EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 8, No. 1, 2015, 64-80
ISSN 1307-5543 – www.ejpam.com

Cyclic Isodual and Formally Self-dual Codes over $\mathbb{F}_q + v\mathbb{F}_q$

Aicha Batoul[1], Kenza Guenda[1], Abidin Kaya[2], Bahattin Yildiz[2,*]

[1] *Faculty of Mathematics USTHB,University of Science and Technology of Algiers, Algeria*
[2] *Department of Mathematics, Fatih University, Istanbul, Turkey.*

Abstract. In this paper, we investigate the structure and properties of duadic, isodual cyclic and formally self-dual codes over the ring $R = \mathbb{F}_q + v\mathbb{F}_q$ with $v^2 = v$. In addition to the theoretical work on the structure of these codes, we construct examples of good codes over different alphabets from cyclic self-dual and formally self-dual codes over R.

2010 Mathematics Subject Classifications: 94B15, 94B05

Key Words and Phrases: Isodual Codes, Duadic codes, formally self-dual codes, cyclic codes

1. Introduction

Duadic codes over finite fields form an important class of linear codes for both theoretical and practical reasons in error-correcting codes. They were first introduced by Leon *et al.* [10] as generalized quadratic residue cyclic codes over fields. Rushanan [12] generalized them to duadic abelian codes. Duadic codes over rings were introduced by Langevin *et al.* [9] and over $\mathbb{F}_2 + u\mathbb{F}_2$ by San Ling *et al.* [11].

Codes over $\mathbb{F}_p + v\mathbb{F}_p$, p a prime integer, were first introduced by Bachoc in [1] together with a new weight. They are shown to be connected to lattices and have since then generated interest among coding theorists. For some of the work in the literature about these codes and related codes we refer the readers to [6, 11–13, 16]. Recently, Zhu *et al.* considered the structure of cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$ in [17].

Formally self-dual codes are also an important class of codes that have generated a lot of interest since they have weight enumerators that are invariant under the MacWilliams transform and sometimes have better parameters than self-dual codes. This gives them a potential for applications to such areas as invariant theory, lattices and designs.

The aim of this paper is to introduce and study duadic codes, isodual cyclic codes and formally self-dual codes over the ring $\mathbb{F}_q + v\mathbb{F}_q$ which is isomorphic to $\mathbb{F}_q \times \mathbb{F}_q$ for q a prime

*Corresponding author.

Email addresses: abatoul@usthb.dz (A. Batoul), kguenda@usthb.dz (K. Guenda), akaya@fatih.edu.tr (A. Kaya), byildiz@fatih.edu.tr (B. Yildiz)

power. We first give some preliminaries about the ring $R = \mathbb{F}_q + v\mathbb{F}_q$ and linear codes over R. Then we introduce a weight and an associated Gray map. Thus we characterize duadic codes and isodual cyclic codes over the ring and tabulate some good codes obtained from isodual cyclic codes. We finish by giving several constructions of formally self-dual codes together with many examples of good formally self-dual codes obtained as Gray images.

2. Preliminaries

In this section, we introduce some basic results on linear codes over the ring $R = \mathbb{F}_q + v\mathbb{F}_q$, q a prime power, where $v^2 = v$. Let $\mathbb{F}_q$ be the finite field of order q and $\mathbb{F}_q^*$ the multiplicative group of $\mathbb{F}_q$. It is known that $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ is a principal ideal ring. We adopt the notation $\langle g(x)\rangle$ to denote the ideal in $\mathbb{F}_p[x]/\langle x^n-1\rangle$ generated by $g(x)$ with $g(x)$ being a monic divisor of $x^n - 1$, in this case $g(x)$ is called a generator polynomial. Throughout this paper, we let R denote the commutative ring

$$\mathbb{F}_q + v\mathbb{F}_q = \{a + vb \mid a, b \in \mathbb{F}_q\} \text{ with } v^2 = v.$$

It turns out R is a principal ideal ring and has only two non-trivial ideals, namely,

$$\langle v\rangle = \{av \mid a \in \mathbb{F}_q\} \text{ and } \langle 1 - v\rangle = \{b(1 - v) \mid b \in \mathbb{F}_q\}.$$

We can easily prove that $\langle v\rangle$ and $\langle 1 - v\rangle$ are maximal ideals in R, hence R is not a chain ring. Let R^n be the R-module of n-tuples over R. A linear code C over R of length n over R is an R-submodule of R^n.

For any linear code C of length n over R the dual $C^\perp$ is defined as

$$C^\perp = \{u \in R^n \mid u \cdot w = 0,\ \forall\, w \in C\}$$

where $u \cdot w$ denotes the standard Euclidean inner product of u and w in R^n. Note that $C^\perp$ is linear whether or not C is linear. The Gray map Ψ from R to $\mathbb{F}_q \oplus \mathbb{F}_q$ given by $\Psi(c) = (a, a + b)$, is a ring isomorphism, which means that R is isomorphic to the ring $\mathbb{F}_q \oplus \mathbb{F}_q$ therefore R is a finite Frobenius ring.

For the case where q is a prime the linear and duality preserving Gray map
$\psi(a + bv) = (-b, 2a + b)$ from [16] is used for computational results in Tables 1, 2 and 3.

If C is linear then $|C||C^\perp| = |R|^n$ see [15]. A linear code C over R is said to be cyclic if it satisfies

$$(c_{n-1}, c_0, \dots, c_{n-2}) \in C, \text{ whenever } (c_0, c_1, \dots, c_{n-1}) \in C.$$

It is well known that cyclic codes of length n over R can be identified with an ideal in the quotient ring $R[x]/\langle x^n - 1\rangle$ via the R-module isomorphism as follows:

$$\begin{aligned} R^n &\longrightarrow R[x]/\langle x^n - 1\rangle \\ (c_0, c_1, \dots, c_{n-1}) &\mapsto c_0 + c_1x + \dots + c_{n-1}x^{n-1}. \end{aligned} \tag{1}$$

Let A, B be codes over R. We denote

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

Note that any element c of R^n can be expressed as $av + b(1-v)$ where $a, b \in \mathbb{F}_q^n$. Let C be a linear code of length n over R. Define

$$C_1 = \{a \in \mathbb{F}_p^n \,|\, va + (1-v)b \in C \text{ for some } b \in \mathbb{F}_q^n\}$$

and

$$C_2 = \{b \in \mathbb{F}_p^n \,|\, va + (1-v)b \in C \text{ for some } a \in \mathbb{F}_q^n\}.$$

Obviously C_1 and C_2 are linear codes over $\mathbb{F}_q$. By the definition of C_1 and C_2 we have that C can be uniquely expressed as $C = vC_1 \oplus (1-v)C_2$. So C_1 and C_2 are unique. We observe that in that case we have $|C| = |C_1||C_2|$.

The extended code of a code C over $\mathbb{F}_q + v\mathbb{F}_q$ will be denoted by $\widetilde{C}$, which is the code obtained by adding a specific column to the generator matrix of C.

