

# Automorphisms of doubly-even self-dual binary codes.

Annika Günther and Gabriele Nebe

## ABSTRACT

The automorphism group of a binary doubly-even self-dual code is always contained in the alternating group. On the other hand, given a permutation group  $G$  of degree  $n$  there exists a doubly-even self-dual  $G$ -invariant code if and only if  $n$  is a multiple of 8, every simple self-dual  $\mathbb{F}_2G$ -module occurs with even multiplicity in  $\mathbb{F}_2^n$ , and  $G$  is contained in the alternating group.

## 1. Introduction.

Self-dual binary codes have become of great interest, also because of Gleason's theorem [4] that establishes a connection between coding theory and invariant theory of finite groups. Optimal self-dual codes often have the additional property of being doubly-even, which means that the weight of every codeword is divisible by 4 (see Definition 1). It follows from Gleason's theorem that the length  $n$  of a doubly-even self-dual code  $C \leq \mathbb{F}_2^n$  is a multiple of 8, see [7, Theorem 3c], for instance.

This note studies the automorphism group  $\text{Aut}(C) := \{\pi \in \text{Sym}_n \mid C\pi = C\}$  of such a code.

Theorem 5.1 shows that the automorphism group of any doubly-even self-dual code is always contained in the alternating group, a very basic result which astonishingly does not seem to be known. On the other hand Theorem 5.2 characterizes the permutation groups  $G \leq \text{Sym}_n$  that fix a doubly-even self-dual binary code. This result generalizes results by Sloane and Thompson [9] and Martínez-Pérez and Willems [11].

The first section considers codes as modules for their automorphism group. The main result is the characterization of permutation groups that act on a self-dual code in Theorem 2.1. Section 4 treats permutation groups as subgroups of the 2-adic orthogonal groups. The most important observation is Lemma 4.2 that expresses the sign of a permutation as a certain spinor norm. Given a self-dual doubly-even binary code  $C$ , the automorphism group of the even unimodular  $\mathbb{Z}_2$ -lattice obtained from  $C$  by construction A (see Section 3) is contained in the kernel of this spinor norm. This immediately yields Theorem 5.1. Theorem 5.2 follows from this result together with Theorem 2.1.

## 2. Codes.

DEFINITION 1. A binary code  $C$  of length  $n$  is a linear subspace of  $\mathbb{F}_2^n$ . Let  $b : \mathbb{F}_2^n \times \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ ,  $b(x, y) := \sum_{i=1}^n x_i y_i$  be the standard scalar product. The dual code is

$$C^\perp := \{v \in \mathbb{F}_2^n \mid b(v, c) = 0 \text{ for all } c \in C\}.$$

The code  $C$  is called *self-orthogonal* if  $C \subseteq C^\perp$  and *self-dual* if  $C = C^\perp$ . The *weight*  $\text{wt}(c)$  of a codeword  $c \in C$  is the number of its nonzero entries. The code  $C$  is called *doubly-even*, or *Type II*, if the weight of every word in  $C$  is a multiple of 4.

This section investigates binary linear codes as modules for a subgroup  $G$  of their automorphism groups. The main result is Theorem 2.1 that characterizes the permutation groups acting on some self-dual code. To this aim we need the representation theoretic notion of self-dual modules, cf. Definition 2. Note that this paper uses two different notions of duality. The dual of an  $\mathbb{F}_2G$ -module  $S$  over the finite group  $G$  is the  $\mathbb{F}_2G$ -module  $S^* = \text{Hom}_{\mathbb{F}_2}(S, \mathbb{F}_2)$ , whereas the dual of a code  $C \leq \mathbb{F}_2^n$  is as in Definition 1. For  $G \leq \text{Aut}(C)$  the code  $C$  is also an  $\mathbb{F}_2G$ -module, which is represented with respect to a distinguished basis.

**DEFINITION 2.** Let  $S$  be a right  $G$ -module. Then the *dual module*  $S^* = \text{Hom}_{\mathbb{F}_2}(S, \mathbb{F}_2)$  is a right  $G$ -module via  $fg(s) := f(sg^{-1})$ , for  $f \in S^*$ ,  $g \in G$  and  $s \in S$ . If  $S \cong S^*$  then  $S$  is called *self-dual*.

**THEOREM 2.1.** Let  $G \leq \text{Sym}_n$ . Then there exists a self-dual code  $C \leq \mathbb{F}_2^n$  with  $G \leq \text{Aut}(C)$  if and only if every self-dual simple  $\mathbb{F}_2G$ -module  $S$  occurs in the  $\mathbb{F}_2G$ -module  $\mathbb{F}_2^n$  with even multiplicity.

