EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 6, No. 1, 2013, 89-106
ISSN 1307-5543 – www.ejpam.com

Self-Dual Codes over R_k and Binary Self-Dual Codes

Steven Dougherty[1], Bahattin Yıldız[2,*], Suat Karadeniz[2]

[1] *Department of Mathematics, Scranton University, Scranton, PA, USA*
[2] *Department of Mathematics, Fatih University, Istanbul, Turkey*

Abstract. We study self-dual codes over an infinite family of rings, denoted R_k, which has been recently introduced to the literature. We prove that for each self-dual code over R_k, $k \geq 2$, there exist a corresponding binary self-dual code, a real unimodular lattice, a complex unimodular lattice, a quaternionic lattice and an infinite family of self-dual codes. We prove the existence of Type II codes of all lengths over R_k, for $k \geq 3$, and we obtain some extremal binary self-dual codes including the extended binary Golay code as the Gray images of self-dual codes over R_k for some suitable k. The binary self-dual codes obtained from R_k all have automorphism groups whose orders are a multiple of 2^k.

2010 Mathematics Subject Classifications: 94B05

Key Words and Phrases: Self-dual codes, codes over rings, extremal codes, lattices

1. Introduction

Self-dual codes are an important class of codes and an extensive literature exists on self-dual codes over finite fields. Self-dual codes over rings have received attention especially with respect to their connection to unimodular lattices and invariant theory; see [4], [9] and [5] for a description and extensive bibliographies. They can also be used to construct designs by using the Assmus-Mattson theorem. In [6], self-dual codes were studied over the ring $\mathbb{F}_2 + u\mathbb{F}_2$ and they were connected to complex unimodular lattices. In [2], the ring $\mathbb{F}_2 + u\mathbb{F}_2$ was generalized to Σ_{2m} and self-dual codes over this ring were used to construct quaternionic unimodular lattices and associated Jacobi forms. We shall generalize these rings to an infinite family of rings denoted by R_k and use these rings to construct binary self-dual codes and real, complex and quaternionic unimodular lattices. Codes over the ring R_k were first studied in [7].

In the literature there are constructions for extremal binary self-dual codes with automorphism groups of order 2, p (an odd prime), p^2 and pq. As was shown in [7], codes over R_k are all invariant under a group of automorphisms of size 2^k. This means that self-dual codes

*Corresponding author.

Email addresses: doughertys1@scranton.edu (S. Dougherty), byildiz@fatih.edu.tr (B.Yildiz), skaradeniz@fatih.edu.tr (S.Karadeniz)

constructed from R_k will all have automorphism groups whose orders are a multiple of 2^k. So, we believe that studying self-dual codes over R_k fills a gap in the literature of binary self-dual codes. We have illustrated several examples at the end of the paper.

The rest of the paper is organized as follows: In Section 2, we will present some definitions and notations about the rings R_k and about codes over R_k. In Section 3, we will discuss the projection maps and lifts between R_k and $R_{k'}$, for $k \neq k'$, in connection with self-dual codes.

Section 4 will consist of the description of the binary images of self-dual codes over R_k. In particular, the existence of Type II codes of all lengths over R_k, for $k \geq 3$, and of all even lengths over R_2 will be established. An upper bound on the minimum Lee distance of self-dual codes will also be given.

In Section 5, we will give a characterization of self-dual codes over R_k of length 1 and 2. In particular, a full characterization of one-generator self-dual codes of length 1 and 2 will be given.

Section 6 will highlight the connection between self-dual codes over R_k and real, complex, and quaternionic unimodular lattices. We will finish the paper with some examples of extremal binary self-dual codes including the extended binary Golay code obtained from the codes over R_k for some suitable k.

2. Definitions and Notations

For finite $k \geq 1$, we define a family of rings by

$$R_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/\langle u_i^2 = 0, u_i u_j = u_j u_i \rangle. \tag{1}$$

We let R_∞ be the ring

$$R_\infty = \mathbb{F}_2[u_1, u_2, \ldots]/\langle u_i^2 = 0, u_i u_j = u_j u_i \rangle, \tag{2}$$

and $R_0 = \mathbb{F}_2$.

For all k, finite or infinite, R_k is a commutative ring. Note that the ring R_∞ is an infinite ring while R_k is a finite ring for finite values of k.

To describe the elements of R_k we let, for $A \subseteq \{1, 2, \ldots, k\}$

$$u_A := \prod_{i \in A} u_i \tag{3}$$

with $u_\emptyset = 1$. Elements of R_k, then can be represented as

$$\sum_{A \subseteq \{1, \ldots, k\}} c_A u_A, \quad c_A \in \mathbb{F}_2. \tag{4}$$

It is easily observed that the ring R_k is local whose maximal ideal is given by $\langle u_1, u_2, \ldots, u_k \rangle$ and $|R_k| = 2^{(2^k)}$. R_k is not a principal ideal ring nor is it a chain ring. But, it is a Frobenius ring. It is shown in [11] that codes over Frobenius rings satisfy MacWilliams theorems. See [11] for other foundational results on codes over Frobenius rings.

In [7], it is shown that an element of R_k is a unit if and only if the coefficient of $u_\emptyset$ is 1 and that each unit is also its own inverse. See [7] for proofs of these and other foundational results for finite k. The proofs are similar for R_∞. Throughout, unless otherwise specified, k can be any natural number greater than 0 or can be ∞.

We say that a linear code of length n over R_k is an R_k-submodule of R_k^n. Notice that a code over R_∞ is an infinite module.

We define the inner product on R_k^n in the usual way, that is $[\mathbf{v},\mathbf{w}]_k = \sum \mathbf{v}_i \mathbf{w}_i$. The dual $C^\perp$ is defined as $C^\perp = \{\mathbf{v} \in R_k^n \mid [\mathbf{v},\mathbf{w}]_k = 0 \text{ for all } \mathbf{w} \in C\}$. By [11], we know that for finite k a linear code C over R_k of length n satisfies $|C||C^\perp| = |R_k|^n$. 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 [6] as follows.

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

$$\phi_k(\mathbf{c}) = \left(\phi_{k-\mathbf{1}}(\mathbf{c_2}), \phi_{k-\mathbf{1}}(\mathbf{c_1}) + \phi_{k-\mathbf{1}}(\mathbf{c_2})\right),$$

with ϕ_0 being the identity map on $\mathbb{F}_2$.

The Lee weight of a codeword is the Hamming weight of the image of the codeword under ϕ_k. The Lee distance is defined similarly. It's clear that the Gray map ϕ_k is a linear weight preserving map from R_k^n to $\mathbb{F}_2^{2^k n}$ as was shown in [7].

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.

It is immediate that ϕ_k is one-to-one and that $w_L(u_A) = 2^{|A|}$ for each $A \subseteq \{1,2,\ldots,k\}$, see [7] for details.

