Bull. Korean Math. Soc. **54** (2017), No. 4, pp. 1111–1122
https://doi.org/10.4134/BKMS.b150764
pISSN: 1015-8634 / eISSN: 2234-3016

CYCLIC AND CONSTACYCLIC SELF-DUAL CODES OVER R_k

Suat Karadeniz, Ismail Gokhan Kelebek, and Bahattin Yildiz

Abstract. In this work, we consider constacyclic and cyclic self-dual codes over the rings R_k. We start with theoretical existence results for constacyclic and cyclic self-dual codes of any length over R_k and then construct cyclic self-dual codes over $R_1 = \mathbb{F}_2 + u\mathbb{F}_2$ of even lengths from lifts of binary cyclic self-dual codes. We classify all free cyclic self-dual codes over R_1 of even lengths for which non-trivial such codes exist. In particular we demonstrate that our constructions provide a counter example to a claim made by Batoul et al. in [1] and we explain why their claim fails.

1. Introduction

Both cyclic codes and self-dual codes over different alphabets have been the focus of many works related to coding theory for a long time now. Cyclic codes have a rich algebraic structure, making them relatively easier to study and to encode and decode. Self-dual codes have a combinatorial aspect which makes them quite popular as well as connections with several fields such as lattices, invariant theory, cryptography and designs.

Starting with [16], a combination of these two structures has become something of interest to study by researchers. In [3], a complete classification of cyclic self-dual codes of odd lengths over the ring $\mathbb{F}_2 + u\mathbb{F}_2$ was given. Researchers have considered the same problem over different fields and rings in [1], [2], [6], [15].

In this work, we consider constacyclic and cyclic self-dual codes over R_k, the family of rings introduced in [9], that extends such rings as $R_1 = \mathbb{F}_2 + u\mathbb{F}_2$ and $R_2 = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. Being a family of Frobenius rings ([17]), they have been studied quite extensively from many different angles; see [8], [9], [10], [13], [18] for more.

Received September 17, 2015; Accepted January 14, 2016.
2010 *Mathematics Subject Classification.* Primary 94B05, 94B99; Secondary 11T71, 13M99.
Key words and phrases. cyclic codes, constacyclic codes, cyclic self-dual codes, lift, projection.

The main motivation for the current work is twofold: First we consider a theorem in [2] in which it was stated that a necessary condition for a λ-constacyclic self-dual code over $\mathbb{F}_q$ to exist is that $\lambda^2 = 1$. Since in R_k, all units satisfy this property, our first goal was to determine whether λ-constacyclic self-dual codes over R_k of all lengths exist for all units $\lambda \in R_k$. The second is that since cyclic self-dual codes over R_1 of odd lengths were classified completely, and binary cyclic self-dual codes up to certain lengths were characterized in [11], we considered cyclic self-dual codes over R_1 of even lengths. In doing so we introduced the notion of independence in R_k and laid down the theoretical background on lifting binary cyclic self-dual codes to cyclic self-dual codes over R_1 (and R_k in general). Using lifts of binary cyclic self-dual codes were able to classify all free cyclic self-dual codes over R_1 of even lengths for which non-trivial such codes exist. In due process we obtained many good cyclic self-dual codes over R_1 from such lifts, providing a counter example to a claim by Batoul et al. in [1] (Theorem 4.14) in which they claimed that a self-dual code of even length over a finite chain ring with residue field $\mathbb{F}_2$ cannot be the lift of a binary self-dual cyclic code.

The rest of the work is organized as follows. Section 2 contains the preliminaries about the rings R_k, self-dual, cyclic and constacyclic codes. In Section 3 we settle the question of existence of cyclic and constacyclic codes over R_k of any length. In Section 4 we consider the projections, lifts and independence in R_k, laying the ground for computational results. Section 5 contains the computational results and examples; in particular it contains tables of good cyclic self-dual codes of certain even lengths over the ring R_1, obtained from lifts of binary cyclic self-dual codes. We finish with a remark on the claim in [1] we have disproved and explain why the claim fails.

2. Preliminaries

The family of rings denoted by R_k have been introduced in [9]. Leaving the details of these rings to the aforementioned work, we recall some of the basic properties, the proofs of which can be found in [9]. For $k \geq 1$, let

$$R_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/\langle u_i^2 = 0, u_i u_j = u_j u_i \rangle. \tag{2.1}$$

We actually take $R_0 = \mathbb{F}_2$, the binary field. The basis elements of R_k can be viewed, using subsets $A \subseteq \{1, 2, \ldots, k\}$ by letting

$$u_A := \prod_{i \in A} u_i \tag{2.2}$$

with the convention that $u_\emptyset = 1$. Then any element of R_k can be represented as

$$\sum_{A \subseteq \{1,\ldots,k\}} c_A u_A, \qquad c_A \in \mathbb{F}_2. \tag{2.3}$$

The ring R_k is a local ring with maximal ideal $\langle u_1, u_2, \ldots, u_k\rangle$ and $|R_k| = 2^{(2^k)}$. It is neither a principal ideal ring nor a chain ring when $k \geq 2$, but is a Frobenius ring for all $k \geq 0$.

