neq s \) does not exist.

(3.1.2) Properties: For any \( k \in \mathbb{N}, s, t \in \mathbb{N}^k \) and prime power \( q \) the functions \( q(.) \) and \( q^{ex}(.) \) have the following properties.

\[
\begin{align*}
q(s) & \leq q^{ex}(s), \\
q(s) & \leq q(t), \\
q(s) & \leq q^{ex}(t).
\end{align*}
\]

To illustrate (15), observe that \(q^{ex}(5,4,4) = 8\) (cf. Appendix A) and \(q^{ex}(5,4,3) = 9\), which can be seen by easy verification.
3.2 Upper bounds

The following theorem provides a trivial upper bound for \( n_q(\cdot) \) and \( n^\text{ex}_q(\cdot) \) and an easy way to construct linear UEP codes.

**Theorem:** For any prime power \( q \), \( k \in \mathbb{N} \), \( v \in \mathbb{N} \), \( s \in \mathbb{N}^k \) and \( k_0 = 0 < k_1 < k_2 < \ldots < k_v = k \) we have

\[
\begin{align*}
    n^\text{ex}_q(s_1, \ldots, s_k) &\leq \sum_{u=0}^{v-1} n^\text{ex}_q(s_{k_u} + 1, s_{k_u+2}, \ldots, s_{k_{u+1}}), \\
    \text{(16)}
\end{align*}
\]

The same inequality holds for \( n_q(\cdot) \) (Replace \( n^\text{ex}_q(\cdot) \) in (16) by \( n_q(\cdot) \)).

**Proof:** For \( u = 0, 1, \ldots, v-1 \) let \( G \) be a generator matrix of a \([n^\text{ex}_q(s_{k_u} + 1, \ldots, s_{k_{u+1}}), k_{u+1} - k_u] \) code over \( \mathbb{F}_q \) with separation vector \( s_{k_u} + 1, \ldots, s_{k_{u+1}} \). Then

\[
G := \begin{bmatrix}
G_0 & 0 & 0 \\
0 & G_1 & 0 \\
0 & 0 & G_{v-1}
\end{bmatrix}
\]

is the generator matrix of a \([n^\text{ex}_q(s_{k_u} + 1, \ldots, s_{k_{u+1}}), k] \) code with separation vector \( s \).

**Corollary:** For any prime power \( q \), \( k \in \mathbb{N} \) and \( s \in \mathbb{N}^k \) we have

\[
\begin{align*}
    n^\text{ex}_q(s) &\leq \sum_{i=1}^{k} s_i. \\
    \text{(18)}
\end{align*}
\]

**Proof:** Apply Theorem (3.2.1) with \( v = k \) and for \( i = 1, \ldots, k \), \( k_i = i \) and \( G_i \) the \( 1 \times s_i \) all-one matrix.

Hence for any \( s \in \mathbb{N}^k \) it is possible to construct a \( k \)-dimensional code over \( \mathbb{F}_q \) with separation vector \( s \).
3.3 Lower bounds

We start with a trivial lower bound on \( n_q(s) \).

(3.3.1) **Theorem:** For any \( k \in \mathbb{N} \), prime power \( q \) and nonincreasing \( k \)-vector \( s \in \mathbb{N}^k \), \( n_q(s) \) satisfies the inequality

\[
 n_q(s) \geq 1 + n_q(s_1-1, s_2-1, \ldots, s_k-1). \tag{19}
\]

**Proof:** By deleting a column from a \( k \) by \( n_q(s) \) matrix \( G \) with separation vector \( \overline{s}(G) = (s_1, \ldots, s_k) \) we obtain a \( k \) by \( n_q(s) - 1 \) matrix \( G' \) with separation vector \( \overline{s}(G') = (s_1-1, s_2-1, \ldots, s_k-1) \).

(3.3.2) **Theorem:** For \( q = 2 \) and any \( k \in \mathbb{N} \), \((s_1, \ldots, s_k) \in \mathbb{N}^k \) we have

\[
 n_2(s_1, s_2, \ldots, s_k) \geq n_2(2\left\lfloor \frac{s_1+1}{2} \right\rfloor, 2\left\lfloor \frac{s_2+1}{2} \right\rfloor, \ldots, 2\left\lfloor \frac{s_k+1}{2} \right\rfloor) - 1. \tag{20}
\]

The same inequality holds when we replace \( n_2(.) \) by \( n^\text{ex}_2(.) \).

**Proof:** By adding an overall parity-check to a binary \([n = n_2(s_1, \ldots, s_k), k] \) code with a separation vector of at least \((s_1, \ldots, s_k) \), we obtain an \([n+1, k] \) code with a separation vector of at least \((2\left\lfloor (s_1+1)/2 \right\rfloor, 2\left\lfloor (s_2+1)/2 \right\rfloor, \ldots, 2\left\lfloor (s_k+1)/2 \right\rfloor) \).

(3.3.3) **Example:** \( n_2(5, 4, 3) = 8 \), \( n_2(6, 4, 4) = 9 \) (cf. Appendix A).

(3.3.4) **Theorem:** For a linear \([n, k] \) code over \( \mathbb{F}_q \) with nonincreasing separation vector \( s \) the weight distribution \( \left( A_i \right)_{i=0}^n \) must satisfy the inequality

\[
 \sum_{i \geq s_j} A_i \geq q^k - q^{k-j}. \tag{21}
\]

for all \( j = 1, \ldots, k \).

**Proof:** For any \( j \in \{1, \ldots, k\} \) a codeword corresponding to a message \( m \in \mathbb{F}_q^k \) such that \( m_i \neq 0 \) for some \( i \in \{1, \ldots, j\} \) has a weight of at least \( s_j \).
The weight distribution \((A_i)_{i=0}^{n}\) of a linear \([n,k,s]\) code also has to satisfy the following conditions.

(i): \(A_0 = 1; A_i = 0\) for \(i = 1,\ldots,s_k-1\); \(\sum_{i=0}^{n} A_i = q^k\)

and

(ii): \(\sum_{i=0}^{n} p_m(i;n)A_i \geq 0\) for \(m = 0,1,\ldots,n\),

where \(p_m(x;n)\) are the so-called Krawtchouk polynomials defined by

\[
p_m(x;n) := \sum_{j=0}^{m} (-1)^j (q-1)^{k-j} \binom{n-x}{j} \binom{n-x}{m-j}.
\]  

(22)

for \(m = 0,1,\ldots,n\) and \(x \in \mathbb{R}\) (cf. MacWilliams and Sloane (1978), Ch. 5 Theorem 6).

Combining the conditions (i) and (ii) with formula (21) we obtain a set of inequalities for the weight distribution of a code and hence a necessary condition on the existence of certain linear UEP codes. In many cases we can even add more conditions on \((A_i)_{i=0}^{n}\).

(3.3.5) Example: The weight distribution \((A_i)_{i=0}^{9}\) of a \([9,5,(4,4,4,3,3)]\) binary code has to satisfy

\[
A_0 = 1, A_1 = A_2 = 0, A_3 = 2, A_i \in \mathbb{N} \text{ for } i = 4,\ldots,9,
\]

\[
A_4 + A_5 + A_6 = 15, A_5 + A_7 + A_9 = 14,
\]

and formula (22) for \(m = 1,2,6,7\), i.e.

\[
\begin{align*}
A_4 - A_5 - 3A_6 - 5A_7 - 7A_8 - 9A_9 & \geq -15 \\
-A_4 - A_5 + 2A_7 + 10A_8 + 9A_9 & \geq -9 \\
-A_4 - A_5 + 2A_6 - 7A_8 + 21A_9 & \geq -25 \\
-A_4 + A_5 - 2A_7 + 10A_8 - 9A_9 & \geq -9.
\end{align*}
\]

It is easy to verify that this has no solution and hence a \([9,5,(4,4,4,3,3)]\) binary code does not exist.

(3.3.6) Theorem: For any \(k \in \mathbb{N}\), any prime power \(q\) and any nonincreasing \(k\)-vector \(s \in \mathbb{N}^k\) we have

\[
n_q(s_1,s_2,\ldots,s_k) \geq 1 + n_q(s_1,s_2,\ldots,s_{k-1}).
\]  

(23)
Proof: By deleting the column \( e_k := (0,0,\ldots,0,1)^T \) and the \( k \)th row of an optimal canonical generator matrix of a linear \([n=n_q(s_1,\ldots,s_k),k]\) code over \( \mathbb{F}_q \) with a separation vector of at least \( s \), we obtain a generator matrix of an \([n-1,k-1]\) code with a separation vector of at least \((s_1,s_2,\ldots,s_{k-1})\).

(3.3.7) Corollary: For any \( k,j \in \mathbb{N}, 1 \leq j \leq k \), prime power \( q \) and nonincreasing \( k \)-vector \( s \in \mathbb{N}^k \) we have

\[
n_q(s_1, s_2, \ldots, s_k) \geq j + n_q(s_1, s_2, \ldots, s_{k-j}).
\]

(3.3.8) Corollary: For any \( k \in \mathbb{N} \), prime power \( q \) and nonincreasing \( k \)-vector \( s \in \mathbb{N}^k \) we have

\[
n_q(s_1, s_2, \ldots, s_k) \geq s_1 + k - 1.
\]

For \( s_1 = s_2 = \ldots = s_k \), Corollary (3.3.8) reduces to the Singleton Bound (cf. MacWilliams and Sloane (1978), Ch. I Theorem 11). By this last corollary we see that in a Maximum-Distance-Separable Code all information positions have the maximal protection level which is possible, i.e. \( \lfloor (n-k+1)/2 \rfloor \).

(3.3.9) Example:
\[
n_2(6,6,4,4,4) \geq n_2(6,6,4,4) + 1 = 12.
\]
\[
n_2(6,6,4,4,4) \geq n_2(6,6) + 3 = 12.
\]
Actually \( n_2(6,6,4,4,4) = 12 \) (cf. Appendix A).

(3.3.10) Theorem: For \( k,v \in \mathbb{N} \) and a nonincreasing \( k \)-vector \( s \in \mathbb{N}^k \) such that \( s_{v-1} > s_v \) and \( \sum_{i=v}^{k} s_i \leq n_{q_{ex}}(s) - 1 \) we must have

\[
n_{q_{ex}}(s_1, \ldots, s_k) \geq n_q(s_1-1, \ldots, s_{v-1}-1, s_v, \ldots, s_k) + 1.
\]

Proof: Let \( k,v \in \mathbb{N} \) and \( s \in \mathbb{N}^k \) be such that \( s_{v-1} > s_v \) and \( \sum_{i=v}^{k} s_i \leq n_{q_{ex}}(s) - 1 \) and let \( G \) be a minimal weight generator matrix of an \([n=n_{q_{ex}}(s),k,s]\) code over \( \mathbb{F}_q \). Since \( \sum_{i=v}^{k} s_i \leq n - 1 \), \( G \) has a column containing zero elements in the last \( k - v + 1 \) positions. Deleting this column from \( G \) we obtain an \((n-1)\) by \( k \) matrix \( G' \), whose separation vector satisfies \( s(G') \geq (s_1-1, \ldots, s_{v-1}-1, s_v, \ldots, s_k) \), since \( s_{v-1} > s_v \).
(3.3.11) Example: A binary linear code with separation vector $(6,4,4,3,3,3,3)$ has a length of at least 13. Hence by Theorem (3.3.10), $n^\text{ex}_2(6,4,4,3,3,3,3) \geq n_2(5,3,3,3,3,3,3) + 1 \geq 14$ (cf. Appendix A).

(3.3.12) Theorem: For any $k \in \mathbb{N}$, prime power $q$ and any nonincreasing $k$-vector $\underline{s} \in \mathbb{N}^k$ we have

$$n^\text{ex}_q(s_1, \ldots, s_k) \geq s_i + n_q(s_1, \ldots, \hat{s}_{i-1}, s_{i+1}, \ldots, s_k) \quad (27)$$

for any $i \in \{1, \ldots, k\}$, where

$$\hat{s}_j := \begin{cases} s_j - \left\lfloor \frac{(q-1)s_i}{q} \right\rfloor & \text{for } j < i \\ \frac{s_j}{q} & \text{for } j > i. \end{cases} \quad (28)$$

Proof: Let $C$ be a linear $[n^\text{ex}(s), k, \underline{s}]$ code over $\mathbb{F}_q$ and let $G$ be a minimal weight generator matrix for $C$. By Lemma (2.2.2), $\text{wt}(G_{i*}) = s_i$ for all $i = 1, \ldots, k$.

Fix $i \in \{1, \ldots, k\}$. Without loss of generality the first $s_i$ columns of $G$ have a 1 in the $i$th row. Deleting these first $s_i$ columns and the $i$th row from $G$, we obtain a $(k-1)$ by $(n-s_i)$ matrix, $\hat{G}$. Clearly $\hat{G}$ has rank $(k-1)$, otherwise there would be a nonzero linear combination of rows of $G$ which equals 0, and hence the corresponding linear combination of rows of $\hat{G}$

would have a distance less than $s_i$ to $\alpha \hat{G}_{i*}$ for some $\alpha \in \mathbb{F}_q \setminus \{0\}$, a contradiction. Hence $\hat{G}$ is a generator matrix of an $[n-s_i, k-1]$ code with a separation vector $\hat{\underline{s}} := \underline{s}(\hat{G}) = (\hat{s}_1, \ldots, \hat{s}_{i-1}, \hat{s}_{i+1}, \ldots, \hat{s}_k)$.