The proof of this theorem is prepared in a few lemmas.

**LEMMA 2.2.** Let  $S$  be a simple self-dual  $\mathbb{F}_2G$ -module, and assume that  $S$  carries a non-degenerate symmetric  $G$ -invariant bilinear form  $\varphi : S \times S \rightarrow \mathbb{F}_2$ . Then  $\varphi$  is unique, up to isometry.

*Proof.* Since  $\varphi$  is non-degenerate and  $G$ -invariant, it induces an  $\mathbb{F}_2G$ -isomorphism  $\alpha_\varphi : S \rightarrow S^*$ ,  $s \mapsto (s' \mapsto \varphi(s, s'))$ . Let  $\psi : S \times S \rightarrow \mathbb{F}_2$  be another non-degenerate symmetric  $G$ -invariant bilinear form on  $S$ , then  $\alpha_\psi = \alpha_\varphi \circ \vartheta$  for some  $\vartheta$  in the finite field  $\mathfrak{E} := \text{End}_G(S)$  of all  $\mathbb{F}_2G$ -endomorphisms of  $S$ , and hence

$$\psi(s, s') = \alpha_\psi(s)(s') = \alpha_\varphi(\vartheta(s))(s') = \varphi(\vartheta(s), s')$$

for all  $s, s' \in S$ . Consider the involution  $\text{ad}$  on  $\mathfrak{E}$  given by  $\varphi(s, \alpha(s')) = \varphi(\alpha^{\text{ad}}(s), s')$ , for  $s, s' \in S$ . Since both  $\varphi$  and  $\psi$  are symmetric we have

$$\varphi(\vartheta(s), s') = \psi(s, s') = \psi(s', s) = \varphi(\vartheta(s'), s) = \varphi(s, \vartheta(s')) = \varphi(\vartheta^{\text{ad}}(s), s')$$

for all  $s, s' \in S$  and hence  $\vartheta \in \mathfrak{F} = \{\alpha \in \mathfrak{E} \mid \alpha^{\text{ad}} = \alpha\}$ . The involution  $\text{ad}$  is either the identity on  $\mathfrak{E}$  or a field automorphism of order 2. In the first case  $\mathfrak{F} = \mathfrak{E} = \{\alpha \in \mathfrak{E} \mid \alpha^{\text{ad}} = \alpha\}$  since squaring is an automorphism of the finite field  $\mathfrak{E}$ . In the second case the map  $\mathfrak{E} \rightarrow \mathfrak{F}$ ,  $\alpha \mapsto \alpha \alpha^{\text{ad}}$  is the norm map onto the fixed field  $\mathfrak{F}$ . Hence in either case there exists some  $\gamma \in \mathfrak{E}$  with  $\gamma \gamma^{\text{ad}} = \vartheta$ . Now  $\gamma$  induces an isometry between the spaces  $(S, \varphi)$  and  $(S, \psi)$  since  $\psi(s, s') = \varphi(\vartheta(s), s') = \varphi(\gamma^{\text{ad}}(\gamma(s)), s') = \varphi(\gamma(s), \gamma(s'))$  for all  $s, s' \in S$ .  $\square$

**LEMMA 2.3.** Let  $G \leq \text{Sym}_n$  and let  $N \leq M \leq \mathbb{F}_2^n$  be  $G$ -submodules (i.e.  $G$ -invariant codes). Then  $(M/N)^* \cong N^\perp/M^\perp$ .

*Proof.* Let  $M_N^* := \{f \in \text{Hom}_{\mathbb{F}_2}(M, \mathbb{F}_2) \mid f(n) = 0 \text{ for all } n \in N\} \leq M^*$ . Then  $M_N^*$  is canonically isomorphic to  $(M/N)^*$ . Let  $\beta : N^\perp \rightarrow M_N^*$ ,  $n' \mapsto (m \mapsto b(m, n'))$ . Then  $\beta$  is well-defined and surjective, since  $\Upsilon : \mathbb{F}_2^n \rightarrow M^*$ ,  $v \mapsto (m \mapsto b(m, v))$  is surjective, and  $\Upsilon(v) \in M_N^*$  if and only if  $v \in N^\perp$ . Clearly  $\beta$  has kernel  $M^\perp$  and hence  $N^\perp/M^\perp \cong M_N^* \cong (M/N)^*$ .  $\square$