An element of R_k is a unit if and only if the coefficient of $u_\emptyset$ is 1 and each unit is also its own inverse. We also have the following:

$$\forall a \in R_k \quad a^2 = \begin{cases} 1 & \text{if } a \text{ is a unit} \\ 0 & \text{otherwise.} \end{cases} \tag{2.4}$$

A linear code of length n over R_k is defined to be an R_k-submodule of R_k^n.

We attach the usual inner product on this ambient space R_k^n, that is $\langle \overline{a}, \overline{b}\rangle_k = \sum a_i b_i$. The dual $C^\perp$ is defined as $C^\perp = \{\overline{y} \in R_k^n \mid \langle \overline{y}, \overline{x}\rangle_k = 0 \text{ for all } \overline{x} \in C\}$. We say that a code is self-orthogonal if $C \subseteq C^\perp$ and self-dual if $C = C^\perp$.

We define the Gray map inductively, extending it naturally from the Gray map on R_1 from [7] as follows.

For $\overline{c} \in R_k^n$, write $\overline{c} = \overline{c}_1 + u_k\overline{c}_2$ with $\overline{c}_1, \overline{c}_2 \in R_{k-1}^n$, then we can define

$$\phi_k(\overline{c}) = (\phi_{k-1}(\overline{c}_2), \phi_{k-1}(\overline{c}_1) + \phi_{k-1}(\overline{c}_2))\,,$$

with ϕ_0 being the identity map on $\mathbb{F}_2$. For example on R_1 we have $\phi_1(\overline{c}_1 + u\overline{c_2}) = (\overline{c}_2, \overline{c}_1 + \overline{c}_2)$ and on R_2,

$$\phi_2(\overline{a} + u\overline{b} + v\overline{c} + uv\overline{d}) = (\overline{d}, \overline{c} + \overline{d}, \overline{b} + \overline{d}, \overline{a} + \overline{b} + \overline{c} + \overline{d}).$$

The Lee weight w_L of a codeword is the Hamming weight of the image of the codeword under ϕ_k. Then the Gray map is a linear weight preserving map from R_k^n to $\mathbb{F}_2^{n2^k}$.

If all the codewords of a self-dual code have doubly-even Lee weight, then the code is said to be Type II, otherwise it is said to be Type I. The following lemma from [10] shows that the Gray map is duality-preserving:

Lemma 2.1. *If C is a self-dual code over R_k of length n, then $\phi_k(C)$ is a binary self-dual code of length $2^k n$. The Lee weight distribution of C and the Hamming weight distribution of $\phi_k(C)$ are the same. In particular, if C is Type I, then so is $\phi_k(C)$ and the same is true for Type II codes as well.*

A cyclic shift on R_k^n is a permutation τ such that

$$\tau(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0, c_1, \ldots, c_{n-2}). \tag{2.5}$$

A linear code C over R_k of length n is said to be a cyclic code if it is invariant under the cyclic shift, i.e., $\tau(C) = C$.

For a unit $\lambda \in R_k$, the λ-constacyclic shift on R_k^n is the map

$$\tau_\lambda(c_0, c_1, \ldots, c_{n-1}) = (\lambda c_{n-1}, c_0, c_1, \ldots, c_{n-2}). \tag{2.6}$$

A linear code C over R_k of length n is said to be a λ-constacyclic code if it is invariant under the constacyclic shift, i.e., $\tau_\lambda(C) = C$.

Using the natural polynomial representation of codewords over R_k in $R_k[x]$, that is representing the vector $(a_0, a_1, \ldots, a_{n-1})$ by the polynomial $\sum a_i x^i$, we see that for a codeword $\overline{c} \in R_k^n$, $\tau(\overline{c})$ corresponds to $xc(x)$ in $R_k[x]/(x^n - 1)$,

whereas $\tau_\lambda(\overline{c})$ corresponds to $xc(x)$ in $R_k[x]/(x^n - \lambda)$. The following then is clearly a characterization of constacyclic and cyclic codes over R_k:

Proposition 2.2. *A subset C of R_k^n is a linear cyclic code of length n over R_k if and only if its polynomial representation is an ideal of the ring $\mathcal{R}_{k,n} := R_k[x]/(x^n - 1)$. C is λ-constacyclic if and only if it corresponds to an ideal in $\mathcal{R}_{k,n,\lambda} := R_k[x]/(x^n - \lambda)$.*

The binary image of a cyclic code over R_k is equivalent to a quasi-cyclic code by the following theorem from [8]:

Theorem 2.3. *Let C be a cyclic code of length n over R_k. Then $\phi_k(C)$ is equivalent to a binary quasi-cyclic code of length $2^k n$ and index 2^k.*

3. The existence of cyclic and constcyclic self-dual codes over R_k

We begin with the following theorem:

Theorem 3.1. *Let R be a finite commutative Frobenius ring. Assume that self-dual codes of length 1 exist over R. Then cyclic self-dual codes of all lengths exist over R.*

Proof. Assume that $r \in R$ generates a self-dual code of length 1. Then the direct sum of the length 1 code, i.e., the code generated by the matrix $r \cdot I_n$ is a cyclic self-dual code over R of length n. □