Lemma 1. *Let R^* denote the group of units of R then $R^* = v\mathbb{F}_q^* \oplus (1-v)\mathbb{F}_q^*$.*

Proof. Since R decomposes as a direct sum $R = v\mathbb{F}_q \oplus (1-v)\mathbb{F}_q$. Then R^* decomposes naturally as a direct product of groups; $R^* = v\mathbb{F}_q^* \oplus (1-v)\mathbb{F}_q^*$. So if $\lambda \in R^*$, then $\lambda = \lambda_1 v + (1-v)\lambda_2$ where each $\lambda_i \in \mathbb{F}_q^*$, for $1 \le i \le 2$. □

A monomial linear transformation of R^n is an R-linear transformation τ such that there exist scalars $\lambda_1, \ldots, \lambda_n$ in R^* and a permutation $\sigma \in S_n$, the group of permutations of the set $\{1, 2, \ldots, n\}$, such that, for all $(x_1, x_2, \ldots, x_n) \in R^n$, we have

$$\tau(x_1, \ldots, x_n) = (\lambda_1 x_{\sigma(1)}, \lambda_2 x_{\sigma(2)}, \ldots, \lambda_n x_{\sigma(n)}).$$

Two linear codes C and C' of length n are called monomially equivalent if there exists a monomial transformation of R^n such that $\tau(C) = C'$.

An isodual code is a linear code which is equivalent to its dual. The class of isodual codes is important in coding theory, in particular because it contains the self-dual codes as a subclass. In addition, isodual codes are contained in the larger class of formally self-dual codes, and they are related to isodual lattices [1]. In this work, by the equivalence of two codes we will mean the monomoial equivalence. Hence in our context an isodual code is a linear code which is monomially equivalent to its dual.

3. Cyclic Codes over $R = \mathbb{F}_q + v\mathbb{F}_q$

In this section, we let $R_n = R[x]|\langle x^n - 1\rangle$. As usual we identify R_n by the set of all polynomials over R of degree less than n. The following results are quite analogous to the ones obtained in [16] for the ring $\mathbb{F}_2 + v\mathbb{F}_2$, and thus the proofs being the same, will be omitted here:

Theorem 1. *Let $C = vC_1 \oplus (1-v)C_2$ be a linear cyclic code of length n over R. then C is cyclic code of length n over R if and only if C_1 and C_2 are cyclic codes of length n over $\mathbb{F}_q$.*

The following theorem tells us that C is also principally generated in that case:

Theorem 2. *Let $C = vC_1 \oplus (1-v)C_2$ be a cyclic code of length n over R. There exist a unique polynomial $f(x)$ such that $C = \langle f(x) \rangle$, where $f(x) = vf_1(x) + (1-v)f_2(x)$*

Corollary 1. *Let $C = vC_1 \oplus (1-v)C_2$ be a cyclic code of length n over R and $f_1(x)$, $f_2(x)$ are the generator polynomials of C_1 and C_2 respectively. Then $|C| = q^{2n-deg(f_1(x))-deg(f_2(x))}$.*

For the proof of the following theorem we introduce some notations. Since the ring R has two maximal ideals $\langle v \rangle$ and $\langle 1-v \rangle$ with the same residue field $\mathbb{F}_p$ thus we have two canonical projections defined as follows:

$$\begin{aligned} \psi_1 : R = \mathbb{F}_q + v\mathbb{F}_q &\longrightarrow \mathbb{F}_q \\ va + (1-v)b &\longmapsto \psi_1(va + (1-v)b) = a \end{aligned}$$

and

$$\begin{aligned} \psi_2 : R = \mathbb{F}_q + v\mathbb{F}_q &\longrightarrow \mathbb{F}_q \\ va + (1-v)b &\longmapsto \psi_2(va + (1-v)b) = b. \end{aligned}$$

Denote by $\psi_1(u)$ and $\psi_2(u)$ the images of an element $u \in R$. These two projections can be extended naturally from R^n to $\mathbb{F}_q^n$ and from $R[x]$ to $\mathbb{F}_q[x]$. Let

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$$

where $a_i \in R$, $0 \leq i \leq n-1$, and we denote

$$\begin{aligned} \psi_1(f(x)) =& \psi_1(a_0) + \psi_1(a_1)x + \psi_1(a_2)x^2 + \ldots + \psi_1(a_{n-1})x^{n-1} \\ \psi_2(f(x)) =& \psi_2(a_0) + \psi_2(a_1)x + \psi_2(a_2)x^2 + \ldots + \psi_2(a_{n-1})x^{n-1}. \end{aligned}$$

Hence $f(x)$ has a unique expression as $f(x) = v\psi_1(f(x)) + (1-v)\psi_2(f(x))$.

Theorem 3. *Let $C = vC_1 \oplus (1-v)C_2$ be a cyclic code of length n over R, then its dual code $C^\perp$ is also cyclic and moreover we have $C^\perp = vC_1^\perp \oplus (1-v)C_2^\perp$.*

Proof. Let $C = vC_1 \oplus (1-v)C_2$ so $\psi_1(C) = C_1$ and $\psi_2(C) = C_2$ are cyclic codes over $\mathbb{F}_q$ then $C_1^\perp$ and $C_2^\perp$ are also cyclic codes. Let $D = vC_1^\perp \oplus (1-v)C_2^\perp$ so by Theorem 1 D is a cyclic code of length n over R we can prove that $C^\perp = D$. □

Corollary 2. *Let $C = \langle vf_1(x), (1-v)f_2(x) \rangle$ be a cyclic code of length n over R, with $f_1(x)$ and $f_2(x)$ as the generator polynomials of C_1 and C_2 respectively such that $x^n - 1 = f_1(x)h_1(x)$ and $x^n - 1 = f_2(x)h_2(x)$. Then*

(i) $C^\perp = \langle vh_1^*(x), (1-v)h_2^*(x) \rangle$ *and* $|C^\perp| = q^{deg(f_1(x)+deg(f_2(x)))}$,

(ii) $C^\perp = \langle h(x) \rangle$ *where* $h(x) = vh_1^*(x) + (1-v)h_2^*(x)$.

The following Lemma is a well known result, for its proof see for example [5].

Lemma 2. *A linear cyclic code over $\mathbb{F}_q$ with generator polynomial $f(x)$ is self-orthogonal if and only if $h(x)h^*(x) \mid (x^n-1)$, where $h^*(x) = x^{deg(h(x))}h(x^{-1})$ is the reciprocal polynomial of $h(x)$ with $h(x) = (x^n-1)/f(x)$.*

The following follows easily from the previous lemma:

Theorem 4. *Suppose $C = \langle f(x) \rangle$ is cyclic code over R, where $f(x) = vf_1(x)+(1-v)f_2(x)$, then*

$$C \subset C^{\perp} \text{ if and only if } C_1 \subset C_1^{\perp} \text{ and } C_2 \subset C_2^{\perp},$$

where $C_1 = \langle f_1(x) \rangle$ and $C_2 = \langle f_2(x) \rangle$.

