Finite Fields and Their Applications 15 (2009) 517–533

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A mass formula for self-dual permutation codes

Annika Günther

Lehrstuhl D für Mathematik, RWTH Aachen University, Templergraben 64, 52064 Aachen, Germany

ARTICLE INFO

Article history:
Received 14 October 2008
Revised 24 March 2009
Available online 1 May 2009
Communicated by W. Cary Huffman

Keywords:
Permutation codes
Number of self-dual codes
Mass formula
Group ring codes

ABSTRACT

For a module V over a finite semisimple algebra A we give the total number of self-dual codes in V. This enables us to obtain a mass formula for self-dual codes in permutation representations of finite groups over finite fields of coprime characteristic.

1. Introduction

In the classical sense, a code is a linear subspace of $\mathbb{F}^N$, where $\mathbb{F}$ is a finite field. Many codes which are of interest in coding theory have the additional structure of a module over a ring R. The cyclic codes, for instance, which are invariant under a cyclic shift of the coordinates, are the submodules of the regular module over the group algebra $\mathbb{F}C_N$, where C_N is the cyclic group of order N.

In this paper a code is a submodule of a right A-module V, where A is a finite dimensional algebra over $\mathbb{F}$. This includes the group codes considered by several authors – see for instance [1–3] – which are ideals in a group algebra $\mathbb{F}G$, where G is a finite group, and also the extended cyclic codes considered in [4], which are $\mathbb{F}C_N$-submodules of $\mathbb{F}C_N \oplus \mathbb{F}$, where C_N acts trivially on the additional coordinate.

The module V will be assumed to carry a non-degenerate equivariant form φ (cf. Definition 2.2) – in the case of group algebras $A = \mathbb{F}G$ these are non-degenerate G-invariant forms. For a code $C \leqslant V$ we define the orthogonal code

$$C^{\perp} = C^{\perp,\varphi} := \{ v \in V \mid \varphi(v, c) = 0 \text{ for all } c \in C \},$$

which is, again, a right A-module. If $C = C^{\perp}$ then the code C is called self-dual.

E-mail address: annika.guenther@math.rwth-aachen.de.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2009.04.001

The situation in which a self-dual code $C \leqslant V$ exists has been characterized in [5] in the case where $A = V = \mathbb{F}G$, using representation theoretic methods. In this paper the total number $M_{(V,\varphi)}$ of self-dual codes in a general A-module V over a semisimple algebra A is given, provided that there exists at least one such code. It is shown that this number basically depends on the composition factors of V, except if $\mathbb{F}$ has even characteristic and φ is symmetric. Still, the latter case remains relatively transparent if A is a group algebra – then, $M_{(V,\varphi)}$ additionally depends on the existence of an isotropic vector $v \in V$, i.e. $\varphi(v, v) = 0$.

The number $M_{(V,\varphi)}$ is determined via a Morita equivalence $\mathcal{F}$ given in Section 2, which maps (V, φ) onto a module (U, φ') over $Z(A)$. In the case where $A = \mathbb{F}G$ is a group algebra and $\mathbb{F}$ is a splitting field for G, this corresponds the Morita equivalence given in [6]. Note that [6] includes the modular case, i.e. the case where A is not semisimple. We show that the equivalence $\mathcal{F}$ preserves the number of self-dual codes. Since A is semisimple, $Z(A)$ is a ringdirect sum of fields. This reduces the determination of $M_{(V,\varphi)}$, in Section 3.3, basically to an enumeration of all self-dual codes in a vector space endowed with a certain form. This situation is well understood; enumeration formulae are given in [7] and [8], for instance, and are cited in Section 3.2 for reader's convenience.

In Section 4 we give a group $\mathrm{Aut}_{\mathrm{weak}}(V)$ which acts on the set $\mathcal{C}(V)$ of self-dual codes in V, and define some suitable subgroups $\Gamma \leqslant \mathrm{Aut}_{\mathrm{weak}}(V)$ which respect certain properties of codes, like the isometry type, or, in the case where V is a permutation module, i.e. has a distinct basis, the weight distribution.

The total number $M_{(V,\varphi)}$ of self-dual codes in V is then the sum of the orbit lengths under Γ – the mass formula (Theorem 4.2) is a reformulation of this fact, which relates the ratio $\frac{M_{(V,\varphi)}}{|\Gamma|}$ to the stabilizer orders of Γ-orbits, hence is a useful tool to prove completeness of a classification of all self-dual codes in V. As an example, we classify in Section 4.2 the self-dual binary $[48, 24]$-codes with an automorphism of order 23.

2. Morita theory for codes

Let A be an algebra and let $\bar{\ }$ be an involution of A, i.e. a bijective additive map satisfying $\overline{ab} = \bar{b}\bar{a}$ and $\bar{\bar{a}} = a$ for all $a, b \in A$. Morita theory for algebras with involution has been studied in [9] and [10], in particular with regard to the connections between Hermitian modules (cf. Definition 2.1) over two different algebras A, E over the same ring, where the Hermitian forms over A factorize through $\otimes_E$. This section studies Hermitian modules V over a semisimple algebra A over a finite field $\mathbb{F}$, with involution, and its center $E = Z(A)$, which is fixed under $\bar{\ }$, hence naturally carries an involution.

This context naturally arises in the study of codes and their automorphisms, which is resumed in Sections 3 and 4. There the algebra $A = \mathbb{F}G$ is a group algebra, for some subgroup $G \leqslant S_k$ of the symmetric group on k points such that the characteristic of $\mathbb{F}$ does not divide the order of G. The module $V = \mathbb{F}^k$ is then the associated permutation module over $\mathbb{F}G$. The group algebra $\mathbb{F}G$ carries a natural $\mathbb{F}$-linear involution given by $g \mapsto g^{-1}$, for $g \in G$. We will investigate the number of self-dual codes $C \leqslant \mathbb{F}^k$ which are G-submodules of V, i.e. $C\pi = C$ for all $\pi \in G$. Orthogonality is in this context defined with respect to the standard scalar product

$$(\,,\,) : \mathbb{F}^k \times \mathbb{F}^k \to \mathbb{F}, \qquad (v, v') \mapsto \sum_{i=1}^{k} v_i v'_i,$$

which takes values in $\mathbb{F}$ and is G-invariant, i.e. $(v, v') = (vg, v'g)$ for all $v, v' \in V$ and $g \in G$. This gives rise to the definition of the category $\mathrm{Mod}_A^{(\mathbb{F})}$ of equivariant A-modules (cf. Definition 2.2), which is Morita equivalent to the category $\mathrm{Mod}_A^{(A)}$ (cf. Definition 2.1). In analogy with the construction given in [9, Theorem 8.2] we are able to construct a Morita equivalence $\mathcal{F} : \mathrm{Mod}_A^{(A)} \to \mathrm{Mod}_E^{(E)}$ in Theorem 2.8.

Definition 2.1.

(i) A Hermitian form on a right A-module V is a biadditive mapping $\phi : V \times V \to A$ such that

$$\phi(v, wa) = \phi(v, w)a \quad \text{and} \quad \phi(v, w) = \overline{\phi(w, v)}$$

for all $v, w \in V$ and $a \in A$. If ϕ is non-degenerate, i.e. if

$$\operatorname{rad}(\phi) := \{ v \in V \mid \phi(v, w) = 0 \text{ for all } w \in V \} = \{0\}$$

then (V, ϕ) is called a Hermitian right A-module. Analogously one defines Hermitian left A-modules.

(ii) Let $\operatorname{Mod}_A^{(A)}$ be the category of Hermitian right A-modules. The morphisms from the object (V, ϕ) to the object (V', ϕ') are the A-module homomorphisms $\psi : V \to V'$ satisfying $\phi'(\psi(v), \psi(w)) = \phi(v, w)$ for all $v, w \in V$. Since any such homomorphism is injective, the morphisms are also called monometries.

Remark 1. Write $A = \bigoplus_{i=1}^{t} D_i^{n_i \times n_i}$, where the D_i are field extensions of $\mathbb{F}$. Then the involution $\overline{\ }$ preserves the center $Z(A) = \bigoplus_{i=1}^{t} D_i$, hence restricts to an automorphism of order 1 or 2 on $Z(A)$. So there are field automorphisms $\alpha_i \in \operatorname{Aut}(D_i)$ and a permutation $\pi \in S_t$ of order 1 or 2 such that

$$\overline{(z_1, \ldots, z_t)} = \left(z_{\pi(1)}^{\alpha_1}, \ldots, z_{\pi(t)}^{\alpha_t}\right)$$

for all $(z_1, \ldots, z_t) \in Z(A)$, where always $D_i \cong D_{\pi(i)}$ and α_i and $\alpha_{\pi(i)}$ are of the same order. We extend the automorphism α_i to an involution $\alpha_i : D_i^{n_i \times n_i} \to D_i^{n_i \times n_i}$, $M_i \mapsto (M_i^{\alpha_i})^{\mathrm{tr}}$, where M_i^{tr} is the transpose of the matrix M_i and α_i is applied componentwise. We obtain an involution

$$^J : A \to A, \qquad (M_1, \ldots, M_t) \mapsto \left(\left(M_{\pi(1)}^{\alpha_1}\right)^{\mathrm{tr}}, \ldots, \left(M_{\pi(t)}^{\alpha_t}\right)^{\mathrm{tr}}\right).$$

The composition $\overline{\ } \circ {}^J : A \to A$ is an automorphism of A restricting to the identity on the center of A. So by the theorem of Skolem and Noether (see for instance [11, Theorem 1.4]), the composition $\overline{\ } \circ {}^J$ is given by conjugation with a unit $u = (u_1, \ldots, u_t) \in A^*$. Hence

$$\overline{(M_1, \ldots, M_t)} = u(M_1, \ldots, M_t)^J u^{-1} = \left(u_1 \left(M_{\pi(1)}^{\alpha_1}\right)^{\mathrm{tr}} u_1^{-1}, \ldots, u_t \left(M_{\pi(t)}^{\alpha_t}\right)^{\mathrm{tr}} u_t^{-1}\right)$$

for all $(M_1, \ldots, M_t) \in A$. Note that by the above equation, the unit u must satisfy $u^{-1}\bar{u} \in Z(A)$ and $u^{-1}u^J \in Z(A)$, since $\overline{\ }$ and ^{J} both have order 1 or 2.

