On duadic codes

Citation for published version (APA):

Document status and date:
Published: 01/01/1986

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 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

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.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the “Taverne” license above, please follow below link for the End User Agreement:
www.tue.nl/taverne

Take down policy
If you believe that this document breaches copyright please contact us at:
openaccess@tue.nl
providing details and we will investigate your claim.
MASTER'S THESIS

On Duadic Codes

by

Michiel H.M. Smid

AMS subject classification 94B15

EUT Report 86-WSK-04
ISSN 0167-9708
Coden : TEUEDE

Eindhoven

May 1986
Abstract

We define a class of q-ary cyclic codes, the so-called duadic codes. These codes are a direct generalization of QR codes. The results of Leon, Masley and Pless on binary duadic codes are generalized. Duadic codes of composite length and a low minimum distance are constructed. We consider duadic codes of length a prime power, and we give an existence test for cyclic projective planes. Furthermore, we give bounds for the minimum distance of all binary duadic codes of length ≤241.
List of symbols

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$GF(q)$</td>
<td>finite field of order $q$</td>
</tr>
<tr>
<td>0</td>
<td>zero vector</td>
</tr>
<tr>
<td>1</td>
<td>all-one vector</td>
</tr>
<tr>
<td>$[n,k]$</td>
<td>linear code of length $n$ and dimension $k$</td>
</tr>
<tr>
<td>$[n,k,d]$</td>
<td>$[n,k]$ code with minimum distance $d$</td>
</tr>
<tr>
<td>$\text{dim } C$</td>
<td>dimension of the linear code $C$</td>
</tr>
<tr>
<td>$\text{wt}(x)$</td>
<td>weight of the vector $x$</td>
</tr>
<tr>
<td>$\text{wt}(c(x))$</td>
<td>weight of the polynomial $c(x)$</td>
</tr>
<tr>
<td>$d(x,y)$</td>
<td>distance of the vectors $x$ and $y$</td>
</tr>
<tr>
<td>$\overline{C}$</td>
<td>extended code of the code $C$</td>
</tr>
<tr>
<td>$C^\perp$</td>
<td>dual code of the code $C$</td>
</tr>
<tr>
<td>$(x,y)$</td>
<td>inner-product of the vectors $x$ and $y$</td>
</tr>
<tr>
<td>$GF(q)[x]$</td>
<td>polynomial ring over $GF(q)$</td>
</tr>
<tr>
<td>$GF(q)[x]/(x^n-1)$</td>
<td>residue class ring $GF(q)[x] \mod (x^n-1)$</td>
</tr>
<tr>
<td>$(a,b)$</td>
<td>greatest common divisor of $a$ and $b$</td>
</tr>
<tr>
<td>$&lt;g(x)&gt;$</td>
<td>ideal in $GF(q)[x]/(x^n-1)$ generated by $g(x)$</td>
</tr>
<tr>
<td>$j(x)$</td>
<td>polynomial $1+x+x^2+\ldots+x^{n-1}$</td>
</tr>
<tr>
<td>$C_1 + C_2$</td>
<td>orthogonal direct sum of $C_1$ and $C_2$</td>
</tr>
<tr>
<td>$C_1 \perp C_2$</td>
<td>cyclotomic coset containing $i$</td>
</tr>
<tr>
<td>$\mu_a$</td>
<td>permutation $i\mapsto ai \mod n$</td>
</tr>
<tr>
<td>$\mu_a: S_1 \rightarrow S_2$</td>
<td>(2.1.1)</td>
</tr>
<tr>
<td>$q=0 \mod n$</td>
<td>(2.1.3)</td>
</tr>
<tr>
<td>$q=\varnothing \mod n$</td>
<td>(2.1.3)</td>
</tr>
<tr>
<td>$</td>
<td>S</td>
</tr>
<tr>
<td>$\text{ord}_n(a)$</td>
<td>multiplicative order of $a \mod n$</td>
</tr>
<tr>
<td>$\nu(m)$</td>
<td>(3.2.1)</td>
</tr>
<tr>
<td>$p</td>
<td>a$</td>
</tr>
<tr>
<td>$p\nmid a$</td>
<td>$p$ does not divide $a$</td>
</tr>
<tr>
<td>$p^2</td>
<td>a$</td>
</tr>
<tr>
<td>$S_{1,m}, S_{2,m}$</td>
<td>(3.2.5)</td>
</tr>
<tr>
<td>$I$</td>
<td>identity matrix</td>
</tr>
<tr>
<td>$J$</td>
<td>all-one matrix</td>
</tr>
<tr>
<td>$A^T$</td>
<td>transpose of the matrix $A$</td>
</tr>
</tbody>
</table>
Preface

In 1984, Leon, Masley and Pless introduced a new class of binary cyclic codes, the so-called duadic codes. These codes are defined in terms of their idempotents, and they are a direct generalization of quadratic residue codes.

In this thesis, duadic codes over an arbitrary finite field are defined in terms of their generator polynomials. In the binary case, this definition is equivalent to that of Leon, Masley and Pless.

In Chapter 1, we give a short introduction to coding theory. In Chapter 2, duadic codes of length \( n \) over \( \text{GF}(q) \) are defined. We show that they exist iff \( q = \text{mod } n \), i.e., if \( n = p_1^{m_1}p_2^{m_2} \cdots p_k^{m_k} \) is the prime factorization of \( n \), then duadic codes of length \( n \) over \( \text{GF}(q) \) exist iff \( q = \text{mod } p_i \), \( i=1,2,\ldots,k \).

Examples of duadic codes are quadratic residue codes, some punctured generalized Reed-Muller codes, and cyclic codes for which the extended code is self-dual. Furthermore, we give a construction of duadic codes of composite length with a low minimum distance. As an example, if \( n \) is divisible by 7, then there is a binary duadic code of length \( n \) with minimum distance 4.

In Chapter 3, we generalize the two papers of Leon, Masley and Pless on binary duadic codes. We show e.g., that the minimum odd-like weight in a duadic code satisfies a square root bound, just as in the case of quadratic residue codes.

In Chapter 4, we study duadic codes of length a prime power. It turns out that if \( p \nmid (q^t - 1) \), where \( t = \text{ord}_p(q) \), that duadic codes of length \( p^m \) over \( \text{GF}(q) \) have minimum distance \( \leq p^z \). If \( z=1 \), then we can strengthen this upper bound, and we can also give a lower bound on the minimum distance. As a consequence, we can determine the minimum distance of duadic codes of length \( p^m \) for several values of \( p \). For example, all binary duadic codes of length \( 7^m \) (\( m>1 \)) have minimum distance 4.

In Chapter 5, we consider tournaments which are obtained from splittings, and we ask whether they can be doubly-regular.

In Chapter 6, we show that a duadic code, whose minimum odd-like weight satisfies the specialized square root bound with equality, contains a projective plane. Furthermore, we give an (already known) existence test for cyclic projective planes.
Chapter 7 deals with single error-correcting duadic codes. We show that a binary duadic code with minimum distance 4 must have a length divisible by 7. In a special case we give an error-correction procedure. It turns out that most patterns of two errors can be corrected.

In the last section of Chapter 7, we show that if a duadic code of length $n \geq 9$ over GF(4) with minimum distance 3 exists, then $n$ is divisible by 3.

In Chapter 8, we give lower bounds on the minimum distance of cyclic codes. These bounds are used to analyze binary duadic codes of length $\leq 241$.

At the end of Chapter 8, we give a table of all these codes.
Chapter 1: Introduction to error-correcting codes

In this chapter we give a short introduction to coding theory. For a more extensive treatment the reader is referred to [10,12].

Section 1.1: Definitions

Let $q$ be a prime power, and let $GF(q)$ be the field consisting of $q$ elements.

A code $C$ of length $n$ over $GF(q)$ is a subset of the vector space $(GF(q))^n$. The elements of $C$ are called codewords.

A $k$-dimensional subspace of $(GF(q))^n$ is called a linear code. We call such a code a $q$-ary $[n,k]$ code.

If $x$ is a vector, then the weight $wt(x)$ of $x$, is the number of its non-zero coordinates. The distance $d(x,y)$ of two vectors $x$ and $y$, is the number of coordinates in which they differ. Note that $d(x,y) = wt(x-y)$.

If $C$ is a code, then the minimum distance $d$ of $C$ is defined as $d := \min\{d(x,y) | x,y \in C, x \neq y\}$.

If $C$ is a linear code, then the minimum distance $d$ of $C$ equals the minimum non-zero weight, i.e., $d = \min\{wt(x) | x \in C, x \neq 0\}$.

An $[n,k]$ code with minimum distance $d$ is denoted an $[n,k,d]$ code.

Let $C$ be an $[n,k]$ code over $GF(q)$. The extended code $\bar{C}$ is the $[n+1,k]$ code defined by

$$\bar{C} := \{(x_1,x_2,\ldots,x_{n+1}) | (x_1,x_2,\ldots,x_n) \in C, \sum_{i=1}^{n+1} x_i = 0\}.$$

Note that $\bar{C}$ is an even-like code.

The dual code $C^\perp$ of $C$ is defined as

$$C^\perp := \{x \in (GF(q))^n | \forall y \in C, (x,y) = 0\},$$

where $(,)$ is the usual inner-product, $(x,y) = x_1y_1 + x_2y_2 + \ldots + x_ny_n$. $C^\perp$ is an $[n,n-k]$ code.
If \( C \subseteq C^\perp \), then the code \( C \) is called **self-orthogonal**, and if \( C = C^\perp \), then \( C \) is called **self-dual**.

A **generator matrix** for \( C \) is a \( k \times n \) matrix \( G \), whose rows are a basis for \( C \). A **parity check matrix** \( H \) for \( C \) is a generator matrix for \( C^\perp \).

The matrices \( G \) and \( H \) satisfy \( G.H^T = 0 \).

Note that \( x \in C \) iff \( Hx^T = 0 \).

**Section 1.2: Cyclic codes**

A linear code \( C \) of length \( n \) is called **cyclic** if

\[ \forall (c_0, c_1, \ldots, c_{n-1}) \in C \implies (c_{n-1}, c_0, \ldots, c_{n-2}) \in C. \]

Now make the following identification between \((GF(q))^n\) and the residue class ring \( GF(q)[x]/(x^n - 1) \):

\[ (c_0, c_1, \ldots, c_{n-1}) \inGF(q))^n \iff c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1} \in GF(q)[x]/(x^n - 1). \]

Then we can interpret a linear code as a subset of \( GF(q)[x]/(x^n - 1) \).

(1.2.1) **Theorem**: A linear code \( C \) of length \( n \) over \( GF(q) \) is cyclic iff \( C \) is an ideal in \( GF(q)[x]/(x^n - 1) \).

We shall only consider cyclic codes of length \( n \) over \( GF(q) \) where \( (n, q) = 1 \).

Let \( C \) be a cyclic code in \( (GF(q))^n \), and let \( g(x) \) be the unique monic polynomial of lowest degree in \( C \). Then the ideal \( C \) is generated by \( g(x) \), i.e.,

\[ C = \langle g(x) \rangle := \{ a(x)g(x) \mod (x^n - 1) | a(x) \in GF(q)[x] \}. \]

The polynomial \( g(x) \) is called the **generator polynomial** of \( C \). If \( C \) has dimension \( k \), then \( g(x) \) has degree \( n-k \). Note that \( g(x) \) is a divisor of \( x^n - 1 \). It follows that there is a polynomial \( h(x) \), called the **check polynomial** of \( C \), such that \( x^n - 1 = g(x)h(x) \) (in \( GF(q)[x] \)).

This gives \( c(x) \in C \) iff \( c(x)h(x) = 0 \) (in \( GF(q)[x]/(x^n - 1) \)).

The dual code of \( C \) equals \( \langle h(x) \rangle \), which is obtained from \( \langle h(x) \rangle \), by reversing the order of the symbols.
Let $a$ be a primitive $n$-th root of unity in an extension field of $\text{GF}(q)$, and let $S \subseteq \{0,1,\ldots,n-1\}$. We can define a cyclic code $C$ of length $n$ over $\text{GF}(q)$ as follows:

$$c(x) \in C \iff c(a^i) = 0, \ i \in S$$

(and every cyclic code can be defined in this way).

The set $\{a^i | i \in S\}$ is called a defining set for $C$. If this set is the maximal defining set for $C$, then it is called complete.

Note that if $A$ is a complete defining set, we have $a^i \in A \Rightarrow a^q i \in A$.

(1.2.2) Lemma: If a cyclic code $C$ contains an odd-like vector, then it also contains the all-one vector $j(x)$.

Proof: Let $g(x)$ resp. $h(x)$ be the generator resp. check polynomial of $C$. Since $C$ contains an odd-like vector, we have $g(1) \neq 0$, and hence $h(1) = 0$.

So $j(x) = \frac{x^n - 1}{x - 1} \cdot h(x) \cdot g(x) \in C$. Q.E.D.

Section 1.3: The idempotent of a cyclic code

(1.3.1) Theorem: A cyclic code $C$ contains a unique codeword $e(x)$, which is an identity element for $C$.

Since $(e(x))^2 = e(x)$, this codeword is called the idempotent of $C$. Furthermore, the code $C$ is generated by $e(x)$, since all codewords $c(x)$ can be written as $c(x)e(x)$.

(1.3.2) Theorem: If $C_1$ and $C_2$ are cyclic codes with idempotents $e_1(x)$ and $e_2(x)$, then

(i) $C_1 \cap C_2$ has idempotent $e_1(x)e_2(x)$,

(ii) $C_1 + C_2$ has idempotent $e_1(x) + e_2(x) - e_1(x)e_2(x)$.

Let $a$ be a primitive $n$-th root of unity in an extension field of $\text{GF}(q)$, and let $C$ be the cyclic code of length $n$ over $\text{GF}(q)$ with complete defining set $\{a^i | i \in S\}$. 

Theorem: If $e(x) \in GF(q)[x]/(x^n-1)$, then $e(x)$ is the idempotent of $C$ iff
$$e(a^i) = 0 \text{ if } i \in S, \text{ and } e(a^i) = 1 \text{ if } i \in \{0, 1, \ldots, n-1\} \setminus S.$$ 

Proof: (i) Suppose $e(a^i) = 0$ if $i \in S$, and $e(a^i) = 1$ if $i \in T := \{0, 1, \ldots, n-1\} \setminus S$.

Let $g(x) := \prod (x-a^i)$ (g(x) is the generator polynomial of $C$).

Then $g(x)$ divides $e(x)$, so $e(x) \in C$.

Let $h(x) := \prod (x-a^i) = \frac{x^n-1}{g(x)}$. Then $h(x)$ divides $1-e(x)$, so there is a polynomial $b(x)$, such that $1-e(x) = b(x)h(x)$.

Let $a(x)g(x)$ be a codeword in $C$. Then $a(x)g(x)e(x) \equiv a(x)g(x) \mod (x^n-1)$. Hence $e(x)$ is an identity element for $C$.

(ii) If $e(x)$ is the idempotent of $C$, then $(e(x))^2 = e(x)$, and $e(x)$ generates the code. \hfill \Box
Chapter 2 : Duadic codes

In this chapter we define duadic codes over GF(q) in terms of their generator polynomials. We show that in the binary case our definition is equivalent to that of Leon, Masley and Pless [6], who defined binary duadic codes in terms of their idempotents. Furthermore we investigate for which lengths duadic codes exist, and we give some examples. In the last section of this chapter we give a construction of duadic codes of composite length with a low minimum distance.

Section 2.1 : Definition of duadic codes

Let q be a prime power, and let n be an odd integer, such that \( (n,q) = 1 \). If \( 0 \leq i < n \), then the cyclotomic coset of \( i \mod n \) is the set
\[
C_i := \{ i, q_1 i \mod n, q_2 i \mod n, \ldots \}.
\]
If \( a \) is an integer such that \( (a,n) = 1 \), then \( \mu_a \) denotes the permutation \( i \mapsto ai \mod n \).

**(2.1.1) Definition** : Let \( S_1 \) and \( S_2 \) be unions of cyclotomic cosets \( \mod n \), such that \( S_1 \cap S_2 = \emptyset \) and \( S_1 \cup S_2 = \{1,2,\ldots,n-1\} \). Suppose there is an \( a \), \( (a,n) = 1 \), such that the permutation \( \mu_a \) interchanges \( S_1 \) and \( S_2 \). Then \( \mu_a : S_1 \leftrightarrow S_2 \) is called a splitting \( \mod n \).

Let \( a \) be a primitive \( n \)-th root of unity in an extension field of GF(q), and let \( \mu_a : S_1 \leftrightarrow S_2 \) be a splitting \( \mod n \).

Define \( g_1(x) := \prod_{i \in S_1} (x - \alpha^i) \), \( g_2(x) := \prod_{i \in S_2} (x - \alpha^i) \).

Note that \( g_1(x) \) and \( g_2(x) \) are polynomials in \( \text{GF}(q)[x] \), since
\[
g_k(x^q) = (g_k(x))^q, \quad k=1,2.
\]

**(2.1.2) Definition** : A cyclic code of length \( n \) over \( \text{GF}(q) \) is called a duadic code if its generator polynomial is one of the following:
\( g_1(x) \), \( g_2(x) \), \( (x-1)g_1(x) \) or \( (x-1)g_2(x) \).
Example: Let \( n \) be an odd prime, such that \( q \equiv 0 \mod n \) (i.e., there is an \( x \neq 0 \mod n \), such that \( q = x^2 \mod n \); if such an \( x \neq 0 \mod n \) does not exist, then we write \( q \equiv \varnothing \mod n \)).

Now take \( S_1 := \{ 0 < i < n | i \equiv 0 \mod n \} \), \( S_2 := \{ 0 < i < n | i \equiv \varnothing \mod n \} \).

Since \( q \equiv 0 \mod n \), the sets \( S_1 \) and \( S_2 \) are unions of cyclotomic cosets \( \mod n \).

Let \( a \in S_2 \). Then \( \mu_a : S_1 \to S_2 \) is a splitting \( \mod n \), and the corresponding duadic codes are quadratic residue codes (QR codes, cf. [10]).

Now let \( q = 2 \). We shall show that Definition (2.1.2) is equivalent to the definition of Leon, Massey and Pless in [6].

Let \( \mu_a : T_1 \to T_2 \) be a splitting \( \mod n \), and define

\[
\begin{align*}
e_1(x) &= \sum_{i \in T_1} x^i, \\
e_2(x) &= \sum_{i \in T_2} x^i \quad \text{(these are polynomials in } \GF(2)[x])
\end{align*}
\]

Note that \( (e_k(x))^2 = e_k(x), \ k=1,2 \).

Definition (Leon, Massey, Pless):

A binary cyclic code of length \( n \) is called a duadic code if its idempotent is one of the following:

\( e_1(x), e_2(x), 1+e_1(x) \) or \( 1+e_2(x) \).

Theorem: A binary cyclic code is duadic according to (2.1.2) iff it is duadic according to (2.1.4).

Proof: Let \( a \) be a primitive \( n \)-th root of unity in an extension field of \( \GF(2) \).

(i) Let \( \mu_a : S_1 \to S_2 \) be a splitting \( \mod n \), and let \( C_k \) be the duadic code (according to (2.1.2)) with generator polynomial

\[
g_k(x) = \prod_{i \in S_k} (x-a^i), \ k=1,2.
\]

Suppose the code \( C_k \) has idempotent \( e_k(x) = \sum_{i \in T_k} x^i, \ k=1,2 \).

Since \( C_1 \cap C_2 = \langle g_1(x)g_2(x) \rangle = \langle j(x) \rangle \) has idempotent \( j(x) \), we have \( e_1(x)e_2(x) = j(x) \).