Corollary 3. *Suppose $C = vC_1 \oplus (1-v)C_2$ is a cyclic code of arbitrary length n over R then*

$$C \subset C^{\perp} \text{ if and only if } C_1 \subset C_1^{\perp} \text{ and } C_2 \subset C_2^{\perp}.$$

Lemma 3. *Let C_1 and C_2 be two linear codes of length n over $\mathbb{F}_q$ and*

$$C = vC_1 \oplus (1-v)C_2 = \{(vc_1 + (1-v)c_2),\, c_1 \in C_1,\, c_2 \in C_2\}.$$

We have

$$C^{\perp} = vC_1^{\perp} \oplus (1-v)C_2^{\perp} = \{(vc_1 + (1-v)c_2),\, c_1 \in C_1^{\perp},\, c_2 \in C_2^{\perp}\}$$

C is self-dual if and only if C_1 and C_2 are self-dual.

Proposition 1. *Let C_1, C_2, C_1' and C_2' be four linear codes of length n over $\mathbb{F}_q$. Then*

$$C = vC_1 \oplus (1-v)C_2 = \{(vc_1 + (1-v)c_2),\, c_1 \in C_1,\, c_2 \in C_2\}$$

is equivalent to

$$C' = vC_1' \oplus (1-v)C_2' = \{(vc_1' + (1-v)c_2'),\, c_1' \in C_1',\, c_2' \in C_2'\}$$

over R if and only if C_1 and C_2 are equivalent respectively to C_1' and C_2'.

Proof. Let τ_1 and τ_2 two monomial permutations such that $\tau_1(C_1) = C_1'$ and $\tau_2(C_2) = C_2'$. Define the map

$$\begin{aligned} \tau : R^n &\longrightarrow R^n \\ va + (1-v)b &\longmapsto v\tau_1(a) + (1-v)\tau_2(b)) \end{aligned}$$

We have $\tau(C) = v\tau(C) \oplus (1-v)\tau(C) = v\tau_1(C_1) \oplus (1-v)\tau_2(C_2) = vC_1' \oplus (1-v)C_2' = C'$.

Conversely, let τ be a monomial permutation such that $\tau(C) = C'$, since $\mathbb{F}_q \subset \mathbb{F}_q + v\mathbb{F}_q$, we can take the restriction of τ over $\mathbb{F}_q$. Then define $\tau_i = \psi_i \circ \tau$, $1 \le i \le 2$ thus $C' = vC_1' \oplus (1-v)C_2' = \tau(C) = \tau(vC_1 \oplus (1-v)C_2) = v\psi_1 \circ \tau(C) \oplus (1-v)\psi_2 \circ \tau(C) = v\psi_1 \circ \tau(C_1) \oplus (1-v)\psi_2 \circ \tau(C_2)$. Since C_1' and C_2' are unique then $\psi_1 \circ \tau(C_1) = C_1'$ and $\psi_2 \circ \tau(C_2) = C_2'$. □

4. Duadic Codes over $R = \mathbb{F}_q + v\mathbb{F}_q$

Before giving our constructions of duadic codes over $\mathbb{F}_q + v\mathbb{F}_q$, we recall some results about duadic codes over finite fields which we will use thereafter.

4.1. Duadic Codes over Finite Fields

It is well known that every cyclic code over $\mathbb{F}_q$ has a polynomial that generates it as an ideal in the finite ring $\mathbb{F}_q[x]/(x^n-1)$. In general there are many generators for a given cyclic code. However, if we consider the monic generator of least degree then it is unique. Such a polynomial is called the generator of the code and naturally it has to be a divisor of x^n-1. Therefore, there is one-to-one correspondence between cyclic codes of length n over $\mathbb{F}_q$, and divisors of x^n-1.

Let a be an integer such that $(a,n)=1$. The function μ_a defined on $\mathbb{Z}_n = \{0,1,\ldots,n-1\}$ by $\mu_a(i) \equiv ia \pmod n$ is a permutation of the coordinate positions $\{0,1,2,\ldots,n-1\}$ and is called a multiplier. Multipliers also act on polynomials and this gives the following ring automorphism

$$\begin{aligned} \mu_a : \mathbb{F}_q[x]/(x^n-1) &\longrightarrow \mathbb{F}_q[x]/(x^n-1) \\ f(x) &\mapsto \mu_a(f(x)) = f(x^a). \end{aligned} \tag{2}$$

Suppose that $f(x) = a_0 + a_1x + \ldots + a_rx^r$ is a polynomial of degree r with $f(0) = a_0 \neq 0$. Then the monic reciprocal polynomial of $f(x)$ is

$$f^*(x) = f(0)^{-1}x^r f(x^{-1}) = f(0)^{-1}x^r(\mu_{-1}(f(x))) = a_0^{-1}(a_r + a_{r-1}x + \ldots + a_0x^r).$$

If a polynomial is equal to its reciprocal polynomial, then it is called a self-reciprocal polynomial over $\mathbb{F}_q$. If $g(x)$ is a generator polynomial of a cyclic code C of length n over $\mathbb{F}_q$, then the dual code $C^\perp$ of C is the cyclic code whose generator polynomial is $h^*(x)$ where $h^*(x)$ is the monic reciprocal polynomial of $h(x) = (x^n-1)/g(x)$. Thus the cyclic code C is self-dual if and only if $g(x) = h^*(x)$.

Let S_1 and S_2 be unions of q-cyclotomic cosets modulo m such that $S_1 \cap S_2 = \emptyset$, $S_1 \cup S_2 = \mathbb{Z}_m \setminus \{0\}$ and $\mu_a S_i \mod m = S_{(i+1) \mod 2}$. Then the triple μ_a, S_1, S_2 is called a splitting modulo m. The odd-like duadic codes D_1 and D_2 are the cyclic codes over $\mathbb{F}_q$ with defining sets S_1 and S_2 and generator polynomials $f_1(x) = \Pi_{i \in S_1}(x-\alpha^i)$ and $f_2(x) = \Pi_{i \in S_2}(x-\alpha^i)$, respectively. The even-like duadic codes C_1 and C_2 are the cyclic codes over $\mathbb{F}_q$ with defining sets $\{0\} \cup S_1$ and $\{0\} \cup S_2$, respectively.

For the remainder of the paper, the notation $q = \square \mod m$ means that q is a quadratic residue modulo m. For a prime power q and integer m such that $\gcd(q,m)=1$, we denote by $ord_m(q)$ the multiplicative order of q modulo m. This is the smallest integer l such that $q^l \equiv 1 \pmod m$. In the following we give necessary and sufficient conditions for the existence of duadic codes.

Theorem 5. *[14] Duadic codes of length m over $\mathbb{F}_q$ exist if and only if $q = \square \mod m$, i.e, if $m = p_1^{s_1}p_2^{s_2}\ldots p_k^{s_k}$ is the prime factorization of the odd integer m where each $s_i > 0$, then duadic codes of length m over $\mathbb{F}_q$ exist if and only if $q = \square \mod p_i$ $i = 1,2,\ldots,k$.*

Remark 1. *In general the same splitting modulo an odd integer m can be given by different multipliers. For more details see [5, page 214]. When we consider the multiplier μ_{-1}, we mean any multiplier which gives the same splitting as the multiplier μ_{-1}.*

The multiplier μ_{-1} plays a special role in determining the duals of duadic codes just as it does for duals in general cyclic codes. In the following we give some important result which concerns the multiplier μ_{-1}.

