Self-dual codes and modules for finite groups in characteristic two

Conchita Martínez-Pérez*
Departamento de Matemáticas
Universidad de Zaragoza,
50009 Zaragoza

Wolfgang Willems
Institut für Algebra und Geometrie
Fakultät für Mathematik
Otto-von-Guericke-Universität
39016 Magdeburg

Abstract- **Using representation theoretical methods we investigate self-dual group codes and their extensions in characteristic 2. We prove that the existence of a self-dual extended group code heavily depends on the structure of the group algebra KG. The structure needed can be translated to an easy to handle criteria in elementary number theory. Surprisingly, in the binary case such a code is doubly even if the converse of Gleason's theorem holds true, i.e., the length of the code is divisible by 8. Furthermore we give a short representation theoretical proof of an earlier result of Sloane and Thompson which states that a binary self-dual group code is never doubly even provided the Sylow 2-subgroups of G are cyclic. It turns out that exactly in the case of a cyclic or Klein four group as Sylow 2-subgroup doubly even group codes do not exist.**

Index Terms- **self-dual modules, splitting fields, self-dual group codes, extended codes**

*Most of this work was carried out while the author was visiting the Otto-von-Guericke University of Magdeburg in August 2002. She was supported by the Department of Mathematics and by BFM2001-1667-C03-01.

1 Introduction

Representation theory of finite groups has not been used much in the past when solving problems in coding theory. On the one hand one may say "Well, but note that most codes do not have a non-trivial automorphism group, so no group acts on in a natural way." On the other hand many interesting codes, specially those which play a role in practise, allow such a group action. In this case representation theory naturally comes in and their methods turn out to be very powerful, in particular if one deals with duality questions. According to this property there are two functors, one mapping $C \to C^\perp$ where $C^\perp$ denotes the usual dual of the code C, the other mapping $C \to C^*$ where $C^* = \mathrm{Hom}(V, K)$ denotes the dual G-module. Exploiting the interaction of these two duality functors, in particular the KG-isomorphism $K^n/C^\perp \cong C^*$, we are led to new and interesting facts about self-dual group or extended group codes. For instance, in characteristic 2 we shall prove that an extended self-dual group code exists if and only if the primes dividing the group order satisfy some number theoretical conditions which can be checked easily. Moreover in the binary case such a code turns out to be doubly even if and only if the length of the code is divisible by 8. This is remarkable since it proves the converse of Gleason's theorem in case of extended group codes. For group codes we shall give a short proof of a result of Sloane and Thompson, namely that a self-dual group code is never doubly even if the Sylow 2-subgroups are cyclic. Apart from this case and a Klein four group as Sylow 2-subgroups self-dual doubly even codes always exist.

Throughout the paper all modules are assumed to be of finite dimension over the underlying finite field K. For facts in group and representation theory we refer to [1] or chapter VII in [6], and for coding theory to [9].

2 Preliminaries

In this section we collect some more or less known facts about modules over group algebras which we freely use in the sequel. By K and F we always denote fields and by G a finite group. Note that the dual $V^* = \mathrm{Hom}_K(V, K)$ of a KG-module V carries a G-structure which is given by

$$v(fg) = (vg^{-1})f \text{ for } v \in V,\ f \in V^*,\ g \in G.$$

Lemma 2.1 *Let $W = e \oplus_{i=1}^n V_i$ be a KG-module with irreducible pairwise non-isomorphic KG-modules V_i. Then, for n odd, $W \cong W^*$ implies $V_i \cong V_i^*$ for some i.*

Proof: By the Krull-Schmidt Theorem, the assumption $W \cong W^*$ implies $\{V_1, \ldots, V_n\} = \{V_1^*, \ldots, V_n^*\}$ up to isomorphisms. Now, if $V_i \not\cong V_i^*$ for all i then n must be even.

