Submitted exclusively to the London Mathematical Society
doi:10.1112/0000/000000

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 [**6**] 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 [**9**, Theorem 3c], for instance.

This note studies the automorphism group $\mathrm{Aut}(C) := \{\pi \in \mathrm{Sym}_n \mid C\pi = C\}$ 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 $G \leq \mathrm{Sym}_n$ that fix a doubly-even self-dual binary code. This result generalizes results by Sloane and Thompson [**12**] and Martínez-Pérez and Willems [**14**].

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 $b : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2, b(x,y) := \sum_{i=1}^n x_i y_i$ 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* $\mathrm{wt}(c)$ 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.

2000 *Mathematics Subject Classification* 94B05 (primary), 20G25, 11E95 (secondary).

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 $S^* = \mathrm{Hom}_{\mathbb{F}_2}(S, \mathbb{F}_2)$, whereas the dual of a code $C \leq \mathbb{F}_2^n$ is as in Definition 1. For $G \leq \mathrm{Aut}(C)$ 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* $S^* = \mathrm{Hom}_{\mathbb{F}_2}(S, \mathbb{F}_2)$ 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 $G \leq \mathrm{Sym}_n$. Then there exists a self-dual code $C \leq \mathbb{F}_2^n$ with $G \leq \mathrm{Aut}(C)$ 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 $\varphi : S \times S \to \mathbb{F}_2$. Then φ is unique, up to isometry.*

Proof. Since φ is non-degenerate and G-invariant, it induces an $\mathbb{F}_2G$-isomorphism $\alpha_\varphi : S \to S^*,\ s \mapsto (s' \mapsto \varphi(s, s'))$. Let $\psi : S \times S \to \mathbb{F}_2$ be another non-degenerate symmetric G-invariant bilinear form on S, then $\alpha_\psi = \alpha_\varphi \circ \vartheta$ for some ϑ in the finite field $\mathfrak{E} := \mathrm{End}_G(S)$ 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 $^{\mathrm{ad}}$ on $\mathfrak{E}$ given by $\varphi(s, \alpha(s')) = \varphi(\alpha^{\mathrm{ad}}(s), s')$, for $s, s' \in S$. Since both φ and ψ are symmetric we have

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

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

LEMMA 2.3. *Let $G \leq \mathrm{Sym}_n$ 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 $M_N^* := \{f \in \mathrm{Hom}_{\mathbb{F}_2}(M, \mathbb{F}_2) \mid f(n) = 0 \text{ for all } n \in N\} \leq M^*$. Then M_N^* is canonically isomorphic to $(M/N)^*$. Let $\beta : N^\perp \to M_N^*,\ n' \mapsto (m \mapsto b(m, n'))$. Then β is well-defined and surjective, since $\Upsilon : \mathbb{F}_2^n \to M^*,\ v \mapsto (m \mapsto b(m, v))$ is surjective, and $\Upsilon(v) \in M_N^*$ if and only if $v \in N^\perp$. Clearly β has kernel $M^\perp$ and hence $N^\perp/M^\perp \cong M_N^* \cong (M/N)^*$. □

COROLLARY 2.4. *Let $G \leq \mathrm{Sym}_n$. If there exists a self-dual code $C \leq \mathbb{F}_2^n$ with $G \leq \mathrm{Aut}(C)$ then every self-dual simple G-module occurs with even multiplicity in a composition series of the $\mathbb{F}_2G$-module $\mathbb{F}_2^n$.*

Proof. Let $C = N_k \geq N_{k-1} \geq \ldots \geq N_1 \geq N_0 = \{0\}$ be a composition series of the $\mathbb{F}_2G$-module C. Then

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

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. □

LEMMA 2.5. *Let S be a simple self-dual $\mathbb{F}_2G$-module endowed with a non-degenerate G-invariant symmetric bilinear form φ. 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 $X := \{(s_1, s_1, s_2, s_2, \ldots, s_{k/2}, s_{k/2})\} \leq U$ satisfies $X = X^{\perp,\psi}$. □

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

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

Any proper $\mathbb{F}_2G$-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 $\mathbb{F}_2G$-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 φ_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. □

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 $G \leq \mathrm{Sym}_n$ be a permutation group and write

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

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

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

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

Proof. If H_i and H_j are conjugate for some $i \ne j$ 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 $\mathbb{F}_2^{B_i \dot\cup B_j} \cong \mathbb{F}_2^{|B_i|} \perp \mathbb{F}_2^{|B_j|}$ of two isomorphic $\mathbb{F}_2 G$-modules. It is hence enough to show the proposition for a transitive permutation group $G \le \mathrm{Sym}_n$ with stabilizer $H := \mathrm{Stab}_G(1)$ for which $[N_G(H) : H] \in 2\mathbb{Z}$. Let $(f_1, \ldots, f_n)$ be the standard basis of $\mathbb{F}_2^n$ such that $\pi \in \mathrm{Sym}_n$ maps f_j to $f_{j\pi}$ for all $j = 1, \ldots, n$ 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. □