The complete weight enumerator of a code C over R_k^n is defined as:

$$cwe_C(\mathbf{X}) = \sum_{\mathbf{c}\in C} \prod_{i=1}^{n} x_{c_i}. \tag{5}$$

The Hamming weight of a vector $\mathbf{c}$ is denoted by $wt(\mathbf{c})$ and is the number of non-zero coordinates of the element. The minimum weight is the minimum of all non-zero weights in the code. We denote the minimum Hamming distance by $d_H(C)$ and the minimum Lee distance by $d_L(C)$. The Hamming weight enumerator is defined as:

$$W_C(x,y) = \sum_{\mathbf{c}\in C} x^{n-wt(\mathbf{c})} y^{wt(\mathbf{c})}. \tag{6}$$

The Lee weight enumerator is defined to be

$$L_C(z) = \sum_{\mathbf{c}\in C} z^{Le(\mathbf{c})}, \tag{7}$$

where $Le(\mathbf{c})$ is the Lee weight of the codeword $\mathbf{c}$. The MacWilliams relations for both of these weight enumerators are given in [7].

3. Projections and Lifts

For $j \geq k \geq 0$, define $\Pi_{j,k} : R_j \to R_k$ by $\Pi_{j,k}(u_i) = 0$ if $i > k$ and the identity elsewhere. That is $\Pi_{j,k}$ is the projection of R_j to R_k. Note that if $j \leq k$, then $\Pi_{j,k}$ is taken to be the identity map on R_j. We allow j to be ∞ as well and denote this map by $\Pi_{\infty,k}$.

If $C = \Pi_{j,k}(C')$ for some C' and $j \geq k$, then C' is said to be a lift of C.

Theorem 1. *Let C be a self-dual code over R_j then $\Pi_{j,k}(C)$ is a self-orthogonal code over R_k.*

Proof. Let $\mathbf{v} = (v_1, \ldots, v_n)$ and $\mathbf{w} = (w_1, \ldots, w_n)$ be vectors in C. We have that

$$\Pi_{j,k}(\sum v_i w_i) = \sum (\Pi_{j,k}(v_i)\Pi_{j,k}(w_i)).$$

If $\sum v_i w_i = 0$ in R_j then $\Pi_{j,k}(0) = 0$ so $\langle \Pi_{j,k}(v), \Pi_{j,k}(w) \rangle_k = 0$. Therefore the code is self-orthogonal.

The image need not necessarily be self-dual. For example, consider the code $\langle u_2 \rangle$ in R_2. This code is self-dual but its image under $\Pi_{2,1}$ is the zero code which is not self-dual.

Theorem 2. *Let $v_1, v_2, \ldots, v_s$ generate a self-dual code over R_k (of length 1), then $v_1, v_2, \ldots, v_s$ generate a self-dual code over R_j for all $j > k$.*

Proof. Let C_j be the code generated by $v_1, v_2, \ldots, v_s$ over R_j. We proceed by induction. We know C_k is a self-dual code by assumption.

Assume C_j is a self-dual code. We have that $C_{j+1} = C_j \oplus u_{j+1} C_j$, where $C_j \cap u_{j+1} C_j = \emptyset$. Then we have that $|C_{j+1}| = |C_j||C_j| = \sqrt{2^{2^j}}\sqrt{2^{2^j}} = \sqrt{2^{2^{j+1}}}$. Then for vectors $\mathbf{v}, \mathbf{w}, \mathbf{v}', \mathbf{w}' \in C_j$ we have, since C_j is self-dual by assumption,

$$[\mathbf{v} + u_{j+1}\mathbf{v}', \mathbf{w} + u_{j+1}\mathbf{w}']_{j+1} = [\mathbf{v}, \mathbf{w}]_j + u_{j+1}[\mathbf{v}, \mathbf{w}']_j + u_{j+1}[\mathbf{v}', \mathbf{w}]_j + u_{j+1}^2[\mathbf{v}', \mathbf{w}']_j = 0.$$

Hence C_{j+1} is self-dual since it is self-orthogonal and has the proper cardinality. Therefore by mathematical induction C_j is a self-dual code for all finite j.

Next we shall prove that C_∞ is self-dual.

If $\mathbf{v}, \mathbf{w} \in C_\infty$ then there exists j with $\mathbf{v}, \mathbf{w} \in C_j$ and hence $[\mathbf{v}, \mathbf{w}]_j = 0$ which implies $[\mathbf{v}, \mathbf{w}]_\infty = 0$. If $\mathbf{w} \in C_\infty^\perp$ then $\mathbf{w} \in C_j^\perp$ for some j which gives that $\mathbf{w} \in C_j$ and hence in C_∞. Therefore C_∞ is self-dual.

Corollary 1. *If C is a self-dual code over R_k then there exists a self-dual code C' over R_j, for $j > k$, with $\Pi_{j,k}(C') = C$.*

Notice that the lifts of a self-dual code are also self-dual as we have defined it, but not all projections are self-dual.

For any ideal I of R_k we have that $Ann(I) = I^\perp$.

The following lemma appears in [7].

Lemma 1. *The code $\langle u_i \rangle$ of length 1 is a self-dual code in R_k for all $k \geq i$.*

Proof. This was proved for finite k in [7]. It is true for infinite k by Theorem 2.

If C and D are self-dual codes over R_k then define $C \times D$ as $\{(\mathbf{v}, \mathbf{w}) \mid \mathbf{v} \in C, \mathbf{w} \in D\}$. It is easy to see that this code is self-orthogonal and of the proper cardinality. Therefore the code is self-dual.

Theorem 3. *Self-dual codes over R_k exist for all lengths and for all $k \geq 1$.*

Proof. The ideal $I_{u_i} = \langle u_i \rangle$ is a self-dual code of length 1 for all i, by Lemma 1. By taking direct products, we conclude that self-dual codes exists for all lengths, for all $k \geq 1$.

4. Binary Images

The following is defined in [7]. View R_k as a vector space over $\mathbb{F}_2$ with basis $\{u_A : A \subseteq \{1, 2, \ldots, k\}\}$, and define the Gray map of each u_A and then extend it linearly to all of R_k. Fix an ordering on the subsets of $\{1, 2, \ldots, k\}$, that will be defined recursively as follows:

$$\{1, 2, \ldots, k\} = \{1, 2, \ldots, k-1\} \cup \{k\}.$$

We can now define the coordinate-wise Gray map. We denote this map by $\psi_k : R_k \to \mathbb{F}_2^{2^k}$ and define it as follows:

$$\psi_k(u_A) = (c_B)_{B \subseteq \{1,2,\ldots,k\}},$$

where

$$c_B = \begin{cases} 1 & \text{if } B \subseteq A \\ 0 & \text{otherwise.} \end{cases}.$$

We then extend ψ_k linearly to all of R_k and define the Lee weight of an element in R_k to be the Hamming weight of its image. We get a linear distance preserving map from R_k^n to $\mathbb{F}_2^{2^k n}$. It follows immediately that

$$w_L(u_A) = 2^{|A|}. \tag{8}$$

The map ψ_k was shown to be equivalent to ϕ_k in [7]. The following lemma also appears in [7].