Let $j \in \{1, \ldots, k\}$, $j \neq i$ and let $m \in \mathbb{F}_q^k$ be such that $m_i = 0$, $m_j \neq 0$ and $\underline{c} := mG = (c_1 | c_2)$, where $c_1$ has length $s_i$, satisfies $\text{wt}(c_1) = \hat{s}_j$. Since $m_j \neq 0$, we have that

$$\text{wt}(c_1) + \hat{s}_j \geq s_j. \quad (29)$$

Furthermore, for some $\alpha \in \mathbb{F}_q \setminus \{0\}$ at least $\left\lceil \text{wt}(c_1)/(q-1) \right\rceil$ components of $\alpha c_1$ equal 1, and hence

$$\text{wt}(G_{i*} - \alpha \underline{c}) \leq s_i - \left\lceil \text{wt}(c_1)/(q-1) \right\rceil + \hat{s}_j. \quad (30)$$

On the other hand we have that
\[ \text{wt}(G_{k^*}) = \max \{s_i, s_j \}. \]  

(31)

Combining (29), (30) and (31) gives formula (28), and hence (27) holds.

(3.3.13) **Lemma:** For any \( k \in \mathbb{N} \), prime power \( q \) and any nonincreasing \( k \)-vector \( s \in \mathbb{N}^k \) a linear \([n_q(s), k]\) code with a nonincreasing separation vector \( s^* \) such that \( s \leq s^* \leq s_1 \) exists. (\( s_1 \) is the all-one vector of length \( k \)).

**Proof:** Let \( G \) be a minimal weight generator matrix of an \([n=n_q(s), k]\) code. If \( s(G)_1 > s_1 \) then replace a nonzero element in the first row of \( G \) by zero, to obtain a matrix \( G' \) whose separation vector satisfies \( s(G') \geq s \) and \( s(G')_1 = s_1 - 1 \). We can repeat this procedure until we obtain an \( k \times n \) matrix \( G^* \) with \( s \leq s(G^*) \leq s_1 \).

Combining (3.3.12) and (3.3.13) gives the following corollary.

(3.3.14) **Corollary:** For any \( k \in \mathbb{N} \), prime power \( q \) and nonincreasing \( k \)-vector \( s \in \mathbb{N}^k \), \( n_q(s) \) satisfies the inequalities

\[ n_q(s_1, \ldots, s_k) \geq s_1 + n_q\left(\left\lfloor \frac{s_2}{q} \right\rfloor, \ldots, \left\lfloor \frac{s_k}{q} \right\rfloor\right), \]

(32)

\[ n_q(s_1, \ldots, s_k) \geq \sum_{i=1}^{k} \left\lfloor \frac{s_i}{q^{i-1}} \right\rfloor. \]

(33)

**Proof:** According to Lemma (3.3.13), \( n_q(s) = n_{q^e}(s') \) for some \( s \leq s' \leq s_1 \) and hence by Theorem (3.3.12) we have that \( n_q(s) = n_{q^e}(s') \geq s_1 + n_q\left(\left\lfloor \frac{s_2}{q} \right\rfloor, \ldots, \left\lfloor \frac{s_k}{q} \right\rfloor\right) \). Repeating this gives formula (33).

For \( s_1 = s_2 = \ldots = s_k \), Corollary (3.3.14) reduces to the Griesmer Bound (cf. MacWilliams and Sloane (1978), Ch. 17 Theorem 24). Deleting the \( \left\lfloor \right\rfloor \) brackets in formula (33) we obtain an analog of the Plotkin Bound (cf. MacWilliams and Sloane (1978), Ch. 2 Theorem 1) for linear UEP codes.

Lemma (3.3.13) also implies the following corollary.

(3.3.15) **Corollary:** For any \( k \in \mathbb{N} \), prime power \( q \) and any nonincreasing \( k \)-vector \( s \in \mathbb{N}^k \) we have
This corollary allows us to use the bounds on $n_{q_{\text{ex}}}(.)$ to obtain bounds on $n_{q_{\text{s}}}(.)$.

(3.3.16) Examples:

(i): What is the minimum length of a binary linear code with a separation vector of at least $(5, 4, 3, 3, 3, 3)$?

By Theorem (3.3.15) we have

$$n_{2}(5, 4, 3, 3, 3, 3) = \min \{ n_{2}^{\text{ex}}(s) \mid (5, 4, 3, 3, 3, 3) \leq s \leq (5, 5, 5, 5, 5) \}.$$ 

By (3.3.12), $n_{2}^{\text{ex}}(s) \geq 3 + n_{2}(4, 3, 2, 2, 2) = 12$ for $(5, 4, 3, 3, 3, 3) \leq s \leq (5, 5, 5, 5, 5, 5)$. 

By (3.3.1), $n_{2}^{\text{ex}}(5, 4, 4, 4, 4, 4) \geq n_{2}(4, 3, 3, 3, 3, 3) = 12$. 

By (3.3.12), $n_{2}^{\text{ex}}(s) \geq 5 + n_{2}(3, 2, 2, 2, 2) = 12$ for $(5, 5, 3, 3, 3, 3) \leq s \leq (5, 5, 5, 5, 5, 5)$. 

For values of $n_{2}(.)$ see Appendix A.

Hence $n_{2}(5, 4, 3, 3, 3, 3) \geq 12$. A $[12, 6, (5, 5, 4, 4, 4, 4)]$ code exists, so $n_{2}(5, 4, 3, 3, 3, 3) = 12$.

(ii): What is the minimum length of a binary linear code with a separation vector of at least $(6, 6, 6, 5, 5)$?

By Theorem (3.3.15) we have

$$n_{2}(6, 6, 6, 5, 5) = \min \{ n_{2}^{\text{ex}}(s) \mid (6, 6, 6, 5, 5) \leq s \leq (6, 6, 6, 6, 6) \}.$$ 

By (3.3.10), $n_{2}^{\text{ex}}(6, 6, 6, 5, 5) \geq n_{2}(5, 5, 5, 5, 5) = 14$. 

By (3.3.10), $n_{2}^{\text{ex}}(6, 6, 6, 5) \geq n_{2}(5, 5, 5, 5, 5) = 14$. 

$n_{2}^{\text{ex}}(6, 6, 6, 6) = 14$ (cf. Helgert and Stinaff (1973)). 

Hence $n_{2}(6, 6, 6, 5, 5) = 14$.

The separation vectors of all optimal binary linear UEP codes of length less than or equal to 15 are listed in Table A.1 of Appendix A.

3.4 Notes

Katsman (1980) has shown Corollary (3.3.14) for $q = 2$. In many cases a combination of Corollary (3.3.15) and the bounds on $n_{q_{\text{ex}}}(.)$ give better results than Corollary (3.3.14). For instance, compare the results of Corollary (3.3.14) for $n_{2}(5, 4, 3, 3, 3, 3)$ and $n_{2}(6, 6, 6, 5, 5)$ with those obtained in Example (3.3.16):
Another interesting fact is to observe that Theorem (3.3.12) gives better results than the bound of Katsman (cf. Katsman (1980)), i.e. Theorem (3.3.12) for \( i = 1 \) and \( q = 2 \). For example, Theorem (3.3.12) gives

\[
\begin{align*}
\text{ex}_2(n,6,6,3,3,3,3,3) &\geq 6 + n_2(3,2,2,2,2,2) = 14 \\
\text{ex}_2(n,6,6,6,5,5,5,5) &\geq 3 + n_2(5,5,2,2,2) = 15
\end{align*}
\]

A nonlinear \((n,q^k,s)\) UEP code also satisfies

\[
n \geq \sum_{i=1}^{k} s_i / q^{i-1}
\]

This can be proven by generalizing the proof of the Plotkin bound for nonlinear codes (cf. MacWilliams and Sloane (1978), Ch. 2 Theorem 1).
4. CONSTRUCTIONS OF LINEAR UNEQUAL ERROR PROTECTION CODES

In this chapter we give some constructions of LUEP codes. In Section 4.1 we construct certain families of (length-) optimal LUEP codes and in Section 4.2 we describe methods for combining codes to obtain LUEP codes of larger length.

4.1 Certain families of codes

By trying to construct LUEP codes with the parameters given in Table A.1 (cf. Appendix A), that are binary optimal LUEP codes of small length, the following classes of binary codes came up (the empty entries should be read as zeros).

(4.1.1) Construction: For \( k \in \mathbb{N}, \)

\[
\begin{bmatrix}
11 \ldots 11 \\
111111 \\
1111 \\
111
\end{bmatrix}
\]

is a generator matrix of an optimal binary \([k+10,3,(k+6,6,4)]\) code.

Proof: It is easy to check that the code has separation vector \((k+6,6,4)\). Furthermore by formula (32) and Table A.1 we have \( n_2(k+6,6,4) \geq k+6+n_2(3,2) = k+10 \) and \( n_2(s) > k+10 \) for \( s \geq (k+6,6,4), s \neq (k+6,6,4) \) (by \( s \geq t \) we mean, as before, \( s_i \geq t_i \) for all \( i \)).

(4.1.2) Construction: For \( k \in \mathbb{N}, \)

\[
\begin{bmatrix}
11 \ldots 11 \\
111111 \\
1111 \\
111
\end{bmatrix}
\]

is a generator matrix of an optimal binary \([k+13,3,(k+8,8,4)]\) code.
Proof: It is easy to check that the code has separation vector $(k+8,8,4)$. Furthermore by formula (32) and Table A.1 we have $n_2(k+8,8,4) \geq k+8+n_2(4,2) = k+13$ and $n_2(s) > k+13$ for $s \geq (k+8,8,4)$, $s \neq (k+8,8,4)$.

**Construction (4.1.3)**: For $k \in \mathbb{N}$,

$$
\begin{bmatrix}
1 & \ldots & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{bmatrix}
$$

(38)

is a generator matrix of an optimal binary $[k+14,3,(k+8,8,8)]$ code.

Proof: It is easy to check the parameters of the code. Furthermore by formula (32) and Table A.1 we have $n_2(k+8,8,8) \geq k+8+n_2(4,4) = k+14$ and $n_2(s) > k+14$ for $s \geq (k+8,8,8)$, $s \neq (k+8,8,8)$.

**Construction (4.1.4)**: For $n,k \in \mathbb{N}$, $n \geq k+1$, the $k$ by $n$ matrix

$$
\begin{bmatrix}
I_k & 1 & 1 & \ldots & 1 \\
1 & \vdots & \ddots & \ddots & \vdots \\
1 & 1 & \ldots & 1 & 1 \\
\end{bmatrix}
$$

(39)

is a generator matrix of an optimal binary $[n,k,(n-k+1,2,2,\ldots,2)]$ code.

Proof: It is easy to check that the parameters of the code are correct. Furthermore by formula (32) we have that the length of a $k$-dimensional binary code with separation vector $(n-k+1,2,2,\ldots,2)$ is at least $n$, and with a separation vector larger than $(n-k+1,2,2,\ldots,2)$ is at least $n+1$ (by $s > t$ we mean $s \geq t$ and $s \neq t$).

**Construction (4.1.5)**: For $n,k \in \mathbb{N}$, $n \geq 2k+1$, the $k$ by $n$ matrix

$$
\begin{bmatrix}
I_{k-1} & I_{k-1} & \ldots & I_{k-1} & 1 \\
1 & 1 & \ldots & 1 & 1 \\
\end{bmatrix}
$$

(40)

is a generator matrix of an binary optimal $[n,k,(n-k,4,4,\ldots,4)]$ code.
Proof: It is easy to check that the parameters of the code are correct. By formula (32) we have that the length of a \( k \)-dimensional binary code with separation vector \((n-k,4,4,\ldots,4)\) is at least \( n \), and with a separation vector larger than \((n-k,4,4,\ldots,4)\) is at least \( n+1 \).

(4.1.6) Construction: for \( k \in \mathbb{N} \),

\[
\begin{bmatrix}
1 & \cdots & 1 \\
I_{k-1} & I_{k-1} & \vdots \\
& & 1
\end{bmatrix}
\]

is a generator matrix of an optimal binary \([2k-1,k,(k-1,3,3,\ldots,3)]\) code.

Proof: It is easy to verify that the parameters of the code are correct. By formula (32) we have that the length of a \( k \)-dimensional binary code with separation vector \((k-1,3,3,\ldots,3)\) is at least \( 2k-1 \).

Applying formula (32) for a \( k \)-vector \( \mathbf{s} \) such that \( s_1 \geq k \) and \( s_i \geq 3 \) for \( i = 2, \ldots, k \) shows that \( n_2(\mathbf{s}) \geq 2k \).

Applying Theorem (3.3.12) and formula (32) for a \( k \)-vector \( \mathbf{s} \) such that \( s_1 = k-1, s_2 \geq 4, s_i \geq 3 \) for \( i = 3, \ldots, k-1 \), and \( s_k = 3 \) shows that

\[
n_2^{ex}(\mathbf{s}) \geq 3 + n_2(s_1-1, \ldots, s_{k-1}-1) \\
\geq 3 + s_1 - 1 + n_2\left(\left\lceil \frac{(s_1-1)}{2}\right\rceil, \ldots, \left\lceil \frac{(s_{k-1}-1)}{2}\right\rceil\right) \\
\geq 3 + k-2 + n_2(2,1,1,\ldots,1) \\
\geq 3 + k-2 + k-1 = 2k.
\]

Furthermore it is easy to check that a binary \([2k-1,k,(k-1,4,4,\ldots,4)]\) code does not exist.

Finally, the length of a \( k \)-dimensional binary code with a separation vector of at least \((k-1,5,6,\ldots,4)\) is at least \( 2k \).

