On duadic codes

TECHNISCHE HOGESCHOOL EINDHOVEN
NEDERLAND
ONDERAFDELING DER WISKUNDE
EN INFORMATICA

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

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.

Contents

List of symbols

$GF(q)$	finite field of order q
$\underline{0}$	zero vector
$\underline{1}$	all-one vector
$[n,k]$	linear code of length n and dimension k
$[n,k,d]$	$[n,k]$ code with minimum distance d
$\dim C$	dimension of the linear code C
$wt(\underline{x})$	weight of the vector $\underline{x}$
$wt(c(x))$	weight of the polynomial $c(x)$
$d(\underline{x},\underline{y})$	distance of the vectors $\underline{x}$ and $\underline{y}$
$\overline{C}$	extended code of the code C
$C^{\perp}$	dual code of the code C
$(\underline{x},\underline{y})$	inner-product of the vectors $\underline{x}$ and $\underline{y}$
$GF(q)[x]$	polynomial ring over $GF(q)$
$GF(q)[x]/(x^n-1)$	residue class ring $GF(q)[x]$ mod (x^n-1)
(a,b)	greatest common divisor of a and b
$<g(x)>$	ideal in $GF(q)[x]/(x^n-1)$ generated by $g(x)$
$j(x)$	polynomial $1+x+x^2+\ldots+x^{n-1}$
$C_1 + C_2$	$\{\underline{c}_1+\underline{c}_2 \mid \underline{c}_1 \in C_1, \underline{c}_2 \in C_2\}$
$C_1 \perp C_2$	orthogonal direct sum of C_1 and C_2
C_i	cyclotomic coset containing i
μ_a	permutation $i \to ai$ mod n
$\mu_a : S_1 \rightleftarrows S_2$	(2.1.1)
$q \equiv \square \bmod n$	(2.1.3)
$q \equiv \not\square \bmod n$	(2.1.3)
$\lvert S \rvert$	number of elements of the set S
$\mathrm{ord}_n(a)$	multiplicative order of a mod n
$v_p(m)$	(3.2.1)
$p \mid a$	p divides a
$p \nmid a$	p does not divide a
$p^z \parallel a$	$p^z \mid a$ and $p^{z+1} \nmid a$
$S_{1,m}$, $S_{2,m}$	(3.2.5)
I	identity matrix
J	all-one matrix
A^T	transpose of the matrix A

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 GF(q) are defined. We show that they exist iff $q \equiv \square \bmod n$, i.e., if $n = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k}$ is the prime factorization of n, then duadic codes of length n over GF(q) exist iff $q \equiv \square \bmod p_i$, $i=1,2,\ldots,k$.

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 $p^z \| (q^t-1)$, where $t=\mathrm{ord}_p(q)$, that duadic codes of length p^m ($m \geq z$) over 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 ≤ 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 $\underline{x}$ is a vector, then the weight $wt(\underline{x})$ of $\underline{x}$, is the number of its non-zero coordinates. The distance $d(\underline{x},\underline{y})$ of two vectors $\underline{x}$ and $\underline{y}$, is the number of coordinates in which they differ. Note that $d(\underline{x},\underline{y})=wt(\underline{x}-\underline{y})$.

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

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

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

A vector $\underline{x}$ in $(GF(q))^n$ is called even-like if $\sum x_i = 0$, otherwise it is called odd-like. If a code contains only even-like vectors, then it is called an even-like code.

If $q=2$, then an even-like vector has even weight, and an odd-like vector has odd weight.

Let C be an $[n,k]$ code over $GF(q)$.

The extended code $\overline{C}$ is the $[n+1,k]$ code defined by

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

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

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

$C^\perp := \{\underline{x}\in(GF(q))^n|\forall_{\underline{y}\in C}[(\underline{x},\underline{y})=0]\}$, where (,) is the usual inner-product, $(\underline{x},\underline{y})=x_1y_1+x_2y_2+\ldots+x_ny_n$. $C^\perp$ is an $[n,n-k]$ code.

If $C \subset C^{\perp}$, 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 x 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 $\underline{x} \in C$ iff $H\underline{x}^T=\underline{0}$.

Section 1.2 : Cyclic codes

A linear code C of length n is called cyclic if

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

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

$$(c_0,c_1,\ldots,c_{n-1}) \in (GF(q))^n \rightleftarrows c_0+c_1x+c_2x^2+\ldots+c_{n-1}x^{n-1} \in GF(q)[x]/(x^n-1).$$

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.,
$C = \langle g(x)\rangle := \{a(x)g(x) \bmod (x^n-1) \mid a(x) \in GF(q)[x]\}$.
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 $\langle h(x)\rangle^{\leftarrow}$, which is obtained from $\langle h(x)\rangle$, by reversing the order of the symbols.

Let α be a primitive n-th root of unity in an extension field of GF(q), and let $S \subset \{0,1,\ldots,n-1\}$. We can define a cyclic code C of length n over GF(q) as follows :
$c(x)\in C$ iff $c(\alpha^i)=0$, $i\in S$
(and every cyclic code can be defined in this way).
The set $\{\alpha^i | i\in S\}$ 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 $\alpha^i \in A \Rightarrow \alpha^{qi} \in A$.

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

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

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

<u>Proof</u> : (i) Suppose $e(\alpha^i)=0$ if $i\in S$, and $e(\alpha^i)=1$ if $i\in T:=\{0,1,\dots,n-1\}\setminus S$.
Let $g(x) := \prod_{i\in S}(x-\alpha^i)$ ($g(x)$ is the generator polynomial of C).

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

Let $h(x) := \prod_{i\in T}(x-\alpha^i) = \frac{x^n-1}{g(x)}$. 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 $a(x)g(x)e(x) \equiv a(x)g(x) \bmod (x^n-1)$.
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. □

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
$C_i := \{i, qi \bmod n, q^2 i \bmod n, q^3 i \bmod n, \ldots\}$.
If a is an integer such that $(a,n)=1$, then μ_a denotes the permutation $i \to ai \bmod n$.

(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 μ_a interchanges S_1 and S_2.
Then $\mu_a : S_1 \rightleftarrows S_2$ is called a splitting mod n.

Let α be a primitive n-th root of unity in an extension field of GF(q), and let $\mu_a : S_1 \rightleftarrows S_2$ 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 GF(q)[x], since $g_k(x^q) = (g_k(x))^q$, k=1,2.

(2.1.2) Definition : A cyclic code of length n over 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 $(x-1)g_2(x)$.

(2.1.3) Example : Let n be an odd prime, such that $q \equiv \square \bmod n$ (i.e., there is an $x \not\equiv 0 \bmod n$, such that $q \equiv x^2 \bmod n$; if such an $x \not\equiv 0 \bmod n$ does not exist, then we write $q \equiv \not\square \bmod n$).
Now take $S_1 := \{0<i<n \mid i \equiv \square \bmod n\}$, $S_2 := \{0<i<n \mid i \equiv \not\square \bmod n\}$.
Since $q \equiv \square \bmod n$, the sets S_1 and S_2 are unions of cyclotomic cosets mod n.
Let $a \in S_2$. Then $\mu_a : S_1 \rightleftarrows S_2$ 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, Masley and Pless in [6].
Let $\mu_a : T_1 \rightleftarrows T_2$ be a splitting mod n, and define

$$e_1(x) := \sum_{i \in T_1} x^i, \quad e_2(x) := \sum_{i \in T_2} x^i \quad \text{(these are polynomials in } GF(2)[x]).$$

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

(2.1.4) Definition (Leon, Masley, 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 $1+e_2(x)$.

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

Proof : Let α be a primitive n-th root of unity in an extension field of GF(2).
(i) Let $\mu_a : S_1 \rightleftarrows S_2$ be a splitting mod n, and let C_k be the duadic code (according to (2.1.2)) with generator polynomial
$g_k(x) = \prod_{i \in S_k} (x-\alpha^i)$, k=1,2. Suppose the code C_k has idempotent

$$e_k(x) = \sum_{i \in T_k} x^i, \quad k=1,2.$$

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
$e_1(x)+e_2(x)+e_1(x)e_2(x)=1$, 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 $e_1(\alpha^{ai})\begin{cases} = 0 \text{ if } i\in S_2, \\ = 1 \text{ if } i\in\{0,1,2,\ldots,n-1\}\setminus S_2, \end{cases}$
we have $e_2(x) = e_1(x^a)$ (cf. Theorem (1.3.3)).
We have shown that $\mu_a:T_1\setminus\{0\} \rightleftarrows T_2\setminus\{0\}$ 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 $\mu_a:T_1 \rightleftarrows T_2$ be a splitting mod n, and let C_k be the duadic
code (according to (2.1.4)) with idempotent $e_k(x) = \varepsilon_0 + \sum_{i\in T_k} x^i$, k=1,2
($\varepsilon_0\in GF(2)$ 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 $\{\alpha^i \mid i\in S_k\}$, 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 $e_1(\alpha^i)+e_2(\alpha^i)=1+j(\alpha^i)=1$ $(i\neq 0)$, 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 $e_2(\alpha^{ai})=e_1(\alpha^i)=0$, so $ai\in S_2$.
It follows that $\mu_a:S_1 \rightleftarrows S_2$ 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_k' 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.

(2.1.7) 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.
A splitting mod n exists (and hence duadic codes of length n over GF(q)) iff $q \equiv \square \bmod p_i$, $i=1,2,\ldots,k$.

Before proving this theorem, we give some lemmas.

(2.1.8) Lemma : Let p be an odd prime.
A splitting mod p exists iff $q \equiv \square \bmod p$.

Proof : (i) In (2.1.3) we have seen that a splitting mod p exists if $q \equiv \square \bmod p$.
(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 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 $|H|$ element
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. $q \equiv \square \bmod p$. □

(2.1.9) Lemma : Let p be an odd prime, such that $q \equiv \square \bmod p$, 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 $\mu_a : S_1 \rightleftarrows S_2$ be a splitting mod p^m, and let $\mu_a : T_1 \rightleftarrows T_2$ be a splitting mod p (remark that both splittings are given by μ_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 $\mu_a : R_1 \rightleftarrows R_2$ is a splitting mod p^{m+1}. □

(2.1.10) Lemma : Let l and m be odd integers, $(l,m)=1$, such that splittings mod l and mod m exist.
Then there is a splitting mod lm.

Proof : Let $\mu_a:S_1 \rightleftarrows S_2$ mod l and $\mu_b:T_1 \rightleftarrows T_2$ mod m be splittings.
Define $R_k := \{im \mid i\in S_k\} \cup \{i+jm \mid i\in T_k, 0\le j<l\}$, $k=1,2$.
Choose c such that $c\equiv a$ mod l, $c\equiv b$ mod m (such a c exists by the Chinese Remainder Theorem). Note that $(c,lm)=1$.
Then $\mu_c:R_1 \rightleftarrows R_2$ is a splitting mod lm. □

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 $\mu_a:S_1 \rightleftarrows S_2$ be a splitting mod n, and let p be a prime, $p|n$.
Choose m such that $n=pm$.
Now define $T_k := \{1\le i<p \mid im\in S_k\}$, $k=1,2$. Then $\mu_a:T_1 \rightleftarrows T_2$ is a splitting mod p, and then Lemma (2.1.8) shows that $q\equiv\square$ mod p. □

(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 $p_i\equiv\pm1$ mod 8, $i=1,2,\ldots,k$.
(ii) Ternary duadic codes of length n exist iff $p_i\equiv\pm1$ mod 12, $i=1,2,\ldots,k$.
(iii) Duadic codes of length n over 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 $p\nmid q$, and let $m\ge1$. 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}. □

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 $p_1^{m_1}$, $x\equiv x_2$ mod $p_2^{m_2}$, ... , $x\equiv x_k$ mod $p_k^{m_k}$.

Then $q \equiv x^2 \bmod p_i^{m_i}$, $i=1,2,\ldots,k$, and hence $q \equiv x^2 \bmod n$.
The converse is obvious. □

(2.1.14) Corollary : Duadic codes of length n over GF(q) exist iff $q \equiv \square \bmod n$.