Lemma 2. *Let C be a linear code over R_k of length n. Then*

$$\psi_k(C^\perp) = (\psi_k(C))^\perp$$

where $(\psi_k(C))^\perp$ denotes the ordinary dual of $\psi_k(C)$ as a binary code.

Theorem 4. *Let C be a self-dual code over R_k of length n, then $\psi_k(C)$ is a binary self-dual code of length $2^k n$. If C is a Type II code then $\psi_k(C)$ is Type II and if C is Type I then $\psi_k(C)$ is Type I.*

Proof. If $C = C^\perp$ then by Lemma 2, $\psi_k(C) = \psi_k(C^\perp) = \psi_k(C)^\perp$.

Since ψ_k is distance preserving, the following corollary immediately follows from the bounds given in [10]. Note that for $k \geq 2$, the length of the binary image of a code over R_k will always be divisible by 4, hence the case $n \equiv 22 \pmod{24}$ is not possible for the image of an R_k code. Hence we need not consider that special case for binary codes.

Corollary 2. *Let $d_L(n,I)$ and $d_L(n,II)$ denote the minimum distance of a Type I and Type II code over R_k of length n, respectively. Then for $k \geq 2$ we have*

$$d_L(n,I), d_L(n,II) \leq 4\left\lfloor \frac{2^{k-2}n}{6} \right\rfloor + 4.$$

Another corollary follows from the fact that a self-dual binary code must contain the all 1-vector, and as the pre-image under ψ_k of the all 1-vector corresponds to the all $u_1u_2\dots u_k$-vector in R_k we get the following corollary.

Corollary 3. *Any self-dual code over R_k must contain the all $u_1u_2\dots u_k$-vector.*

Example 1. *We have seen that $\langle u_i \rangle$ is a self-dual code of length 1 in R_k for all k with $i \leq k$. Let $C_k = \langle u_i \rangle$ be the code over R_k. Then $\psi_k(C_k)$ is a self-dual code of length 2^k with minimum Hamming distance 2.*

It is well known that if a binary Type II code of length n exists, then n must be a multiple of 8. We first show that Type II codes over R_k of any length exist for all $k \geq 3$. Note that, by taking direct sums, it is enough to show that Type II codes of length 1 exist over R_k for any $k \geq 3$. Let $k \geq 3$, take the code C over R_k of length 1 generated by $\{u_A : 1 \in A, A \neq \{1\}\} \cup \{u_2u_3\dots u_k\}$. Note that C can be viewed as an $\mathbb{F}_2$-vector space with basis

$$\{u_1u_2, u_1u_3, \dots, u_1u_2\dots u_k, u_2u_3\dots u_k\}.$$

Since every basis element is orthogonal to every other basis element, C is self-orthogonal. To prove self-duality of C we just have to look at the size. The number of subsets of $\{1,2,\dots,k\}$ that contain 1 properly is $2^{k-1}-1$. Adding the vector $u_2u_3\dots u_k$, we see that $|C| = 2^{2^{k-1}} = \sqrt{2^{2^k}}$. So C is self-dual. Note that every element of C is an $\mathbb{F}_2$-linear combination of the u_A where $|A| \geq 2$, so the Lee weight of every codeword is divisible by 4 and the minimum Lee weight of C is 4. Thus we have proved the following theorem.

Theorem 5. *Type II codes over R_k of all lengths exist for any $k \geq 3$.*

The case when $k = 1$ was resolved in [6]. So we only need to look at the case when $k = 2$. Note that if C is any linear code over R_2 of length n, then $\psi_2(C)$ is a binary linear code of length $4n$. By the observation about the lengths of binary Type II codes, we know that we should only look for Type II codes of even lengths over R_2. Again, by taking direct sums if necessary, we only need to look for a Type II code of length 2 over R_2. Indeed, let C be the linear code over R_2 of length 2, generated by the vector $(1, 1+u_1u_2)$. It turns out that C is a self-dual code with Lee weight enumerator $1+14z^4+z^8$, so it is Type II. In fact the binary image of C is an $[8,4,4]$ code which is the extended Hamming code. Thus we have proved that following result.

Theorem 6. *Type II codes exist over R_2 for all even lengths.*

Consider the complete weight enumerator of a self-dual code C. It is held invariant by the action of the MacWilliams relations. That is the complete weight enumerator is held invariant by the matrix M_k, where

$$M_k = \frac{1}{\sqrt{2^{2^k}}} T_k.$$

The matrix T_k is defined as follows.

Let $\sum_{A\subseteq\{1,2,\ldots,k\}} c_A u_A \in R_k$. Then (c_A) can be thought of as a binary vector of length 2^k. Let $wt(c_A)$ be the Hamming weight of this vector.

Then

$$\chi_1(\sum_{A\subseteq\{1,2,\ldots,k\}} c_A u_A) = (-1)^{wt(c_A)}. \tag{9}$$

Let T be a square 2^{2^k} by 2^{2^k} matrix indexed by the elements of R_k and define

$$T_{a,b} = \chi_a(b) = \chi_1(ab). \tag{10}$$

The complete weight enumerator is also held invariant by the action of multiplication by a unit. It is shown in [7] that these actions are all generated by multiplication by the unit $1+u_s$ for $1 \leq s \leq k$. Let A_s be the permutation matrix that gives the permutation $\alpha \to (1+u_s)\alpha$.

Then the group of invariants of a Type I code over R_k is

$$G_I = \langle M_k, A_1, \ldots, A_s \rangle. \tag{11}$$

Let B_k be the diagonal matrix indexed by the elements of R_k with

$$(B_k)_\alpha = i^{Le(\alpha)},$$

where $i^2 = -1$.

Then the weight enumerator of a Type II code is also held invariant by B_k. Then the group of invariants of a Type II code over R_k is

$$G_{II} = \langle M_k, B_k, A_1, \ldots, A_s \rangle. \tag{12}$$

The invariants for the Hamming weight enumerator is the same for any ring of order 2^{2^k}. That is, it is held invariant by the matrix $\frac{1}{\sqrt{2^{2^k}}} \begin{pmatrix} 1 & (2^{2^k}-1) \\ 1 & -1 \end{pmatrix}$. The Hamming weight enumerator does not change for Type II codes. It follows that weight enumerator is a polynomial in $x + (2^{2^k}-1)y$ and $y(x-y)$. See [8] for details.

The Lee weight enumerator for a code over R_k is indistinguishable from the Hamming weight enumerator for binary self-dual codes. Therefore, the Lee weight of a Type II code is a polynomial in the weight enumerator of the extended length 8 Hamming code and the extended binary Golay code of length 24. The Lee weight enumerator of a Type I code is a polynomial in $1+z^2$ and the weight enumerator of the extended length 8 Hamming code.

5. Self-Dual Codes of Length 1 and 2

5.1. Length 1 Self-Dual Codes over R_k

We first note that if a length 1 code C, generated by $a + u_k b$, with $a, b \in R_{k-1}$ is self-orthogonal, then we must have that a is a non-unit in R_{k-1}, because if a were a unit, then we would have $(a + u_k b)^2 = a^2 = 1 \neq 0$.