**COROLLARY 2.4.** *Let  $G \leq \text{Sym}_n$ . If there exists a self-dual code  $C \leq \mathbb{F}_2^n$  with  $G \leq \text{Aut}(C)$  then every self-dual simple  $G$ -module occurs with even multiplicity in a composition series of the  $\mathbb{F}_2 G$ -module  $\mathbb{F}_2^n$ .*

*Proof.* Let  $C = N_k \geq N_{k-1} \geq \dots \geq N_1 \geq N_0 = \{0\}$  be a composition series of the  $\mathbb{F}_2 G$ -module  $C$ . Then

$$C = C^\perp = N_k^\perp \leq N_{k-1}^\perp \leq \dots \leq N_1^\perp \leq N_0^\perp = \mathbb{F}_2^n$$

is a composition series of  $\mathbb{F}_2^n/C^\perp$ , since dualizing yields an antiautomorphism  $W \mapsto W^\perp$  of the submodule lattice of  $\mathbb{F}_2^n$ . The composition factors satisfy

$$N_{i-1}^\perp/N_i^\perp \cong (N_i/N_{i-1})^*,$$

cf. Lemma 2.3. Hence the claim follows.  $\square$

**LEMMA 2.5.** *Let  $S$  be a simple self-dual  $\mathbb{F}_2 G$ -module endowed with a non-degenerate  $G$ -invariant symmetric bilinear form  $\varphi$ . The module  $(U, \psi) := \perp_{i=1}^k (S, \varphi)$  contains a submodule  $X$  with*

$$X = X^{\perp, \psi} := \{u \in U \mid \psi(u, x) = 0 \text{ for all } x \in X\}$$

*if and only if  $k$  is even.*

*Proof.* If  $U$  contains such a submodule  $X = X^{\perp, \psi}$  then  $k$  is even according to Corollary 2.4. Conversely, if  $k$  is even then  $X := \{(s_1, s_1, s_2, s_2, \dots, s_{k/2}, s_{k/2})\} \leq U$  satisfies  $X = X^{\perp, \psi}$ .  $\square$

*Proof.* (of Theorem 2.1) If  $C \leq \mathbb{F}_2^n =: V$  is a self-dual  $G$ -invariant code then every self-dual simple module occurs with even multiplicity in a composition series of  $V$  (see Corollary 2.4). Conversely, assume that every self-dual composition factor occurs in  $V$  with even multiplicity, and let  $M \leq M^\perp \leq V$  be a maximally self-orthogonal  $G$ -invariant code, i.e. there is no self-orthogonal  $G$ -invariant code in  $V$  which properly contains  $M$ .

On the  $G$ -module  $M^\perp/M$  there exists a  $G$ -invariant non-degenerate symmetric bilinear form

$$\varphi : M^\perp/M \times M^\perp/M \rightarrow \mathbb{F}_2, \quad (m' + M, m'' + M) \mapsto (m', m'').$$

Any proper  $\mathbb{F}_2 G$ -submodule  $X$  of  $(M^\perp/M, \varphi)$  with  $X \subseteq X^{\perp, \varphi}$  (cf. Lemma 2.5) would lift to a self-orthogonal  $G$ -invariant code in  $V$  properly containing  $M$ , which we excluded in our assumptions. This implies that every  $\mathbb{F}_2 G$ -submodule  $X \leq M^\perp/M$  has a  $G$ -invariant complement  $X^{\perp, \varphi}$ , i.e.  $M^\perp/M$  is isomorphic to a direct sum of simple self-dual modules (see for instance [3, Proposition (3.12)]),  $(M^\perp/M, \varphi) \cong \perp_{S \cong S^*} (S, \varphi_S)^{n_S}$ , where  $\varphi_S$  is a non-degenerate  $G$ -invariant bilinear form on  $S$ , which is unique up to isometry by Lemma 2.2.

