Self-dual codes over chain rings

Simon Eisenbarth and Gabriele Nebe

Abstract. In this paper, we study self-dual codes over commutative Artinian chain rings. Let R be such a ring, x be a generator of the unique maximal ideal of R and $a \in \mathbb{N}_0$ maximal such that $x^a \neq 0$. A code C over R of length t is an R-submodule of the free module R^t. Multiplying powers of x to C defines the finite chain of subcodes

$$C \supseteq C^{(1)} := Cx \supseteq C^{(2)} := Cx^2 \supseteq \cdots \supseteq C^{(a)} := Cx^a \supseteq \{0\}.$$

In this paper, we show that if C is a self-dual code in R^t, then $C^{(a)}$ is a (hermitian) self-dual code over the residue field $\mathbb{F} = R/\langle x \rangle$ if and only if C a free R-module (thus isomorphic to $R^{\frac{t}{2}}$). In this case, all codes $C^{(i)}$ are self-dual codes in suitable bilinear or Hermitian spaces W_i over $\mathbb{F}$ and we describe a method to construct all lifts C a given self-dual code $C^{(a)}$ over $\mathbb{F}$ that are self-dual, free codes over R. We apply this technique to codes over finite fields of characteristic p admitting an automorphism whose order is a power of p. For illustration, we show that the well-known Pless Code P_{36} is the only extremal, ternary code of length 36 with an automorphism of order 3, strengthening a result of Huffman, who showed the assertion for all prime orders ≥ 5.

Mathematics Subject Classification (2010). Primary 94B05; Secondary 11T71.

Keywords. Self-dual codes, chain rings, automorphisms.

1. Introduction

The theory of error-correcting codes was introduced by Golay and Hamming in 1949 and 1950, respectively. While originally defined over finite fields, linear codes over rings have been studied increasingly in the last years. The research first focused on integer residue rings, especially $\mathbb{Z}/4\mathbb{Z}$, as some nonlinear binary codes are the image of linear codes over this ring under the so called Gray map (see [7]), but also other rings were considered.

Special attention received finite rings with a linear lattice of ideals (the so called chain rings). Their properties lie closest to the properties of finite fields, so it is expected that the structure of codes over these rings resembles those of classical coding theory. Furthermore, the class of finite chain rings contains some important infinite families of rings, for example the integer residue rings of prime power order, Galois rings, and certain group rings.

In this paper, we study self-dual codes over commutative Artinian chain rings. Let R be such a ring, x a generator of the unique maximal ideal of R and $a \in \mathbb{N}_0$ maximal with $x^a \neq 0$. A code C over R of length t is an R-submodule of the free module R^t. Multiplying powers of x to C defines the finite chain of subcodes

$$C \supseteq C^{(1)} := Cx \supseteq C^{(2)} := Cx^2 \supseteq \cdots \supseteq C^{(a)} := Cx^a \supseteq \{0\}.$$

The papers [2], [4], and [15], apply similar ideas to the special case of self-dual binary codes with an automorphism g of order 2. So here $R = \mathbb{F}_2 C_2$, $x = (1 + g)$ and $a = 1$. The main result of

[15] is a special case of Theorem 2.8 (c) in the present paper, stating that $C \cdot (1+g)$ is canonically isomorphic to a self-dual code over $\mathbb{F}_2$ if and only if the code C is a free R-module.
In section 2, we transfer this result to the more general situation, showing that that if C is a self-dual code in R^t, then $C^{(a)}$ is a (hermitian) self-dual code over the residue field $\mathbb{F} = R/\langle x\rangle$ if and only if C is a free R-module (thus isomorphic to $R^{\frac{t}{2}}$). Given $C^{(i+1)}$ we construct a suitable bilinear or Hermitian spaces W_i over $\mathbb{F}$ (for all i) such that the lifts $C^{(i)}$ of $C^{(i+1)}$ are in bijection to certain self-dual codes in W_i (see Theorem 2.12). This gives rise to a new method described in Algorithm 2.15 to successively lift the codes $C^{(i+1)}$ to finally classify all self-dual, free codes $C = C^{(0)}$ (of high minimum distance).
In section 4, we apply this technique to codes over finite fields of characteristic p admitting an automorphism whose order is a power of p. For illustration, we show that the well-known Pless Code P_{36} is the only extremal, ternary code of length 36 with an automorphism of order 3, strengthening a result of Huffman (see [11]), showing the assertion for all prime orders ≥ 5.

2. Codes over chain rings

Throughout the paper let R be a commutative Artinian chain ring with 1 and let $^- : R \to R$ be an involution, i.e. a ring automorphism of order one or two. If $\mathfrak{m}$ denotes the maximal ideal of R, then $^-$ induces an involution of the residue field $\mathbb{F} = R/\mathfrak{m}$ which we again denote by $^-$. If this involution is the identity on the residue field, then there is $\epsilon \in \{1, -1\}$ such that $\overline{x} \equiv \epsilon x \pmod{Rx^2}$ for any generator x of $\mathfrak{m}$. If $^-$ has order 2 on $\mathbb{F}$ (which we refer to as the Hermitian case) then by Hilbert 90 we may choose a generator x of $\mathfrak{m}$ such that $\overline{x} \equiv x \pmod{Rx^2}$. We fix once and for all such a generator x of the maximal ideal of R such that

$$\overline{x} \equiv \epsilon x \pmod{Rx^2}$$

with $\epsilon = 1$ in the Hermitian case. Let $a \in \mathbb{N}_0$ be maximal such that $x^a \neq 0$. Then

$$R \supset Rx \supset Rx^2 \supset \cdots \supset Rx^{a+1} = \{0\}$$

is the complete chain of all ideals in R and all indecomposable R-modules are of the form

$$S_b := Rx^b \text{ for some } 0 \leq b \leq a$$

where $S_0 = R$ is the free module of rank 1 and S_a is the unique simple R-module. We denote the composition length (or Jordan-Hölder length) of a module V by $\ell(V)$, so in particular $\ell(S_b) = a - b + 1$.

To consider codes let $t \in \mathbb{N}$ and

$$V = R^t = \{(v_1, \ldots, v_t) \mid v_i \in R\}$$

denote the free R-module of rank t. We define the $^-$-Hermitian standard inner product

$$\langle \cdot, \cdot \rangle : V \times V \to R, \langle v, w\rangle := \sum_{j=1}^{t} v_j \overline{w_j} \tag{2.1}$$

on V.

Definition 2.1. We call an R-submodule C of V a *code of length* t (over R). Let $C \leq V$ be some code. Then by the theorem of Krull, Remak, Schmidt, there are unique $t_0, t_1, \ldots, t_a \in \mathbb{Z}_{\geq 0}$ such that

$$C \cong S_0^{t_0} \oplus S_1^{t_1} \oplus \ldots \oplus S_a^{t_a}.$$

We call $(t_0, t_1, \ldots, t_a)$ the *type* of C. The *dual* code is

$$C^\perp := \{v \in V \mid \langle v, w\rangle = 0 \text{ for all } w \in C\}$$

and C is called *self-dual* if $C = C^\perp$ and *self-orthogonal* if $C \subseteq C^\perp$.

Lemma 2.2. *Let $C \leq R^t$ be a code of type $(t_0, t_1, \ldots, t_a)$.*

(a) *The type of Cx is $(0, t_0, \ldots, t_{a-1})$.*
(b) *The type of $C^\perp$ is $(t - \sum_{i=0}^a t_i, t_a, \ldots, t_1)$.*
(c) $\ell(C) + \ell(C^\perp) = \ell(V)$.