Now \( \dim(C_1+C_2) = \dim C_1 + \dim C_2 - \dim (C_1 \cap C_2) = n \).
so $C_1 + C_2 = (GF(2))^n$. Comparing idempotents we find
\[ e_1(x) + e_2(x) + e_1(x)e_2(x) = 1, \text{ and hence} \]
\[ e_1(x) + e_2(x) = x + x^2 + x^3 + \ldots + x^{n-1}. \]
It follows that $T_1 \setminus \{0\} \cap T_2 \setminus \{0\} = \emptyset$ and $T_1 \setminus \{0\} \cup T_2 \setminus \{0\} = \{1, 2, \ldots, n-1\}$. It is obvious that $T_1$ and $T_2$ are unions of cyclotomic cosets mod $n$. Since $e_1(a^i) = \begin{cases} 0 & \text{if } i \in S_2, \\ 1 & \text{if } i \in \{0, 1, 2, \ldots, n-1\} \setminus S_2, \end{cases}$ we have $e_2(x) = e_1(x^2)$ (cf. Theorem (1.3.3)).
We have shown that $\mu : T_1 \setminus \{0\} 
\supset T_2 \setminus \{0\}$ is a splitting mod $n$, and hence $C_1$ and $C_2$ are duadic codes according to (2.1.4).
By comparing zeros, we see that the duadic codes generated by $(x-1)g_1(x)$ resp. $(x-1)g_2(x)$ have idempotents $1 + e_2(x)$ resp. $1 + e_1(x)$, and hence they are duadic codes according to (2.1.4).

(ii) Let $\mu : T_1 \supset T_2$ be a splitting mod $n$, and let $C_k$ be the duadic code (according to (2.1.4)) with idempotent $e_k(x) = \epsilon_0 + \sum x^i$, $k = 1, 2$ ($\epsilon_0 \in GF(2)$ is chosen such that $e_k(x)$ has odd weight).
Note that $e_1(x) + e_2(x) = 1 + j(x)$.
Suppose the code $C_k$ has complete defining set $\{a^i | i \in S_k\}$, $k = 1, 2$.
Obviously $S_1$ and $S_2$ are unions of cyclotomic cosets mod $n$, and $0 \notin S_k$, $k = 1, 2$.
Since $e_1(a^i) + e_2(a^i) = 1 + j(a^i) = 1$ ($i \neq 0$), we have $S_1 \cap S_2 = \emptyset$, and $S_1 \cup S_2 = \{1, 2, \ldots, n-1\}$.
If $i \in S_1$, then $e_2(a^i) = e_1(a^i) = 0$, so $ai \in S_2$.
It follows that $\mu : S_1 \supset S_2$ is a splitting mod $n$, so $C_1$ and $C_2$ are duadic codes according to (2.1.2).
Let $C_1'$ resp. $C_2'$ be the duadic code with idempotent $1 + e_2(x)$ resp. $1 + e_1(x)$. By comparing zeros we see that $C_1'$ is the even weight subcode of $C_k$, so $C_k'$ is duadic according to (2.1.2), $k = 1, 2$.

(2.1.6) Remark: In [14] Pless introduced a class of cyclic codes over $GF(4)$, called Q-codes, in terms of their idempotents. In the same way as in Theorem (2.1.5) it can be shown that these codes are duadic codes over $GF(4)$ and vice versa.
The next theorem tells us for which lengths duadic codes exist.
Again, let \( q \) be a prime power.

**Theorem (2.1.7):** Let \( n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} \) be the prime factorization of the odd integer \( n \).
A splitting mod \( n \) exists (and hence duadic codes of length \( n \) over \( \text{GF}(q) \)) iff \( q = d \mod p_i \), \( i = 1, 2, \ldots, k \).

Before proving this theorem, we give some lemmas.

**Lemma (2.1.8):** Let \( p \) be an odd prime.
A splitting mod \( p \) exists iff \( q = d \mod p \).

**Proof:**
(i) In (2.1.3) we have seen that a splitting mod \( p \) exists if \( q = d \mod p \).

(ii) Suppose a splitting mod \( p \) exists.
Let \( N \) be the number of non-zero cyclotomic cosets mod \( p \), then \( N \) must be even. Let \( G \) be the cyclic multiplicative group of \( \text{GF}(p) \), and let \( H \) be the subgroup of \( G \) generated by \( q \). Let \( Q \) be the subgroup of \( G \) consisting of the squares mod \( p \). Note that each coset mod \( p \) contains \( |H| \) elements. Then we have \(|G| = N, |H| = 2|Q| \), and hence \(|H| \) divides \(|Q| \).
Because a cyclic group contains for each divisor \( d \) of its order exactly one subgroup of order \( d \), we see that \( H \) is a subgroup of \( Q \).
We have shown that \( q \in Q \), i.e. \( q = d \mod p \).

**Lemma (2.1.9):** Let \( p \) be an odd prime, such that \( q = d \mod p \), and let \( m \geq 1 \). Then there is a splitting mod \( p^m \).

**Proof:** The proof is by induction on \( m \).
For \( m = 1 \) the assertion follows from Lemma (2.1.8).
Now let \( \mu_a : S_1 \leftrightarrow S_2 \) be a splitting mod \( p^m \), and let \( \mu_a : T_1 \leftrightarrow T_2 \) be a splitting mod \( p \) (remark that both splittings are given by \( \mu_a \)). Define \( R_k := \{ip \mid i \in S_k \} \cup \{i+jp \mid i \in T_k, 0 \leq j < p^m \}, k = 1, 2 \).
It is easy to show that \( \mu_a : R_1 \leftrightarrow R_2 \) is a splitting mod \( p^{m+1} \).

**Lemma (2.1.10):** Let \( 1 \) and \( m \) be odd integers, \( (1,m) = 1 \), such that splittings mod \( 1 \) and mod \( m \) exist.
Then there is a splitting mod \( 1m \).
Proof: Let $\mu_a: S_1 \rightarrow S_2 \mod 1$ and $\mu_b: T_1 \rightarrow T_2 \mod m$ be splittings.

Define $R_k := \{i\mid i \in S_k\} \cup \{i+jm\mid i \in T_k, 0 \leq j < 1\}, k=1,2.$

Choose $c$ such that $c\equiv a \mod 1, c\equiv b \mod m$ (such a $c$ exists by the Chinese Remainder Theorem). Note that $(c,1m)=1$.

Then $\mu_c: R_1 \rightarrow R_2$ is a splitting mod $lm$. \hfill \Box

Proof of Theorem (2.1.7):

(i) Suppose $q\equiv \square \mod p_i, i=1,2,\ldots,k$. From Lemmas (2.1.9) and (2.1.10) it follows that a splitting mod $n$ exists.

(ii) Let $\mu_a: S_1 \rightarrow S_2$ be a splitting mod $n$, and let $p$ be a prime, $p|n$. Choose $m$ such that $n=pm$.

Now define $T_k := \{i\mid i < p| \in \mathbb{N}\}, k=1,2$. Then $\mu_a: T_1 \rightarrow T_2$ is a splitting mod $p$, and then Lemma (2.1.8) shows that $q\equiv \square \mod p$. \hfill \Box

(2.1.11) Examples: Let $n = p_1^{m_1}p_2^{m_2}\ldots p_k^{m_k}$ be the prime factorization of the odd integer $n$.

(i) Binary duadic codes of length $n$ exist iff $p_i\equiv \square \mod 8, i=1,2,\ldots,k$.

(ii) Ternary duadic codes of length $n$ exist iff $p_i\equiv \square \mod 12, i=1,2,\ldots,k$.

(iii) Duadic codes of length $n$ over $\mathbb{GF}(4)$ exist for all odd $n$.

(2.1.12) Theorem: Let $n = p_1^{m_1}p_2^{m_2}\ldots p_k^{m_k}$ be the prime factorization of the odd integer $n$. Let $q$ be a prime power such that $(n,q)=1$.

Then $q\equiv \square \mod n$ iff $q\equiv \square \mod p_i, i=1,2,\ldots,k$.

We shall first prove the following lemma.

(2.1.13) Lemma: Let $p$ be an odd prime such that $p|q$, and let $m\geq 1$.

If $q\equiv \square \mod p^m$, then $q\equiv \square \mod p^{m+1}$.

Proof: Suppose $q\equiv \square \mod p^m$. Then there are integers $x$ and $k$, such that $q = x^2 + kp^m$. Now choose $t$ such that $2xt\equiv k \mod p$ (note that $(p,q)=1$, and hence $(p,x)=1$). Then $q\equiv (x+tp^m)^2 \mod p^{m+1}$. \hfill \Box

Proof of Theorem (2.1.12):

Suppose $q\equiv \square \mod p_i, i=1,2,\ldots,k$. Then, by Lemma (2.1.13), we have $q\equiv \square \mod p_i^{m_i}, i=1,2,\ldots,k$.

So there are integers $x_i$, such that $q\equiv x_i^2 \mod p_i^{m_i}, i=1,2,\ldots,k$.

By the Chinese Remainder Theorem, there is an integer $x$, such that $x\equiv x_1 \mod p_1^{m}, x\equiv x_2 \mod p_2^{m}, \ldots, x\equiv x_k \mod p_k^{m}$. \hfill \Box
Then \( q = x^2 \mod p_i^{m_i} \) for \( i = 1, 2, \ldots, k \), and hence \( q = x^2 \mod n \).

The converse is obvious. \( \square \)

\((2.1.14)\) **Corollary**: Duadic codes of length \( n \) over \( \text{GF}(q) \) exist iff \( q = \varnothing \mod n \).

### Section 2.2: Examples of duadic codes

In the last section we saw that QR codes of prime length over \( \text{GF}(q) \) are duadic codes. We now give some other examples. For a list of binary duadic codes the reader is referred to Chapter 8.

\((2.2.1)\) We take \( q = 2^r \), \( n = q - 1 \).

Remark that each cyclotomic coset \( \mod n \) contains exactly one element.

Now let \( S_1 := \{ i \mid 1 \leq i \leq n-1 \} \), \( S_2 := \{ i \mid \frac{n+1}{2} \leq i \leq n-1 \} \). Then \( \varphi : S_1 \rightarrow S_2 \) is a splitting \( \mod n \). The corresponding duadic codes of length \( n \) over \( \text{GF}(q) \) are Reed-Solomon codes with minimum distance \( \frac{n+1}{2} \) (cf. [10]).

\((2.2.2)\) Again take \( q = 2^r \). Let \( m \) be odd, \( n = q^m - 1 \).

Let \( c_q(i) \) be the sum of the digits of \( i \), if \( i \) is written in the \( q \)-ary number system. We define \( S_1 := \{ 1 \leq i < n \mid c_q(i) < \frac{m(q-1)-1}{2} \} \), \( S_2 := \{ 1 \leq i < n \mid c_q(i) \geq \frac{m(q-1)+1}{2} \} \).

Since \( c_q(i) = c_q(qi \mod n) \), the sets \( S_1 \) and \( S_2 \) are unions of cyclotomic cosets \( \mod n \).

Since \( c_q(-i \mod n) = m(q-1) - c_q(i) \), the sets \( S_1 \) and \( S_2 \) are interchanged by \( \varphi_{-1} \).

Hence we have a splitting \( \varphi_{-1}: S_1 \rightarrow S_2 \mod n \).

The corresponding duadic codes are punctured generalized Reed-Muller codes \( \text{RM}(m, \frac{m(q-1)-1}{2}, q)^* \) with minimum distance \( \frac{1}{2}(q+2)q^\frac{1}{2}(m-1) - 1 \) (cf. [9]).

If we take \( m = 1 \), then we get the Reed-Solomon codes of \( (2.2.1) \).

If \( q = 2 \), we get the punctured Reed-Muller codes \( \text{RM}(\frac{m-1}{2}, m)^* \) with minimum distance \( 2^\frac{1}{2}(m+1) - 1 \) (cf. [12]).

\((2.2.3)\) **Theorem**: Let \( C \) be a cyclic code of length \( n \) over \( \text{GF}(q) \), and suppose that the extended code \( \overline{C} \) is self-dual. Then \( C \) is a duadic code, and the splitting is given by \( \varphi_{-1} \).
Proof: Let $\alpha$ be a primitive $n$-th root of unity, and let $\{\alpha^i | i \in S_1\}$ be the complete defining set of $C$.

If $0 \in S_1$, then $C$ is an even-like code, so it is an $[n,\frac{n+1}{2}]$ self-dual code, which is impossible. Hence $0 \not\in S_1$.

The code $C^\perp$ has complete defining set $\{\alpha^{-i} | i \in S_2 \cup \{0\}\}$, where $S_2 := \{1, 2, \ldots, n-1\} \setminus S_1$.

Let $C'$ be the even-like subcode of $C$. Since $\overline{C}$ is self-dual, we have $C' \subseteq C^\perp$, and hence $C' = C^\perp$ (note that $\dim C' = \dim C^\perp$).

If we compare the defining sets of $C'$ and $C^\perp$, we see that $S_2 = -S_1 \mod n$.

Hence $\mu_{-1} : S_1 \rightarrow S_2$ is a splitting $\mod n$, which shows that $C$ is a duadic code.

Section 2.3: A construction of duadic codes of composite length

Let $\mu_a : T_1 \rightarrow T_2 \mod 1$ and $\mu_a : U_1 \rightarrow U_2 \mod m$ be splittings (both splittings are given by $\mu_a$).

Let $a$ be a primitive $n$-th root of unity in an extension field of $GF(q)$, where $n = \ell m$.

Then $\beta = a^{\frac{1}{\ell}}$ is a primitive $m$-th root of unity.

Let $C_0$ be the even-like duadic code of length $m$ over $GF(q)$ with complete defining set $\{\beta^i | i \in U_1 \cup \{0\}\}$ and minimum distance $d$.

We shall construct a duadic code of length $n$ with minimum distance $\leq d$.

If we take $S_k := \{im | i \in T_k\} \cup \{i+jm | i \in U_k, 0 \leq j < 1\}, k=1,2$, then we have a splitting $\mu_a : S_1 \rightarrow S_2 \mod n$.

Let $C$ be the duadic code of length $n$ over $GF(q)$ with complete defining set $\{\alpha^i | i \in S_1\}$.

(2.3.1) Theorem: The code $C$ has minimum distance $\leq d$.

Proof: Let $c_0(x)$ be a codeword in $C_0$ of weight $d$. Then the word $c(x) := c_0(x^i) \in GF(q)[x]/(x^n-1)$ also has weight $d$.

Note that $c(\alpha^i) = c_0(\alpha^i) = c(\beta^i)$.

Let $k \in S_1$.

(i) If $k = \ell m \mod n$, where $i \in T_1$, then $c(\alpha^k) = c_0(\beta^{im}) = c_0(1) = 0$.

(ii) If $k = i+jm \mod n$, where $i \in U_1$, $0 \leq j < 1$, then $c(\alpha^k) = c_0(\beta^i) = 0$.

It follows that $c(x)$ is a codeword in $C$.
(2.3.2) **Remark**: Since the codeword $c(x)$ in the proof is even-like, we see that the even-like subcode of $C$ also has minimum distance $\leq d$.

(2.3.3) **Theorem**: Let $l$ and $m$ be odd integers, $(l,m)=1$, and suppose that splittings mod $l$ and mod $m$ exist. If an even-like duadic code of length $m$ has minimum distance $d$, then there is a duadic code of length $n:=lm$ with minimum distance $\leq d$.

**Proof**: Let $\mu_a$ resp. $\mu_b$ give splittings mod $l$ resp. mod $m$. Choose $c$ such that $c=a \mod l$, $c=b \mod m$, and continue as on page 11. \(\square\)

(2.3.4) **Examples**: (i) Take $q=2$, $n$ divisible by 7 (we suppose that duadic codes of length $n$ exist). Write $n=7^k \mod m$, $7\mid n$.

The even-weight duadic code of length 7 has minimum distance 4. According to (2.3.1) and (2.3.2) there is an even-weight duadic code of length $7^k$ with minimum distance $\leq 4$.

If we apply Theorem (2.3.3) (suppose that $m>1$), we get a duadic code of length $n$ with minimum distance $\leq 4$.

(ii) Now we take $q=4$, and $n$ divisible by 3.

In the same way it can be shown that there is a duadic code of length $n$ over $GF(4)$ with minimum distance $\leq 3$.

In Chapter 7 we shall study binary duadic codes with minimum distance 4, and duadic codes over $GF(4)$ with minimum distance 3.
Chapter 3: Properties of duadic codes

In this chapter we generalize the results about binary duadic codes from [7].

Section 3.1: Some general theorems

Let \( \nu_a : \mathbb{Z}_1 \rightarrow \mathbb{Z}_2 \) be a splitting mod \( n \), and let \( a \) be a primitive \( n \)-th root of unity in an extension field of \( \mathbb{F}_q \).

Let \( C_k \) be the duadic code of length \( n \) over \( \mathbb{F}_q \) with defining set \( \{a^i | i \in S_k \} \), and with even-like subcode \( C_k' \). Let \( e_k(x) \) be the idempotent of \( C_k \) \( (k=1,2) \).

(3.1.1) \( \text{Theorem} \):

(i) \( \dim C_k = \frac{n+1}{2}, \dim C_k' = \frac{n-1}{2}, k=1,2. \)
(ii) \( C_1 \cap C_2 = \langle 1 \rangle, C_1 + C_2 = (\mathbb{F}_q)^n. \)
(iii) \( C_1' \cap C_2' = \{0\}, C_1' + C_2' = \{x \in (\mathbb{F}_q)^n | x \text{ even-like}\}. \)
(iv) \( C_k = C_k' \perp \langle 1 \rangle, k=1,2 \) (\( \perp \) denotes an orthogonal direct sum).
(v) \( e_1(x)e_2(x) = \frac{1}{n} \cdot j(x) \) \( (\frac{1}{n} \) is the multiplicative inverse of \( n = 1+1+\ldots+1 \) in \( \mathbb{F}_q \)).
(vi) \( e_1(x) + e_2(x) = 1 + \frac{1}{n} \cdot j(x). \)
(vii) \( C_1' \) has idempotent \( 1-e_2(x) \), \( C_2' \) has idempotent \( 1-e_1(x) \).

Proof: (i) is obvious.

(ii) \( C_1 \cap C_2 \) has defining set \( \{a^i | i=1,2,\ldots,n-1\} \), which shows that \( C_1 \cap C_2 = \langle 1 \rangle \). From \( \dim (C_1+ C_2) = \dim C_1 + \dim C_2 - \dim (C_1 \cap C_2) = n \), it follows that \( C_1 + C_2 = (\mathbb{F}_q)^n \). The proof of (iii) is the same.

(iv) Since \( C_k \) contains odd-like vectors, we have \( 1 \notin C_k' \), and so \( C_k' \perp \langle 1 \rangle \subseteq C_k \). The code \( C_k' \) contains only even-like vectors, so \( C_k' \cap \langle 1 \rangle = \{0\} \). It follows that \( \dim (C_k' + \langle 1 \rangle) = \dim C_k \).

Since for all \( x \in C_k' \), \( (c,1) = 0 \), we have proved that \( C_k' \perp \langle 1 \rangle = C_k \), \( k=1,2 \).

(v) and (vi) follow from (ii), (iii) and Theorem (1.3.2).

(vii) follows from Theorem (1.3.3).

(3.1.2) \( \text{Theorem} \): The codes \( C_k \) and \( C_k' \) are dual iff \( \nu_{-1} \) gives the splitting \( (k=1,2) \).
(3.1.3) **Theorem**: The codes $C_1$ and $C_2'$ are dual iff $\mu_{-1}$ leaves them invariant.

**Proof**: Compare the defining sets of $C_1$ and $C_2'$. □

(3.1.4) **Theorem**: Let $c$ be an odd-like codeword in $C_k$ with weight $d$. Then the following holds:

(i) $d^2 \geq n$.

Now suppose the splitting is given by $\mu_{-1}$. Then

(ii) $d^2 - d + 1 \geq n$,

(iii) if $q = 2$ and $d^2 - d + 1 > n$, then $d^2 - d + 1 \geq n + 12$,

(iv) if $q = 2$, then $d = \frac{n}{2} \mod 4$, and all weights in $C_k'$ are divisible by 4.

**Proof**: The proofs of (i), (ii) and (iii) are the same as for QR codes (cf. [10],[17]).

(iv) We know that $n \equiv \pm 1 \mod 8$ (from (2.1.11)). From Definition (2.1.4) it follows that the idempotent of $C_k'$ has weight $\frac{n+1}{2}$ or $\frac{n-1}{2}$. Since this idempotent must have even weight, it follows that it has weight divisible by 4. Using Theorem (3.1.2), we see that $C_k'$ is self-orthogonal. Hence all weights in $C_k'$ are divisible by 4.