Now, since in R_k, u_i generates a self-dual code of length 1 for all $i = 1, 2, \ldots, k$ we have the following corollary:

Corollary 3.2. *Cyclic self-dual codes of all lengths exist over R_k, for all $k \geq 1$.*

The following theorem from [2] describes the duals of constacyclic codes over rings:

Theorem 3.3 ([2, Theorem 1])**.** *Let R be a ring and λ a unit in R. Then the dual of a λ-constacyclic code over R is λ^{-1}-constacyclic.*

The theoretical consequence of this theorem is that in R_k, where each unit λ satisfies $\lambda^2 = 1$, self-dual constacyclic codes might exist. But in fact it is easy to see that since $\langle u_i \rangle$ and $\langle \lambda u_i \rangle$ are the same self-dual code of length 1, Corollary 3.2 can easily be extended to λ-constacyclic codes for any unit $\lambda \in R_k$:

Corollary 3.4. *Let λ be any unit in R_k. Then λ-constacylic self-dual codes over R_k of any length n exist.*

In [13], it was shown that when n is odd, the map that takes x to $(1 + v)x$ establishes a ring isomorphism between the quotient rings $R_2[x]/(x^n - 1)$ and $R_2[x]/(x^n - (1 + v))$ resulting in the statement that cyclic codes of odd length are isomorphic to $(1 + v)$-constacyclic codes of the same length. The idea used in the proof can easily be generalized without much change to include any unit λ such that $\lambda^2 = 1$ and any commutative Frobenius ring of characteristic 2. In

particular, since every unit λ in R_k satisfies $\lambda^2 = 1$, we can extend the result to all λ-constacyclic codes over R_k. What remains is to mention orthogonality. But since $\lambda^2 = 1$, we have $(\lambda r_1)(\lambda r_2) = r_1 r_2$ for all $r_1, r_2 \in R_k$ and any unit $\lambda \in R_k$. Thus we have proven the following theorem:

Theorem 3.5. *Suppose n is odd and λ is any unit in R_k. Then the map $x \mapsto \lambda x$ establishes an isomorphism between cyclic self-dual codes of length n over R_k and λ-constacyclic self-dual codes over R_k of the same length.*

We will actually say something more about constacyclic codes for particular units. The subgroup $\mathcal{U}_b = \langle 1+u_1, 1+u_2, \ldots, 1+u_k \rangle$ of the unit group of R_k is called the subgroup of *basic units*. In [9], it is shown that multiplying by basic units corresponds to a permutation of coordinates in the Gray image, thus we have the following lemma:

Lemma 3.6 (Lemma 2.1 in [12])**.** (1) *The Lee weight of each basic unit is* 1*. In fact, any element in R_k of Lee weight* 1 *must be a basic unit.*

(2) *If for $\alpha, \beta \in R_k$, we have $\alpha = r \cdot \beta$ for some $r \in \mathcal{U}_b$, then $w_L(\alpha) = w_L(\beta)$.*

Thus in the case of basic units we can say something more:

Theorem 3.7. *Suppose n is odd and λ is a basic unit in R_k. Assume that C is a cyclic self-dual code of length n over R_k. Then applying the map $x \mapsto \lambda x$ to elements of C, we obtain a λ-constacyclic self-dual code $\tilde{C}$ of length n over R_k. Moreover, the Lee weight distribution of C and $\tilde{C}$ are the same.*

We finish this section with the construction for a family of cyclic and constacyclic self-dual codes over R_k of minimum Lee weight 4, for $k \geq 2$.

Theorem 3.8. *For $n \geq 2$, the polynomial whose coefficient vector is the length n vector $(u, v, v, \ldots, v)$ generates a cyclic self-dual code over R_2 of minimum Lee weight* 4*. In fact the polynomial with coefficients $(u_i, u_j, u_j, \ldots, u_j)$, $i \neq j$ also generates a cyclic self-dual code of minimum Lee weight* 4 *over R_k for all $k \geq 2$.*

Proof. The proof will be done for the case when $k = 2$. The same ideas can be used to extend the proof for the general case as well. Now, let C be the code generated over R_2 by the vector $\overline{c} = (u, v, v, \ldots, v)$ and all its cyclic shifts. Note that $\langle \tau^i(\overline{c}), \tau^j(\overline{c}) \rangle = 2uv + (n-2)v^2 = 0$ for all i, j with $i \neq j$ and it is equal to $u^2 + (n-1)v^2 = 0$ if $i = j$. So, we easily see that C is self-orthogonal. Then, since R_2 is Frobenius, we must have $|C| \cdot |C^\perp| = 16^n$. Self-orthogonality of C implies that $C \subseteq C^\perp$, which implies $|C| \leq |C^\perp|$. Putting this into the equation above, we get

$$|C| \leq 4^n. \tag{3.1}$$

Now consider, the set

$$S = \{\overline{c}, \tau(\overline{c}), \ldots, \tau^{n-1}(\overline{c}), v \cdot \overline{c}, v \cdot \tau(\overline{c}), \ldots, v \cdot \tau^{n-1}(\overline{c})\}.$$