Lemma 2.2 *Let F/K be a finite Galois extension with Galois group Γ. If W is an irreducible KG-module, then*

a) $W \otimes_K F \cong e \oplus_{\alpha \in U} V^\alpha$ with $e \in \mathbb{N}$, $U \leq \Gamma$ and V an irreducible FG-module. Furthermore, if $\operatorname{char} K > 0$ then $e = 1$.

b) $W \cong W^*$ if and only if $W \otimes_K F \cong (W \otimes_K F)^*$, and this happens if and only if $V^* \cong V^\alpha$ for some $\alpha \in U$. Moreover, if $|U|$ is odd then $W \cong W^*$ if and only if $V \cong V^*$. In particular, if $[F/K]$ is odd then there is a non-trivial irreducible self-dual G-module over F if and only if there is one over K.

c) If $[F/K]$ is odd and $\operatorname{char} K > 0$ then there is an irreducible FG-module of even dimension if and only if there is one for KG.

Proof: a) This is 1.18 and 1.15 in ([6], Chap. VII).
b) The first equivalence follows by Deuring-Noether's Theorem (see [6], Chap. VII, 1.22) as $W^* \otimes_K F \cong (W \otimes_K F)^*$. For the second assertion, note that $V^* \cong V^\alpha$ implies $V^\beta = (V^*)^{\alpha^{-1}})^\beta = (V^{\alpha^{-1}\beta})^*$ for all $\beta \in U$, hence $W \otimes_K F \cong (W \otimes_K F)^*$. On the other hand if $W \otimes_K F \cong (W \otimes_K F)^*$ then $V^* \cong V^\alpha$ by the Krull-Schmidt Theorem. Now, assume that $|U|$ is odd. If $W \cong W^*$ then $W \otimes_K F \cong (W \otimes_K F)^*$ and by Lemma 2.1, $(V^\alpha)^* \cong V^\alpha$ for some $\alpha \in U$. Thus we get

$$V^* \cong ((V^\alpha)^*)^{\alpha^{-1}} \cong (V^\alpha)^{\alpha^{-1}} \cong V.$$

The converse holds true since $V \cong V^*$ implies $V^\alpha \cong (V^\alpha)^*$ for all α.
c) By assumption, $\operatorname{char} K > 0$ and therefore $e = 1$ in a). Since $\dim_K W = |U| \dim_F V$ the assertion follows.

In the sequel we need several times Brauer's permutation Lemma which can be found in most books on representation theory. The way we use it here was proved in [7]. In order to state it we need the following notations. Let $\beta_1, \ldots, \beta_k$ denote the set of irreducible Brauer characters of G over an algebraically closed field of characteristic $p > 0$. By a result of Brauer, k is also the number of p-regular conjugacy classes of G (see [5], VII, 3.9). Let $g_1, \ldots, g_k$ denote representatives of these classes. Suppose there is a group, say H, which acts on the one hand on the set of irreducible Brauer characters of G by $\beta_i \to \beta_i^h$ and on the other hand on the set of p-regular classes of G by $g_i^G \to (g_i^G)^h$ for $h \in H$.

Lemma 2.3 (**Brauer's permutation Lemma)** *If the two permutation actions of H satisfy*

$$\beta_i^h(g_j) = \beta_i(g_j^h)$$

for all i, j and all $h \in H$ then we have:
For any $h \in H$ the number of cycles of a fixed length on $\{\beta_1, \ldots, \beta_k\}$ and $\{g_1, \ldots, g_k\}$ is the same. In particular, the number of fixed points of h on the set of irreducible Brauer characters is equal to the number of fixed points on the set of p-regular classes.

In applications the action of H is very often a Galois action. In order to describe this action we fix a finite field F of characteristic p. Let K be a subfield of F and let $\Gamma = \mathrm{Gal}(F/K)$. If $|K| = p^a = q$ and $|F| = q^b$ then each $\alpha \in \Gamma$ corresponds to a unique l with $1 \leq l \leq b$ such that

$$\alpha : f \longrightarrow f^{q^l}$$

for $f \in F$. (Remember that α is a power of the Frobenius map.) Now we define the action of Γ on G by

$$\alpha : g \longrightarrow g^{q^l}.$$

Let $g, h \in G$ be p-regular elements and suppose that $g^\alpha = (h^\alpha)^x$ for some $x \in G$. Then we obtain

$$g^{q^l} = g^\alpha = (h^\alpha)^x = (h^{q^l})^x = (h^x)^{q^l}.$$

Since g and h are p-regular we have

$$\langle g \rangle = \langle g^{q^l} \rangle = \langle (h^x)^{q^l} \rangle = \langle h^x \rangle.$$