According to our assumptions, every simple self-dual  $G$ -module occurs with even multiplicity in  $M^\perp/M$ , i.e. all the  $n_S$  are even. But this means that the  $n_S$  must all be zero, according to Lemma 2.5, that is,  $M = M^\perp$  is a self-dual code in  $V$ .  $\square$

The criterion in Theorem 2.1 is not so easily tested. The next result gives a group theoretic condition that is sufficient for the existence of a self-dual  $G$ -invariant code. To this aim let  $G \leq \text{Sym}_n$  be a permutation group and write

$$\{1, \dots, n\} = B_1 \dot{\cup} \dots \dot{\cup} B_s$$

as a disjoint union of  $G$ -orbits and let  $H_i := \text{Stab}_G(x_i)$  be the stabilizer in  $G$  of some element  $x_i \in B_i$  ( $i = 1, \dots, s$ ). For  $1 \leq i \leq s$  let

$$m_i := |\{j \in \{1, \dots, s\} \mid H_i \text{ is conjugate to } H_j\}| \text{ and } n_i := [N_G(H_i) : H_i].$$

**PROPOSITION 2.6.** *Assume that the product  $n_i m_i$  is even for all  $1 \leq i \leq s$ . Then there is a  $G$ -invariant self-dual binary code  $C \leq \mathbb{F}_2^n$ .*

*Proof.* If  $H_i$  and  $H_j$  are conjugate for some  $i \neq j$  then the permutation representations of  $G$  on  $B_i$  and  $B_j$  are equivalent and by Theorem 2.1 there is a self-dual  $G$ -invariant code in the direct sum  $\mathbb{F}_2^{B_i \cup B_j} \cong \mathbb{F}_2^{|B_i|} \perp \mathbb{F}_2^{|B_j|}$  of two isomorphic  $\mathbb{F}_2 G$ -modules. It is hence enough to show the proposition for a transitive permutation group  $G \leq \text{Sym}_n$  with stabilizer  $H := \text{Stab}_G(1)$  for which  $[N_G(H) : H] \in 2\mathbb{Z}$ . Let  $(f_1, \dots, f_n)$  be the standard basis of  $\mathbb{F}_2^n$  such that  $\pi \in \text{Sym}_n$  maps  $f_j$  to  $f_{j\pi}$  for all  $j = 1, \dots, n$  and choose  $\eta \in N_G(H) - H$  such that  $\eta^2 \in H$ . Put  $N := \langle H, \eta \rangle$  and

$$G = \dot{\cup}_{s \in S} Ns = \dot{\cup}_{s \in S} (Hs \dot{\cup} H\eta s).$$

Define  $C := \langle f_{1s} + f_{1\eta s} : s \in S \rangle_{\mathbb{F}_2}$ . Then  $C$  is a  $G$ -invariant code in  $\mathbb{F}_2^n$  and  $C = C^\perp$  since the given basis of  $C$  consists of  $|S| = n/2$  pairwise orthogonal vectors of weight 2.  $\square$

### 3. From codes to lattices.

There is a well-known construction, called construction A (see [2, Section (7.2)]) that associates to a pair  $(R, C)$  of a ring  $R$  with prime ideal  $\varphi$  and residue field  $R/\varphi \cong \mathbb{F}$  and a code  $C \leq \mathbb{F}^n$  an  $n$ -dimensional lattice over  $R$ . We will apply this construction for binary codes and two different base rings:  $R = \mathbb{Z}$  and  $R = \mathbb{Z}_2$ , the ring of 2-adic integers, where the prime ideal  $\varphi = 2R$  in both cases. So let  $R$  be one of these two rings and let  $K$  denote the field of fractions of  $R$  and let  $V := \langle b_1, \dots, b_n \rangle_K$  be a vector space over  $K$  with bilinear form defined by

$$(\ , \ ) : V \times V \rightarrow K, (b_i, b_j) := \frac{1}{2} \delta_{ij} = \begin{cases} 1/2 & i = j \\ 0 & i \neq j \end{cases}$$

and associated quadratic form  $q : V \rightarrow K, q(v) := \frac{1}{2}(v, v)$ . The orthogonal group of  $V$  is

$$O(V) := \{g \in \text{GL}(V) \mid (vg, wg) = (v, w) \text{ for all } v, w \in V\}.$$

**DEFINITION 3.** A lattice  $L \leq V$  is the  $R$ -span of a basis of  $V$ . The *dual lattice*

$$L^\# := \{v \in V \mid (v, \ell) \in R \text{ for all } \ell \in L\}$$

is again a lattice in  $V$ .  $L$  is called *integral* if  $L \subseteq L^\#$  or equivalently  $(\ell_1, \ell_2) \in R$  for all  $\ell_1, \ell_2 \in L$ .  $L$  is called *even* if  $q(\ell) \in R$  for all  $\ell \in L$  and *odd* if  $L$  is integral and there is some  $\ell \in L$  with  $q(\ell) \notin R$ .  $L$  is called *unimodular* if  $L = L^\#$ . The *orthogonal group* of  $L$  is

$$O(L) := \{g \in O(V) \mid Lg = L\}.$$

The following remark lists elementary properties of the lattice obtained from a code by construction A which can be seen by straightforward calculations.