It is clearly seen that S is an independent set over $\mathbb{F}_2$. Since C is linear over R_2, all $\mathbb{F}_2$-linear combinations of vectors in S belong to C. This means we have

$$|C| \geq 2^{2n} = 4^n. \tag{3.2}$$

Now, combining (3.1) and (3.2) we get $|C| = 4^n = |C^\perp|$. Thus C must be a cyclic self-dual code. Note that $v \cdot \overline{c}$ has Lee weight 4 and it is easy to see that there is no codeword of weight 2. Thus the minimum weight is 4. In fact more can be said when n is even. Note that in that case the generators in S have weights divisible by 4, which means that the cyclic self-dual code of even length obtained in this way is a Type II code. □

Remark 3.9. For the R_2-case, the previous result can easily be extended to $(1 + uv)$-constacyclic self-dual codes as well. In general, it can be extended to $(1 + u_i u_j)$-constacyclic self-dual codes.

Corollary 3.10. *Putting $n = 2, 3, 4, 5$ in the theorem, thus taking (u, v), (u, v, v), (u, v, v, v) and (u, v, v, v, v) as the base vectors, we obtain Type II extremal binary self-dual codes of lengths* 8 *and* 16 *and Type I extremal binary self-dual codes of length* 12 *and* 20 *from both cyclic and constacyclic self-dual codes over R_2.*

4. Projections, lifts and independence

Let $\mu_k : R_k \to \mathbb{F}_2$ be defined as the projection modulo $\langle u_1, u_2, \ldots, u_k \rangle$. Then μ_k preserves orthogonality and cyclicity. We will need notions of *independence* over the ring R_k and free codes. By a free code over R_k we mean a code that is generated as a free R_k-module with a basis. The row operations and the properties of the ring R_k implies that any free code over R_k can be brought to an equivalent form where it is generated by the rows of the matrix $[I_m|A]$, with I_m denoting the $m \times m$ identity matrix. Let's start with the following definition:

Definition 4.1. Let $S = \{\overline{c}_1, \overline{c}_2, \ldots, \overline{c}_m\}$ be a set of vectors in R_k^n. We say that S is linearly independent over R_k if $\alpha_1\overline{c}_1 + \cdots + \alpha_m\overline{c}_m = 0$ with $\alpha_i \in R_k$ implies $\alpha_i = 0$ for all i. Throughout the paper, when we say independent we mean linearly independent.

Note that the rows of a standard generating matrix of a free code will be independent. One should also observe that if S is linearly independent over R_k, then we must have $\overline{c}_i \notin I_{u_1,u_2,\ldots,u_k}$. Thus each vector in S must contain some units. In other words $\overline{0} \notin \mu_k(S)$.

When $\mu_k(\overline{c}) = \overline{x} \in \mathbb{F}_2^n$, we will say $\overline{c}$ is an R_k-lift of the binary vector $\overline{x}$. When taking lifts we just replace 0 by any non-unit in R_k and 1 by any unit in R_k.

The following theorem starts us on independence and projections:

Theorem 4.2. *Let $S = \{\overline{c}_1, \overline{c}_2, \ldots, \overline{c}_m\}$ be a subset of R_1^n such that the projection $\mu_1(S)$ is an independent subset of $\mathbb{F}_2^n$. Then S is independent over R_1.*

Proof. Since $\mu_1(S)$ is independent, $\overline{0} \notin \mu_1(S)$. So all vectors in S are free vectors, meaning that they each have units in them. Now suppose that

$$\alpha_1\overline{c}_1 + \cdots + \alpha_m\overline{c}_m = 0$$

for $\alpha_i \in R_1$. Apply the projection μ_1 to this equation and we get

$$\mu_1(\alpha_1)\mu_1(\overline{c}_1) + \cdots + \mu_1(\alpha_m)\mu_1(\overline{c}_m) = 0$$

in $\mathbb{F}_2$. Since $\mu_1(S)$ is independent we must have $\mu_1(\alpha_i) = 0$ for all $i = 1, 2, \ldots, m$. But this means $\alpha_i = 0$ or u for each $i = 1, 2, \ldots, m$. Now, if $\alpha_i = 0$ for all $i = 1, 2, \ldots, m$, then we are done. So assume without loss of generality that $\alpha_1 = \alpha_2 = \cdots = \alpha_\ell = u$ for some $\ell > 0$. Then going back to the original equation we get $u(\overline{c}_1 + \cdots + \overline{c}_\ell) = 0$ in R_1, which implies that $\overline{c}_1 + \cdots + \overline{c}_\ell \in \{0, u\}^n$. But then taking the projections yields $\mu_1(\overline{c}_1) + \cdots + \mu_1(\overline{c}_\ell) = 0$ in $\mathbb{F}_2^n$, contradicting the independence of $\mu_1(S)$. □

Considering the inductive construction of R_k from R_{k-1} and the corresponding projections, we can extend the previous theorem to any R_k, using an inductive argument:

Theorem 4.3. *Let $S = \{\overline{c}_1, \overline{c}_2, \ldots, \overline{c}_m\}$ be a subset of R_k^n such that the projection $\mu_k(S)$ is an independent subset of $\mathbb{F}_2^n$. Then S is independent over R_k.*