Proof. (a) is clear and (c) follows from (b). To see (b) let $(t'_0, t'_1, \ldots, t'_a)$ denote the type of $C^\perp$. As R is Artinian and hence self-injective we have the exact sequence

$$0 \to C^\perp \to V \to \mathrm{Hom}_R(C, R) \to 0$$

and $\mathrm{Hom}_R(C, R) \cong C$ as an R-module. So $C \cong V/C^\perp$. The type of $V/C^\perp = R^t/(\oplus_{b=0}^a S_b^{t'_b})$ is the one of

$$\oplus_{b=0}^a (R/Rx^b)^{t'_b} \oplus R^{t-\sum_{b=0}^a t'_b} \cong \oplus_{b=0}^a S_{a-b+1}^{t'_b} \oplus S_0^{t-\sum_{b=0}^a t'_b}$$

which shows that $t_0 = t - \sum_{b=0}^a t'_b$ and $t_{a-b+1} = t'_b$ for $1 \leq b \leq a$. □

For later use we need the following observation:

Lemma 2.3. *Let $C \subseteq C^\perp$ be a self-orthogonal code of type $(t_0, t_1, \ldots, t_a)$. Then for $j = 0, \ldots, a$*

$$\sum_{i=0}^{j} t_i \leq t - \sum_{i=0}^{a-j} t_i.$$

If $C^\perp x \subseteq C$ then for $j = 0, \ldots, a-1$

$$t - \sum_{i=0}^{a-j} t_i \leq \sum_{i=0}^{j+1} t_i.$$

Proof. If $C \subseteq C^\perp$ then the module

$$C^\perp \cong S_0^{t-\sum_{i=0}^a t_i} \oplus S_1^{t_a} \oplus \ldots \oplus S_a^{t_1}$$

contains a submodule isomorphic to $S_0^{t_0} \oplus S_1^{t_1} \oplus \ldots S_a^{t_a}$. Therefore $t_0 \leq t - \sum_{i=0}^a t_i$, $t_0 + t_1 \leq t - \sum_{i=0}^a t_i + t_a = t - \sum_{i=0}^{a-1} t_i$ etc.
Similarly if $C^\perp x \subseteq C$ then $S_0^{t_0} \oplus S_1^{t_1} \oplus \ldots S_a^{t_a}$ contains a submodule isomorphic to $S_1^{t-\sum_{i=0}^a t_i} \oplus S_2^{t_a} \oplus \ldots \oplus S_a^{t_2}$ which yields the other inequalities. □

2.1. The socle

In this section we take advantage of the fact that multiplication by x^a defines an isomorphism between the residue field and the socle of R:

Remark 2.4. The isomorphism

$$\varphi : \mathbb{F} = R/Rx \to Rx^a = S_a, r + Rx \mapsto rx^a$$

satisfies

$$\varphi(\overline{r + Rx}) = \overline{r}x^a = \epsilon^a \overline{rx^a}$$

so φ commutes or anti-commutes with the involutions.

For a code C of type $(t_0, \ldots, t_a)$ the socle of C

$$\mathrm{soc}(C) = \{c \in C \mid c \cdot x = 0\} \cong S_a^{t_0 + \cdots + t_a}$$

is a subspace of the socle $\mathrm{soc}(V) = Vx^a$ of dimension $\sum_{i=0}^a t_i$.

Remark 2.5. On $\mathbb{F}^t$ we have the standard Hermitian dot inner product

$$v \cdot w := \sum_{i=1}^{t} v_i \overline{w_i}.$$

The map

$$\pi : \mathrm{soc}(V) = Vx^a \to \mathbb{F}^t, (v_1, \ldots, v_t) \mapsto (\varphi^{-1}(v_1), \ldots, \varphi^{-1}(v_t))$$

is an $\mathbb{F}$-linear isomorphism satisfying

$$\pi(vx^a) \cdot \pi(wx^a) = \varphi^{-1}(\langle vx^a, w\rangle) = \epsilon^a \varphi^{-1}(\langle v, wx^a\rangle)$$

for all $v, w \in V$.

If $C \leq V$ is a code of length t over R, then Cx^a and $\mathrm{soc}(C)$ are subcodes of $\mathrm{soc}(V) = Vx^a$.

Proposition 2.6. $(\pi(C^\perp x^a))^\perp = \pi(\mathrm{soc}(C))$.

Proof. Let $(t_0, \ldots, t_a)$ be the type of C. Then by Lemma 2.2 we obtain $\dim(\pi(C^\perp x^a)) = t - \sum_{i=0}^{a} t_i$ and $\dim(\pi(\mathrm{soc}(C))) = \sum_{i=0}^{a} t_i$. So it is enough to show that $\pi(\mathrm{soc}(C)) \subseteq (\pi(C^\perp x^a))^\perp$. So let $s = (s_1, \ldots, s_t) \in \mathrm{soc}(C)$ and $z = (z_1, \ldots, z_t) \in C^\perp$. Then

$$\pi(zx^a) \cdot \pi(s) = \epsilon^a \varphi^{-1}(\langle z, s\rangle) = \epsilon^a \varphi^{-1}(0) = 0$$

and hence $\pi(s) \in (\pi(C^\perp x^a))^\perp$. □

Remark 2.7. If $C^\perp x^a \subseteq C$ then $C^\perp x^a \subseteq \mathrm{soc}(C)$ and hence $\pi(C^\perp x^a)$ is a self-orthogonal subcode of $\pi(\mathrm{soc}(V)) = \mathbb{F}^t$ with respect to the standard Hermitian dot inner product.

2.2. Self-dual codes

¿From now on we assume that $C = C^\perp$ is a self-dual code of length t. As a corollary to Lemma 2.2 we find the following theorem (see [2] and [15] for $R = \mathbb{F}_2 C_2$).

Theorem 2.8. *Let $C = C^\perp \leq V$ be a self-dual code of length t.*
(a) The type $(t_0, t_1, \ldots, t_a)$ of C satisfies $t_1 = t_a$, $t_2 = t_{a-1}$, ... and

$$t_0 = \begin{cases} \frac{t}{2} - \sum_{b=1}^{a/2} t_b & \text{if } a \text{ is even} \\ \frac{t - t_{(a+1)/2}}{2} - \sum_{b=1}^{(a-1)/2} t_b & \text{if } a \text{ is odd.} \end{cases}$$

(b) $\pi(Cx^a)$ is a self-orthogonal code in $(\mathbb{F}^t, \cdot)$ with $(\pi(Cx^a))^\perp = \pi(\mathrm{soc}(C))$.
(c) C is a free R-module (i.e. $t_1 = \ldots = t_a = 0$ and so $t_0 = t/2$) if and only if $Cx^a = \mathrm{soc}(C)$ if and only if $\pi(Cx^a)$ is a self-dual code in $(\mathbb{F}^t, \cdot)$.