REMARK 1. Let  $M = \langle b_1, \dots, b_n \rangle_R$  be the lattice generated by the basis above and let  $C \leq \mathbb{F}_2^n$  be a binary code. Then the  $R$ -lattice

$$L := A(R, C) := \left\{ \sum_{i=1}^n a_i b_i \mid a_i \in R, (a_1 + 2R, \dots, a_n + 2R) \in C \right\}$$

is called the *codelattice* of  $C$ . Note that  $2M \subset L \subset M$  and  $L$  is the full preimage of  $C \cong L/2M$  under the natural epimorphism  $M \rightarrow (R/2R)^n = \mathbb{F}_2^n$ . The lattice  $L$  is even if and only if the code  $C$  is doubly-even. The dual lattice is  $A(R, C)^\# = A(R, C^\perp)$  and hence  $L$  is unimodular if and only if  $C$  is self-dual, and  $L$  is an even unimodular lattice if and only if  $C$  is a doubly-even self-dual code.

The symmetric group  $\text{Sym}_n$  acts as orthogonal transformations on  $V$  by permuting the basis vectors. This yields an injective homomorphism

$$\iota : \text{Sym}_n \rightarrow O(V), \quad \iota(\pi) : b_i \mapsto b_{i\pi}.$$

If  $G = \text{Aut}(C)$  is the automorphism group of  $C$  then  $\iota(G) \leq O(A(R, C))$ .

#### 4. Permutations as elements of the orthogonal group.

Let  $\mathbb{Q}_2$  denote the field of 2-adic numbers,  $v_2 : \mathbb{Q}_2 \rightarrow \mathbb{Z} \cup \{\infty\}$  its natural valuation and  $\mathbb{Z}_2 := \{x \in \mathbb{Q}_2 \mid v_2(x) \geq 0\}$  the ring of 2-adic integers with unit group  $\mathbb{Z}_2^* := \{x \in \mathbb{Z}_2 \mid v_2(x) = 0\}$ . Let  $V := \langle b_1, \dots, b_n \rangle_{\mathbb{Q}_2}$  be a bilinear space over  $\mathbb{Q}_2$  of dimension  $n > 1$  as in Section 3, in particular  $(b_i, b_j) = \frac{1}{2}\delta_{ij}$ . The orthogonal group  $O(V)$  is generated by all reflections

$$\sigma_v : V \rightarrow V, x \mapsto x - \frac{(x, v)}{q(v)}v$$

along vectors  $v \in V$  with  $q(v) \neq 0$  (see [5, Satz (3.5)], [8, Theorem 43:3]). Then the spinor norm defines a group homomorphism  $h : O(V) \rightarrow C_2$  as follows:

DEFINITION 4. Let  $h : O(V) \rightarrow C_2 = \{1, -1\}$  be defined by  $h(\sigma_v) := (-1)^{v_2(q(v))}$  for all reflections  $\sigma_v \in O(V)$ . Let  $O^h(V) := \{g \in O(V) \mid h(g) = 1\}$  denote the kernel of this epimorphism.

Note that the definition of  $h$  depends on the chosen scaling of the quadratic form. It follows from the definition of the spinor norm (see [8, Section 55]) that

LEMMA 4.1. *The map  $h$  is a well-defined group epimorphism.*

The crucial observation that yields the connection to coding theory in Section 5 is the following easy lemma.

LEMMA 4.2. *Let  $\iota : \text{Sym}_n \rightarrow O(V)$  be the homomorphism from Remark 1. Then  $h \circ \iota = \text{sign}$ .*

*Proof.* The symmetric group  $\text{Sym}_n$  is generated by transpositions  $\tau_{i,j} = (i, j)$  for  $i \neq j$ . Such a transposition interchanges  $b_i$  and  $b_j$  and fixes all other basis vectors and hence  $\iota(\tau_{i,j}) = \sigma_{b_i - b_j}$ . Clearly

$$h(\sigma_{b_i - b_j}) = (-1)^{v_2(q(b_i) + q(b_j))} = (-1)^{-1} = -1 = \text{sign}(\tau_{i,j}).$$

□

LEMMA 4.3. *Let  $L \leq V$  be an even unimodular lattice. Then  $O(L) \leq O^h(V)$ .*