Theorem 6. *[5, Theorem 6.4.2] If C_1 and C_2 are a pair of even-like duadic codes over $\mathbb{F}_q$, with D_1 and D_2 the associated pair of duadic codes, the following are equivalent:*

(i) $C_1^{\perp} = D_1$

(ii) $C_2^{\perp} = D_2$

(iii) $\mu_{-1}(C_1) = C_2$

(iv) $\mu_{-1}(C_2) = C_1$.

Theorem 7. *[5, Theorem 6.4.3] If C_1 and C_2 are a pair of even-like duadic codes over $\mathbb{F}_q$, with D_1 and D_2 the associated pair of duadic codes. Then the following are equivalent:*

(i) $C_1^{\perp} = D_2$

(ii) $C_2^{\perp} = D_1$

(iii) $\mu_{-1}(C_1) = C_1$

(iv) $\mu_{-1}(C_2) = C_2$.

In the following we investigate when a splitting modulo an odd integer m is given by the multiplier μ_{-1} and when it is left invariant by it.

Theorem 8. *[14] Let $\mathbb{F}_q$ be a finite field and $m = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$ be a prime factorization of the odd integer m, such that $q \equiv \square \bmod m$.*

(i) If $p_i \equiv -1 \bmod 4$, $i = 1, 2, \dots, k$ Then all splittings $\bmod m$ are given by μ_{-1},

(ii) If at least one $p_i \equiv 1 \bmod 4$, $i \in \{1, 2, \dots, k\}$, then there is a splitting $\bmod m$ which is not given by μ_{-1}.

The following theorem gives us the relation between the generators and the splitting:

Proposition 2. *[2, Proposition 4.4] Let $\mathbb{F}_q$ be a finite field and m a positive odd integer such that $(m, q) = 1$ and $q = \square \bmod m$. Thus there exists a pair of odd-like duadic codes over $\mathbb{F}_q$, D_1 and D_2 generated respectively by $f_1(x)$ and $f_2(x)$ such that $x^m - 1 = (x-1) f_1(x) f_2(x)$. Then the following holds.*

(i) If the splitting modulo m is given by μ_{-1} then $f_1^*(x) = f_2(x)$ and $f_2^*(x) = f_1(x)$.

(ii) If the splitting modulo m is not given by μ_{-1} then $f_1^*(x) = f_1(x)$ and $f_2^*(x) = f_2(x)$.

Remark 2. *So with the assumption of Proposition 2, we have that either $f_1(x)$ and $f_2(x)$ are self-reciprocal polynomials or one is the reciprocal of the other.*

Proposition 3. *[2, Proposition 4.8] Let q be a prime power and m an odd integer. Then $ord_m(q)$ is odd if and only if there exists a pair of odd like duadic codes $D_1 = \langle g_1(x)\rangle$ and $D_2 = \langle g_2(x)\rangle$ given by the the multiplier μ_{-1} and such that $g_1^*(x) = g_2(x)$.*

Let q be a prime power and m an odd integer such that $q \equiv \square \mod m$. Let $f_1(x)$ and $f_2(x)$ be the generators polynomials of $[m, \frac{m+1}{2}]$ odd-like duadic codes over $\mathbb{F}_q$, and $(x-1)f_1(x)$ and $(x-1)f_2(x)$ be the generators polynomials of $[m, \frac{m-1}{2}]$ even-like duadic codes over $\mathbb{F}_q$.

Definition 1. *Let $D_1 = \langle vf_1(x), (1-v)f_2(x)\rangle$ and $D_2 = \langle vf_2(x), (1-v)f_1(x)\rangle$ and $C_1 = \langle v(x-1)f_1(x), (1-v)(x-1)f_2(x)\rangle$ and $C_2 = \langle v(x-1)f_2(x), (1-v)(x-1)f_1(x)\rangle$. These four codes are called Duadic codes over $R =$ of length m.*

In the following we give some properties of duadic codes over R. As in the case of duadic codes over finite fields, the properties of duadic codes over R differ for the cases when the splitting is given by μ_{-1} or not (i.e., the polynomials $f_1(x)$ and $f_2(x)$ are self-reciprocal or reciprocals of each other.)

Proposition 4. *With the same assumptions as for Definition 1, the following hold:*

(i) $|D_1| = q^{m+1} = |D_2|$,

(ii) $|C_1| = q^{m-1} = |C_2|$.

Proof. For the (i) Part, we know that $|D_2| = |D_1| = |\langle f_1(x)\rangle||\langle f_2(x)\rangle|$. Hence the result follows.

For the (ii) Part; we know that

$$|C_2| = |C_1| = |\langle (x-1)f_1(x)\rangle||\langle (x-1)f_2(x)\rangle| = q^{\frac{m-1}{2}} q^{\frac{m-1}{2}} = q^{m-1}.$$

□

Proposition 5. *With the same assumptions as for Definition 1, we obtain that: D_1 and C_1 are equivalent to D_2 and C_2 respectively.*

Proof. Let $D_1 = \langle vf_1(x), (1-v)f_2(x)\rangle$ and $D_2 = \langle vf_2(x), (1-v)f_1(x)\rangle$ and $C_1 = \langle v(x-1)f_1(x), (1-v)(x-1)f_2(x)\rangle$ and $C_2 = \langle v(x-1)f_2(x), (1-v)(x-1)f_1(x)\rangle$. Since $\langle f_1(x)\rangle$ is equivalent by multiplier to $\langle f_2(x)\rangle$ and $\langle (x-1)f_1(x)\rangle$ is equivalent by multiplier to $\langle (x-1)f_2(x)\rangle$. By Proposition 1 we have the result. □

Proposition 6. *With the assumption of Definition 1 the following holds*

(i) If the splitting is given by μ_{-1} then C_1 and C_2 are self-orthogonal and $D_1^\perp = C_1$, $D_2^\perp = C_2$,

(ii) If the splitting is not given by μ_{-1} then $D_1^\perp = C_2$, $D_2^\perp = C_1$.

Proof. The proof follows easily from Proposition 2. □

Lemma 4. *[5, Theorem 6.4.12] Let $\langle f_1(x)\rangle$ and $\langle f_2(x)\rangle$ be a pair of odd-like duadic codes of length m over $\mathbb{F}_q$. Assume that*

$$1+\alpha^2 m = 0 \tag{3}$$

has a solution in $\mathbb{F}_q$. Then

(i) If μ_{-1} gives the splitting from $\langle f_1(x)\rangle$ to $\langle f_2(x)\rangle$ then $\widetilde{\langle f_1(x)\rangle}$ and $\widetilde{\langle f_1(x)\rangle}$ are self-dual,

(ii) If the splitting from $\langle f_1(x)\rangle$ to $\langle f_2(x)\rangle$ is not given by μ_{-1} then $\widetilde{\langle f_1(x)\rangle}$ and $\widetilde{\langle f_1(x)\rangle}$ are duals of each other.