Thus g and h^x commute and we get

$$(g^{-1}h^x)^{q^l} = 1,$$

hence $g = h^x$. This shows that the action of Γ on the p-regular conjugacy classes of G is injective, hence a permutation. Now suppose that F is a splitting field for G. If $\mathrm{IBr}_p(G) = \{\beta_1, \ldots, \beta_k\}$ is the set of irreducible Brauer characters in characteristic p and $\{g_1, \ldots, g_k\}$ a set of representatives for the p-regular conjugacy classes of G then

$$\beta_i^\alpha(g_j) = \beta_i(g_j)^\alpha = \beta_i(g_j)^{q^l} = \beta_i(g_j^{q^l}) = \beta_i(g_j^\alpha)$$

for all i, j and all $\alpha \in \Gamma$. Thus Brauer's permutation Lemma applies.

Notations 2.4 For any prime t and any positive integer n with $t \nmid n$ let $s_t(n)$ denote the smallest positive integer such that

$$n \mid t^{s_t(n)} - 1.$$

Obviously, $t^{s_t(n)}$ is the size of a minimal field of characteristic t containing a primitive n-th root of unity and $s_t(n)$ is the order of t in the group $\mathbb{Z}_n^*$ of units in $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Thus $s_t(n) \mid \phi(n)$ where ϕ denotes the Euler function. In particular, if p is a prime then $s_t(p) \mid p-1$. Moreover, if m is any positive integer, then $n \mid t^m - 1$ if and only if $s_t(n) \mid m$. Furthermore, for a finite group G we put

$$s_t(G) = \operatorname{lcm}\{s_t(p) \mid \ p \mid |G|,\ p \text{ a prime and } p \neq t\}.$$

Finally, for $s, n \in \mathbb{N}$ we may factorize s into $s = s_n s_{n'}$ where $\gcd(s_{n'}, n) = 1$ and s_n contains only primes which divide n. The factor s_n is called the n-part of s.

Remark 2.5 For a finite group G let K_G denote the finite field of size t^k where

$$k = \operatorname{lcm}\{s_t(p^a) \mid \ p^a \mid |G|,\ p \text{ a prime},\ a \in \mathbb{N} \text{ and } p \neq t\}.$$

For $g \in G$ let $\operatorname{ord}(g)$ denote the order of g and $\operatorname{ord}_n(g)$ its n-part ($n \in \mathbb{N}$). Thus for any prime $p \neq t$ we have

$$\operatorname{ord}_p(g) \mid t^{s_t(\operatorname{ord}_p(g))} - 1 \mid t^k - 1.$$

In particular, $\operatorname{ord}_{t'}(g) \mid t^k - 1$. Thus, by ([6], Chap VII, 2.6), the field K_G is a splitting field of characteristic t for G and all its subgroups.

Lemma 2.6 *For a prime $p \neq t$ and $a \in \mathbb{N}$ we have*

$$s_t(p^a) = p^j s_t(p) \quad \textit{for some} \quad j \in \{0, 1, \ldots, a-1\}.$$

Proof: We proceed by induction on a. The case $a = 1$ is trivial. So we may assume $a > 1$ and $s_t(p^{a-1}) = p^j s_t(p)$ for some j with $0 \leq j \leq a-2$. Let F resp. K be minimal fields of characteristic t containing a primitive p^a-th root of unity, say β, resp. a primitive p^{a-1}-th root of unity, say α. We may assume that $K \subseteq F$ and $\beta^p = \alpha$. By minimality of F, we have $F = K[\beta]$. If $\beta \notin K$ then $x^p - \alpha \in K[x]$ is irreducible and therefore $\dim_K F = |F : K| = p$. Otherwise we have $F = K$. As $|K| = t^{s_t(p^{a-1})}$ we obtain $t^{p s_t(p^{a-1})} = |K|^p = |F| = t^{s_t(p^a)}$ in the first case, and $s_t(p^{a-1}) = s_t(p^a)$ in the second. Thus the claim follows.

Corollary 2.7

a) $s_t(p^a)_q = s_t(p)_q$ *for all primes* $q \neq p$.

b) $(\log_t |K_G|)_q = s_t(G)_q$ *if* q *is a prime and* $q \nmid |G|$.