Proof. The first assertion is a direct consequence of Lemma 2.2. The code Cx^a is isomorphic to $S_a^{t_0}$ and as $Cx^a \cdot x = \{0\}$, it is contained in $\mathrm{soc}(C)$ and the second assertion follows from Proposition 2.6. Then $\pi(Cx^a)$ is a self-dual code in $(\mathbb{F}^t, \cdot)$ if and only if $Cx^a = \mathrm{soc}(C)$ (π is an isomorphism) if and only if both codes have the same $\mathbb{F}$-dimension. As the dimension of $\pi(Cx^a)$ is t_0 and the one of $\pi(\mathrm{soc}(C))$ is $t_0 + t_1 + \cdots + t_a$, they are equal if and only if $t_1 = \cdots = t_a = 0$, i.e. C is a free R-module of rank $t_0 = t/2$. □

In the following we assume that C is a self-dual code of even length t and type $(t/2, 0, \ldots, 0)$, i.e. C is a free R-module. Then the subcodes

$$C^{(i)} := Cx^i \text{ of type } (0^i, t/2, 0^{a-i})$$

form the following chain

$$V \supset {C^{(a)}}^\perp \supset \cdots \supset {C^{(1)}}^\perp \supset C^\perp = C \supset C^{(1)} \supset \cdots \supset C^{(a)} \supset \{0\}.$$

Lemma 2.9. *For $0 \leq i \leq a$ we have ${C^{(i)}}^{\perp} = C + Vx^{a+1-i}$. Furthermore the type of ${C^{(i)}}^{\perp}$ is $(t/2, 0^{a-i}, t/2, 0^{i-1})$.*

Proof. It is easy to see that $C + Vx^{a+1-i} \subseteq {C^{(i)}}^{\perp}$ by direct computation. Moreover for the composition lengths we obtain

$$\ell(C^{(i)}) = \ell(S_i^{t/2}) = \frac{t}{2}(a - i + 1)$$

and

$$\begin{aligned}\ell(C + Vx^{a+1-i}) &= \ell(C/(Vx^{a+1-i} \cap C)) + \ell(Vx^{a+1-i}) = \ell(C/C^{(a+1-i)}) + ti \\ &= \frac{t}{2}(a + 1 - i) + ti = \frac{t}{2}(a + 1 + i).\end{aligned}$$

So

$$\ell(C^{(i)}) + \ell(C + Vx^{a+1-i}) = t(a + 1) = \ell(V)$$

implies that $\ell(C + Vx^{a+1-i}) = \ell({C^{(i)}}^{\perp})$ so by the inclusion above we find the statement of Lemma 2.9. □

Corollary 2.10. ${C^{(i)}}^{\perp} x^i = Cx^i + V(x^{a+1-i}x^i) = Cx^i = C^{(i)}$.

Let $D \leq Vx^{i+1}$ be a code of type $(0^{i+1}, t/2, 0^{a-i-1})$ with $D^{\perp}x^{i+1} = D$. Note that this is fulfilled by every code $C^{(i+1)}$. We put

$$W_i := D^{\perp}x^i/D \cong \mathbb{F}^t$$

and define

$$(\cdot,\cdot)_i : W_i \times W_i \to \mathbb{F}, (cx^i + D, bx^i + D)_i := \varphi^{-1}(\langle c, b\rangle x^i).$$

Lemma 2.11. *$(\cdot,\cdot)_i$ is a well-defined, non-degenerate inner product which is Hermitian in the Hermitian case and $\epsilon^{(i+a)}$-symmetric bilinear otherwise.*

Proof. First we show that the inner product is well-defined. For $c, c' \in D^{\perp}$ we have $cx^i + D = c'x^i + D$ if and only if there is $d \in D^{\perp}$, $v \in V$ with $c' = c + dx + vx^{a+1-i}$. For such $c' = c + dx + vx^{a+1-i}$ and $b' = b + d' + v'x^{a+1-i}$ we have

$$\begin{aligned}\langle c', b'\rangle x^i &= \langle c + dx + vx^{a+1-i}, b + d'x + v'x^{a+1-i}\rangle x^i \\ &= \langle c, b\rangle x^i + \langle c, d'x\rangle x^i + \langle dx, b\rangle x^i + \langle dx, d'x\rangle x^i \\ &= \langle c, b\rangle x^i\end{aligned}$$

where the first equality holds because $x^{a+1-i}x^i = 0$ and the second equality as $dxx^i \in D^{\perp}x^{i+1} = D$ and $c, d'x \in D^{\perp}$ and similarly $d'x\overline{x}^i \in D^{\perp}x^{i+1} = D$ and $b, dx \in D^{\perp}$. For $c, b \in D^{\perp}$ we have

$$(\langle c, b\rangle x^i)x = \langle cx^{i+1}, b\rangle = 0$$

as $cx^{i+1} \in D^{\perp}x^{i+1} = D$ and $b \in D^{\perp}$. So $\langle c, b\rangle x^i \in S_a$ and the inner product is well-defined. Furthermore we have

$$\begin{aligned}(bx^i, cx^i)_i &= \varphi^{-1}(\langle b, c\rangle x^i) = \varphi^{-1}\left(\overline{\langle c, b\rangle}x^i\right) = \varphi^{-1}\left(\overline{\langle c, b\rangle\overline{x^i}}\right) \\ &= \epsilon^a\overline{\varphi^{-1}(\langle c, b\rangle\overline{x^i})} = \epsilon^a\overline{\varphi^{-1}(\langle c, b\rangle\epsilon^i x^i)} = \epsilon^{(i+a)}\overline{\varphi^{-1}(\langle c, b\rangle x^i)} \\ &= \epsilon^{(i+a)}(cx^i, bx^i)_i.\end{aligned}$$

To compute the radical let $bx^i \in D^{\perp}x^i$ such that $(cx^i, bx^i)_i = 0$ for every $c \in D^{\perp}$. We conclude that $\langle c, b\rangle x^i = \langle c, bx^i\rangle = 0$ for every $c \in D^{\perp}$, which means that $bx^i \in D$ and the radical is zero hence $(\cdot,\cdot)_i$ is non-degenerate. □

Note that

$$X_i := (\mathrm{soc}(V) + D)/D = (Vx^a + D)/D \leq W_i$$

is a maximal totally isotropic subspace of W_i with respect to $(\cdot,\cdot)_i$.

The next theorem can be seen as a generalization of Theorem 2.8 as it identifies a lift D' of D, i.e. a self-orthogonal code isomorphic to $S_i^{t/2}$ with $D'x = D$, as a maximal isotropic subspace of W_i.

Theorem 2.12. *Let D, W_i and $(\cdot,\cdot)_i$ be as above. The codes $D' \leq Vx^i$ with $D'x = D$ and ${D'}^{\perp}x^i = D'$ yield exactly the maximal isotropic subspaces D'/D in $(W_i, (\cdot,\cdot)_i)$ that complement X_i, i.e.*

$$W_i = D'/D \oplus X_i.$$

Proof. By assumption we have $D = D'x \subseteq D'$ so ${D'}^{\perp} \subseteq D^{\perp}$ and hence $D' = {D'}^{\perp}x^i \subseteq D^{\perp}x^i$ so $D'/D \leq W_i$. For $cx^i, bx^i \in D'$ we can assume wlog that $b \in {D'}^{\perp}$ and compute that

$$(cx^i, bx^i)_i = \varphi^{-1}(\langle cx^i, b\rangle) = \varphi^{-1}(0) = 0$$

so D'/D is an isotropic subspace of W_i. Moreover if $b \in D^{\perp}$ satisfies $\langle cx^i, b\rangle = 0$ for all $c \in {D'}^{\perp}$, then $b \in D'$, so D'/D is a maximal isotropic subspace of W_i. In particular $D'/D \cong \mathbb{F}^{t/2}$. Now $D'x = D \cong S_{i+1}^{t/2}$ implies that $D' \cong S_i^{t/2}$ and hence $\mathrm{soc}(V) \cap D' \cong S_a^{t/2} \cong \mathrm{soc}(V) \cap D$ so $\mathrm{soc}(V) \cap D' = \mathrm{soc}(V) \cap D$ and $D'/D \cap X_i = \{0\}$ which proves one direction of the Theorem. Now we start with an isotropic complement Y of X_i in W_i. Take D' to be the full preimage of Y in $D^{\perp}x^i$. Then $D' \leq Vx^i$ and

$$D'x = (D' + \mathrm{soc}(V))x = D^{\perp}x^i x = D.$$

This implies that the type of D' is $(0^i, t/2, 0^{a-i})$. We also conclude that $D \subseteq D'$ and ${D'}^{\perp} \subseteq D^{\perp}$. Moreover, as Y is maximal isotropic, we have

$${D'}^{\perp}x^i + D/D = Y^{\perp} = Y = D'/D$$

so $D' = {D'}^{\perp}x^i + D$. By Lemma 2.2 the Type of ${D'}^{\perp}$ is $(t/2, 0^{a-i}, t/2, 0^{i-2})$ and hence ${D'}^{\perp}x^i \cong D'$ so ${D'}^{\perp}x^i = D'$. □