Section 2.2 : Examples of duadic codes

In the last section we saw that QR codes of prime length over 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 $S_1 := \{i \mid 1 \le i \le \frac{n-1}{2}\}$, $S_2 := \{i \mid \frac{n+1}{2} \le i \le n-1\}$. Then $\mu_{-1} : S_1 \rightleftarrows S_2$ is a splitting mod n. The corresponding duadic codes of length n over 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
$S_1 := \{1 \le i < n \mid c_q(i) \le \frac{m(q-1)-1}{2}\}$, $S_2 := \{1 \le i < n \mid c_q(i) \ge \frac{m(q-1)+1}{2}\}$.
Since $c_q(i) = c_q(qi \bmod n)$, the sets S_1 and S_2 are unions of cyclotomic cosets mod n.
Since $c_q(-i \bmod n) = m(q-1) - c_q(i)$, the sets S_1 and S_2 are interchanged by μ_{-1}.
Hence we have a splitting $\mu_{-1} : S_1 \rightleftarrows S_2 \bmod n$.
The corresponding duadic codes are punctured generalized Reed-Muller codes $RM(m, \frac{m(q-1)-1}{2}, q)^*$ 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 $RM(\frac{m-1}{2}, m)^*$ 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 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 μ_{-1}.

Proof : Let α 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 $0 \notin S_1$.
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 $C' \subset C^\perp$, 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 $S_2 \equiv -S_1$ mod n.
Hence $\mu_{-1} : S_1 \rightleftarrows S_2$ 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 $\mu_a : T_1 \rightleftarrows T_2$ mod l and $\mu_a : U_1 \rightleftarrows U_2$ mod m be splittings (both splittings are given by μ_a).
Let α be a primitive n-th root of unity in an extension field of GF(q), where $n := lm$.
Then $\beta := \alpha^l$ 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 $S_k := \{im | i \in T_k\} \cup \{i+jm | i \in U_k, 0 \leq j < l\}$, $k=1,2$, then we have a splitting $\mu_a : S_1 \rightleftarrows S_2$ 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 $c(x) := c_0(x^l) \in GF(q)[x]/(x^n-1)$ also has weight d.
Note that $c(\alpha^k) = c_0(\alpha^{kl}) = c_0(\beta^k)$.
Let $k \in S_1$.
(i) If $k \equiv im$ mod n, where $i \in T_1$, then $c(\alpha^k) = c_0(\beta^{im}) = c_0(1) = 0$.
(ii) If $k \equiv i+jm$ mod n, where $i \in U_1$, $0 \leq j < l$, 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 μ_a resp. μ_b give splittings mod l resp. mod m.
Choose c such that $c \equiv a$ mod l, $c \equiv b$ mod m, and continue as on page 11. □

(2.3.4) Examples : (i) Take $q=2$, n divisible by 7 (we suppose that duadic codes of length n exist).
Write $n=7^k m$, $7 \nmid m$.
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 ≤ 4.
If we apply Theorem (2.3.3) (suppose that $m>1$), we get a duadic code of length n with minimum distance ≤ 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 ≤ 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 $\mu_a : S_1 \rightleftarrows S_2$ be a splitting mod n, and let α be a primitive n-th root of unity in an extension field of GF(q).
Let C_k be the duadic code of length n over GF(q) with defining set $\{\alpha^i \mid i \in S_k\}$, and with even-like subcode C_k'. Let $e_k(x)$ be the idempotent of C_k (k=1,2).

(3.1.1) : Theorem :

(i) $\dim C_k = \frac{n+1}{2}$, $\dim C_k' = \frac{n-1}{2}$, k=1,2.

(ii) $C_1 \cap C_2 = \langle \underline{1} \rangle$, $C_1 + C_2 = (GF(q))^n$.

(iii) $C_1' \cap C_2' = \{\underline{0}\}$, $C_1' + C_2' = \{\underline{c} \in (GF(q))^n \mid \underline{c} \text{ even-like}\}$.

(iv) $C_k = C_k' \perp \langle \underline{1} \rangle$, k=1,2 ($\perp$ denotes an orthogonal direct sum).

(v) $e_1(x)e_2(x) = \frac{1}{n}j(x)$ ($\frac{1}{n}$ is the multiplicative inverse of $n = \underbrace{1+1+\ldots+1}_{n}$ in GF(q)).

(vi) $e_1(x) + e_2(x) = 1 + \frac{1}{n}j(x)$.

(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 $\{\alpha^i \mid i=1,2,\ldots,n-1\}$, which shows that $C_1 \cap C_2 = \langle \underline{1} \rangle$. From $\dim(C_1+C_2) = \dim C_1 + \dim C_2 - \dim(C_1 \cap C_2) = n$, it follows that $C_1+C_2=(GF(q))^n$. The proof of (iii) is the same.
(iv) Since C_k contains odd-like vectors, we have $\underline{1} \in C_k$, and so $C_k' + \langle \underline{1} \rangle \subset C_k$. The code C_k' contains only even-like vectors, so $C_k' \cap \langle \underline{1} \rangle = \{\underline{0}\}$. It follows that $\dim(C_k' + \langle \underline{1} \rangle) = \dim C_k$.
Since for all $\underline{c} \in C_k'$, $(\underline{c}, \underline{1}) = 0$, we have proved that $C_k' \perp \langle \underline{1} \rangle = C_k$, 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) Theorem : The codes C_k and C_k' are dual iff μ_{-1} gives the splitting (k=1,2).

Proof : Compare the defining sets of C_k' and $C_k^{\perp}$. □

(3.1.3) Theorem : The codes C_1 and C_2' are dual iff μ_{-1} leaves them invariant.

Proof : Compare the defining sets of $C_1^{\perp}$ and C_2'. □

(3.1.4) Theorem : Let $\underline{c}$ 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 μ_{-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 $d \equiv n \bmod 4$, 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 $n \equiv \pm 1 \bmod 8$ (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 $\underline{c}'$ in C_k' such that $\underline{c}=\underline{c}'+\underline{1}$ (cf. Theorem (3.1.1)(iv)). So $d=wt(\underline{c}')+wt(\underline{1})-2(\underline{c}',\underline{1}) \equiv n \bmod 4$. □

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

Section 3.2 : Splittings and the permutation μ_{-1}

In this section we investigate when a splitting is given by μ_{-1}, and also when a splitting is left invariant by μ_{-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 $ord_n(a)$ 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 $t:=\mathrm{ord}_p(a)$, $z:=v_p(a^t-1)$, i.e. $p^z \| (a^t-1)$. Then

$$\mathrm{ord}_{p^m}(a) \begin{cases} = t \text{ if } m\le z, \\ = tp^{m-z} \text{ if } m\ge z. \end{cases}$$

(3.2.3) Lemma : Let $n = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$ 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) $\mathrm{ord}_n(a) = \mathrm{lcm}(\mathrm{ord}_{p_i^{m_i}}(a))_{i=1,2,\dots,k}$,

(ii) $v_2(\mathrm{ord}_n(a)) = v_2(\mathrm{lcm}(\mathrm{ord}_{p_i}(a))_{i=1,2,\dots,k})$.

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 μ_a gives a splitting, then μ_{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 $\mu_a : S_1 \rightleftarrows S_2$ be a splitting mod n, where n=km, k>1, m>1.
Define $S(k) := \{1\le i<n \mid (i,n)=k\}$.
Since $(a,n)=1$, the permutation μ_a acts on S(k), i.e. if $i\in S(k)$, then ai mod n $\in S(k)$. So there are disjoint subsets $S_{i,m}$ of $S(k) \cap S_i$, i=1,2, with $S(k)=S_{1,m} \cup S_{2,m}$, which are interchanged by μ_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.

(3.2.6) Lemma : Let $n = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$ be the prime factorization of the odd integer n, and let $\mu_a : S_1 \rightleftarrows S_2$ be a splitting mod n. Let $r := \mathrm{ord}_n(a)$. Then the following holds:

(i) r is even,

(ii) μ_a gives the same splitting as μ_{-1} iff $r \equiv 2 \bmod 4$,

(iii) if μ_{-1} leaves the splitting invariant, then
$\mathrm{ord}_{p_i}(a) \equiv 0 \bmod 4$, $i=1,2,\dots,k$,

(iv) suppose $v_2(\mathrm{ord}_{p_i}(a))$ is the same for each i, say v, then μ_a gives the same splitting as μ_{-1} if $v=1$, and μ_{-1} leaves the splitting invariant if $v>1$.

Proof : (i) follows from Lemma (3.2.4).
(ii) Suppose $r \equiv 2 \bmod 4$, i.e. $u := \frac{r}{2}$ is odd. Let $1 \le i \le k$, $p := p_i$, $m := m_i$. Since μ_a gives the same splitting as μ_{a^u}, we see that μ_{a^u} interchanges $S_{1,p}$ and $S_{2,p}$ (using the notation of (3.2.5)), and hence $a^u \not\equiv 1 \bmod p$.
We know that $a^{2u} \equiv 1 \bmod p$, so $a^u \equiv -1 \bmod p$. Now from $a^{2u} \equiv 1 \bmod p^m$ and since p cannot divide both a^u+1 and a^u-1, it follows that $a^u \equiv -1 \bmod p^m$. Hence $a^u \equiv -1 \bmod n$, and μ_a gives the same splitting as μ_{-1}.
Conversely suppose that μ_a gives the same splitting as μ_{-1}.
Suppose $r \equiv 0 \bmod 4$.
By Lemma (3.2.3)(ii), there is an i, such that $\mathrm{ord}_p(a) = 4w$ for some w (again $p := p_i$). Now $a^{2w} \equiv -1 \bmod p$, so $\mu_{a^{2w}}$ interchanges $S_{1,p}$ and $S_{2,p}$, since μ_{-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 μ_{-1} leaves the splitting invariant.
Let $1 \le i \le k$, $p := p_i$, $s := \mathrm{ord}_p(a)$. We know that s is even, $s = 2t$. Then $a^t \equiv -1 \bmod p$, so μ_{a^t} leaves $S_{1,p}$ invariant, since μ_{-1} does. Lemma (3.2.4) shows that t is even, and hence $s \equiv 0 \bmod 4$.
(iv) Suppose $v := v_2(\mathrm{ord}_{p_i}(a))$ is the same for each i.
If $v=1$, then by Lemma (3.2.3)(ii) we have $r \equiv 2 \bmod 4$, so μ_a gives the same splitting as μ_{-1}.
Suppose $v>1$. For each i there is an odd w_i such that $\mathrm{ord}_{p_i^{m_i}}(a) = 2^v w_i$. It follows that $a^{2^{v-1} w_i} \equiv -1 \bmod p_i^{m_i}$.
Let $w := \mathrm{lcm}(w_i)_{i=1,2,\dots,k}$. Then $2^v w = \mathrm{ord}_n(a)$, and $a^{2^{v-1} w} \equiv -1 \bmod p_i^{m_i}$ for each i.
So $a^{2^{v-1} w} \equiv -1 \bmod n$. Since $2^{v-1} w$ is even, μ_{-1} leaves the splitting

invariant. □

(3.2.7) Theorem : Let $n = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$ be the prime factorization of the odd integer n, such that $q \equiv \square \bmod p_i$, $p_i \equiv -1 \bmod 4$, $i=1,2,\dots,k$.
Then all splittings mod n are given by μ_{-1}.

Proof : Let μ_a give a splitting mod n, and let $r := \mathrm{ord}_n(a)$.
By Lemma (3.2.6) it suffices to show that $r \equiv 2 \bmod 4$.
Let $1 \le i \le k$, $p := p_i$. We saw in (3.2.5) that μ_a acts like a splitting on $S(\frac{n}{p})$. Hence $s := \mathrm{ord}_p(a)$ is even, and $a^{\frac{1}{2}s} \equiv -1 \bmod p$.
Since $-1 \equiv \not\square \bmod p$, it follows that $\frac{s}{2}$ is odd.
Then Lemma (3.2.3)(ii) shows that $r \equiv 2 \bmod 4$. □

(3.2.8) Theorem : Let n be as in Theorem (3.2.7), except that at least one $p_i \equiv 1 \bmod 4$.
Then there is a splitting mod n, which is not given by μ_{-1}.