Here $\widetilde{\langle f_i(x)\rangle} = \{\widetilde{c} | c \in \langle f_i(x)\rangle for\, 1 \le i \le 2 and\, \widetilde{c} = c_0 \dots c_{m-1} c_\infty with\, c_\infty = -\alpha\Sigma_{i=0}^{m-1} c_i\}$.

Theorem 9. *Let $D_1 = \langle v f_1(x), (1-v) f_2(x)\rangle$ and $D_2 = \langle v f_2(x), (1-v) f_1(x)\rangle$ a pair of odd-like duadic codes over R as given in Definition 1. Assume that*

$$1+\alpha^2 m = 0 \tag{4}$$

has a solution in $\mathbb{F}_q$. Then

(i) If the splitting is given by μ_{-1}, then $\widetilde{D_1} = v\widetilde{\langle f_1(x)\rangle} \oplus (1-v)\widetilde{\langle f_2(x)\rangle}$ and $\widetilde{D_2} = v\widetilde{\langle f_2(x)\rangle} \oplus (1-v)\widetilde{\langle f_1(x)\rangle}$ are self-dual over R,

(ii) If the splitting is not given by μ_{-1}, then $\widetilde{D_1} = v\widetilde{\langle f_1(x)\rangle} \oplus (1-v)\widetilde{\langle f_2(x)\rangle}$ and $\widetilde{D_2} = v\widetilde{\langle f_2(x)\rangle} \oplus (1-v)\widetilde{\langle f_1(x)\rangle}$ are isodual over R.

Proof. For part (i) we observe that since $\widetilde{D_i}^\perp = v\widetilde{\langle f_i(x)\rangle}^\perp \oplus (1-v)\widetilde{\langle f_j(x)\rangle}^\perp$ for $1 \le i, j \le 2$, $i \neq j$, the result follows by Lemma 4.

The result in part (ii) follows from Lemma 4 and Proposition 1. □

Example 1. *Over $\mathbb{F}_5$ we have*

$$x^{11} - 1 = (x+4)(x^5 + x^4 + 4x^3 + 4x^2 + 3x + 1)(x^5 + 4x^4 + 4x^3 + x^2 + 3x + 4).$$

Since $11 \equiv -1 \bmod 4$, *then by Theorem 8 there exists one splitting given by μ_{-1}. The solutions of* (4) *are* $\alpha = \pm 2$. *So*

$$\begin{aligned}\widetilde{D_1} &= v\widetilde{\langle (x^5+x^4+4x^3+4x^2+3x+1)\rangle} \oplus (1-v)\widetilde{\langle (x^5+4x^4+4x^3+x^2+3x+4)\rangle}\\ \widetilde{D_2} &= v\widetilde{\langle (x^5+4x^4+4x^3+x^2+3x+4)\rangle} \oplus (1-v)\widetilde{\langle (x^5+x^4+4x^3+4x^2+3x+1)\rangle}\end{aligned}$$

are self-dual codes of length 12 *over* $R = \mathbb{F}_5 + v\mathbb{F}_5$.

Example 2. *Over $\mathbb{F}_5$ we have*

$$\begin{aligned}x^{29}-1 =&(x+28)(x^{14}+2x^{13}+4x^{12}+4x^{10}+4x^9+3x^8+x^7+3x^6+4x^5+4x^4+4x^2+2x+1)\\ &\times(x^{14}+4x^{13}+4x^{12}+2x^{11}+2x^{10}+4x^9+3x^7+4x^5+2x^4+2x^3+4x^2+4x+1).\end{aligned}$$

Let

$$\begin{aligned}f_1(x) =&x^{14}+2x^{13}+4x^{12}+4x^{10}+4x^9+3x^8+x^7+3x^6+4x^5+4x^4+4x^2+2x+1\\ f_2(x) =&x^{14}+4x^{13}+4x^{12}+2x^{11}+2x^{10}+4x^9+3x^7+4x^5+2x^4+2x^3+4x^2+4x+1.\end{aligned}$$

Since $19 \equiv 1 \bmod 4$*, then by Theorem 8 there exists a splitting witch is not given by* μ_{-1}*. The solution of* (4) *are* $\alpha = \pm 2$*. So* $\widetilde{D_1} = v\widetilde{\langle f_1(x)\rangle} \oplus (1-v)\widetilde{\langle f_2(x)\rangle}$ *and* $\widetilde{D_2} = v\widetilde{\langle f_2(x)\rangle} \oplus (1-v)\widetilde{\langle f_1(x)\rangle}$ *are isodual codes of length* 30 *over* $R = \mathbb{F}_5 + v\mathbb{F}_5$.

5. The Existence of Cyclic Isodual Codes over R

We have seen in Section 3 that the existence of cyclic self-dual codes over R depends on the existence of cyclic self-dual codes over $\mathbb{F}_q$. But by [6] these latter codes do not exist when q is odd. This shows that if q is odd, then there are no cyclic self-dual codes over R. For that in this section, conditions are given on the existence of cyclic isodual codes over R. In the following we give some explicit constructions of monomial isodual cyclic codes over R.

The following Proposition will be useful later.

Proposition 7. *Let C_1 and C_2 be two linear codes of length n over $\mathbb{F}_q$. Then C_1 and C_2 are isodual codes if and only if*

$$C = vC_1 \oplus (1-v)C_2 = \{(vc_1 + (1-v)c_2),\, c_1 \in C_1,\, c_2 \in C_2\}$$

is an isodual code of length n over R.

Proof. The proof is the same as for Proposition 1. □

In [2] we gave several constructions of isodual cyclic codes over finite fields. In the next examples using Proposition 7, the construction of new cyclic codes over R are given.

Example 3. *Over $\mathbb{F}_3$ we have $x^7-1=(x+2)(x^6+x^5+x^4+x^3+x^2+x+1)$. Then*

$$x^{14}-1=(x+2)(x^6+x^5+x^4+x^3+x^2+x+1)(x+1)(x^6-x^5+x^4-x^3+x^2-x+1),$$

and the cyclic codes C_1 and C_2 generated respectively by

$$(x+2)(x^6-x^5+x^4-x^3+x^2-x+1) \text{ and } (x+1)(x^6+x^5+x^4+x^3+x^2+x+1)$$

are isodual. So the cyclic code generated by

$$v(x+2)(x^6-x^5+x^4-x^3+x^2-x+1)+(1-v)(x+1)(x^6+x^5+x^4+x^3+x^2+x+1)$$

is an isodual code over $\mathbb{F}_3+v\mathbb{F}_3$ with minimum Lee weight 4.