Note that the converse of the previous theorem is also true if the vectors in S are free vectors. Assume for example that $S = \{\overline{c}_1, \overline{c}_2, \ldots, \overline{c}_m\}$ is an independent subset of R_k^n with $\mu_k(\overline{c}_i) \neq 0$, and let

$$\alpha_1\mu_k(\overline{c}_1) + \cdots + \alpha_m\mu_k(\overline{c}_m) = 0$$

be given with $\alpha_i \in \mathbb{F}_2$. Now if $\alpha_i = 0$ for all $i = 1, 2, \ldots, m$, then we are done. So assume without loss of generality that $\alpha_1 = \alpha_2 = \cdots = \alpha_\ell = 1$ for some $\ell > 0$. Then the equation would reduce to

$$\mu_k(\overline{c}_1) + \cdots + \mu_k(\overline{c}_\ell) = 0,$$

which implies that

$$\overline{c}_1 + \overline{c}_2 + \cdots + \overline{c}_\ell \in I^n_{u_1, u_2, \ldots, u_k}.$$

But this would imply that

$$u_1u_2 \ldots u_k(\overline{c}_1 + \overline{c}_2 + \cdots + \overline{c}_\ell) = 0$$

in R_k^n, contradicting the independence of S. Thus we have the following useful corollary:

Corollary 4.4. *Suppose that C is a free cyclic or a λ-constacyclic self-dual code over R_k of length n. Then n must be even and $\mu_k(C)$ must be a cyclic self-dual binary code.*

Because of the properties of μ_k, we know that if C is a cyclic or λ-constacyclic code over R_k, then $\mu_k(C)$ is a binary cyclic code. Since μ_k preserves duality as well, we can easily say that if C is a cyclic or λ-constacyclic self-dual code over R_k, then $\mu_k(C)$ is a self-orthogonal binary cyclic code. Of course in many cases $\mu_k(C)$ might turn out to be zero.

Now assume that $C = \langle f(x) \rangle$ is a cyclic or constacyclic self-dual code over R_k of length n. First of all, by [9], we know that $\mu_k(f(x))$ cannot be relatively prime to $x^n - 1$. But in fact we can say more.

Theorem 4.5. *Suppose that $C = \langle f(x) \rangle$ is a cyclic or a λ-constacyclic self-dual code over R_k of length n, for some unit λ in R_k. Then*

$$Rank\left(\langle \mu_k(f(x)) \rangle\right) \leq \frac{n}{2}.$$

Proof. If $C = \langle f(x) \rangle$ is a cyclic or a λ-constacyclic self-dual code over R_k of length n, then $\mu_k(C) = \langle \mu_k(f(x)) \rangle$ is a self-orthogonal binary code. This means $\mu_k(C) \subseteq \mu_k(C)^{\perp}$. But, since $|\mu_k(C)| \cdot |\mu_k(C)^{\perp}| = 2^n$, we must have $|\mu_k(C)|^2 \leq 2^n$, leading to the required assertion. □

Thus we have the following quite useful corollary:

Corollary 4.6. *Suppose that $C = \langle f(x) \rangle$ is a cyclic or a λ-constacyclic self-dual code over R_k of length n. If $GCD(\mu_k(f(x)), x^n - 1) = d(x)$, then we must have $deg(d(x)) \geq n/2$.*

5. Computational results

We begin with a few examples of general constructions and then proceed to a systematic construction of cyclic self-dual codes over R_1 of non-trivial lengths. The constructions have all been carried out using Magma Computational Algebra ([5]).

Example 5.1. Let $f(x) = 1 + ux + ux^2 + ux^3 + x^4 + vx^5 + uvx^6 + vx^7$. The cyclic code $C = \langle f(x) \rangle$ of length 8 generated over R_2 is a cyclic self-dual code of length 8 whose binary image is the extremal Type II code of length 32 with weight enumerator

$$W_C(z) = 1 + 620z^8 + 13888z^{12} + 36518z^{16} + 13888z^{20} + 620z^{24} + z^{32}$$

with an automorphism group of order $2^{15} * 3^2 * 5 * 7$.

Example 5.2. Let $f(x) = x^2 + x^3 + x^4 + ux^5 + (1 + u)x^6$ be a polynomial in $R_1[x]$. The $(1 + u)$-constacyclic code generated by $f(x)$ is a constacyclic self-dual code of length 7 whose binary image is an extremal Type I code of length 14 and weight enumerator

$$1 + 14z^4 + 49z^6 + 49z^8 + 14z^{10} + z^{14}.$$

Cyclic self-dual codes over $R_1 = \mathbb{F}_2 + u\mathbb{F}_2$ of odd lengths have been characterized and studied in [3]. Since in [4] they also gave a decoding algorithm for cyclic codes of over R_1 of odd lengths, they have been of interest to study. We will now focus on free cyclic self-dual codes over R_1 of even length. In doing so we will make use of Theorem 4.2 together with the characterization of binary cyclic self-dual codes that can be found in [11]. Thus, we know that if C is a free cyclic self-dual code of length n over R_1, then n must be even and $\mu_1(C)$ must be a binary cyclic self-dual code. Taking binary cyclic self-dual codes of even length n with high minimum weight, we can obtain a cyclic self-dual code over R_1 of high minimum distance from the lifts. The following theorem, which can be found in [14] narrows the search field considerably:

Theorem 5.3. *Suppose C is a linear code over $\mathbb{F}_2 + u\mathbb{F}_2$ and that $C' = \mu_1(C)$ is its projection to $\mathbb{F}_2$ with $\mu_1(C) \neq 0$. If d and d' represent the minimum Lee and Hamming distances of C and C' respectively, then we have $d \leq 2d'$.*

More generally, if d is the minimum Lee weight of a linear code C over R_k and d' is the minimum hamming weight of $\mu_k(C) \neq 0$, then $d \leq 2^k d'$.

With this in mind, looking at the binary cyclic self-dual codes from [11], we see that the lengths we should study are 14, 28, 30, 42 and 46.

5.1. Cyclic self-dual codes over R_1 of length 14

Taking $f(x) = u + ux + ux^2 + ux^3 + ux^4 + ux^5 + x^6 + x^7 + ux^8 + ux^9 + x^{10} + x^{11} + x^{12} + x^{13}$, the cyclic code generated by $f(x)$ over R_1 is a cyclic self-dual code of length 14 and minimum Lee weight 4. The Gray image is then a 2-quasi-cylic self-dual code of length 28 and minimum distance 4.

5.2. Cyclic self-dual codes over R_1 of length 28

In [11], it is shown that there are two non-trivial binary cyclic self-dual codes of length 28, which we lift to obtain cyclic self-dual codes of length 28 over R_1. The lifts of the first one all have minimum Lee distance 4, which we discard as the binary images then would be binary codes of length 56 and minimum distance 4. However the search through lifts of the second generator turns out to be more fruitful. We obtain codes with 6 different weight enumerators which we describe below. To save space, $1 + u$ is replaced by 3 in writing the generators.

TABLE 1. Cyclic self-dual codes over R_1 of length 28

Generator	Type	Partial Weight Enumerator
$13^3u^2103^12^02^12^10^{10}u0^2$	Type II	$1 + 147z^8 + 9072z^{12} + 610113z^{16} + \cdots$
$13^21u^23u1310^21^20^{11}10$	Type I	$1 + 56z^6 + 315z^8 + 1512z^{10} + 7840z^{12} + \cdots$
$13^21u^2103^12^02^12^10^{12}u$	Type II	$1 + 315z^8 + 10080z^{12} + 596169z^{16} + \cdots$
$1^330^2101^30^21^20^{10}u0u$	Type I	$1 + 147z^8 + 224z^{10} + 5040z^{12} + \cdots$
$1^2310u3u31^20^21^20^9u^20^2$	Type I	$1 + 427z^8 + 10752z^{12} + 16384z^{14} + \cdots$
$1^330^23u3^210^21^20^{10}u^20$	Type II	$1 + 427z^8 + 10752z^{12} + 586873z^{16} + \cdots$

5.3. Cyclic self-dual codes over R_1 of length 30

Our search through lifts of the only non-trivial binary cyclic self-dual code of length 30 have resulted in the following Type I codes all of which have minimum Lee distance 8:

TABLE 2. Cyclic self-dual codes over R_1 of length 30

Generator	Partial Weight Enumerator
$1^2 01^2 31u0u1u01^3 0^{13}u$	$1 + 60z^8 + 180z^{10} + 2975z^{12} + 33720z^{14} + \cdots$
$13u3^2 1^2 u0^2 3u01^3 0^{11}u0^2$	$1 + 150z^8 + 216z^{10} + 4245z^{12} + 32400z^{14} + \cdots$
$1301^2 3^2 0u^2 3u01^3 0^{10}u0^3$	$1 + 60z^8 + 396z^{10} + 2975z^{12} + 31560z^{14} + \cdots$
$1301^3 3u^2 030^2 1^3 0^{10}u0^2 u$	$1 + 690z^8 + 11865z^{12} + 28800z^{14} + \cdots$

5.4. Cyclic self-dual codes over R_1 of length 42

In [11] 9 different binary cyclic self-dual codes of length 42 were found. One of these is trivial which we have discarded. The remaining 8 are grouped into reciprocal pairs. Thus we considered the four possible generators to lift to R_1. Only in two of the generators the search resulted in codes with high minimum distances. The generators to lift are $gen1 = 1^4 0^2 101^3 0^2 101^3 0^2 1^2 0^{20}$ and $gen2 = 1^2 0101^3 010^4 1^4 01^3 0^{20}$. From the lifts of $gen1$ we found 20 cyclic self-dual codes over R_1 of length 42 and minimum Lee distance 8 and from lifts of $gen2$ we managed to find 5 cyclic self-dual codes over R_1 of length 42 and minimum Lee distance 8. We tabulate these results together with the partial weight distributions.