Proof : Suppose that $p_1 \equiv 1 \bmod 4$.
Let $n_i \equiv \not\square \bmod p_i$, $i=1,2,\dots,k$.
Let $a \equiv n_i \bmod p_i^{m_i}$, $i=1,2,\dots,k$ (such an a exists by the Chinese Remainder Theorem).
Suppose there is an i such that $p_i | a$. Then $n_i \equiv a \equiv 0 \bmod p_i$; but $n_i \equiv \not\square \bmod p_i$. So $(a,n)=1$.
Now consider μ_a as acting on the non-zero cyclotomic cosets mod n.
Then each orbit of μ_a has an even number of cyclotomic cosets:
Let $1 \le x < n$, b and m integers such that $a^b x \equiv q^m x \bmod n$, so we have an orbit of b cosets.
Write $x=yz$, $n=uz$, $(y,u)=1$. Then $u \ne 1$, and $(a^b - q^m)y \equiv 0 \bmod u$.
Choose i such that $p_i | u$, then $(a^b - q^m)y \equiv 0 \bmod p_i$.
Since $(y,u)=1$, we have $a^b \equiv q^m \bmod p_i$. Since $a \equiv \not\square \bmod p_i$ and $q \equiv \square \bmod p_i$, we see that b is even.

Hence there are splittings given by μ_a.
Let $\mu_a : S_1 \rightleftarrows S_2$ be such a splitting.
Then μ_a interchanges S_{1,p_1} and S_{2,p_1}. Let $k := \mathrm{ord}_{p_1}(a)$.
Then k is even, and $a^{\frac{1}{2}k} \equiv -1 \bmod p_1$. Since $-1 \equiv \square \bmod p_1$, $\frac{k}{2}$ must be even.
Hence $\mu_{-1}(S_{1,p_1}) = S_{1,p_1}$, and μ_{-1} cannot give the same splitting as μ_a. □

(3.2.9) Theorem : Let $p\equiv 1 \bmod 4$ be a prime, such that $q\equiv\Box \bmod p$, and let $m\geq 1$.
Then either a splitting mod p^m is given by μ_{-1}, or it is left invariant by μ_{-1}.

Proof : This follows from Lemma (3.2.6)(iv). $\Box$

(3.2.10) 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 $q\equiv\Box \bmod p_i$, $i=1,2,\ldots,k$. Suppose there is an integer b, such that $n \mid (q^b+1)$.
Then $p_i\equiv 1 \bmod 4$, $i=1,2,\ldots,k$, and each splitting mod n is left invariant by μ_{-1}.

Proof : Since $q^b\equiv -1 \bmod p_i$, we have $-1\equiv\Box \bmod p_i$, and hence $p_i\equiv 1 \bmod 4$. Each cyclotomic coset mod n is left invariant by μ_{-1}, so μ_{-1} leaves each splitting mod n invariant. $\Box$

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 $t:=\mathrm{ord}_p(q)$, and let z be such that $p^z \| (q^t-1)$.
Then, by Theorem (3.2.2), $\mathrm{ord}_{p^m}(q)=tp^{m-z}$ if $m\geq z$.
Let $m>z$.
Now suppose i is an integer such that $p\nmid i$, and let C_i be the cyclotomic coset mod p^m which contains i, i.e. $C_i=\{q^j i \bmod p^m \mid j\geq 0\}$.

(4.1.1) Theorem : $C_i + p^z \equiv C_i \bmod p^m$.

Proof : Let $j\geq 0$. We shall prove that $q^j i + p^z \in C_i$.
If k and k' are integers such that $q^{kt}\equiv q^{k't} \bmod p^m$,
then $q^{(k-k')t}\equiv 1 \bmod p^m$, so $tp^{m-z}|(k-k')t$. It follows that $k\equiv k' \bmod p^{m-z}$.
So the integers $q^{kt}-1$, $k=0,1,2,\dots,p^{m-z}-1$, are different mod p^m.
Now choose integers a_k, $k=0,1,2,\dots,p^{m-z}-1$, such that $q^{kt}-1=a_k p^z$.
Then a_k, $k=0,1,2,\dots,p^{m-z}-1$, are different mod p^{m-z}. Hence there is a k, such that $a_k\equiv q^{-j}i^{-1} \bmod p^{m-z}$ (q^{-j} and i^{-1} are inverses mod p^m).
Then $q^{kt}-1 = a_k p^z \equiv q^{-j}i^{-1}p^z \bmod p^m$, and hence
$q^j i + p^z \equiv q^{j+kt} i \bmod p^m$. □

(4.1.2) Corollary : If $p^{m-z}\nmid i$, then $C_i + p^{m-1} \equiv C_i \bmod p^m$.

Let $\mu_a : S_1 \rightleftarrows S_2$ be a splitting mod n, where $n:=p^m$, and let α 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 $\{\alpha^i \mid i\in S_1\}$ and with idempotent e(x).

Since $e(x^q)=(e(x))^q=e(x)$, we can write $e(x)$ as

$$e(x) = \sum_i e_i \sum_{j\in C_i} x^j \quad , \; e_i\in GF(q), \text{ where } i \text{ runs through a set of}$$

cyclotomic coset representatives.

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

Corollary (4.1.2) shows that

$$c(x) = (1-x^{p^{m-1}}) \sum_{i:p^{m-z}|i} e_i \sum_{j\in C_i} x^j \text{ . Assume w.l.o.g. that } 1\in S_1.$$

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

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

(4.1.3) <u>Theorem</u> : Let p be an odd prime, q a prime power, such that $q\equiv\square \bmod p$. Let $t:=\mathrm{ord}_p(q)$, and let z be such that $p^z \| (q^t-1)$. 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 $q\equiv\square \bmod p$. Furthermore, $t:=\mathrm{ord}_p(q)$, and we assume that $p^2\nmid(q^t-1)$.

Let $m>1$.

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

(4.2.1) <u>Lemma</u> : If $p\nmid i$, then $C_i^{(1)} \subset C_i^{(m)}$.

<u>Proof</u> : Let $j\in C_i^{(1)}$, and let k be an integer such that $j\equiv q^k i \bmod p$.

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

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-1}.

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

Then $q^{k+st}i = q^k i\,(1+a_s p) \equiv j \bmod p^m$, and hence $j\in C_i^{(m)}$. $\square$

Let $\mu_a : S_1 \rightleftarrows S_2$ be a splitting mod n, where $n := p^m$, and define $S_k' := \{i \in S_k \mid 1 \le i < p\}$, $k=1,2$.

(4.2.2) <u>Lemma</u> : $\mu_a : S_1' \rightleftarrows S_2'$ is a splitting mod p.

<u>Proof</u> : Let $i \in S_1'$. From Lemma (4.2.1) it follows that $C_i^{(1)} \subset C_i^{(m)} \subset S_1$, so $qi \bmod p \in S_1'$. Since $C_{ai}^{(1)} \subset C_{ai}^{(m)} \subset S_2$, we have $ai \bmod p \in S_2'$. □

Let α be a primitive n-th root of unity in an extension field of GF(q). Then $\beta := \alpha^{p^{m-1}}$ is a primitive p-th root of unity. We define

C as the duadic code of length n with defining set $\{\alpha^i \mid i \in S_1\}$ and minimum distance d,

C' as the duadic code of length p with defining set $\{\beta^i \mid i \in S_1'\}$ and minimum distance d',

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

(4.2.3) <u>Theorem</u> : We have $d' \le d \le d''$.

<u>Proof</u> : 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)

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

c(x) has (possibly) non-zeros only on positions $\equiv 0 \bmod p^{m-1}$.
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 $d \le d''$.
Since $c^*(\beta^i) = c^*(\alpha^{ip^{m-1}}) = c(\alpha^i) = (1-\alpha^{ip^{m-1}})e(\alpha^i) \begin{cases} =0 & \text{if } i \in S_1' \cup \{0\}, \\ \ne 0 & \text{if } i \in S_2', \end{cases}$

we have $C^* \subset C''$.

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 $g(y)\equiv a(y)c^*(y) \bmod (y^p-1)$, and hence $C'' \subset C^*$.

(ii) Let $C_0 := \{(c_0,c_{p^{m-1}},c_{2p^{m-1}},\dots,c_{(p-1)p^{m-1}}) \mid (c_0,c_1,\dots,c_{n-1})\in C\}$.

If we show that $C_0 = C'$, then we have proved that $d'\le d$.
We know that $C_i + p^{m-1} \equiv C_i \bmod p^m$ if $p^{m-1}\nmid i$ (cf. Theorem (4.1.2)).
It follows that the idempotent $e(x)$ of C looks like $(r:=p^{m-1})$

position:	0	1 2 3...(r−1)	r	(r+1)...(2r−1)	2r	...	(p−1)r	(p−1)r+1...(n−
e(x) :	$*$	$\underline{c}$	$*$	$\underline{c}$	$*$		$*$	$\underline{c}$

where the $*$'s are elements of $GF(q)$.

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

Again define $y:=x^{p^{m-1}}$, $e^*(y):=e'(x) \in GF(q)[y]/(y^p-1)$.
Since $e^*(\beta^k) = e'(\alpha^k) = e(\alpha^k)\begin{cases} = 0 \text{ if } k\in S_1', \\ = 1 \text{ if } k\in S_2' \cup \{0\}, \end{cases}$
the polynomial $e^*(y)$ is the idempotent of C' (cf. Theorem (1.3.3)).
Hence $C' \subset C_0$.
Now consider $x^k e(x)$ on the positions $\equiv 0 \bmod p^{m-1}$, call this vector $\underline{c}_k$ ($\underline{c}_k$ has length p):
a) if $k\not\equiv 0 \bmod p^{m-1}$, then $\underline{c}_k \in \langle\underline{1}\rangle$,
b) if $k=bp^{m-1}$ for some $0\le b<p$, then $\underline{c}_k = y^k e^*(y) \in C'$.
Since the code C_0 is generated by the vectors $\underline{c}_k$, $k=0,1,2,\dots,n-1$, we have proved that $C_0 \subset \langle C',\underline{1}\rangle = C'$. □

Section 4.3 : Examples

(4.3.1) Theorem : Let $p\equiv\pm 1 \bmod 8$ be a prime, such that $\mathrm{ord}_p(2)=\frac{p-1}{2}$, and suppose that $p^2 \nmid (2^{\frac{1}{2}(p-1)}-1)$.
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 $p^2 \nmid (2^t-1)$, where $t=\mathrm{ord}_p(2)$. This condition is very weak: There are just two primes $p < 6.10^9$, such that $2^{p-1}\equiv 1 \bmod p^2$:
$p=1093$, $t=364$, $2^t\equiv 1 \bmod p^2$, $2^t\equiv 1064432260 \bmod p^3$,
and
$p=3511$, $t=1755$, $2^t\equiv 1 \bmod p^2$, $2^t\equiv 21954602502 \bmod p^3$
(cf. [15]).

(4.3.4) Take q=4. Let n be an odd integer, such that $\mathrm{ord}_n(2)$ is odd. Then binary and quaternary cyclotomic cosets mod n are equal, i.e. $\{2^j i \bmod n \mid j\geq 0\} = \{4^j i \bmod n \mid j\geq 0\}$ 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).

(4.3.5) 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). □

(4.3.6) 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 μ_{-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 $n \equiv 3 \bmod 4$.
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 x n matrix A by

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

This matrix is called the adjacency matrix of the tournament.
From the definition of a tournament it follows that

(5.1.1) $A + A^T + I = J$.

(5.1.2) Lemma : If the tournament is regular, then

(i) $AJ = JA = \frac{n-1}{2} J$,

(ii) $A^T A = AA^T$.