These observations show that the code in (4.1.6) is optimal.
(4.1.7) Construction: For $k \in \mathbb{N}$,

\[
\begin{bmatrix}
1 & 1 & 1 & \cdots & 1 & 1 & I_{k-1} \\
1 & 1 & 1 & \cdots & 1 & 1 & I_{k-1} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
1 & 1 & 1 & \cdots & 1 & 1 & I_{k-1} \\
1 & 1 & 1 & \cdots & 1 & 1 & I_{k-1} \\
\end{bmatrix}
\]

(42)

is a generator matrix of a binary $[4k,2k,(k+2,k+2,4,4,\ldots,4)]$ code.

For $k = 2,3$ the codes in (4.1.7) are optimal (cf. Table A.1), but in general they are not.

(4.1.8) Construction: For $k \in \mathbb{N}, k \geq 3$,

\[
\begin{bmatrix}
1 & 1 & 1 & \cdots & 1 & 1 & I_k \\
1 & 1 & 1 & \cdots & 1 & 1 & I_k \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
1 & 1 & 1 & \cdots & 1 & 1 & I_k \\
1 & 1 & 1 & \cdots & 1 & 1 & I_k \\
\end{bmatrix}
\]

(43)

is a generator matrix of a length-optimal binary $[4k+1,k+2,(2k,2k,5,5,\ldots,5)]$ code.

Proof: It is easy to check that the code has the given parameters.
By formula (33) the length of a code with dimension $k+2$ and separation vector $(2k,2k,5,5,\ldots,5)$ is at least $4k+1$.

(4.1.9) Construction: For $k,m \in \mathbb{N}$,

\[
\begin{bmatrix}
1 & 1 & 1 & \cdots & 1 & 1 & \cdots & 1 \\
1 & 1 & 1 & \cdots & 1 & 1 & \cdots & 1 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
1 & 1 & 1 & \cdots & 1 & 1 & \cdots & 1 \\
1 & 1 & 1 & \cdots & 1 & 1 & \cdots & 1 \\
\end{bmatrix}
\]

(44)
is a generator matrix of an optimal binary $[3k+2m+3,k+m+2,(k+m+2,2k+2,4,4,\ldots,4)]$ code.

Proof: It is easy to verify that the code has the given parameters. Furthermore by formula (33) we have that the length of a $(k+m+2)$-dimensional binary code with separation vector $(k+m+2,2k+2,4,4,\ldots,4)$ is at least $3k+2m+3$, and with a separation vector larger than $(k+m+2,2k+2,4,4,\ldots,4)$ is at least $3k+2m+4$.

4.2 Combining codes

In this section we consider constructions which combine (LUEP) codes to obtain LUEP codes of larger length, such as the direct sum and direct product construction, the $|u|u+v|$ construction, and concatenation.

(4.2.1) Construction: For $k,m,n \in \mathbb{N}$, and a nonincreasing $k$-vector $s \in \mathbb{N}^k$ such that $s_1 \leq n/2$ let $G_1$ be an optimal generator matrix of a binary $[n,k,s]$ code $C_1$, and for $i = 0,1,\ldots,2^m-1$ let $A_i$ be an $m$ by $n$ matrix whose columns are all equal to the binary representation of $i$, i.e. $\sum_{u=1}^{2^m} (A_i^u)_v 2^u = i$ for all $v = 1,\ldots,n$. Then the $(m+k)$ by $n2^m$ matrix

$$ G_2 := \begin{bmatrix} A_0 & A_1 & A_2 & \cdots & A_{2^m-1} \\ G_1 & G_1 & G_1 & \cdots & G_1 \end{bmatrix} $$

is a generator matrix of a binary $[n2^m,m+k,(n2^m-1,2^m,s)]$ code $C_2$. If $C_1$ is optimal, so is $C_2$.

Proof: It is easy to check that the parameters of the code $C_2$ are correct. Suppose that $C_1$ is optimal. Then by formula (32) the length of a $(k+m)$-dimensional binary code with separation vector $(n2^m-1,2^m,s)$ is at least $n(2^m-1)+n_2(s_1,\ldots,s_k) = n2^m$ and with a separation vector larger than $(n2^m-1,2^m,s)$ is at least $n2^m+1$. 

(4.2.2) Examples:

(i): If in (4.2.1) we take $m = 1$ and for $G_1$ a generator matrix of a binary $[2^t-1,2^t-t-1,(3,3,\ldots,3)]$ Hamming code, then $G_2$ is a generator matrix
of an optimal \([2^{t+1}-2, 2^t-t, (2^t-1, 6, 6, \ldots, 6)]\) binary code.

(ii): If in \((4.2.1)\) we take \(m = 1\) and for \(G_1\) an optimal generator matrix of an optimal binary \([7, 5, (3, 2, 2, 2, 2)]\) code, then we obtain an optimal \([14, 6, (7, 6, 4, 4, 4, 4)]\) code.

\((4.2.3)\) The direct sum construction: If for \(i = 1, 2\), \(C_i\) is an \([n_i, k_i, s_i^{(i)}]\) linear code, then the direct sum \(\{ (c_1 | c_2) \mid c_1 \in C_1, c_2 \in C_2 \}\) is an \([n_1+n_2, k_1+k_2, s^{(1)}_{\text{min}} | s^{(2)}_{\text{min}}]\) linear code.

\((4.2.4)\) The \(u | u+v\) construction: If for \(i = 1, 2\), \(C_i\) is an \([n_i, k_i, s_i^{(i)}]\) linear code with an optimal generator matrix \(G_i\), then

\[
G := \begin{bmatrix}
G_1 & G_1 \\
G_2 & 0
\end{bmatrix}
\]  

is a generator matrix of a \([2n, k_1+k_2, s]\) code \(C\), where

\[
s_i \geq \min \{ 2s_i^{(1)}, \max \{ s_i^{(1)}, s_k^{(2)} \} \} \text{ for } i = 1, \ldots, k_1,
\]

and

\[
s_{k_1+i} \geq s_{i}^{(2)} \text{ for } i = 1, \ldots, k_2
\]

\((s\) is not necessarily nonincreasing in this case).

**Proof:** For \(m^{(1)} \in \mathbb{F}_q^{k_1}, m^{(2)} \in \mathbb{F}_q^{k_2}, m = (m^{(1)} | m^{(2)})\) we have for \(i = 1, \ldots, k_1\) that

\[
\text{wt}(mG) \geq 2s_i^{(1)} \text{ if } m_i^{(1)} \neq 0, m_i^{(2)} = 0,
\]

\[
\text{wt}(mG) \geq \max \{ s_i^{(1)}, s_{k_2}^{(2)} \} \text{ if } m_i^{(1)} \neq 0, m_i^{(2)} \neq 0,
\]

and for \(j = 1, \ldots, k_2\) that

\[
\text{wt}(mG) \geq s_j^{(2)} \text{ if } m_j^{(1)} = 0, m_j^{(2)} \neq 0,
\]

\[
\text{wt}(mG) \geq \max \{ s_j^{(2)}, s_{k_1}^{(1)} \} \text{ if } m_j^{(1)} \neq 0, m_j^{(2)} \neq 0.
\]

This proves formula \((47)\).\(\square\)
(4.2.5) Example: If in (4.2.5) \( C_1 \) is the binary [13,12] even-weight code and \( C_2 \) is a binary [13,6,(5,5,5,5,4,4)] code, then \( s(G)_i \geq 4 \) for \( i = 1, \ldots, 12 \) and \( i = 17, 18 \), and \( s(G)_i \geq 5 \) for \( i = 13, 14, 15, 16 \). Now \( C \) is a [26,18,(5,5,5,5,4,4)] code. The length of an 18-dimensional binary code with a separation vector of at least \((5,5,5,5,4,4,\ldots,4)\) is at least 25 (by Corollary (3.3.14)).

(4.2.6) Construction: If for \( i = 1, 2 \), \( X_i \) is a \( k_i \times n_i \)-matrix over \( \mathbb{F}_q \) and \((u|v)\), where \( u \) is a \( k_i \)-vector, is the separation vector of the matrix \((X_1^T X_2^T)\), and \( Y \) is a \( k_1 \times n_2 \)-matrix over \( \mathbb{F}_q \) with separation vector \( w \), then

\[
\begin{bmatrix}
X_1 & Y \\
X_2
\end{bmatrix}
\]

is a generator matrix of an \([n_1+n_2,k_1+k_2,(s_1^{(1)}|s_2^{(2)})]\) code, where

\[
s_1^{(1)} \geq u + w \quad \text{and} \quad s_2^{(2)} \geq v.
\]

Proof: Trivial.

(4.2.7) Example: If \( G_1 \) is a 5 x 12 binary matrix such that \( s(G_1) = (5,5,5,5,4) \) and \( G_2 \) is a 2 x 3 binary matrix such that \( s(G_2) = (2,2) \), then

\[
\begin{bmatrix}
G_1 & G_2 \\
& 0
\end{bmatrix}
\]

is a generator matrix of a length-optimal (cf. Table A.1) binary \([15,5,(7,7,5,5,4)]\) code.

(4.2.8) The direct product construction: By taking the direct product (cf. MacWilliams and Sloane (1978), Ch. 18 Section 2) of an \([n_1,k_1,s_1]\) code and an \([n_2,k_2,s_2]\) code, both over the same field, we obtain an \([n_1n_2,k_1k_2,s_1+s_2]\) code, where \( \otimes \mathbb{R} \) denotes the Kronecker product over \( \mathbb{R} \). This is shown by the following two theorems.

(4.2.9) Theorem: For the matrices \( A \) and \( B \) over a common finite field \( \mathbb{F} \) the separation vector of the Kronecker product of \( A \) and \( B \), \( A \otimes \mathbb{F} B \), equals the Kronecker product of the separation vectors of \( A \) and \( B \), i.e.
\[ s(A \otimes_F B) = s(A) \otimes_R s(B). \]  

(50)

Proof: Let \( A \) be a \( k_1 \) by \( n_1 \) matrix and let \( B \) be a \( k_2 \) by \( n_2 \) matrix. Let \((i,j) \in \{1,\ldots,k_1\} \times \{1,\ldots,k_2\} \). For any \( k_1 \) by \( k_2 \) matrix \( M \) over \( \mathbb{F} \) such that \( M_{ij} \neq 0 \) we have \( \text{wt}((MB)^*_{ij}) \geq s(B)_j \), and hence

\[ \sum_{u=1}^{n_1} \text{wt}((AMB)^*_{uj}) \geq s(A)_i s(B)_j. \]

For \( m_1 \in \mathbb{F}^{k_1} \), \( m_2 \in \mathbb{F}^{k_2} \) such that \( m_1_{ij} \neq 0, m_2_{ij} \neq 0 \) and \( \text{wt}(m_1 A) = s(A)_i \), \( \text{wt}(m_2 B) = s(B)_j \) we have that \( (m_1 m_2)^*_{ij} \neq 0 \) and

\[ \sum_{u=1}^{n_1} \text{wt}((A_{m_1}^{T} B_{m_2}^{T})^*_{uj}) = s(A)_i s(B)_j. \]

From these observations it follows that \( A \otimes_F B \) is an optimal generator matrix for its rowspace if and only if \( A \) and \( B \) are both optimal generator matrices for their rowspaces.

(4.2.10) Theorem: For generator matrices \( A \) and \( B \) over a common finite field \( \mathbb{F} \), \( A \otimes_F B \) is an optimal generator matrix for its rowspace if and only if \( A \) and \( B \) are both optimal generator matrices for their rowspaces.

Proof: Suppose \( A \) and \( B \) are optimal generator matrices for their rowspaces. Let \( A \) and \( B \) be minimal weight generator matrices for the rowspaces of \( A \) and \( B \). Hence \( s(A) = \_s(A) = (\text{wt}(A_{1,*}), \ldots, \text{wt}(A_{k,*})) \) and \( s(B) = \_s(B) = (\text{wt}(B_{1,*}), \ldots, \text{wt}(B_{k_*})) \). Furthermore we have that

\[ \sum_{i=1}^{k_1} \text{wt}((A \otimes_F B)^*_{i,*}) = (\sum_{i=1}^{k_1} \text{wt}(A_{i,*}))(\sum_{i=1}^{k_2} \text{wt}(B_{i,*})). \]

From this it follows that \( A \otimes_F B \) is a minimal weight generator matrix for its rowspace and so by Theorem (2.2.4) it is optimal. Since \( s(A \otimes_F B) = \_s(A \otimes_F B) \), \( A \otimes_F B \) is also optimal for its rowspace.

On the other hand suppose that \( A \) is not optimal. Then for an optimal generator matrix \( A' \) of the rowspace of \( A \) we have that \( s(A') \geq s(A) \) and \( s(A') \neq s(A) \). This implies that \( s(A' \otimes_F B) \geq s(A \otimes_F B) \) and \( s(A' \otimes_F B) \neq s(A \otimes_F B) \), i.e. \( A \otimes_F B \) is not optimal for its rowspace.

(4.2.11) Concatenation: Let \( C \) be an \([N,K,S=(S_1,\ldots,S_K)]\) linear code over \( \text{GF}(q^k) \) with an optimal generator matrix \( G_C \) and let \( D \) be an \([n,k,d]\) linear code over \( \text{GF}(q) \) with generator matrix \( G_D \).

The encoding procedure of the concatenation of these codes is as follows.
Let \( \mathbf{m} = (m_1, \ldots, m_K, \ldots, m_1, \ldots, m_K) \) be a \( Kk \)-tuple over \( GF(q) \).

This \( Kk \)-tuple is equivalent with a \( K \)-tuple \( \mathbf{M} = (M(1), \ldots, M(K)) \) over \( GF(q^K) \), which is encoded into \( (A(1), \ldots, A(N)) := (M(1), \ldots, M(K)) \mathbf{C} \).