Proof: Assertion a) follows immediately by 2.6. To get b) we have to look only at $s_t(p)$ for primes p with $p \mid |G|$ and $p \nmid t$. By assumption, such primes p satisfy $p \neq q$ and the assertion follows by part a).

Theorem 2.8 *Let* G *be a finite group and let* F *be a minimal splitting field for* G *in characteristic* t. *If* $|F| = t^s$ *then for any prime* q *with* $q \nmid |G|$ *we have*

$$s_q = s_t(G)_q.$$

Proof: We fix a prime q with $q \nmid |G|$. Note that K_G is a splitting field for G, by 2.5. As F is a minimal splitting field we get $F \subseteq K_G$. Now, if $k_t(G) = \log_t |K_G|$ then $s_q \mid k_t(G)_q = s_t(G)_q$, by 2.7.

To prove $s_t(G)_q \mid s_q$ we put $q^a = s_t(G)_q$. Note that

$$q^a = s_t(G)_q = \operatorname{lcm}\{s_t(p)_q \mid \ p \mid |G|,\ p \text{ a prime and } p \neq t\}.$$

Clearly, we may assume that $a > 0$. Thus there exists a prime $p \neq t$ for which $s_t(p)_q = q^a$ and an element $x \in G$ of order p. Assume by contradiction that $s_q < s_t(G)_q$. Then there exists a field K with $F \subseteq K \subseteq K_G$ and $|K_G : K| = q$. Since K is a splitting field for G the group $\Gamma = \mathrm{Gal}(K_G/K)$ acts trivially on the set of t-regular conjugacy classes of G by Brauer's permutation lemma. Thus, if $\Gamma = \langle \alpha \rangle$ then

$$x^g = x^\alpha = x^{t^{k_t(G)/q}}$$

for x t-regular and $g \in G$. Note that $g \in N_G(\langle x \rangle)$ and therefore $x = x^{g^q}$ as α is of order q. This implies $g^q \in C_G(\langle x \rangle)$, hence $g \in C_G(\langle x \rangle)$. Thus we have $x = x^{t^{k_t(G)/q}}$. Since x is of order p we get $p \mid t^{k_t(G)/q} - 1$ and therefore $s_t(p) \mid k_t(G)/q$. Thus $s_t(G)_q < k_t(G)_q$ a contradiction to 2.7 and the proof is complete.

3 Extended group codes

By a group code we denote an ideal in the group algebra KG where G is a finite group. An extended group code is a KG-submodule of $K \oplus KG$ where

G acts trivially on the additional component K. In coding theory one often deals with this special kind of codes. Note that a binary self-dual extended group code is an extended code in the classical sense.

In what follows the underlying field is always assumed to be finite and of characteristic 2. Furthermore, to be brief, we put $s(G) = s_2(G)$. To prove one of the main results we need

Proposition 3.1 *Let $G = C_n$ be a cyclic group of odd order n. If $(\log_2 |K|)_2 < s(G)_2$ then there exists an irreducible KG-module V with $K \not\cong V \cong V^*$.*

Proof: Let F be a field of size $2^{s(n)}$. Note that F is a minimal splitting field for G and thus, by 2.8, we have $s(n)_2 = s(G)_2$. Furthermore, by assumption,

$$1 \leq (\log_2 |K|)_2 < s(G)_2 = s(n)_2.$$

Thus $s(n)$ is even and there exists a subfield, say L, of F with $|F : L| = 2$. Let $\mathrm{Gal}(F/L) = < \alpha >$. Since

$$n \mid 2^{s(n)} - 1 = (2^{s(n)/2} - 1)(2^{s(n)/2} + 1)$$

we may write $n = ab$ with $a \mid 2^{s(n)/2} - 1$ and $b \mid 2^{s(n)/2} + 1$. Clearly, $b \neq 1$, by definition of $s(n)$. If ξ is a primitive n-th root of unity in F then the irreducible FG-modules are given by ξ^i for $i = 1, \ldots, n$. Note that

$$(\xi^a)^\alpha = \xi^{a 2^{s(n)/2}} = \xi^{-a}$$

since $n \mid a(2^{s(n)/2} + 1)$. Thus $W^\alpha \cong W^*$ if W denotes the module corresponding to ξ^a. Furthermore, $n \nmid a$ as $b \neq 1$. Hence $W \not\cong F$ and the assertion of the Proposition follows by 2.2.