We will prove that if a is a non-unit and b is a unit, then $\langle a + u_k b \rangle$ is a self-dual code. For this we will first introduce the following map:

$$\Psi_k : R_k \to R_{k-1}^2$$

defined by

$$\Psi_k(a + u_k b) = (b, a + b). \tag{13}$$

It is easy to verify that Ψ_k is a linear bijection from R_k^n to R_{k-1}^{2n} and furthermore it is distance preserving. The following lemma will help us resolve the previous question.

Lemma 3. *If C is a length 1 code over R_k generated by $a + u_k b$ with $a, b \in R_{k-1}$, then $\Psi_k(C)$ is a length 2 code over R_{k-1} generated by $(b, a + b)$ and (a, a).*

Proof. We note that $(x + u_k y)(a + u_k b) = ax + (xb + ay)u_k$ for all $x, y \in R_{k-1}$ and hence

$$\Psi_k((x + u_k y)(a + u_k b)) = (xb + ay, xb + ay + ax) = x(b, a + b) + y(a, a).$$

Since x and y are arbitrary elements in R_{k-1}, we see that $\Psi_k(C)$ must be generated by $(b, a + b)$ and (a, a).

Theorem 7. *Let C be the length 1 code over R_k generated by $a + u_k b$ where a is a non-unit and b is a unit in R_{k-1}. Then C is self-dual.*

Proof. We first note that $(a + u_k b)(a + u_k b) = a^2 + u_k(ab + ab) = 0$ since a is a non-unit. Therefore, C is a self-orthogonal code. By multiplying by b, which is a unit, we might assume that C is generated by $a' + u_k$ where a' is a non-unit in R_{k-1}. Since C is self-orthogonal we only need to prove that it has the right cardinality. But now looking at $\Psi_k(C)$, we see that by Lemma 3, it is generated by $(1, 1 + a')$ and (a', a'). Since $a'(1, 1 + a') = (a', a')$, we see that $\Psi_k(C)$ is actually generated over R_{k-1} by $(1, 1 + a')$, and so it has size $2^{2^{k-1}}$. But since Ψ_k is bijective, we see that C is a length 1 code over R_k of size $2^{2^{k-1}}$ and so it must be self-dual.

Note that by changing the indices of the u_i if necessary, we can generalize the previous theorem as follows:

Corollary 4. *Let C be a length 1 code over R_k generated by $a + u_i b$ for some i with $1 \leq i \leq k$, where a is a non-unit and b is a unit in R_k, such that a and b are not au_i, nor is bu_i equal to 0, that is, u_i is not a part of either expression. Then C is a self-dual code.*

This gives us a large class of length 1 self-dual codes. Namely, if the generator is a non-unit of the form $u_i + c$ for some i, then the code it generates turns out to be self-dual.

Theorem 8. *Every self-dual code generated by a single element is generated by an element of the form given in Theorem 7.*

Proof. We shall prove that if a one-generator code is not of the form described above, i.e., if every set in the support of the generator contains at least two elements, then it cannot generate a self-dual code over R_k. To prove this, we let a be a non-unit in R_k with $k \geq 2$ and every component in a is of the form u_A with $|A| \geq 2$. We will prove that $C = \langle a \rangle$ cannot be self-dual. Of course, C is self-orthogonal, giving that $C \subseteq C^{\perp}$. To prove that C is not self-dual, we will exhibit an element in $C^{\perp}$ that is not in C. We let u_B be an element with minimal $B \neq \emptyset$ such that $a \cdot u_B = 0$. For example, if $a = u_1 u_2$, we can choose u_B to be u_1 or u_2. If $a = u_1u_2 + u_3u_4$, then we can choose u_B to be u_1u_3 or u_1u_4 or u_2u_3 or u_2u_4. Note that $u_B = u_1 \dots u_k$ if and only if a is of the form $u_1 + u_2 + \dots + u_k$, so in our case we know that $|B| < k$. After rearranging the indices if necessary, we might assume, without loss of generality, that $u_B = u_1u_2 \dots u_s$, with $s < k$.

Now, by definition, $u_B \in C^{\perp}$. Therefore, it is enough to show that $u_B \notin C$.

Assume that $r \cdot a = u_1u_2 \dots u_s$. If a contains just one component, then we would have $s = 1$ and we know in that case $u_1 \notin C$. Because $u_B = u_1 \dots u_s$, we must have

$$a = u_1a_1 + u_2a_2 + \dots + u_sa_s,$$

where $a_1, a_2, \dots, a_s$ are non-zero non-units. Additionally, a_i does not contain any of the $u_1, u_2, \dots, u_{i-1}$ for $i = 2, 3 \dots, s$.

Since a_s contains some of $u_{s+1}, \dots, u_k$, in order for ra to be $u_1u_2 \dots u_s$, r must contain u_s. Therefore we can write $r = r_1u_s$. Now, $au_s = u_1u_sa_1 + u_2u_sa_2 + \dots u_{s-1}u_sa_{s-1}$. We know that $u_{s-1}u_sa_{s-1} \neq 0$, because if it were, $u_{B\setminus\{s-1\}}$ would annihilate a, contradicting the minimality of B. Again since u_sa_{s-1} contains elements from $u_{s+1}, \dots, u_k$, we must have that r_1 contains u_{s-1}. Continuing this way, we see that $r = u_1u_2 \dots u_s$. But in that case it is impossible to have $ra = u_1u_2 \dots u_s$.

Thus, we have classified all one-generator length 1 self-dual codes over R_k for $k \geq 2$.

Not all length one self-dual codes are principal ideals. For example, the code $\langle u_1u_2, u_1u_3, u_2u_3 \rangle$ over R_3 is self-dual but not principal.

We generalize this to the following theorem.

Theorem 9. *Let k be odd, with $D_1, D_2, \dots, D_s$ the subsets of $\{1, 2, \dots, k\}$ of size $\lceil \frac{k}{2} \rceil$ where $s = \binom{k}{\lceil \frac{k}{2} \rceil}$. Then $C = \langle u_{D_1}, u_{D_2}, \dots, u_{D_s} \rangle$ is a self-dual code of length 1.*

Proof. For any D_i, D_j we have $|D_i \cup D_j| = |D_i| + |D_j| - |D_i \cap D_j|$. Since $\lceil \frac{k}{2} \rceil + \lceil \frac{k}{2} \rceil > k$ and the maximum of $|D_i \cup D_j|$ is k we have $|D_i \cap D_j| > 0$. This implies that $u_{D_i}u_{D_j} = 0$ for all i, j. Hence C is self-orthogonal.

Assume that $\sum u_B \in C^{\perp}$. This implies that $(\sum u_B)u_{D_i} = 0$ for all i. If is easy to see that this implies that $u_Bu_{D_i} = 0$ for all i. Thus $B \cap D_i \neq \emptyset$ for all i. This implies that each B must have cardinality at least $k - \lceil \frac{k}{2} \rceil + 1 = \lceil \frac{k}{2} \rceil$ when k is odd. Thus B is a subset of $\{1, 2, \dots, k\}$ with cardinality at least $\lceil \frac{k}{2} \rceil$. Hence $u_B \in \langle u_{D_1}, u_{D_2}, \dots, u_{D_s} \rangle$, that is $u_B \in C$. Therefore $C = C^{\perp}$.