2.3. Equivalence of codes

Let $U := \{r \in R \mid r\overline{r} = 1\}$ denote the unitary group of R. Then the action of the *monomial group*

$$\mathrm{Mon}_t(R) := \{\mathrm{diag}(u_1, \ldots, u_t)\pi \mid u_i \in U, \pi \in S_t\} \leq \mathrm{GL}_t(R)$$

on R^t respects duality. The monomial group is a semidirect product of the normal subgroup of diagonal matrices U^t and the subgroup of permutation matrices $P_t \cong S_t$, which is isomorphic to the symmetric group. As for fields (see [11, Lemma 1]) one shows the following property which is known to hold more generally in group theory.

Lemma 2.13. *Let $g \in \mathrm{Mon}_t(R)$ be an element of order r such that $\gcd(r, |U|) = 1$. Then g is conjugate in $\mathrm{Mon}_t(R)$ to some element of P_t.*

We call two codes $C, D \leq R^t$ *equivalent*, $C \sim D$, if there is some $g \in \mathrm{Mon}_t(R)$ with $C \cdot g = D$. The *automorphism group* $\mathrm{Aut}(C)$ is the stabilizer of C in $\mathrm{Mon}_t(R)$.

Our main strategy to construct self-dual codes over R is to successively construct self-dual codes over the residue field $\mathbb{F}$. Recall that the involution on R induces an involution $^-$ on $\mathbb{F} = R/xR$. Put $U(\mathbb{F}) := \{u \in \mathbb{F} \mid u\overline{u} = 1\}$.

Lemma 2.14. *The natural epimorphism induces an epimorphism $U \to U(\mathbb{F}), u \mapsto u + xR$.*

Proof. We first note that if $\mathrm{char}(\mathbb{F}) = 2$ and $^-$ is the identity on $\mathbb{F}$ then $U(\mathbb{F}) = \{1\}$ and the epimorphism is clearly surjective. So assume that either $2 \neq 0 \in \mathbb{F}$ or $^-$ is not the identity on $\mathbb{F}$. Let $u \in R$ such that $u\overline{u} = 1 + rx^j$ for some $r \in R$ with $\overline{r} \equiv r \pmod{xR}$ and $j \geq 1$. We need to find $v \in R$ such that

$$(u + vx^j)\overline{(u + vx^j)} = 1 + r'x^{j+1}$$

for some $r' \in R$. This results in solving

$$-r \equiv u\overline{v} + \overline{u}v \pmod{xR} \qquad (\star)$$

If $^-$ is the identity on $\mathbb{F}$ then $(\star)$ reads as $-r \equiv 2uv \pmod{xR}$ which has the solution $v \equiv \frac{-r}{2u} \pmod{xR}$ as $2u \in R^*$. If $^-$ is not the identity of $\mathbb{F}$ then $(\star)$ is equivalent to writing $-r + xR$ as the trace of some element in the finite field $\mathbb{F} = R/xR$. As the field trace is surjective and u is a unit, we can find such v. □

The *monomial group* over $\mathbb{F}$ is

$$\mathrm{Mon}_t(\mathbb{F}) := \{\mathrm{diag}(u_1, \ldots, u_t)\pi \mid \pi \in S_t, u_i \in U(\mathbb{F})\}.$$

Its action respects duality w.r.t. $\cdot$ and $(\cdot,\cdot)_i$. By Lemma 2.14 we obtain a group epimorphism

$$\mathrm{Mon}_t(R) \to \mathrm{Mon}_t(\mathbb{F}).$$

2.4. An algorithm to construct all self-dual free codes of length t

In the previous section we analyzed the structure of self-dual codes of length t over R that are free as an R-module. This structure can be used in an obvious way to build all such codes C by iteratively constructing the codes $C^{(i)} = Cx^i$ $(i = a, a-1, \ldots, 0)$ as self-dual submodules of $\mathbb{F}^t \cong W_i$. By Theorem 2.8 (c) the code $C^{(a)}$ is a (Hermitian) self-dual code in $\mathbb{F}^t$.

Algorithm 2.15. Input: *R, t, and the involution $^- : R \to R$*
Output: *A system $\mathcal{D}_0 = \{C_1, \ldots, C_h\}$ of representatives of the equivalence classes of free self-dual codes in $(V, \langle\cdot,\cdot\rangle)$.*
Algorithm:

(0) *Compute $\mathcal{D}_a := \{D_1^{(a)}, \ldots, D_{h_a}^{(a)}\}$ a system of representatives of equivalence classes of (Hermitian) self-dual codes in $(\mathbb{F}^t, \cdot)$.*
(1) *For $i = a-1, a-2, \ldots, 0$ assume that we are given $\mathcal{D}_{i+1} := \{D_1^{(i+1)}, \ldots, D_{h_{i+1}}^{(i+1)}\}$ a system of representatives of equivalence classes of codes $D \leq Vx^{i+1}$ of type $(0^{i+1}, t/2, 0^{a-i-1})$ with $D^{\perp}x^{i+1} = D$.*
(2) *Put $\mathcal{D}_i := \{\}$.*
(3) *For $j = 1, \ldots, h_{i+1}$ put $D := D_j^{(i+1)}$, $W_i := D^{\perp}x^i/D$ as in Lemma 2.11 and compute the set $\mathcal{Y} := \{D' \leq Vx^i \mid D'x = D, D'^{\perp}x^i = D'\}$ using Theorem 2.12.*
(4) *For all $D' \in \mathcal{Y}$ check if D' is equivalent to some code in $\mathcal{D}_i$. If not then include D' to $\mathcal{D}_i$.*
(5) *If $i = 0$ then return $\mathcal{D}_0$.*

For the computation of the set $\mathcal{Y}$ in Algorithm 2.15 (3) we need to compute the isotropic complements Y of X_i in $(W_i, (\cdot,\cdot)_i)$. To this aim we choose some complement $\tilde{Y}$ of X_i in W_i. As W_i is non-degenerate and X_i is maximal isotropic in W_i, the space $\tilde{Y}_i$ is isomorphic to $\mathrm{Hom}(X_i, \mathbb{F})$. In particular there are suitable bases of X_i resp. $\tilde{Y}_i$ such that the Gram matrix of $(\cdot,\cdot)_i$ is of the form

$$\begin{pmatrix} 0 & I \\ \epsilon^{a+i}I & G \end{pmatrix}$$

for some ϵ^{a+i}-Hermitian matrix G.

Remark 2.16. There is an isotropic complement Y of X_i in W_i, if and only if $G \in \mathcal{H}$, where

$$\mathcal{H} := \{X + \epsilon^{a+i}\overline{X}^{tr} \mid X \in \mathbb{F}^{t/2\times t/2}\}.$$

Note that $\mathcal{H}$ is the space of all ϵ^{a+i}-Hermitian matrices, if and only if either $2 \neq 0$ in $\mathbb{F}$ or $^-$ is not the identity. If $2 = 0$ in $\mathbb{F}$ and $^- = \mathrm{id}$, then $G \in \mathcal{H}$ if and only if $G_{ii} = 0$ for all $1 \leq i \leq t/2$.