Example 4. *For $q = 7$ and $m = 9$, $7 \equiv 1 \mod 3$, so there exist duadic codes generated by f_i, $1 \le i \le 2$. Since $3 \equiv -1 \mod 4$, by Theorem 8 all splittings are given by μ_{-1}, and we have*

$$(x^9 - 1) = (x-1)(x+3)(x+5)(x^3+3)(x^3+5),$$

so that $f_1(x) = (x+3)(x^3+3)$ and $f_2(x) = (x+5)(x^3+5)$. Thus

$$(x^9 - 1) = (x-1)f_1(x)f_2(x) = (x-1)f_1(x)f_1^*(x),$$

and the cyclic codes of length 18 over $\mathbb{F}_7$ generated by $(x-1)f_i(x)f_i(-x)$ and $(x-1)f_j(x)f_j(-x)$ are isodual over $\mathbb{F}_7$. So the cyclic codes generated by

$$v(x-1)f_i(x)f_i(-x) + (1-v)(x-1)f_j(x)f_j(-x)$$

is an isodual code over $\mathbb{F}_7 + v\mathbb{F}_7$ with minimum Lee weight 5.

We complete this section by giving some more examples in Table 1 where C is an isodual cyclic code of length $2n$ over $\mathbb{F}_p + v\mathbb{F}_p$ with generator polynomial

$$g(x) = v(x-1)f_1(x)f_1(-x) + (1-v)(x+1)f_2(x)f_2(-x)$$

and a polynomial $f(x) = a_0 + a_1x + \ldots + a_mx^m$ is abbreviated as $a_0a_1\ldots a_m$.

Table 1: Isodual Cyclic Codes of Length $2n$ over $\mathbb{F}_p + v\mathbb{F}_p$

n	p	f_1	f_2	$\varphi(C)$
11	3	221201	201211	$[44,22,9]_3$
23	3	222110202001	200101022111	$[92,46,15]_3$
11	5	411421	431441	$[44,22,9]_5$
19	5	4424222301	4023331321	$[76,38,13]_5$

5.1. Construction of Self-dual and Isodual Codes over $\mathbb{F}_{2^r} + v\mathbb{F}_{2^r}$

Theorem 10. *[2, Theorem 4.16] Let $n = 2^a m$ with m an odd integer such that and $D_i = \langle f_i(x)\rangle$, $1 \le i \le 2$ be duadic codes over $\mathbb{F}_{2^r}$. Then for $1 \le i \le 2$, the cyclic codes generated by*

$$f_i(x) = (x-1)^{2^{a-1}} f_i^{2^a}(x),$$

are self-dual or isodual.

Theorem 11. *Let $n = 2^a m$ with m an odd integer such that and $D_i = \langle f_i(x)\rangle$, $1 \le i \le 2$ be duadic codes over $\mathbb{F}_{2^r}$. Then for $1 \le i \le 2$, the cyclic codes over $\mathbb{F}_{2^r} + v\mathbb{F}_{2^r}$ generated by*

$$f(x) = v(x-1)^{2^{a-1}} f_i^{2^a}(x) + (1-v)(x-1)^{2^{a-1}} f_j^{2^a}(x),$$

are self-dual or isodual.

Proof. If the splitting is given by μ_{-1} then the cyclic codes generated respectively by $(x-1)^{2^{a-1}}f_1^{2^a}(x)$ and $(x-1)^{2^{a-1}}f_2^{2^a}(x)$ are self-dual over $\mathbb{F}_{2^r}$ thus $f(x)$ generate a self-dual cyclic code over $\mathbb{F}_{2^r}+v\mathbb{F}_{2^r}$.

If the splitting is not given by μ_{-1} then the cyclic codes generated respectively by $(x-1)^{2^{a-1}}f_1^{2^a}(x)$ and $(x-1)^{2^{a-1}}f_2^{2^a}(x)$ are isodual over $\mathbb{F}_{2^r}$ thus $f(x)$ generate an isodual cyclic code over $\mathbb{F}_{2^r}+v\mathbb{F}_{2^r}$. □

Example 5. *Let $n=34$ and $q=2$, so that $m=17$ and $17\equiv 1 \bmod 8$. Then duadic codes of length 17 over $\mathbb{F}_2$ exist. The factorization of $x^{34}-1$ over $\mathbb{F}_2$ is*

$$(x-1)^2(x^8+x^5+x^4+x^3+1)^2(x^8+x^7+x^6+x^4+x^2+x+1)^2.$$

Since $17\equiv 1 \pmod 4$, $x^8+x^5+x^4+x^3+1$ is not the reciprocal polynomial of $x^8+x^7+x^6+x^4+x^2+x+1$, thus

$$C_1=\langle (x-1)(x^8+x^7+x^6+x^4+x^2+x+1)\rangle,$$

and

$$C_2=\langle (x-1)(x^8+x^5+x^4+x^3+1)\rangle,$$

are isodual cyclic codes of length 34 over $\mathbb{F}_2$. While the cyclic code $C=vC_1+(1-v)C_2$ is isodual over $\mathbb{F}_2+v\mathbb{F}_2$.

Example 6. *For $n=14$, $x^{14}-1=(x-1)^2(x^3+x+1)^2(x^3+x^2+1)^2$, over $\mathbb{F}_2$. Since $ord_7(2)=3$ is odd, x^3+x+1 is the reciprocal polynomial of x^3+x^2+1. Then*

$$C_1=\langle (x-1)(x^3+x+1)\rangle,$$

and

$$C_2=\langle (x-1)(x^3+x^2+1)\rangle,$$

are self-dual cyclic codes of length 14 over $\mathbb{F}_2$. and the cyclic code $C=vC_1+(1-v)C_1$ is self-dual over $\mathbb{F}_2+v\mathbb{F}_2$.

5.1.1. Construction of Self-dual and Isodual Codes over $\mathbb{F}_2+v\mathbb{F}_2$

Let $x=(x_1,x_2,\dots,x_n)$ and $y=(y_1,y_2,\dots,y_n)$ be two elements of $(F_2+vF_2)^n$. The Hermitian inner product is defined as $\langle x,y\rangle_H=\sum x_i\overline{y_i}$ where $\overline{0}=0$, $\overline{1}=1$, $\overline{v}=1+v$ and $\overline{1+v}=v$. The dual $C_H^{\perp}$ with respect to the Hermitian inner product of $C$is defined as

$$C_H^{\perp}=\{x\in(\mathbb{F}_{2^r}+v\mathbb{F}_{2^r})\,|\,\langle x,y\rangle_H=0 \text{ for all } y\in C\}$$

C is Hermitian self-dual if $C=C_H^{\perp}$.

Proposition 8. *[1] If $C=(1+v)C_1\oplus vC_2$ then C is Euclidean self-dual if and only if C_1 and C_2 are binary self-dual codes. $C=(1+v)C_1\oplus vC_2$ is Euclidean Type IV self-dual if and only if $C_1=C_2$.*

Proposition 9. *[1] If $C = (1+v)C_1 \oplus vC_2$ then C is Hermitian self-dual if and only if $C_1 = C_2^{\perp}$. $C = (1+v)C_1 \oplus vC_2$ is Hermitian Type IV self-dual if and only if C_1 and $C_1^{\perp}$ are even codes.*

Theorem 12. *Let $n = 2^a m$ with m an odd integer such that and $D_i = \langle f_i(x)\rangle$, $1 \le i \le 2$ be duadic codes over $\mathbb{F}_2$. Then for $1 \le i \le 2$, the cyclic codes over $R_2 = \mathbb{F}_2 + v\mathbb{F}_2$ generated by*

$$f(x) = v(x-1)^{2^{a-1}} f_i^{2^a}(x) + (1-v)(x-1)^{2^{a-1}} f_j^{2^a}(x),$$

are Euclidean self-dual or Hermitian self-dual codes.