Definition 2.2.

(i) An equivariant form on V (with respect to $\overline{\ }$) is a biadditive mapping $\varphi : V \times V \to \mathbb{F}$ such that

$$\varphi(va, w) = \varphi(v, w\bar{a}), \qquad \varphi(v, w) = \overline{\varphi(w, v)} \quad \text{and} \quad \varphi(v, w\lambda) = \varphi(v, w)\lambda$$

for all $v, w \in V$, $a \in A$ and $\lambda \in \mathbb{F}$. The form φ is called non-degenerate if $\operatorname{rad}(\varphi) = \{0\}$, cf. Definition 2.1. If φ is non-degenerate then (V, φ) is called an equivariant A-module. Analogously one defines equivariant left A-modules.

(ii) Let $\operatorname{Mod}_A^{(\mathbb{F})}$ be the category of equivariant A-modules, with the monometries as morphisms (cf. Definition 2.1).

The categories $\mathrm{Mod}_A^{(A)}$ and $\mathrm{Mod}_A^{(F)}$ are equivalent, which has been shown in [12], for instance. The proof is as follows. Let $\mathrm{Trace}_{\mathrm{reg}} : A \to \mathbb{F}$ be the reduced trace, i.e. if $A = \bigoplus_{i=1}^{t} D_i^{n_i \times n_i}$ and $M = (M_1, \ldots, M_t) \in A$ then $\mathrm{Trace}_{\mathrm{reg}}(M) = \sum_{i=1}^{t} \mathrm{Tr}_{D_i/\mathbb{F}}(\mathrm{Trace}(M_i))$. The functor

$$T : \mathrm{Mod}_A^{(A)} \to \mathrm{Mod}_A^{(\mathbb{F})}, \qquad (V, \phi) \mapsto \big(V, \mathrm{Trace}_{\mathrm{reg}}(\phi)\big)$$

establishes an equivalence. Note that $\mathrm{Trace}_{\mathrm{reg}}(\phi)$ is non-degenerate whenever ϕ has this property, since $\mathrm{rad}(\mathrm{Trace}_{\mathrm{reg}}(\phi)) = \mathrm{rad}(\phi)$, due to the non-degeneracy of $\mathrm{Trace}_{\mathrm{reg}} : A \times A \to \mathbb{F}$, $(a, b) \mapsto \mathrm{Trace}_{\mathrm{reg}}(ab)$, cf. [13, Proposition 7.41].

In addition, the functor T preserves orthogonality (cf. Definition 2.3). This property ensures that any $(V, \phi) \in \mathrm{Mod}_A^{(A)}$ contains as many self-dual codes as $T((V, \phi))$.

Definition 2.3. Let $\mathcal{M}, \mathcal{M}'$ be categories of Hermitian or equivariant modules over the algebras $A_{\mathcal{M}}$ and $A_{\mathcal{M}'}$, respectively. A functor $F : \mathcal{M} \to \mathcal{M}'$, $(V, \beta) \mapsto (F_0(V), F_1(\beta))$ is said to preserve orthogonality if

$$F_0\big(C^{\perp,\beta}\big) = F_0(C)^{\perp, F_1(\beta)}$$

for every submodule $C \leqslant V$.

The main result of this section is the following.

Theorem 2.4. *There is an orthogonality-preserving equivalence between the categories* $\mathrm{Mod}_A^{(\mathbb{F})}$ *and* $\mathrm{Mod}_E^{(E)}$, *where* $E = Z(A)$ *is the center of* A, *with the restriction of* $\bar{\ }$ *to* E *as involution.*

The equivalence stated in Theorem 2.4 will be constructed as a composition

$$\mathrm{Mod}_A^{(\mathbb{F})} \xrightarrow{T^{-1}} \mathrm{Mod}_A^{(A)} \xrightarrow{\mathcal{F}} \mathrm{Mod}_E^{(E)},$$

where T is as above. The functor $\mathcal{F}$ is defined in Theorems 2.7 and 2.8, respectively. The latter theorem also states that $\mathcal{F}$ is an equivalence.

Remark 2. Let (W, ψ) be a Hermitian (resp. equivariant) left A-module. Consider W as a right module W_E over $E = Z(A)$ via $we := \bar{e}w$ for $w \in W$ and $e \in E$. Then (W_E, ψ) is also a Hermitian (resp. equivariant) right E-module, where the involution of E is the restriction of $\bar{\ }$.

The functor $\mathcal{F}$ transforms A-valued forms into E-valued forms. For its construction we need the following definition.

Definition 2.5. Let $A \cong \bigoplus_{i=1}^{t} D_i^{n_i \times n_i}$, where the D_i are field extensions of $\mathbb{F}$. Define

$$\mathrm{Trace}_{A/E} : A \to E, \qquad (M_1, \ldots, M_t) \mapsto \big(\mathrm{Trace}(M_1) I_{n_1}, \ldots, \mathrm{Trace}(M_t) I_{n_t}\big).$$

Finally, we need the notion of self-dual modules – note that this paper uses two different notions of duality. An A-module S is called self-dual if $S \cong S^* \cong \mathrm{Hom}_{\mathbb{F}}(S, \mathbb{F})$ (cf. Definition 2.6), whereas a submodule $C \leqslant (V, \phi)$ is called self-dual if $C = C^{\perp}$, where

$$C^{\perp} = \big\{ v \in V \;\big|\; \phi(v, c) = 0 \text{ for all } c \in C \big\}.$$

To distinguish these two notions, and also since we are mainly interested in the coding-theoretic applications (i.e. where V has a distinguished $\mathbb{F}$-basis), we talk about self-dual codes in the latter situation.

Definition 2.6. Let S be a right A-module and consider $\mathbb{F}$ as a right module over itself via $m \cdot \lambda := m\bar{\lambda}$, for $m, \lambda \in \mathbb{F}$. Then the dual module S^* is

$$S^* = \mathrm{Hom}_{\mathbb{F}}(S, \mathbb{F}) = \left\{ f : S \to \mathbb{F} \;\middle|\; f \text{ is additive and } f(s\lambda) = f(s) \cdot \lambda = f(s)\bar{\lambda} \text{ for all } s \in S,\ \lambda \in \mathbb{F} \right\},$$

which is a right A-module via $fa(s) := f(s\bar{a})$, for $f \in S^*$, $a \in A$ and $s \in S$. The module S is called self-dual if and only if $S \cong S^*$.

The following theorem introduces a functor $\mathrm{Mod}_A^{(A)} \to \mathrm{Mod}_E^{(E)}$, via a Hermitian left A-module (W, ψ). A similar construction has been made in [9].

Theorem 2.7. *Let (W, ψ) be a Hermitian left A-module such that*

$$\psi(w_1, w_2)w_3 = \mathrm{Trace}_{A/E}\big(\psi(w_3, w_2)\big)w_1 \qquad (\star\star)$$

for all $w_1, w_2, w_3 \in W$. Consider W as a right module over $E = Z(A)$ as in Remark 2. Define a functor

$$F_W := F_{(W,\psi)} : \mathrm{Mod}_A^{(A)} \to \mathrm{Mod}_E^{(E)}, \qquad (V, \phi) \mapsto (V \otimes_A \otimes_A W_E, \phi \otimes \psi),$$

where $\phi \otimes \psi := ((v \otimes w, v' \otimes w') \mapsto \mathrm{Trace}_{A/E}(\phi(v', v)\psi(w, w')))$. Then F_W preserves orthogonality.

Proof. To show that $\phi \otimes \psi$ is well defined one has to check that it is A-balanced, i.e. that

$$\mathrm{Trace}_{A/E}\big(\phi(v'a', va)\psi(w, w')\big) = \mathrm{Trace}_{A/E}\big(\phi(v', v)\psi(aw, a'w')\big)$$

for all $v, v' \in V$, $w, w' \in W$ and $a \in A$. Since ϕ and ψ are Hermitian, the left-hand side of the above equation equals

$$\mathrm{Trace}_{A/E}\big(\phi(v'a', v)a\psi(w, w')\big) = \mathrm{Trace}_{A/E}\big(\overline{\phi(v, v'a')}\psi(aw, w')\big) = \mathrm{Trace}_{A/E}\big(\overline{a'\phi(v, v')}\psi(aw, w')\big).$$

Due to the elementary properties of the Trace function, the arguments of the latter term may be permuted by a cyclic shift, i.e. the latter equals

$$\mathrm{Trace}_{A/E}\big(\overline{\phi(v, v')}\psi(aw, w')\bar{a'}\big) = \mathrm{Trace}_{A/E}\big(\phi(v', v)\overline{a'\psi(w', aw)}\big) = \mathrm{Trace}_{A/E}\big(\phi(v', v)\psi(aw, aw')\big),$$

as claimed. It remains to show that F_W preserves orthogonality, i.e. that

$$F_W(C)^{\perp,\phi\otimes\psi} = F_W\big(C^{\perp,\phi}\big)$$

for all submodules $C \leqslant V$, where $(V, \phi) \in \mathrm{Mod}_A^{(A)}$.