Note that for k even one would need sets of size $\frac{k}{2}+1$ to be self-orthogonal. But $k-(\frac{k}{2}+1)=\frac{k}{2}-1$. Hence the code is not self-dual since there exist sets of size $\frac{k}{2}-1$ that are not disjoint from all sets of size $\frac{k}{2}+1$. For example, if $k=4$, the code $\langle u_1u_2u_3, u_1u_2u_4, u_1u_3u_4, u_2u_3u_4\rangle$ would generate a self-orthogonal code but $u_1u_2 \in C^\perp$ and not in C.

5.2. Length 2 Self-Dual Codes over R_k

We first note that, for any $a \in R_k$, with $k \geq 1$, $a^2 = 1$ if a is a unit and $a^2 = 0$ otherwise. This tells us that every codeword in a length 2 self-dual code over R_k must be of the form (a_1, a_2) where the a_i are units or of the form (b_1, b_2) where the b_i are non-units. We first start with the following proposition.

Proposition 1. *Let C be a linear code over R_k of length 2 generated by $(1, 1+u_1u_2\dots u_k)$ with $k \geq 2$. Then C is a Type II code with minimum distance 4.*

Proof. We have that $\langle(1,1+u_1u_2\dots u_k),(1,1+u_1u_2\dots u_k)\rangle_k = 0$ in R_k giving that C is self-orthogonal. Because there is a 1 in the first coordinate, every R_k-multiple of $(1, 1+u_1\dots u_k)$ is distinct, and so we have $|C| = |R_k| = 2^{2^k}$. Since $|R_k^2| = 2^{2^{k+1}} = |C|\cdot|C^\perp|$ we see that $|C^\perp| = |C| = 2^{2^k}$. We know that C is self-orthogonal which implies that C is self-dual.

To prove that the weight of every element is divisible by 4, we first observe that

$$a\cdot(u_1u_2\dots u_k) = \begin{cases} u_1u_2\dots u_k & \text{if } a \text{ is a unit} \\ 0 & \text{if } a \text{ is a non-unit.} \end{cases}$$

This means we have

$$a\cdot(1,1+u_1u_2\dots u_k) = \begin{cases} (a, a+u_1u_2\dots u_k) & \text{if } a \text{ is a unit} \\ (a,a) & \text{if } a \text{ is a non-unit.} \end{cases}$$

If a is a non-unit, then $w_L(a(1,1+u_1\dots u_k)) = w_L(a,a) = 2w_L(a)$. Therefore the Lee weight is a multiple of 4 since, by [7], we know that the Lee weight of every non-zero non-unit is even.

If a is a unit, then

$$w_L(a(1,1+u_1\dots u_k)) = w_L(a, a+u_1u_2\dots u_k) = w_L(a) + w_L(a+u_1\dots u_k) = 2^k$$

by [7]. When $k \geq 2$ this is divisible by 4.

We have found a class of Type II codes over R_k of length 2 for all $k \geq 2$. The binary images of these codes are Type II codes with parameters $[2^{k+1}, 2^k, 4]$, which are extremal when $k=2$ and $k=3$.

The following proposition can be proven in exactly the same way as the previous proposition.

Proposition 2. *Let C be the length 2 code over R_k, for $k \geq 4$, generated by $\mathbf{c} = (1, 1+u_1u_2+u_3 \dots u_k)$. Then C is a Type II self-dual code over R_k with minimum Lee distance 8. Hence the binary image is an extremal Type II code when $k = 4$.*

The following is an easy observation that can be proven in the same manner.

Proposition 3. *Let C be a linear code over R_k of length 2 generated by (a, b) where a and b are units in R_k. Then C is a self dual code.*

Conversely, any self-dual code of length 2 over R_k that contains a vector of the form (a_1, a_2), where the a_i are units, must be generated by that vector and hence be a one-generator code.

Of course, a vector of the form (b_1, b_2) where the b_i are non-units, cannot generate a self-dual code by itself, because multiplying it by $u_1 \dots u_k$ would yield the zero vector, hence the size of such a code can be at most 2^{2^k-1}. Thus we need a second generator in such a case.

6. Lattices

There is a vast literature connecting codes and lattices. See [3] for details and an extensive literature.

Let F be either $\mathbb{R}, \mathbb{C}$ or $\mathbb{H}$ and let $\mathcal{O}$ be $\mathbb{Z}, \mathbb{Z}[\mathbf{i}]$, or $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$, respectively.

A lattice in F^n is a free $\mathcal{O}$-module. The standard inner product attached to the ambient space is defined as

$$\mathbf{v} \cdot \mathbf{u} = \sum v_i \overline{u_i}, \tag{14}$$

where the involution is the identity for the real numbers and the standard involution for the complex numbers and the quaternions.

We define $L^* = \{\mathbf{u} \in F^n \mid \mathbf{u} \cdot \mathbf{v} \in \mathcal{O}$ for all $\mathbf{v} \in L\}$. For the quaternions we only need to define one orthogonal here since $\mathbf{u} \cdot \mathbf{v} \in \mathcal{O}$ if and only if $\mathbf{v} \cdot \mathbf{u} \in \mathcal{O}$. If the lattice L satisfies $L \subseteq L^*$ it is said to be integral and if the lattice L satisfies $L = L^*$ then it is said to be unimodular.

The norm of a vector $\mathbf{v}$ is $N(\mathbf{v}) = \mathbf{v} \cdot \mathbf{v}$. If the norm of every vector in a unimodular lattice is an even integer then we say the lattice is even.

We describe a family of reduction maps.

Define

$$h_{\mathbb{H}} : \mathcal{O}^n \to R_2^n, \tag{15}$$

to be the linear map where $h_{\mathbb{H}}(\mathbf{i}+1) = u_1$, $h_{\mathbb{H}}(\mathbf{j}+1) = u_2$, and $h_{\mathbb{H}}(\mathbf{k}+1) = u_1 + u_2 + u_1u_2$.

Define

$$h_{\mathbb{C}} : \mathcal{O}^n \to R_1^n, \tag{16}$$

to be the linear map where $h_{\mathbb{C}}(\mathbf{i}+1) = u_1$.

Define

$$h_{\mathbb{R}} : \mathcal{O}^n \to R_0^n, \tag{17}$$

where $R_0 = \mathbb{F}_2$ and $h_{\mathbb{R}}(n) = n \pmod 2$.