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 $\mu_{-1}:S_1 \overset{\rightarrow}{\leftarrow} S_2$ be a splitting mod n (S_1 and S_2 are unions of cyclotomic cosets $\{i,qi,q^2i,\ldots\}$ mod n).
Now define the directed graph T on the vertices $\{0,1,2,\ldots,n-1\}$ as follows:

i dominates j iff $(j-i) \bmod n \in S_1$.

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 $p \equiv 3 \bmod 4$ be a prime, and let q be a prime power such that $q \equiv \square \bmod p$.
Let $S_1 := \{1 \le i < p \mid i \equiv \square \bmod p\}$, $S_2 := \{i \le i < p \mid i \equiv \not\square \bmod p\}$.
Then $\mu_{-1}:S_1 \overset{\rightarrow}{\leftarrow} S_2$ is a splitting mod p. Let A be the adjacency matrix of the corresponding tournament.
The n x 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 $A = \frac{1}{2}(S + J - I)$, it follows that $AA^T = \frac{p+1}{4} I + \frac{p-3}{4} J$, and hence the splitting $\mu_{-1}: S_1 \rightleftarrows S_2$ is doubly-regular.
I have not been able to find any other doubly-regular splittings.

(5.2.2) Theorem : A splitting $\mu_{-1}: S_1 \rightleftarrows S_2$ mod n is doubly-regular iff $|S_1 \cap (S_1+k)| = \frac{n-3}{4}$, $k=1,2,\dots,n-1$.

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 $q \equiv \square$ mod p, z an integer such that $p^z \| (q^t-1)$, where $t = \mathrm{ord}_p(q)$. Let $m > z$. Then there is no doubly-regular splitting mod p^m.

Proof : Let $\mu_{-1}: S_1 \rightleftarrows S_2$ be a splitting mod p^m, and define $T_1 := \{i \in S_1 \mid i \equiv 0 \bmod p^{m-z}\}$, $S_1' := S_1 \setminus T_1$.
From Corollary (4.1.2) it follows that $S_1' + p^{m-1} \equiv S_1'$ mod p^m.
Therefore $|S_1 \cap (S_1 + p^{m-1})| \geq |S_1'| = |S_1| - |T_1| = \frac{p^m-1}{2} - \frac{p^z-1}{2} >$
$> \frac{p^m-3}{4}$. 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 $\underline{c}$ is a vector, then the set $\{i \mid c_i \neq 0\}$ is called the support of $\underline{c}$. Now if a code contains codewords such that their supports are the lines of a projective plane Π, then we say that the code contains Π.

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 μ_{-1}.
Let $c(x) = \sum_{i=1}^{d} c_i x^{e_i}$ 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 $\mathbb{Z}$ mod n.
Now call the elements of $\mathbb{Z}$ 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 x 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 $c_r c_s$. 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 $s\equiv 2 \bmod 4$, 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 $(n^2+n+1)x(n^2+n+1)$ matrix A, which has as its rows the characteristic vectors of the lines of the plane.
Let p be a prime such that $p\| n$, 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 μ_{-1}.

Proof : Let α 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 $\{\alpha^{-i} | i\in S_2 \cup \{0\}\}$, 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 $\mu_{-1}:S_1 \rightleftarrows S_2$ 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 $\underline{c}$ be a row of the matrix A (so $\underline{c}$ is a codeword in C).
Since $\Sigma c_i = n+1 \equiv 1 \mod p$, we have $(\underline{c},-1) \in \overline{C}$.
Now $(\underline{c},-1)$ has inner-product 0 with itself, so $n+1+1\equiv 2\equiv 0 \mod p$.
Hence p=2. □

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

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

(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 $p \mid n$, $r \mid (n^2+n+1)$, $p \equiv \not\square \mod r$. 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 $\mu_{-1}: S_1 \rightleftarrows S_2 \mod 157$, where S_1 and S_2 are unions of cyclotomic cosets $\{i,3i,3^2i,\ldots\} \mod 157$. But $3^{39}\equiv -1 \mod 157$, so all cyclotomic cosets mod 157 are left invariant by μ_{-1}. Hence a splitting mod 157 cannot be given by μ_{-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 α be a primitive n-th root of unity, and suppose w.l.o.g. that α is in the complete defining set of C. Then the nonzero even-weight vectors in C have $\alpha^0,\alpha^1,\alpha^2$ 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 $n\equiv 0 \bmod 7$.

Proof : Let $c(x)=1+x^i+x^j+x^k$ be a codeword in C of weight 4, and let α be a primitive n-th root of unity such that $c(\alpha)=0$.
If $i+j\equiv k \bmod n$, then $c(\alpha)=(1+\alpha^i)(1+\alpha^j)=0$, so $\alpha^i=1$ or $\alpha^j=1$, which is impossible. Hence

$$i+j\not\equiv k,\ j+k\not\equiv i,\ k+i\not\equiv j \bmod n. \qquad (*)$$

Suppose the splitting is given by μ_a. Then $c(x^{-a})=1+x^{-ai}+x^{-aj}+x^{-ak}$ is a codeword in $C^{\perp}$.
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 $ai\equiv -i \bmod n$.
The vectors $c(x)=1+x^i+x^j+x^k$ and $x^i c(x^{-a})=x^i+x^{2i}+x^{i-aj}+x^{i-ak}$ have inner-product 0, so $\{0,j,k\} \cap \{2i,i-aj,i-ak\} \neq \emptyset$.

Now suppose e.g. that $i\equiv aj \bmod n$, then $i\equiv -j \bmod n$.
Since $c(x)$ and $c(x^{-a})$ have inner-product 0, we have $ak\equiv -k \bmod n$.
Also $c(x)$ and $x^{2i}c(x^{-a})$ have inner-product 0, so
$\{0,-i,k\} \cap \{2i,3i,k+2i\} \neq \emptyset$. Note that $2i\not\equiv 0$, $3i\not\equiv 0 \bmod n$.
Because of $(*)$ there are two possibilities:
(i) $-i\equiv k+2i \bmod n$: Then $c(x)=1+x^{i}+x^{-i}+x^{-3i}$ and $x^{3i}c(x^{-a})=x^{3i}+x^{4i}+x^{2i}+1$ 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 $7i\equiv 0 \bmod n$, so $n\equiv 0 \bmod 7$.
(ii) $k\equiv 3i \bmod n$: In the same way, $c(x)$ and $x^{3i}c(x^{-a})$ have inner-product 0, so $\{0,i,-i\} \cap \{2i,4i,6i\} \neq \emptyset$. Hence $7i\equiv 0 \bmod n$, $n\equiv 0 \bmod 7$. □

(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 $n\equiv 0 \bmod 7$.

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, $p|n$. Then $2^{m-1}.2\equiv 1 \bmod p$, so $2\equiv\Box \bmod p$.
(ii) If m is even, then $3|n$, but $2\equiv\not\Box \bmod 3$. □

(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 μ_3.
Then $n\equiv 0 \bmod 7$.

Proof : Let $c(x)=1+x^{i}+x^{j}+x^{k}$ be a codeword of weight 4, and let α 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 $\xi:=\alpha^{b}$, $\eta:=\alpha^{b+j}$. Then $\alpha^{b+i}=\xi+1$ and $\alpha^{b+k}=\eta+1$.
The codeword $x^{b}c(x)$ has α^{9} as a zero, so $\xi^{9}+(\xi+1)^{9}+\eta^{9}+(\eta+1)^{9}=0$.
It follows that $(\xi+\eta)^{8}=\xi+\eta$. Since $\xi+\eta\neq 0$, 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 μ_{-1}.
Then $n\equiv 0 \bmod 7$.

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

$$i+j\not\equiv k,\ j+k\not\equiv i,\ k+i\not\equiv j \mod n. \qquad (*)$$

By Theorem (3.1.4), all even weights in C are divisible by 4. Hence $(1+x^i)c(x)=1+x^j+x^k+x^{2i}+x^{i+j}+x^{i+k}$ is a codeword of weight 4.
So $|\{0,j,k,2i,i+j,i+k\}|=4$. Because of $(*)$ there are 4 possibilities:
(i) $j\equiv 2i \mod n$: $(1+x^{2i})c(x)=1+x^i+x^k+x^{3i}+x^{4i}+x^{k+2i}$ is a codeword of weight 4, so $|\{0,i,k,3i,4i,k+2i\}|=4$.
Again because of $(*)$, we have two possibilities:

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

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

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

(7.1.6) Remark : From the above proof it follows that the codeword $c(x)$ is one of the following:
$1+x^i+x^{2i}+x^{4i}$, $1+x^i+x^{2i}+x^{-2i}$, $1+x^i+x^{-i}+x^{3i}$, $1+x^i+x^{-i}+x^{-3i}$, 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 μ_{-1}. Then C contains exactly n codewords of weight 4.

Proof : Let $c(x)$ be a codeword of weight 4, w.l.o.g. $c(x)=1+x^i+x^{2i}+x^{4i}$, 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) $d(x)=1+x^j+x^{2j}+x^{4j}$, $7j\equiv 0 \mod n$:
$c(x)+d(x)=x^i+x^{2i}+x^{4i}+x^j+x^{2j}+x^{4j}$ 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) $d(x)=1+x^{j}+x^{2j}+x^{-2j}$, $7j\equiv 0 \bmod n$:
Now we find $\{i,2i,4i\} \cap \{j,2j,-2j\} \neq \emptyset$.
If $i\equiv j$, then $c(x)+d(x)=x^{4i}+x^{-2i}$ has weight 0, so $6i\equiv 0 \bmod n$.
A contradiction.
If $i\equiv 2j$, then $c(x)+d(x)=x^{4j}+x^{-2j}$, so $6j\equiv 0 \bmod n$. A contradiction.
If $i\equiv -2j$, then $x^{2j}c(x)=d(x)$.
If $2i\equiv j$, then $c(x)+d(x)=x^{i}+x^{-4i}$, so $5i\equiv 0 \bmod n$. A contradiction.
If $2i\equiv 2j$, then $i\equiv j \bmod n$, a contradiction.
If $2i\equiv -2j$, then $x^{2i}d(x)=c(x)$.
If $4i\equiv j$, then $c(x)+d(x)=x^{2i}+x^{-i}$, so $3i\equiv 0 \bmod n$. A contradiction.
If $4i\equiv 2j$, then $2i\equiv j$, a contradiction.
If $4i\equiv -2j$, then $x^{4i}d(x)=c(x)$.

(iii) $d(x)=1+x^{j}+x^{-j}+x^{3j}$, $7j\equiv 0 \bmod n$:
Consider $x^{j}d(x)=1+x^{j}+x^{2j}+x^{4j}$, i.e. case (i).

(iv) $d(x)=1+x^{j}+x^{-j}+x^{-3j}$, $7j\equiv 0 \bmod n$:
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 μ_{-1}. It turns out that most patterns of two errors can be corrected.

Let $\mu_{-1}:S_1 \rightleftarrows S_2$ 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 $c_2(x)=1+x^{i}+x^{2i}+x^{4i}$ ($7i\equiv 0 \bmod n$) be a codeword in C_2 of weight 4 (cf.(7.1.6)).

(7.2.1) <u>Lemma</u> : Let $c(x)$ be a polynomial of weight 4.
Then $c(x)\in C_1$ iff $c(x)c_2(x)\equiv 0 \bmod (x^{n}-1)$.