The inclusion $F_W(C^{\perp,\phi}) \subseteq F_W(C)^{\perp,\phi\otimes\psi}$ follows immediately from the definition of the form $\phi \otimes \psi$.

For the inclusion $F_W(C)^{\perp,\phi\otimes\psi} \subseteq F_W(C^{\perp,\phi})$, let $\sum_{i=1}^k v_i \otimes w_i \in F_W(C)^{\perp,\phi\otimes\psi}$. Then

$$\mathrm{Trace}_{A/E}\left(\sum_{i=1}^k \phi(c, v_i)\psi(w_i, w')\right) = \mathrm{Trace}_{A/E}\left(\phi\left(c, \sum_{i=1}^k v_i\psi(w_i, w')\right)\right) = 0$$

for all $c \in C$ and $w' \in W$. Now C is a right A-module and ϕ is Hermitian, hence the latter equation implies that

$$\mathrm{Trace}_{A/E}\left(\phi\left(c, \sum_{i=1}^k v_i\psi(w_i, w')\right)a\right) = 0$$

for all $c \in C$, $w' \in W$ and $a \in A$. This implies that always $\phi(c, \sum_{i=1}^{k} v_i \psi(w_i, w')) = 0$, due to the non-degeneracy of $\mathrm{Trace}_{A/E} : A \times A \to E,\ (x, y) \mapsto \mathrm{Trace}_{A/E}(xy)$.

Hence always $\sum_{i=1}^{k} v_i \psi(w_i, w') \in C^{\perp,\phi}$ and hence $\sum_{i=1}^{k} v_i \psi(w_i, w') \otimes w'' \in F_W(C^{\perp,\phi})$ for all $w'' \in W$. Choosing $w', w'' \in W$ with $\mathrm{Trace}_{A/E}(\psi(w', w'')) = 1$, this yields

$$\sum_{i=1}^{k} v_i \psi(w_i, w') \otimes w'' = \sum_{i=1}^{k} v_i \otimes \psi(w_i, w') w'' = \sum_{i=1}^{k} v_i \otimes \mathrm{Trace}_{A/E}\big(\psi(w'', w')\big) w_i$$
$$= \sum_{i=1}^{k} v_i \otimes w_i \in F_W\big(C^{\perp,\phi}\big).$$

The fact that F_W preserves orthogonality implies that $\phi \otimes \psi$ is non-degenerate since

$$\mathrm{rad}(\phi \otimes \psi) = F_W(V)^{\perp,\phi\otimes\psi} = F_W\big(V^{\perp,\phi}\big) = F_W\big(\mathrm{rad}(\phi)\big) = \{0\}. \qquad \square$$

The functor $\mathcal{F}$ is now obtained by a particular choice of W in Theorem 2.7.

Theorem 2.8. *Let $\mathfrak{S}$ be a system of representatives for the isomorphism classes of simple left A-modules, and let $\mathcal{W} := \bigoplus_{S\in\mathfrak{S}} S$. Fix a non-degenerate Hermitian form ψ on $\mathcal{W}$ such that (W, ψ) satisfies condition $(\star\star)$ from Theorem 2.7. Then $\mathcal{F} := F_{(\mathcal{W},\psi)} : \mathrm{Mod}_A^{(A)} \to \mathrm{Mod}_E^{(E)}$ is an equivalence of categories which preserves orthogonality.*

Note that condition $(\star\star)$ in Theorem 2.7 is natural and that, in the situation of Theorem 2.8, there always exists a form ψ satisfying this condition: Write $A = \bigoplus_{i=1}^{t} D_i^{n_i\times n_i}$ and let π be a permutation on t points, $\alpha_i \in \mathrm{Aut}(D_i)$ and $u = (u_1, \ldots, u_t) \in A^*$ with $\overline{M_i} = u_i (M_{\pi(i)}^{\alpha_i})^{\mathrm{tr}} u_i^{-1}$, for $M_i \in D_i^{n_i\times n_i}$ (cf. Remark 1). We may assume that $u\bar{u}^{-1} = 1$, cf. [14].

On $\mathcal{W} \cong \bigoplus_{i=1}^{t} D_i^{n_i\times 1}$ there exists a non-degenerate Hermitian form

$$\psi : \mathcal{W} \times \mathcal{W} \to A, \qquad \left(\bigoplus_{i=1}^{t} d_i, \bigoplus_{i=1}^{t} f_i\right) \mapsto \bigoplus_{i=1}^{t} d_i \big(f_{\pi(i)}^{\alpha_i}\big)^{\mathrm{tr}} u_i^{-1}.$$

We show that ψ satisfies condition $(\star\star)$, i.e. that $\psi(d_i, f_{\pi(i)}) g_i = \mathrm{Trace}_{A/E}(\psi(g_i, f_{\pi(i)})) d_i$ for all $d_i, g_i \in D_i^{n_i\times 1} \leqslant \mathcal{W}$ and $f_{\pi(i)} \in D_{\pi(i)}^{n_{\pi(i)}\times 1} \leqslant \mathcal{W}$ (note that $n_{\pi(i)} = n_i$ and $D_{\pi(i)} = D_i$). The element $(f_{\pi(i)}^{\alpha_i})^{\mathrm{tr}} \in D_i^{1\times n_i}$ and $u_i^{-1} g_i \in D_i^{n_i\times 1}$, hence

$$\big(f_{\pi(i)}^{\alpha_i}\big)^{\mathrm{tr}} u_i^{-1} g_i = \mathrm{Trace}\big(u_i^{-1} g_i \big(f_{\pi(i)}^{\alpha_i}\big)^{\mathrm{tr}}\big) = \mathrm{Trace}\big(g_i \big(f_{\pi(i)}^{\alpha_i}\big)^{\mathrm{tr}} u_i^{-1}\big),$$

where $\mathrm{Trace} : D_i^{n_i\times n_i} \to D_i$ denotes the usual trace of a matrix. Hence

$$\psi(d_i, f_{\pi(i)}) g_i = d_i \big(f_{\pi(i)}^{\alpha_i}\big)^{\mathrm{tr}} u_i^{-1} g_i = d_i\, \mathrm{Trace}\big(g_i \big(f_{\pi(i)}^{\alpha_i}\big)^{\mathrm{tr}} u_i^{-1}\big) = \mathrm{Trace}_{A/E}\big(g_i \big(f_{\pi(i)}^{\alpha_i}\big)^{\mathrm{tr}} u_i^{-1}\big) d_i$$
$$= \mathrm{Trace}_{A/E}\big(\psi(g_i, f_{\pi(i)})\big) d_i,$$

which shows that ψ satisfies condition $(\star\star)$.

We now prove Theorem 2.8.

Proof. Let $\mathcal{W}^{op}$ be the set $\mathcal{W}$ with a right A-module structure given by $w * a := \bar{a} w$ for $a \in A$ and $w \in \mathcal{W}$.

The form $\widehat{\psi} : \mathcal{W}^{op} \times \mathcal{W}^{op} \to A,\ (w, w') \mapsto \psi(w, w')$ is then non-degenerate and Hermitian.
Note that $\mathcal{W}^{op}$ is also a left E-module (since $\mathcal{W}$ is a left A-module). Hence we can define a functor

$$H : \mathrm{Mod}_E^{(E)} \to \mathrm{Mod}_A^{(A)}, \qquad (U, \varphi) \mapsto \big(U \otimes_E \mathcal{W}^{op}, \varphi \otimes \widehat{\psi}\big),$$

where

$$\varphi \otimes \widehat{\psi}(u \otimes w, u' \otimes w') := \varphi(u', u)\widehat{\psi}(w, w').$$

To prove that $\varphi \otimes \widehat{\psi}$ is well defined, one has to check that it is E-balanced, i.e. that

$$\varphi(u'e', ue)\widehat{\psi}(w, w') = \varphi(u', u)\widehat{\psi}(ew, e'w')$$

for all $u, u' \in U,\ w, w' \in \mathcal{W}^{op}$ and $e, e' \in E$. This can be proven by calculations analogous to those in the proof of Theorem 2.7, exploiting the fact that $E = Z(A)$.

In the following we show that H and F are inverse functors.