Proof. If the splitting is given by μ_{-1} then the cyclic codes generated respectively by $(x-1)^{2^{a-1}} f_1^{2^a}(x)$ and $(x-1)^{2^{a-1}} f_2^{2^a}(x)$ are self-dual over $\mathbb{F}_2$. Thus $f(x)$ generates a Euclidean self-dual cyclic code over $\mathbb{F}_2 + v\mathbb{F}_2$.

If the splitting is not given by μ_{-1}then the cyclic codes generated respectively by $(x-1)^{2^{a-1}} f_1^{2^a}(x)$ and $(x-1)^{2^{a-1}} f_2^{2^a}(x)$ are dual of each other over $\mathbb{F}_q$. Then by Proposition 8 $f(x)$ generates a Hermitian self-dual cyclic code over $\mathbb{F}_2 + v\mathbb{F}_2$. □

6. Formally Self-dual Codes over R

Formally self-dual codes are an interesting family of codes. Especially the binary near extremal formally self-dual (f.s.d.) codes have been studied extensively. For more detail we refer the reader to [4, 7, 8] and the references therein. Recently, Karadeniz et al. gave constructions for f.s.d. codes by using circulant matrices in [7]. By using the constructions over a family of binary rings; R_k they were able to obtain f.s.d. codes such as $[72,36,14]_2$, $[72,36,13]_2$ and $[44,22,10]_2$ which have better distances than the best known self-dual codes of the corresponding lengths.

In this section, we generalize two of their constructions which lead to the good computational results mentioned above. Instead of circulant matrices we use λ-circulant matrices and state that double λ-circulant and bordered double λ-circulant codes generates f.s.d. codes over the rings which satisfy $wt(a) = wt(-a)$ for any element a of the ring. We were able to obtain f.s.d. codes with parameters $[32,16,11]_5$, $[32,16,10]_3$, $[20,10,7]_3$, $[8,4,4]_3$ and many examples with the distance of the best known linear code of the same parameters. The results are tabulated in Tables 2 and 3.

An $n \times n$ square matrix M is called λ-circulant if it is in the following form;

$$M = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ \lambda a_n & a_1 & a_2 & \cdots & a_{n-1} \\ \lambda a_{n-1} & \lambda a_n & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda a_2 & \lambda a_3 & \lambda a_4 & \cdots & a_1 \end{pmatrix}.$$

For $\lambda = 1$ the matrix is circulant and there is a vast literature on double circulant and bordered double circulant self-dual codes. In the sequel, let S to be a commutative ring with identity and the weight used satisfies $wt(a) = wt(-a)$ for any element $a \in R$. The constructions are given in the following theorems.

Theorem 13. *[Construction A] Let M be an $n \times n$ λ-circulant matrix then the code generated by $G = \left[\begin{array}{c|c} I_n & M \end{array}\right]$ is a formally self-dual code over R.*

Proof. Let C be the code generated by G and C' be the code generated by $G' = \left[\begin{array}{c|c} M^T & -I_n \end{array}\right]$. It is easily observed that the codes C and C' are orthogonal to each other. Since they both have free rank n and length $2n$ we have $C^{\perp} = C'$. Let C'' be the code generated by $G'' = \left[\begin{array}{c|c} M^T & I_n \end{array}\right]$. Since $wt(a) = wt(-a)$ for any a in R the codes C' and C'' have the same weight enumerator. In order to conclude that C is formally self-dual it is enough to show that C'' is equivalent to C. Let σ be the permutation

$$\sigma = (1, n)(2, n-1)\ldots(k-1, n-k+2)(k, n-k+1)$$

where $k = \lfloor n/2 \rfloor$ and M' be the matrix obtained by applying σ on rows of M and let M'' be the matrix obtained by applying σ on columns of M'. We observe that $M'' = M^T$. Hence, M and M^T are equivalent. Similarly, by applying necessary column permutation we observe G and G'' are equivalent. So, C and C'' are equivalent and therefore C is formally self-dual. □

Theorem 14 (Construction B)**.** *Let M be an $n \times n$ λ-circulant matrix then the code generated by*

$$G^* = \left[\begin{array}{c|cccc} & \alpha & \beta & \cdots & \beta \\ & \beta & & & \\ I_{n+1} & \vdots & & M & \\ & \beta & & & \end{array}\right]$$

is a formally self-dual code over R.

Proof. The proof is analogous to that of the Theorem 13 and therefore is skipped. □

Remark 3. *Note that if R is a ring of characteristic 2 then the constructions give isodual codes.*

Example 7. *Let $S = \mathbb{F}_3 + v\mathbb{F}_3$ and $\lambda = 1 + v$ and $n = 5$ and M be the following λ-circulant matrix*

$$M = \begin{pmatrix} 0 & 1+2v & 2v & 2 & 2 \\ 2+2v & 0 & 1+2v & 2v & 2 \\ 2+2v & 2+2v & 0 & 1+2v & 2v \\ v & 2+2v & 2+2v & 0 & 1+2v \\ 1+2v & v & 2+2v & 2+2v & 0 \end{pmatrix}$$

then $G = \left[\begin{array}{c|c} I_5 & M \end{array}\right]$ generates a formally self-dual code of length 10 over $\mathbb{F}_3 + v\mathbb{F}_3$ and the Gray image of the code is a $[20, 10, 7]_3$ f.s.d. code which has a better distance than the best possible self-dual code and also optimal as a linear code. The code has partial Lee weight distribution $1 + 240z^7 + 780z^8 + \ldots$ and an automorphism group of order 40.

The computational results for Constructions A and B are given in Tables 2 and 3 where in order to save space the element $x + yv$ is abbreviated as xy, the elements for the first row of M are separated by | and A_d denotes the number of codewords with minimum weight. We use $*$ to indicate that the code is optimal as a linear code and similarly b indicates that the code has the best known distance among the linear codes of these parameters, according to the online database in [3].