Now we regard \( A(i) \) as a \( k \)-tuple \( (a_1(i), \ldots, a_k(i)) \) over \( GF(q) \) and encode it into \( (c_1(i), \ldots, c_n(i)) := (a_1(i), \ldots, a_k(i)) \mathbf{D} \) \( (i = 1, \ldots, N) \).

If \( \mathbf{m} \) is a \( q \)-ary \( Kk \)-tuple such that \( m_i \neq 0 \), then \( \mathbf{M} \neq 0 \) and hence \( \mathbf{A} := \mathbf{M} \mathbf{C} \) satisfies \( wt(\mathbf{A}) \geq S_j \), which in turn implies that \( wt(\mathbf{C}) \geq S_j d \).

Hence we have shown the following theorem.

\[
(4.2.12) \text{Theorem: The concatenation of an } [N,K,S=(S_1,\ldots,S_K)] \text{ outer code over } GF(q^K) \text{ and an } [n,k,d] \text{ inner code over } GF(q) \text{ is an } [Nn,Kk,s] \text{ linear code over } GF(q), \text{ where }
\]
\[
s(j-1)k+i \geq dS_j \tag{51}
\]
for \( i = 1, \ldots, k \) and \( j = 1, \ldots, K \).

\[
(4.2.13) \text{Examples: Let } \alpha \text{ be a primitive element of } GF(4) \text{ and } \mathbf{D} \text{ be the binary } [3,2,2] \text{ even-weight code.}
\]

(i): For the optimal \([7,3,(5,4,4)]\) code \( \mathbf{C} \) over \( GF(4) \) with generator matrix

\[
\begin{bmatrix}
1 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & \alpha & \alpha^2 \\
0 & 0 & 1 & 0 & 1 & \alpha^2 & \alpha
\end{bmatrix}
\]

the concatenated code of \( \mathbf{C} \) and \( \mathbf{D} \) is a \([21,6,(10,10,8,8,8,8)]\) binary code. The maximal minimum distance of a binary \([21,6]\) code equals 8 (cf. Helgert and Stinaff (1973)).

(ii): For the optimal \([8,4,(5,4,4,4)]\) code \( \mathbf{C} \) over \( GF(4) \) with generator matrix

\[
\begin{bmatrix}
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 1 & \alpha & \alpha^2 & 0 & 0 \\
0 & 1 & 0 & 1 & \alpha & 0 & \alpha^2 & 0 \\
0 & 0 & 1 & 1 & \alpha & 0 & 0 & \alpha^2
\end{bmatrix}
\]

the concatenated code of \( \mathbf{C} \) and \( \mathbf{D} \) is a \([24,8,(10,10,8,8,8,8,8,8)]\) binary code.
(4.2.14) Theorem: For \( k, K, n, N, d \in \mathbb{N}, N \geq 2^k + 1 \) the concatenation of the \([N, 2, (n-1, 2^k)]\) outer code over \( GF(2^k) \) with generator matrix
\[
\begin{bmatrix}
1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 0 \\
1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{2^k-2} & 0 & 0 & 1
\end{bmatrix}
\]
where \( \alpha \) is a primitive element of \( GF(2^k) \), and an \([n, k, d]\) inner code over \( GF(2) \) gives an \([Nn, 2k, s]\) binary code, where
\[
s_i \geq (N-1)d \quad \text{for } i = 1, \ldots, k,
\]
and
\[
s_i \geq 2^k d \quad \text{for } i = k+1, \ldots, 2k.
\]
If \( n = (2^k-1)d/2^{k-1} \) (i.e. equality in the Plotkin Bound), then equality holds in (53) and the concatenated code is optimal.

Proof: We find formula (53) by applying Theorem (4.2.12). By Corollary (3.3.14) a \( 2k \)-dimensional binary code with a separation vector of at least \( s \), where \( s_i = (N-1)d \) for \( i = 1, \ldots, k \) and \( s_i = 2^k d \) for \( i = k+1, \ldots, 2k \), has a length of at least
\[
\sum_{i=0}^{k-1} \left( \frac{(N-1)d}{2^{i+1}} \right) + \sum_{i=0}^{k-1} \left( \frac{d}{2^{i+1}} \right) \geq Nd(2^k-1)/2^{k-1}.
\]
If \( n = (2^k-1)d/2^{k-1} \) then equality must hold in formula (54) and hence in (53). This also shows that the concatenated code is optimal.

(4.2.15) Example: Take the \([11, 2, (10, 8)]\) code over \( GF(8) \) as the outer code and the \([7, 3, 4]\) simplex code over \( GF(2) \) as the inner code to obtain an optimal \([77, 6, (40, 40, 40, 32, 32, 32)]\) binary code. In general all concatenated codes constructed in Theorem (4.2.14) with the inner code being a simplex code are optimal LUEP codes, because simplex codes satisfy the Plotkin Bound with equality.
4.3 Notes

The Theorems (4.2.9) and (4.2.10) are from Dunning and Robbins (1978). Other methods for combining codes can be found in Zinov'ev and Zyablov (1979), and Boyarinov and Katsman (1981).
5. CYCLIC UNEQUAL ERROR PROTECTION CODES

In this chapter we consider cyclic UEP codes and try to find the separation vector of these codes. In Section 5.1 we give an optimal generator matrix for a cyclic UEP code and we show how the separation vector can be determined from the weight distributions of the cyclic subcodes. Section 5.2 shows that certain classes of cyclic UEP codes can easily be decoded by using Majority Logic Decoding Methods.

5.1 The separation vector of a cyclic UEP code

A cyclic $[n,k]$ code over $\mathbb{F}_q$ is the direct sum of the minimal ideals in $\mathbb{F}_q[x]/(x^n-1)$ contained in it (cf. MacWilliams and Sloane (1978), Ch. 7 and 8).

(5.1.1) Theorem: For a cyclic code $C$ which is the direct sum of the minimal ideals with generator matrices $M_1, M_2, \ldots, M_v$,

$$G := \begin{bmatrix} M_1 \\ \hline M_2 \\ \hline \vdots \\ \hline M_v \end{bmatrix}$$

is an optimal generator matrix.

Proof: For $\rho \in \text{WT}(C)$, $<C(\rho)>$ is a cyclic code. Hence $<C(\rho)>$ is the sum of a number of minimal ideals of $\mathbb{F}_q[x]/(x^n-1)$. By applying Theorem (2.1.3) we get the theorem.

The following corollaries are immediate consequences of Lemma (2.1.2) and the above proof.

(5.1.2) Corollary: For a minimal ideal in $\mathbb{F}_q[x]/(x^n-1)$ all components of the separation vector are mutually equal.
(5.1.3) Corollary: For a cyclic code $C$ with an optimal generator matrix $G$ defined by formula (55) the $i$th and $j$th component of the separation vector $s = s(G)$ are equal if the $i$th and $j$th row of $G$ are in the same minimal ideal of $\mathbb{F}_q[x]/(x^n-1)$.

If the generator polynomial of a cyclic code $C$ has minimal weight, i.e. its weight equals the minimum distance $d$ of the code, then all components of the separation vector are mutually equal, because $C = \langle C(d) \rangle$ (cf. Theorem (2.1.3)). If this is not the case, we can compute the separation vector of a cyclic code by comparing the weight distributions of its cyclic subcodes.

(5.1.4) Theorem: For $i = 1, 2$ let $M_i$ be a minimal ideal in $\mathbb{F}_q[x]/(x^n-1)$ with minimum distance $d_i$ and weight distribution $(A_j^{(i)})_{j=0}^n$ such that $M_1 \neq M_2$ and $d_1 \geq d_2$. Let $(A_j)_{j=0}^n$ be the weight distribution of their direct sum $M_1 \oplus M_2$. Then the components of the separation vector of $M_1 \oplus M_2$ are all equal to the minimum distance $d$ of $M_1 \oplus M_2$ if $d < d_2$ or if $d = d_2$ and $A_d^{(2)} < A_d$; they take two different values if $d = d_2$ and $A_d^{(2)} = A_d$, namely $d_2$ and $\min \{ j \mid A_j^{(2)} < A_j \}$.

Proof: If $d < d_2$ or if $d = d_2$ and $A_d^{(2)} < A_d$ then a sum of an element in $M_1 \setminus \{0\}$ and one in $M_2 \setminus \{0\}$ exists such that its weight equals $d$. For $d = d_2$ and $A_d^{(2)} = A_d$ if $A_j^{(2)} < A_j$ then a sum of an element in $M_1 \setminus \{0\}$ and one in $M_2 \setminus \{0\}$ exists such that its weight equals $j$; if $A_j^{(2)} = A_j$ it does not. Combining these observations with Theorem (5.1.1) and Corollary (5.1.3) proves the theorem.

(5.1.5) Examples:
(i): Let $\alpha \in \text{GF}(2^{10})$ be a primitive $33$rd root of unity and let $C$ be the binary cyclic $[33, 23]$ code with nonzeros $\{ \alpha^i \mid i \in C_{11} \cup C_{12} \cup C_0 \cup C_3 \}$, where $C_i$ denotes the cyclotomic coset modulo 33 over $\text{GF}(2)$ containing $i$. Let $M_i$ denote the minimal ideal in $\mathbb{F}_2[x]/(x^{33} - 1)$ having nonzeros $\{ \alpha^j \mid j \in C_i \}$. Then $C = M_1 \oplus M_2 \oplus M_3$ and $G := \begin{bmatrix} M_1^T & M_2^T & M_3^T \end{bmatrix}^T$ is an optimal generator matrix of $C$, where $M_i$ denotes a generator matrix of $M_i$ $(i = 0, 1, 3, 11)$. $s = s(G)$.

Table 5.1 provides the minimum distances of all cyclic subcodes of $C$ (taken from Peterson and Weldon (1972), Appendix D).
The code $C$ has minimum distance 3 and $C$ and $\mathcal{M}_0 \oplus \mathcal{M}_3$ both contain 11 codewords of weight 3. Combining this with Theorem (5.1.4) and Table 5.1 we find that $s_{13} = s_{14} = \ldots = s_{23} = 3$ and $s_4, s_5, \ldots, s_{12} \geq 3$. $C$ contains no codewords of weight 4 and 165 codewords of weight 5. From Table 5.1 we see that the codewords of weight 5 in $C$ can only occur in the cyclic subcodes (1): $\mathcal{M}_0 \oplus \mathcal{M}_3$, (2): $\mathcal{M}_0 \oplus \mathcal{M}_6$, (3): $\mathcal{M}_0 \oplus \mathcal{M}_3 \oplus \mathcal{M}_7$, and (4): $\mathcal{M}_0 \oplus \mathcal{M}_3 \oplus \mathcal{M}_7$. However, (1), (2), and (3) contain no codewords of weight 5, as one can easily check. Hence a codeword $c$ in $C$ of weight 5 is the sum $\sum c_i \alpha^i$ of nonzero elements $c_i \in \mathcal{M}_i$ ($i = 0, 1, 3, 11$). This shows that $s_1 = s_2 = \ldots = s_{12} = 5$ (by Corollary (5.1.3) and Theorem (5.1.4)).

So the code $C$ provides a protection level 2 to twelve message positions and a protection level 1 to the remaining eleven positions.

(ii): Let $\alpha \in GF(2^{12})$ be a primitive 35th root of unity and let $C$ be the binary cyclic $[35, 22]$ code with nonzeros $\{ \alpha^i \mid i \in \mathcal{C}_5 \cup \mathcal{C}_7 \cup \mathcal{C}_1 \cup \mathcal{C}_{15} \}$. Then $C = \mathcal{M}_5 \oplus \mathcal{M}_7 \oplus \mathcal{M}_1 \oplus \mathcal{M}_{15}$ and $G := [M_5^T M_7^T M_1^T M_{15}^T]^T$ is an optimal generator matrix of $C$. $s_c = s(G)$. The minimum distances of the cyclic subcodes of $C$ are listed in Table 5.2 (cf. Peterson and Weldon (1972), Appendix D).

The cyclic subcodes $\mathcal{M}_1, \mathcal{M}_{15}$ and $\mathcal{M}_1 \oplus \mathcal{M}_{15}$ have minimum distances resp. 8, 20, and 4. Hence by Theorem (5.1.4) we have that $s_8 = s_9 = \ldots = s_{22} = 4$. The number of codewords of weight 4 in $C$ resp. $\mathcal{M}_1 \oplus \mathcal{M}_{15}$ both equal 35 and all weights in $C$ are even, hence $s_4, s_5, \ldots, s_7 \geq 6$. The minimum distance of $\mathcal{M}_1 \oplus \mathcal{M}_7$ equals 6, hence $s_4 = s_5 = s_6 = s_7 = 6$.

<table>
<thead>
<tr>
<th>nonzeros</th>
<th>min. dist.</th>
<th>nonzeros</th>
<th>min. dist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 3 11</td>
<td>33 10</td>
<td>0 1 3 11</td>
<td>3 10</td>
</tr>
<tr>
<td>x</td>
<td>12</td>
<td>x</td>
<td>6</td>
</tr>
<tr>
<td>x</td>
<td>6</td>
<td>x</td>
<td>3</td>
</tr>
<tr>
<td>x</td>
<td>22</td>
<td>x</td>
<td>10</td>
</tr>
<tr>
<td>x x</td>
<td>11</td>
<td>x x x x</td>
<td>3</td>
</tr>
<tr>
<td>x x</td>
<td>3</td>
<td>x x x x</td>
<td>6</td>
</tr>
<tr>
<td>x x</td>
<td>11</td>
<td>x x x x</td>
<td>3</td>
</tr>
<tr>
<td>x x</td>
<td>6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 5.1: The minimum distances of the cyclic subcodes of $C$. 