There is a codeword $c'$ in $C_k'$ such that $c = c' + 1$ (cf. Theorem (3.1.1)(iv)). So $d = \text{wt}(c') + \text{wt}(1) - 2(c', 1) \equiv n \mod 4$. □

In Chapter 6 we shall consider duadic codes for which equality holds in (3.1.4)(ii).

**Section 3.2: Splittings and the permutation $\mu_{-1}$**

In this section we investigate when a splitting is given by $\mu_{-1}$, and also when a splitting is left invariant by $\mu_{-1}$. In both cases we know the duals of the corresponding duadic codes by Theorems (3.1.2) and (3.1.3).

(3.2.1) **Notations**: If $a$ and $n$ are integers, $(a, n) = 1$, then $\text{ord}_n(a)$ denotes the multiplicative order of $a \mod n$. 
If $p$ is a prime and $m$ a positive integer, then we denote by $v_p(m)$ the exponent to which $p$ appears in the prime factorization of $m$.

The proof of the following theorem can be found in [8].

(3.2.2) **Theorem** : Let $p$ be an odd prime, and let $a$ be an integer such that $p \nmid a$. Let $t := \text{ord}_p(a)$, $z := v_p(a^{t-1}-1)$, i.e. $p \nmid (a^{t-1}-1)$. Then

$$
\text{ord}_p(m)(a) = \begin{cases} 
t & \text{if } m \leq z, \\
t p^{m-z} & \text{if } m > z.
\end{cases}
$$

(3.2.3) **Lemma** : Let $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ be the prime factorization of the odd integer $n$ (assume that the $p_i$'s are distinct primes). Let $a$ be an integer such that $(a,n)=1$. Then the following holds:

(i) $\text{ord}_n(a) = \text{lcm}(\text{ord}_{p_i}^m(a))_{i=1,2,\ldots,k}$

(ii) $v_2(\text{ord}_n(a)) = v_2(\text{lcm}(\text{ord}_{p_i}^m(a))_{i=1,2,\ldots,k})$.

**Proof** : (i) is obvious. The proof of (ii) follows from (3.2.2).

The following trivial lemma will be used several times.

(3.2.4) **Lemma** : If $a$ gives a splitting, then $a_i$ gives the same splitting if $i$ is odd, and it leaves the splitting invariant if $i$ is even.

(3.2.5) **Remark** : Let $\mu_a : S_1 \to S_2$ be a splitting mod $n$, where $n = km$, $k>1$, $m>1$.

Define $S(k) := \{1 \leq i < n \mid (i,n)=k\}$.

Since $(a,n)=1$, the permutation $\mu_a$ acts on $S(k)$, i.e. if $i \in S(k)$, then $a_i \equiv a \pmod{n} \in S(k)$. So there are disjoint subsets $S_{1,m}$ of $S(k) \cap S_1$, $i=1,2$, with $S(k) = S_{1,m} \cup S_{2,m'}$, which are interchanged by $\mu_a$.

If $m$ is a prime, this splitting of $S(k)$ looks like a splitting mod $m$, except that all the elements of $S(k)$ are multiples of $k$. 
Lemma: Let \( n = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k} \) be the prime factorization of the odd integer \( n \), and let \( \mu_a : S_1 \rightarrow S_2 \) be a splitting mod \( n \).

Let \( r := \text{ord}_n(a) \). Then the following holds:

(i) \( r \) is even,

(ii) \( \mu_a \) gives the same splitting as \( \mu_{-1} \) iff \( r \equiv 2 \pmod{4} \),

(iii) if \( \mu_{-1} \) leaves the splitting invariant, then \( \text{ord}_{p_i}(a) \equiv 0 \pmod{4} \), \( i = 1, 2, \ldots, k \),

(iv) suppose \( v_2(\text{ord}_n(a)) \) is the same for each \( i \), say \( v \), then \( \mu_a \) gives the same splitting as \( \mu_{-1} \) if \( v = 1 \), and \( \mu_{-1} \) leaves the splitting invariant if \( v > 1 \).

Proof: (i) follows from Lemma (3.2.4).

(ii) Suppose \( r \equiv 2 \pmod{4} \), i.e. \( u := \frac{r}{2} \) is odd. Let \( 1 \leq i \leq k \), \( p_i = p_i \), \( m_i = m_i \).

Since \( \mu_a \) gives the same splitting as \( \mu_u \), we see that \( \mu_a \) interchanges \( S_1, p \) and \( S_2, p \) (using the notation of (3.2.5)), and hence \( a^u \equiv 1 \pmod{p} \).

We know that \( a^2 \equiv 1 \pmod{p} \), so \( a^u \equiv -1 \pmod{p} \). Now from \( a^2 \equiv 1 \pmod{p^m} \) and since \( p \) cannot divide both \( a^u + 1 \) and \( a^u - 1 \), it follows that \( a^u \equiv -1 \pmod{p^m} \).

Hence \( a^u \equiv -1 \pmod{n} \), and \( \mu_a \) gives the same splitting as \( \mu_{-1} \).

Conversely suppose that \( \mu_a \) gives the same splitting as \( \mu_{-1} \).

Suppose \( r \equiv 0 \pmod{4} \).

By Lemma (3.2.3)(ii), there is an \( i \), such that \( \text{ord}_p(a) = 4w \) for some \( w \) (again \( p = p_i \)). Now \( a^{2w} \equiv -1 \pmod{p} \), so \( \mu_a^{2w} \) interchanges \( S_1, p \) and \( S_2, p \), since \( \mu_{-1} \) does. On the other hand (by Lemma (3.2.4)) \( \mu_a^{2w} \) leaves \( S_1 \), and hence \( S_1, p \), invariant. So we have a contradiction.

(iii) Suppose \( \mu_{-1} \) leaves the splitting invariant.

Let \( 1 \leq i \leq k \), \( p_i = p_i \), \( s := \text{ord}_p(a) \). We know that \( s \) is even, \( s = 2t \).

Then \( a^t \equiv 1 \pmod{p} \), so \( \mu_a^t \) leaves \( S_1, p \) invariant, since \( \mu_{-1} \) does.

Lemma (3.2.4) shows that \( t \) is even, and hence \( s \equiv 0 \pmod{4} \).

(iv) Suppose \( v := v_2(\text{ord}_n(a)) \) is the same for each \( i \).

If \( v = 1 \), then by Lemma (3.2.3)(ii) we have \( r \equiv 2 \pmod{4} \), so \( \mu_a \) gives the same splitting as \( \mu_{-1} \).

Suppose \( v > 1 \). For each \( i \) there is an odd \( w_i \) such that \( \text{ord}_{p_i}(a) = 2^{v_i} w_i \).

It follows that \( a^{2^{v_i-1} w_i} \equiv -1 \pmod{p_i^{m_i}} \).

Let \( w := \text{lcm}(w_i) \), \( i = 1, 2, \ldots, k \). Then \( a^{2^{v_i} w} = \text{ord}_n(a) \), and \( a^{2^{v_i} w} \equiv -1 \pmod{p_i^{m_i}} \) for each \( i \).

So \( a^{2^{v_i} w} \equiv -1 \pmod{n} \). Since \( 2^{v_i} w \) is even, \( \mu_{-1} \) leaves the splitting.
(3.2.7) Theorem: Let \( n = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k} \) be the prime factorization of the odd integer \( n \), such that \( q^m \equiv 1 \mod p_i \), \( p_i \equiv -1 \mod 4 \), \( i = 1, 2, \ldots, k \).

Then all splittings mod \( n \) are given by \( u_{-1} \).

Proof: Let \( u_a \) give a splitting mod \( n \), and let \( r = \text{ord}_n (a) \).

By Lemma (3.2.6) it suffices to show that \( r \equiv 2 \mod 4 \).

Let \( 1 \leq i \leq k \), \( p_i = p_i \). We saw in (3.2.5) that \( u_a \) acts like a splitting on \( S(\frac{n}{p_i}) \). Hence \( s = \text{ord}_{p_i}(a) \) is even, and \( a^{\frac{s}{2}} \equiv -1 \mod p_i \).

Since \(-1 \equiv 0 \mod p_i \), it follows that \( \frac{s}{2} \) is odd.

Then Lemma (3.2.3)(ii) shows that \( r \equiv 2 \mod 4 \).

(3.2.8) Theorem: Let \( n \) be as in Theorem (3.2.7), except that at least one \( p_i \equiv 1 \mod 4 \).

Then there is a splitting mod \( n \), which is not given by \( u_{-1} \).

Proof: Suppose that \( p_i \equiv 1 \mod 4 \).

Let \( n_i \equiv 0 \mod p_i \), \( i = 1, 2, \ldots, k \).

Let \( a \equiv n_i \mod p_i^{m_i} \), \( i = 1, 2, \ldots, k \) (such an \( a \) exists by the Chinese Remainder Theorem).

Suppose there is an \( i \) such that \( p_i \mid a \). Then \( n_i \equiv a \equiv 0 \mod p_i \); but \( n_i \equiv 0 \mod p_i \). So \( (a, n) = 1 \).

Now consider \( u_a \) as acting on the non-zero cyclotomic cosets mod \( n \).

Then each orbit of \( u_a \) has an even number of cyclotomic cosets:

Let \( 1 \leq x < n \), \( b \) and \( m \) integers such that \( a^b x \equiv q^m x \mod n \), so we have an orbit of \( b \) cosets.

Write \( x = yz \), \( n = uz \), \((y, u) = 1 \). Then \( u \not\equiv 1 \), and \( (a^b - q^m) y \equiv 0 \mod u \).

Choose \( i \) such that \( p_i \mid u \), then \( (a^b - q^m) y \equiv 0 \mod p_i \).

Since \((y, u) = 1 \), we have \( a^b \equiv q^m \mod p_i \). Since \( a \equiv 0 \mod p_i \) and \( q^m \equiv 0 \mod p_i \), we see that \( b \) is even.

Hence there are splittings given by \( u_a \).

Let \( u_a : S_1 \rightarrow S_2 \) be such a splitting.

Then \( u_a \) interchanges \( S_1, p_i \) and \( S_2, p_i \). Let \( k = \text{ord}_{p_i}(a) \).

Then \( k \) is even, and \( a^{\frac{k}{2}} \equiv -1 \mod p_i \). Since \(-1 \equiv 0 \mod p_i \), \( k \) must be even.

Hence \( u_{-1} (S_1, p_i) = S_1, p_i \), and \( u_{-1} \) cannot give the same splitting as \( u_a \). \( \square \)
(3.2.9) **Theorem:** Let \( p \equiv 1 \mod 4 \) be a prime, such that \( q \equiv 0 \mod p \), and let \( m > 1 \).

Then either a splitting \( \mod p^m \) is given by \( \mu_{-1} \), or it is left invariant by \( \mu_{-1} \).

**Proof:** This follows from Lemma (3.2.6)(iv).

(3.2.10) **Theorem:** Let \( n = p_1^{m_1}p_2^{m_2} \cdots p_k^{m_k} \) be the prime factorization of the odd integer \( n \), such that \( q \equiv 0 \mod p_i \), \( i = 1, 2, \ldots, k \).

Suppose there is an integer \( b \), such that \( n \mid (q^b + 1) \).

Then \( p_i \equiv 1 \mod 4 \), \( i = 1, 2, \ldots, k \), and each splitting \( \mod n \) is left invariant by \( \mu_{-1} \).

**Proof:** Since \( q^b \equiv -1 \mod p_i \), we have \( -1 \equiv 0 \mod p_i \), and hence \( p_i \equiv 1 \mod 4 \).

Each cyclotomic coset \( \mod n \) is left invariant by \( \mu_{-1} \), so \( \mu_{-1} \) leaves each splitting \( \mod n \) invariant.
Chapter 4: Duadic codes of length a prime power

In this chapter we give an upper bound for the minimum distance of duadic codes of length a prime power. In a special case we can strengthen this upper bound, and also give a lower bound for the minimum distance. As a consequence, we can determine the minimum distance of duadic codes of length $p^m$ for several values of $p$.

Section 4.1: The general upper bound

Let $p$ be an odd prime, $q$ a prime power, $(p,q)=1$. Let $t:=\text{ord}_p(q)$, and let $z$ be such that $p^z \parallel (q^t-1)$. Then, by Theorem (3.2.2), $\text{ord}_p(q)=tp^{m-z}$ if $m \geq z$.

Let $m>z$.

Now suppose $i$ is an integer such that $p^z|i$, and let $C_i$ be the cyclotomic coset mod $p^m$ which contains $i$, i.e. $C_i=\{q^ji \mod p^m | j \geq 0\}$.

(4.1.1) Theorem: $C_i + p^z = C_i \mod p^m$.

Proof: Let $j \geq 0$. We shall prove that $q^ji + p^z \in C_i$.

If $k$ and $k'$ are integers such that $q^{kt} = q^{kt'} \mod p^m$, then $q^{(k-k')t} \equiv 1 \mod p^m$, so $tp^{m-z} \mid (k-k')t$. It follows that $k \equiv k' \mod p^{m-z}$.

So the integers $q^{kt-1}$, $k=0,1,2,\ldots,p^{m-z}-1$, are different mod $p^m$.

Now choose integers $a_k$, $k=0,1,2,\ldots,p^{m-z}-1$, such that $q^{kt-1} = a_k p^z$.

Then $a_k, k=0,1,2,\ldots,p^{m-z}-1$, are different mod $p^{m-z}$. Hence there is a $k$, such that $a_k = q^{j-i-1} \mod p^{m-z}$ ($q^{-j}$ and $i^{-1}$ are inverses mod $p^m$).

Then $q^{j-i-1} = a_k p^z = q^{-j-i}p^z \mod p^m$, and hence

$q^j + p^z = q^{j+kt-i} \mod p^m$. 

(4.1.2) Corollary: If $p^{m-z} \mid i$, then $C_i + p^{m-1} = C_i \mod p^m$.

Let $\alpha: S_1 \to S_2$ be a splitting mod $n$, where $n=p^m$, and let $\alpha$ be a primitive $n$-th root of unity in an extension field of $GF(q)$. Let $C$ be the duadic code of length $n$ over $GF(q)$ with defining set $\{\alpha^i | i \in S_1\}$ and with idempotent $e(x)$.
Since \(e(x^q) = (e(x))^q = e(x)\), we can write \(e(x)\) as

\[ e(x) = \sum_i e_i \sum_{j \in C_i} x^j, \]

where \(i\) runs through a set of cyclotomic coset representatives.

Now consider the codeword \(c(x) := (1-x^p^{-m-1})e(x)\).

Corollary (4.1.2) shows that

\[ c(x) = (1-x^p^{-m-1}) \sum_i e_i \sum_{j \in C_i} x^j. \]

Assume w.l.o.g. that \(1 \in S\).

Since \(c(a) = (1-a^p^{-m-1}) \neq 0\), we have \(c(x) \neq 0\).

It is obvious that \(c(x)\) has weight \(\leq p^z\). We have proved:

(4.1.3) Theorem: Let \(p\) be an odd prime, \(q\) a prime power, such that \(q \equiv 0 \mod p\). Let \(t := \text{ord}_p(q)\), and let \(z\) be such that \(p^{z} \mid (q^t - 1)\). Then all duadic codes of length \(p^m\), \(m \geq z\), have minimum distance \(\leq p^z\).

Section 4.2: The case \(z=1\)

In this section \(p\) is an odd prime, \(q\) a prime power, such that \(q \equiv 0 \mod p\). Furthermore, \(t := \text{ord}_p(q)\), and we assume that \(p^2 \mid (q^t - 1)\).

Let \(m>1\).

We denote by \(C_i^{(k)}\) the cyclotomic coset mod \(p^k\) which contains \(i\).

(4.2.1) Lemma: If \(p \mid i\), then \(C_i^{(1)} \subset C_i^{(m)}\).

Proof: Let \(j \in C_i^{(1)}\), and let \(k\) be an integer such that \(j = q^k i \mod p\).

Choose integers \(a_s, s=0,1,2,\ldots, p^{m-1}-1\), such that \(q^{st} = a_{s+1}\).

In the proof of Theorem (4.1.1) we have seen that the integers \(a_s, s=0,1,2,\ldots, p^{m-1}-1\), are different mod \(p^m\).

So there is an \(s\), such that \(a_s = q^{-k} i (j - q^k i) \mod p^{m-1}\) (\(q^{-k}\) and \(i^{-1}\) are inverses mod \(p^{m-1}\)).

Then \(q^{k+st} = q^k i (1+a_s p) = j \mod p^m\), and hence \(j \in C_i^{(m)}\). \(\square\)
Let $u:S_1 \rightarrow S_2$ be a splitting mod $n$, where $n=p^m$, and define

$$S'_k := \{i \in S_k | 1 \leq i < p\}, k=1,2.$$

(4.2.2) **Lemma:** $u:S'_1 \rightarrow S'_2$ is a splitting mod $p$.

**Proof:** Let $i \in S'_1$. From Lemma (4.2.1) it follows that $C_i^{(1)} \subseteq C_i^{(m)} \subseteq S_1$, so $q_i \mod p \in S'_1$. Since $C_{ai}^{(1)} \subseteq C_{ai}^{(m)} \subseteq S_2$, we have $ai \mod p \in S'_2$. \qed

Let $\alpha$ be a primitive $n$-th root of unity in an extension field of $GF(q)$. Then $\beta := \alpha^p$ is a primitive $p$-th root of unity. We define $C$ as the duadic code of length $n$ with defining set $\{\alpha^i | i \in S_1\}$ and minimum distance $d$,

$C'$ as the duadic code of length $p$ with defining set $\{\beta^i | i \in S'_1\}$ and minimum distance $d'$,

and $C''$ as the even-like subcode of $C'$, with minimum distance $d''$.

(4.2.3) **Theorem:** We have $d' \leq d \leq d''$.

**Proof:** Let $e(x)$ be the idempotent of $C$, $e(x) = \sum_{i} e_i \sum_{j \in C_i} x^j$, $e_i \in GF(q)$, $i$ runs through a set of cyclotomic coset representatives.

(i) Consider the codeword (of $C$)

$$c(x) := (1-x^{p^{m-1}})e(x) = (1-x^{p^{m-1}}) \sum_{i:p^{m-1}} e_i \sum_{j \in C_i} x^j \quad (cf. \ page \ 20).$$

c(x) has (possibly) non-zeros only on positions $=0 \mod p^{m-1}$.

Now define a new variable $y := x^{p^{m-1}}$, and let $c^*(y) := c(x)$, a vector in $GF(q)[y]/(y^{p-1})$.

Let $C^*$ be the cyclic code of length $p$ over $GF(q)$, generated by $c^*(y)$. If we show that $C^* = C''$, then we have proved that $d \leq d''$.

Since $c^*(\beta^i) = c^*(\alpha^{ip^{m-1}}) = c(\alpha^i) = (1-\alpha^{ip^{m-1}})e(\alpha^i) \{=0 \ if \ i \in S'_1 \cup \{0\}, \ 

\neq 0 \ if \ i \in S'_2\}$,

we have $C^* \subseteq C''$. 
Let \( g(y) \) be the generator polynomial of \( C'' \).

Since \( \gcd(c^*(y), y^{p-1}) = g(y) \), there are polynomials \( a(y) \) and \( b(y) \)
such that \( a(y)c^*(y) + b(y)(y^{p-1}) = g(y) \), so \( g(y) = a(y)c^*(y) \mod (y^{p-1}) \),
and hence \( C'' \subset C^* \).

(ii) Let \( C'_0 := \{ (c_0, c_{m-1}, \ldots, c_{(p-1)p-1}) \mid (c_0, c_1, \ldots, c_{n-1}) \in C \} \).

If we show that \( C'_0 = C' \), then we have proved that \( d' \leq d \).

We know that \( C_i + p^{m-1} = C_i \mod p^m \) if \( p^{m-1} \mid i \) (cf. Theorem (4.1.2)).