(i) First, let $(V, \phi) \in \mathrm{Mod}_A^{(A)}$ and show that $H(F((V, \phi)))$ and (V, ϕ) are isometric. Clearly, $V \otimes_A \mathcal{W} \otimes_E \mathcal{W}^{op} \cong A$ as right A-modules via $\alpha : (v \otimes w \otimes \hat{w}) \mapsto v\widehat{\psi}(w, \hat{w})$.
To see that α is an isometry, we calculate that

$$\begin{aligned}
&(\phi \otimes \psi) \otimes \widehat{\psi}(v \otimes w \otimes \hat{w}, v' \otimes w' \otimes \hat{w}') \\
&\quad = \phi \otimes \psi(v' \otimes w', v \otimes w)\widehat{\psi}(\hat{w}, \hat{w}') \\
&\quad = \mathrm{Trace}_{A/E}\big(\phi(v, v')\psi(w', w)\big)\widehat{\psi}(\hat{w}, \hat{w}') = \mathrm{Trace}_{A/E}\big(\psi\big(\phi(v, v')w', w\big)\big)\widehat{\psi}(\hat{w}, \hat{w}') \\
&\quad = \widehat{\psi}\big(\hat{w}, \hat{w}' * \mathrm{Trace}_{A/E}\big(\psi\big(\phi(v, v')w', w\big)\big)\big) = \widehat{\psi}\big(\hat{w}, \mathrm{Trace}_{A/E}\big(\psi\big(w, \phi(v, v')w'\big)\big)\hat{w}'\big) \\
&\quad \overset{(\star\star)}{=} \widehat{\psi}\big(\hat{w}, \psi\big(\hat{w}', \phi(v, v')w'\big)w\big) = \widehat{\psi}\big(\hat{w}, w * \psi\big(\phi(v, v')w', \hat{w}'\big)\big) \\
&\quad = \widehat{\psi}(\hat{w}, w)\psi\big(\phi(v, v')w', \hat{w}'\big) = \widehat{\psi}(\hat{w}, w)\phi(v, v')\widehat{\psi}(w', \hat{w}') \\
&\quad = \widehat{\psi}(\hat{w}, w)\phi\big(v, v'\widehat{\psi}(w', \hat{w}')\big) = \overline{\phi\big(v'\widehat{\psi}(w', \hat{w}'), v\big)\widehat{\psi}(w, \hat{w})} \\
&\quad = \overline{\phi\big(v'\widehat{\psi}(w', \hat{w}'), v\widehat{\psi}(w, \hat{w})\big)} = \phi\big(v\widehat{\psi}(w, \hat{w}), v'\widehat{\psi}(w', \hat{w}')\big) \\
&\quad = \phi\big(\alpha(v \otimes w \otimes \hat{w}), \alpha(v' \otimes w' \otimes \hat{w}')\big)
\end{aligned}$$

for all $(v \otimes w \otimes \hat{w}),\ (v' \otimes w' \otimes \hat{w}') \in U \otimes \mathcal{W} \otimes \mathcal{W}^{op}$.

(ii) Now let $(U, \varphi) \in \mathrm{Mod}_E^{(E)}$ and show that $F(H((U, \varphi)))$ and (U, φ) are isometric. The natural isomorphism $\gamma : U \otimes_E \mathcal{W}^{op} \otimes_A \mathcal{W} \to U,\ (u \otimes \hat{w} \otimes w) \mapsto u\,\mathrm{Trace}_{A/E}(\widehat{\psi}(\hat{w}, w))$ is an isometry since

$$\begin{aligned}
&(\varphi \otimes \widehat{\psi}) \otimes \psi(u \otimes \hat{w} \otimes w, u' \otimes \hat{w}' \otimes w') \\
&\quad = \mathrm{Trace}_{A/E}\big(\varphi \otimes \widehat{\psi}(u' \otimes \hat{w}', u \otimes \hat{w})\psi(w, w')\big) \\
&\quad = \mathrm{Trace}_{A/E}\big(\varphi(u, u')\widehat{\psi}(\hat{w}'\hat{w})\psi(w, w')\big) = \varphi(u, u')\,\mathrm{Trace}_{A/E}\big(\widehat{\psi}\big(\hat{w}', \hat{w} * \psi(w, w')\big)\big) \\
&\quad = \varphi(u, u')\,\mathrm{Trace}_{A/E}\big(\widehat{\psi}\big(\hat{w}', \psi(w', w)\hat{w}\big)\big) = \varphi(u, u')\,\mathrm{Trace}_{A/E}\big(\widehat{\psi}(\hat{w}')\big) \\
&\quad \overset{(\star\star)}{=} \varphi(u, u')\,\mathrm{Trace}_{A/E}\big(\widehat{\psi}(\hat{w}', \mathrm{Trace}_{A/E}\big(\psi(\hat{w}, w)\big)w')\big) \\
&\quad = \varphi(u, u')\,\mathrm{Trace}_{A/E}\big(\widehat{\psi}\big(\hat{w}', w'\,\mathrm{Trace}_{A/E}\big(\psi(w, \hat{w})\big)\big)\big) \\
&\quad = \varphi(u, u')\,\mathrm{Trace}_{A/E}\big(\widehat{\psi}(\hat{w}', w')\big)\,\mathrm{Trace}_{A/E}\big(\psi(w, \hat{w})\big)
\end{aligned}$$

$$= \varphi\big(u, u' \operatorname{Trace}_{A/E}\big(\widehat{\psi}(\hat{w}', w')\big)\big) \operatorname{Trace}_{A/E}\big(\widehat{\psi}(w, \hat{w})\big)$$
$$= \varphi\big(u \operatorname{Trace}_{A/E}\big(\widehat{\psi}(\hat{w}, w)\big), u' \operatorname{Trace}_{A/E}\big(\widehat{\psi}(\hat{w}', w')\big)\big)$$
$$= \varphi\big(\gamma(u \otimes \hat{w} \otimes w), \gamma(u' \otimes \hat{w}' \otimes w')\big)$$

for all $(u \otimes \hat{w} \otimes w)$, $(u' \otimes \hat{w}' \otimes w') \in U \otimes \mathcal{W}^{op} \otimes \mathcal{W}$. □

3. Enumeration of self-dual codes

The Morita equivalence $\mathcal{F}$ defined in Theorem 2.8 establishes a bijection between the self-dual codes in (V, ϕ) and the self-dual codes in its Morita equivalent module $\mathcal{F}((V, \phi)) \in \operatorname{Mod}_E^{(E)}$, where $E = Z(A)$ is a direct sum of finite fields.

Except when q is even and $\bar{}$ is the identity, $\mathcal{F}((V, \phi))$ will be determined up to isometry by the composition factors of V in Section 3.1. For every self-dual code $C \leqslant V$, the image $\mathcal{F}(C) \leqslant \mathcal{F}(V)$ is a direct sum of self-dual codes over finite fields, or over a ring $L \oplus L$, where L is a finite field. Enumeration formulae for codes of this kind have been given in [7], e.g. and are reproduced in Section 3.2. As a corollary, the number of self-dual codes in (V, ϕ) is given in Section 3.3.

To fix some notation, let $\mathfrak{S}$ denote a system of representatives for the isomorphism classes of simple right A-modules. For $S \in \mathfrak{S}$, let $D_S := \operatorname{End}_A(S)$ and let n_S denote the multiplicity of the simple module S in V.

3.1. Determination of the Morita equivalent module $\mathcal{F}((V, \phi))$

The module V decomposes into an orthogonal sum, which is respected by the functor $\mathcal{F}$.

Remark 3. For $S \in \mathfrak{S}$, denote by V_S the S-homogeneous component of V. Then there is an orthogonal decomposition

$$V = \perp_{S \in \mathfrak{S},\, S \cong S^*} V_S \perp_{\{T, T^*\} \subseteq \mathfrak{S},\, T \ncong T^*} (V_T \oplus V_{T^*}). \qquad (\star)$$

In particular, the restriction ϕ_U of ϕ to a summand U in $(\star)$ is non-degenerate and equivariant, and if $C \leqslant V$ is a self-dual code then $C \cap U$ is a self-dual code in U with respect to ϕ_U.

Lemma 3.2 gives the images under $\mathcal{F}$ of the orthogonal summands of V. To this aim the following result proven in [15] is useful.

Lemma 3.1. *Let $e_S \in Z(A)$ be the central primitive idempotent belonging to the simple module $S \in \mathfrak{S}$. Then $\overline{e_S} = e_{S^*}$. In particular S is self-dual if and only if $\overline{e_S} = e_S$.*

Lemma 3.2. *Let $S \in \mathfrak{S}$, and let e_S be the central primitive idempotent belonging to S. Let n be an integer, and by $\mathcal{F}$ denote the Morita equivalence from Theorem* 2.8.

(i) *Assume that $S \cong S^*$. There is a natural isomorphism $D_S \cong e_S Z(A)$, of which the image is invariant under $\bar{}$ according to Lemma* 3.1. *Thus $\bar{}$ induces an involution $\bar{}^{(S)}$ on D_S, which will be further investigated in Lemma* 3.3.
Assume that S^n carries a non-degenerate equivariant form φ. Then $\mathcal{F}((S^n, \varphi)) \cong ((D_S)^n, \varphi')$, where φ' is equivariant with respect to $\bar{}^{(S)}$.
If (S^n, φ) contains a self-dual code then so does $\mathcal{F}((S^n, \varphi))$, since $\mathcal{F}$ preserves orthogonality. Hence if $\mathbb{F}$ has odd characteristic then $\mathcal{F}((S^n, \varphi)) \cong \perp_{i=1}^{\frac{n}{2}} \mathbb{H}(D_S)$ is an orthogonal sum of hyperbolic planes $\mathbb{H}(\mathbb{F})$ over D_S (cf. [16, *Chapter* 1, *Corollary* 3.10, *Theorem* 6.4 *and Chapter* 7, *Theorem* 6.3]*). The same holds in even characteristic, if $\bar{}^{(S)}$ is not the identity.*

If the characteristic of $\mathbb{F}$ is even and $^{-(S)}$ is the identity then either $\mathcal{F}((S^n,\phi))$ is an orthogonal sum of hyperbolic planes as above, or $\mathcal{F}((S^n,\phi)) \cong \perp_{i=1}^{\frac{n}{2}-1} \mathbb{H}(D_S) \perp W$, where $W \cong (\mathbb{F}^2, \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right))$.