The code $C$ contains no codewords of weight 4 and 165 codewords of weight 5.
Table 5.2: The minimum distances of the cyclic subcodes of C.

The number of codewords of weight 6 in $C_{15}$ equals 490, while $C$ contains 595 codewords of weight 6, hence $s_1 = s_2 = s_3 = 6$.
So seven components of the separation vector of $C$ equal 6, fifteen of them equal 4.

5.2 Majority Logic Decoding of cyclic UEP codes

In this section we discuss certain classes of cyclic UEP codes which can be decoded by Majority Logic Decoding. It is easy to implement this method and it is very useful whenever the number of orthogonal checks on a message digit equals (or is not much less than) the separation component corresponding to that message position. We restrict ourselves to binary codes.

Fix $n \in \mathbb{N}$, $n$ odd, and let $T_0, T \in \mathbb{N}$ be such that $T_0 < T < n$ and $T_0 | T | n$.
Let $p_i(x), i = 0, 1, \ldots, w$ be irreducible polynomials in $\mathbb{F}_2[x]$ such that $p_0(x)$ has exponent $T_0$ (i.e. the minimal $j$ such that $p_0(x) | x^j+1$) and

$$(x^{n+1}) = \bigotimes_{i=0}^{w} p_i(x).$$

Let $v \leq w$ be such that none of the polynomials $p_i(x), i = 1, 2, \ldots, v-1$ has an exponent which divides $T$ and let $C$ be the code with check polynomial

$$h(x) = \bigotimes_{i=0}^{v-1} p_i(x).$$
Then by Theorem (5.1.1) $G := (M_0^T | M_1^T | \ldots | M_{v-1}^T)^T$, where for $i = 0, 1, \ldots, v-1$ the rows of $M_i$ are the cyclic shifts of $(x^{n+1})/p_i(x)$, is an optimal generator matrix for $C$.

Let $k_i$ denote the degree of $p_i(x)$ for $i = 0, 1, \ldots, v-1$. The $[n,k_0]$ cyclic subcode with check polynomial $p_0(x)$ consists of $n/T_0$ repetitions of the $[T_0, k_0]$ code with generator polynomial $(x^{n+1})/p_0(x)$. Let this $[T_0, k_0]$ code have an orthogonal check set of size $\delta$ on any code position (cf. Cameron and van Lint (1980), Ch. II). For $k_0 = 1$ one has that $T_0 = 1$ and $\delta = 0$. Then the following theorem provides a lower bound on the $k_0$ separation components corresponding to $M_0$ in terms of $T,T_0$, and $\delta$.

(5.2.1) Theorem: The first $k_0$ components of the separation vector of the code defined above are larger than or equal to $T(\delta + 1)/T_0$.

Proof: With a message $m = (m_0, m_1, \ldots, m_{k-1}) \in \mathbb{F}_2^k$ resp. a codeword $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_2^n$ we associate the polynomials $m(x) := \sum_{i=0}^{k-1} m_i x^i$ resp. $c(x) := \sum_{i=0}^{n-1} c_i x^i$. By $C_{x^i}(q(x))$ we denote the coefficient of $x^i \mod n$ in the polynomial $q(x) \mod (x^{n+1})$.

Note the following:

(i): For $j \in \{0, 1, \ldots, T-1\}$ and $q(x) \in \mathbb{F}_2[x]/(x^{n+1})$ we have that

$$\sum_{i=0}^{(n/T)-1} C_{x^{j+iT}}(q(x)) = C_{x^j}(x^{n+1})q(x)/(x^{T+1}).$$

(ii): For $i = 1, 2, \ldots, v-1$ and $u, j \in \mathbb{N}$ we have that

$$C_{x^{j+uT_0}}((x^{n+1})/(x^{T+1}))(x^{n+1}/p_i(x)) = 0,$$

since $p_i(x)(x^{T_0})/(x^{n+1})$.

(iii): For $\lambda(x) = \sum_{i=0}^{T_0-1} \lambda_i x^i := (x^{n+1})/p_0(x)$, $j \in \{0, 1, \ldots, T_0-1\}$ and $u \in \{0, 1, \ldots, (T/T_0)-1\}$ we have that

$$C_{x^{j+uT_0}}((x^{n+1})/(x^{T+1}))(x^{n+1}/p_0(x)) = \lambda_j,$$

since $n/T$ is odd.

Combining (i), (ii), and (iii) with the fact that $\lambda_{T_0-k_0} = \ldots = \lambda_{T_0-1} = 0$ we get for $j = 0, 1, \ldots, T_0-1$ and $u = 0, 1, \ldots, (T/T_0)-1$ that
\[
\sum_{i=0}^{(n/T)-1} c_{iT+uT_0+j}
\]

\[
= \sum_{i=0}^{(n/T)-1} \sum_{t=0}^{k_s-1} m_{k_s-1+t} x^t (x^{n+1}/p_s(x))
\]

\[
= \sum_{s=0}^{\lambda_j} \sum_{t=0}^{k_s-1} m_{k_s-1+t} \sum_{i=0}^{(n/T)-1} c_{iT+uT_0+j} x^t (x^{n+1}/p_s(x))
\]

\[
= \sum_{t=0}^{k_0-1} m_t \sum_{i=0}^{(n/T)-1} c_{iT+uT_0+j} x^t (x^{n+1}/p_0(x))
\]

\[
= \sum_{t=0}^{k_s-1} m_{k_s-1+t} x^t (x^{n+1}/p_s(x))
\]

\[
= \sum_{t=0}^{k_0-1} m_t x^t (x^{n+1}/p_0(x))
\]

\[
= \sum_{t=0}^{k_0-1} m_t \frac{x^t (x^{n+1})}{(x^{n+1})/p_0(x)}
\]

\[
= \sum_{t=0}^{k_0-1} m_t \frac{x^t}{p_0(x)} = \sum_{t=0}^{k_0-1} m_t \lambda_j m_j - t
\]

where \(k_s := 0\).

Hence we have that

\[
\sum_{i=0}^{(n/T)-1} c_{iT+uT_0+j} = \sum_{t=0}^{k_0-1} m_t \lambda_j m_j - t
\]

holds for \(j = 0, 1, \ldots, T_0 - 1\) and \(u = 0, 1, \ldots, (T/T_0) - 1\).

For \(j \in \{0, 1, \ldots, T_0 - 1\}\) the \([T_0, k_0]\) code, \(\Lambda\), with generator polynomial \(\lambda(x)\) has an orthogonal check set of size \(\delta\) on position \(j\). Unlike the usual definition we define these checks to be subsets \(A_1(j), A_2(j), \ldots, A_\delta(j)\) of \(\{0, 1, \ldots, T_0 - 1\}\) which satisfy the following three conditions.

\[
\delta = \bigcup_{r=1}^\delta A_r(j) \subseteq \{0, 1, \ldots, T_0 - 1\}\setminus\{j\},
\]

\[
y_j = \sum_{p \in A_r(j)} y_p \text{ for all } y \in \Lambda \text{ and all } r \in \{1, \ldots, \delta\}.
\]

We define the weight of a check \(A_r(j)\) as the number of elements in \(A_r(j)\).

In an analog way as we have shown formula (59), we can show that the equality
\[ \sum_{i=0}^{(n/T)-1} \sum_{p \in A_r} c_{iT+uT_0+p} = \sum_{t=0}^{\tau} \lambda_t m_{j-t} \quad (63) \]

holds for \( j = 0, 1, \ldots, T_0 - 1 \), \( u = 0, 1, \ldots, (T/T_0) - 1 \), and \( r = 1, \ldots, \delta \), by combining the formulas (56), (57), (59), and (62).

Because \( A_1^{(j)}, \ldots, A_\delta^{(j)} \) satisfy (60) and (61), formulas (59) and (63) provide \( T(\delta+1)/T_0 \) orthogonal checks on \( \sum_{t=0}^{\tau} \lambda_t m_{j-t} \).

The \( k_0 \) linear functions \( \sum_{t=0}^{\tau} \lambda_t m_{j-t} \), \( j = 0, 1, \ldots, k_0 - 1 \) are linearly independent, since \( \lambda_0 = 1 \). Hence the \( k_0 \) message positions corresponding to \( M_0 \) have a separation component of at least \( T(\delta+1)/T_0 \).

\( \square \)

(5.2.2) \textbf{Example:} \( n = 63, T = 21, T_0 = 7, p_0(x) = x^3 + x + 1 \).

\[ h(x) := \bigcap_{i=0}^{6} p_i(x), \]

where \( p_i(x), i = 1, \ldots, 6 \) are the six irreducible factors of \( x^{63} + 1 \) with exponents equal to 63. We have that \( \lambda(x) = 1 + x + x^2 + x^4 \), which is the generator polynomial of a \([7,3]\) code with three orthogonal checks \([1,5], [2,3], \) and \([4,6]\) on code position 0. By Theorem (5.2.1) the \([63,39]\) code with check polynomial \( h(x) \) has a separation vector with three components larger than or equal to 12. This code has minimum distance 4. A \([63,39]\) BCH code has minimum distance 9.

Now consider two irreducible polynomials \( p(x) \) and \( q(x) \) in \( \mathbb{F}_2[x]/(x^{n+1}) \) with degrees resp. \( k_p \) and \( k_q \) and exponents resp. \( T_p \) and \( T_q \) such that \( T_p \) and \( T_q \) are relatively prime. Let \( C_p \) and \( C_q \) be resp. \([T_p, k_p]\) and \([T_q, k_q]\) codes with check polynomials resp. \( p(x) \) and \( q(x) \). Furthermore let \( C_p \) have an orthogonal check set of size \( \delta \) on any code position such that any check has the same even weight, i.e. any code symbol equals the sum of 2w other ones for some fixed integer \( w \).

Define \( C \) to be the binary cyclic \([T_pT_q, k_p+k_q+1]\) code with check polynomial \( p(x)q(x) \) and \( C^* \) the binary cyclic \([T_pT_q, k_p+k_q+1]\) code with check polynomial \( (x+1)p(x)q(x) \). The following theorem provides a lower bound on the separation vector \( s \) and \( s^* \) of resp. \( C \) and \( C^* \) if their encoding is defined by the generator matrices resp. \( G = (M_p^T | M_q^T)^T \) and \( G^* = (M_p^T | M_q^T | M_0^T)^T \), where \( M_p, M_q, M_0 \) are generator matrices of the minimal ideals in \( \mathbb{F}_2[x]/(x^{n+1}) \) with check polynomials resp. \( p(x), q(x), \) and \( (x+1) \).
(5.2.3) **Theorem:**

(i): The separation vector \( s \) of the code \( C \) defined above satisfies

\[
 s_i \geq T \delta_p + 1 \quad \text{if} \quad C \quad \text{is an even-weight code},
\]

\[
 s_i \geq T \delta_p \quad \text{otherwise},
\]

for \( i = 1, \ldots, k \).

(ii): The separation vector \( s^* \) of the code \( C^* \) defined above satisfies

\[
 s^*_i \geq T \delta_p
\]

for \( i = 1, \ldots, k \).

**Proof:**

(i): Without loss of generality we consider the first message digit \( m_0 \).

Let \( G_p \) and \( G_q := \left[ y_1 | y_2 | \ldots | y_{T_q} \right] \) be systematic generator matrices of \( C_p \) resp. \( C_q \). Without loss of generality the first column of \( G_p \) equals \( e_0 := (1,0,0,\ldots,0)^T \).

Since \( C_p \) has an orthogonal check set of size \( \delta_p \) on any code position such that any check has the same even weight, say \( 2w \), we have \( 2w \delta_p \) mutually different columns \( a_i^{(1)}, a_i^{(2)}, \ldots, a_i^{(2w)} \), \( i = 1, \ldots, \delta_p \) of \( G_p \) such that

\[
a_i^{(1)} + a_i^{(2)} + \ldots + a_i^{(2w)} = e_0
\]

for \( i = 1, \ldots, \delta_p \). The matrix

\[
 G := \begin{bmatrix}
 G_p & G_p & \cdots & G_p \\
 G_q & G_q & \cdots & G_q \\
 \end{bmatrix}
\]

is an optimal generator matrix of \( C \). Because \( \gcd(T_p, T_q) = 1 \), any pair \( \left[ x^T \right] \), where \( x \) and \( y \) are columns of resp. \( G_p \) and \( G_q \), occurs exactly once as a column of \( G \). By combining this fact with formula (66), we get that for any \( i \in \{1, \ldots, \delta_p \} \) and any \( j \in \{1, \ldots, T_q \} \) the equality
Formula (68) implies that orthogonal checks on the message digit $m_0$.

If $C_\eta$ is an even-weight code,

$$m_0 = c_0 + c_{T_\eta} + c_{2T_\eta} + \ldots + c_{(T_\eta-1)T_\eta}$$

is an additional check for $m_0$, orthogonal to the previous ones.

(ii): Immediate consequence of (i).

If in addition $C_\eta$ also has an orthogonal check set of size $\delta_\eta$ on any code position such that any check has the same even weight, then we have the following lower bound for $s$.