<u>Proof</u> : (i) Let $c(x)\in C_1$. Then $c(x)c_2(x)\in C_1 \cap C_2 = \{\underline{0},\underline{1}\}$.
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) $k+i\equiv 0 \bmod n$: It turns out that $c(x)=1+x^{6i}+x^{i}+x^{4i}=x^i c_2(x^{-1}) \in C_1$, or $c(x)=1+x^{6i}+x^{5i}+x^{3i}=c_2(x^{-1}) \in C_1$.

b) $k+2i\equiv 0 \bmod n$: In the same way we find
$c(x)=1+x^{5i}+x^{i}+x^{2i}=x^{2i}c_2(x^{-1}) \in C_1$,
or $c(x)=1+x^{5i}+x^{6i}+x^{3i}=c_2(x^{-1}) \in C_1$.

c) $k+4i\equiv 0 \bmod n$: Here we get $c(x)=1+x^{3i}+x^{6i}+x^{5i}=c_2(x^{-1}) \in C_1$, or
$c(x)=1+x^{3i}+x^{4i}+x^{2i}=x^{4i}c_2(x^{-1}) \in C_1$. □

(7.2.2) <u>Theorem</u> : Let $e(x)=x^j+x^k$ be a polynomial of weight 2.
Suppose that for all $h=0,1,2,\dots,n-1$, we have
$\{j,k\} \not\subset \{h,h+3i,h+5i,h+6i\} \bmod n$.
Then the polynomial $e(x)c_2(x) \bmod (x^n-1)$ uniquely determines the exponents j and k.

<u>Proof</u> : Suppose $(x^j+x^k)c_2(x)=(x^l+x^m)c_2(x)$, $l\neq m$.

(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 $x^j+x^k+x^l+x^m \in C_1$. Since the only codewords of weight 4 in 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. □

Now error-correction goes as follows.
Let $c_1(x)\in C_1$ 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 $C_1 \cap C_2 = \{\underline{0},\underline{1}\}$, 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 $\binom{4}{2}.n$ 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≡0 mod 3.

Proof : Suppose n≥11. Let $GF(4)=\{0,1,\omega,\omega^2\}$, $\omega^2+\omega=1$.
Let $c(x)=1+c_ix^i+c_jx^j$ 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 μ_a. Then $c(x^{-a})$ is a codeword in $C^\perp$.
So c(x) and $c(x^{-a})$ have inner-product 0.
Therefore $\{i,j\} \cap \{-ai,-aj\} \neq \emptyset$. We consider all possibilities.
(i) ai≡-i mod n: Since c(x) and $c(x^{-a})$ have inner-product 0, we have aj≡-j mod n.
Also c(x) and $x^ic(x^{-a})$ have inner-product 0, so $\{0,j\} \cap \{2i,i+j\} \neq \emptyset$.
There are two possible cases:
a) 2i≡j mod n: c(x) and $x^ic(x^{-a})$ have inner-product 0, so 3i≡0 mod n, and hence n≡0 mod 3.
b) i+j≡0 mod n: In the same way we find 3i≡0 mod n.

(ii) aj≡-j mod n: In the same way we find n≡0 mod 3.

(iii) ai≡-j mod n: Since c(x) and $x^{ai}c(x^{-a})$ have inner-product 0, we have $\{i,-ai\} \cap \{ai,ai+a^2i\} \neq \emptyset$.
a) $ai+a^2i\equiv i$ mod 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≡2ai mod n: $\left.\begin{array}{l} ai+a^2i\equiv 3a^2i \\ i\equiv 2ai\equiv 4a^2i \end{array}\right\}$ so $a^2i\equiv 0$ mod n, a contradiction.
2) i≡-2ai mod n: Let α be a primitive n-th root of unity such

that $c(\alpha^a)=0$, so $1+\omega\alpha^{ai}+\omega^2\alpha^{aj}=0$.

Take the square: $1+\omega^2\alpha^{2ai}+\omega\alpha^{ai}=0$ $(2aj\equiv ai \bmod n)$.

Add these two relations: $\alpha^{aj}=\alpha^{2ai}$, so $j\equiv 2i \bmod n$.

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

b) $ai\equiv -2i \bmod n$: $c(\alpha^a)=1+\omega\alpha^{ai}+\omega^2\alpha^{2ai}=0$, and

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

If we add these equations, then we find $3i\equiv 0 \bmod n$.

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

Contradiction.

(iv) $aj\equiv -i \bmod n$: 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 $n\equiv 0 \bmod 3$.

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 α be a primitive n-th root of unity in an extension field of GF(q). The set $A=\{\alpha^{i_1},\alpha^{i_2},\ldots,\alpha^{i_m}\}$ is called a consecutive set of length m , if there is a primitive n-th root of unity β, 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 β be a primitive n-th root of unity, and suppose that A contains the consecutive sets $\{\beta^{i+ja},\beta^{i+1+ja},\ldots,\beta^{i+\delta-2+ja}\}$, $0\leq j\leq s$, where $(a,n)<\delta$.
Then $d\geq\delta+s$.

(8.1.3) Examples : (i) q=2, n=73. Let α 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. $\{\alpha^i \mid i\in C_3\cup C_9\cup C_{11}\cup C_{17}\}$, contains $\{\beta^i \mid 1\leq i\leq 8\}$, where $\beta:=\alpha^3$.
So by the BCH bound, the code C has minimum distance ≥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 α is a primitive n-th root of unity). The complete defining set of the even-weight subcode contains $\{\alpha^i \mid i=3,12,21,30,39,48,57,66,75,84,93\}\cup$
$\{\alpha^i \mid i=37,46,55,64,73,82,91,100,109,118,0\}$.
Then the HT bound shows that the even-weight subcode of C has minimum distance ≥13, hence ≥14. Since the splitting is given by μ_{-1}, Theorem (3.1.4) shows that C has minimum distance ≥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 $wt(c(x)) \geq |A|$.

(8.1.6) Example : q=2, n=73. Let α 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 $wt(c(x)) \geq 9$, 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 $\{\alpha^i | i \in C_3 \cup C_9\} \cap S = \emptyset$.
The following sets are independent w.r.t. S:
$\emptyset$, $\{\alpha^{65}\}$, $\{\alpha^{64}\}$, $\{\alpha^{64},\alpha^{65}\}$, $\{\alpha^{61}, \alpha^{62}\}$, $\{\alpha^{61},\alpha^{62},\alpha^{65}\}$, $\{\alpha^0,\alpha^1,\alpha^4,\alpha^{12}\}$,
$\{\alpha^{63},\alpha^{64},\alpha^{65},\alpha^{67},\alpha^2\}$, $\{\alpha^{48},\alpha^{49},\alpha^{50},\alpha^{51},\alpha^{53},\alpha^{61}\}$,
$\{\alpha^{32},\alpha^{33},\alpha^{34},\alpha^{35},\alpha^{37},\alpha^{45},\alpha^{46}\}$, $\{\alpha^{61},\alpha^{62},\alpha^{63},\alpha^{64},\alpha^{65},\alpha^{66},\alpha^1,\alpha^2\}$,
$\{\alpha^{50},\alpha^{51},\alpha^{52},\alpha^{53},\alpha^{54},\alpha^{55},\alpha^{63},\alpha^{64},\alpha^3\}$.
Then Theorem (8.1.5) shows that $wt(c(x)) \geq 9$, 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, α is a primitive n-th root of unity, A is a defining set for the binary duadic code C, μ_a gives the splitting, d is the minimum distance of C, and d_0 is the minimum odd weight of C.

(8.2.1) $n=89$, $A=\{\alpha^i \mid i=1,9,13,33\}$, μ_{-1}.
Since the complete defining set contains $\{\alpha^i \mid i=15,30,45,60,75,1,16,31\}$, we have $d\geq 9$. Then Theorem (3.1.4) gives $d\geq 12$.

(8.2.2) $n=89$, $A=\{\alpha^i \mid i=3,9,11,19\}$, μ_{-1}.
The code has zeros α^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) $n=119$, $A=\{\alpha^i \mid i=3,7,13,51\}$, μ_3.
The complete defining set contains $\{\alpha^i \mid 101\leq i\leq 105\}$, so $d\geq 6$.
Let $c(x)$ be a codeword of weight 6 with zero-set S.
Then $c(\alpha)\neq 0$, since otherwise $c(\alpha^i)=0$, $i=117,118,0,1,2,\ldots,10$.
Also $c(\alpha^{11})\neq 0$ since otherwise $c(\alpha^i)=0$, $i=107,108,\ldots,117,118,0$.
The following sets are independent w.r.t. S (we only give the exponents of α):
$\emptyset$, $\{4\}$, $\{4,5\}$, $\{4,5,6\}$, $\{95,101,102,103\}$, $\{96,100,102,103,104\}$, $\{104,108,109,110,111,112\}$, $\{97,101,102,103,104,105,1\}$.
So $wt(c(x))\geq 7$, a contradiction. Hence $d\geq 7$. Then Theorem (3.1.4) gives $d\geq 8$.

(8.2.4) Notation : We introduce a notation to abbreviate a sequence of independent sets.
The string $(\underline{a}_0, s_0, \underline{a}_1, s_1, \underline{a}_2, s_2, \ldots)$ has to be interpreted as the following sequence of sets:

$$\emptyset,\ \{\alpha^{a_0}\},\ \{\alpha^{a_0+s_0}\},\ \{\alpha^{a_0+s_0}, \alpha^{a_1}\},\ \{\alpha^{a_0+s_0+s_1}, \alpha^{a_1+s_1}\},$$

$$\{\alpha^{a_0+s_0+s_1}, \alpha^{a_1+s_1}, \alpha^{a_2}\},\ \{\alpha^{a_0+s_0+s_1+s_2}, \alpha^{a_1+s_1+s_2}, \alpha^{a_2+s_2}\}, \ldots$$

As an example, the sequence of independent sets in (8.2.3) is abbreviated as $(\underline{4}, 1, \underline{4}, 1, \underline{4}, 97, \underline{95}, 1, \underline{100}, 8, \underline{109}, -7, \underline{1})$.

(8.2.5) $n=127$, $A=\{\alpha^i \mid i=3,5,7,11,19,21,23,55,63\}$, μ_{-1}.
The code has zeros α^{19i}, $1 \le i \le 12$, so $d \ge 13$.
Theorem (3.1.4) gives $d \ge 15$.

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

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

(8.2.8) $n=127$, $A=\{\alpha^i \mid i=9,11,13,15,19,31,43,47\ 63\}$, μ_{-1}.
The code has zeros α^{90+25i}, $0 \le i \le 13$, so $d \ge 15$.

(8.2.9) $n=127$, $A=\{\alpha^i \mid i=3,7,9,13,19,21,29,47,63\}$, μ_{-1}.
The code has zeros $\alpha^{100+11i}$, $0\le i\le 13$, so $d\ge 15$.

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

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

(8.2.12) $n=127$, $A=\{\alpha^i \mid i=1,5,13,15,27,29,31,43,55\}$, μ_{-1}.
The code has zeros α^{54i}, $1\le i\le 12$, so $d\ge 13$. Hence by Theorem (3.1.4), $d\ge 15$.

(8.2.13) $n=127$, $A=\{\alpha^i \mid i=1,3,7,19,23,29,43,47,55\}$, μ_{-1}.
We know that $d_0\ge 15$. Let $c(x)$ be a codeword of even weight ≤ 12 with zero-set S.

(i) $c(\alpha^{15})\neq 0$, since otherwise $c(\alpha^{97+15i})=0$, $0\le i\le 14$.

(ii) Suppose $c(\alpha^5)=0$. Then $c(\alpha^{13})\neq 0$, since otherwise $c(\alpha^{57+35i})=0$, $0\le i\le 14$. The following sets are independent w.r.t. S:
$(\underline{60},-21,\underline{60},-10,\underline{60},30,\underline{60},-40,\underline{30},36,\underline{35},-10,\underline{35},30,\underline{35},-10,\underline{35},51,$ $\underline{30},-10,\underline{30},-10,\underline{30},-10,\underline{30})$, so $wt(c(x))\ge 13$.
Hence $c(\alpha^5)\neq 0$.

(iii) $c(\alpha^{27})\neq 0$, since otherwise we have the following independent sets w.r.t. S:

$(\underline{15},1,\underline{15},71,\underline{13},19,\underline{30},-16,\underline{15},-12,\underline{113},-74,\underline{5},-1,\underline{40},21,\underline{26},33,\underline{60},$
$-1,\underline{60},-1,\underline{60},-1,\underline{60})$ so $wt(c(x))\geq 13$.