(ii) *Assume that $S \not\cong S^*$, and consider again the natural isomorphism $D_S \cong e_S Z(A)$. Then $\overline{D_S} = D_{S^*}$ according to Lemma* 3.1 *and hence the sum $D_S \oplus D_{S^*}$ is invariant under $^-$. Let φ be a non-degenerate equivariant form on $(S \oplus S^*)^n$. Then $(S \oplus S^*)^n$ contains a self-dual code. Hence $\mathcal{F}((S \oplus S^*)^n, \varphi) \cong ((D_S)^n \oplus (D_S)^n, \varphi') \cong \perp_{i=1}^{n} \mathbb{H}(\mathbb{F})$ is an orthogonal sum of hyperbolic planes, where φ' is equivariant with respect to the restriction of $^-$ to $D_S \oplus D_{S^*}$. Here $(D_S)^n \oplus (D_{S^*})^n$ is a $(D_S \oplus D_{S^*})$-module in the natural way. Hence the self-dual codes in this module correspond to the subspaces of $(D_S)^n$.*

Lemma 3.3. *For a simple self-dual A-module $S \cong S^*$ consider the natural embeddings $\mathbb{F} \hookrightarrow D_S \hookrightarrow Z(A)$. According to Lemma* 3.2(i) *the involution $^-$ on A restricts to an involution on D_S. This restriction is either the identity on D_S or a field automorphism of order* 2. *Clearly the latter holds if $^-$ is non-trivial on $\mathbb{F}$.*

Assume that $\overline{f} = f$ for all $f \in \mathbb{F}$. Then the following are equivalent:

(i) *$\bar{d} = d$ for all $d \in D_S$,*
(ii) *if $L \supseteq \mathbb{F}$ is a field extension with $L \cong D_S$ then every composition factor of the right $A \otimes_{\mathbb{F}} L$-module $S \otimes_{\mathbb{F}} L$ is self-dual.*

Proof. Let $A_L := A \otimes_{\mathbb{F}} L$ and let $^{-(L)}$ be the L-linear extension of $^-$ to A_L defined by $\overline{a \otimes l} := \bar{a} \otimes l$ for all $a \in A$ and $l \in L$, which is well-defined since $\mathbb{F}$ is fixed by $^-$. In particular $^-$ is trivial on $D_S \subseteq A$ if and only if $^{-(L)}$ is trivial on $D_S \otimes_{\mathbb{F}} L$. Let $e \in D_S$ be the central primitive idempotent belonging to S, and let $e = e_1 + \cdots + e_n$ be a decomposition into central primitive idempotents e_i of A_L, according to a decomposition of $S \otimes_{\mathbb{F}} L$ into simple modules over $D_S \otimes_{\mathbb{F}} L$. The e_i generate $D_S \otimes_{\mathbb{F}} L$ as a vector space over L and hence $^{-(L)}$ is trivial on $D_S \otimes_{\mathbb{F}} L$ if and only if it fixes all of the e_i, i.e. if and only if every composition factor $e_i A_L$ of $S \otimes_{\mathbb{F}} L$ satisfies $e_i A_L = \overline{e_i} A_L \cong (e_i A_L)^*$ (see Lemma 3.1). □

3.2. Enumeration of self-dual codes over finite fields

The formulae in this section are given in [7].

Lemma 3.4. *(See Ex. 10.4 of [7].) Let $\mathbb{F} = \mathbb{F}_q$ be a finite field, where $q = r^2$, and let $^r : x \mapsto x^r \in \mathcal{G}al(\mathbb{F}_q/\mathbb{F}_r)$ be the field automorphism of order* 2. *Let φ be a non-degenerate form on $\mathbb{F}^n$ which is equivariant with respect to ^{r}. If $(\mathbb{F}^n, \varphi)$ contains a self-dual code then the number of self-dual codes in U equals*

$$\Upsilon_u(n,q) := \prod_{i=1}^{n} \left(q^{\frac{i}{2}} - (-1)^i\right) \left(\prod_{j=1}^{\frac{n}{2}} \left(q^j - 1\right) \right)^{-1}. \tag{3}$$

Lemma 3.5. *(See Ex. 11.3 of [7].) Let $\mathbb{F} = \mathbb{F}_q$ be a finite field, where q is odd, and let φ be a non-degenerate symmetric bilinear form on $\mathbb{F}^n$. If $(\mathbb{F}^n, \varphi)$ contains a self-dual code then the number of self-dual codes in U equals*

$$\Upsilon_o^+(n,q) := \prod_{i=0}^{\frac{n}{2}-1} \left(q^i + 1\right). \tag{4}$$

Lemma 3.6. *(See Ex. 11.3 of [7].) Let $\mathbb{F} = \mathbb{F}_q$ be a finite field, where q is even, and let φ be a non-degenerate symmetric bilinear form on $\mathbb{F}^n$ such that $(\mathbb{F}^n, \varphi) \cong \perp_{i=1}^{\frac{n}{2}} \mathbb{H}(\mathbb{F})$ is an orthogonal sum of hyperbolic planes, i.e. totally isotropic. Then the number of self-dual codes in U equals*

$$\Upsilon_o^+(n,q) := \prod_{i=1}^{\frac{n}{2}} \left(q^i + 1\right). \tag{5}$$

The following lemma is an immediate corollary of Lemma 3.6.

Lemma 3.7. *Let $\mathbb{F} = \mathbb{F}_q$ be a finite field, where q is even. Let φ be a non-degenerate symmetric bilinear form on $\mathbb{F}^n$ such that $(\mathbb{F}^n, \varphi) \cong \perp_{i=1}^{\frac{n}{2}-1} \mathbb{H}(\mathbb{F}) \perp W$, where $W \cong \left(\mathbb{F}^2, \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right)$. Then the number of self-dual codes in $(\mathbb{F}^n, \varphi)$ equals*

$$\Upsilon_o^-(n, q) := \Upsilon_o^+(n-2, q).$$

Moreover, we need an enumeration formula for vector spaces, cf. Lemma 3.2(ii).

Lemma 3.8. *Let U be a vector space over the finite field $\mathbb{F} = \mathbb{F}_q$, $n := \dim(U)$. Then the number of subspaces of U equals*

$$\Xi(n, q) := \sum_{k=0}^{n} \prod_{i=0}^{n-k-1} \frac{q^{n-i} - 1}{q^{n-k-i} - 1}.$$

3.3. Enumeration of self-dual codes in (V, φ)

As before, let $\mathbb{F} = \mathbb{F}_q$ be a finite field with q elements and let A be a finite semisimple algebra over $\mathbb{F}$.

Let $\mathfrak{S}$ be a system of representatives for the isomorphism classes of simple right A-modules, and for $S \in \mathfrak{S}$ let $d_S := \dim_{\mathbb{F}}(\mathrm{End}_A(S))$. By n_S denote the multiplicity of S in V. The involution $\overline{\ }$ restricts to an involution of the Morita equivalent algebra $E = Z(A) = \bigoplus_{S \in \mathfrak{S}} \mathrm{End}_A(S)$ (cf. Lemma 3.3), and also to a field automorphism of $\mathbb{F}$ (cf. Remark 1), where $\mathbb{F}$ is naturally embedded into $Z(A)$ by $f \mapsto f \cdot 1$. The restriction to $\mathbb{F}$ is either the identity or a field automorphism of order 2 – we distinguish these two cases to enumerate the self-dual codes in $(V, \varphi) \in \mathrm{Mod}_A^{(\mathbb{F})}$, which in what follows is assumed to contain at least one such code.

As corollaries from the previous subsections we obtain the following enumeration formulae.

Corollary 3.9. *If $q = r^2$ and $\overline{f} = f^r$ for all $f \in \mathbb{F}_q$ then the number of self-dual codes in (V, φ) equals*

$$M_{(V,\varphi)} = \prod_{S \in \mathfrak{S},\, S \cong S^*} \Upsilon_u\left(n_S, q^{d_S}\right) \prod_{\{T, T^*\} \subseteq \mathfrak{S},\, T \ncong T^*} \Xi\left(n_T, q^{d_T}\right).$$

Corollary 3.10. *Assume that q is odd and $\overline{f} = f$ for all $f \in \mathbb{F}$. Let*

$$\mathfrak{S}' := \left\{ S \in \mathfrak{S} \;\middle|\; S \cong S^* \text{ and } \bar{e} = e \text{ for all } e \in \mathrm{End}_A(S) \right\}.$$

Then the number of self-dual codes in (V, φ) equals

$$M_{(V,\varphi)} = \prod_{S' \in \mathfrak{S}'} \Upsilon_o\left(n_{S'}, q^{d_{S'}}\right) \prod_{S \in \mathfrak{S} - \mathfrak{S}',\, S \cong S^*} \Upsilon_u\left(n_S, q^{d_S}\right) \prod_{\{T, T^*\} \subseteq \mathfrak{S},\, T \ncong T^*} \Xi\left(n_T, q^{d_T}\right).$$

In the remaining case where q is even and ϕ is symmetric, it is in general not possible to determine $\mathcal{F}((V, \varphi))$ only from the composition factors of V, cf. Lemma 3.2(i). Yet this is possible if $A = \mathbb{F}G$ is a group algebra over the finite group G.

It is well known that if the field L, of even characteristic, is a splitting field for the finite group G of odd order then the trivial module is the only self-dual irreducible LG-module. An application of Lemma 3.3 then yields that the restriction of $\overline{\ }$ to $Z(A) = E = \bigoplus_{S \in \mathfrak{S}} \mathrm{End}_A(S)$ is non-trivial on every of these summands, except for the summand belonging to the trivial module.