*Proof.* By [5, Satz 4.6] the orthogonal group  $O(L)$  is generated by reflections

$$O(L) = \langle \sigma_\ell \mid \ell \in L, v_2(q(\ell)) = 0 \rangle.$$

Since  $h(\sigma_\ell) = (-1)^{v_2(q(\ell))} = 1$  for those vectors  $\ell$ , the result follows. □

We now assume that  $n$  is a multiple of 8 and choose an orthonormal basis  $(e_1, \dots, e_n)$  of  $V$  (i.e.  $(e_i, e_j) = \delta_{ij}$ ). Let  $L := \langle e_1, \dots, e_n \rangle_{\mathbb{Z}_2}$  be the unimodular lattice generated by these vectors  $e_i$  and let

$$L_0 := \{ \ell \in L \mid q(\ell) \in \mathbb{Z}_2 \} = \langle e_1 + e_2, \dots, e_1 + e_n, 2e_1 \rangle$$

be its even sublattice. Then  $L_0^\# = \langle e_1, \dots, e_{n-1}, v := \frac{1}{2} \sum_{i=1}^n e_i \rangle$ . Since  $n$  is a multiple of 8 the vector  $2v \in L_0$  and  $(v, v) = \frac{n}{4}$  is even. Hence  $L_0^\# / L_0 \cong \mathbb{F}_2^2$  and the three lattices  $L_i$  with  $L_0 < L_i < L_0^\#$  corresponding to the three 1-dimensional subspaces of  $L_0^\# / L_0$  are given by

$$L_1 := \langle L_0, v \rangle, \quad L_2 := \langle L_0, v - e_1 \rangle, \quad L_3 = L.$$

Note that  $L_1$  and  $L_2$  are even unimodular lattices, whereas  $L_3$  is odd. In particular  $O(L) = O(L_0)$  acts as the subgroup

$$\{1, -1\} = C_2 \cong \{I_2, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\} \leq \text{GL}_2(\mathbb{F}_2)$$

on  $L_0^\# / L_0$  (with respect to the basis  $(v + L_0, e_1 + L_0)$ ). Let  $f : O(L) \rightarrow C_2 = \{\pm 1\}$  denote the resulting epimorphism. So the elements in the kernel of  $f$  (which equals  $O(L) \cap O^h(V)$  as shown in the next lemma) fix both lattices  $L_1$  and  $L_2$  and all other elements in  $O(L)$  interchange  $L_1$  and  $L_2$ .

LEMMA 4.4.  $f = h|_{O(L)}$

*Proof.* Let  $R(L_0) := \langle \sigma_\ell \mid \ell \in L_0, q(\ell) \in \mathbb{Z}_2^* \rangle$  be the reflection subgroup of  $O(L_0)$ . By [6, Satz 6]  $R(L_0)$  is the kernel of  $f$ . Since  $h(\sigma_\ell) = 1$  for all  $\sigma_\ell \in R(L_0)$ , the group  $R(L_0) \subset O(L) \cap O^h(V)$  is also contained in the kernel of  $h$ . The reflection  $\sigma_{e_1}$  along the vector  $e_1 \in L$  is in the orthogonal group  $O(L) = O(L_0)$ , interchanges the two lattices  $L_1$  and  $L_2$ , and satisfies  $h(\sigma_{e_1}) = -1$ . Since  $R(L_0)$  is a normal subgroup of index at most 2 in  $O(L)$ , we obtain  $O(L) = \langle R(L_0), \sigma_{e_1} \rangle$  and the lemma follows. □

## 5. The main results.

THEOREM 5.1. *Let  $C = C^\perp \leq \mathbb{F}_2^n$  be a doubly-even self-dual code. Then the automorphism group of  $C$  is contained in the alternating group.*

*Proof.* We apply construction A from Section 3 to the code  $C$  to obtain the codelattice  $L := A(\mathbb{Z}_2, C)$ . By Remark 1 the lattice  $L$  is an even unimodular lattice. Hence by Lemma 4.3 its orthogonal group  $O(L) \leq O^h(V)$  is in the kernel of the epimorphism  $h$  from Definition 4. The image of  $\text{Aut}(C)$  under the homomorphism  $\iota$  from Remark 1 is contained in  $O(L)$ , hence

$\iota(\text{Aut}(C)) \leq O(L) \leq O^h(V)$ . Since  $h \circ \iota = \text{sign}$  by Lemma 4.2 we have  $\text{sign}(\text{Aut}(C)) = \{1\}$  and therefore  $\text{Aut}(C) \leq \text{Alt}_n$ .  $\square$

**THEOREM 5.2.** *Let  $G \leq \text{Sym}_n$ . Then there is a self-dual doubly-even code  $C = C^\perp \leq \mathbb{F}_2^n$  with  $G \leq \text{Aut}(C)$  if and only if the following three conditions are fulfilled:*

- (a)  $8 \mid n$ .
- (b) Every self-dual composition factor of the  $\mathbb{F}_2 G$ -module  $\mathbb{F}_2^n$  occurs with even multiplicity.
- (c)  $G \leq \text{Alt}_n$ .