It follows that the idempotent \( e(x) \) of \( C \) looks like \( (r := p^{m-1}) \)

\[
\begin{array}{cccccccc}
\text{position:} & 0 & 1 & 2 & \ldots & (r-1) & r & (r+1) & \ldots & (2r-1) & 2r & \ldots & (p-1)r & (p-1)r+1 & \ldots & (n-1)
\end{array}
\]

\[
e(x) : \begin{cases} 
\star & \star & \star & \star & \star & \star & \star 
\end{cases}
\]

where the \( \star \)'s are elements of \( \text{GF}(q) \).

Let \( e'(x) := \sum_{i:p^{m-1}} \sum_{j \in C_i} x^j e_i, \) then \( e(a^k) = e'(a^k), \) \( k = 0, 1, 2, \ldots, n-1. \)

Again define \( y := x^{p^{m-1}}, \) \( \ast(y) := e'(x) \in \text{GF}(q)[y]/(y^{p^m}-1). \)

Since \( e'(b^{k}) = e'(a^k) = e(a^k) \mid = 0 \) if \( k \in S'_1, \)
\[
\begin{cases} 
1 \text{ if } k \in S'_2 \cup \{0\}, 
\end{cases}
\]

the polynomial \( \ast(y) \) is the idempotent of \( C' \) (cf. Theorem (1.3.3)).

Hence \( C' \subset C'_0 \).

Now consider \( x^k e(x) \) on the positions \( \equiv 0 \mod p^{m-1} \), call this vector \( c_k \)
\( (c_k \text{ has length } p) \):

a) if \( k \equiv 0 \mod p^{m-1} \), then \( c_k \in <1> \),

b) if \( k = bp^{m-1} \) for some \( 0 \leq b < p \), then \( c_k = y^k e'(y) \in C' \).

Since the code \( C'_0 \) is generated by the vectors \( c_k, k = 0, 1, 2, \ldots, n-1, \)
we have proved that \( C'_0 \subset <C', 1> = C'. \) \( \Box \)
Section 4.3: Examples

(4.3.1) Theorem: Let \( p \equiv 1 \mod 8 \) be a prime, such that \( \text{ord}_p(2) = \frac{p-1}{2} \), and suppose that \( p^2 \mid (2^{\frac{p-1}{2}} - 1) \).

Let \( d \) be the minimum distance of the binary even-weight QR code of length \( p \), and let \( m > 1 \).

Then all binary duadic codes of length \( p^m \) have minimum distance \( d \).

Proof: Since the only duadic codes of length \( p \) are QR codes, Theorem (4.2.3) shows that duadic codes of length \( p^m \) have minimum distance \( d-1 \) or \( d \) (here we use the fact that the QR code of length \( p \) has minimum distance \( d-1 \)). From Theorem (3.1.4) it follows that this minimum distance must be even.

(4.3.2) Example: All binary duadic codes of length \( 31^m \), \( m > 1 \), have minimum distance 8.

Proof: Duadic codes resp. even-weight duadic codes of length 31 have minimum distance 7 resp. 8. The assertion follows from Theorems (3.1.4) and (4.2.3).

(4.3.3) Remark: Let \( q = 2 \). In Section 4.2 we only consider primes \( p \) such that \( p^2 \mid (2^t - 1) \), where \( t = \text{ord}_p(2) \). This condition is very weak: There are just two primes \( p < 6 \cdot 10^9 \), such that \( 2^{p-1} \equiv 1 \mod p^2 \):

\[
\begin{align*}
p &= 1093, \quad t = 364, \quad 2^t \equiv 1 \mod p^2, \quad 2^t = 1064432260 \mod p^3, \\
p &= 3511, \quad t = 1755, \quad 2^t \equiv 1 \mod p^2, \quad 2^t = 21954602502 \mod p^3
\end{align*}
\]

(cf. [15]).

(4.3.4) Take \( q = 4 \). Let \( n \) be an odd integer, such that \( \text{ord}_n(2) \) is odd. Then binary and quaternary cyclotomic cosets mod \( n \) are equal, i.e.

\( \{2^i \mod n \mid j \geq 0\} = \{4^i \mod n \mid j \geq 0\} \) for each \( i \).

It follows that a duadic code \( C \) of length \( n \) over \( GF(4) \) is generated by binary vectors. Pless (cf. [14]) has shown that in this case the code \( C \) has the same minimum distance as its binary subcode, which is a duadic code over \( GF(2) \).
Example: All duadic codes of length $7^m$, $m > 1$, over GF(4) have minimum distance 4.

Proof: This follows from (4.3.1) and (4.3.4).

Example: All duadic codes of length $3^m$, $m > 1$, over GF(4) have minimum distance 3.

Proof: Let $C$ be a duadic code of length $3^m$ over GF(4). Theorem (4.2.3) shows that $C$ has minimum distance $d = 2$ or 3. By Theorem (3.1.4), minimum weight codewords are even-like. Then the BCH bound (cf. (8.1.1)) gives $d \geq 3$. 
Chapter 5: Splittings and tournaments

In this chapter we study tournaments which are obtained from splittings given by $\mu_{-1}$. First we give some theory about tournaments (cf. [16]).

Section 5.1: Introduction

A complete graph $K_n$ is a graph on $n$ vertices, such that there is an edge between any two vertices. If such a graph is directed, i.e. each edge has a direction, then it is called a tournament.

If $x$ is a vertex of a directed graph, then the in-degree, resp. out-degree, of $x$ is the number of edges coming in, resp. going out of $x$.

A tournament on $n$ vertices is called regular if there is a constant $k$, such that each vertex has in-degree and out-degree $k$. It is obvious that in that case $n=2k+1$. The tournament is called doubly-regular if the following holds. There is a constant $t$, such that for any two vertices $x$ and $y$ ($x \neq y$), there are exactly $t$ vertices $z$ such that both $x$ and $y$ dominate $z$ ($x$ dominates $z$ if there is an edge pointing from $x$ to $z$). In that case the number of vertices equals $n=4t+3$, so $n \equiv 3 \mod 4$.

Note that a doubly-regular tournament is also regular.

Let $T$ be a tournament on $n$ vertices. We assume w.l.o.g. that the vertices of $T$ are $\{0,1,2,\ldots,n-1\}$.

Now define the $n \times n$ matrix $A$ by

$$A_{ij} := \begin{cases} 1 & \text{if } i \text{ dominates } j, \\ 0 & \text{otherwise.} \end{cases} \quad (0 \leq i,j < n)$$

This matrix is called the adjacency matrix of the tournament.

From the definition of a tournament it follows that

\begin{align*}
(5.1.1) \quad A + A^T + I &= J. \\
(5.1.2) \quad \text{Lemma } : & \text{ If the tournament is regular, then} \\
& \quad (i) \quad AJ = JA = \frac{n-1}{2} J, \\
& \quad (ii) \quad A^T A = AA^T.
\end{align*}
Proof: (i) follows from the definition of a regular tournament, and (ii) follows from (5.1.1).

(5.1.3) Lemma: The following statements are equivalent:
(i) The tournament is doubly-regular,
(ii) \( AA^T = \frac{n+1}{4} I + \frac{n-3}{4} J \),
(iii) \( A^2 + A + \frac{n+1}{4} I = \frac{n+1}{4} J \).

Proof: Apply the definition, (5.1.1) and (5.1.2).

Section 5.2: Tournaments obtained from splittings

Let \( n \) be odd, \( q \) a prime power.

Let \( \mu_1 : S_1 \rightarrow S_2 \) be a splitting mod \( n \) \((S_1 \text{ and } S_2 \text{ are unions of cyclotomic cosets } \{i,q_i,q_i^2\ldots\} \text{ mod } n)\).

Now define the directed graph \( T \) on the vertices \( \{0,1,2,\ldots,n-1\} \) as follows:

\( i \) dominates \( j \) iff \( (j-i) \text{ mod } n \in S_1 \).

The adjacency matrix \( A \) of \( T \) is a circulant, and

\[
A_{ij} = \begin{cases} 
1 & \text{if } j-i \in S_1, \\
0 & \text{if } j-i \in S_2 \cup \{0\}.
\end{cases}
\]

From the definition of a splitting it follows that \( T \) is a regular tournament. If \( T \) is doubly-regular, then the splitting is called doubly-regular.

(5.2.1) Example: Let \( p \equiv 3 \mod 4 \) be a prime, and let \( q \) be a prime power such that \( q \equiv 0 \mod p \).

Let \( S_1 := \{i \leq p \mid i \equiv 0 \mod p\} \), \( S_2 := \{i \leq p \mid i \equiv \# \mod p\} \).
Then \( \mu_1 : S_1 \rightarrow S_2 \) is a splitting mod \( p \). Let \( A \) be the adjacency matrix of the corresponding tournament.

The \( n \times n \) matrix \( S \) defined by

\[
S_{ij} := \begin{cases} 
1 & \text{if } j-i \in S_1, \\
-1 & \text{if } j-i \in S_2, \\
0 & \text{if } i=j,
\end{cases}
\]
is a Paley-matrix and satisfies $SS^T = pI - J$, $S + S^T = 0$ (cf. [10]).

Since $A = \frac{1}{4}(S + J - I)$, it follows that $AA^T = \frac{p+1}{4} I + \frac{p-3}{4} J$, and hence the splitting $u_{-1}:S_1 \rightarrow S_2$ is doubly-regular.

I have not been able to find any other doubly-regular splittings.

(5.2.2) **Theorem**: A splitting $u_{-1}:S_1 \rightarrow S_2$ mod $n$ is doubly-regular iff $\mid S_1 \cap (S_1 + k) \mid = \frac{n-3}{4}$, $k=1,2,\ldots,n-1$.

**Proof**: This follows from Lemma (5.1.3)(ii).

We shall use this theorem to give a nonexistence theorem.

(5.2.3) **Theorem**: Let $p$ be an odd prime, $q$ a prime power such that $q \equiv 0 \mod p$, $z$ an integer such that $p^2 \| (q^{t-1})$, where $t=\text{ord}_p(q)$.

Let $m > z$. Then there is no doubly-regular splitting mod $p^m$.

**Proof**: Let $u_{-1}:S_1 \rightarrow S_2$ be a splitting mod $p^m$, and define

$T_1 := \{ i \in S_1 | i \equiv 0 \mod p^{m-z} \}$, $S_1' := S_1 \setminus T_1$.

From Corollary (4.1.2) it follows that $S_1' + p^{m-1} = S_1' \mod p^m$.

Therefore $\mid S_1 \cap (S_1 + p^{m-1}) \mid \geq \mid S_1' \mid = \mid S_1 \mid - \mid T_1 \mid = \frac{p^{m-1} - p^{z-1}}{2} > \frac{p^{m-3}}{4}$. Now apply Theorem (5.2.2).
Chapter 6: Duadic codes and cyclic projective planes

In this chapter we study duadic codes for which equality holds in Theorem (3.1.4)(ii). Such codes "contain" projective planes. We shall explain what we mean by this.

If \( c \) is a vector, then the set \( \{ i | c_i \neq 0 \} \) is called the support of \( c \).

Now if a code contains codewords such that their supports are the lines of a projective plane \( \Pi \), then we say that the code contains \( \Pi \).

Furthermore, we give an existence test for cyclic projective planes. For the theory of projective planes, the reader is referred to [3].

Section 6.1: Duadic codes which contain projective planes

Let \( C \) be a duadic code of length \( n \) over GF(q), and suppose the splitting is given by \( p \).

Let \( c(x) = \sum_{i=1}^{d} c_i x^i \) be an odd-like codeword of weight \( d \).

We know that \( d^2 - d + 1 \geq n \).

6.1.1 Theorem: If \( d^2 - d + 1 = n \), then the following holds:

(i) The code \( C \) contains a projective plane of order \( d-1 \),

(ii) \( C \) has minimum distance \( d \),

(iii) \( c_i = c_j \) for all \( 1 \leq i, j \leq d \).

Proof: (i) From Theorem (3.1.1)(ii) it follows that there is an \( A \) in GF(q), \( A \neq 0 \), such that \( c(x)c(x^{-1}) = A.j(x) \), so

\[
\sum_{i \neq j} c_i c_j x^{e_i - e_j} = A(x + x^2 + \ldots + x^{n-1})
\]

Since \( d(d-1) = n-1 \), all exponents \( 1, 2, \ldots, n-1 \), appear exactly once as a difference \( e_i - e_j \).

So the set \( D := \{ e_1, e_2, \ldots, e_d \} \) is a difference set in \( Z \) mod \( n \).

Now call the elements of \( Z \) mod \( n \) points, and call the sets \( D + k \), \( k = 0, 1, 2, \ldots, n-1 \), lines. Then we have a projective plane of order \( d-1 \).

(ii) Consider the \( d \times n \) matrix \( M \), with rows \( c_i x^{-e_i} c(x) \), \( i = 1, 2, \ldots, d \).

The 0-th column of \( M \) contains nonzero elements.
Since $d^2 = d + n - 1$ and $c(x)c(x^{-1}) = A_j(x)$, every other column of $M$ contains exactly one nonzero element.

Let $C'$ be the even-like subcode of $C$.

We know that $C^\perp = C'$ (cf. Theorem (3.1.2)).

Let $c'(x)$ be a codeword of $C'$, and assume w.l.o.g. that $c'(x)$ has a nonzero on position 0. Since every row of $M$ has inner-product 0 with $c'(x)$, we see that $c'(x)$ has weight $\geq d + 1$.

(iii) Consider again the matrix $M$. Let $1 \leq i < j < k \leq d$ (remark that $d \geq 3$).

Every column of $M$ (except the 0-th) contains exactly one nonzero element, and all these elements are of the form $c c_j$. Since the sum of the rows of $M$ equals $A_j(x)$, we have $c_i c_j = c_i c_k = c_j c_k = A$, so $c_i = c_j = c_k$.

In [13], Pless showed that there is a binary duadic code which contains a projective plane of order $2^s$ if and only if $s$ is odd.

Furthermore, she showed in [14], that if $s$ is either odd or $s = 2 \mod 4$, then there is a duadic code over GF(4) which contains a projective plane of order $2^s$.

Section 6.2: An existence test for cyclic projective planes

Consider a cyclic projective plane of order $n$.

The incidence matrix of this plane is the $(n^2 + n + 1) \times (n^2 + n + 1)$ matrix $A$, which has as its rows the characteristic vectors of the lines of the plane.

Let $p$ be a prime such that $p \mid n$, and let $t \geq 1$, $q := p^t$, $N := n^2 + n + 1$.

Let $C$ be the cyclic code of length $N$ over GF(q) generated by the matrix $A$.

Bridges, Hall and Hayden [2] have shown that $\dim C = \frac{N + 1}{2}$ and $C^\perp \subset C$.

(6.2.1) Theorem: $C$ is a duadic code of length $N$ over GF(q) with minimum distance $n + 1$, and the splitting is given by $\mu_{-1}$.

Proof: Let $\alpha$ be a primitive $N$-th root of unity in an extension field of GF(q), and let $\{\alpha^i | i \in S_1\}$ be the complete defining set of $C$. The rows of the matrix $A$ are odd-like, so $0 \notin S_1$.

The code $C^\perp$ has complete defining set $\{\alpha^{-1} | i \in S_2 \cup \{0\}\}$, where

$S_2 := \{1, 2, \ldots, N - 1\} \setminus S_1$. Since $C^\perp \subset C$, we have $S_1 \subset S_2 \cup \{0\}$, and hence $-S_1 = S_2$ (note that $|S_1| = |S_2|$).

So we have a splitting $\mu_{-1} : S_1 \mapsto S_2 \mod n$, which shows that $C$ is a
duadic code.
Then Theorem (6.1.1) shows that $C$ has minimum distance $n+1$.  

(6.2.2) **Remark**:
If the extended code $\overline{C}$ is self-dual, then $p=2$.

**Proof**:
Let $c$ be a row of the matrix $A$ (so $c$ is a codeword in $C$).
Since $\Sigma c_i = n+1 \equiv 1 \mod p$, we have $(c,-1) \in \overline{C}$.
Now $(c,-1)$ has inner-product 0 with itself, so $n+1+1=2=0 \mod p$.
Hence $p=2$.  

(6.2.3) **Theorem**:
Suppose a cyclic projective plane of order $n$ exists.
Let $p$ and $r$ be primes, such that $p|n$, $r|(n^2+n+1)$.
Then $p\equiv 0 \mod r$.

**Proof**:
By Theorem (6.2.1) there is a duadic code of length $n^2+n+1$
over $\text{GF}(p)$, and then Theorem (2.1.7) shows that $p\equiv 0 \mod r$.  

(6.2.4) **Remarks**:
(i) Theorem (6.2.3) is a weaker version of a theorem in [1], which says:
Suppose a cyclic projective plane of order $n$ exists. Let $p$ and $r$ be
primes, such that $p|n$, $r|(n^2+n+1)$, $p\not\equiv 0 \mod r$. Then $n$ is a square.

(ii) Wilbrink [18] has shown:
If a cyclic projective plane of order $n$ exists, then
a) if 2$|n$, then $n=2$,
b) if 3$|n$, then $n=3$.

(iii) In [5], Jungnickel and Vedder have shown:
If a cyclic projective plane of even order $n>4$ exists, then $n\equiv 0 \mod 8$.

We shall give some examples, which cannot be ruled out with Theorem (6.2.3).

(6.2.5) **Examples**:
(i) Suppose a cyclic projective plane of order 12
exists. Then according to Theorem (6.2.1) there is a splitting
$\mu_{-1}:S_1 \leftrightarrow S_2 \mod 157$, where $S_1$ and $S_2$ are unions of cyclotomic cosets
$\{1,3i,3^2i,\ldots\} \mod 157$. But $3^{39} \equiv -1 \mod 157$, so all cyclotomic cosets
mod 157 are left invariant by $\mu_{-1}$. Hence a splitting mod 157 cannot
be given by $\mu_{-1}$, and the projective plane does not exist.
(ii) Suppose a cyclic projective plane of order 18 exists. By Theorem (6.2.1) there is a binary duadic code of length \(18^2+18+1=7^3\) with minimum distance 19. But in Theorem (4.3.1) we have seen that binary duadic codes of length \(7^3\) have minimum distance 4. So we have a contradiction.
Chapter 7: Single error-correcting duadic codes

In this chapter we study binary duadic codes with minimum distance 4, and duadic codes over GF(4) with minimum distance 3.

Section 7.1: Binary single error-correcting duadic codes

Let $C$ be a binary duadic code of length $n>7$ (so $n\geq 17$, cf. Example (2.1.11)). By Theorem (3.1.4) the odd weight vectors in $C$ have weight at least 5.

Let $a$ be a primitive $n$-th root of unity, and suppose w.l.o.g. that $a$ is in the complete defining set of $C$. Then the nonzero even-weight vectors in $C$ have $a^0, a^1, a^2$ as zeros, so their weights are at least 4 by the BCH bound (cf. (8.1.1)). We conclude that the code $C$ has minimum distance at least 4.

(7.1.1) Theorem: Let $C$ be a binary duadic code of length $n$ and minimum distance 4.
Then $n \equiv 0 \mod 7$.

Proof: Let $c(x)=1+x^i+x^j+x^k$ be a codeword in $C$ of weight 4, and let $a$ be a primitive $n$-th root of unity such that $c(a)=0$.

If $i+j\equiv k \mod n$, then $c(a)=(1+a^i)(1+a^j)=0$, so $a^i=1$ or $a^j=1$, which is impossible. Hence

\[ i+j \neq k, \quad j+k \neq i, \quad k+i \neq j \mod n. \quad (*) \]

Suppose the splitting is given by $\mu_a$. Then $c(x^{-a})=1+x^{-ai}+x^{-aj}+x^{-ak}$ is a codeword in $C^d$.

It follows that $c(x)$ and $c(x^{-a})$ have inner-product 0, so $\{i,j,k\} \cap \{-ai,-aj,-ak\} \neq \emptyset$.

The rest of the proof consists of considering all possibilities. We shall only give some examples, showing how these possibilities lead to the theorem.

Suppose $ai \equiv -i \mod n$.