To investigate the number of self-dual codes in this summand under $\mathfrak{F}$ one has to distinguish whether (V,φ) is symplectic, i.e. whether $\varphi(v,v)=0$ for all $v\in V$. As an application of Lemma 3.2 one obtains

Corollary 3.11. *Assume that $A=\mathbb{F}_qG$ is a group algebra over the finite group G, where q is even and G has odd order, and that $\overline{f}=f$ for all $f\in\mathbb{F}$. By $\mathbf{1}$ denote the trivial $\mathbb{F}G$-module.*

The number of self-dual codes in (V,ϕ) equals

$$M_{(V,\varphi)}=\Upsilon_o^{\sigma}(n_{\mathbf{1}},q)\prod_{S\in\mathfrak{S},\,\mathbf{1}\ncong S\cong S^*}\Upsilon_u\left(n_S,q^{d_S}\right)\prod_{\{T,T^*\}\subseteq\mathfrak{S},\,T\ncong T^*}\Xi\left(n_T,q^{d_T}\right),$$

where $\sigma=+$ if (V,φ) is totally isotropic and, otherwise, $\sigma=-$.

3.4. Example: Binary extended cyclic codes

Let $\mathbb{F}=\mathbb{F}_2$ and $A=\mathbb{F}C_n$, where C_n is the cyclic group with n elements for some odd integer n. A binary extended cyclic code, as defined in [4], is an A-submodule of

$$V=A\oplus\mathbf{1}=\mathbb{F}^{n+1},$$

where $\mathbf{1}$ is the trivial A-module, i.e. C_n acts on V by cyclic shifts of the first n coordinates and fixes the $(n+1)$st coordinate. The standard scalar product φ on V satisfies $\varphi(v,v')=\varphi(vg,v'g)$ for all $v,v'\in V$ and $g\in C_n$, hence is equivariant with respect to the $\mathbb{F}$-linear involution on $\mathbb{F}C_n$ given by $g\mapsto g^{-1}$ for $g\in C_n$.

The situation where a self-dual binary extended cyclic code exists has been characterized in [4] as follows.

Theorem 3.12. *There exists a self-dual binary extended cyclic code $C\leqslant V=\mathbb{F}C_n\oplus\mathbf{1}$ if and only if $-1\notin\langle 2\rangle\leqslant(\mathbb{Z}/p\mathbb{Z})^*$ for all prime divisors p of n, i.e. the order of 2 mod p is odd.*

Remark 4. If the order of 2 mod p is odd then 2 is a square mod p and hence $p\equiv_8\pm1$ by quadratic reciprocity. If $p\equiv_8-1$ then -1 is not a square and hence $-1\notin\langle 2\rangle\leqslant(\mathbb{Z}/p\mathbb{Z})^*$. However, if $p\equiv_8 1$ then the order of 2 may be even or odd mod p. For $p=41$ the order of 2 is 20, for $p=73$ the order is 9.

The structure of the module $V=\mathbb{F}C_n$ is easy to describe and the number of self-dual codes in V is particularly easy to determine, cf. Example 3.13. The criterion for the existence of a self-dual binary extended cyclic code in Example 3.13 has been given in [17, Theorem 3.3] in a more general context.

Example 3.13. There exists a self-dual binary extended cyclic code $C\leqslant V=\mathbb{F}C_n\oplus\mathbf{1}$ if and only if the trivial module is the only self-dual irreducible $\mathbb{F}C_n$-module. In this case there are

$$M_{(V,\varphi)}=2^{\frac{|\mathfrak{S}|-1}{2}}$$

such codes, where $\mathfrak{S}$ is a system of representatives for the isomorphism classes of simple right $\mathbb{F}C_n$-modules.

Proof. Assume that there exists a self-dual code $C\leqslant V$. Then according to [5], Corollary 2.4, every self-dual simple $\mathbb{F}C_n$-module occurs in a composition series of V with even multiplicity. On the other hand, every simple $\mathbb{F}C_n$-module occurs in V with multiplicity 1, except for the trivial module, which occurs in V with multiplicity 2. Hence

$$V\cong\perp_{\{T,T^*\}\subseteq\mathfrak{S},\,T\ncong\mathbf{1}}(T\oplus T^*)\perp\mathbf{1}\perp\mathbf{1}.\qquad(\bigstar)$$

Conversely, if the trivial module is the only self-dual irreducible $\mathbb{F}C_n$-module then clearly V decomposes as in (★). Let $T \oplus T^*$ be a summand in (★) and let e be the central primitive idempotent belonging to T. Then $\bar{e}$ is the central primitive idempotent belonging to T^* according to Remark 3.1, hence annihilates T. Thus

$$\varphi(t, t') = \varphi(te, t') = \varphi(t, t'\bar{e}) = \varphi(t, 0) = 0$$

for all $t, t' \in T$, i.e. $T \subseteq T^{\perp}$. Choose a subset $\mathcal{T} \subseteq \mathfrak{S} - \{\mathbf{1}\}$ such that for every non-trivial irreducible A-module T, either T or T^* is contained in $\mathcal{T}$. Then

$$C := \langle T \mid T \in \mathcal{T} \rangle + \big\langle (1, \ldots, 1) \big\rangle$$

is a self-dual code in V.

An application of Corollary 3.11 then yields

$$M_{(V,\varphi)} = \Upsilon_o^-(2,2) \prod_{\{T,T^*\} \subseteq \mathfrak{S},\, T \ncong \mathbf{1}} \Xi\big(1, 2^{d_T}\big) = 2^{\frac{|\mathfrak{S}|-1}{2}},$$

where the value of $d_T = \dim(\mathrm{End}_A(T))$ is irrelevant since $\Xi(1, 2^{d_T})$ counts the number of subspaces of a one-dimensional vector space over a field of size 2^{d_T}. □

Example 3.14.

(i) *Binary extended cyclic codes of length* 8. The order of 2 in the unit group $\mathbb{F}_7^*$ of $\mathbb{F}_7$ equals 3. More precisely, the subgroup of $\mathbb{F}_7^*$ generated by 2 has index 2 and the cosets are $\mathbb{F}_7^* = \{1, 2, 4\} \dot{\cup} \{3, 5, 6\}$. This yields central primitive idempotents $e, f \in \mathbb{F}_2 C_7$,

$$e = 1 + a + a^2 + a^4 \quad \text{and} \quad f = 1 + a^3 + a^5 + a^6,$$

where a is a generator of C_7. These satisfy $ef = 0$ and $\bar{e} = f$. Hence $V = \mathbb{F}_2 C_7 \oplus \mathbb{F}_2 = \mathbb{F}_2^8$ contains exactly the two self-dual codes

$$C = \big\langle Ve, (1, \ldots, 1) \big\rangle \quad \text{and} \quad D = \big\langle Vf, (1, \ldots, 1) \big\rangle$$

with generator matrices

$$M_C := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix} \quad \text{and} \quad M_D := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

These codes are permutation equivalent to the extended Hamming code e_8 of length 8.

(ii) Let p be a prime with $p \equiv_8 -1$. Then there exist exactly $2^{\frac{t}{2}}$ self-dual binary extended cyclic codes of length $p + 1$, where $t := [\mathbb{F}_p^* : \langle 2 \rangle]$ is the index of the subgroup generated by 2 in the unit group $\mathbb{F}_p^*$ of $\mathbb{F}_p$.

(iii) *Self-dual binary codes over* $\mathbb{F}_2(C_3 \wr C_3)$. The wreath product

$$G := C_3 \wr C_3 = \big\langle (1,2,3), (4,5,6), (7,8,9), (1,4,7)(2,5,8)(3,6,9) \big\rangle$$

acts on 9 points, hence yields a permutation module $\widetilde{V}$ of dimension 9 over $A = \mathbb{F}_2 G$. Let $V := \widetilde{V} \oplus \widetilde{V} \oplus \mathbf{1} \oplus \mathbf{1}$, then V decomposes as

$$V = T_6^2 \perp T_2^2 \perp \mathbf{1}^4,$$

where T_2 and T_6 are irreducible modules of dimension 2 and 6 over $\mathbb{F}_2$, both self-dual with an endomorphism ring isomorphic to $\mathbb{F}_4$. Hence the total number of self-dual codes in V equals

$$M_V = \Upsilon_o^-(4,2) \cdot \Upsilon_u(2,4)^2 = 3^3 = 27.$$

3.5. Example: Doubly-even binary codes

A doubly-even binary code of length n is a subspace $C \leqslant \mathbb{F}_2^n$ such that the weight $\mathrm{wt}(c)$ of every codeword $c \in C$, i.e. the number of its nonzero entries, is a multiple of 4. Self-dual doubly-even codes with respect to the standard scalar product $\varphi : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$ exist if and only if n is a multiple of 8 (see for instance [18]).

The permutation group of a code is $P(C) := \{\pi \in S_n \mid C\pi = C\}$, where S_n is the symmetric group on n points. In this subsection we view codes as modules over the group algebra $\mathbb{F}_2 G$, where $G \leqslant P(C)$ acts naturally by permuting the coordinates, and ask for the number of self-dual doubly-even codes with a certain subgroup $G \leqslant S_n$ contained in their automorphism group, i.e. for the self-dual codes in the $\mathbb{F}_2 G$-module $V := \mathbb{F}_2^n$.

We confine ourselves to the case where the order of G is odd, i.e. the group algebra $\mathbb{F}_2 G$ is semisimple, in order to apply the results of Section 2. Hence in what follows assume that the order of G is odd. Theorem 3.17 gives the number of G-invariant doubly-even self-dual codes, provided that there exists at least one such code. (By a result proven in [19], such a code exists if and only if n is a multiple of 8 and there exists any self-dual code in $\mathbb{F}_2^n$.)