Lemma 3.2 *Let G be a group of odd order. If the trivial module is the only self-dual irreducible KG-module then there exists a central idempotent $e \in KG$ such that $C = eKG \leq C^\perp$ is an orthogonal group code and $C^\perp = C \oplus e_0 K$.*

Proof: By Maschke's Theorem (see [1], p. 116) we have

$$KG = e_0 K \oplus (W_1 \oplus \ldots \oplus W_t) \oplus (W_1^* \oplus \ldots \oplus W_t^*)$$

with non-trivial irreducible KG-modules W_i and $e_0 = \sum_{g \in G} g$. This leads to a decomposition $1 = e_0 + e + e^*$ with centrally orthogonal idempotents e_0, e, e^* and $eKG = W_1 \oplus \ldots \oplus W_t$, resp. $e^* KG = W_1^* \oplus \ldots \oplus W_t^*$. By a result of Okuyama and Tsushima [10], we have $e^*KG \cong (eKG)^* \cong \bar{e}KG$ where $^-$ denotes the algebra antiautomorphism of KG defined by $\overline{g} \mapsto g^{-1}$ for $g \in G$. Thus, by ([8], 3.12), e^* and $\bar{e}$ are conjugate in the unit group of KG. Since the idempotents are central we obtain $e^* = \bar{e}$.

Now we put $C = eKG$. Then

$$(eKG, eKG) = (1, KG\overline{e}eKG) = (1, 0) = 0$$

as $e\overline{e} = ee^* = 0$. Thus $C \subseteq C^\perp$. Since $e_0K \subseteq C^\perp$ we obtain $\dim C^\perp = C \oplus e_0K$.

The next result completely characterizes all situations in which self-dual extended group codes exist. Note that in marked contrast self-dual group codes exist if and only if the characteristic of the underlying field is 2 (which is always assumed in this section) and $2 \mid |G|$.

Theorem 3.3 *If G is a group of odd order then the following conditions are equivalent.*

a) $s(G)_2 \leq (\log_2 |K|)_2$.

b) All irreducible KG-modules are of odd dimension.

c) The trivial module is the only self-dual irreducible KG-module.

d) For any odd positive integer l there exist a G-invariant self-dual code in $K \oplus KG \oplus KG \oplus \ldots \oplus KG$ with l copies of KG.

e) There exists a self-dual extended group code for G.

Proof: a) $\Rightarrow$ *b)* Note that $F = KK_G$ is a splitting field for G by 2.5, and $|F : K|$ is odd by assumption. Since $|G|$ is odd all irreducible FG-modules are of odd dimension. Thus, by 2.2, all irreducible KG-modules are of odd dimension as well.

b) $\Rightarrow$ c) This is Fong's lemma (see [6], VII, 8.13).

c) $\Rightarrow$ d) Let e_0, e be central idempotents in KG as in 3.2. Let $e_0(i)$ resp. $e(i)$ denote the idempotents corresponding to e_0 resp. e of the i-th copy of KG in $KG \oplus \ldots \oplus KG$. Now, it is easy to check that

$$(1_K + e_0(1))K + (e_0(2) + e_0(3))K + \ldots + (e_0(l-1) + e_0(l))K + \bigoplus_{j=1}^{l} e(j)KG$$

is a G-invariant self-dual code in $K \oplus KG \oplus KG \oplus \ldots \oplus KG$.
d) $\Rightarrow$ e) This is trivial.
e) $\Rightarrow$ c) Let C be a self-dual group code in $V = K \oplus KG$. Since $V/C = V/C^{\perp} \cong C^*$ as KG-modules each non-trivial self-dual irreducible KG-module has even multiplicity in KG. On the other hand, if $|K|$ is large enough this multiplicity must be odd as $|G|$ is odd. But note that the multiplicities do not change if we restrict the size of the field (see 2.2). Thus all non-trivial irreducible KG-modules are not self-dual.
c) $\Rightarrow$ a) Now suppose that $s(G)_2 > (\log_2 |K|)_2$. We shall prove that a non-trivial self-dual KG-module exists which is a contradiction to the above statement. By definition we have