The vectors $c(x)=1+x^i+x^j+x^k$ and $x c(x^{-a})=x^i+x^{-2i}+x^{-i-aj}+x^{-i-ak}$ have inner-product 0, so $\{0,j,k\} \cap \{2i,-aj,-ak\} \neq \emptyset$. 
Now suppose e.g. that \( i = aj \mod n \), then \( i = -j \mod n \).

Since \( c(x) \) and \( c(x^{-a}) \) have inner-product 0, we have \( ak \equiv -i \mod n \).

Also \( c(x) \) and \( x^2c(x^{-a}) \) have inner-product 0, so
\[
\{ 0, -i, k \} \cap \{ 2i, 3i, k+2i \} \neq \emptyset.
\]

Note that \( 2i \not\equiv 0, 3i \not\equiv 0 \mod n \).

Because of (*) there are two possibilities:

(i) \(-i \equiv k+2i \mod n\): Then \( c(x)=1+x^i+x^{i-3} \) and \( x^3c(x^{-a})=x^3+x^{i+4}x^{i+2} \)
have inner-product 0, so \( \{ i, -i, -3i \} \cap \{ 2i, 3i, 4i \} \neq \emptyset \).

Since \((2,n) = (3,n) = (5,n) = 1\), it follows that \( 7i \equiv 0 \mod n \), so \( n \equiv 0 \mod 7 \).

(ii) \( k \equiv 3i \mod n\): In the same way, \( c(x) \) and \( x^3c(x^{-a}) \) have inner-product 0,
so \( \{ 0, i, -i \} \cap \{ 2i, 4i, 6i \} \neq \emptyset \). Hence \( 7i \equiv 0 \mod n \), \( n \equiv 0 \mod 7 \).

(7.1.2) Remark: We saw in Example (2.3.4) that a binary duadic code of length \( n > 7 \) and minimum distance 4 exists, if \( n \equiv 0 \mod 7 \).

We shall now give complete proofs of some special cases of Theorem (7.1.1).

(7.1.3) Lemma: Binary duadic codes of length \( n = 2^m - 1 \) exist iff \( m \) is odd.

Proof: We apply Theorem (2.1.7).

(i) Let \( m \) be odd, \( p \) a prime, \( p \mid n \). Then \( 2^{m-1} \cdot 2 = 1 \mod p \), so \( 2 \equiv 0 \mod p \).

(ii) If \( m \) is even, then \( 3 \mid n \), but \( 2 \equiv 0 \mod 3 \).

(7.1.4) Theorem: Let \( C \) be a binary duadic code of length \( n = 2^m - 1 \) (\( m \) odd) and minimum distance 4, and suppose the splitting is given by \( \mu_j \).

Then \( n \equiv 0 \mod 7 \).

Proof: Let \( c(x) = 1 + x^i + x^j + x^k \) be a codeword of weight 4, and let \( \alpha \) be a primitive element of \( GF(2^m) \) such that \( c(\alpha) = 0 \).

Choose an integer \( b \) such that \( \alpha^b(1 + \alpha^{-i}) = 1 \), and define
\[ \xi = \alpha^b, \eta = \alpha^{b+i}. \]

Then \( \alpha^{b+i} = \xi + 1 \) and \( \alpha^{b+k} = \eta + 1 \).

The codeword \( x^b c(x) \) has \( \alpha^2 \) as a zero, so \( \xi^9 + (\xi+1)^9 + \eta^9 + (\eta+1)^9 = 0 \).

It follows that \( (\xi + \eta)^8 = \xi + \eta \). Since \( \xi + \eta \not\equiv 0 \), we find \( (\xi + \eta)^7 = 1 \).

(7.1.5) Theorem: Let \( C \) be a binary duadic code of length \( n \) and minimum distance 4. Suppose the splitting is given by \( \mu_{-1} \).

Then \( n \equiv 0 \mod 7 \).
Proof: Let \( c(x) = 1 + x^i + x^j + x^k \) be a codeword of weight 4. In the proof of Theorem (7.1.1) we have seen that

\[
i + j \not\equiv k, \ j + k \not\equiv i, \ k + i \not\equiv j \mod n. \quad (*)
\]

By Theorem (3.1.4), all even weights in \( C \) are divisible by 4. Hence \((1+x^i)c(x) = 1 + x^i + x^k + x^{2i} + x^{i+j} + x^{i+k}\) is a codeword of weight 4.

So \(|\{0, j, k, 2i, i+j, i+k\}| = 4\). Because of (*) there are 4 possibilities:

(i) \( j = 2i \mod n \): \((1+x^{2i})c(x) = 1 + x^i + x^k + x^{3i} + x^{4i} + x^{k+2i}\) is a codeword of weight 4, so \(|\{0, i, k, 3i, 4i, k+2i\}| = 4\).

Again because of (*), we have two possibilities:

a) \( k = 4i \mod n \): \((1+x^{3i})c(x) = 1 + x^{i} + x^{2i} + x^{3i} + x^{5i} + x^{7i}\) has weight 4, so \(7i \equiv 0 \mod n\).

b) \( k + 2i = 0 \mod n \): \((1+x^{3i})c(x) = 1 + x^{2i} + x^{3i} + x^{4i} + x^{5i} + x^{6i} - 2i\) has weight 4, so \(7i \equiv 0 \mod n\).

(ii) \( i + j = 0 \mod n \): In the same way we find \( k = 3i \) or \( k = -3i \mod n\), and in both cases we get \(7i \equiv 0 \mod n\).

The cases (iii) \( k = 2i \mod n \), and (iv) \( i + k = 0 \mod n \), are similar.

(7.1.6) Remark: From the above proof it follows that the codeword \( c(x) \) is one of the following:

\[
1 + x^i + x^j + x^k, \ 1 + x^i + x^2i + x^{3i} + x^{4i} + x^{7i}, \ 1 + x^i + x^3i + x^4i + x^5i + x^6i - 2i, \ 1 + x^i + x^4i + x^7i, \ \text{where} \ 7i \equiv 0 \mod n.
\]

(7.1.7) Theorem: Let \( C \) be a binary duadic code of length \( n \) and minimum distance 4, and suppose the splitting is given by \( u^{-1}\). Then \( C \) contains exactly \( n \) codewords of weight 4.

Proof: Let \( c(x) \) be a codeword of weight 4, w.l.o.g.

\[
c(x) = 1 + x^i + x^{2i} + x^{4i}, \ \text{where} \ 7i \equiv 0 \mod n.
\]

It is obvious that all shifts of \( c(x) \) are different. Hence \( C \) contains at least \( n \) codewords of weight 4.

Let \( d(x) \) be a codeword of weight 4, such that the coefficient of \( x^0 \) is 1. We shall prove that \( d(x) \) is a shift of \( c(x) \).

By (7.1.6) there are four possibilities for \( d(x) \):

(i) \( d(x) = 1 + x^i + x^{2i} + x^{4i}, \ 7i \equiv 0 \mod n\):

\[
c(x) + d(x) = x^i + x^j + x^{2i} + x^{3i} + x^{4i} + x^{5i} + x^{6i} + x^{7i} \]

is a codeword of weight 0 or 4, so \( \{i, 2i, 4i\} \cap \{j, 2j, 4j\} \neq \emptyset \). In each case we find \( c(x) = d(x) \).
(ii) \( d(x) = 1 + x^1 + x^{2j} + x^{-2j}, \quad 7j \equiv 0 \mod n \): 

Now we find \( \{i, 2i, 4i\} \cap \{j, 2j, -2j\} \neq \emptyset \). 

If \( i = j \), then \( c(x) + d(x) = x^{4i} + x^{-2i} \) has weight 0, so \( 6i \equiv 0 \mod n \). 

A contradiction.

If \( i = 2j \), then \( c(x) + d(x) = x^{4j} + x^{-2j} \), so \( 6j \equiv 0 \mod n \). A contradiction.

If \( i = -2j \), then \( x^{2j} c(x) = d(x) \).

If \( 2i = j \), then \( c(x) + d(x) = x^i + x^{-4i} \), so \( 5i \equiv 0 \mod n \). A contradiction.

If \( 2i = 2j \), then \( i \equiv j \mod n \), a contradiction.

If \( 2i = -2j \), then \( x^{2i} d(x) = c(x) \).

If \( 4i = j \), then \( c(x) + d(x) = x^{2i} + x^{-3i} \), so \( 3i \equiv 0 \mod n \). A contradiction.

If \( 4i = 2j \), then \( ?i = j \), a contradiction.

If \( 4i = -2j \), then \( x^{4i} d(x) = c(x) \).

(iii) \( d(x) = 1 + x^1 + x^{-1} + x^{3j}, \quad 7j \equiv 0 \mod n \): 

Consider \( x^j d(x) = 1 + x^j + x^{2j} + x^{4j} \), i.e. case (i).

(iv) \( d(x) = 1 + x^1 + x^{-1} + x^{-3j}, \quad 7j \equiv 0 \mod n \): 

Consider \( x^j d(x) \), i.e. case (ii).

Section 7.2 : An error-correction procedure

In this section we give an error-correction procedure for binary duadic codes with minimum distance 4 and splitting given by \( u_1 \).

It turns out that most patterns of two errors can be corrected.

Let \( u_1 : S_1 \rightarrow S_2 \) be a splitting mod n, with corresponding binary duadic codes \( C_1 \) and \( C_2 \) of length n. Suppose the codes \( C_1 \) and \( C_2 \) have minimum distance 4.

Let \( c_2(x) = 1 + x^1 + x^{2i} + x^{4i} \) (\( 7i \equiv 0 \mod n \)) be a codeword in \( C_2 \) of weight 4 (cf. (7.1.6)).

(7.2.1) **Lemma** : Let \( c(x) \) be a polynomial of weight 4.

Then \( c(x) \in C_1 \) iff \( c(x)c_2(x) \equiv 0 \mod (x^n - 1) \).

**Proof** : (i) Let \( c(x) \in C_1 \). Then \( c(x)c_2(x) \in C_1 \cap C_2 = \{0, 1\} \).

Since \( c(x)c_2(x) \) has even weight, we have \( c(x)c_2(x) = 0 \).
(ii) Let \( c(x) = x^j + x^k + x^l + x^m \), such that \( c(x)c_2(x) = 0 \).

We may assume w.l.o.g. that \( j = 0 \).

Each exponent of \( c(x)c_2(x) \) must occur an even number of times, e.g. the exponent 0.

Because of symmetry, there are three possibilities:

a) \( k + i = 0 \) mod \( n \): It turns out that \( c(x) = 1 + x^{6i} + x^{4i} + x^i \) \( \in \mathbb{C}_1 \),
   or \( c(x) = 1 + x^{5i} + x^{3i} + x^i = c_2(x^{-1}) \) \( \in \mathbb{C}_1 \).

b) \( k + 2i = 0 \) mod \( n \): In the same way we find
   \( c(x) = 1 + x^{5i} + x^{2i} + x^{4i} \) \( \in \mathbb{C}_1 \),
   or \( c(x) = 1 + x^{5i} + x^{3i} + x^{2i} = c_2(x^{-1}) \) \( \in \mathbb{C}_1 \).

c) \( k + 4i = 0 \) mod \( n \): Here we get \( c(x) = 1 + x^{3i} + x^{6i} + x^{5i} = c_2(x^{-1}) \) \( \in \mathbb{C}_1 \), or
   \( c(x) = 1 + x^{3i} + x^{4i} + x^{2i} = x^{4i} c_2(x^{-1}) \) \( \in \mathbb{C}_1 \).

\[ \Box \]

(7.2.2) **Theorem**: Let \( e(x) = x^j + x^k \) be a polynomial of weight 2.

Suppose that for all \( h = 0, 1, ..., n-1 \), we have
\[ \{j, k\} \notin \{h, h+3i, h+5i, h+6i\} \mod n. \]

Then the polynomial \( e(x)c_2(x) \mod (x^n-1) \) uniquely determines the exponents \( j \) and \( k \).

Proof: Suppose \( (x^j + x^k)c_2(x) = (x^l + x^m)c_2(x), \ 1 \neq m. \)

(i) If \( \{j, k, l, m\} < 4 \), then \( \{j, k\} = \{l, m\}. \)

(ii) Suppose \( \{j, k, l, m\} = 4 \). Then by Lemma (7.2.1) we have
\[ x^j + x^k + x^l + x^m \in \mathbb{C}_1. \]
Since the only codewords of weight 4 in \( \mathbb{C}_1 \) are the shifts of \( c_2(x^{-1}) \), there is an integer \( h \), such that
\[ \{j, k\} \subset \{h, h+3i, h+5i, h+6i\}, \] a contradiction. \[ \Box \]

Now error-correction goes as follows.

Let \( c_1(x) \in \mathbb{C}_1 \) be sent over a noisy channel, and suppose we receive \( r(x) \).
Let \( e(x) = r(x) - c_1(x) \) be the error-vector.

Since \( c_1(x)c_2(x) \) has even weight and \( C_1 \cap C_2 = \{0, 1\} \), we have \( c_1(x) c_2(x) = 0 \).

Compute \( r(x)c_2(x) = e(x)c_2(x) \).

(i) If \( r(x)c_2(x) \) is a shift of \( c_2(x) \), then we assume that one error has been made. Since all shifts of \( c_2(x) \) are different, we can determine \( e(x) \), and hence \( c_1(x) \).

(ii) If \( r(x)c_2(x) \) is not a shift of \( c_2(x) \), then more than one error has been made.

Suppose \( e(x) \) satisfies the conditions of Theorem (7.2.2).

Then we can find \( e(x) \), and hence \( c_1(x) \).
There are $\binom{n}{2}$ ways of making two errors. From the condition of Theorem (7.2.2), we see that at most $\binom{n}{2} - 6n$ patterns of two errors cannot be corrected. Hence with the above procedure we can correct at least $\binom{n}{2} - 6n$ patterns of two errors.

Section 7.3: Duadic codes over GF(4) with minimum distance 3

Let $C$ be a duadic code of length $n > 3$ over GF(4).

In the same way as at the beginning of Section 7.1 we find that $C$ has minimum distance at least 3.

(7.3.1) Theorem: Let $C$ be a duadic code of length $n > 3$ over GF(4) with minimum distance 3.

Then $n = 5$ or $n = 7$ or $n \equiv 0 \pmod{3}$.

Proof: Suppose $n \geq 11$. Let $GF(4) = \{0, 1, \omega, \omega^2\}$, $\omega^2 + \omega = 1$.
Let $c(x) = 1 + c_i x^i + c_j x^j$ be a codeword of weight 3.

By Theorem (3.1.4), $c(x)$ is even-like, so $c_i + c_j = 1$. It follows that $\{c_i, c_j\} = \{\omega, \omega^2\}$. Take w.l.o.g. $c_i = \omega$, $c_j = \omega^2$.

Suppose the splitting is given by $\mu_a$. Then $c(x-a)$ is a codeword in $C^*$. So $c(x)$ and $c(x-a)$ have inner-product 0.

Therefore $\{i, j\} \cap \{-a_i, -a_j\} \neq \emptyset$. We consider all possibilities.

(i) $a_i = -i \pmod{n}$: Since $c(x)$ and $c(x-a)$ have inner-product 0, we have $a_j = -j \pmod{n}$.
Also $c(x)$ and $x^i c(x-a)$ have inner-product 0, so $\{0, j\} \cap \{2i, i+j\} \neq \emptyset$.

There are two possible cases:

a) $2i \equiv j \pmod{n}$: $c(x)$ and $x^i c(x-a)$ have inner-product 0, so $3i \equiv 0 \pmod{n}$, and hence $n \equiv 0 \pmod{3}$.

b) $i + j \equiv 0 \pmod{n}$: In the same way we find $3i \equiv 0 \pmod{n}$.

(ii) $a_j = -j \pmod{n}$: In the same way we find $n \equiv 0 \pmod{3}$.

(iii) $a_i = -j \pmod{n}$: Since $c(x)$ and $x^{a_i} c(x-a)$ have inner-product 0, we have $\{i, -a_i\} \cap \{ai, ai + a_i^2\} \neq \emptyset$.

a) $ai + a_i^2 \equiv i \pmod{n}$: $x^{ai} c(x)$ and $c(x-a)$ have inner-product 0, so $\{ai, i+ai\} \cap \{-ai, i+ai\} \neq \emptyset$.

1) $i \equiv 2ai \pmod{n}$: $ai + a_i^2 \equiv 3a_i^2$ so $a_i \equiv 0 \pmod{n}$, a contradiction.

2) $i \equiv -2ai \pmod{n}$: Let $\alpha$ be a primitive $n$-th root of unity such
that $c(\alpha^3) = 0$, so $1 + \omega^a a_1 + \omega^2 a_j = 0$.

Take the square: $1 + \omega^a a_1 + \omega^2 a_j = 0$ (2aj=ai mod n).

Add these two relations: $a_j = 2a_i$, so $j = 2i$ mod n.

Now $c(x) = 1 + \omega^a x^i + \omega^2 x^2i$ and $c(x^{-a}) = 1 + \omega^a x^2i + \omega^2 x^3i$ have inner-product $1 + \omega^3 + \omega^3 = 1 \neq 0$. Contradiction.

b) $a_i = -2i$ mod n: $c(\alpha^a) = 1 + \omega^a a_i + \omega^2 a_i = 0$, and

$(c(\alpha^a))^2 = 1 + \omega^a 2a_i + \omega^2 4a_i = 0$.

If we add these equations, then we find $3i = 0$ mod n.

But $c(x) = 1 + \omega^i x^i + \omega^2 x^2i$ and $c(x^{-a}) = 1 + \omega^2 x^2i + \omega^2 x^3i$ have inner-product $\neq 0$.

Contradiction.

(iv) $a_j = -i$ mod n: This gives in the same way a contradiction.

(7.3.2) Remark: We have proved in Example (2.3.4) that a duadic code of length $n > 3$ over GF(4) with minimum distance 3 exists if $n \equiv 0 \mod 3$. 
Chapter 8: Binary duadic codes of length ≤241

In this chapter we give some bounds on the minimum distance of cyclic codes. These bounds will be used to analyze binary duadic codes of length ≤241.

Section 8.1: Bounds on the minimum distance of cyclic codes

Let \( \alpha \) be a primitive \( n \)-th root of unity in an extension field of \( \text{GF}(q) \).

The set \( A = \{ \alpha^1, \alpha^2, \ldots, \alpha^m \} \) is called a consecutive set of length \( m \), if there is a primitive \( n \)-th root of unity \( \beta \), and an exponent \( i \), such that \( A = \{ \beta^i, \beta^{i+1}, \ldots, \beta^{i+m-1} \} \).

The proofs of the next two theorems can be found in [10].

(8.1.1) Theorem (BCH bound): Let \( A \) be a defining set for a cyclic code with minimum distance \( d \). If \( A \) contains a consecutive set of length \( \delta-1 \), then \( d \geq \delta \).

(8.1.2) Theorem (HT bound, Hartmann and Tzeng): Let \( A \) be a defining set for a cyclic code with minimum distance \( d \). Let \( \beta \) be a primitive \( n \)-th root of unity, and suppose that \( A \) contains the consecutive sets \( \{ \beta^{i+ja}, \beta^{i+j+ja}, \ldots, \beta^{i+\delta-2+ja} \} \), \( 0 \leq j \leq s \), where \( (a,n) \neq \delta \).

Then \( d \geq \delta + s \).

(8.1.3) Examples: (i) \( q=2, n=73 \). Let \( \alpha \) be a primitive \( n \)-th root of unity, and let \( C \) be the duadic code of length \( n \) with defining set \( \{ \alpha^3, \alpha^9, \alpha^{11}, \alpha^{17} \} \). The complete defining set of \( C \), i.e., \( \{ \alpha^i \mid i \in C \cup \mathbb{C}_{11} \cup \mathbb{C}_{17} \} \), contains \( \{ \beta^i \mid i \leq 8 \} \), where \( \beta := \alpha^3 \).

So by the BCH bound, the code \( C \) has minimum distance \( \geq 9 \).