The group algebra $\mathbb{F}_2 G$ carries an $\mathbb{F}_2$-linear involution given by $g \mapsto g^{-1}$, for $g \in G$, and the standard scalar product φ is equivariant with respect to this involution.

Clearly every self-dual code in V contains the all-ones vector $\mathrm{one} := (1, \ldots, 1) \in V$.The subspace $\langle \mathrm{one} \rangle^\perp \leqslant V$ consists exactly of the even-weight vectors in V. Moreover, every vector $v \in \langle \mathrm{one} \rangle^\perp$ satisfies

$$\mathrm{wt}(v + \mathrm{one}) = n - \mathrm{wt}(v) \equiv_4 \mathrm{wt}(v).$$

Hence the quotient $\widetilde{V} := \langle \mathrm{one} \rangle^\perp / \langle \mathrm{one} \rangle$ carries a well-defined quadratic form

$$q : \widetilde{V} \to \mathbb{F}_2, \qquad v + \mathrm{one} \mapsto \frac{\mathrm{wt}(v)}{2} \mod 2,$$

with polar form

$$(\widetilde{v}, \widetilde{v}') \mapsto q(\widetilde{v} + \widetilde{v}') - q(\widetilde{v}) - q(\widetilde{v}') = \widetilde{\varphi}(\widetilde{v}, \widetilde{v}'),$$

where $\widetilde{\varphi}$ is the non-degenerate equivariant bilinear form on $\widetilde{V}$ naturally induced by φ via

$$\widetilde{\varphi} : \widetilde{V} \times \widetilde{V} \to \mathbb{F}_2, \qquad \big(v + \langle \mathrm{one} \rangle, v' + \langle \mathrm{one} \rangle\big) \mapsto \varphi(v, v')$$

(cf. [20]). This yields a correspondence between the doubly-even self-dual codes in V and the maximal totally isotropic submodules of $\widetilde{V}$ – a self-dual code $C \leqslant V$ is doubly-even if and only if q vanishes on $C/\langle \mathrm{one} \rangle \leqslant \widetilde{V}$, i.e. $C/\langle \mathrm{one} \rangle$ is maximal totally isotropic. This correspondence was already established in [21] in the case where G acts trivially on V.

Again, let $\mathfrak{S}$ be a system of representatives for the isomorphism classes of simple right $\mathbb{F}_2 G$-modules. Consider the decomposition

$$\widetilde{V} = \perp_{S \in \mathfrak{S},\, S \cong S^*} \widetilde{V}_S \perp_{\{T, T^*\} \subseteq \mathfrak{S},\, T \ncong T^*} \widetilde{V}_{T \oplus T^*},$$

where $\widetilde{V}_X$ is the X-homogeneous component of $\widetilde{V}$, for $X \in \mathfrak{S}$, and $\widetilde{V}_{T\oplus T^*} = \widetilde{V}_T \oplus \widetilde{V}_{T^*}$. Then every maximal totally isotropic submodule $\widetilde{C} \leqslant \widetilde{V}$ is of the form

$$\widetilde{C} = \perp_{S\in\mathfrak{S},\, S\cong S^*} (C \cap \widetilde{V}_S) \perp_{\{T,T^*\}\subseteq\mathfrak{S},\, T\ncong T^*} (C \cap \widetilde{V}_{T\oplus T^*}), \qquad (*)$$

and every summand $C \cap \widetilde{V}_S$ or $C \cap \widetilde{V}_{T\oplus T^*}$ is a maximal totally isotropic submodule of $\widetilde{V}_S$ or $\widetilde{V}_{T\oplus T^*}$, respectively, since q is linear on $\widetilde{C}$.

Hence the total number of maximal totally isotropic submodules of $\widetilde{V}$ is the product of the number of maximal totally isotropic submodules in the summands of $(*)$.

Theorem 3.15. *Let $U \leqslant \widetilde{V}$ be a submodule such that the trivial module $\mathbf{1}$ does not occur in U. Then every self-dual code in U is doubly-even.*

Proof. Let $\widetilde{C} = \widetilde{C}^{\perp} \leqslant U$ be a self-dual code. Then q is linear on $\widetilde{C}$, i.e. $q \in \mathrm{Hom}_{\mathbb{F}_2 G}(\widetilde{C}, \mathbf{1})$ with kernel

$$\ker(q) = \{c \in \widetilde{C} \mid \mathrm{wt}(c) \equiv_4 0\} =: \widetilde{C}_0,$$

the doubly-even subcode of $\widetilde{C}$. The image of q is isomorphic to a factor module of $\widetilde{C}$. Since $\mathbf{1}$ does not occur in $\widetilde{C}$, this enforces that q vanishes on $\widetilde{C}$, i.e. $\widetilde{C} = \widetilde{C}_0$ is doubly-even. □

Now consider the quadratic space $(\widetilde{V}_{\mathbf{1}}, q_{\mathbf{1}}) \cong (\mathbb{F}_2^n, q_{\mathbf{1}})$, with non-degenerate polar form $\widetilde{\varphi}_{\mathbf{1}}$, the restriction of $\widetilde{\varphi}$ to $\widetilde{V}_{\mathbf{1}}$. Clearly V contains a doubly-even self-dual code if and only if $(\widetilde{V}_{\mathbf{1}}, q_{\mathbf{1}})$ has Witt index $\frac{n}{2}$. The total number of maximal totally isotropic subspaces is then well-known and given in [7], for instance.

Theorem 3.16. *(See Ex. 11.3 of [7].) Let $n := \dim(\widetilde{V}_{\mathbf{1}})$. If V contains a doubly-even self-dual code then the number of maximal totally isotropic subspaces of $(\widetilde{V}_{\mathbf{1}}, q_{\mathbf{1}})$ equals*

$$\varpi(n) := \prod_{i=0}^{\frac{n}{2}-1} \left(2^i + 1\right).$$

Theorems 3.15 and 3.16 now enable us to determine the number of doubly-even self-dual codes in V from the composition factors of V. Again, for a simple module $X \in \mathfrak{S}$, denote by n_X the multiplicity of X in V.

Theorem 3.17. *If (V, φ) contains a doubly-even self-dual code then the total number of doubly-even self-dual codes in V equals*

$$M^{\mathrm{II}}_{(V,\varphi)} = \varpi(n_{\mathbf{1}} - 2) \prod_{S\in\mathfrak{S},\, \mathbf{1}\ncong S\cong S^*} \Upsilon_u\left(n_S, q^{d_S}\right) \prod_{\{T,T^*\}\subseteq\mathfrak{S},\, T\ncong T^*} \Xi\left(n_T, q^{d_T}\right).$$

4. The mass formula

For a right A-module V carrying an equivariant form φ (cf. Definition 2.2), let

$$\mathcal{C}(V) := \left\{C \leqslant V \mid C = C^{\perp} = \left\{v \in V \mid \varphi(v, c) = 0 \text{ for all } c \in C\right\}\right\}.$$

One may be interested in an overview of the isometry types or weight distributions which occur here, rather than in the set $\mathcal{C}(V)$ itself. Hence in what follows, we define a finite group $\mathrm{Aut}(V)$ acting on $\mathcal{C}(V)$ such that properties like the isometry type of $C \in \mathcal{C}(V)$ or the weight distribution are left invariant under the operation of suitable subgroups of $\mathrm{Aut}(V)$.

4.1. Weak isometries of V and the mass formula

Definition 4.1. A bijective additive map $\psi : V \to V$ is called a weak isometry of V if $\varphi(v, v') = \varphi(\psi(v), \psi(v'))$ and $\psi(va) = \psi(v)a^\alpha$ for some automorphism α of A and all $v, v' \in V$. The weak isometries form a group $\mathrm{Aut}_{\mathrm{weak}}(V)$, with the composition as multiplication, which contains as a subgroup $\mathrm{Aut}(V) := \mathrm{End}_A(V) \cap \mathrm{Aut}_{\mathrm{weak}}(V)$, the isometries of V.

Clearly $\mathrm{Aut}_{\mathrm{weak}}(V)$ acts on $\mathcal{C}(V)$. Now consider the action of some subgroup $\Gamma \leqslant \mathrm{Aut}_{\mathrm{weak}}(V)$. By $[C]$ denote the orbit containing C. If

$$\Gamma(C) = \{\psi \in \Gamma \mid \psi(C) = C\}$$

is the stabilizer of C in Γ then $[C]$ has length $[\Gamma : \Gamma(C)]$ and we obtain

Theorem 4.2 *(Mass formula).*

$$\frac{M_V}{|\Gamma|} = \sum_{[C] \subseteq \mathcal{C}(V)} \frac{1}{|\Gamma(C)|}.$$

The mass formula gives a method of classifying the self-dual codes in V with respect to a property which is an invariant of the action of Γ on $\mathcal{C}(V)$ – one may restrict to orbit representatives and weight them by the reciprocal order of their automorphism group, until the value of the left-hand side of Theorem 4.2 has been reached. For instance, the group $\mathrm{Aut}(V)$ has the isometry type of $C \in \mathcal{C}(V)$ as an invariant and hence Eq. (4.2) can be used to classify the self-dual codes in V up to isometry.