TABLE 3. Cyclic self-dual codes over R_1 of length 42 from the lifts of $gen1$

Generator	Partial Weight Enumerator
$13^2 1u^2 301^3 0u101^3 0^2 1^2 0^{19}u$	$1 + 21z^8 + 637z^{12} + 1224z^{14} + \cdots$
$13^2 1u03u1^3 u0301^3 0^2 1^2 0^{18}u0$	$1 + 21z^8 + 217z^{12} + 2688z^{14} + \cdots$
$1^4 0u1u1^3 u^2 301^3 0^2 1^2 0^{18}u^2$	$1 + 21z^8 + 252z^{10} + 301z^{12} + 1008z^{14} + \cdots$
$13^3 u^2 301^3 0u101^3 0^2 1^2 0^{17}u0^2$	$1 + 21z^8 + 217z^{12} + 3408z^{14} + \cdots$
$1^3 30u1u1^3 u^2 301^3 0^2 1^2 0^{17}u^2 0$	$1 + 21z^8 + 217z^{12} + 1512z^{14} + \cdots$
$13^3 u03u1^3 u0301^3 0^2 1^2 0^{17}u^3$	$1 + 21z^8 + 217z^{12} + 3360z^{14} + \cdots$
$1^2 3^2 0^2 1u131u0101^3 0^2 1^2 0^{16}u0u0$	$1 + 21z^8 + 217z^{12} + 2232z^{14} + \cdots$
$1^2 310u101310u301^3 0^2 1^2 0^{16}u^2 0^2$	$1 + 21z^8 + 217z^{12} + 3024z^{14} + \cdots$
$131^2 u^2 3u131u^2 101^3 0^2 1^2 0^{16}u^3 0$	$1 + 21z^8 + 553z^{12} + 2904z^{14} + \cdots$
$1^2 310^2 1u131u0101^3 0^2 1^2 0^{16}u^4$	$1 + 21z^8 + 84z^{10} + 637z^{12} + 4752z^{14} + \cdots$
$1^3 30^2 1u1^3 u^2 301^3 0^2 1^2 0^{15}u0^2 u^2$	$1 + 567z^8 + 21679z^{12} + 384z^{14} + \cdots$
$13^2 1u0301^3 0u101^3 0^2 1^2 0^{15}u0u0^2$	$1 + 21z^8 + 84z^{10} + 637z^{12} + 5040z^{14} + \cdots$
$131^2 0u1u1^3 0^2 101^3 0^2 1^2 0^{13}u0^5 u$	$1 + 21z^8 + 217z^{12} + 2400z^{14} + \cdots$
$131^2 0^2 101^3 u^2 301^3 0^2 1^2 0^{13}u0^4 u0$	$1 + 21z^8 + 217z^{12} + 840z^{14} + \cdots$
$1^2 31u^2 301^3 u0301^3 0^2 1^2 0^{13}u0^4 u^2$	$1 + 21z^8 + 637z^{12} + 2520z^{14} + \cdots$
$13^3 0^2 1u1310u301^3 0^2 1^2 0^{13}u0^2 u0^3$	$1 + 21z^8 + 217z^{12} + 2352z^{14} + \cdots$
$1^3 3u^2 3u1310^2 301^3 0^2 1^2 0^{13}u0^2 u0^2 u$	$1 + 21z^8 + 553z^{12} + 3192z^{14} + \cdots$
$1^4 u^2 3u1310^2 301^3 0^2 1^2 0^{13}u0^2 u^2 0^2$	$1 + 21z^8 + 637z^{12} + 1176z^{14} + \cdots$
$13^2 10^2 10131u0101^3 0^2 1^2 0^{13}u0u^2 0u^2$	$1 + 21z^8 + 637z^{12} + 2184z^{14} + \cdots$
$13^2 10u3u1^3 0^2 101^3 0^2 1^2 0^{13}u^2 0u0^2 u$	$1 + 21z^8 + 301z^{12} + 5760z^{14} + \cdots$

TABLE 4. Cyclic self-dual codes over R_1 of length 42 from the lifts of $gen2$

Generator	Partial Weight Enumerator
$1^2 0301^3 030^3 u131^2 01^3 0^{19} u$	$1 + 84z^8 + 1540z^{12} + 3024z^{14} + \cdots$
$13u3u3^2 1030^3 u313101^3 0^{18} u0$	$1 + 84z^8 + 1540z^{12} + 2352z^{14} + \cdots$
$13u1u3^2 1010^4 1^3 101^3 0^{18} uu$	$1 + 84z^8 + 252z^{10} + 1540z^{12} + 11472z^{14} + \cdots$
$13u1031^2 u10^2 u^2 3^2 1^2 01^3 0^{17} u^2 0$	$1 + 210z^8 + 5026z^{12} + 7776z^{14} + \cdots$
$1301u3^3 u1u0u^2 131^2 01^3 0^{15} u0^2 u^2$	$1 + 336z^8 + 21112z^{12} + 424284z^{16} + 225792z^{18} + \cdots$

Remark 5.4. The last entry in Table 4 is an interesting example of a code as the first non-zero weight not divisible by 4 is 18. It seems to have few non-zero weights, which would make it of interest for combinatorial reasons.