(iv) $c(\alpha^{11})\neq 0$, since otherwise we have the following independent sets w.r.t. S:

$(\underline{5},-1,\underline{5},-2,\underline{5},41,\underline{89},50,\underline{104},-8,\underline{5},-74,\underline{10},-8,\underline{5},-2,\underline{13},46,\underline{51},-1,\underline{51},$
$-1,\underline{51},-1,\underline{51})$.

The following sets are independent w.r.t. S:
$(\underline{5},-5,\underline{44},3,\underline{5},1,\underline{99},19,\underline{60},-17,\underline{33},84,\underline{89},-44,\underline{51},2,\underline{49},-46,\underline{5},89,\underline{113},-35,$
$\underline{15},-55,\underline{15})$, so $wt(c(x))\geq 13$, a contradiction.
We have proved that $d\geq 14$. Then Theorem (3.1.4) shows that $d\geq 15$.

(8.2.14) $n=127$, $A=\{\alpha^i \mid i=3,15,19,21,23,29,47,55,63\}$, μ_{-1}.
The code has zeros α^{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) $c(\alpha^{27})\neq 0$, since otherwise $c(\alpha^{93+3i})=0$, $0\leq i\leq 11$.
(ii) $c(\alpha^{31})\neq 0$, since otherwise $c(\alpha^{i})=0$, $113\leq i\leq 127$.
(iii) Suppose $c(\alpha^7)=0$.

a) $c(\alpha)\neq 0$, since otherwise $c(\alpha^{19+9i})=0$, $0\leq i\leq 12$.

b) $c(\alpha^5)\neq 0$, since otherwise we have the following independent sets w.r.t. S:

$(\underline{1},64,\underline{1},-9,\underline{1},-1,\underline{64},-9,\underline{64},1,\ \underline{1},-9,\underline{1},-1,\underline{64},-9,\underline{64},1,\underline{1},-9,\underline{1},$
$-1,\underline{64},-9,\underline{1})$.

The following sets are independent w.r.t. S:
$(\underline{1},-1,\underline{1},-1,\underline{1},95,\underline{40},1,\underline{103},-4,\underline{40},34,\underline{5},-16,\underline{108},-17,\underline{40},20,\underline{115},-1,$
$\underline{115},-1,\underline{108},-17,\underline{108})$, so $wt(c(x))\geq 13$, a contradiction.
Hence $c(\alpha^7)\neq 0$.

(iv) Suppose $c(\alpha)=0$. Then $c(\alpha^9)\neq 0$, since otherwise $c(\alpha^{37+9i})=0$, $0\leq i\leq 12$.
The following sets are independent w.r.t. S:
$(\underline{56},-10,\underline{56},19,\underline{56},9,\underline{56},44,\underline{9},-9,\underline{9},-9,\underline{9},-9,\underline{9},-9,\underline{9},-9,\underline{9},-9,\underline{9},-9,$
$\underline{9},-8,\underline{9})$. So $c(\alpha)\neq 0$.

The following sets are independent w.r.t. S:
$(\underline{1},81,\underline{108},2,\underline{102},-81,\underline{121},9,\underline{121},12,\underline{97},76,\underline{108},1,\underline{1},-8,\underline{102},-1,\underline{1},-71,\underline{1},$
$70,\underline{1},-8,\underline{1})$, so $wt(c(x))\geq 13$, a contradiction. Hence $d\geq 13$.
Then Theorem (3.1.4) gives $d\geq 15$.

(8.2.15) $n=127$, $A=\{\alpha^i \mid i=3,5,9,13,15,19,21,29,63\}$, μ_{-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:
$(\underline{31},-5,\underline{121},24,\underline{124},-29,\underline{115},45,\underline{31},50,\underline{79},-3,\underline{79},-8,\underline{115},-31,\underline{22},-1,\underline{22},-1,$
$\underline{22},-1,\underline{22},-1,\underline{22})$, so $wt(c(x))\geq 13$.
We have proved that $d\geq 13$, and hence $d\geq 15$.

(8.2.16) $n=127$, $A=\{\alpha^i \mid i=1,3,5,9,15,23,27,29,43\}$, μ_{-1}.
The code has zeros α^{57+7i}, $0\leq i\leq 9$, 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:
$(\underline{21},-21,\underline{21},24,\underline{21},-21,\underline{21},24,\underline{21},-21,\underline{21},24,\underline{21},-21,\underline{21},24,\underline{21},-21,\underline{21},24,\underline{21},$
$-21,\underline{21},3,\underline{21})$, a contradiction.
Then, by Theorem (3.1.4), $d\geq 15$.

(8.2.17) $n=127$, $A=\{\alpha^i \mid i=5,7,9,13,19,29,31,43,63\}$, μ_{-1}.
Let $c(x)$ be a codeword of even weight ≤ 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 $c(x)$:
$(\underline{3},17,\underline{87},16,\underline{61},-22,\underline{59},-1,\underline{96},-13,\underline{46},-11,\underline{55},-46,\underline{117},-12,\underline{84},42,\underline{55},-20,$
$\underline{21},-1,\underline{21},-1,\underline{21})$, so $wt(c(x))\geq 13$.
Hence, by Theorem (3.1.4), $d\geq 15$.

(8.2.18) $n=127$, $A=\{\alpha^i \mid i=3,11,15,19,23,43,47,55,63\}$, μ_{-1}.
The code has zeros α^i, $43\leq i\leq 50$, so $d\geq 9$, and hence $d\geq 12$.
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:
$(\underline{77},-29,\underline{102},7,\underline{108},14,\underline{42},-4,\underline{33},-8,\underline{31},-19,\underline{14},-16,\underline{77},-27,\underline{51},-2,\underline{51},-1,$
$\underline{51},-1,\underline{51},-1,\underline{51})$, a contradiction.
So $d\geq 15$, by Theorem (3.1.4).

(8.2.19) $n=127$, $A=\{\alpha^i \mid i=9,13,15,19,21,29,31,47,63\}$, μ_{-1}.
The code has zeros α^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 $c(\alpha^i)\neq 0$, $i=5,11,27$.
The following sets are independent w.r.t. S:
$(\underline{77},38,\underline{80},47,\underline{88},-4,\underline{80},-6,\underline{77},-6,\underline{69},-30,\underline{40},-3,\underline{77},-39,\underline{40},-1,\underline{20},-1,$
$\underline{20},-1,\underline{20},-1,\underline{20})$, a contradiction. Hence $d\geq 15$.

(8.2.20) $n=127$, $A=\{\alpha^i \mid i=1,3,5,9,11,15,21,23,27\}$, μ_{-1}.
The code has zeros α^{3i}, $1\leq i\leq 12$, so $d\geq 13$.
Then Theorem (3.1.4) gives $d\geq 15$.

(8.2.21) $n=127$, $A=\{\alpha^i \mid i=3,9,15,23,27,29,43,47,63\}$, μ_{-1}.
The code has zeros α^{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, $c(\alpha^i)\neq 0$, $i=1,7,21,55$. The following sets are independent w.r.t. S:
$(\underline{2},-3,\underline{2},-3,\underline{2},16,\underline{1},84,\underline{37},-10,\underline{56},-3,\underline{56},-26,\underline{1},-3,\underline{110},-9,\underline{42},-53,\underline{2},-2,$
$\underline{1},-1,\underline{1})$, a contradiction. Hence $d\geq 15$.

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

(8.2.23) $n=127$, $A=\{\alpha^i \mid i=5,7,11,13,27,31,43,55,63\}$, μ_{-1}.
The code has zeros α^{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, $c(\alpha^i)\neq 0$, $i=3,9,21$.
The following sets are independent w.r.t. the zero-set of $c(x)$:
$(\underline{9},26,\underline{9},-2,\underline{42},7,\underline{84},-18,\underline{96},-11,\underline{41},-6,\underline{36},-9,\underline{6},-30,\underline{12},-5,\underline{6},-7,\underline{12},-1,$
$\underline{12},-1,\underline{12})$, a contradiction. So $d\geq 15$.

(8.2.24) $n=127$, $A=\{\alpha^i \mid i=1,3,5,11,15,19,23,43,55\}$, μ_{-1}.
We know that $d_0\geq 15$. Let $c(x)$ be a codeword of even weight ≤ 12 with zero-set S. By computer, $c(\alpha^i)\neq 0$, $i=7,13,63$.
The following sets are independent w.r.t. S:
$(\underline{26},-1,\underline{26},-20,\underline{26},-1,\underline{52},28,\underline{119},-31,\underline{95},-19,\underline{67},-10,\underline{56},-34,\underline{70},-17,\underline{7},-3,$
$\underline{7},-1,\underline{7},-1,\underline{7})$, so $wt(c(x))\geq 13$, a contradiction.
Hence, by Theorem (3.1.4), $d\geq 15$.

(8.2.25) $n=127$, $A=\{\alpha^i \mid i=1,5,7,9,23,27,29,31,43\}$, μ_{-1}.
The code has zeros α^{89+13i}, $0\le i\le 11$, so $d\ge 13$.
Then, by Theorem (3.1.4), $d\ge 15$.

(8.2.26) $n=127$, $A=\{\alpha^i \mid i=1,5,9,11,13,15,19,31,43\}$, μ_{-1}.
The complete defining set of C contains $\{\alpha^{5i} \mid 1\le i\le 10\}$, so $d\ge 11$.
Hence $d\ge 12$. Let $c(x)$ be a codeword of weight 12 with zero-set S.
By computer, $c(\alpha^i)\neq 0$, $i=21,27,47$.
The following sets are independent w.r.t. S:
$(\underline{89},24,\underline{89},-70,\underline{27},26,\underline{54},-1,\underline{51},-42,\underline{27},-1,\underline{61},-8,\underline{54},32,\underline{87},-14,\underline{74},-1,\underline{74},$
$-1,\underline{74},-1,\underline{74})$, a contradiction.
Then Theorem (3.1.4) gives $d\ge 15$.

(8.2.27) $n=127$, $A=\{\alpha^i \mid i=1,3,13,15,21,27,29,47,55\}$, μ_{-1}.
The code has zeros α^{35i}, $1\le i\le 14$, so $d\ge 15$.
a) Let $c(x)$ be a codeword of weight 15 with zero-set S.
(i) $c(\alpha^9)\neq 0$, since otherwise $c(\alpha^{35i})=0$, $1\le i\le 15$.
(ii) Suppose $c(\alpha^{19})=0$.
Then $c(\alpha^{45})\neq 0$, since otherwise the following sets are independent w.r.t. S:
$(\underline{9},29,\underline{9},39,\underline{9},12,\underline{34},21,\underline{68},-26,\underline{68},-13,\underline{68},-13,\underline{68},-13,\underline{68},-13,\underline{68},-13,$
$\underline{68},-13,\underline{68},-13,\underline{68},-13,\underline{68},-13,\underline{68},-13,\underline{68})$.
The following sets are independent w.r.t. S:
$(\underline{17},67,\underline{45},36,\underline{45},-26,\underline{68},-17,\underline{106},4,\underline{68},-26,\underline{68},-13,\underline{68},-13,\underline{68},-26,\underline{68},$
$-13,\underline{68},-13,\underline{68},-13,\underline{68},-13,\underline{68},-13,\underline{68},-13,\underline{68})$, so $wt(c(x))\ge 16$, a contradiction. Hence $c(\alpha^{19})\neq 0$.
The following sets are independent w.r.t. S:
$(\underline{17},92,\underline{17},-15,\underline{72},-13,\underline{72},50,\underline{50},-2,\underline{72},-33,\underline{17},22,\underline{72},21,\underline{38},-52,\underline{100},29,$
$\underline{72},-33,\underline{17},-35,\underline{17},-35,\underline{17},-35,\underline{17},-35,\underline{17})$, a contradiction.
We have proved that $d\ge 16$.

b) Let $c(x)$ be a codeword of weight 16 with zero-set S.
(i) $c(\alpha^9)\neq 0$, since otherwise $c(\alpha^{35i})=0$, $0\le i\le 15$.
(ii) Suppose $c(\alpha^{19})=0$.
Then $c(\alpha^{45})\neq 0$, since otherwise the following sets are independent w.r.t. S:
$(\underline{68},52,\underline{68},-13,\underline{68},63,\underline{72},17,\underline{34},21,\underline{68},-26,\underline{68},-13,\underline{68},-13,\underline{68},-13,\underline{68},$
$-13,\underline{68},-13,\underline{68},-13,\underline{68},-13,\underline{68},-13,\underline{68},-13,\underline{68},-13,\underline{68})$.