4.2. Example: Permutation modules

Let $A = \mathbb{F}G$ be a semisimple group algebra over the finite group G and let V be a permutation module for G, i.e. $V = \mathbb{F}^k$ has a distinguished basis, with respect to which G acts as permutations and which we assume to be an orthonormal basis. The existence of a distinguished basis enables us to define the complete weight enumerator of a code $C \leqslant V$,

$$\mathrm{cwe}(C) = \sum_{(c_1,\ldots,c_k) \in C} \prod_{i=1}^{k} x_{c_i} \in \mathbb{C}[x_f : f \in \mathbb{F}].$$

The weight enumerator contains information on C which is of interest in coding theory, like the minimum weight of C. It is invariant under permutations of the coordinates of C, that is, $\mathrm{cwe}(C\pi) = \mathrm{cwe}(C)$ for all $C \in \mathcal{C}(V)$ and $\pi \in S_k$, where S_k is the symmetric group on k points. In general, the permutation equivalent code $C\pi$ is not contained in $\mathcal{C}(V)$, i.e. S_k does not act on $\mathcal{C}(V)$.

If V is faithful then the action of G on V induces an embedding $j : G \hookrightarrow S_k$. Let

$$\mathcal{N} := N_{S_k}(G) \leqslant \mathrm{Aut}_{\mathrm{weak}}(V)$$

be the normalizer of $j(G)$ in S_k. Every $\eta \in \mathcal{N}$ naturally induces a bijection $v \mapsto v\eta$ of V, which is a weak automorphism of V – if α_η is the $\mathbb{F}$-linear automorphism of $A = \mathbb{F}G$ given by $g \mapsto \alpha_\eta(g) = \eta^{-1}g\eta$ then $vg\eta = v\eta\eta^{-1}g\eta = v\eta\alpha_\eta(g)$ for all $v \in V$ and $g \in G$.

Hence $\mathcal{N}$ acts on $\mathcal{C}(V)$, yielding a mass formula

$$\frac{M_V}{|\mathcal{N}|} = \sum_{[C]_{\mathcal{N}} \subseteq \mathcal{C}(V)} \frac{1}{|\mathcal{N}(C)|}, \qquad (*)$$

where $[C]_{\mathcal{N}}$ is the orbit of $\mathcal{N}$ containing C and $\mathcal{N}(C)$ is the stabilizer of C under $\mathcal{N}$.

Table 1

i	$\lvert\mathcal{N}(C_i)\rvert$	$d(C)$	Number of words of weight 24
1	92	2	3754060
2	92	2	3765560
3	92	2	3749000
4	92	2	3759120
5	2024	2	2704156
6	23276	2	3829960
7	23276	2	3829960
8	1012	4	11092764
9	46	8	7691340
10	46	8	7691340
11	46	8	7701000
12	11638	8	7787940
13	11638	8	7787940
14	46	12	7681680

Clearly the complete weight enumerator is an invariant of this operation. Another invariant is the conjugacy class of $P(C)$ in S_k, where $P(C) = \{\sigma \in S_k \mid C\sigma = C\} \leqslant S_k$ is the permutation group of $C \in \mathcal{C}(V)$, since $P(C\eta) = \eta^{-1}P(C)\eta$ for every $\eta \in \mathcal{N}$.

In general there is no larger subgroup $\mathcal{U}$ with $\mathcal{N} \subsetneq \mathcal{U} \subseteq S_k$ such that $\mathcal{U}$ acts on $\mathcal{C}(V)$, since $\mathcal{N}$ normalizes the Bravais group $\mathcal{B}(V) := \bigcap_{C\in\mathcal{C}(V)} P(C)$, cf. Theorem 4.3.

Theorem 4.3. *If $\mathcal{B}(V) = G$ then $\mathcal{N}$ is the largest subgroup of S_k which acts on $\mathcal{C}(V)$.*

Proof. Let $\pi \in S_k$ such that π acts on $\mathcal{C}(V)$. Then $\pi \in \mathcal{N}$ since

$$G = \mathcal{B}(V) = \bigcap_{C\in\mathcal{C}(V)} P(C\pi) = \pi^{-1}\Bigg(\bigcap_{C\in\mathcal{C}(V)} P(C)\Bigg)\pi = \pi^{-1}\mathcal{B}(V)\pi = \pi^{-1}G\pi. \qquad \square$$

Example 4.4. *Self-dual binary codes of length* 48 *with an automorphism of order* 23. The extended quadratic residue code $q_{48} \leqslant \mathbb{F}_2^{48}$ is, up to permutation equivalence, the only self-dual $[48, 24, 12]$-code, i.e. the only extremal binary self-dual code of length 48, cf. for instance [22]. The code q_{48} has an automorphism $\sigma \in S_{48}$ of order 23 which acts on the coordinates of q_{48} with four orbits. Hence q_{48} is a submodule of

$$V = \mathbb{F}_2C_{23} \oplus \mathbb{F}_2C_{23} \oplus \mathbf{1} \oplus \mathbf{1}$$

over the semisimple algebra $A = \mathbb{F}_2C_{23}$. The algebra A has three irreducible modules, which are the trivial module $\mathbf{1}$, a module T of dimension 11 and its dual $T^* \ncong T$ with an endomorphism ring of dimension $d_T = 11$. Hence V has a decomposition $V = \mathbf{1}^4 \perp (T \oplus T^*)^2$ and the total number of self-dual codes in V equals

$$M_V = \Upsilon_o^-(4, 2)\Xi\left(2, 2^{11}\right) = 3 \cdot \left(2^{11} + 3\right) = 6153.$$

Considering normalizer equivalence, i.e. the orbits of $N_{S_{48}}(\sigma)$ on the set $\mathcal{C}(V)$ of all self-dual codes in V, there are only 14 equivalence classes of codes. Representatives $C_1, \ldots, C_{14}$ for these classes can easily be computed in MAGMA [23] using the mass formula $(*)$, which then is

$$\frac{6153}{46552} = 4 \cdot \frac{1}{92} + \frac{1}{2024} + 2 \cdot \frac{1}{23276} + \frac{1}{1012} + 4 \cdot \frac{1}{46} + 2 \cdot \frac{1}{11638}.$$

Table 1 lists the stabilizer orders $\mathcal{N}(C_i)$ of the codes $C_1, \ldots, C_{14}$ and gives the number of words of weight 24 in each code, which is helpful to distinguish codes which are not permutation equivalent.

Explicit calculation in MAGMA shows that the codes C_6 and C_7 are permutation equivalent, and the codes C_{12} and C_{13} are permutation equivalent but C_9 and C_{10} are not. Hence there are, up to permutation equivalence, 12 self-dual codes in V.

References

[1] S. Berman, On the theory of group codes, Cybernetics 3 (1969) 25–31.
[2] G. Hughes, Structure theorems for group ring codes with an application to self-dual codes, Des. Codes Cryptogr. 24 (2001) 5–14.
[3] F. MacWilliams, N. Sloane, J. Thompson, Good self dual codes exist, Discrete Math. 3 (1972) 153–162.
[4] C. Martínez-Pérez, W. Willems, Self-dual extended cyclic codes, Appl. Algebra Engrg. Comm. Comput. 1 (2006) 1–16.
[5] W. Willems, A note on self-dual group codes, IEEE Trans. Inform. Theory 48 (2002) 3107–3109.
[6] W. Willems, A. Zimmermann, On Morita theory for self-dual modules, Q. J. Math. (Oxford) (2008) 1–14.
[7] D. Taylor, The Geometry of the Classical Groups, Sigma Ser. Pure Math., vol. 9, Heldermann-Verlag, Berlin, 1992.
[8] M. Kneser, Quadratische Formen, Springer, 2001.
[9] A. Fröhlich, A. McEvett, Forms over rings with involution, J. Algebra 12 (1969) 79–104.
[10] C.M. Hernandez, M.R. Sanchez, Relative hermitian Morita theory. I. Morita equivalences of algebras with involution, J. Algebra 162 (1993) 146–167.
[11] M. Knus, A. Merkurjev, M. Rost, J. Tignol, The Book of Involutions, Amer. Math. Soc. Colloq. Publ., vol. 44, Amer. Math. Soc., Providence, RI, 1998.
[12] G. Nebe, On the cokernel of the Witt decomposition map, J. Theor. Nombres Bordeaux 12 (2000) 489–501.
[13] C. Curtis, I. Reiner, Methods of Representation Theory, vol. 1, Wiley Classics Lib., 1981.
[14] A. Günther, Automorphisms of self-dual codes, PhD thesis, RWTH Aachen University, in preparation.
[15] T. Okuyama, Y. Tsushima, On a conjecture of P. Landrock, J. Algebra 104 (1986) 203–208.
[16] W. Scharlau, Quadratic and Hermitian Forms, Grundlehren Math. Wiss., vol. 270, Springer, 1985.
[17] C. Martínez-Pérez, W. Willems, Self-dual codes and modules for finite groups in characteristic two, IEEE Trans. Inform. Theory 50 (2004) 1798–1903.
[18] F. MacWilliams, N. Sloane, The Theory of Error-Correcting Codes, North-Holland Math. Library, vol. 16, North-Holland Publishing Co, 1977.
[19] A. Günther, G. Nebe, Automorphisms of doubly-even self-dual binary codes, LMS Bulletin, in press.
[20] E. Rains, N. Sloane, Self-dual codes, in: V. Pless, W. Huffman (Eds.), Handbook of Coding Theory, North-Holland, Amsterdam, 1998, pp. 177–294.
[21] A. Munemasa, A mass formula for Type II codes over finite fields of characteristic two, in: Codes and Designs, Columbus, OH, 2000, Ohio State Univ. Math. Res. Inst. Publ. 10 (2002) 207–214.
[22] E. Rains, Shadow bounds for self-dual codes, IEEE Trans. Inform. Theory 44 (1998) 134–139.
[23] W. Bosma, J. Cannon, C. Playoust, The magma algebra system. I. The user language, J. Symbolic Comput. 24 (1997) 235–265.