*Proof.*  $\Rightarrow$ : (a) is clear since the length of any doubly-even self-dual code is a multiple of 8. (b) follows from Theorem 2.1 and (c) is a consequence of Theorem 5.1.  
 $\Leftarrow$ : By Theorem 2.1 the condition (b) implies the existence of a self-dual code  $X = X^\perp$  with  $G \leq \text{Aut}(X)$ . If  $X$  is doubly-even then we are done. So assume that  $X$  is not doubly even and consider the codelattices

$$L := A(\mathbb{Z}, X) \text{ and } L_X := A(\mathbb{Z}_2, X) = L \otimes \mathbb{Z}_2.$$

Then  $L$  is a positive definite odd unimodular  $\mathbb{Z}$ -lattice and hence its 2-adic completion  $L \otimes \mathbb{Z}_2 = L_X$  is an odd unimodular  $\mathbb{Z}_2$ -lattice having an orthonormal basis (see for instance [5, Satz (26.7)]). Hence  $L_X$  is isometric to the lattice  $L$  constructed just before Lemma 4.4. Since  $G \leq \text{Alt}_n$ , the group  $\iota(G) \leq O(L_X)$  lies in the kernel of the homomorphism  $f$  from Lemma 4.4 and therefore fixes the two even unimodular lattices  $L_1$  and  $L_2$  intersecting  $L_X$  in its even sublattice. Let  $M = \langle b_1, \dots, b_n \rangle_{\mathbb{Z}_2}$  be the lattice from Remark 1 such that  $2M < L_X < M$  and identify  $M/2M = \bigoplus_{i=1}^n \mathbb{Z}_2/2\mathbb{Z}_2 b_i = \bigoplus_{i=1}^n \mathbb{F}_2 b_i$  with  $\mathbb{F}_2^n$ . Then the code  $C := L_1/2M \leq \mathbb{F}_2^n$  (such that  $L_1 = A(\mathbb{Z}_2, C)$ ) is a self-dual doubly-even code with  $G \leq \text{Aut}(C)$ .  $\square$

## 6. An application to group ring codes.

As an application of our main Theorem 5.2 we obtain a result (Theorem 6.3) on the existence of self-dual doubly-even binary group codes, given in [9] and also in [11]. Binary group codes are ideals of the group ring  $\mathbb{F}_2 G$ , where  $G$  is a finite group, i.e. these are exactly the codes in  $\mathbb{F}_2^{|G|}$  with  $\rho_G(C) \leq \text{Aut}(C)$ , where  $\rho_G : G \rightarrow \text{Sym}_G$ ,  $g \mapsto (h \mapsto hg)$  is the regular representation of  $G$ . Clearly  $\rho_G(C) \leq \text{Alt}_G$  if and only if the image  $\rho_G(S)$  of any Sylow 2-subgroup  $S \in \text{Syl}_2(G)$  is contained in the alternating group. Let  $k := [G : S]$  be the index of  $S$  in  $G$ . Then  $k$  is odd and the restriction of  $\rho_G$  to  $S$  is  $(\rho_G)|_S = k\rho_S$ . Hence  $\rho_G(C) \leq \text{Alt}_G$  if and only if  $\rho_S(C) \leq \text{Alt}_S$ .

**LEMMA 6.1.** *Let  $S \neq 1$  be a 2-group. Then  $\rho_S(C) \leq \text{Alt}_S$  if and only if  $S$  is not cyclic.*

*Proof.* If  $S = \langle s \rangle$  is cyclic, then  $\rho_S(s)$  is a  $|S|$ -cycle in  $\text{Sym}_S$  and hence its sign is  $-1$  (because  $|S|$  is even). On the other hand assume that  $S$  is not cyclic. Then  $S$  has a normal subgroup  $N$  such that  $S/N \cong C_2 \times C_2$  is generated by elements  $aN, bN \in S/N$  of order 2, with  $abN = baN$ . Let  $A := \langle a, N \rangle$  and  $B = \langle b, N \rangle$ . Then

$$S = \langle A, B \rangle = A \dot{\cup} bA = B \dot{\cup} aB$$

and  $b$  induces an isomorphism between the regular  $A$ -module  $A$  and  $bA$ , so  $A$  is in the kernel of the sign homomorphism. Similarly  $a$  gives an isomorphism between the regular  $B$ -module  $B$  and  $aB$ , so also  $B$  is in the kernel of the sign homomorphism.  $\square$

The following observation follows from Proposition 2.6 and is proven in [10, Theorem 1.1].