(5.2.4) **Theorem:**

(i): If $\text{wt}(x^{q+1}/q(x))$ is even and $T_\eta \delta_\eta + 1 \geq T_\eta (\delta_\eta + 1)$, then the separation vector $s$ of the $[T_\eta T_\eta, k+\alpha]$ code with check polynomial $p(x)q(x)$ satisfies

$$s_i \geq T_\eta \delta_\eta + 1 \quad \text{for } i = 1, \ldots, k_p,$$

(ii): If $\text{wt}(x^{q+1}/q(x))$ is odd and $T_\eta \delta_\eta \geq T_\eta (\delta_\eta + 1)$, then the separation vector $s$ of the $[T_\eta T_\eta, k+\alpha]$ code with check polynomial $p(x)q(x)$ satisfies

$$s_i \geq T_\eta \delta_\eta \quad \text{for } i = 1, \ldots, k_p,$$

$$s_i \geq T_\eta (\delta_\eta + 1) \quad \text{for } i = k_\eta +1, \ldots, k_\eta + k_\eta.$$
Proof:

(i): For \( i = 1, \ldots, k \) formula (69) was shown in Theorem (5.2.3).
Without loss of generality we consider the message digit \( m_{k_p} \).
For \( j = 0, 1, \ldots, T_p - 1, m_{k_p} \) equals
\[
m_{k_p} = c_{jT_q} + \sum_{i=0}^{P} m_i G_i, jT_q,
\]
where \( G \) is the matrix of (67). If an error of weight less than or
equal to \( \left\lfloor \frac{T_p (\delta + 1)}{2} \right\rfloor \) occurs, then the message digits \( m_0, \ldots, m_{k_p-1} \)
are correctly decodable, since \( T_p \delta + 1 \geq T_p (\delta + 1) \). If we fill
in these values of \( m_0, \ldots, m_{k_p-1} \) in formula (71), then the \( T_p (\delta + 1) \)
checks on \( m_{k_p} \) obtained from the formulas (68) and (71) are mutually
orthogonal. Hence \( s_{k_p} \geq T_p (\delta + 1) \).

(ii): Analogous to (i).

(5.2.5) **Example:** Take \( p(x) := x^3 + x + 1, q(x) := x^4 + x^3 + x^2 + x + 1 \). \( T_p = 7, T_q = 5 \).
The \([7,3]\) code \( C_p \) with check polynomial \( p(x) \) has an orthogonal check set
of size \( \delta_p = 3 \) on any code position, where all checks have weight 2 (for
example, for the 0-position we have the checks \{1, 5\}, \{2, 3\}, and \{4, 6\}).
The \([5,4]\) code \( C_q \) with check polynomial \( q(x) \) has an orthogonal check set
of size \( \delta_q = 1 \) on any code position, where the check has weight 4 (for
example, for the 0-position we have the check \{1, 2, 3, 4\}). By Theorem (5.2.4)
the \([35,7]\) code \( C \) with check polynomial \( p(x)q(x) \) has a separation vector
\( s \) which satisfies \( s \geq (16, 16, 16, 14, 14, 14, 14) \).

\[
pabcdefghijklmnopqrstuvwxyz
<table>
<thead>
<tr>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

ABCD EFAB DGEF BCDG FABC GEFA CDGE

Fig. 5.1: Generator matrix of the \([35,7]\) code
with check polynomial \((x^3 + x + 1)(x^4 + x^3 + x^2 + x + 1)\).
Fig. 5.1 shows an optimal generator matrix for \( C \), together with the checks on \( m_0 \) and \( m_3 \). The message bit \( m_0 \) is equal to the following sixteen orthogonal checks.

\[
\begin{align*}
a: & \quad c_1 + c_{26} \\
b: & \quad c_2 + c_{17} \\
c: & \quad c_3 + c_{23} \\
d: & \quad c_4 + c_{34} \\
e: & \quad c_5 + c_{15} \\
f: & \quad c_6 + c_{11} \\
g: & \quad c_8 + c_{33} \\
h: & \quad c_9 + c_{24} \\
i: & \quad c_{10} + c_{30} \\
j: & \quad c_{12} + c_{22} \\
k: & \quad c_{13} + c_{18} \\
l: & \quad c_{16} + c_{31} \\
m: & \quad c_{19} + c_{29} \\
n: & \quad c_{20} + c_{25} \\
o: & \quad c_{27} + c_{32} \\
p: & \quad c_0 + c_7 + c_{14} + c_{21} + c_{28}.
\end{align*}
\]

The message bit \( m_3 \) is equal to the following fourteen "orthogonal" checks.

\[
\begin{align*}
A: & \quad c_1 + c_8 + c_{22} + c_{29} \\
B: & \quad c_2 + c_9 + c_{16} + c_{23} \\
C: & \quad c_3 + c_{17} + c_{24} + c_{31} \\
D: & \quad c_4 + c_{11} + c_{18} + c_{32} \\
E: & \quad c_6 + c_{13} + c_{27} + c_{34} \\
F: & \quad c_7 + c_{14} + c_{21} + c_{28} \\
G: & \quad c_{12} + c_{19} + c_{26} + c_{33}
\end{align*}
\]

Actually the separation vector of \( C \) equals \((16,16,16,14,14,14,14,14)\), as one can easily check.

The \([35,8]\) code \( C^* \) with check polynomial \((x+1)p(x)q(x)\) has a separation vector equal to \((15,15,15,7,7,7,7,7)\). For \( C^*, a, b, \ldots, o \) are fifteen orthogonal checks on \( m_0 \); \( A, B, \ldots, G \) are seven orthogonal checks on \( m_3 \). For the message bit \( m_7 \) we have the following seven checks.

\[
\begin{align*}
c_0 & + c_7 + c_{14} + c_{21} + c_{28} + m_0 \\
c_1 & + c_8 + c_{15} + c_{22} + c_{29} + m_0 + m_1 \\
c_2 & + c_9 + c_{16} + c_{23} + c_{30} + m_0 + m_1 + m_2 \\
c_3 & + c_{10} + c_{17} + c_{24} + c_{31} + m_1 + m_2 \\
c_4 & + c_{11} + c_{18} + c_{25} + c_{32} + m_0 + m_2 \\
c_5 & + c_{12} + c_{19} + c_{26} + c_{33} + m_1 \\
c_6 & + c_{13} + c_{20} + c_{27} + c_{34} + m_2.
\end{align*}
\]
We can extend Theorem (5.2.3) to codes with a check polynomial which is a product of more than two irreducible polynomials in $\mathbb{F}_2[x]$.

(5.2.6) Theorem: For $i = 1, \ldots, v$ let $p_i(x)$ be an irreducible polynomial in $\mathbb{F}_2[x]$ of degree $k_i$ and exponent $T_i$ such that $\gcd(T_i, T_j) = 1$ for all $i, j$, $i \neq j$, and let the $[T_i, k_i]$ binary code with check polynomial $p_i(x)$ have an orthogonal check set of size $\delta_i$ such that all checks have the same even weight. Then the code $C$ of length $n = \sum_{i=1}^{v} T_i$ and dimension $\sum_{i=1}^{v} k_i$ with check polynomial $\prod_{i=1}^{v} p_i(x)$ has a separation vector $s$ which satisfies

$$s_j \geq \frac{n \delta_i}{T_i}$$

for $i = 1, \ldots, v$ and $j = (\sum_{u=1}^{i-1} k_u) + 1, \ldots, \sum_{u=1}^{i} k_u$.

Proof: Analogous to Theorem (5.2.3).

In many cases we can do much better than formula (75) by adding other checks, e.g. checks like the ones in formula (71). This will be shown in the next example.

(5.2.7) Example: Take $p(x) := x^3 + x + 1$, $q(x) := x^2 + x + 1$, $r(x) := x^4 + x^3 + x^2 + x + 1$. $T_p = 7$, $T_q = 3$, $T_r = 5$.

Let $C$ be the $[105,9]$ code with check polynomial $p(x)q(x)r(x)$. $C$ has an optimal generator matrix $G := (M_p^T M_q^T M_r^T)$, where $M_p$, $M_q$, and $M_r$ are repetitions of resp.

\[
\begin{bmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
\end{bmatrix}
\]

The $[7,3]$ code with generator matrix $P$ has three orthogonal checks $\{1,5\}$, $\{2,3\}$, and $\{4,6\}$ of weight 2 on code position 0. The $[3,2]$ code with generator matrix $Q$ has one check $\{1,2\}$ of weight 2 on code position 0. The $[5,4]$ code with generator matrix $R$ has one check $\{1,2,3,4\}$ of weight 4 on code position 0. Hence $\delta_p = 3, \delta_q = 1$, and $\delta_r = 1$.

Any vector $(x^T, y^T, z^T)^T$, where $x, y, z$ are columns of resp. $P, Q$, and $R$, occurs exactly once as a column of $G$. Now for any $i \in \{1, \ldots, T_q\}$ and
and \( j \in \{1, \ldots, T_r\} \) we have

\[
\begin{bmatrix}
P*1 \\
Q*1 \\
R*1
\end{bmatrix} + \begin{bmatrix}
P*2 \\
Q*2 \\
R*2
\end{bmatrix} + \begin{bmatrix}
P*3 \\
Q*3 \\
R*3
\end{bmatrix} + \begin{bmatrix}
P*4 \\
Q*4 \\
R*4
\end{bmatrix} + \begin{bmatrix}
P*5 \\
Q*5 \\
R*5
\end{bmatrix} = \begin{bmatrix}
1 \\
0 \\
0
\end{bmatrix}.
\tag{76}
\]

This implies \( T_T \Delta = 45 \) orthogonal checks on \( m_0 \). These checks do not contain the fifteen code digits \( \{ c_j \mid j \equiv 0 \mod 7 \}\), which correspond to the columns of \( G \) given in Fig. 5.2.

From Fig. 5.2 it is easy to see that

\[
a: \quad c_0 + c_{21} + c_{42} + c_{49} + c_{98}
b: \quad c_7 + c_{14} + c_{63} + c_{70} + c_{91}
c: \quad c_{28} + c_{35} + c_{56} + c_{77} + c_{84}
\tag{77}
\]

are three additional orthogonal checks on \( m_0 \), which are orthogonal to the 45 checks implied by formula (76). Hence we have 48 orthogonal checks on \( m_0 \).

Analogously we can find 48 orthogonal checks on \( m_1 \) and \( m_2 \).

For any \( i \in \{1, \ldots, T_p\} \) and any \( j \in \{1, \ldots, T_r\} \) we have
This implies \( T \cdot T \cdot \bar{\delta} = 35 \) orthogonal checks on \( m_3 \). These checks do not contain the code digits \( \{ c_j \mid j \equiv 0 \mod 3 \} \), which correspond to the columns of \( G \) given in Fig. 5.3.

\[
\begin{bmatrix}
P_{*i} \\
Q_{*i} \\
R_{*j}
\end{bmatrix}
+ \begin{bmatrix}
P_{*i} \\
Q_{*2} \\
R_{*j}
\end{bmatrix} = e_3 := (0,0,0,1,0,0,0,0,0)^T. \quad (78)
\]

From Fig. 5.3 it is easy to see that

\[
\begin{align*}
a & : c_0 + c_9 + c_{12} + c_{36} + c_{93} \\
b & : c_{18} + c_{21} + c_{39} + c_{45} + c_{72} \\
c & : c_{30} + c_{42} + c_{48} + c_{66} + c_{69} \\
d & : c_{51} + c_{63} + c_{75} + c_{84} + c_{102} \\
e & : c_{15} + c_{33} + c_{54} + c_{81} + c_{87} \\
f & : c_{3} + c_{57} + c_{90} + c_{96} + c_{99} \\
g & : c_{6} + c_{24} + c_{27} + c_{60} + c_{78}
\end{align*}
\]

are seven additional orthogonal checks on \( m_3 \), which are orthogonal to the 35 checks implies by formula (78). Hence we have 42 orthogonal checks on \( m_3 \).

Analogously we can find 42 checks on \( m_4 \).

For any \( i \in \{1, \ldots, T_p\} \) and any \( j \in \{1, \ldots, T_q\} \) we have
This implies that \( T \delta = 21 \) orthogonal checks on \( m_5 \). These checks do not contain the 21 code digits \( \{ c_j \mid j \equiv 0 \mod 5 \} \). Since \( s_1, s_2, \ldots, s_5 \geq 42 \),

\[
c_j + \sum_{i=0}^{4} m_i G_{ij}
\]

for \( j \in \{0, 5, 10, \ldots, 100\} \) build 21 additional checks on \( m_5 \) (cf. the proof of Theorem (5.2.4)). Hence we have 42 "orthogonal" checks on \( m_5 \). Analogously we can find 42 checks on \( m_6, m_7, \) and \( m_8 \).

We have shown that the \([105, 9]\) code with check polynomial

\[
(3 + x + 1)(2 + x + 1)(4 + 3 - x + x + 1) \]

has a separation vector of at least \((48, 48, 48, 42, 42, 42, 42, 42, 42, 42)\). Actually equality holds, as one can easily check. So we have derived a Majority Logic Decoding Scheme for the code that reaches the actual separation vector.

For a binary cyclic code whose check polynomial is the product of \((x+1)\) and two primitive polynomials we have the following theorem.

\[(5.2.8) \text{Theorem: For the primitive polynomials } p(x), q(x) \in \mathbb{F}_2[x] \text{ of degrees } k_p \text{ resp. } k_q \text{ such that } k_p > k_q \text{ and } \gcd(k_p, k_q) = 1 \text{ the binary cyclic code } \]

\[
[2^{(p-1)}(2^{q-1}), k_p + k_q + 1] \text{ with check polynomial } (x+1)p(x)q(x) \text{ has a separation vector } s \text{ which satisfies}
\]

\[
s_i = \begin{cases} 
    k_p - 1 & \text{for } i = 1, \ldots, k_p \\
    k_q - 1 & \text{for } i = k_p + 1, \ldots, k_p + k_q + 1
\end{cases}
\]

Proof: The \([2^{p-1}, k_p] \) cyclic code \( C_p \) with primitive check polynomial \( p(x) \) of degree \( k_p \) is a simplex code (i.e., all elements of \( \mathbb{F}_2^{k_p} \backslash \{0\} \) occur as columns in a generator matrix of \( C_p \)). Hence we have an orthogonal check set of size \( \delta_p = (2^{p-1} - 1) \) on any code position, where all weights of the checks equal 2. The same holds for the \([2^{q-1}, k_q] \) code \( C_q \) with primitive check polynomial \( q(x) \);

\( \delta_q = (2^{q-1} - 1) \). Since \( \gcd(k_p, k_q) = 1 \), we may apply Theorem (5.2.3)(ii) to the first \( k_p \) message bits as well as to the message bits \( m_{k_p}, \ldots, m_{k_p+k_q-1} \).
Furthermore

\[ \text{wt}((x^n + 1)/p(x) + \sum_{i=0}^{\frac{n-1}{k}} x^i) = k \binom{q}{2} \binom{p-1}{2} \quad \text{and} \]

\[ \text{wt}((x^n + 1)/q(x) + \sum_{i=0}^{\frac{n-1}{k}} x^i) = k \binom{p-1}{2} \binom{q-1}{2}, \]

where \( n := (2^p-1)(2^q-1). \)

These observations imply formula (82).