If the code D lifts to a code D', then there is such an isotropic complement Y of X_i and we choose bases B and B' of X_i resp. Y_i such that the Gram matrix of $(\cdot,\cdot)_i$ with respect to the basis (B, B') of W_i is of the form

$$\begin{pmatrix} 0 & I \\ \epsilon^{a+i}I & 0 \end{pmatrix}.$$

Proposition 2.17. *The self-dual complements of X_i in W_i are exactly the subspaces $\langle B' + AB\rangle$ with $A \in \mathbb{F}^{t/2\times t/2}$ satisfying*

$$\overline{A}^{tr} + \epsilon^{a+i}A = 0.$$

The set of all such matrices A forms a vector space of dimension d over the fixed field of $^-$ in $\mathbb{F}$, where

char($\mathbb{F}$)	ϵ^{a+i}	$^-$	d
$\neq 2$	1	id	$t(t-2)/8$
all	-1	id	$t(t+2)/8$
all	1	$\neq$ id	$t^2/4$

Proof. Every complement of X_i has some basis $B' + AB$ with $A \in \mathbb{F}^{t/2\times t/2}$. This basis is isotropic, if and only if

$$\begin{pmatrix} I & A \end{pmatrix}\begin{pmatrix} 0 & I \\ \epsilon^{a+i}I & 0 \end{pmatrix}\begin{pmatrix} I \\ \overline{A}^{tr} \end{pmatrix} = \overline{A}^{tr} + \epsilon^{a+i}A = 0.$$

The dimension d is hence the dimension of the space of all skew-symmetric, symmetric, respectively skew-hermitian matrices. □

3. Gray images of self-dual $\mathbb{Z}_4$-linear codes

Many papers use the methods above for chain rings of order 4, in particular $\mathbb{F}_2[x]/(x^2)$ and $\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$. This section relates our methods over the ring $R = \mathbb{Z}/4\mathbb{Z}$ to the ones applied in [19] to show more general bounds on the minimum distance of codes over R. Recall that the Gray map $\Phi : R^t \to \mathbb{F}_2^{2t}$ is defined by mapping the letters $(0, 1, -1, 2)$ to $((0,0),(1,0),(0,1),(1,1))$ respectively. The Gray map defines an isometry between the Lee distance on R^t and the Hamming distance on $\mathbb{F}_2^{2t}$, but it should be noted that it is not a group homomorphism, in particular $\Phi(C)$ needs not be a linear code. We obtain the following generalization of the result in [13] which was certainly known to Rains but is not explicitly observed in [19]:

Theorem 3.1. *Let m be odd and $C = C^\perp \leq R^{12m}$ be a self-dual R-linear code. Then the Gray image $\Phi(C) \subseteq \mathbb{F}_2^{24m}$ has minimum distance $\leq 4m$. In particular $\Phi(C)$ does not have the parameters of an extremal Type II code.*

Proof. (of Theorem 3.1) By Theorem 2.8 (b) $\pi(2C) \leq \mathbb{F}_2^{12m}$ is a self-orthogonal binary code of length $12m$ with $\pi(2C)^\perp = \pi(\mathrm{soc}(C))$. As C is self-dual we obtain for all $c \in C$

$$0 = (c,c) = \sum_{i=1}^{12m} c_i^2 = |\{i \mid c_i \in \{\pm 1\}\}| + 4\mathbb{Z} = \mathrm{wt}(\pi(2c)) + 4\mathbb{Z}$$

in particular $\pi(2C)$ is doubly-even. As m is odd and hence $12m$ is not a multiple of 8 the code $\pi(2C)$ is not self-dual. By the bound in [19] (for $12m \equiv_{24} 12$) we find that $d(\pi(2C)^\perp) \leq 4((m-1)/2) + 2 = 2m$. Therefore the Gray image $\Phi(\mathrm{soc}(C))$ contains a vector of Hamming weight $4m$. □

4. Automorphisms of linear codes

The study of automorphisms of extremal codes has been initiated by Conway and Pless [5] and independently by Huffman [10] motivated by a question asked by Neil Sloane in 1972 [20]. In the meantime there is a huge amount of literature investigating putative extremal codes invariant under a given automorphism (see for instance [3], [15] or [2]). The study of automorphisms of p-power order of codes over a finite field of characteristic p can be seen as one important application of the methods developed in Section 2.

4.1. The general setup

Let $\mathbb{F}$ be a finite field of characteristic p and $^- : \mathbb{F} \to \mathbb{F}$ be some automorphism of order 1 or 2. In classical coding theory a linear code over $\mathbb{F}$ or length n is a subspace C of $\mathbb{F}^n$. The dual code $C^\perp$ is the orthogonal space with respect to the *standard Hermitian dot inner product*

$$v \cdot w = \sum_{j=1}^{n} v_j \overline{w_j}.$$

The unitary group $U(\mathbb{F})$ defined in Section 2.3 has order 1 or 2, $U(\mathbb{F}) = \{1, -1\}$ if $^- = \mathrm{id}$. If $^- \neq \mathrm{id}$ then $|\mathbb{F}|$ is a square and $|U(\mathbb{F})| = \sqrt{|\mathbb{F}|} + 1$.

One major application of the results of the previous section is the study of codes over finite fields $\mathbb{F}$ of characteristic p admitting an automorphism g of order $q = p^e$. Then the group ring $R := \mathbb{F}\langle g\rangle$ is an Artinian chain ring with ideals Rx^i $(0 \leq i \leq q)$ where $x := (1 - g)$. It carries a natural involution defined by

$$\overline{\sum_{i=0}^{q-1} \alpha_i g^i} := \sum_{i=0}^{q-1} \overline{\alpha_i} g^{-i}.$$

As $\overline{x} + x = (1 - g^{-1}) + (1 - g) = (1 - g)(1 - g^{-1})$ we get

Remark 4.1. $\overline{x} = -x + x\overline{x} = -x - x^2 - \ldots - x^{q-1}$ so $\epsilon = -1$ in the notation of Section 2. In the Hermitian case we choose $u \in \mathbb{F}$ with $u\overline{u} = -1$ and replace x by ux to obtain $\overline{x} \equiv x \pmod{Rx^2}$.

The canonical epimorphism of $R = \mathbb{F}\langle g\rangle$ onto $\mathbb{F}$ is usually called the *augmentation* defined by

$$\mathrm{aug}(\sum_{i=0}^{q-1} \alpha_i g^i) = \sum_{i=0}^{q-1} \alpha_i.$$

Note that $(1 - g)\mathbb{F}\langle g\rangle$ is the kernel of the augmentation map. We will also need the $\mathbb{F}$-linear *trace* mapping $\sum_{i=0}^{q-1} \alpha_i g^i$ to the coefficient α_0.