The following sets are independent w.r.t. S:
$(\underline{17},-24,\underline{68},-13,\underline{68},-14,\underline{18},1,\underline{68},-17,\underline{106},4,\underline{68},-26,\underline{68},-13,\underline{68},-13,\underline{68},$
$-26,\underline{68},-13,\underline{68},-13,\underline{68},-13,\underline{68},-13,\underline{68},-13,\underline{68},-13,\underline{68})$.
Hence $c(\alpha^{19})\neq 0$.

The following sets are independent w.r.t. S:
$(\underline{17},57,\underline{100},17,\underline{34},-4,\underline{100},22,\underline{17},-13,\underline{50},-2,\underline{72},-33,\underline{17},22,\underline{72},21,\underline{38},-52,$
$\underline{100},29,\underline{72},-33,\underline{17},-35,\underline{17},-35,\underline{17},-35,\underline{17},-35,\underline{17})$, so $wt(c(x))\geq 17$, a contradiction.

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

(8.2.28) $n=127$, $A=\{\alpha^i \mid i=5,15,19,23,29,31,43,55,63\}$, μ_{-1}.
The code has zeros α^{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, $c(\alpha^i)\neq 0$, $i=1,3,7$.
The following sets are independent w.r.t. S:
$(\underline{112},-66,\underline{112},12,\underline{48},-8,\underline{96},3,\underline{12},-20,\underline{4},-4,\underline{24},-4,\underline{24},-5,\underline{14},-23,\underline{96},-3,\underline{1},$
$-1,\underline{1},-1,\underline{1})$, a contradiction.
Then Theorem (3.1.4) gives $d\geq 15$.

(8.2.29) $n=127$, $A=\{\alpha^i \mid i=5,7,9,11,13,19,21,31,63\}$, μ_{-1}.
The code has zeros α^{7i}, $1\leq i\leq 10$, so $d\geq 11$. Hence $d\geq 12$.
Let $c(x)$ be a codeword of weight 12.
Then, by computer, $c(\alpha^i)\neq 0$, $i=3,23,27,29,55$.
The following sets are independent w.r.t. the zero-set of $c(x)$:
$(\underline{3},33,\underline{3},-3,\underline{46},-2,\underline{110},-6,\underline{83},-4,\underline{101},-3,\underline{96},-24,\underline{89},-39,\underline{51},-13,\underline{12},-1,\underline{12},$
$-1,\underline{12},-1,\underline{12})$, a contradiction.
We have proved that $d\geq 15$.

(8.2.30) $n=127$, $A=\{\alpha^i \mid i=1,7,13,21,27,29,31,47,55\}$, μ_{-1}.
The code has zeros α^{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 $c(\alpha^i)\neq 0$, $i=3,5,15,23,43$.
The following sets are independent w.r.t. S:
$(\underline{75},-20,\underline{75},-13,\underline{114},-7,\underline{30},-3,\underline{53},-1,\underline{65},-10,\underline{92},-14,\underline{106},-27,\underline{5},-20,\underline{5},-3,\underline{3},$
$-1,\underline{3},-1,\underline{3})$, a contradiction. Then Theorem (3.1.4) gives $d\geq 15$.

(8.2.31) $n=127$, $A=\{\alpha^i \mid i=1,3,7,9,11,23,27,43,47\}$, μ_{-1}.
The code has zeros α^{87+21i}, $0\le i\le 13$, so $d\ge 15$.

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

(i) $c(\alpha^5)\ne 0$, since otherwise $c(\alpha^{3+21i})=0$, $0\le i\le 17$.

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

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

$(\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},42,\underline{80},-21,\underline{5},-40,\underline{5})$.

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

$(\underline{5},41,\underline{5},1,\underline{100},12,\underline{38},-2,\underline{100},51,\underline{66},21,\underline{66},-64,\underline{66},-21,\underline{66},9,\underline{33},75,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66})$, a contradiction.

Hence $c(\alpha^{55})\ne 0$.

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

$(\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},-43,\underline{66},-42,\underline{118},25,\underline{91},-46,\underline{66},9,\underline{33},75,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66})$, a contradiction.

So $d\ge 16$.

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

(i) Again $c(\alpha^5)\ne 0$.

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

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

$(\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},42,\underline{80},-21,\underline{5},-85,\underline{40},45,\underline{5})$.

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

$(\underline{5},41,\underline{5},1,\underline{100},12,\underline{38},-2,\underline{100},51,\underline{66},21,\underline{66},-64,\underline{66},-21,\underline{66},42,\underline{33},-33,\underline{33},75,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66})$, a contradiction.

Hence $c(\alpha^{55})\ne 0$.

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

$(\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},-43,\underline{66},-42,\underline{118},25,\underline{91},-46,\underline{66},42,\underline{33},-33,\underline{33},75,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66},21,\underline{66})$, a contradiction.

So $d\ge 17$.

Then Theorem (3.1.4) gives $d\ge 19$.

(8.2.32) $n=151$, $A=\{\alpha^i \mid i=1,3,7,15,35\}$, μ_{-1}.
From Theorem (3.1.4) we know that $d_0\ge 15$, $d_0\equiv 3 \bmod 4$.
Furthermore, all even weights are divisible by 4.
The code has zeros α^{61+3i}, $0\le i\le 8$, so $d\ge 10$. Hence $d\ge 12$.

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:
$(\underline{10},44,\underline{10},-3,\underline{40},25,\underline{139},-5,\underline{72},-1,\underline{72},-11,\underline{37},-7,\underline{5},-26,\underline{39},103,\underline{29},-22,\underline{121},$
$-3,\underline{5},-41,\underline{40},-50,\underline{72},-11,\underline{72},-1,\underline{72},-1,\underline{72})$, 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:
$(\underline{5},-1,\underline{5},56,\underline{36},-1,\underline{36},-32,\underline{78},-14,\underline{119},-7,\underline{18},-27,\underline{135},-24,\underline{119},35,\underline{40},-13,\underline{80},$
$-77,\underline{113},-37,\underline{119},-11,\underline{119},-1,\underline{119},-1,\underline{119})$, a contradiction.

We have proved that $d\geq 19$.

(8.2.33) $n=151$, $A=\{\alpha^{i}\mid i=1,3,7,17,35\}$, μ_{-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 ≤ 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 $c(x)$:
$(\underline{120},1,\underline{67},-10,\underline{67},-14,\underline{54},-1,\underline{95},-10,\underline{134},-1,\underline{132},-28,\underline{144},-43,\underline{72},-10,\underline{134},$
$-48,\underline{72},-1,\underline{72},-1,\underline{72})$, a contradiction.
Hence $d\geq 15$.

(8.2.34) $n=151$, $A=\{\alpha^{i}\mid i=1,3,7,11,17\}$, μ_{-1}.
The code has zeros α^{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:
$(\underline{23},2,\underline{94},-4,\underline{33},-4,\underline{125},-1,\underline{107},-3,\underline{92},-6,\underline{37},-34,\underline{40},-8,\underline{80},-28,\underline{5},-2,$
$\underline{5},-1,\underline{5},-1,\underline{5})$, a contradiction.
Hence, by Theorem (3.1.4), $d\geq 15$.

(8.2.35) $n=161$, $A=\{\alpha^{i}\mid i=5,11,35,69\}$, μ_{-1}.
The code has zeros α^{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:
$(\underline{139},-101,\underline{131},-52,\underline{146},-9,\underline{139},-1,\underline{139},-1,\underline{139},-1,\underline{139},-1,\underline{139},-1,\underline{139})$,
a contradiction.
Then, by Theorem (3.1.4), we have $d\geq 12$.

(8.2.36) $n=223$, $A=\{\alpha^i \mid i=1,3,5\}$, μ_{-1}.
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, $c(\alpha^i) \neq 0$, $i=9,13,19$.
The following sets are independent w.r.t. S:
$(\underline{50},-4,\underline{50},-1,\underline{50},-1,\underline{83},-3,\underline{106},-1,\underline{188},-23,\underline{19},-11,\underline{19},186,\underline{81},-47,\underline{177},-65,$
$\underline{175},-5,\underline{89},-47,\underline{29},-18,\underline{9},-7,\underline{9},-1,\underline{9},-1,\underline{9})$, a contradiction.
We have proved that $d \geq 19$.

(8.2.37) $n=233$, $A=\{\alpha^i \mid i=5,9,17,29\}$, μ_{-1}.
The code has zeros α^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, $c(\alpha^i) \neq 0$, $i=1,3,7,27$.
The following sets are independent w.r.t. S:
$(\underline{111},-1,\underline{108},-3,\underline{183},-4,\underline{189},-2,\underline{188},-1,\underline{4},-7,\underline{94},-3,\underline{89},-6,\underline{86},-1,\underline{86},-1,$
$\underline{86},-1,\underline{86},-1,\underline{86})$, a contradiction.
Hence $d \geq 16$, by Theorem (3.1.4).

(8.2.38) $n=233$, $A=\{\alpha^i \mid i=1,3,9,27\}$, μ_{-1}.
The code has zeros α^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, $c(\alpha^i) \neq 0$, $i=5,7,17,29$.
The following sets are independent w.r.t. S:
$(\underline{49},-2,\underline{139},-1,\underline{56},-3,\underline{208},-5,\underline{44},-1,\underline{44},-35,\underline{93},-23,\underline{139},-47,\underline{58},-54,\underline{41},-48,$
$\underline{225},-80,\underline{147},-3,\underline{141},-68,\underline{78},-1,\underline{78},-1,\underline{78},-1,\underline{78})$, a contradiction.
Then Theorem (3.1.4) gives $d \geq 17$.

(8.2.39) $n=233$, $A=\{\alpha^i \mid i=1,17,27,29\}$, μ_7.
We know that $d_0 \geq 17$.
The even-weight subcode has zeros $\alpha^{131+17i}$, $0 \leq i \leq 12$, so $d \geq 14$.
Let $c(x)$ be a codeword of weight 14 or 16 with zero-set S.
By computer, $c(\alpha^i) \neq 0$, $i=3,5,7,9$.
The following sets are independent w.r.t. S:
$(\underline{200},-2,\underline{138},-3,\underline{164},-1,\underline{113},-7,\underline{164},-1,\underline{183},-21,\underline{100},-26,\underline{56},-9,\underline{167},87,\underline{123},$
$18,\underline{31},126,\underline{96},-26,\underline{177},60,\underline{5},-3,\underline{3},-1,\underline{3},-1,\underline{3})$, a contradiction.
Hence $d \geq 17$.

(8.2.40) $n=241$, $A=\{\alpha^i \mid i=5,9,11,13,25\}$, μ_{11}.
Theorem (3.1.4) gives $d_0 \geq 17$.
The even-weight subcode has zeros α^{41+25i}, $0 \leq i \leq 16$, so the even-weight subcode has minimum distance ≥ 18.
Hence $d \geq 17$.