$$s(G)_2 = \max \{ s(p)_2 \mid p \text{ a prime, } p \mid |G| \} = s(p)_2$$

for a suitable prime p dividing $|G|$. In particular, there exists an element $x \in G$ of order p such that $k_2 < s(p)_2 = s(\langle x \rangle)_2$ where $k = \log_2 |K|$. Thus, by 3.1, there is an irreducible $K\langle x \rangle$-module, say V, with $K \ncong V \cong V^*$. By Brauer's permutation lemma, we get $x^{-1} = x^{\alpha}$ with $\alpha \in \mathrm{Gal}(KK_G/K)$ where K_G is the field defined in 2.5 and $x \neq 1$. Applying Brauer's permutation lemma again we obtain a non-trivial irreducible self-dual $(KK_G)G$-module, hence, by 2.2 b), a non-trivial irreducible self-dual KG-module.

We would like to mention here that a non-trivial irreducible KG-module always has even dimension by Fong's lemma. But the convers fails to be true in general.

Example 3.4 Let $G = C_{21} = C_7 \times C_3$ where C_n is a cyclic group of order n and let K be a field with 8 elements. Note that K is not a splitting field for G. A minimal splitting field has 64 elements. One easily checks that KG has 14 irreducible modules where 7 of them are of dimension 1 and the other 7 of dimension 2, but only one of the 2-dimensional modules is self-dual.

In order to prove the existence of a self-dual extended group code the theorem above provides different criteria. Both part b), and c) as well are of representation theoretical nature and in general difficult to check. However part a) is easy to handle, in particular if $|K| = 2$. In this case $s(G)$ must be odd. This affords only the computation of $s(p)$ for odd primes $p \mid |G|$ with $p \equiv 1 \bmod 8$ as the next lemma shows

Lemma 3.5 *Let p be an odd prime.*

a) If $p \equiv -1 \bmod 8$ then $s_2(p)$ is odd.

b) If $p \equiv \pm 3 \bmod 8$ then $s_2(p)$ is even.

Proof: a) If $p \equiv -1 \bmod 8$ then 2 is a square in $\mathbb{Z}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$ (see for instance 2.4.4 in [12]) and $\frac{p-1}{2}$ is odd. Thus there exists an integer x with $x^2 = 2 \bmod p$ and we get $1 = (x^2)^{\frac{p-1}{2}} = 2^{\frac{p-1}{2}}$.
b) If $p \equiv \pm 3 \bmod 8$ then 2 is not a square mod p (see again 2.4.4 in [12]). In particular $s_2(p)$ must be even.

Let n be a positive integer and $l \mid n$. A l-quasicyclic code of length n over the field K is a K-subspace of K^n which is invariant under l cyclic shifts. For brevity, such codes are called l-qc codes. Obviously, the 1-qc codes are the cyclic codes.

Let G be a cyclic group of order $e = \frac{n}{l}$. An l-qc code C of lenth n can be seen as a G-invariant subspace of $KG \oplus \ldots \oplus KG$ with l copies of KG. Thus for n odd theorem 3.3 completely characterizes the situations in which self-dual extended l-qc codes exist. More precisely we have

Corollary 3.6 *Let l be a positive integer with $l \mid n = 2m-1$ ($m \in \mathbb{N}$). Then there exist a self-dual extended l-qc code of length $2m$ over K if and only if*

$$\log_2(|K|)_2 \geq \max\{s(p)_2 \mid \ p \textit{ a prime}, \ p \mid \frac{n}{l}\}.$$

By a well-known result of Gleason (see for instance [12], 6.3.8), a binary self-dual doubly even weight code has a length which is divisible by 8. For extended group codes the converse holds true, i.e.,

Theorem 3.7 *All binary self-dual extended group codes which have a length divisible by 8 are doubly even.*