4.2. The fixed point free case

The theory of Section 2 can be applied directly if we assume that C is a self-dual code admitting an automorphism of prime order $p = \mathrm{char}(\mathbb{F})$ that acts without fixed points on $\{1, \ldots, n\}$. In this case $n = tp$ is a multiple of p and this automorphism is conjugate in $\mathrm{Mon}_n(\mathbb{F})$ to

$$g = (1, 2, \ldots, p)(p + 1, p + 2, \ldots, 2p) \cdots ((t - 1)p + 1, \ldots, tp).$$

So replacing C by some equivalent code, we may assume that $g \in \mathrm{Aut}(C)$. Moreover $\mathbb{F}^n \cong R^t =: V$ is a free R-module of rank t, where $R = \mathbb{F}\langle g\rangle$ is as before. So we are in the situation of Section 2 with $a = p - 1$ (which is even if $p \neq 2$). If $t = 1$ then the codes in V are the well-known cyclic codes. The general case is not much harder:

Remark 4.2. The mapping

$$\mathbb{F}^n \to R^t, (c_1, \ldots, c_{pt}) \mapsto (\sum_{i=1}^{p} c_i g^{i-1}, \ldots, \sum_{i=1}^{p} c_{(t-1)p+i} g^{i-1})$$

defines an isomorphism of $\mathbb{F}\langle g\rangle$-modules transfering the standard Hermitian dot inner product into the trace of $\langle\cdot,\cdot\rangle$, i.e.

$$c \cdot d = \text{trace}(\langle c, d\rangle).$$

So this mapping defines a one-to-one correspondence between the self-dual codes in R^t (with respect to $\langle\cdot,\cdot\rangle$ defined in Equation (2.1)) and the self-dual codes $C \leq \mathbb{F}^n$ with $g \in \mathrm{Aut}(C)$. The usual notion of equivalence transfers to the action of the centralizer $\mathrm{Mon}_t(R) = C_{\mathrm{Mon}_n(\mathbb{F})}(g)$.

The socle of the R-module V is the set

$$\mathrm{soc}(V) = \{d := (\underbrace{d_1, \ldots, d_1}_{p}, \ldots, \underbrace{d_t, \ldots, d_t}_{p}) \mid d_i \in \mathbb{F}, 1 \leq i \leq t\}$$

and is canonically isomorphic to $\mathbb{F}^t$ via

$$\pi : \mathrm{soc}(V) \to \mathbb{F}^t, d \mapsto (d_1, \ldots, d_t).$$

For a code C with $g \in \mathrm{Aut}(C)$ we define the fixed code of $\langle g\rangle$ to be

$$C(g) := \{c \in C \mid c \cdot g = c\} = C \cap \mathrm{soc}(V) = \mathrm{soc}(C).$$

We define a map

$$\Phi : V \to \mathbb{F}^t, (v_1, \ldots, v_t) \mapsto (\mathrm{aug}(v_1), \ldots, \mathrm{aug}(v_t)).$$

Note that $\Phi(v) = \pi(v \cdot (1-g)^{p-1})$. As $(1-g)^a = (1-g)^{p-1} = 1 + g + \ldots + g^{p-1}$ Proposition 2.6 translates as follows.

Proposition 4.3. *Let $C \leq \mathbb{F}^{pt}$ with $g \in \mathrm{Aut}(C)$. Then with respect to the standard dot inner product on $\mathbb{F}^t$*

$$\Phi(C^\perp)^\perp = \pi(C(g)).$$

4.3. Automorphisms with fixed points

Let $C = C^\perp \leq \mathbb{F}^n$ a self-dual code with respect to the standard Hermitian dot inner product. The first lemma is elementary linear algebra and does not need any automorphisms. It is known as the balance principle and for instance proven in [12, Theorem 9.4.1].

Lemma 4.4. *C has a generator matrix of the form*

$$\begin{pmatrix} B & 0 \\ 0 & D \\ E & F \end{pmatrix} \text{ where } B \in \mathbb{F}^{k_1 \times qt}, D \in \mathbb{F}^{k_2 \times f}, k_3 = \frac{n}{2} - k_1 - k_2 = Rk(E) = Rk(F).$$

Define

$$\mathcal{B} := \langle (B|0)\rangle, \mathcal{B}^* := \langle B\rangle, \mathcal{B}_E := \langle \begin{pmatrix} B \\ E \end{pmatrix}\rangle, \mathcal{D}^* := \langle D\rangle, \mathcal{D}_F := \langle \begin{pmatrix} D \\ F \end{pmatrix}\rangle.$$

Then $\mathcal{B}_E^\perp = \mathcal{B}^*$ and $\mathcal{D}_F^\perp = \mathcal{D}^*$.

Let $p := \mathrm{char}(\mathbb{F})$ and assume that there is some element $g \in \mathrm{Aut}(C)$ of p-power order q. Then by Lemma 2.13 the element g is conjugate in $\mathrm{Mon}_n(\mathbb{F})$ to some element σ of $P_n \cong S_n$. Assume that σ has only cycles of length q and 1. Replacing C by some equivalent code we hence may assume wlog that

$$g = (1, 2, \ldots, q)(q+1, q+2, \ldots, 2q) \cdots ((t-1)q+1, \ldots, tq)(tq+1) \cdots (n)$$

where $f = n - qt$ is the number of fixed points of g. Then $\mathbb{F}^n \cong R^t \oplus \mathbb{F}^f \cong R^t \oplus S_{q-1}^f$ where $R = \mathbb{F}\langle g\rangle$ is the chain ring from Section 4.1 and in the notation of Lemma 4.4 the code C is constructed as

$$C = \{(x, y) \mid x \in \mathcal{B}_E, y \in \mathcal{D}_F, \psi(x) = y + \mathcal{D}^*\}$$

from self-orthogonal codes

$$\mathcal{B}^* \subseteq \mathcal{B}^{*\perp} = \mathcal{B}_E \leq R^t$$

and

$$\mathcal{D}^* \subseteq \mathcal{D}^{*\perp} = \mathcal{D}_F \leq \mathbb{F}^f$$

using a g-equivariant anti-isometry $\psi : \mathcal{B}^{*\perp}/\mathcal{B}^* \to \mathcal{D}^{*\perp}/\mathcal{D}^*$. Though we could formulate the result in the language of Section 4.1 as illustrated in the previous section, we prefer to use the more explicit language as in the relevant literature.

Proposition 4.5. *(See* [3] *for $q = 2$ and Proposition* 4.3 *for $f = 0$)*
Let $V(g) := \{v \in \mathbb{F}^n \mid v \cdot g = v\}$ so that $C(g) := V(g) \cap C$ is the fixed code of g. Define

$$\pi_g : V(g) \to \mathbb{F}^t, (\underbrace{c_1, \ldots, c_1}_{q}, \underbrace{c_2, \ldots, c_2}_{q}, \ldots, \underbrace{c_t, \ldots, c_t}_{q}, x_1, \ldots, x_f) \mapsto (c_1, \ldots, c_t)$$

and

$$\Phi_g : \mathbb{F}^n \to \mathbb{F}^t, (c_1, \ldots, c_n) \mapsto (c_1 + c_2 + \ldots + c_q, \ldots, c_{(t-1)q+1} + \ldots + c_{tq}).$$

Then Φ_g is a $\langle g \rangle$-invariant homomorphism satisfying

$$v \cdot w = \pi_g(v) \cdot \Phi_g(w) \text{ for all } v \in V(g), w \in \mathbb{F}^n. \qquad (\star)$$