**THEOREM 6.2.** *There is a self-dual binary group code  $C \leq \mathbb{F}_2G$  if and only if the order of  $G$  is even.*

*Proof.*  $\Rightarrow$ : Clear, since  $\dim(C) = \frac{|G|}{2}$  for any  $C = C^\perp \leq \mathbb{F}_2G$ .  
 $\Leftarrow$ : Follows from Proposition 2.6, because  $\rho_G$  is a transitive permutation representation and the full group  $G$  is the normalizer of the stabilizer  $H := \text{Stab}_G(1) = 1$ .  $\square$

**THEOREM 6.3.** (see [9],[11].) *Let  $G$  be a finite group. Then  $\mathbb{F}_2G$  contains a doubly-even self-dual group code if and only if the order of  $G$  is divisible by 8 and the Sylow 2-subgroups of  $G$  are not cyclic.*

*Proof.* The condition that the group order be divisible by 8 is equivalent to condition (a) of Theorem 5.2 and also implies (with Theorem 6.2) that there is some self-dual  $G$ -invariant code in  $\mathbb{F}_2G$ , which is equivalent to condition (b) of Theorem 5.2 by Theorem 2.1. The condition on the Sylow 2-subgroups of  $G$  is equivalent to  $\rho_G(G) \leq \text{Alt}_G$  by Lemma 6.1 and hence to condition (c) of Theorem 5.2.  $\square$

Our last application concerns the automorphism group  $G = \text{Aut}(C)$  of a putative extremal Type II code  $C$  of length 72. The paper [1] shows that any automorphism of  $C$  of order 2 acts fixed point freely, so any Sylow 2-subgroup  $S$  of  $G$  acts as a multiple of the regular representation. In particular  $|S|$  divides 8. Our results show that  $S$  is not cyclic of order 8, which already follows from [9, Theorem 1].

**COROLLARY 6.4.** *Let  $C$  be a self-dual doubly-even binary code of length 72 with minimum distance 16. Then  $C$  does not have an automorphism of order 8.*

### References

1. S. Bouyuklieva, On the automorphisms of order 2 with fixed points for the extremal self-dual codes of length  $24m$ . *Designs, Codes, Cryptogr.* **25**, 5-13 (2002)
2. J.H. Conway, N.J.A. Sloane, *Sphere packings, lattices and groups*. Springer Grundlehren 290, 1993.
3. C.W. Curtis, I. Reiner, *Methods of Representation Theory I*. Wiley classics 1990.
4. A. M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities. in *Actes, Congrès International de Mathématiques (Nice, 1970)*, Gauthiers-Villars, Paris, 1971, Vol. 3, pp. 211–215.
5. M. Kneser, R. Scharlau, *Quadratische Formen*. Springer 2002
6. M. Kneser, Erzeugung ganzzahliger orthogonaler Gruppen durch Spiegelungen. *Mathem. Annalen* 255, 453-462 (1981)
7. F.J. MacWilliams, N.J.A. Sloane, *Self-Dual Codes and Invariant Theory*. North-Holland Mathematical Library
8. O.T. O'Meara, *Introduction to Quadratic Forms*. Springer Grundlehren 117, 1973.
9. N.J.A. Sloane, J.G. Thompson, Cyclic Self-Dual Codes. *IEEE Trans. Inform. Theory* 29, 1983
10. W. Willems, A note on self-dual group codes. *IEEE Trans. Inform. Theory* 48 (2002), no. 12, 3107–3109.
11. C. Martínez-Pérez, W. Willems, Self-dual codes and modules for finite groups in characteristic two. *IEEE Trans. Inform. Theory* 50 (2004), no. 8, 1798–1803.

A. Günther and G. Nebe,  
 Lehrstuhl D für Mathematik,  
 RWTH Aachen University 52056 Aachen,  
 Germany

annika.guenther@math.rwth-aachen.de,  
 gabriele.nebe@math.rwth-aachen.de