(ii) \( q=2, n=127 \). Let \( C \) be the duadic code of length \( n \) and defining set \( \{ \alpha^i \mid i=1,3,5,15,19,21,23,29,55 \} \) (again \( \alpha \) is a primitive \( n \)-th root of unity). The complete defining set of the even-weight subcode contains \( \{ \alpha^i \mid i=3,12,21,30,39,48,57,66,75,84,93 \} \) U \( \{ \alpha^i \mid i=37,46,55,64,73,82,91,100,109,118,0 \} \).

Then the HT bound shows that the even-weight subcode of \( C \) has minimum distance \( \geq 13 \), hence \( \geq 14 \). Since the splitting is given by \( u_{-1} \), Theorem (3.1.4) shows that \( C \) has minimum distance \( \geq 15 \).
The next bound is due to van Lint and Wilson [11]. First we need a definition.

(8.1.4) **Definition**: Let $S$ be a subset of the field $F$. We define recursively a family of subsets of $F$, which are called independent with respect to $S$, as follows:

(i) $\emptyset$ is independent w.r.t. $S$,

(ii) if $A$ is independent w.r.t. $S$, $A \subset S$, $b \notin S$, then $A \cup \{b\}$ is independent w.r.t. $S$,

(iii) if $A$ is independent w.r.t. $S$, $c \in F$, $c \neq 0$, then $cA$ is independent w.r.t. $S$.

(8.1.5) **Theorem**: Let $c(x)$ be a polynomial with coefficients in $F$, and let $S := \{a \in F | c(a) = 0\}$. Then for every $A \subset F$ which is independent w.r.t. $S$, we have $\text{wt}(c(x)) \geq |A|$.

(8.1.6) **Example**: $q=2$, $n=73$. Let $\alpha$ be a primitive $n$-th root of unity, and let $C$ be the duadic code of length $n$ with defining set $\{\alpha^i | i=1,13,17,25\}$ and minimum distance $d$. The complete defining set of $C$ contains $\{\alpha^i | 49 \leq i \leq 55\}$, hence $d \geq 8$ by the BCH bound.

Now suppose $c(x)$ is a codeword of weight 8.

If $c(\alpha^3) = 0$, then $c(\alpha^i) = 0$, $48 \leq i \leq 55$, so $\text{wt}(c(x)) \geq 9$, a contradiction.

If $c(\alpha^9) = 0$, then $c(\alpha^i) = 0$, $i=61,62,\ldots,72,0,1,2$, also a contradiction.

So if $S := \{a | c(a) = 0\}$, then $\{\alpha^i | i \in C \setminus U S\} \cap S = \emptyset$.

The following sets are independent w.r.t. $S$:

- $\emptyset$, $\{\alpha^{65}\}$, $\{\alpha^{64}\}$, $\{\alpha^{64},\alpha^{65}\}$, $\{\alpha^{61},\alpha^{62}\}$, $\{\alpha^{61},\alpha^{62},\alpha^{65}\}$, $\{\alpha,\mathbf{1},\alpha,\mathbf{2}\}$,
- $\{\alpha,\alpha^{2},\alpha^{3},\alpha^{5},\alpha^{6},\alpha^{7}\}$, $\{\alpha,\alpha^{2},\alpha^{3},\alpha^{5},\alpha^{6},\alpha^{7}\}$, $\{\alpha,\alpha^{2},\alpha^{3},\alpha^{5},\alpha^{6},\alpha^{7}\}$, $\{\alpha,\alpha^{2},\alpha^{3},\alpha^{5},\alpha^{6},\alpha^{7}\}$, $\{\alpha,\alpha^{2},\alpha^{3},\alpha^{5},\alpha^{6},\alpha^{7}\}$, $\{\alpha,\alpha^{2},\alpha^{3},\alpha^{5},\alpha^{6},\alpha^{7}\}$.

Then Theorem (8.1.5) shows that $\text{wt}(c(x)) \geq 9$, a contradiction.

We have proved that $d \geq 9$.

(8.1.7) **Remark**: In [4], Hogendoorn gives a program that searches for sequences of independent sets. In the next section, this program will be used several times.
Section 8.2: Analysis of binary duadic codes of length ≤ 241

In [7] there is a list of all binary duadic codes of length ≤ 241, defined in terms of idempotents (cf. Definition (2.1.4)). For each code, the minimum distance, or an upper bound for it, is given.

Since we want to apply the theorems of Section 8.1 to get lower bounds for the minimum distance, the zeros of the idempotents were determined by computer.

The lower bounds were found either by hand, or using a program of Hogendoorn [4], cf. (8.1.7).

In the rest of this section we shall give the details.

In each case, n is the code-length, \( a \) is a primitive n-th root of unity, \( A \) is a defining set for the binary duadic code \( C, \mu_a \) gives the splitting, \( d \) is the minimum distance of \( C \), and \( d_0 \) is the minimum odd weight of \( C \).

(8.2.1) \( n=89, A=\{a^i \mid i=1,9,13,33\}, u_1 \).

Since the complete defining set contains \( \{a^i \mid i=15,30,45,60,75,1,16,31\} \), we have \( d\geq 9 \). Then Theorem (3.1.4) gives \( d\geq 12 \).

(8.2.2) \( n=89, A=\{a^i \mid i=3,9,11,19\}, u_1 \).

The code has zeros \( a^i, i=19,38,57,76,6,25,44,63 \), so \( d\geq 9 \).

Again Theorem (3.1.4) gives \( d\geq 12 \).

(8.2.3) \( n=119, A=\{a^i \mid i=3,7,13,51\}, u_3 \).

The complete defining set contains \( \{a^i \mid 101 \leq i \leq 105\} \), so \( d\geq 6 \).

Let \( c(x) \) be a codeword of weight 6 with zero-set \( S \).

Then \( c(a)\neq 0 \), since otherwise \( c(a^i)\neq 0, i=117,118,0,1,2,\ldots,10 \).

Also \( c(a^{11})\neq 0 \) since otherwise \( c(a^i)\neq 0, i=107,108,\ldots,117,118,0 \).

The following sets are independent w.r.t. \( S \) (we only give the exponents of \( a \)): \( \emptyset, \{4\}, \{4,5\}, \{4,5,6\}, \{95,101,102,103\}, \{96,100,102,103,104\}, \{104,108,109,110,111,112\}, \{97,101,102,103,104,105\} \).

So \( \text{wt}(c(x))\geq 7 \), a contradiction. Hence \( d\geq 7 \). Then Theorem (3.1.4) gives \( d\geq 8 \).
Notation: We introduce a notation to abbreviate a sequence of independent sets.
The string \((a_0, s_0, s_1, a_1, s_2, \ldots)\) has to be interpreted as the following sequence of sets:
\[
\emptyset, \{a_0\}, \{a_0 + s_0\}, \{a_0 + s_0 + a_1\}, \{a_0 + s_0 + a_1 + s_1\}, \\
\{a_0 + s_0 + s_1 + a_1 + s_1 + a_2\}, \{a_0 + s_0 + s_1 + s_2 + a_1 + s_1 + a_2\}, \ldots
\]
As an example, the sequence of independent sets in (8.2.3) is abbreviated as \((4, 1, 4, 1, 4, 97, 95, 1, 100, 8, 109, -7, 1)\).

\[
(8.2.5) \ n=127, \ A=\{a^i | i=3, 5, 7, 11, 19, 21, 23, 55, 63\}, \ \mu_{-1}.
\]
The code has zeros \(a^{19i}, 1 \leq i \leq 12\), so \(d \geq 13\).
Theorem (3.1.4) gives \(d \geq 15\).

\[
(8.2.6) \ n=127, \ A=\{a^i | i=1, 3, 5, 7, 9, 19, 23, 29, 43\}, \ \mu_{-1}.
\]
By Theorem (3.1.4), \(d_0 \geq 15\), and by the BCH bound, \(d \geq 11\), hence \(d \geq 12\).
Let \(c(x)\) be a codeword of weight 12.
Then \(c(a^{11}) \neq 0\) by the BCH bound. The following sets are independent w.r.t. the zero-set of \(c(x)\):
\[
(11, -1, 11, -1, 11, -6, 11, 53, 88, 9, 69, -59, 22, 2, 11, -8, 22, 2, 11, 14, 44, -15, \\
22, 63, 11), \ \text{so wt}(c(x)) \geq 13, \ \text{a contradiction}.
\]
Then Theorem (3.1.4) gives \(d \geq 15\).

\[
(8.2.7) \ n=127, \ A=\{a^i | i=3, 5, 7, 9, 11, 23, 27, 43, 63\}, \ \mu_{-1}.
\]
The code has zeros \(a^{91i}, 1 \leq i \leq 8\), so \(d \geq 9\). Hence \(d \geq 12\), by Theorem (3.1.4).
Let \(c(x)\) be a codeword of weight 12 with zero-set \(S\).
By the BCH bound, \(c(a) \neq 0\) and \(c(a^{19}) \neq 0\).
Using Hogendoorn's program, the computer showed that the code with defining set \(A \cup \{a^{21}\}\) has minimum distance at least 13.
So \(c(a^{21}) \neq 0\). The following sets are independent w.r.t. \(S\):
\[
(1, 84, 2, -62, 1, 23, 25, -2, 21, -11, 41, 34, 1, -22, 1, -53, 41, -8, 32, -21, 8, -1, \\
1, 1, -1, 1), \ \text{so wt}(c(x)) \geq 13, \ \text{a contradiction}.
\]
By Theorem (3.1.4), we have \(d \geq 15\).

\[
(8.2.8) \ n=127, \ A=\{a^i | i=9, 11, 13, 15, 19, 31, 43, 47 \ 63\}, \ \mu_{-1}.
\]
The code has zeros \(a^{90+25i}, 0 \leq i \leq 13\), so \(d \geq 15\).
(8.2.9) $n=127$, $A=\{a^i | i=3,7,9,13,19,21,29,47,63\}$, $\mu_{-1}$.
The code has zeros $a^{100+11i}$, $0\leq i\leq 13$, so $d\geq 15$.

(8.2.10) $n=127$, $A=\{a^i | i=3,9,11,15,21,23,27,47,63\}$, $\mu_{-1}$.
The complete defining set of $C$ contains $\{a^{3i} | 1\leq i\leq 10\}$, so $d\geq 11$.
Then Theorem (3.1.4) gives $d\geq 12$. Let $c(x)$ be a codeword of weight 12 with zero-set $S$.
Then $c(a^5)\neq 0$, since otherwise $c(a^3i)=0$, $0\leq i\leq 12$.
The following sets are independent w.r.t. $S$:
$(66,-19,66,2,80,-8,66,3,66,-45,33,-3,33,-3,33,-3,33,-3,33,-3,$
$80,96,66)$, so $\text{wt}(c(x))\geq 13$, a contradiction.
Hence $d\geq 15$, by Theorem (3.1.4).

(8.2.11) $n=127$, $A=\{a^i | i=3,5,7,19,23,29,43,55,63\}$, $\mu_{-1}$.
The code has zeros $a^{23+5i}$, $0\leq i\leq 8$, so $d\geq 10$, and hence $d\geq 12$ by Theorem (3.1.4). Let $c(x)$ be a codeword of weight 12 with zero-set $S$.
Then $c(a^9)\neq 0$ (otherwise $c(a^{23+5i})=0$, $0\leq i\leq 12$) and $c(a^{13})\neq 0$ (otherwise $c(a^{76+7i})=0$, $0\leq i\leq 13$).
The following sets are independent w.r.t. $S$:
$(9,47,9,69,68,-58,68,66,81,-76,52,53,68,-5,68,-5,68,-5,68,-5,$
$9,47,9,)$, so $\text{wt}(c(x))\geq 13$, a contradiction. Then, by Theorem (3.1.4), $d\geq 15$.

(8.2.12) $n=127$, $A=\{a^i | i=1,5,13,15,27,29,31,43,55\}$, $\mu_{-1}$.
The code has zeros $a^{54i}$, $1\leq i\leq 12$, so $d\geq 13$. Hence by Theorem (3.1.4), $d\geq 15$.

(8.2.13) $n=127$, $A=\{a^i | i=1,3,7,19,23,29,43,47,55\}$, $\mu_{-1}$.
We know that $d_0\geq 15$. Let $c(x)$ be a codeword of even weight $\leq 12$ with zero-set $S$.
(i) $c(a^{15})\neq 0$, since otherwise $c(a^{97+15i})=0$, $0\leq i\leq 14$.
(ii) Suppose $c(a^5)=0$. Then $c(a^{13})\neq 0$, since otherwise $c(a^{57+35i})=0$, $0\leq i\leq 14$. The following sets are independent w.r.t. $S$:
$(60,-21,60,-10,60,30,60,-40,30,36,35,-10,35,30,35,-10,35,51,$
$30,-10,30,-10,30)$, so $\text{wt}(c(x))\geq 13$.
Hence $c(a^5)\neq 0$.
(iii) $c(a^{27})\neq 0$, since otherwise we have the following independent sets w.r.t. $S$:...
(15,1,15,71,13,19,30,16,15,12,113,74,5,-1,40,21,26,33,60,
\neg 1,60,\neg 1,60,\neg 1,60) \text{ so } \wt(c(x)) \geq 13.

(iv) \(c(a^{11}) \neq 0\), since otherwise we have the following independent sets w.r.t. \(S\):
\[(5,1,-1,2,5,41,89,50,104,8,5,10,8,5,2,13,46,51,2,1,51,2,1,51).\]
The following sets are independent w.r.t. \(S\):
\[(5,-5,44,3,1,99,19,60,-17,33,64,89,-44,51,2,49,-46,5,89,113,-35,
\neg 15,-55,15), \text{ so } \wt(c(x)) \geq 13, \text{ a contradiction.}\]

We have proved that \(d \geq 14\). Then Theorem (3.1.4) shows that \(d \geq 15\).

(8.2.14) \(n=127\), \(A=\{a^i \mid i=3,15,19,21,23,29,47,55,63\}, \nu=1\).
The code has zeros \(a^{19i}\), \(1 \leq i \leq 8\), so \(d \geq 9\). Hence \(d \geq 12\) by Theorem (3.1.4).

Let \(c(x)\) be a codeword of weight 12 with zero-set \(S\).

(i) \(c(a^7) \neq 0\), since otherwise \(c(a_9) = 0\), \(0 \leq i \leq 11\).

(ii) \(c(a^{31}) \neq 0\), since otherwise \(c(a^i) = 0\), \(113 \leq i \leq 127\).

(iii) Suppose \(c(a^7) = 0\).

a) \(c(a) \neq 0\), since otherwise \(c(a^{19i}) = 0\), \(0 \leq i \leq 12\).

b) \(c(a^5) \neq 0\), since otherwise we have the following independent sets w.r.t. \(S\):
\[(1,64,1,-9,1,-1,64,-9,64,1,1,-9,1,-1,64,-9,64,1,-9,1,
\neg 1,64,-9,1).\]
The following sets are independent w.r.t. \(S\):
\[(1,-1,1,-1,95,40,1,103,-4,40,34,5,-16,108,-17,40,20,115,-1,
\neg 15,-1,108,-17,108), \text{ so } \wt(c(x)) \geq 13, \text{ a contradiction.}\]

Hence \(c(a^7) \neq 0\).

(iv) Suppose \(c(a) = 0\). Then \(c(a^9) \neq 0\), since otherwise \(c(a^{37+9i}) = 0\), \(0 \leq i \leq 12\).
The following sets are independent w.r.t. \(S\):
\[(56,-10,56,19,56,9,56,44,9,-9,9,-9,9,-9,9,-9,9,-9,9), \text{ so } c(a) \neq 0.\]
The following sets are independent w.r.t. \(S\):
\[(1,81,108,2,102,-81,121,9,121,12,97,76,108,1,1,8,102,-1,1,-71,1,
70,1,-8,1), \text{ so } \wt(c(x)) \geq 13, \text{ a contradiction. Hence } d \geq 13.\]

Then Theorem (3.1.4) gives \(d \geq 15\).

(8.2.15) \(n=127\), \(A=\{a^i \mid i=3,5,9,13,15,19,21,29,63\}, \nu=1\).

By the BCH bound we have \(d \geq 11\), hence \(d \geq 12\) by Theorem (3.1.4).
Let $c(x)$ be a codeword of weight 12 with zero-set $S$.

Then $c(\alpha^{31}) \neq 0$ and $c(\alpha^{11}) \neq 0$ by computer (i.e., the computer showed that the codes with defining sets $A \cup \{\alpha^{31}\}$ and $A \cup \{\alpha^{11}\}$ both have minimum distance at least 13, using Hogendoorn's program).

The following sets are independent w.r.t. $S$:

$$\{31, -5, 121, 24, 124, -29, 115, 45, 31, 50, 79, -3, 79, -8, 115, -31, 22, 1, 122, 1, 22, -1, 22, -1, 22\},$$

so $\text{wt}(c(x)) \geq 13$.

We have proved that $d \geq 13$, and hence $d \geq 15$.

(8.2.16) $n=127$, $A=\{\alpha^i | i=1, 3, 5, 9, 15, 23, 27, 29, 43\}$, $\mu_1$.

The code has zeros $\alpha^{57+i}$, $0 \leq i \leq 9$, so $d \geq 11$, and hence $d \geq 12$.

Let $c(x)$ be a codeword of weight 12 with zero-set $S$.

Then $c(\alpha^{21}) \neq 0$, since otherwise $c(\alpha^{3i})=0$, $0 \leq i \leq 14$.

The following sets are independent w.r.t. $S$:

$$\{21, -21, 21, 24, 21, -21, 21, 24, 21, -21, 21, 24, 21, -21, 21, 24, 21, -21, 21, 3, 21\},$$

a contradiction.

Then, by Theorem (3.1.4), $d \geq 15$.

(8.2.17) $n=127$, $A=\{\alpha^i | i=5, 7, 9, 13, 19, 29, 31, 43, 63\}$, $\mu_1$.

Let $c(x)$ be a codeword of even weight $\leq 12$.

Then, by computer, $c(\alpha^i) \neq 0$, $i=3, 21, 23, 47, 55$.

The following sets are independent w.r.t. the zero-set of $c(x)$:

$$\{3, 17, 87, 16, 61, -22, 59, -1, 96, -13, 46, -11, 55, -46, 117, -12, 84, 42, 55, -20, 21, -1, 21, -1, 21\},$$

so $\text{wt}(c(x)) \geq 13$.

Hence, by Theorem (3.1.4), $d \geq 15$.

(8.2.18) $n=127$, $A=\{\alpha^i | i=3, 11, 15, 19, 23, 43, 47, 55, 63\}$, $\mu_1$.

The code has zeros $\alpha^i$, $43 \leq i \leq 50$, so $d \geq 12$.

Let $c(x)$ be a codeword with weight 12 and zero-set $S$.

By computer, $c(\alpha^i) \neq 0$, $i=5, 7, 21, 27, 31$.

The following sets are independent w.r.t. $S$:

$$\{77, -29, 102, 7, 108, 14, 42, -4, 33, -8, 31, -19, 14, -16, 77, -27, 51, -2, 51, -1, 51, -1, 51\},$$

a contradiction.

So $d \geq 15$, by Theorem (3.1.4).

(8.2.19) $n=127$, $A=\{\alpha^i | i=9, 13, 15, 19, 21, 29, 31, 47, 63\}$, $\mu_1$.

The code has zeros $\alpha^i$, $119 \leq i \leq 126$, so $d \geq 9$, and hence $d \geq 12$. 
Let $c(x)$ be a codeword of weight 12 with zero-set $S$. The computer showed that $c(a_i) \neq 0$, $i=5, 11, 27$.

The following sets are independent w.r.t. $S$:

$$\{77, 38, 80, 47, 88, -4, 80, -6, 77, -6, 69, -30, 40, -3, 77, -39, 40, -1, 20, -1, 20, -1, 20\},$$

a contradiction. Hence $d \geq 15$.

(8.2.20) $n=127$, $A=\{a_i^i\mid i = 1, 3, 5, 9, 11, 15, 21, 23, 27\}$, $\mu_{-1}$.
The code has zeros $\alpha^{3i}$, $1 \leq i \leq 12$, so $d \geq 13$.