Let $\mathcal{B}$ be as in Lemma 4.4 *with $k_1 = tq$ and put $B(g) := C(g) \cap \mathcal{B}$. Then $\Phi_g(C)$ is a self-orthogonal code with*

$$\Phi_g(C)^\perp = \pi_g(B(g)), \Phi_g(\mathcal{B})^\perp = \pi_g(C(g)).$$

Proof. The equation $(\star)$ follows by direct computation. Since $B(g) \subseteq C = C^\perp$ and $C(g), \mathcal{B} \subseteq C = C^\perp$ the equation $(\star)$ implies that $\pi_g(B(g)) \subset \Phi_g(C)^\perp$ and $\pi_g(C(g)) \subset \Phi_g(\mathcal{B})^\perp$. Moreover, if $c = (c_1, \ldots, c_n) \in C$ then

$$\begin{aligned} d :=& c \cdot (1 + g + \ldots + g^{q-1}) \\ =& (\underbrace{\sum_{i=1}^{q} c_i, \ldots, \sum_{i=1}^{q} c_i}_{q}, \ldots, \underbrace{\sum_{i=1}^{q} c_{(t-1)q+i}, \ldots, \sum_{i=1}^{q} c_{(t-1)q+i}}_{q}, \underbrace{0, \ldots, 0}_{f}) \in B(g) \end{aligned}$$

satisfies $\pi_g(d) = \Phi_g(c)$, so $\Phi_g(\mathcal{B}) \subset \Phi_g(C) \subset \pi_g(B(g)) \subset \pi_g(C(g))$.
Now assume that $(d_1, \ldots, d_t) \in \Phi_g(C)^\perp$. Then the vector

$$v := (\underbrace{d_1, \ldots, d_1}_{q}, \ldots, \underbrace{d_t, \ldots, d_t}_{q}, \underbrace{0, \ldots, 0}_{f}) \in \mathbb{F}^n$$

is fixed under g, has the last f coordinates equal to 0. Moreover $v \in C^\perp = C$, since

$$v \cdot c = \pi_g(v) \cdot \Phi_g(c) = 0 \text{ for all } c \in C.$$

So $v \in B(g)$ and in total $\Phi_g(C)^\perp \subset \pi_g(B(g))$.
Now assume that $d := (d_1, \ldots, d_t) \in \Phi_g(\mathcal{B})^\perp$. For any $x \in \mathbb{F}^f$ the element

$$v_x := (\underbrace{d_1, \ldots, d_1}_{q}, \ldots, \underbrace{d_t, \ldots, d_t}_{q}, x) \in V(g)$$

satisfies $\pi_g(v_x) = d$ and for any $b \in \mathcal{B}$ the inner product

$$v_x \cdot b = \pi_g(v_x) \cdot \Phi_g(b) = d \cdot \Phi_g(b) = 0.$$

As the projection from C onto $\mathcal{B}_E$ is surjective and $\mathcal{B}_E = (\mathcal{B}^*)^\perp$ we conclude that there is some $x \in \mathbb{F}^f$ such that $v_x \in C(g)$. □

5. Extremal ternary self-dual codes of length 36

To illustrate how to apply the methods from Section 2 to the situation considered in Section 4 we consider ternary codes with an automorphism of order 3.

In [11] Cary Huffman classified all extremal self-dual ternary codes of length 28 to 40 that have an automorphism of prime order ≥ 5 resp. ≥ 7 (see also [16] for the length 48 case). By [11, Theorem 5] there is a unique self-dual $[36, 18, 12]$-code having an automorphism of prime order ≥ 5, the well known Pless code P_{36} (see [18]), whose automorphism group is

$$\mathrm{Aut}(P_{36}) \cong (\mathrm{PSL}_2(17) \times C_4).2$$

of order $2^7 3^2 17$. In this section we use the theory developed in Section 2 to show that the Pless code is the unique extremal self-dual ternary code of length 36 having an automorphism of order 3 or a non-trivial automorphism of order 2. Combining this result with the one in [11] and [6] we obtain the following theorem.

Theorem 5.1. *Let $C = C^\perp \leq \mathbb{F}_3^{36}$ be a ternary self-dual code of length 36 with minimum distance $d(C) = 12$. Then either $C \cong P_{36}$ or $\mathrm{Aut}(C)$ is a subgroup of $C_8 = \langle g \mid g^4 = -1 \rangle$.*

The classification of codes with automorphism group C_8 boils down to classifying LCD codes (so $C \cap C^\perp = \{0\}$) with $C \leq \mathbb{F}_9^9$ such that $d(C) \geq 4$ and $d(C^\perp) \geq 4$. If we assume that the automorphism group is of order 4, then the problem is equivalent to listing Hermitian self-dual codes of length 18 over $\mathbb{F}_9$ with minimum distance 8 or 9. Both problems seem to be attackable with a huge computation, but they are beyond the scope of this paper.

So for the rest of this section let $C = C^\perp \leq \mathbb{F}_3^{36}$ be a ternary self-dual code of length 36 with minimum distance $d(C) = 12$. And let $g \in \mathrm{Aut}(C)$ be an automorphism of order 3. Then g is conjugate in the full monomial group to some permutation and replacing C by some equivalent code we may assume that

$$g = (1, 2, 3) \cdots (3t - 2, 3t - 1, 3t)$$

for some $1 \leq t \leq 12$. Put $f := 36 - 3t$.

Lemma 5.2. *$t = 12$ and $f = 0$.*

Proof. We first apply the balance principle from Lemma 4.4 to obtain a self-orthogonal $\langle g \rangle$-invariant code $\mathcal{B}^*$ in the free $\mathbb{F}_3\langle g \rangle$-module $V = \mathbb{F}_3\langle g \rangle^t$ with

$$\mathcal{B}^* \subseteq (\mathcal{B}^*)^\perp = \mathcal{B}_E \leq \mathbb{F}_3^{3t} \cong \mathbb{F}_3\langle g \rangle^t.$$

As $\mathcal{B}_E \cdot (1-g) \subseteq \mathcal{B}$, Lemma 2.3 implies that the isomorphism type (t_0, t_1, t_2) of $\mathcal{B}^* \cong S_0^{t_0} \oplus S_1^{t_1} \oplus S_2^{t_2}$ satisfies

$$\begin{array}{lcl} 2t_0 + 2t_1 + t_2 & \geq & t \\ 2t_0 + t_1 + t_2 & \leq & t \\ 2t_0 + 2t_1 & \leq & t. \end{array}$$

We now apply Proposition 2.6 to the code $\mathcal{B}^*$ instead of C. We have $\mathcal{B}_E \cdot (1 - g) \subseteq \mathcal{B}^*$ and $\mathrm{soc}(\mathcal{B}^*) = \mathcal{B}^*(g)$ so by Remark 2.7 and Proposition 4.3

$$\Phi(\mathcal{B}_E) \subseteq \Phi(\mathcal{B}_E)^\perp = \pi(\mathcal{B}^*(g)).$$

In particular $\pi(\mathcal{B}^*(g)) \leq \mathbb{F}_3^t$ is the dual of a self-orthogonal code of length t, has dimension $t_0 + t_1 + t_2 \geq t/2$ and minimum distance $\geq \frac{12}{3} = 4$. Moreover $\pi(\mathcal{B}^*(g))$ always contains the dual of a maximal self-orthogonal code, so the bounds in [14] imply that $t = 10, 11$, or $t = 12$ and $f = 6, 3, 0$ in the respective cases. So in any case $f \leq 12 = d(C)$ and hence $\mathcal{D}^* = 0$ and $\dim(\mathcal{B}^*) = 3t_0 + 2t_1 + t_2 = 18 - f$.