Each of these maps is a ring homomorphism and it can be seen that $h^{-1}(C)$ is a free $\mathcal{O}$-module. The lattices induced from a code C are defined as follows:

$$\Lambda_{\mathbb{H}}(C) := \frac{1}{\sqrt{2}} h_{\mathbb{H}}^{-1}(C) = \{v \in \mathcal{O}^n \mid v \pmod{2\mathcal{O}} \in C\}. \tag{18}$$

$$\Lambda_{\mathbb{C}}(C) := \frac{1}{\sqrt{2}} h_{\mathbb{C}}^{-1}(C) = \{v \in \mathcal{O}^n \mid v \pmod{2\mathcal{O}} \in C\}. \tag{19}$$

$$\Lambda_{\mathbb{R}}(C) := \frac{1}{\sqrt{2}} h_{\mathbb{R}}^{-1}(C) = \{v \in \mathcal{O}^n \mid v \pmod{2\mathcal{O}} \in C\}. \tag{20}$$

Lemma 4. *If C is a self-dual code over R_2 then $\Lambda_{\mathbb{H}}(C)$ is a quaternionic unimodular lattice. If C is a self-dual code over R_1 then $\Lambda_{\mathbb{C}}(C)$ is a complex unimodular lattice. If C is a self-dual code over $R_0 = \mathbb{F}_2$ then $\Lambda_{\mathbb{R}}(C)$ is a real unimodular lattice.*

Proof. The first result can be found in [2]. Notice that in the notation of [2], α corresponds to u_1, β corresponds to u_2 and γ corresponds to $u_1+u_2+u_1u_2$. The second result can be found in [6] where the rings is written as $\mathbb{F}_2 + u\mathbb{F}_2$ and u corresponds to u_1. The third result can be found in [1] and numerous other papers, see [3].

Let $k \geq 2$.

For $\alpha \in R_k$ write $\alpha = \alpha_0 + \alpha_1 u_{k-1} + \alpha_2 u_k + \alpha_3 u_{k-1} u_k$ with $\alpha_i \in R_{k-2}$. Then define $\Phi_2 : R_k \to R_2^{2^{k-2}}$ by $\Phi_2(\alpha) = \phi_{k-2}(\alpha_0) + \phi_{k-2}(\alpha_1)u_1 + \phi_{k-2}(\alpha_2)u_2 + \phi_{k-2}(\alpha_3)u_1u_2$.

For $\alpha \in R_k$ write $\alpha = \alpha_0 + \alpha_1 u_k$ with $\alpha_i \in R_{k-1}$. Then define $\Phi_1 : R_k \to R_2^{2^{k-1}}$ by $\Phi_1(\alpha) = \phi_{k-1}(\alpha_0) + \phi_{k-1}(\alpha_1)u_1$.

Theorem 10. *Let $k \geq 2$. If C is a self-dual code over R_k of length n then $\Phi_2(C)$ is a self-dual code over R_2 of length $2^{k-2}n$. If C is a self-dual code over R_k of length n then $\Phi_1(C)$ is a self-dual code over R_2 of length $2^{k-1}n$.*

Proof. The proof follows from Theorem 4.

Theorem 11. *Let C be a self-dual code over R_k of length n, $k \geq 2$ with $i, j \leq k$. Then $\Lambda_{\mathbb{H}}(\Phi_2(C))$ is a quaternionic unimodular lattice of length $2^{k-2}n$, $\Lambda_{\mathbb{C}}(\Phi_1(C))$ is a complex unimodular lattice of length $2^{k-1}n$, and $\Lambda_{\mathbb{R}}(\phi_k(C))$ is a real unimodular lattice of length $2^k n$.*

Proof. Follows by applying Lemma 4 and Theorem 10.

7. Extremal Binary Self-Dual Codes Obtained from Codes over R_k

Note that, in Section 5, we introduced the map

$$\Psi_k : R_k \to R_{k-1}^2$$

given by $\Psi_k(a+u_k b)=(b,a+b)$. It is easy to verify that Ψ_k is a linear bijection from R_k^n to R_{k-1}^{2n} and furthermore it is distance preserving. Now let $\mathbf{c}_1+u_k\mathbf{d}_1, \mathbf{c}_2+u_k\mathbf{d}_2$ be two vectors in R_k^n such that

$$< \mathbf{c}_1+u_k\mathbf{d}_1, \mathbf{c}_2+u_k\mathbf{d}_2 >_k = 0.$$

This means

$$< \mathbf{c}_1, \mathbf{c}_2 >_{k-1} = 0, \quad < \mathbf{c}_1, \mathbf{d}_2 >_{k-1} + < \mathbf{c}_2, \mathbf{d}_1 >_{k-1} = 0. \tag{21}$$

It follows that

$$\begin{aligned} < \Psi_k(\mathbf{c}_1+u_k\mathbf{d}_1), \Psi_k(\mathbf{c}_2+u_k\mathbf{d}_2) >_{k-1} &= < (\mathbf{d}_1, \mathbf{c}_1+\mathbf{d}_1), (\mathbf{d}_2, \mathbf{c}_2+\mathbf{d}_2) >_{k-1} \\ &= < \mathbf{d}_1, \mathbf{d}_2 >_{k-1} + < \mathbf{c}_1+\mathbf{d}_1, \mathbf{c}_2+\mathbf{d}_2 >_{k-1} \\ &= < \mathbf{d}_1, \mathbf{d}_2 >_{k-1} + < \mathbf{c}_1, \mathbf{c}_2 >_{k-1} + < \mathbf{c}_1, \mathbf{d}_2 >_{k-1} \\ &\quad + < \mathbf{c}_2, \mathbf{d}_1 >_{k-1} + < \mathbf{d}_1, \mathbf{d}_2 >_{k-1} \\ &= 0 \end{aligned}$$

by (21). This leads to the following lemma:

Lemma 5. *If C is a self-dual code over R_k of length n, then $\Psi_k(C)$ is a self-dual code over R_{k-1} of length $2n$.*

Proof. Note that the above observation tells us that Ψ preserves self-orthogonality. But, since Ψ_k is an injective map, the sizes of the codes are preserved as well, which implies that if C is a self-dual code of length n over R_k, then $\Psi_k(C)$ is a self-dual code of length $2n$ over R_{k-1}.

Combining this with Theorem 4, we obtain the following result:

Theorem 12. *Suppose C is a self-dual code over R_k of length n, and that its binary image $\psi_k(C)$ is a binary self-dual code with parameters $[2^k n, 2^{k-1}n, d]$. Then there exists a self-dual code D over R_{k-1} of length $2n$ such that $\psi_{k-1}(D)$ is a binary self-dual code with the same parameters and moreover is equivalent to $\psi_k(C)$.*

Consequently, when we are trying to get some known binary codes as the images of linear codes over R_k, it suffices to find the largest k for which we can do that. Because if it is linear over R_k, then it will be linear over R_i for all $i \le k$.

7.1. Examples

We are now ready to give some known binary self-dual codes as the images of self-dual codes over R_k.

Corollary 4.4 in [7] states that if a binary code is the image of a code over R_k then the automorphism group of the code contains k distinct automorphisms which are involutions corresponding to multiplication in the ring by $1+u_i$ for $i=1\ldots k$. Hence, the codes described below have a rich automorphism structure containing at least the group generated by these involutions. In general, it is important to find the largest k such that a binary code is the image of a code over R_k since this says the most about its automorphism group.