Then Theorem (3.1.4) gives $d \geq 15$.

(8.2.21) $n=127$, $A=\{a_i^i\mid i = 3, 9, 15, 23, 27, 29, 43, 47, 63\}$, $\mu_{-1}$.
The code has zeros $\alpha^{96+3i}$, $0 \leq i \leq 10$, so $d \geq 12$.

Let $c(x)$ be a codeword with weight 12 and zero-set $S$.

By computer, $c(a_i) \neq 0$, $i = 1, 7, 21, 55$. The following sets are independent w.r.t. $S$:

$$(\bar{2}, -3, 2, -3, 2, 16, 1, 84, 37, -10, 56, -3, 56, -26, 1, -3, 110, -9, 62, -53, 2, -2, 1, -1, 1),$$

a contradiction. Hence $d \geq 15$.

(8.2.22) $n=127$, $A=\{a_i^i\mid i = 1, 3, 7, 11, 19, 21, 23, 47, 55\}$, $\mu_{-1}$.
The complete defining set of $C$ contains $\{a_{50+17i}\mid 0 \leq i \leq 11\}$, so $d \geq 13$. Then Theorem (3.1.4) gives $d \geq 15$.

(8.2.23) $n=127$, $A=\{a_i^i\mid i = 5, 7, 11, 13, 27, 31, 43, 55, 63\}$, $\mu_{-1}$.
The code has zeros $\alpha^{103+3i}$, $0 \leq i \leq 7$, so $d \geq 9$. Hence $d \geq 12$.

Let $c(x)$ be a codeword of weight 12.

Then, by computer, $c(a_i) \neq 0$, $i = 3, 9, 21$.

The following sets are independent w.r.t. the zero-set of $c(x)$:

$$(9, 26, 9, -2, 42, 7, 84, -18, 96, -11, 41, -9, 36, -4, 9, -30, 12, -5, 6, -7, 12, -1, 12, -1, 12),$$

a contradiction. So $d \geq 15$.

(8.2.24) $n=127$, $A=\{a_i^i\mid i = 1, 3, 5, 11, 15, 19, 23, 43, 55\}$, $\mu_{-1}$.

We know that $d_0 \geq 15$. Let $c(x)$ be a codeword of even weight $\leq 12$ with zero-set $S$. By computer, $c(a_i) \neq 0$, $i = 7, 13, 63$.

The following sets are independent w.r.t. $S$:

$$(26, -1, 26, -20, 26, -1, 52, 28, 119, -31, 95, -19, 67, -10, 56, -34, 70, -17, 7, -3, 7, -1, 7, -1, 7),$$

so $\text{wt}(c(x)) \geq 13$, a contradiction.

Hence, by Theorem (3.1.4), $d \geq 15$. 

(8.2.25) $n=127$, $A=\{a_i \mid i=1,5,7,9,23,27,29,31,43\}$, $\mu_1$.

The code has zeros $\alpha^{89+13i}$, $0 \leq i \leq 11$, so $d \geq 13$.

Then, by Theorem (3.1.4), $d \geq 15$.

(8.2.26) $n=127$, $A=\{a_i \mid i=1,5,9,11,13,15,19,31,43\}$, $\mu_1$.

The complete defining set of $C$ contains $\{a^{5i} \mid 1 \leq i \leq 10\}$, so $d \geq 11$.

Hence $d \geq 12$. Let $c(x)$ be a codeword of weight 12 with zero-set $S$.

By computer, $c(a^i) \neq 0$, $i=21,27,47$.

The following sets are independent w.r.t. $S$:

$\{9,24,89,-70,27,26,54,-1,51,-42,27,-1,61,-8,54,32,87,-14,74,-1,74,\}$

$\{-1,74,-1,74\}$, a contradiction.

Then Theorem (3.1.4) gives $d \geq 15$.

(8.2.27) $n=127$, $A=\{a_i \mid i=1,3,13,15,21,27,29,47,55\}$, $\mu_1$.

The code has zeros $\alpha^{35i}$, $1 \leq i \leq 14$, so $d \geq 15$.

a) Let $c(x)$ be a codeword of weight 15 with zero-set $S$.

(i) $c(a^9) \neq 0$, since otherwise $c(a^{35i})=0$, $1 \leq i \leq 15$.

(ii) Suppose $c(a^{45})=0$.

Then $c(a^{45}) \neq 0$, since otherwise the following sets are independent w.r.t. $S$:

$\{9,29,2,39,2,12,34,21,68,-26,68,-13,68,-13,68,-13,68,-13,68,-13,68,-13,68\}$

The following sets are independent w.r.t. $S$:

$\{17,67,45,36,45,-26,68,-17,106,4,68,-26,68,-13,68,-13,68,-26,68,-13,68,-13,68,-13,68,-13,68\}$

so $\text{wt}(c(x)) \geq 16$, a contradiction. Hence $c(a^{45}) \neq 0$.

The following sets are independent w.r.t. $S$:

$\{17,92,17,-15,72,-13,72,50,50,-2,72,-33,17,22,72,17,38,-52,100,29,72,-33,17,-35,17,-35,17,-35,17\}$, a contradiction.

We have proved that $d \geq 16$.

b) Let $c(x)$ be a codeword of weight 16 with zero-set $S$.

(i) $c(a^9) \neq 0$, since otherwise $c(a^{35i})=0$, $0 \leq i \leq 15$.

(ii) Suppose $c(a^{45})=0$.

Then $c(a^{45}) \neq 0$, since otherwise the following sets are independent w.r.t. $S$:

$\{68,52,68,-13,68,63,72,17,34,21,68,-26,68,-13,68,-13,68,-13,68,-13,68,-13,68,-13,68\}$.
The following sets are independent w.r.t. $S$:


Hence $c(a^{19}) \neq 0$.

The following sets are independent w.r.t. $S$:

$$(17, 57, 100, 17, 34, -4, 100, 22, 17, -13, 50, -2, 72, -33, 17, 22, 72, 21, 38, -52, 100, 29, 72, -33, 17, -35, 17, -35, 17, -35, 17, -35, 17) ,$$

so $w_\ell(c(x)) \geq 17$, a contradiction.

Hence $d \geq 17$. Then Theorem (3.1.4) shows that $d \geq 19$.

$$(8.2.28) \ n=127, \ A=\{a^i | i=5, 15, 19, 23, 29, 31, 43, 55, 63\} , \ \mu_{-1} .$$

The code has zeros $a^{71+7i}$, $0 \leq i \leq 7$, so $d \geq 9$.

Hence $d \geq 12$, by Theorem (3.1.4).

Let $c(x)$ be a codeword of weight 12 with zero-set $S$.

Then, by computer, $c(a^i) \neq 0$, $i=1, 3, 7$.

The following sets are independent w.r.t. $S$:

$$(112, -66, 112, 12, 48, -8, 96, 3, 12, -20, 4, -4, 24, -4, 24, -5, 14, -23, 96, -3, 1, -1, 1, -1, 1) ,$$

a contradiction.

Then Theorem (3.1.4) gives $d \geq 15$.

$$(8.2.29) \ n=127, \ A=\{a^i | i=5, 7, 9, 11, 13, 19, 21, 31, 63\} , \ \mu_{-1} .$$

The code has zeros $a^{71}$, $1 \leq i \leq 10$, so $d \geq 11$. Hence $d \geq 12$.

Let $c(x)$ be a codeword of weight 12.

Then, by computer, $c(a^i) \neq 0$, $i=3, 23, 27, 29, 55$.

The following sets are independent w.r.t. the zero-set of $c(x)$:

$$(3, 33, -3, 46, -2, 110, -6, 83, -4, 101, -3, 96, -24, 89, -39, 51, -13, 12, -1, 12, -1, 12, -1, 12) ,$$

a contradiction.

We have proved that $d \geq 15$.

$$(8.2.30) \ n=127, \ A=\{a^i | i=1, 7, 13, 21, 27, 29, 31, 47, 55\} , \ \mu_{-1} .$$

The code has zeros $a^{64+19i}$, $0 \leq i \leq 9$, so $d \geq 11$. Hence $d \geq 12$.

Let $c(x)$ be a codeword of weight 12 with zero-set $S$.

The computer showed that $c(a^i) \neq 0$, $i=3, 5, 15, 23, 43$.

The following sets are independent w.r.t. $S$:

$$(75, -20, 75, -13, 114, -7, 30, -3, 53, -1, 65, -10, 92, -14, 106, -27, 5, -20, 5, -3, 3, -1, 3, -1, 3) ,$$

a contradiction. Then Theorem (3.1.4) gives $d \geq 15$. 

- 48 -
(8.2.31) \( n=127, A=\{a^i \mid i=1,3,7,9,11,23,27,43,47\}, u-1. \)

The code has zeros \( \alpha^{87+21i}, 0 \leq i \leq 13 \), so \( d \geq 15. \)

a) Let \( c(x) \) be a codeword of weight 12 with zero-set \( S \).

(i) \( c(a^5) \neq 0 \), since otherwise \( c(a^{3+21i}) = 0, 0 \leq i \leq 17. \)

(ii) Suppose \( c(a^{55}) = 0. \)

Then \( c(a^{19}) \neq 0 \), since otherwise the following sets are independent w.r.t. \( S \):

\[
\{66,21,66,21,66,21,66,21,66,21,66,21,66,21,66,21,66,21,66,21,66,21,42,80,-21,5,-40,5\}.
\]

The following sets are independent w.r.t. \( S \):

\[
\{51,41,5,1,100,12,38,-2,100,51,66,21,66,-64,66,-21,66,9,33,75,66,21,66,21,66,21,66,21,66\}, \text{ a contradiction.}
\]

Hence \( c(a^{55}) \neq 0. \)

The following sets are independent w.r.t. \( S \):

\[
\{66,21,66,21,66,21,66,-43,66,-42,118,25,91,-46,66,9,33,75,66,21,66,21,66,21,66,21,66\}, \text{ a contradiction.}
\]

Hence \( d \geq 16. \)

b) Let \( c(x) \) be a codeword of weight 16 with zero-set \( S \).

(i) Again \( c(a^5) \neq 0. \)

(ii) Suppose \( c(a^{55}) = 0. \)

Then \( c(a^{19}) \neq 0 \), since otherwise the following sets are independent w.r.t. \( S \):

\[
\{66,21,66,21,66,21,66,21,66,21,66,21,66,21,66,21,66,21,66,21,66,21,42,80,-21,5,-85,40,45,5\}.
\]

The following sets are independent w.r.t. \( S \):

\[
\{5,41,5,1,100,12,38,-2,100,51,66,21,66,-64,66,-21,66,9,33,75,66,21,66,21,66,21,66,21,66\}, \text{ a contradiction.}
\]

Hence \( c(a^{55}) \neq 0. \)

The following sets are independent w.r.t. \( S \):

\[
\{66,21,66,21,66,21,66,21,66,21,66,21,66,21,66,21,66,21,66,21,66,21,42,118,25,91,-46,66,9,33,75,66,21,66,21,66,21,66\}, \text{ a contradiction.}
\]

Hence \( d \geq 17. \)

Then Theorem (3.1.4) gives \( d \geq 19. \)

(8.2.32) \( n=151, A=\{a^i \mid i=1,3,7,15,35\}, u-1. \)

From Theorem (3.1.4) we know that \( d_0 \geq 15, d_0 \equiv 3 \mod 4. \)

Furthermore, all even weights are divisible by 4.

The code has zeros \( \alpha^{61+3i}, 0 \leq i \leq 8 \), so \( d \geq 10. \) Hence \( d \geq 12. \)
a) Let \( c(x) \) be a codeword of weight 12 or 16 with zero-set \( S \).

By computer, \( c(\alpha^i) \neq 0 \), \( i=5,11,17,23,37 \).

The following sets are independent w.r.t. \( S \):
\[
(10,44,10,-3,40,25,139,-5,72,-1,37,-7,5,-26,39,103,29,-22,121,
-3,5,-41,40,-50,72,-11,72,-1,37,-1,72),
\]
a contradiction.

b) Let \( c(x) \) be a codeword of weight 15 with zero-set \( S \).

Again by computer, \( c(\alpha^i) \neq 0 \), \( i=5,11,17,23,37 \).

The following sets are independent w.r.t. \( S \):
\[
(5,-1,5,56,36,-1,36,-22,28,14,119,-7,18,-27,135,-24,119,35,40,-13,80,
-77,113,-37,119,-1,119,-1,119,-1,119),
\]
a contradiction.

We have proved that \( d \geq 19 \).

(8.2.33) \( n=151 \), \( A=\{\alpha^i | i=1,3,7,17,35\} \), \( \nu=1 \).

We know that \( d_0 \geq 15 \) and that all even weights are divisible by 4.

Let \( c(x) \) be a codeword of even weight \( \leq 12 \).

Then, by computer, \( c(\alpha^i) \neq 0 \), \( i=5,11,15,23,37 \).

The following sets are independent w.r.t. the zero-set of \( c(x) \):
\[
(120,1,67,-10,67,-14,54,-1,95,-10,134,-1,132,-28,144,-43,72,-10,134,
-48,72,-1,72,-1,72),
\]
a contradiction.

Hence \( d \geq 15 \).

(8.2.34) \( n=151 \), \( A=\{\alpha^i | i=1,3,7,11,17\} \), \( \nu=1 \).

The code has zeros \( \alpha^{13+3i} \), \( 0 \leq i \leq 7 \), so \( d \geq 9 \). Hence \( d \geq 12 \).

Let \( c(x) \) be a codeword of weight 12 with zero-set \( S \).

By computer, \( c(\alpha^i) \neq 0 \), \( i=5,15,23,35,37 \).

The following sets are independent w.r.t. \( S \):
\[
(23,2,94,-4,33,-4,125,-1,107,-3,92,-6,37,-34,40,-8,80,-28,5,-2,
5,-1,5,-1,5),
\]
a contradiction.

Hence, by Theorem (3.1.4), \( d \geq 15 \).

(8.2.35) \( n=161 \), \( A=\{\alpha^i | i=5,11,35,69\} \), \( \nu=1 \).

The code has zeros \( \alpha^{139+i} \), \( 132 \leq i \leq 138 \), so \( d \geq 8 \).

Let \( c(x) \) be a codeword of weight 8 with zero-set \( S \).

Then \( c(\alpha^{139}) \neq 0 \) by the BCH bound.

The following sets are independent w.r.t. \( S \):
\[
(139,-101,131,-52,146,-9,139,-1,139,-1,139,-1,139,-1,139,-1,139),
\]
a contradiction.

Then, by Theorem (3.1.4), we have \( d \geq 12 \).
(8.2.36) \( n=223, \ A=\{a^i|i=1,3,5\}, \ u \).  
We know from Theorem (3.1.4) that \( d_0 \geq 19 \) and that all even weights are divisible by 4.

The BCH bound gives \( d \geq 9 \). Hence \( d \geq 12 \).

Let \( c(x) \) be a codeword of weight 12 or 16 with zero-set \( S \).

Then, by computer, \( c(a^i) \neq 0, i=9,13,19 \).

The following sets are independent w.r.t. \( S \):
\[
(50, -4, 50, -1, 50, -1, 83, -3, 106, -1, 188, -23, 19, -11, 19, 186, 81, -47, 177, -65, 175, -5, 89, -47, 29, -18, 2, -7, 9, -1, 9, -1, 9, -1, 9, -1, 9), \] a contradiction.

We have proved that \( d \geq 19 \).

(8.2.37) \( n=233, \ A=\{a^i|i=5,9,17,29\}, \ u \).

The code has zeros \( a^i \), \( 78 \leq i \leq 85 \), so \( d \geq 9 \). Hence \( d \geq 12 \), by Theorem (3.1.4).

Let \( c(x) \) be a codeword of weight 12 with zero-set \( S \).

Then, by computer, \( c(a^i) \neq 0, i=1,3,7,27 \).

The following sets are independent w.r.t. \( S \):
\[
(111, -1, 108, -3, 183, -4, 189, -2, 188, -1, 4, -7, 94, -3, 89, -6, 86, -1, 86, -1, 86, -1, 86, -1, 86, -1, 86), \] a contradiction.

Hence \( d \geq 16 \), by Theorem (3.1.4).

(8.2.38) \( n=233, \ A=\{a^i|i=1,3,9,27\}, \ u \).

The code has zeros \( a^i \), \( 69 \leq i \leq 77 \), so \( d \geq 10 \). Hence \( d \geq 12 \).

Let \( c(x) \) be a codeword of weight 12 or 16 with zero-set \( S \).

By computer, \( c(a^i) \neq 0, i=5,7,17,29 \).

The following sets are independent w.r.t. \( S \):
\[
(49, -2, 139, -1, 56, -3, 208, -5, 44, -1, 44, -35, 93, -23, 139, -47, 58, -54, 41, -48, 225, -80, 147, -3, 141, -68, 78, -1, 78, -1, 78, -1, 78), \] a contradiction.

Then Theorem (3.1.4) gives \( d \geq 17 \).

(8.2.39) \( n=233, \ A=\{a^i|i=1,17,27,29\}, \ u \).

We know that \( d_0 \geq 17 \).

The even-weight subcode has zeros \( a^{131+17i} \), \( 0 \leq i \leq 12 \), so \( d \geq 14 \).

Let \( c(x) \) be a codeword of weight 14 or 16 with zero-set \( S \).

By computer, \( c(a^i) \neq 0, i=3,5,7,9 \).

The following sets are independent w.r.t. \( S \):
\[
(200, -2, 138, -3, 164, -1, 113, -7, 164, -1, 183, -21, 100, -26, 56, -9, 167, 87, 123, 18, 31, 126, 96, -26, 177, 60, 5, -3, 3, -1, 3, -1, 3), \] a contradiction.

Hence \( d \geq 17 \).
(8.2.40) \( n=241, A=\{a^i | i=5,9,11,13,25\} \), \( u \mid 11 \).

Theorem (3.1.4) gives \( d_0 \geq 17 \).

The even-weight subcode has zeros \( a^{41+25i}, 0 \leq i \leq 16 \), so the even-weight subcode has minimum distance \( \geq 18 \).

Hence \( d \geq 17 \).

(8.2.41) \( n=241, A=\{a^i | i=1,5,9,13,25\} \), \( u \mid 11 \).

We know that \( d_0 \geq 17 \). The even-weight subcode has minimum distance \( \geq 22 \), since it has zeros \( a^{232+25i}, 0 \leq i \leq 20 \).

Let \( c(x) \) be a codeword of weight 17 with zero-set \( S \).

Then, by computer, \( c(a^i) \neq 0, i=3,7,11,21,35 \).

The following sets are independent w.r.t. \( S \):

\[
\begin{align*}
(11,-1,196,-1,61,-4,219,-10,102,-15,139,-7,213,-5,48,-21,89,-74,139, \\
129,55,79,55,-107,48,-56,131,-24,85,-26,11,-1,11,-1,11)
\end{align*}
\]

a contradiction.

We have proved that \( d \geq 19 \).

(8.2.42) \( n=241, A=\{a^i | i=5,7,9,11,13\} \), \( u \mid 11 \).

We have \( d_0 \geq 17 \).

Let \( c(x) \) be a codeword of even weight \( \leq 14 \).

Then, by computer, \( c(a^i) \neq 0, i=1,3,21,25,35 \).

The following sets are independent w.r.t. the zero-set of \( c(x) \):

\[
\begin{align*}
(24,-1,84,-1,120,-3,235,-1,156,-7,73,-20,151,126,71,-3,204,-51,200, \\
-96,163,-39,27,-7,12,-1,12,-1,12)
\end{align*}
\]

a contradiction.

Hence \( d \geq 16 \).
Section 8.3: The table

In this section we give a table of all binary duadic codes of length \( \leq 241 \). For each code we give

(i) \( n \) : the code-length.

(ii) the idempotent : e.g. the duadic code of length 49 has idempotent

\[
0 + \sum_{i \in C_1} x^i + \sum_{i \in C_7} x^i.
\]

(iii) a defining set : e.g. the duadic code of length 49 has defining set \( \{ \alpha^i \mid i \in C_1 \cup C_2 \} \), where \( \alpha \) is a primitive 49-th root of unity.