5.5. Cyclic self-dual codes over R_1 of length 46

Our search through lifts of the non-trivial binary cyclic self-dual code of length 46 have all resulted in Type I codes of minimum Lee distance 8, meaning that the Gray images are 2-quasi-cyclic self-dual codes of parameters $[92, 46, 8]$. We just give one such example together with its weight enumerator. Let $f(x)$ have coefficients as $1^4 0^6 1^6 0^2 1^2 0^2 1^2 0^{22}$. Then the cyclic code generated by $f(x)$ is a cyclic self-dual code of length 46 over R_1 whose partial weight enumerator is given by $1 + 2024z^8 + 5152z^{12} + 128018z^{14} + \cdots$.

6. A remark about Theorem 4.14 in [1]

Batoul et al. claimed in [1] that a self-dual code of even length over a chain ring with residue field $\mathbb{F}_2$ cannot be the lift of a binary cyclic self-dual code. What we have done in Section 4 and Section 5 contradict this claim. Because all the self-dual codes we obtained in Section 5 are of even length and they are all lifts of binary cyclic self-dual codes.

The reason why this claim is false can be seen in the proof of Theorem 4.14 in [1]. In the proof they use the statement that "the residue code of a self-dual code over such a ring must be a doubly even binary code". While this statement is certainly true for the ring $\mathbb{Z}_4$ (since the characteristic is 4, self-dual $\mathbb{Z}_4$-code means the number of units in each row is divisible by 4, thus the residue code is indeed doubly even), it is not true for the case $\mathbb{F}_2 + u\mathbb{F}_2$, which is also a chain ring with residue field $\mathbb{F}_2$. Since the characteristic is 2, the residue code of a self-dual code over $\mathbb{F}_2 + u\mathbb{F}_2$ does not have to be doubly even as can be seen in many of the examples above.

References

[1] A. Batoul, K. Guenda, and T. A. Gulliver, *On self-dual cyclic codes over finite chain rings*, Des. Codes Cryptogr. **70** (2014), no. 3, 347–358.
[2] T. Blackford, *Isodual constacyclic codes*, Finite Fields Appl. **24** (2013), 29–44.
[3] A. Bonnecaze and P. Udaya, *Cyclic codes and Self-dual codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory **45** (1999), no. 4, 1250–1255.

[4] ———, *Decoding of cyclic codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory **45** (1999), no. 6, 2148–2157.
[5] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.
[6] B. Chan and H. Q. Dinh, *A note on isodual constacyclic codes*, Finite Fields Appl. **29** (2014), 243–246.
[7] S. T. Dougherty, P. Gaborit, M. Harada, and P. Solé, *Type II codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory **45** (1999), no. 1, 32–45.
[8] S. T. Dougherty, S. Karadeniz, and B. Yildiz, *Cyclic codes over* R_k, Des. Codes Cryptogr. **63** (2012), no. 1, 113–126.
[9] S. T. Dougherty, B. Yildiz, and S. Karadeniz, *Codes over* R_k*, Gray maps and their binary images*, Finite Fields Appl. **17** (2011), no. 3, 205–219.
[10] ———, *Self-dual codes over* R_k *and binary self-dual codes*, Eur. J. Pure Appl. Math. **6** (2013), no. 1, 89–106.
[11] Y. Jia, S. Ling, and C. Xing, *On self-dual cyclic codes over finite fields*, IEEE Trans. Inform. Theory **57** (2011), no. 4, 2243–2251.
[12] S. Karadeniz, S. T. Dougherty, and B. Yildiz, *Constructing formally self-dual codes over* R_k, Discrete Appl. Math. **167** (2014), 188–196.
[13] S. Karadeniz and B. Yıldız, $(1 + v)$*-constacylic codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, J. Franklin Inst. **348** (2011), no. 9, 2625–2632.
[14] S. Karadeniz, B. Yıldız, and N. Aydın, *Extremal binary self-dual codes of lengths* 64 *and* 66 *from four-circulant constructions over codes* $\mathbb{F}_2 + u\mathbb{F}_2$, FILOMAT to appear.
[15] V. Pless, P. Sole, and Z. Qian, *Cyclic self-dual* $\mathbb{Z}_4$*-codes*, Finite Fields Appl. **3** (1997), no. 1, 48–69.
[16] N. J. A. Sloane and J. G. Thompson, *Cyclic self-dual codes*, IIEEE Trans. Inform. Theory **29** (1983), no. 3, 364–366.
[17] J. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. **121** (1999), no. 3, 555–575.
[18] B. Yıldız and S. Karadeniz, *Cyclic codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Des. Codes Cryptogr. **58** (2011), no. 3, 221–234.

Suat Karadeniz
Department of Mathematics
Fatih University
34500, Istanbul, Turkey
E-mail address: skaradeniz@fatih.edu.tr

Ismail Gokhan Kelebek
Department of Mathematics
Fatih University
34500, Istanbul, Turkey
E-mail address: gkelebek@fatih.edu.tr

Bahattin Yildiz
Department of Mathematics
Fatih University
34500, Istanbul, Turkey
E-mail address: byildiz@fatih.edu.tr