In the case $t = 10$, the code $\pi(\mathcal{B}^*(g)) = \Phi(\mathcal{B}_E)^\perp$ has dimension of at least 6, by the Griesmer bound it can't have dimension 7. So $t_0 + t_1 + t_2 = 6$, together with the bounds of Lemma 2.3 the possible types of $\mathcal{B}^*$ are $(1, 4, 1)$ and $(2, 2, 2)$, the type of $\mathcal{B}_E^*$ is therefore $(4, 1, 4)$ resp. $(4, 2, 2)$. By [8] there

are 5 maximal self-orthogonal codes of length 10, only one of which, C' say, has dual distance 4. So $\pi(\mathcal{B}^*(g)) = (C')^\perp$ and $\pi(\mathcal{B}_E^*(g))$ is an overcode of dimension 9 or 8 of $(C')^\perp$ with minimum distance $\geq (12-f)/3 = 2$. There is a unique such overcode X of dimension 8 (up to the action of $\mathrm{Aut}(C')$). The code X contains two elements $c_1 \neq \pm c_2$ of weight 2 with $|\operatorname{supp}(c_1) \cup \operatorname{supp}(c_2)| = 3$. Wlog $\mathcal{B}_E^*$ hence contains elements

$$x_1 = (c_1 \otimes (1,1,1), 1^6), \text{ and } x_2 = (c_2 \otimes (1,1,1), 1^e(-1)^{6-e}) \text{ for some } e,$$

but then one of $x_1 \pm x_2$ has weight less than 11. A contradiction.
In the case $t = 11$, by [8] there is a unique maximal self-orthogonal code of length 11 with dual distance ≥ 4. Up to the action of its automorphism group, this code only has two overcodes with minimum distance 1 resp. 2. Hence $\pi(\mathcal{B}^*(g))$ is of dimension 6 and with the bounds of Lemma 2.3 the type $\mathcal{B}^*$ is $(4,1,1)$ and the one of $\mathcal{B}_E^*$ is $(5,1,1)$, so $\pi(\mathcal{B}_E^*(g))$ is an overcode of $\pi(\mathcal{B}^*(g))$ of dimension 7. But as already shown, all such overcodes have minimum distance $< (12-f)/3 = 3$. A contradiction. □

So we are left with the classification of all $C = C^\perp \leq \mathbb{F}_3^{36}$ with

$$g = (1,2,3)\cdots(34,35,36) \in \mathrm{Aut}(C).$$

Then $\mathbb{F}_3^{36} = V \cong R^{12}$ is a free $\mathbb{F}_3\langle g\rangle$-module of rank 12. Using Theorem 2.8 we obtain

Proposition 5.3. *C is a free $\mathbb{F}_3\langle g\rangle$-module.*

Proof. By Theorem 2.8 (c) it is enough to consider $\pi(\mathrm{soc}(C)) \leq (\mathbb{F}_3^{12}, \cdot)$. This is the dual of some self-orthogonal code and has minimum distance ≥ 4. As 12 is a multiple of 4 it hence contains a self-dual code of minimum distance ≥ 6. There is a unique such code, the extended quadratic residue code XQ_{11}. An easy computation in MAGMA shows that no proper overcode of XQ_{11} has minimum distance ≥ 4. So $\mathrm{soc}(C) = C \cdot (1-g)^2$ and C is a free module. □

Corollary 5.4. *C contains a subcode $C^{(2)} = XQ_{11} \otimes \langle(1,1,1)\rangle$.*

We now are in the position to apply Algorithm 2.15. The centralizer of g in $\mathrm{Aut}(C^{(2)})$ has 16 orbits on the set of all 3^{21} self-dual complements of $X_1 \leq W_1$ all of which correspond to candidates for codes $C^{(1)}$ of minimum distance 12. For these 16 codes we check all of the 3^{15} self-dual complements of $X_0 \leq W_0$ for minimum distance 12 and find up to equivalence a unique such code $C^{(0)}$. So we have shown the following

Theorem 5.5. *Let $C = C^\perp \leq \mathbb{F}_3^{36}$ with $d(C) = 12$ and $3 \mid |\mathrm{Aut}(C)|$. Then $C \cong P_{36}$.*

To complete the proof of Theorem 5.1 we remark that [6] has shown that P_{36} is the unique extremal code admitting a non-trivial automorphism of order 2. So the automorphism group of any other extremal ternary code of length 36 is contained in $C_8 = \langle g \mid g^4 = -1\rangle$.

References

[1] Martino Borello and Gabriele Nebe. On involutions in extremal self-dual codes and the dual distance of semi self-dual codes. *Finite Fields Appl.*, 33:80–89, 2015.

[2] Martino Borello and Wolfgang Willems. Automorphisms of order $2p$ in binary self-dual extremal codes of length a multiple of 24. *IEEE Trans. Inform. Theory*, 59(6):3378–3383, 2013.

[3] Stefka Bouyuklieva. On the automorphisms of order 2 with fixed points for the extremal self-dual codes of length $24m$. *Des. Codes Cryptogr.*, 25(1):5–13, 2002.

[4] Stefka Bouyuklieva. A method for constructing self-dual codes with an automorphism of order 2. *IEEE Trans. Inform. Theory*, 46(2):496–504, 2000.

[5] J.H. Conway, V. Pless, On primes dividing the group order of a doubly-even (72; 36; 16) code and the group order of a quaternary (24; 12; 10) code. Discrete Math. 38 (1982) 143-156.

[6] Simon Eisenbarth. *Gitter und Codes über Kettenringen*. Thesis. RWTH Aachen University, 2019.

[7] A. Roger Hammons, Jr., P. Vijay Kumar, A. R. Calderbank, N. J. A. Sloane, and Patrick Solé. The $\mathbf{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Trans. Inform. Theory*, 40(2):301–319, 1994.

[8] Masaaki Harada and Akihiro Munemasa. Database of ternary maximal self-orthogonal codes. *http://www.math.is.tohoku.ac.jp/ munemasa/research/codes/mso3.htm*.

[9] Sheridan K. Houghten, Clement W. H. Lam, Larry H. Thiel, and Jeff A. Parker. The extended quadratic residue code is the only $(48, 24, 12)$ self-dual doubly-even code. *IEEE Trans. Inform. Theory*, 49(1):53–59, 2003.

[10] W. Cary Huffman. Automorphisms of codes with applications to extremal doubly even codes of length 48. *IEEE Trans. Inform. Theory*, 28(3):511–521, 1982.

[11] W. Cary Huffman. On extremal self-dual ternary codes of lengths 28 to 40. *IEEE Trans. Inform. Theory*, 38(4):1395–1400, 1992.

[12] W. Cary Huffman and Vera Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.

[13] Michael Kiermaier. There is no self-dual $\mathbb{Z}_4$-linear code whose gray image has the parameters $(72, 2^{36}, 16)$. *IEEE Trans. Inform. Theory*, 59(6):3384–3386, 2013.

[14] Annika Meyer. On dual extremal maximal self-orthogonal codes of type I-IV. *Adv. Math. Commun.*, 4(4):579–596, 2010.

[15] Gabriele Nebe. An extremal $[72, 36, 16]$ binary code has no automorphism group containing $Z_2 \times Z_4$, Q_8, or Z_{10}. *Finite Fields Appl.*, 18(3):563–566, 2012.

[16] Gabriele Nebe. On extremal self-dual ternary codes of length 48. *Int. J. Comb.*, Art. ID 154281, 9, 2012.

[17] Gabriele Nebe, Eric M. Rains, and Neil J. A. Sloane. *Self-dual codes and invariant theory*, volume 17 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2006.

[18] Vera Pless. Symmetry codes over $\mathrm{GF}(3)$ and new five-designs. *J. Combinatorial Theory Ser. A*, 12:119–142, 1972.

[19] Eric Rains. Bounds for self-dual codes over Z_4. *Finite Fields Appl.*, 6(2):146–163, 2000.

[20] N.J.A. Sloane, Is there a (72; 36), d = 16 self-dual code? IEEE Trans. Inform. Theory 19 (1973) 251

Simon Eisenbarth
Lehrstuhl D für Mathematik
RWTH Aachen
Pontdriesch 14/16
D-52062 Aachen

e-mail: simon.eisenbarth@rwth-aachen.de

Gabriele Nebe
Lehrstuhl D für Mathematik
RWTH Aachen
Pontdriesch 14/16
D-52062 Aachen

e-mail: gabriele.nebe@rwth-aachen.de