(iv) \( d \) : the minimum distance, or bounds for it.

Most of the upper bounds are from [7].

Note that binary QR codes have an odd minimum distance (cf. [10]).

(v) \( a \) : the splitting is given by \( \mu_a \).

(vi) a reference.
<table>
<thead>
<tr>
<th>$n$</th>
<th>idempotent</th>
<th>defining set</th>
<th>$d$</th>
<th>$a$</th>
<th>reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>-1</td>
<td>QR code, [10]</td>
</tr>
<tr>
<td>17</td>
<td>0,1</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>QR code, [7]</td>
</tr>
<tr>
<td>23</td>
<td>1</td>
<td>1</td>
<td>7</td>
<td>-1</td>
<td>QR code, [7]</td>
</tr>
<tr>
<td>31</td>
<td>1,5,7</td>
<td>1,5,7</td>
<td>7</td>
<td>-1</td>
<td>QR code, [7]</td>
</tr>
<tr>
<td>31</td>
<td>1,3,5</td>
<td>1,3,5</td>
<td>7</td>
<td>-1</td>
<td>Reed-Muller code, (2.2.2)</td>
</tr>
<tr>
<td>41</td>
<td>0,1</td>
<td>1</td>
<td>9</td>
<td>3</td>
<td>QR code, [7]</td>
</tr>
<tr>
<td>47</td>
<td>1</td>
<td>1</td>
<td>11</td>
<td>-1</td>
<td>QR code, [7]</td>
</tr>
<tr>
<td>49</td>
<td>0,1,7</td>
<td>1,21</td>
<td>4</td>
<td>-1</td>
<td>(4.3.1)</td>
</tr>
<tr>
<td>71</td>
<td>1</td>
<td>1</td>
<td>11</td>
<td>-1</td>
<td>QR code, (3.1.4)</td>
</tr>
<tr>
<td>73</td>
<td>0,1,3,5,11</td>
<td>1,13,17,25</td>
<td>9</td>
<td>-1</td>
<td>(8.1.6)</td>
</tr>
<tr>
<td>73</td>
<td>0,1,3,5,13</td>
<td>3,9,11,17</td>
<td>9</td>
<td>-1</td>
<td>(8.1.3)</td>
</tr>
<tr>
<td>73</td>
<td>0,1,5,9,17</td>
<td>1,9,11,13</td>
<td>12</td>
<td>3</td>
<td>[7]</td>
</tr>
<tr>
<td>73</td>
<td>0,1,3,9,25</td>
<td>1,3,9,25</td>
<td>13</td>
<td>5</td>
<td>QR code, [7]</td>
</tr>
<tr>
<td>79</td>
<td>1</td>
<td>1</td>
<td>15</td>
<td>-1</td>
<td>QR code, [7]</td>
</tr>
<tr>
<td>89</td>
<td>0,1,3,5,13</td>
<td>1,9,13,33</td>
<td>12</td>
<td>-1</td>
<td>(8.2.1)</td>
</tr>
<tr>
<td>89</td>
<td>0,1,3,5,19</td>
<td>3,9,11,19</td>
<td>12</td>
<td>-1</td>
<td>(8.2.2)</td>
</tr>
<tr>
<td>89</td>
<td>0,1,3,11,33</td>
<td>1,3,11,33</td>
<td>15</td>
<td>5</td>
<td>[7]</td>
</tr>
<tr>
<td>89</td>
<td>0,1,5,9,11</td>
<td>1,5,9,11</td>
<td>17</td>
<td>3</td>
<td>QR code, [7]</td>
</tr>
<tr>
<td>97</td>
<td>0,1</td>
<td>1</td>
<td>15</td>
<td>5</td>
<td>QR code, [7]</td>
</tr>
<tr>
<td>103</td>
<td>1</td>
<td>1</td>
<td>19</td>
<td>-1</td>
<td>QR code, [7]</td>
</tr>
<tr>
<td>113</td>
<td>0,1,9</td>
<td>1,9</td>
<td>15</td>
<td>3</td>
<td>QR code, [7]</td>
</tr>
<tr>
<td>113</td>
<td>0,1,3</td>
<td>1,3</td>
<td>18</td>
<td>9</td>
<td>[7]</td>
</tr>
<tr>
<td>119</td>
<td>1,13,17,21</td>
<td>1,11,21,51</td>
<td>4</td>
<td>3</td>
<td>BCH bound</td>
</tr>
<tr>
<td>119</td>
<td>1,7,11,51</td>
<td>1,13,17,21</td>
<td>6</td>
<td>3</td>
<td>BCH bound</td>
</tr>
<tr>
<td>119</td>
<td>1,7,13,17</td>
<td>3,7,13,51</td>
<td>8</td>
<td>3</td>
<td>(8.2.3)</td>
</tr>
<tr>
<td>119</td>
<td>1,7,11,17</td>
<td>3,11,21,51</td>
<td>12</td>
<td>3</td>
<td>[7]</td>
</tr>
<tr>
<td>n</td>
<td>idempotent</td>
<td>defining set</td>
<td>d</td>
<td>a</td>
<td>reference</td>
</tr>
<tr>
<td>---</td>
<td>------------</td>
<td>--------------</td>
<td>---</td>
<td>---</td>
<td>-----------</td>
</tr>
<tr>
<td>127</td>
<td>1,3,9,11,13,15,21,27,47</td>
<td>1,3,5,7,9,11,13,19,21</td>
<td>15</td>
<td>-1</td>
<td>Reed-Muller code, (2.2.2)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,5,9,11,13,15,21,27,47</td>
<td>3,5,7,11,19,21,23,55,63</td>
<td>15</td>
<td>-1</td>
<td>(8.2.5)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,9,13,15,19,21,29,47</td>
<td>1,3,5,7,9,19,23,29,43</td>
<td>15</td>
<td>-1</td>
<td>(8.2.6)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,7,9,11,13,19,21,47</td>
<td>3,5,7,9,11,23,27,43,63</td>
<td>15</td>
<td>-1</td>
<td>(8.2.7)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,7,9,11,13,19,21,27,47</td>
<td>9,11,13,15,19,31,43,47,63</td>
<td>15</td>
<td>-1</td>
<td>(8.2.8)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,5,7,9,13,19,21,29</td>
<td>1,3,5,15,19,21,23,29,55</td>
<td>15</td>
<td>-1</td>
<td>(8.1.3)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,15,21,23,27,29,47,55</td>
<td>3,7,9,13,19,21,29,47,63</td>
<td>15</td>
<td>-1</td>
<td>(8.2.9)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,5,7,9,19,21,23,29</td>
<td>3,9,11,15,21,23,27,47,63</td>
<td>15</td>
<td>-1</td>
<td>(8.2.10)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,5,7,9,11,21,23,27</td>
<td>3,5,7,19,23,29,43,55,63</td>
<td>15</td>
<td>-1</td>
<td>(8.2.11)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,7,9,11,13,21,23,27,47</td>
<td>1,5,13,15,27,29,31,43,55</td>
<td>15</td>
<td>-1</td>
<td>(8.2.12)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,7,9,11,19,21,23,27,47</td>
<td>1,3,7,19,23,29,43,47,55</td>
<td>15</td>
<td>-1</td>
<td>(8.2.13)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,7,9,13,15,21,29,47</td>
<td>3,15,19,21,23,29,47,55,63</td>
<td>15</td>
<td>-1</td>
<td>(8.2.14)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,5,9,15,21,23,27,29</td>
<td>3,5,9,13,15,19,21,23,27</td>
<td>15-16</td>
<td>-1</td>
<td>(8.2.15)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,9,13,15,19,21,23,27,47</td>
<td>1,3,5,9,15,19,21,23,29,43</td>
<td>15-19</td>
<td>-1</td>
<td>(8.2.16)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,5,9,13,15,21,27,29</td>
<td>5,7,9,13,19,29,31,43,63</td>
<td>15-19</td>
<td>-1</td>
<td>(8.2.17)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,9,15,21,23,27,29,47</td>
<td>3,11,15,19,23,43,47,55,63</td>
<td>15-19</td>
<td>-1</td>
<td>(8.2.18)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,9,11,15,21,23,27,47</td>
<td>9,13,15,19,21,29,31,47,63</td>
<td>15-19</td>
<td>-1</td>
<td>(8.2.19)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,7,9,21,23,27,47</td>
<td>1,3,5,9,11,15,21,23,27</td>
<td>15-19</td>
<td>-1</td>
<td>(8.2.20)</td>
</tr>
<tr>
<td>( n )</td>
<td>idempotent</td>
<td>defining set</td>
<td>( d )</td>
<td>( a )</td>
<td>reference</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
<td>-------------------------------</td>
<td>-------</td>
<td>-------</td>
<td>-----------</td>
</tr>
<tr>
<td>127</td>
<td>1,3,5,9,13,15,19,21,29</td>
<td>3,9,15,23,27,29,43,47,63</td>
<td>15-19</td>
<td>-1</td>
<td>(8.2.21)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,9,11,13,15,19,21,29,47</td>
<td>1,3,7,11,19,21,23,47,55</td>
<td>15-19</td>
<td>-1</td>
<td>(8.2.22)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,9,15,19,21,23,29,47</td>
<td>5,7,11,13,27,31,43,55,63</td>
<td>15-19</td>
<td>-1</td>
<td>(8.2.23)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,5,9,15,19,21,23,29</td>
<td>1,3,5,11,15,19,23,43,55</td>
<td>15-19</td>
<td>-1</td>
<td>(8.2.24)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,11,13,15,21,27,47,55</td>
<td>1,5,7,9,23,27,29,31,43</td>
<td>15-19</td>
<td>-1</td>
<td>(8.2.25)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,5,7,9,11,13,19,21</td>
<td>1,5,9,11,13,15,19,31,43</td>
<td>15-19</td>
<td>-1</td>
<td>(8.2.26)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,5,7,11,13,15,21,27,55</td>
<td>1,3,13,15,21,27,29,47,55</td>
<td>19</td>
<td>-1</td>
<td>(8.2.27)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,5,7,21,23,27,29,55</td>
<td>5,15,19,23,29,31,43,63</td>
<td>15-19</td>
<td>-1</td>
<td>(8.2.28)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,5,7,9,21,23,27,29</td>
<td>5,7,9,11,13,19,21,31,63</td>
<td>15-19</td>
<td>-1</td>
<td>(8.2.29)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,5,7,9,13,21,27,29</td>
<td>1,7,13,21,27,29,31,47,55</td>
<td>15-19</td>
<td>-1</td>
<td>(8.2.30)</td>
</tr>
<tr>
<td>127</td>
<td>1,3,5,7,9,11,13,21,27</td>
<td>1,3,7,9,11,23,43,47</td>
<td>19</td>
<td>-1</td>
<td>(8.2.31)</td>
</tr>
<tr>
<td>127</td>
<td>1,9,11,13,15,19,21,31,47</td>
<td>1,9,11,13,15,19,21,31,47</td>
<td>19</td>
<td>-1</td>
<td>QR code, [12]</td>
</tr>
<tr>
<td>137</td>
<td>0,1</td>
<td>1</td>
<td>13-25</td>
<td>3</td>
<td>QR code, (3.1.4)</td>
</tr>
<tr>
<td>151</td>
<td>1,3,5,11,17,13,15,23,35</td>
<td>1,3,7,15,35</td>
<td>19</td>
<td>-1</td>
<td>(8.2.32)</td>
</tr>
<tr>
<td>151</td>
<td>1,3,5,11,15,1,3,7,15,35</td>
<td>1,3,7,17,35</td>
<td>15-19</td>
<td>-1</td>
<td>(8.2.33)</td>
</tr>
<tr>
<td>151</td>
<td>1,5,11,17,13,15,23,47,69</td>
<td>1,5,11,17,37</td>
<td>19</td>
<td>-1</td>
<td>QR code, [12]</td>
</tr>
<tr>
<td>151</td>
<td>1,3,7,11,15,1,3,7,11,17</td>
<td>1,3,7,11,17</td>
<td>15-23</td>
<td>-1</td>
<td>(8.2.34)</td>
</tr>
<tr>
<td>161</td>
<td>0,1,3,35,69,11,23,35</td>
<td>1,11,23,35</td>
<td>4</td>
<td>-1</td>
<td>BCH bound</td>
</tr>
<tr>
<td>161</td>
<td>0,1,3,7,23,17,11,69</td>
<td>1,7,11,69</td>
<td>8</td>
<td>-1</td>
<td>BCH bound, (3.1.4)</td>
</tr>
<tr>
<td>161</td>
<td>0,1,7,11,23,13,23,35</td>
<td>1,3,23,35</td>
<td>8</td>
<td>-1</td>
<td>BCH bound, (3.1.4)</td>
</tr>
<tr>
<td>161</td>
<td>0,1,7,11,69,5,11,35,69</td>
<td>5,11,35,69</td>
<td>12-16</td>
<td>-1</td>
<td>(8.2.35)</td>
</tr>
<tr>
<td>n</td>
<td>idempotent</td>
<td>defining set</td>
<td>d</td>
<td>a</td>
<td>reference</td>
</tr>
<tr>
<td>-------</td>
<td>------------</td>
<td>--------------</td>
<td>-----</td>
<td>-----</td>
<td>----------------------</td>
</tr>
<tr>
<td>167</td>
<td>1</td>
<td>1</td>
<td>15-23</td>
<td>-1</td>
<td>QR code, (3.1.4)</td>
</tr>
<tr>
<td>191</td>
<td>1</td>
<td>1</td>
<td>15-27</td>
<td>-1</td>
<td>QR code, (3.1.4)</td>
</tr>
<tr>
<td>193</td>
<td>0,1</td>
<td>1</td>
<td>15-27</td>
<td>5</td>
<td>QR code, (3.1.4)</td>
</tr>
<tr>
<td>199</td>
<td>1</td>
<td>1</td>
<td>15-31</td>
<td>-1</td>
<td>QR code, (3.1.4)</td>
</tr>
<tr>
<td>223</td>
<td>1,3,9</td>
<td>1,3,5</td>
<td>19-31</td>
<td>-1</td>
<td>(8.2.36)</td>
</tr>
<tr>
<td>223</td>
<td>1,9,19</td>
<td>1,9,19</td>
<td>19-31</td>
<td>-1</td>
<td>QR code, (3.1.4)</td>
</tr>
<tr>
<td>233</td>
<td>0,1,7,9,29</td>
<td>1,7,9,29</td>
<td>17-25</td>
<td>3</td>
<td>QR code, (3.1.4)</td>
</tr>
<tr>
<td>233</td>
<td>0,1,3,9,27</td>
<td>5,9,17,29</td>
<td>16-29</td>
<td>-1</td>
<td>(8.2.37)</td>
</tr>
<tr>
<td>233</td>
<td>0,1,3,7,27</td>
<td>1,3,9,27</td>
<td>17-29</td>
<td>-1</td>
<td>(8.2.38)</td>
</tr>
<tr>
<td>233</td>
<td>0,1,3,5,29</td>
<td>1,17,27,29</td>
<td>17-32</td>
<td>7</td>
<td>(8.2.39)</td>
</tr>
<tr>
<td>239</td>
<td>1</td>
<td>1</td>
<td>19-31</td>
<td>-1</td>
<td>QR code, (3.1.4)</td>
</tr>
<tr>
<td>241</td>
<td>0,1,3,7,9,21</td>
<td>5,9,11,13,25</td>
<td>17-25</td>
<td>11</td>
<td>(8.2.40)</td>
</tr>
<tr>
<td>241</td>
<td>0,1,3,5,7,9</td>
<td>1,5,9,13,25</td>
<td>19-30</td>
<td>11</td>
<td>(8.2.41)</td>
</tr>
<tr>
<td>241</td>
<td>0,1,7,9,13,21</td>
<td>5,7,9,11,13</td>
<td>16-30</td>
<td>11</td>
<td>(8.2.42)</td>
</tr>
<tr>
<td>241</td>
<td>0,1,3,5,9,25</td>
<td>1,3,5,9,25</td>
<td>17-31</td>
<td>11</td>
<td>QR code, (3.1.4)</td>
</tr>
</tbody>
</table>

\( n=217 \): There are 88 possibly inequivalent duadic codes of length 217.

All splittings are given by \( u_{-1} \).

<table>
<thead>
<tr>
<th>minimum distance</th>
<th>4</th>
<th>( \leq 8 )</th>
<th>( \leq 12 )</th>
<th>( \leq 16 )</th>
<th>( \leq 20 )</th>
<th>( \leq 24 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>number of codes</td>
<td>16</td>
<td>32</td>
<td>240</td>
<td>448</td>
<td>144</td>
<td>144</td>
</tr>
</tbody>
</table>
References

Index

<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>adjacency matrix</td>
<td>25</td>
</tr>
<tr>
<td>BCH bound</td>
<td>39</td>
</tr>
<tr>
<td>check polynomial</td>
<td>2</td>
</tr>
<tr>
<td>code</td>
<td>1</td>
</tr>
<tr>
<td>cyclic</td>
<td>2</td>
</tr>
<tr>
<td>duadic</td>
<td>5</td>
</tr>
<tr>
<td>dual</td>
<td>1</td>
</tr>
<tr>
<td>even-like</td>
<td>1</td>
</tr>
<tr>
<td>extended</td>
<td>1</td>
</tr>
<tr>
<td>generalized Reed-Muller</td>
<td>10</td>
</tr>
<tr>
<td>linear</td>
<td>1</td>
</tr>
<tr>
<td>Q-</td>
<td>7</td>
</tr>
<tr>
<td>QR</td>
<td>6</td>
</tr>
<tr>
<td>quadratic residue</td>
<td>6</td>
</tr>
<tr>
<td>Reed-Muller</td>
<td>10</td>
</tr>
<tr>
<td>Reed-Solomon</td>
<td>10</td>
</tr>
<tr>
<td>codeword</td>
<td>1</td>
</tr>
<tr>
<td>consecutive set</td>
<td>39</td>
</tr>
<tr>
<td>cyclotomic coset</td>
<td>5</td>
</tr>
<tr>
<td>defining set</td>
<td>3</td>
</tr>
<tr>
<td>complete</td>
<td>3</td>
</tr>
<tr>
<td>distance</td>
<td>1</td>
</tr>
<tr>
<td>minimum</td>
<td>1</td>
</tr>
<tr>
<td>dominate</td>
<td>25</td>
</tr>
<tr>
<td>even-like</td>
<td>1</td>
</tr>
<tr>
<td>generator matrix</td>
<td>2</td>
</tr>
<tr>
<td>generator polynomial</td>
<td>2</td>
</tr>
<tr>
<td>graph</td>
<td>2</td>
</tr>
<tr>
<td>complete</td>
<td>25</td>
</tr>
<tr>
<td>directed</td>
<td>25</td>
</tr>
<tr>
<td>HT bound</td>
<td>39</td>
</tr>
<tr>
<td>idempotent</td>
<td>3</td>
</tr>
<tr>
<td>incidence matrix</td>
<td>29</td>
</tr>
<tr>
<td>in-degree</td>
<td>25</td>
</tr>
<tr>
<td>independent set</td>
<td>40</td>
</tr>
<tr>
<td>length</td>
<td>1</td>
</tr>
<tr>
<td>odd-like</td>
<td>1</td>
</tr>
<tr>
<td>out-degree</td>
<td>25</td>
</tr>
<tr>
<td>Paley-matrix</td>
<td>27</td>
</tr>
<tr>
<td>parity check matrix</td>
<td>2</td>
</tr>
<tr>
<td>self-dual</td>
<td>2</td>
</tr>
<tr>
<td>self-orthogonal</td>
<td>2</td>
</tr>
<tr>
<td>splitting</td>
<td>5</td>
</tr>
<tr>
<td>doubly-regular</td>
<td>26</td>
</tr>
<tr>
<td>tournament</td>
<td>25</td>
</tr>
<tr>
<td>doubly-regular</td>
<td>25</td>
</tr>
<tr>
<td>regular</td>
<td>25</td>
</tr>
<tr>
<td>weight</td>
<td>1</td>
</tr>
</tbody>
</table>