(8.2.41) $n=241$, $A=\{\alpha^i \mid i=1,5,9,13,25\}$, μ_{11}.
We know that $d_0 \geq 17$. The even-weight subcode has minimum distance ≥ 22, since it has zeros $\alpha^{232+25i}$, $0 \leq i \leq 20$.
Let $c(x)$ be a codeword of weight 17 with zero-set S.
Then, by computer, $c(\alpha^i) \neq 0$, $i=3,7,11,21,35$.
The following sets are independent w.r.t. S:
$(\underline{11},-1,\underline{196},-1,\underline{61},-4,\underline{219},-10,\underline{102},-15,\underline{139},-7,\underline{213},-5,\underline{48},-21,\underline{89},-74,\underline{139},$
$129,\underline{55},79,\underline{55},-107,\underline{48},-56,\underline{131},-24,\underline{85},-26,\underline{11},-1,\underline{11},-1,\underline{11})$,
a contradiction.
We have proved that $d \geq 19$.

(8.2.42) $n=241$, $A=\{\alpha^i \mid i=5,7,9,11,13\}$, μ_{11}.
We have $d_0 \geq 17$.
Let $c(x)$ be a codeword of even weight ≤ 14.
Then, by computer, $c(\alpha^i) \neq 0$, $i=1,3,21,25,35$.
The following sets are independent w.r.t. the zero-set of $c(x)$:
$(\underline{24},-1,\underline{84},-1,\underline{120},-3,\underline{235},-1,\underline{156},-7,\underline{73},-20,\underline{151},126,\underline{71},-3,\underline{204},-51,\underline{200},$
$-96,\underline{163},-39,\underline{27},-7,\underline{12},-1,\underline{12},-1,\underline{12})$, 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 ≤ 241. For each code we give

(i) n : the code-length.

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

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

(iii) a defining set : e.g. the duadic code of length 49 has defining set $\{\alpha^i \mid i \in C_1 \cup C_{21}\}$, where α 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 μ_a.

(vi) a reference.

n	idempotent	defining set	d	a	reference
7	1	1	3	-1	QR code, [10]
17	0,1	1	5	3	QR code, [7]
23	1	1	7	-1	QR code, [7]
31	1,5,7	1,5,7	7	-1	QR code, [7]
31	1,3,5	1,3,5	7	-1	Reed-Muller code, (2.2.2)
41	0,1	1	9	3	QR code, [7]
47	1	1	11	-1	QR code, [7]
49	0,1,7	1,21	4	-1	(4.3.1)
71	1	1	11	-1	QR code, (3.1.4)
73	0,1,3,5,11	1,13,17,25	9	-1	(8.1.6)
73	0,1,3,5,13	3,9,11,17	9	-1	(8.1.3)
73	0,1,5,9,17	1,9,11,13	12	3	[7]
73	0,1,3,9,25	1,3,9,25	13	5	QR code, [7]
79	1	1	15	-1	QR code, [7]
89	0,1,3,5,13	1,9,13,33	12	-1	(8.2.1)
89	0,1,3,5,19	3,9,11,19	12	-1	(8.2.2)
89	0,1,3,11,33	1,3,11,33	15	5	[7]
89	0,1,5,9,11	1,5,9,11	17	3	QR code, [7]
97	0,1	1	15	5	QR code, [7]
103	1	1	19	-1	QR code, [7]
113	0,1,9	1,9	15	3	QR code, [7]
113	0,1,3	1,3	18	9	[7]
119	1,13,17,21	1,11,21,51	4	3	BCH bound
119	1,7,11,51	1,13,17,21	6	3	BCH bound
119	1,7,13,17	3,7,13,51	8	3	(8.2.3)
119	1,7,11,17	3,11,21,51	12	3	[7]

n	idempotent	defining set	d	a	reference
127	1,3,9,11,13, 15,21,27,47	1,3,5,7,9, 11,13,19,21	15	-1	Reed-Muller code, (2.2.2)
127	1,3,5,9,11, 13,15,21,27	3,5,7,11,19, 21,23,55,63	15	-1	(8.2.5)
127	1,3,9,13,15, 19,21,29,47	1,3,5,7,9,19, 23,29,43	15	-1	(8.2.6)
127	1,3,7,9,11, 13,19,21,47	3,5,7,9,11, 23,27,43,63	15	-1	(8.2.7)
127	1,3,7,9,11, 13,21,27,47	9,11,13,15,19, 31,43,47,63	15	-1	(8.2.8)
127	1,3,5,7,9, 13,19,21,29	1,3,5,15,19, 21,23,29,55	15	-1	(8.1.3)
127	1,3,15,21,23, 27,29,47,55	3,7,9,13,19, 21,29,47,63	15	-1	(8.2.9)
127	1,3,5,7,9, 19,21,23,29	3,9,11,15,21, 23,27,47,63	15	-1	(8.2.10)
127	1,3,5,7,9, 11,21,23,27	3,5,7,19,23, 29,43,55,63	15	-1	(8.2.11)
127	1,3,7,9,11, 21,23,27,47	1,5,13,15,27, 29,31,43,55	15	-1	(8.2.12)
127	1,3,7,9,11, 19,21,23,47	1,3,7,19,23, 29,43,47,55	15	-1	(8.2.13)
127	1,3,7,9,13, 21,27,29,47	3,15,19,21,23, 29,47,55,63	15	-1	(8.2.14)
127	1,3,5,9,15, 21,23,27,29	3,5,9,13,15, 19,21,29,63	15-16	-1	(8.2.15)
127	1,3,9,13,15, 21,27,29,47	1,3,5,9,15, 23,27,29,43	15-19	-1	(8.2.16)
127	1,3,5,9,13, 15,21,27,29	5,7,9,13,19, 29,31,43,63	15-19	-1	(8.2.17)
127	1,3,9,15,21, 23,27,29,47	3,11,15,19,23, 43,47,55,63	15-19	-1	(8.2.18)
127	1,3,9,11,15, 21,23,27,47	9,13,15,19,21, 29,31,47,63	15-19	-1	(8.2.19)
127	1,3,7,9,21, 23,27,29,47	1,3,5,9,11, 15,21,23,27	15-19	-1	(8.2.20)

n	idempotent	defining set	d	a	reference
127	1,3,5,9,13, 15,19,21,29	3,9,15,23,27, 29,43,47,63	15-19	-1	(8.2.21)
127	1,3,9,11,13, 15,19,21,47	1,3,7,11,19, 21,23,47,55	15-19	-1	(8.2.22)
127	1,3,9,15,19, 21,23,29,47	5,7,11,13,27, 31,43,55,63	15-19	-1	(8.2.23)
127	1,3,5,9,15, 19,21,23,29	1,3,5,11,15, 19,23,43,55	15-19	-1	(8.2.24)
127	1,3,11,13,15, 21,27,47,55	1,5,7,9,23, 27,29,31,43	15-19	-1	(8.2.25)
127	1,3,5,7,9, 11,13,19,21	1,5,9,11,13, 15,19,31,43	15-19	-1	(8.2.26)
127	1,3,5,7,11, 13,21,27,55	1,3,13,15,21, 27,29,47,55	19	-1	(8.2.27)
127	1,3,5,7,21, 23,27,29,55	5,15,19,23,29, 31,43,55,63	15-19	-1	(8.2.28)
127	1,3,5,7,9, 21,23,27,29	5,7,9,11,13, 19,21,31,63	15-19	-1	(8.2.29)
127	1,3,5,7,9, 13,21,27,29	1,7,13,21,27, 29,31,47,55	15-19	-1	(8.2.30)
127	1,3,5,7,9, 11,13,21,27	1,3,7,9,11, 23,27,43,47	19	-1	(8.2.31)
127	1,9,11,13,15, 19,21,31,47	1,9,11,13,15, 19,21,31,47	19	-1	QR code, [12]
137	0,1	1	13-21	3	QR code, (3.1.4)
151	1,3,5,11,17	1,3,7,15,35	19	-1	(8.2.32)
151	1,3,5,11,15	1,3,7,17,35	15-19	-1	(8.2.33)
151	1,5,11,17,37	1,5,11,17,37	19	-1	QR code, [12]
151	1,3,7,11,15	1,3,7,11,17	15-23	-1	(8.2.34)
161	0,1,3,35,69	1,11,23,35	4	-1	BCH bound
161	0,1,3,7,23	1,7,11,69	8	-1	BCH bound, (3.1.4)
161	0,1,7,11,23	1,3,23,35	8	-1	BCH bound, (3.1.4)
161	0,1,7,11,69	5,11,35,69	12-16	-1	(8.2.35)

n	idempotent	defining set	d	a	reference
167	1	1	15-23	-1	QR code, (3.1.4)
191	1	1	15-27	-1	QR code, (3.1.4)
193	0,1	1	15-27	5	QR code, (3.1.4)
199	1	1	15-31	-1	QR code, (3.1.4)
223	1,3,9	1,3,5	19-31	-1	(8.2.36)
223	1,9,19	1,9,19	19-31	-1	QR code, (3.1.4)
233	0,1,7,9,29	1,7,9,29	17-25	3	QR code, (3.1.4)
233	0,1,3,9,27	5,9,17,29	16-29	-1	(8.2.37)
233	0,1,3,7,27	1,3,9,27	17-29	-1	(8.2.38)
233	0,1,3,5,29	1,17,27,29	17-32	7	(8.2.39)
239	1	1	19-31	-1	QR code, (3.1.4)
241	0,1,3,7,9,21	5,9,11,13,25	17-25	11	(8.2.40)
241	0,1,3,5,7,9	1,5,9,13,25	19-30	11	(8.2.41)
241	0,1,7,9,13,21	5,7,9,11,13	16-30	11	(8.2.42)
241	0,1,3,5,9,25	1,3,5,9,25	17-31	11	QR code, (3.1.4)

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

All splittings are given by μ_{-1}.

minimum distance	4	≤8	≤12	≤16	≤20	≤24
number of codes	16	32	240	448	144	144

References

1. L.D.Baumert, "Cyclic difference sets", Springer Lecture Notes 182, Berlin, Springer Verlag, 1971.
2. W.G.Bridges, M.Hall,Jr. and J.L.Hayden, "Codes and designs", J.Combin.Theory Ser.A 31, 155-174 (1981).
3. M.Hall,Jr., "Combinatorial theory", New York/London, Wiley, 1967.
4. R.A.Hogendoorn, "Toepassing van een nieuwe grens voor de minimum afstand van cyclische codes", Dept.of Math., Tech.Univ. of Eindhoven, The Netherlands, Project report, September 1984.
5. D.Jungnickel and K.Vedder, "On the geometry of planar difference sets", Europ.J.Combinatorics 5, 143-148 (1984).
6. J.S.Leon, J.M.Masley and V.Pless, "Duadic codes", IEEE Trans.Inf.Th., IT-30, No.5, 709-714 (1984).
7. J.S.Leon, J.M.Masley and V.Pless, "On weights in duadic codes", to appear in J.Combin.Theory Ser.A.
8. W.J.LeVeque, "Fundamentals of number theory", Reading, Mass., Addison-Wesley, 1977.
9. J.H.van Lint, "Inleiding in de coderingstheorie", MC Syllabus 31, Amsterdam, Mathematical Centre, 1980.
10. J.H.van Lint, "Introduction to coding theory", New York, Springer Verlag, 1982.
11. J.H.van Lint and R.M.Wilson, "On the minimum distance of cyclic codes", IEEE Trans.Inf.Th., IT-32, No.1, 23-40 (1986).
12. F.J.MacWilliams and N.J.A.Sloane, "The theory of error-correcting codes", Amsterdam, North-Holland, 1977.
13. V.Pless, "Cyclic projective planes and binary,extended cyclic self-dual codes", to appear in J.Combin.Theory Ser.A.
14. V.Pless, "Q-codes", preprint.
15. P.Ribenboim, "1093", The Mathematical Intelligencer", 5, No.2, 28-34 (1983).
16. P.Rowlinson, "On 4-cycles and 5-cycles in regular tournaments", Bull.London Math.Soc. 18, 135-139 (1986).
17. H.C.A.van Tilborg, "On weights in codes", Dept.of Math., Tech. Univ. of Eindhoven, The Netherlands, Rep.71-WSK-03, December 1971.
18. H.A.Wilbrink, "A note on planar difference sets", J.Combin.Theory Ser.A 38, 94-95 (1985).

Index