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 $\wp$ and residue field $R/\wp \cong \mathbb{F}$ and a code $C \le \mathbb{F}^n$ 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 $\wp = 2R$ in both cases. So let R be one of these two rings and let K denote the field of fractions of R and let $V := \langle b_1, \ldots, b_n \rangle_K$ be a vector space over K with bilinear form defined by

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

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

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

DEFINITION 3. A *lattice* $L \le V$ 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 $M = \langle b_1, \ldots, b_n \rangle_R$ be the lattice generated by the basis above and let $C \leq \mathbb{F}_2^n$ be a binary code. Then the R-lattice

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

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 $M \to (R/2R)^n = \mathbb{F}_2^n$. 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 Sym_n acts as orthogonal transformations on V by permuting the basis vectors. This yields an injective homomorphism

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

If $G = \mathrm{Aut}(C)$ 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, $v_2 : \mathbb{Q}_2 \to \mathbb{Z} \cup \{\infty\}$ 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 $V := \langle b_1, \ldots, b_n \rangle_{\mathbb{Q}_2}$ 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

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

along vectors $v \in V$ with $q(v) \neq 0$ (see [**7**, Satz (3.5)], [**10**, Theorem 43:3]). Then the spinor norm defines a group homomorphism $h : O(V) \to C_2$ as follows:

DEFINITION 4. Let $h : O(V) \to C_2 = \{1, -1\}$ 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 [**10**, 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 $\iota : \mathrm{Sym}_n \to O(V)$ be the homomorphism from Remark 1. Then $h \circ \iota =$* sign.

Proof. The symmetric group 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

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

□

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

Proof. By [**7**, 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 ℓ, the result follows. □

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

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

be its even sublattice. Then $L_0^\# = \langle e_1, \ldots, e_{n-1}, v := \frac{1}{2}\sum_{i=1}^n e_i \rangle$. 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

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

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

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

on $L_0^\#/L_0$ (with respect to the basis $(v + L_0, e_1 + L_0)$). Let $f : O(L) \to C_2 = \{\pm 1\}$ 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 [**8**, 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 σ_{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 $\mathrm{Aut}(C)$ under the homomorphism ι from Remark 1 is contained in $O(L)$, hence

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

THEOREM 5.2. *Let $G \leq \mathrm{Sym}_n$. Then there is a self-dual doubly-even code $C = C^\perp \leq \mathbb{F}_2^n$ with $G \leq \mathrm{Aut}(C)$ if and only if the following three conditions are fulfilled:*
(a) $8 \mid n$.
(b) *Every self-dual composition factor of the $\mathbb{F}_2G$-module $\mathbb{F}_2^n$ occurs with even multiplicity.*
(c) $G \leq \mathrm{Alt}_n$.

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 $G \leq \mathrm{Aut}(X)$. 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 [**7**, Satz (26.7)]). Hence L_X is isometric to the lattice L constructed just before Lemma 4.4. Since $G \leq \mathrm{Alt}_n$, 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 $M = \langle b_1, \ldots, b_n \rangle_{\mathbb{Z}_2}$ 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 $G \leq \mathrm{Aut}(C)$. □

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 [**12**] and also in [**14**]. Binary group codes are ideals of the group ring $\mathbb{F}_2G$, where G is a finite group, i.e. these are exactly the codes in $\mathbb{F}_2^{|G|}$ with $\rho_G(G) \leq \mathrm{Aut}(C)$, where $\rho_G : G \to \mathrm{Sym}_G,\ g \mapsto (h \mapsto hg)$ is the regular representation of G. Clearly $\rho_G(G) \leq \mathrm{Alt}_G$ if and only if the image $\rho_G(S)$ of any Sylow 2-subgroup $S \in \mathrm{Syl}_2(G)$ 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 ρ_G to S is $(\rho_G)_{|S} = k\rho_S$. Hence $\rho_G(S) \leq \mathrm{Alt}_G$ if and only if $\rho_S(S) \leq \mathrm{Alt}_S$.

LEMMA 6.1. *Let $S \neq 1$ be a 2-group. Then $\rho_S(S) \leq \mathrm{Alt}_S$ 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 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. □

The following observation follows from Proposition 2.6 and is proven in [**13**, Theorem 1.1].

THEOREM 6.2. *There is a self-dual binary group code $C \leq \mathbb{F}_2 G$ if and only if the order of G is even.*

Proof. $\Rightarrow$: Clear, since $\dim(C) = \frac{|G|}{2}$ for any $C = C^\perp \leq \mathbb{F}_2 G$.
$\Leftarrow$: Follows from Proposition 2.6, because ρ_G is a transitive permutation representation and the the full group G is the normalizer of the stabilizer $H := \mathrm{Stab}_G(1) = 1$. □

THEOREM 6.3. *(see [**12**],[**14**].) Let G be a finite group. Then $\mathbb{F}_2 G$ 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 $\mathbb{F}_2 G$, 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 $\rho_G(G) \leq \mathrm{Alt}_G$ by Lemma 6.1 and hence to condition (c) of Theorem 5.2. □

Our last application concerns the automorphism group $G = \mathrm{Aut}(C)$ 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 [**12**, 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.*

7. *A characteristic 2 proof of Theorems 5.1 and 5.2*

As remarked by Robert Griess one may prove Theorem 5.1 and 5.2 without using characteristic 0 theory.