(5.2.9) Examples:

(i): Take \( k_p = 3, k_q = 2, p(x) = x^3 + x + 1, q(x) = x^2 + x + 1. \)

\[
G := \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}
\]

is an optimal generator matrix for the [21,6] cyclic code \( C \) with check polynomial \((x+1)p(x)q(x). s(G) = (9,9,9,7,7,7).\)

\( m_0, m_3, \) and \( m_5 \) have the following checks.

\[
m_0 = c_1 + c_{19} = c_2 + c_{17} = c_3 + c_9 = c_4 + c_{13} = c_5 + c_8 = c_6 + c_{18} = c_{10} + c_{16} = c_{11} + c_{20} = c_{12} + c_{15}.
\]

\[
m_3 = c_1 + c_8 = c_2 + c_{16} = c_4 + c_{11} = c_5 + c_{19} = c_7 + c_{14} = c_{10} + c_{17} = c_{13} + c_{20}.
\]

\[
m_5 = c_0 + c_1 + c_2 + m_0 + m_2 = c_3 + c_4 + c_5 + m_0 = c_6 + c_7 + c_8 + m_1 + m_2 = c_9 + c_{10} + c_{11} + m_2 = c_{12} + c_{13} + c_{14} + m_0 + m_1 + m_2 = c_{15} + c_{16} + c_{17} + m_1 = c_{18} + c_{19} + c_{20} + m_0 + m_1.
\]

The generator matrix \( G' \) for this code, whose rows are the cyclic shifts of the generator polynomial, has a separation vector \( s(G') = (7,7,7,7,7,7). \)
A binary [21,6] code has a minimum distance of at most 8 (cf. Helgert and Stinaff (1973)).

(ii): Take \( k = 4, k = 3 \), \( p(x) := (x^4 + x + 1) \), \( q(x) := (x^3 + x + 1) \). The [105,8] code with check polynomial \((x+1)p(x)q(x)\) has separation vector \((49,49,49,49,49,49,49,49)\).

We can also extend Theorem (5.2.9) to the following one.

(5.2.10) **Theorem:** For the primitive polynomials \( p_i(x) \in \mathbb{F}_2[x], i = 1, \ldots, v \) of degrees resp. \( k_i, i = 1, \ldots, v \) such that \( k_1 > k_2 > \ldots > k_v \) and \( \gcd(k_i, k_j) = 1 \) for all \( i, j, i \neq j \), the binary cyclic \( \bigotimes_{i=1}^{v} (2^i-1) \) code with check polynomial \((x+1) \bigotimes_{i=1}^{v} p_i(x)\) has a separation vector \( s \) which satisfies

\[
s_i = (2^{j-1}) \sum_{u=1}^{\lfloor j/2 \rfloor} (2^{u-1})/(2^{j-1})
\]

for \( i = \sum_{u=1}^{\lfloor j/2 \rfloor} k_u + 1, \ldots, \sum_{u=1}^{j} k_u \) and \( j = 1, \ldots, v \).

**Proof:** Analogous to the proof of Theorem (5.2.8).

Table B.1 in Appendix B contains the separation vectors of all binary cyclic UEP codes of length less than or equal to 39.

### 5.3 Notes

Theorem (5.1.1) is from Dunning and Robbins (1978). It is easy to prove the Corollaries (5.1.2) and (5.1.3) without the results of Chapter 2, by only using the special configuration of the generator matrix \( G \) in formula (55).

Theorem (5.2.1) is from Dyn'kin and Togonidze (1976). They also mention Theorem (5.2.8) without a proof.
## APPENDIX A: BINARY OPTIMAL LINEAR UEP CODES OF LENGTH LESS THAN OR EQUAL TO 15

<table>
<thead>
<tr>
<th>n</th>
<th>k</th>
<th>d(n,k)</th>
<th>separation vector</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>2</td>
<td>2</td>
<td>32</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>3</td>
<td>42</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>2</td>
<td>322</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>4</td>
<td>52</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>3</td>
<td>422</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>2</td>
<td>3222</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>4</td>
<td>62, 54</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>4</td>
<td>522</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>3</td>
<td>4222</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>2</td>
<td>32222</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>5</td>
<td>72, 64</td>
</tr>
<tr>
<td>8</td>
<td>3</td>
<td>4</td>
<td>622, 544</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>4</td>
<td>5222</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td>2</td>
<td>42222, 33332</td>
</tr>
<tr>
<td>8</td>
<td>6</td>
<td>2</td>
<td>322222</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>6</td>
<td>82, 74</td>
</tr>
<tr>
<td>9</td>
<td>3</td>
<td>4</td>
<td>722, 644, 554</td>
</tr>
<tr>
<td>9</td>
<td>4</td>
<td>4</td>
<td>6222, 5444</td>
</tr>
<tr>
<td>9</td>
<td>5</td>
<td>3</td>
<td>52222, 44442, 43333</td>
</tr>
<tr>
<td>9</td>
<td>6</td>
<td>2</td>
<td>422222, 333322</td>
</tr>
<tr>
<td>9</td>
<td>7</td>
<td>2</td>
<td>3222222</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>6</td>
<td>92, 84, 76</td>
</tr>
<tr>
<td>10</td>
<td>3</td>
<td>5</td>
<td>822, 744, 664</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>4</td>
<td>72222, 6444, 5544</td>
</tr>
<tr>
<td>10</td>
<td>5</td>
<td>4</td>
<td>622222, 54444</td>
</tr>
<tr>
<td>10</td>
<td>6</td>
<td>3</td>
<td>5222222, 4444222, 4333322</td>
</tr>
<tr>
<td>10</td>
<td>7</td>
<td>2</td>
<td>4222222, 3333222</td>
</tr>
<tr>
<td>10</td>
<td>8</td>
<td>2</td>
<td>32222222</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>7</td>
<td>10.2, 94, 86</td>
</tr>
<tr>
<td>11</td>
<td>3</td>
<td>6</td>
<td>922, 844, 764</td>
</tr>
<tr>
<td>11</td>
<td>4</td>
<td>5</td>
<td>82222, 7444, 6644</td>
</tr>
<tr>
<td>11</td>
<td>5</td>
<td>4</td>
<td>722222, 64444, 55444</td>
</tr>
<tr>
<td>11</td>
<td>6</td>
<td>4</td>
<td>6222222, 544444, 533333</td>
</tr>
<tr>
<td>11</td>
<td>7</td>
<td>3</td>
<td>52222222, 44442222, 43333222</td>
</tr>
<tr>
<td>11</td>
<td>8</td>
<td>2</td>
<td>422222222, 333322222</td>
</tr>
<tr>
<td>11</td>
<td>9</td>
<td>2</td>
<td>3222222222</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>8</td>
<td>11.2, 10.4, 96</td>
</tr>
<tr>
<td>12</td>
<td>3</td>
<td>6</td>
<td>10.22, 944, 864, 774, 766</td>
</tr>
<tr>
<td>12</td>
<td>4</td>
<td>6</td>
<td>92222, 8444, 7644</td>
</tr>
<tr>
<td>12</td>
<td>5</td>
<td>4</td>
<td>822222, 74444, 66444, 55554</td>
</tr>
<tr>
<td>12</td>
<td>6</td>
<td>4</td>
<td>7222222, 644444, 554444</td>
</tr>
<tr>
<td>12</td>
<td>7</td>
<td>4</td>
<td>62222222, 5444422, 5333332</td>
</tr>
<tr>
<td>12</td>
<td>8</td>
<td>3</td>
<td>522222222, 444422222, 43333222</td>
</tr>
<tr>
<td>12</td>
<td>9</td>
<td>2</td>
<td>4222222222, 333322222</td>
</tr>
<tr>
<td>12</td>
<td>10</td>
<td>2</td>
<td>3222222222</td>
</tr>
</tbody>
</table>

**Table A.1**: The separation vectors of the binary optimal LUEP codes of length less than or equal to 15 (Part I).
### Table A.1: The separation vectors of the binary optimal LUEP codes of length less than or equal to 15 (Part II).

<table>
<thead>
<tr>
<th>n</th>
<th>k</th>
<th>d(n,k) separation vector</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>2</td>
<td>12.2, 11.4, 10.6, 98</td>
</tr>
<tr>
<td>13</td>
<td>3</td>
<td>11.22, 10.44, 964, 884, 866</td>
</tr>
<tr>
<td>13</td>
<td>4</td>
<td>10.22, 9444, 8644, 7744, 7666</td>
</tr>
<tr>
<td>13</td>
<td>5</td>
<td>922222, 844444, 764444, 66666, 65555</td>
</tr>
<tr>
<td>13</td>
<td>6</td>
<td>8222222, 7444444, 6644444, 555555</td>
</tr>
<tr>
<td>13</td>
<td>7</td>
<td>72222222, 64444444, 63333333, 55444442, 54444444</td>
</tr>
<tr>
<td>13</td>
<td>8</td>
<td>622222222, 544444444, 533333333</td>
</tr>
<tr>
<td>13</td>
<td>9</td>
<td>5222222222, 4444444444, 4333333333</td>
</tr>
<tr>
<td>13</td>
<td>10</td>
<td>4222222222, 3333222222</td>
</tr>
<tr>
<td>13</td>
<td>11</td>
<td>32222222222</td>
</tr>
<tr>
<td>14</td>
<td>2</td>
<td>13.2, 12.4, 11.6, 10.8</td>
</tr>
<tr>
<td>14</td>
<td>3</td>
<td>12.22, 11.44, 10.64, 984, 966</td>
</tr>
<tr>
<td>14</td>
<td>4</td>
<td>11.222, 10.444, 9644, 8844, 8666</td>
</tr>
<tr>
<td>14</td>
<td>5</td>
<td>10.22222, 944444, 864444, 774444, 766666 (a)</td>
</tr>
<tr>
<td>14</td>
<td>6</td>
<td>922222222, 844444444, 764444444, 6666666, 655555</td>
</tr>
<tr>
<td>14</td>
<td>7</td>
<td>8222222222, 7444444444 (b), 664444444, 654444444, 5555555 (c)</td>
</tr>
<tr>
<td>14</td>
<td>8</td>
<td>72222222222, 64444444444, 63333333333, 55444444444, 5444444444</td>
</tr>
<tr>
<td>14</td>
<td>9</td>
<td>622222222222, 544444444444, 533333333333</td>
</tr>
<tr>
<td>14</td>
<td>10</td>
<td>5222222222222, 4444444444444, 4333333333333</td>
</tr>
<tr>
<td>14</td>
<td>11</td>
<td>42222222222222, 33332222222222</td>
</tr>
<tr>
<td>14</td>
<td>12</td>
<td>322222222222222</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>14.2, 13.4, 12.6, 11.8</td>
</tr>
<tr>
<td>15</td>
<td>3</td>
<td>13.22, 12.44, 11.64, 10.84, 10.64, 988</td>
</tr>
<tr>
<td>15</td>
<td>4</td>
<td>12.222, 11.444, 10.644, 9844 (d), 9666</td>
</tr>
<tr>
<td>15</td>
<td>5</td>
<td>11.2222, 10.4444, 96444, 88444, 86666</td>
</tr>
<tr>
<td>15</td>
<td>6</td>
<td>10.22222, 944444, 8644444, 7744444, 7666666, 7666666 (e)</td>
</tr>
<tr>
<td>15</td>
<td>7</td>
<td>922222222, 844444444, 764444444 (f), 6666666, 665555</td>
</tr>
<tr>
<td>15</td>
<td>8</td>
<td>8222222222, 7444444444, 6644444444, 5544444444, 5444444444</td>
</tr>
<tr>
<td>15</td>
<td>9</td>
<td>72222222222, 64444444444, 63333333333, 55444444444, 5444444444</td>
</tr>
<tr>
<td>15</td>
<td>10</td>
<td>622222222222, 544444444444, 533333333333</td>
</tr>
<tr>
<td>15</td>
<td>11</td>
<td>5222222222222, 4444444444444, 4333333333333</td>
</tr>
<tr>
<td>15</td>
<td>12</td>
<td>42222222222222, 33332222222222</td>
</tr>
<tr>
<td>15</td>
<td>13</td>
<td>322222222222222</td>
</tr>
</tbody>
</table>

Any separation vector of a binary linear \([n,k]\) code \((4 \leq n \leq 15, 2 \leq k \leq n-2)\) is less than or equal to one of the separation vectors in the row of Table A.1 corresponding to \(n,k\). If a component of a separation vector consists of two digits it is followed by a point. Let \(d(n,k)\) denote the maximal minimum distance of a binary linear code of length \(n\) and dimension \(k\) (cf. Helgert and Stinaff (1973)).