7.2. $[8,4,4]$ Binary Self-Dual Code

Because of the length of the code, the largest k for which the code can be the image of a code over R_k is 3. If we take C_1 to be the linear code of length 1 over R_3 generated by u_1u_2, u_1u_3 and u_2u_3, then C_1 is a self-dual code with weight enumerator $1+14z^4+z^8$. The binary image is an extremal Type II code with parameters $[8,4,4]$. By the above argument, we know that we can find the same code to be linear over R_2 as well. In that case the generator can be taken as the vector $(1,1+u_1u_2)$.

7.3. $[16,8,4]$ Binary Self-Dual Code

For length 16, the largest k for which the code can be the image of a code over R_k is 4. We take the code C_2 to be the length 1 code over R_4 generated by u_1u_2, u_1u_3, u_1u_4, $u_2u_3u_4$. The code C_2 turns out to be a self-dual code with Lee weight enumerator

$$L_{C_2}(z) = 1+28z^4+198z^8+28z^{12}+z^{16}.$$

The code $\psi_4(C_2)$ is a binary Type II code with parameters $[16,8,4]$ and is extremal. We know that we can get the same code from R_2 and R_3 as well. In particular, $\psi_3(<(1,1+u_1u_2u_3)>)$ and $\psi_2(<(1,1+u_1u_2,1+u_1,1+u_1+u_1u_2),(0,0,1+u_1,1+u_1+u_1u_2)>)$ have the same parameters and weight enumerators.

7.4. The Extended Golay Code

Let C_3 be the linear code over R_3 of length 3 generated by the following vectors

$$(u_2,u_1+u_3+u_1u_2,u_1+u_1u_2),(u_1+u_2,u_1+u_1u_2,u_2+u_3+u_1u_2),(u_3,u_2+u_1u_3,u_1+u_2).$$

Then $\psi_3(C_3)$ is a binary Type II self-dual code with parameters $[24,12,8]$ and C_3 has Lee weight enumerator

$$L_{C_3}(z) = 1+759z^8+2576z^{12}+759z^{16}+z^{24},$$

which is the weight enumerator of the extended binary Golay code.

We can of course get the same code from R_2 as well. In fact, if D is the linear code over R_2 of length 6 generated by

$$(1,0,0,1+u_1u_2,u_2,u_1+u_2),(0,1,0,u_2,1+u_1+u_1u_2,u_1+u_1u_2)$$

and

$$(0,0,1,u_1+u_2,u_1+u_1u_2,1+u_2+u_1u_2),$$

then $\psi_2(D)$ has the same parameters and the weight enumerator.

This code together with the map $\Lambda_{\mathbb{R}}$ produces the Leech lattice.

7.5. Binary Self-Dual Code with Parameters $[32, 16, 8]$

Let C_4 be the linear code over R_5 of length 1 generated by

$$\{u_i u_j u_k \mid 1 \leq i < j < k \leq 5\}.$$

Then C_4 is a self-dual Type II code by Theorem 9, and has Lee weight enumerator

$$L_{C_4}(z) = 1 + 620z^8 + 13888z^{12} + 36518z^{16} + 1388z^{20} + 620z^{24} + z^{32}.$$

So we see that $\psi_5(C_4)$ is an extremal binary Type II code of parameters $[32, 16, 8]$.

Of course by the argument given at the beginning of the section we know that we can get the same code from R_2, R_3 and R_4 as well. For example, if E is the linear code over R_4 of length 2 generated by the vector $(1, 1 + u_1u_2 + u_3u_4)$, then $\psi_4(E)$ has the same parameters and the weight enumerator as the above one.

This code is an example of a code constructed using Theorem 9. It is easy to see that any code constructed with this theorem over R_k will be a $[2^k, 2^{k-1}, 2^{\lceil \frac{k}{2} \rceil}]$ binary self-dual code. The next in the family would be a $[128, 64, 16]$ code.

7.6. Binary Self-Dual Code with Parameters $[40, 20, 8]$

Let C_5 be the linear code over R_2 generated by the matrix $[I_5|A]$ where

$$A = \begin{bmatrix} 1+u_1u_2 & u_1 & u_1 & u_1+u_2 & u_2 \\ u_1 & 1+u_1u_2 & u_1+u_2 & u_1 & u_2 \\ u_1 & u_1+u_2+u_1u_2 & 1+u_1u_2 & u_1u_2 & u_1+u_2+u_1u_2 \\ u_1+u_2 & u_1+u_1u_2 & 0 & 1+u_1u_2 & u_2 \\ u_2+u_1u_2 & u_2 & u_1+u_2+u_1u_2 & u_2 & 1+u_1u_2 \end{bmatrix}.$$

Then C_5 is a self-dual code over R_2 of length 10 with weight enumerator $1 + 125z^8 + 1664z^{10} + 10720z^{12} + \ldots$. The binary image $\psi_2(C_5)$ is a en extremal singly-even self-dual code with parameters $[40, 20, 8]$ and has an automorphism group of order 2^7.

7.7. Binary Self-Dual Code with Parameters $[44, 22, 8]$

Let C_6 be the linear code over R_2 of length 11 generated by the matrix $\left[\begin{array}{c|c} I_5 & \multirow{2}{*}{A} \\ 0 & \end{array}\right]$ where A is the 6×6 matrix given by

$$A = \begin{bmatrix} 1+u_2+u_1u_2 & u_1u_2 & 1+u_2+u_1u_2 & 1+u_2+u_1u_2 & 1+u_2 & 1+u_1 \\ 1+u_2 & 1+u_1+u_2+u_1u_2 & 1+u_2 & 1+u_1+u_2+u_1u_2 & 1+u_2 & u_1 \\ 1+u_1+u_2+u_1u_2 & 1+u_1 & u_1 & u_1+u_1u_2 & u_2 & 1+u_2 \\ u_1 & 1+u_2+u_1u_2 & 1+u_1u_2 & 0 & u_1+u_2 & 1+u_1+u_1u_2 \\ 0 & 1 & u_1 & 1+u_1 & u_1 & 1+u_2 \\ 0 & u_2+u_1u_2 & u_1u_2 & 0 & u_2 & u_2 \end{bmatrix}.$$

Then C_6 is a self-dual code over R_2 of length 11 with weight enumerator $1 + 104z^8 + 512z^{10} + \ldots$. The binary image $\psi_2(C_6)$ is an extremal singly-even self-dual code with parameters $[44, 22, 8]$ with $|Aut(C)| = 2^{16} \cdot 3^2 \cdot 5^2$.