Remark 4. *Note that the codes with parameters* $[32,16,11]_5$, $[32,16,10]_3$ *and* $[20,10,7]_3$ *in Tables 2 and 3 have better minimum distances than the best known self-dual codes for these parameters.*

Table 2: Good formally self-dual codes by Construction A

p	n	λ	First row of M	$\varphi(C)$	$\lvert Aut\rvert$	A_d
3	5	1	(22|10|20|01|21)	$[20,10,7]_3^*$	20	200
3	7	$1-2v$	(21|01|02|11|11|10|10)	$[28,14,9]_3^b$	28	924
3	8	$1-2v$	(22|01|02|22|21|12|01|01)	$[32,16,10]_3^b$	64	2208
3	11	1	(11|11|21|02|01|20|22|12|22|12|10)	$[44,22,11]_3$	44	2948
5	5	$1-2v$	(03|14|33|42|34)	$[20,10,8]_5^*$	40	1000
5	6	$1-2v$	(23|32|01|31|11|21)	$[24,12,9]_5^b$	48	1536
5	7	$1-2v$	(44|31|20|11|23|21|32)	$[28,14,10]_5$	56	1876
5	8	$1-2v$	(42|00|42|11|22|30|11|14)	$[32,16,11]_5^b$	64	3136
5	8	$1-2v$	(00|22|42|10|44|31|10|32)	$[32,16,11]_5^b$	64	3584
5	8	$1-2v$	(01|02|10|32|30|31|12|34)	$[32,16,11]_5^b$	64	3776
5	8	1	(32|13|12|20|11|12|23|32)	$[32,16,11]_5^b$	64	3328
5	8	1	(34|03|33|40|12|21|00|02)	$[32,16,11]_5^b$	64	3264
5	9	$1-2v$	(11|30|32|42|23|43|40|10|04)	$[36,18,12]_5^b$	72	4788
5	11	$1-2v$	(13|32|43|12|23|23|34|13|43|30|43)	$[44,22,13]_5^b$	88	1056
5	12	$1-2v$	(11|00|23|22|44|32|43|23|31|03|00|42)	$[48,24,14]_5$	96	1632
5	13	$1-2v$	(02|13|33|03|24|02|24|42|14|30|04|43|24)	$[52,26,15]_5^b$	104	3328
5	13	$1+v$	(40|03|24|02|43|32|34|13|13|33|34|42|04)	$[52,26,15]_5^b$	104	2912
5	13	$1+v$	(12|40|00|13|32|31|11|44|03|42|03|03|24)	$[52,26,15]_5^b$	104	3224
7	6	$1-2v$	(60|31|24|64|55|50)	$[24,12,9]_7$	72	504
7	7	$1-2v$	(52|04|03|26|15|56|62)	$[28,14,10]_7$	84	168
7	9	1	(03|00|33|02|15|53|65|50|06)	$[36,18,12]_7$	108	1458
7	10	$1-2v$	(03|15|32|34|06|51|44|10|63|54)	$[40,20,13]_7$	120	1920
7	11	$1-2v$	(43|63|22|11|61|26|06|60|25|14|26)	$[44,22,14]_7$	132	924

Table 3: Good formally self-dual codes by Construction B

p	n	λ	First row of M	$\alpha \mid \beta$	$\varphi(C)$	$\lvert Aut \rvert$	A_d
3	4	$1+v$	(11|12|00|02)	11|11	$[20,10,6]_3$	4	48
3	5	1	(02|02|20|12|20)	12|20	$[24,12,8]_3$	40	458
3	6	$1+v$	(00|21|21|22|10|00)	22|22	$[28,14,8]_3$	4	210
3	7	1	(02|01|22|22|00|12|00)	11|22	$[32,16,9]_3$	28	340
3	9	1	(02|21|20|02|10|10|20|12|12)	20|10	$[40,20,11]_3$	36	1232
3	10	1	(00|01|11|01|00|20|22|11|12|22)	02|22	$[44,22,11]_3$	40	280
5	4	$1+v$	(01|11|10|20)	11|22	$[20,10,7]_5$	8	112
5	5	1	(12|10|00|10|22)	20|11	$[24,12,9]_5$	40	1696
5	6	1	(00|20|12|22|10|11)	20|11	$[28,14,10]_5$	48	1632
5	7	1	(21|01|11|22|11|20|20)	01|11	$[32,16,11]_5^b$	56	3152
5	8	$1-2v$	(01|10|01|21|00|00|22)	12|20	$[36,18,11]_5$	8	456
5	10	$1+v$	(14|22|14|14|44|13|34|33|43|14)	34|30	$[44,22,12]_5$	8	144
5	11	$1-2v$	(13|20|24|40|01|44|00|14|12|04|00)	33|31	$[48,24,13]_5$	3	232
5	12	$1-2v$	(14|40|32|23|01|22|22|31|13|33|34|30)	24|31	$[52,26,14]_5$	8	320
7	5	$1-2v$	(06|65|35|21|62)	24|21	$[24,12,9]_7$	12	900
7	6	$1-2v$	(44|06|60|03|45|54)	35|53	$[28,14,10]_7$	12	1110
7	8	1	(06|54|16|05|36|63|01|35)	16|44	$[36,18,12]_7$	96	1320
7	8	$1-2v$	(53|51|60|45|32|30|53|61)	42|45	$[36,18,12]_7$	96	1536

ACKNOWLEDGEMENTS The authors wish to thank the anonymous referees for their useful comments and suggestions.

References

[1] C. Bachoc. *Application of coding theory to the construction of modular lattices*, Journal of Combinatorial Theory Series:A, 78, 92–119. 1997.

[2] A. Batoul, K. Guenda and T.A. Gulliver. *On Isodual Cyclic Codes over Finite Fields and Finite Chain Rings: Monomial Equivalence*, arXiv:1303.1870v1, 2013.

[3] M. Grassl. *Bounds on the minimum distance of linear and quantum codes*, Online available at: www.codetables.de (accessed on 29.04.2014).

[4] S. Han and J-L. Kim. *The non-existence of near extremal formally self-dual codes*, Designs, Codes and Cryptography, 51, 69-77. 2009.

[5] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*, Cambridge University Press, New York, NY, 2003.

[6] Y. Jia, S. Ling and C. Xing. *On Self-dual cyclic codes over finite fields*, IEEE Transactions on Information Theory, 57(4), 2243–2251. 2011.

[7] S. Karadeniz, S. T. Dougherty and B. Yildiz. *Constructing Formally Self-dual codes over R_k*, Discrete Applied Mathematics, 167(1), 188-196. 2014.

[8] J-L. Kim, V. Pless. *A note on formally self-dual even codes of length divisible by 8*, Finite Fields and Applications, 13(2), 224–229. 2007.

[9] P. Langevin. *Duadic $\mathbb{Z}_4$-Codes*, Finite Fields and Applications, 6, 309–326. 2000.

[10] J S. Leon, J. M. Masley and V. Pless. *Duadic codes*, IEEE Transactions on Information Theory, 30, 709–714. 1984.

[11] S. Ling and P. Solé. *Duadic Codes over $F_2 + uF_2$*, Applicable Algebra in Engineering, Communication and Computing, 12(5), 365–379. 2001.

[12] J. J. Rushanan. *Duadic codes and difference sets*, Journal of Combinatorial Theory Series: A, 57, 254–261. 1991

[13] N. J. A. Sloane and J. G. Thompson. *Cyclic self-dual codes*, IEEE Transactions on Information Theory, 29, 364–366. 1983.

[14] M. H. M. Smid. *Duadic codes*, IEEE Transactions on Information Theory, 33(3), 432–433. 1987.

[15] J. Wood. *Duality for modules over finite rings and applications to coding theory*, American Journal of Mathematics, 121, 555–575. 1999.

[16] S. X. Zhu and L. Wang. *A class of constacyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$ and its Gray image*, Discrete Mathematics, 311, 2677–2682. 2011.

[17] S. X. Zhu, Y. Wang and M. J. Shi. *Some results on cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$*, IEEE Transactions on Information Theory, 56(4), 1680–1684. 2010.