The nontrivial codes in Table A.1 are constructed in one of the following ways.
(i): Adding a parity check to another code in the table.
(ii): Shortening or puncturing other codes in the table.
(iii): Adding a column of weight one to a generator matrix of a LUEP code of length one less.
(iv): The following construction:
If the matrix $G_1$ has separation vector $s(G_1)$, then
\[
G_2 := \begin{bmatrix}
0 \\
0 \\
\vdots \\
0 \\
1 & 0 & 0 & \cdots & 0
\end{bmatrix}
\]
has separation vector $s(G_2) = (s(G_1), 2)$.
(v): The constructions in Section 4.1.
(vi): (a). Construction (4.2.1) with $m = 1$ and $G_1$ a generator matrix of a $[7,4,3]$ Hamming code.
(b). Construction (4.2.1) with $m = 1$ and $G_1$ a generator matrix of a $[7,6,2]$ code.
(c). \[
\begin{bmatrix}
\cdots & 1 & 1 & 1 & \cdots \\
\cdots & 1 & 1 & 1 & \cdots \\
\cdots & 1 & 1 & 1 & 1 \\
\cdots & 1 & 1 & 1 & \cdots \\
1 & \cdots & 1 & 1 & \cdots \\
\cdots & 1 & \cdots & \cdots & \cdots \\
\end{bmatrix}
\]
is a generator matrix of a $[14,7,(5,5,5,5,4,4,4)]$ code.
(d). \[
\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & \cdots \\
1 & 1 & 1 & 1 & 1 & \cdots \\
1 & 1 & 1 & 1 & 1 & \cdots \\
1 & 1 & 1 & 1 & 1 & \cdots \\
1 & 1 & 1 & 1 & 1 & \cdots \\
\cdots & 1 & \cdots & \cdots & \cdots & \cdots \\
\end{bmatrix}
\]
is a generator matrix of a $[15,4,(9,8,4,4)]$ code.
(e). \[
\begin{bmatrix}
\cdots & 1 & 1 & 1 & \cdots \\
\cdots & 1 & 1 & 1 & \cdots \\
\cdots & 1 & 1 & 1 & \cdots \\
\cdots & 1 & 1 & 1 & \cdots \\
1 & \cdots & 1 & 1 & \cdots \\
\cdots & 1 & \cdots & \cdots & \cdots \\
\end{bmatrix}
\]
is a generator matrix of a $[15,6,(7,6,5,5,5,4)]$ code.
(f). \[
\begin{bmatrix}
\cdots & 1 & 1 & 1 & \cdots \\
\cdots & 1 & 1 & 1 & \cdots \\
\cdots & 1 & 1 & 1 & \cdots \\
\cdots & 1 & 1 & 1 & \cdots \\
1 & \cdots & 1 & 1 & \cdots \\
\cdots & 1 & \cdots & \cdots & \cdots \\
\end{bmatrix}
\]
is a generator matrix of a $[15,7,(7,6,4,4,4,4,4)]$ code.
Table A.1 has two open places.

(1): Does a $[15,8,s]$ code with $(6,5,3,3,3,3,3,3) \leq s \leq (6,5,4,4,3,3,3)$ exist?

(2): Does a $[15,8,(5,5,5,x,4,4,4,4)]$ code with $x \in \{4,5\}$ exist?

with $G_1$ the matrix in (vi)(c) has separation vector $(5,5,5,5,4,4,4,3)$. By adding a column of weight one to an optimal generator matrix of a $[14,8,(5,4,4,4,4,4,4,4)]$ code, we obtain a $[15,8,(5,5,4,4,4,4,4,4)]$ code.
Table B.1 contains the parameters of all binary cyclic UEP codes of length less than or equal to 39. In this table for each code of length \( n \) the exponents \( i, j, k, \ldots \) of a primitive \( n^{th} \) root of unity \( \alpha \) are given such that \( \alpha^i, \alpha^j, \alpha^k, \ldots \) are nonzeros of the code. For example the first row of the table denotes a binary cyclic \([15,7,(5,5,3,3,3,3,3)]\) code with nonzeros \( \{ \alpha^i \mid i \in C_5 \cup C_0 \cup C_3 \} \), where \( C_i \) \( (i = 5, 0, 3) \) denotes the cyclotomic coset modulo 15 containing \( i \). The order of the nonzeros corresponds to the order of the components in the separation vector. I.e. if the order of the nonzeros is \( i, j, k, \ldots \), then the separation vector equals \( \mathbf{s}(M_i^T | M_j^T | M_k^T | \ldots) \), where \( M_x \) \( (x = i, j, k, \ldots) \) denotes a generator matrix of the minimal ideal in \( \mathbb{F}_2[x]/(x^n+1) \) with nonzeros \( \{ \alpha^y \mid y \in C_x \} \). In the above example \( \mathbf{s}(M_5^T | M_0^T | M_3^T) = (5, 5, 3, 3, 3, 3) \).

The last column of the table contains the minimum length or a bound on the minimum length of a binary linear code with a separation vector of at least the one of the corresponding cyclic code. The separation components (and the corresponding nonzeros) larger than the minimum distance of the code are underlined.
Table B.1: All binary cyclic UEP codes of length less than or equal to 39 (Part I).
<table>
<thead>
<tr>
<th>length</th>
<th>dim.</th>
<th>nonzeros</th>
<th>separation vector $s$</th>
<th>$n(s)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>33</td>
<td>12</td>
<td>11,3</td>
<td>12,12,6,6,6,6,6,6,6,6,6,6</td>
<td>≥ 29</td>
</tr>
<tr>
<td>13</td>
<td>0,1,11</td>
<td></td>
<td>11,10,10,10,10,10,10,10,10,10,10,10,10</td>
<td>≥ 32</td>
</tr>
<tr>
<td>13</td>
<td>11,0,3</td>
<td></td>
<td>11,11,3,3,3,3,3,3,3,3,3,3,3,3</td>
<td>≥ 28</td>
</tr>
<tr>
<td>21</td>
<td>0,1,5</td>
<td></td>
<td>11,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4</td>
<td>≥ 32</td>
</tr>
<tr>
<td>23</td>
<td>0,1,5,11</td>
<td></td>
<td>11,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2</td>
<td>33</td>
</tr>
<tr>
<td>23</td>
<td>1,11,0,3</td>
<td></td>
<td>5,5,5,5,5,5,5,5,5,5,5,5,3,3,3,3,3,3,3,3,3,3</td>
<td>≥ 32</td>
</tr>
<tr>
<td>31</td>
<td>0,1,3,5</td>
<td></td>
<td>3,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2</td>
<td>33</td>
</tr>
<tr>
<td>35</td>
<td>7</td>
<td>5,7</td>
<td>16,16,16,14,14,14,14,14,14,14</td>
<td>≥ 34</td>
</tr>
<tr>
<td>8</td>
<td>5,0,7</td>
<td></td>
<td>15,15,15,7,7,7,7,7,7</td>
<td>≥ 32</td>
</tr>
<tr>
<td>11</td>
<td>7,0,5,15</td>
<td></td>
<td>7,7,7,7,5,5,5,5,5,5,5,5,5,5</td>
<td>22</td>
</tr>
<tr>
<td>13</td>
<td>0,1</td>
<td></td>
<td>15,8,8,8,8,8,8,8,8,8,8,8,8</td>
<td>≥ 33</td>
</tr>
<tr>
<td>15</td>
<td>5,1</td>
<td></td>
<td>12,12,12,8,8,8,8,8,8,8,8,8,8</td>
<td>≥ 33</td>
</tr>
<tr>
<td>16</td>
<td>0,1,15</td>
<td></td>
<td>15,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4</td>
<td>≥ 32</td>
</tr>
<tr>
<td>17</td>
<td>0,1,7</td>
<td></td>
<td>7,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6</td>
<td>≥ 28</td>
</tr>
<tr>
<td>18</td>
<td>5,1,15</td>
<td></td>
<td>8,8,8,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4</td>
<td>≥ 29</td>
</tr>
<tr>
<td>19</td>
<td>0,5,1,15</td>
<td></td>
<td>5,5,5,5,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4</td>
<td>≥ 26</td>
</tr>
<tr>
<td>19</td>
<td>5,1,7</td>
<td></td>
<td>8,8,8,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6</td>
<td>≥ 30</td>
</tr>
<tr>
<td>19</td>
<td>7,1,15</td>
<td></td>
<td>6,6,6,6,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4</td>
<td>≥ 27</td>
</tr>
<tr>
<td>20</td>
<td>0,5,7,1</td>
<td></td>
<td>7,7,7,7,7,7,7,7,6,6,6,6,6,6,6,6,6,6,6,6,6</td>
<td>≥ 31</td>
</tr>
<tr>
<td>22</td>
<td>5,7,1,15</td>
<td></td>
<td>6,6,6,6,6,6,6,6,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4</td>
<td>≥ 31</td>
</tr>
<tr>
<td>25</td>
<td>0,1,3</td>
<td></td>
<td>7,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4</td>
<td>≥ 33</td>
</tr>
<tr>
<td>28</td>
<td>0,1,3,5</td>
<td></td>
<td>5,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4</td>
<td>35</td>
</tr>
<tr>
<td>29</td>
<td>0,1,3,7</td>
<td></td>
<td>7,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2</td>
<td>35</td>
</tr>
</tbody>
</table>

Table B.1: All binary cyclic UEP codes of length less than or equal to 39 (Part II).
<table>
<thead>
<tr>
<th>length</th>
<th>dim.</th>
<th>nonzeros</th>
<th>separation vector $s$</th>
<th>$n(s)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>31</td>
<td>0,1,3,5,15</td>
<td>5,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2,2,2,2,2,2,2,2,2,2,2</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>5,1,3,7</td>
<td></td>
<td>4,4,4,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2,2,2,2,2,2,2,2,2,2,2</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>0,5,1,3,7</td>
<td></td>
<td>3,3,3,3,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2,2,2,2,2,2,2,2,2,2,2</td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>13</td>
<td>0,1</td>
<td>15,12,12,12,12,12,12,12,12,12,12,12,12,12</td>
<td>≥37</td>
</tr>
<tr>
<td>14</td>
<td>13,3</td>
<td></td>
<td>14,14,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6</td>
<td>≥35</td>
</tr>
<tr>
<td>15</td>
<td>0,1,13</td>
<td></td>
<td>13,10,10,10,10,10,10,10,10,10,10,10,10,10,10,10,10,10</td>
<td>≥36</td>
</tr>
<tr>
<td>15</td>
<td>13,0,3</td>
<td></td>
<td>13,13,3,3,3,3,3,3,3,3,3,3,3,3,3,3,3,3,3,3,3</td>
<td>≥33</td>
</tr>
<tr>
<td>25</td>
<td>1,0,3</td>
<td></td>
<td>6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,3,3,3,3,3,3</td>
<td>≥35</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3,3,3,3,3</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>0,1,7</td>
<td></td>
<td>13,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4</td>
<td>39</td>
</tr>
<tr>
<td>27</td>
<td>1,13,0,3</td>
<td></td>
<td>6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,3,3,3,3,3,3,3</td>
<td>≥37</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3,3,3,3,3,3,3,3,3</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>0,1,7,13</td>
<td></td>
<td>12,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2,2,2,2,2,2,2,2,2</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>0,1,3,7</td>
<td></td>
<td>3,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2</td>
<td></td>
</tr>
</tbody>
</table>

Table B.1: All binary cyclic UEP codes of length less than or equal to 39 (Part III).
REFERENCES


INDEX

<table>
<thead>
<tr>
<th>Page</th>
<th>Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>bound</td>
</tr>
<tr>
<td>16</td>
<td>Griesmer</td>
</tr>
<tr>
<td>14</td>
<td>Plotkin</td>
</tr>
<tr>
<td>10</td>
<td>code</td>
</tr>
<tr>
<td>2</td>
<td>length-optimal</td>
</tr>
<tr>
<td>2</td>
<td>Linear Unequal Error Protection</td>
</tr>
<tr>
<td>2</td>
<td>LUEP</td>
</tr>
<tr>
<td>14</td>
<td>Maximum-Distance-Separable</td>
</tr>
<tr>
<td>10</td>
<td>optimal</td>
</tr>
<tr>
<td>28,44</td>
<td>simplex</td>
</tr>
<tr>
<td>26</td>
<td>concatenation</td>
</tr>
<tr>
<td></td>
<td>construction</td>
</tr>
<tr>
<td>25</td>
<td>direct product</td>
</tr>
<tr>
<td>24</td>
<td>direct sum</td>
</tr>
<tr>
<td>24</td>
<td>$</td>
</tr>
<tr>
<td></td>
<td>decoding</td>
</tr>
<tr>
<td>30,33</td>
<td>Majority Logic</td>
</tr>
<tr>
<td>2</td>
<td>Syndrome</td>
</tr>
<tr>
<td>33</td>
<td>exponent</td>
</tr>
<tr>
<td></td>
<td>generator matrix</td>
</tr>
<tr>
<td>3</td>
<td>canonical</td>
</tr>
<tr>
<td>8</td>
<td>minimal weight</td>
</tr>
<tr>
<td>6,30</td>
<td>optimal</td>
</tr>
<tr>
<td>13</td>
<td>Krawtchouk polynomial</td>
</tr>
<tr>
<td>9</td>
<td>Lee metric</td>
</tr>
<tr>
<td>30</td>
<td>minimal ideal</td>
</tr>
<tr>
<td>34,35</td>
<td>orthogonal check set</td>
</tr>
<tr>
<td>8</td>
<td>protection level</td>
</tr>
<tr>
<td>1,7</td>
<td>separation vector</td>
</tr>
</tbody>
</table>