7.8. Binary Self-Dual Code with Parameters $[56, 28, 12]$

The existence of Type I extremal self-dual code of length 56 is not known in the literature, however extremal Type II code of length 56 is known and there is only one possible weight enumerator for such codes, that starts with $1+8190z^{12}+\ldots$. We are going to give two separate constructions for this code, one from R_2 and one from R_3 with different automorphism groups:

From R_2**:** Let C_7 be the linear code over R_2 of length 14, generated by the matrix $[I_7|A]$ where the rows of A are given by

$$\{(1+u_1, 1+u_2, 1, u_1, u_1, 1+u_1, 1+u_1+u_2), (1+u_1u_2, u_1+u_2, 1+u_1+u_2+u_1u_2,\\ 1+u_2+u_1u_2, u_1+u_2+u_1u_2, u_1+u_1u_2, u_1+u_1u_2), (0, 1+u_1+u_2+u_1u_2, 1+u_1,\\ 1+u_1+u_2, u_1+u_1u_2, 1+u_2+u_1u_2, 1+u_1), (1+u_1u_2, 1+u_1+u_1u_2, u_2+u_1u_2,\\ 1+u_1+u_2+u_1u_2, u_1, 1+u_1+u_2+u_1u_2, 1+u_1u_2), (u_2+u_1u_2, u_2+u_1u_2, u_2, u_1+u_2+u_1u_2,\\ 1+u_1+u_2+u_1u_2, 1+u_1+u_2+u_1u_2, 1+u_2), (0, 1, u_1+u_2+u_1u_2, u_2+u_1u_2, 1+u_1+u_2, 1, u_1),\\ (u_1, 1+u_2, u_2+u_1u_2, u_2, 1+u_2+u_1u_2, u_2, 1+u_1+u_2)\}$$

Then $\psi_2(C_7)$ is an extremal binary Type II self-dual code of parameters $[56, 28, 12]$ with an automorphism group of order 4.

From R_3**:** Let C_7' be the linear code over R_3 of length 7 generated by the matrix $\left[\begin{array}{c|c} I_3 & \multirow{2}{*}{A} \\ 0 & \end{array}\right]$, where A is a 4×4 matrix over R_3 whose rows are

$$\{(1+u_3+u_1u_3+u_1u_2u_3, 1+u_1+u_2+u_2u_3+u_1u_2u_3, 1+u_2+u_3+u_1u_2+u_1u_3+u_2u_3\\ +u_1u_2u_3, u_1+u_3+u_1u_2u_3), (u_2+u_1u_2+u_1u_3, 1+u_2+u_3+u_1u_2+u_2u_3, 1+u_3+u_1u_2+u_2u_3\\ , 1+u_1+u_2+u_1u_2+u_1u_3+u_2u_3+u_1u_2u_3), (1+u_1+u_3+u_1u_2u_3, u_2+u_2u_3,\\ 1+u_1u_2+u_1u_3+u_2u_3+u_1u_2u_3, 1+u_1+u_2+u_3+u_1u_2+u_2u_3), (u_1+u_3+u_1u_2+u_1u_3\\ +u_1u_2u_3, u_1+u_3+u_1u_3+u_1u_2u_3, 0, u_1+u_3+u_1u_2+u_1u_3)\}.$$

$\psi_3(C_7')$ is an extremal binary self-dual code of parameters $[56, 28, 12]$ with an automorphism group of order 8.

7.9. Binary Self-Dual Code with Parameters $[64, 32, 12]$

Let C_8 be the linear code over R_3 of length 8 generated by the matrix $[I_4|A]$ where A is a 4×4 matrix over R_3 whose rows are

$$\{(1+u_1+u_1u_2+u_1u_3+u_1u_2u_3, 1+u_1+u_2+u_1u_2+u_1u_3+u_2u_3+u_1u_2u_3, 1+u_3\\ +u_1u_2u_3, u_3+u_2u_3), (u_3+u_1u_2+u_2u_3, 1+u_2+u_1u_2, 1+u_1+u_3+u_2u_3, 1+u_1+u_3\\ +u_1u_3+u_1u_2u_3), (1+u_1+u_3+u_1u_3+u_2u_3+u_1u_2u_3, u_1+u_1u_2+u_2u_3, 1+u_1+u_3+u_1u_2\\ +u_2u_3, 1), (1+u_2+u_3+u_2u_3+u_1u_2u_3, 1+u_1+u_2u_3, u_1+u_1u_3+u_2u_3+u_1u_2u_3,\\ 1+u_1+u_2+u_2u_3+u_1u_2u_3)\}.$$

Then C_8 turns out to be a Type I code with Lee weight distribution $1+1888z^{12}+20736z^{14}+\ldots$ We see that $\psi_3(C_8)$ is an extremal binary Type II code with parameters $[64,32,12]$ and an automorphism group of order 8.

8. conclusion

Binary self-dual codes are a rich source of research in coding theory. There are numerous methods of constructing good self-dual codes, in particular extremal binary self-dual codes, which are self-dual codes that attain the upper bounds. Recently, the family of rings that are called R_k have been introduced in coding theory and have proved to be useful in constructing binary codes with good parameters.

In this work, we worked our the general properties of self-dual codes over R_k and used these codes to obtain binary self-dual codes. We gave alternate constructions for some of the well known good self-dual binary codes such as the extended Hamming code and the extended binary Golay code. Binary codes that are images of codes over R_k have automorphism groups of size that are multiple of 2^k. That is why working over R_k helps construct binary self-dual codes of high automorphism groups.

The rich algebraic structure of R_k can prove to be useful in obtaining better codes in the future. The connection of codes over R_k with some other structures such as lattices and designs can further be explored. We obtained a number of extremal binary self-dual codes of certain lengths from R_k. This can be done for more lengths and to a further extent.

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

References

[1] E. Bannai, S.T. Dougherty, M. Harada, and M. Oura. Type II Codes, Even Unimodular Lattices, and Invariant Rings, *IEEE Transactions on Information Theory*, 45:1194-1205, 1999.

[2] Y.J. Choie and S.T. Dougherty. Codes over Σ_{2m} and Jacobi Forms over the Quaternions, *Applicable Algebra in Engineering, Communications and Computing* 15:129-147, 2004.

[3] J.H. Conway and N.J.A. Sloane. Sphere Packing, Lattices and Groups (2nd ed.), New York: Springer-Verlag, 1993.

[4] J. H. Conway and N. J. A. Sloane. Sphere Packings, Lattices and Groups. Springer-Verlag, NY, 3rd ed., 1998.

[5] S.T. Dougherty, T. A. Gulliver and M. Harada. Type II self-dual codes over finite rings and even unimodular lattices, *Journal of Algebraic Combinatorics*, 9:233–250, 1999.

[6] S.T. Dougherty, M. Harada, P. Gaborit, and P. Solé. Type II Codes Over $F_2 + uF_2$, *IEEE Transactions on Information Theory*, 45:32-45, 1999.

[7] S.T. Dougherty, B. Yıldız and S. Karadeniz. Codes over R_k, Gray Maps and their Binary Images, *Finite Fields and their Applications* 17:205–219, 2011.

[8] F.J. MacWilliams and N.J.A. Sloane. The Theory of Error-Correcting Codes. Amsterdam: North-Holland, 1977.

[9] G. Nebe, E. M. Rains and N. J. A. Sloane. Self-Dual Codes and Invariant Theory. Springer-Verlag, 2006.

[10] E.M. Rains. Shadow Bounds for self-dual Codes, *IEEE Transactions on Information Theory*, 44:134–139, 1998.

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