Assume that n is a multiple of 8 and let $\mathbf{1} := (1, \ldots, 1) \in \mathbb{F}_2^n$ denote the all ones vector. Then

$$V = \mathbf{1}^\perp / \langle \mathbf{1} \rangle = \{ x \in \mathbb{F}_2^n \mid \mathrm{wt}(x) \text{ is even } \} / \langle \mathbf{1} \rangle$$

becomes a quadratic module of dimension $n-2$ over $\mathbb{F}_2$ by putting

$$q : V \to \mathbb{F}_2, \overline{x} := x + \langle \mathbf{1} \rangle \mapsto \frac{1}{2} \mathrm{wt}(x) + 2\mathbb{Z}.$$

The associated bilinear form $b(\overline{x}, \overline{y}) = q(\overline{x} + \overline{y}) - q(\overline{x}) - q(\overline{y}) = x \cdot y$ is inherited from the standard inner product and the maximal isotropic subspaces of V are the images of the doubly-even self-dual codes in $\mathbb{F}_2^n$.

The orthogonal group $O(V, q) \cong O^+_{n-2}(2)$ acts transitively on the set of maximal isotropic subspaces of V. Fix one such subspace U. Then the *Dickson invariant* is

$$D : O(V, q) \to \{1, -1\}; D(g) := (-1)^{\dim(U/U \cap Ug)}$$

a well-defined homomorphism that does not depend on the choice of U ([**11**, Theorem 11.61]).

The symmetric group Sym_n acts by coordinate permutations on $\mathbb{F}_2^n$. Since $\mathbf{1}\pi = \mathbf{1}$ for all $\pi \in \mathrm{Sym}_n$ and permutations preserve the weight this gives rise to an embedding $\iota : \mathrm{Sym}_n \to O(V, q)$. The following lemma also follows from the geometric characterization of the Dickson invariant in [**11**, p. 160] (see also [**5**] and [**4**]).

LEMMA 7.1. $D \circ \iota = \mathrm{sign}$.

Proof. It is enough to find a transposition that is not in the kernel of the Dickson invariant. To this aim choose the Type II code C with generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & \dots & \dots & \dots & 1 & 0 \end{pmatrix}$$

and let $U := C/\langle \mathbf{1} \rangle$. Then $U\iota(\tau_{1,2}) \cap U$ has co-dimension 1 in U. □

Now we can use the Dickson invariant D to replace the spinor norm h to obtain the main results. It is immediate that $\mathrm{Stab}_{O(V,q)}(U) \subset \ker(D)$ (see also [**11**, Exercise 11.19]) from which one obtains Theorem 5.1.

The proof of Theorem 5.2 can also be modified. Condition (b) implies the existence of a self-dual G-invariant code X. If X is doubly-even, then we are done; if not, then let $X_0 := \{x \in X \mid \mathrm{wt}(x) \in 4\mathbb{Z}\}$ denote the doubly-even subcode of X. This is a subcode of codimension 1 in X and $X_0^\perp/X_0 \cong \mathbb{F}_2 \oplus \mathbb{F}_2$ is of dimension 2. Since the length of X is divisible by 8, the full preimages C_1 and C_2 of the other two non-trivial subspaces of $X_0^\perp/X_0$ both are self-dual doubly-even codes. Since the co-dimension of the intersection $\dim(C_i/(C_1 \cap C_2)) = 1$ is odd, any permutation π with $C_1\pi = C_2$ has to have $\mathrm{sign}(\pi) = D(\iota(\pi)) = -1$. Since $G \leq \mathrm{Alt}_n$, all elements of G have to fix both codes C_1 and C_2 and hence these yield G-invariant doubly-even self-dual codes.

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. J. Dieudonné, *Pseudo-discriminant and Dickson invariant.* Pacific J. Math. **5**, 907-910 (1955)
5. R.H. Dye, *A geometric characterization of the special orthogonal groups and the Dickson invariant.* J. LMS (2) **15**, 472-476 (1977)
6. A. M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities. in *Actes, Congrés International de Mathématiques (Nice, 1970)*, Gauthiers-Villars, Paris, 1971, Vol. 3, pp. 211–215.
7. M. Kneser, R. Scharlau, *Quadratische Formen.* Springer 2002
8. M. Kneser, Erzeugung ganzzahliger orthogonaler Gruppen durch Spiegelungen. Mathem. Annalen 255, 453-462 (1981)
9. F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977; 11th impression 2003.
10. O.T. O'Meara, *Introduction to Quadratic Forms.* Springer Grundlehren 117, 1973.
11. C.E. Taylor, *The geometry of the classical groups.* Heldermann Verlag Berlin 1992.
12. N.J.A. Sloane, J.G. Thompson, Cyclic Self-Dual Codes. IEEE Trans. Inform. Theory 29, 1983
13. W. Willems, A note on self-dual group codes. IEEE Trans. Inform. Theory 48 (2002), no. 12, 3107–3109.
14. 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