Proof: Let $|K| = 2$ and let $C = C^\perp \leq K \oplus KG$ be a self-dual extended group code of length $n = 1 + |G|$. According to 3.3 the trivial module is the only self-dual irreducible KG-module. By the proof of 3.2 the module $C = C^\perp$ contains a component of the form eKG with e a central idempotent in KG and $\dim eKG = \frac{|G|-1}{2}$. As $K \oplus KG/C \cong C^*$ there is also a 1-dimensional subspace of $K \oplus e_0K$ contained in C. Since, up to scalars, $v = 1_K + e_0$ is the only non-trivial isotropic vector in $K \oplus e_0K$ we have $C = vK + eKG$. Clearly, $8 \mid n = \mathrm{wt}(v)$. The equation $1 = e_0 + e + \bar{e}$ implies that $\mathrm{supp}(e) \cap \mathrm{supp}(\bar{e}) \subseteq \{1\}$ and $G \setminus \{1\} \subseteq \mathrm{supp}(e) \cup \mathrm{supp}(\bar{e})$. If $1 \notin \mathrm{supp}(e)$ then $\mathrm{wt}(e) = \frac{|G|-1}{2}$ is odd, a contradiction to the fact that e is an isotropic vector. Thus we obtain

$$\mathrm{wt}(e) = 1 + \frac{|G|-1}{2} = \frac{|G|+1}{2}$$

which is divisible by 4. In particular eKG has a basis of vectors whose weights are all divisible by 4, and the same holds true for C. This implies that $C = vK + eKG$ is doubly even (see [12], 3.1.7).

Examples 3.8 a) Let C be a binary extended group code of length $p+1$ where p is an odd prime. If $C = C^{\perp}$ then by 3.3 and 3.5, we obtain $p \equiv -1 \bmod 8$ or $p \equiv 1 \bmod 8$ and $s(p)$ odd. According to 3.7 the code C is doubly even in the first case, but not in the latter.
b) Suppose that $m \in \mathbb{N}$ is odd. Then for all primes p with $p \mid n = 2^m - 1$ we get $s(p)$ odd as $s(p) \mid m$. Thus, by 3.3, there exists a binary self-dual extended cyclic code of length 2^m, and by 3.7, such a code is doubly even if $m \geq 3$.
Now let $m \in \mathbb{N}$ be even. Then $3 \mid n = 2^m - 1$ and $s(3)_2 = 2$. Thus, by 3.3, there is no binary extended cyclic self-dual code of length 2^m. This is also Corollary 1 of [3].
If we specialize $m = 6$ then for $l = 9$

$$1 = (\log_2 |K|)_2 = \max\{s(p)_2 \mid \ p \text{ a prime}, \ p \mid \frac{63}{9} = 7\}$$

and by 3.6 there exists a binary self-dual 9-qc code of length 64.

4 Group codes

Self-dual group codes exist if and only if the underlying field is of characteristic 2 and the group has even order. This is an easy consequence of Maschke's theorem as shown in [13]. Thus we may again assume in this section that the underlying field has order a power of 2.

Example 4.1 Let $G = \langle g \rangle$ be of order 2^m for $m \geq 1$. If $J = \langle x - 1 \mid x \in G \rangle$ denotes the Jacobson radical of KG then the powers J^i $(i = 0, \ldots, m-1)$ are all the ideals in KG. Note that there is only one self-dual ideal, namely $C = J^{2^{m-1}}$. Since

$$0 \neq g^{2^{m-1}} - 1 = (g-1)^{2^{m-1}} \in J^{2^{m-1}} = C$$

we see that C is not doubly even.

In [11] Sloane and Thompson proved that a binary self-dual group code is never doubly even provided a Sylow 2-subgroup of the group is cyclic. We give here a short representation theoretical proof which also shows that codewords of weight $2 \bmod 4$ are contained in eC where e is the central idempotent generating the principal 2-block of KG.

Theorem 4.2 (Sloane, Thompson, [11]) *Let G be a finite group which has a cyclic Sylow 2-subgroup. If $C = C^\perp$ is self-dual group code in KG then C contains a codeword of weight $2 \bmod 4$.*

Proof: Let $T = \langle t \rangle$ be a Sylow 2-subgroup of G with $|T| = 2^m$. Since T is cyclic there exists a normal subgroup $H \trianglelefteq G$ of odd order such that $G/H \cong T$ (see [5], Kap. IV, 2.8). If we put $e = \frac{1}{|H|}\sum_{h\in H} h$ then $eKG = eKT$ is the principal 2-block of $KG = eKG \oplus (1-e)KG$. Since $\bar{e}(1-e) = e(1-e) = 0$ we even have $KG = eKG \perp (1-e)KG$. Furthermore, $C^\perp = C = eC \perp (1-e)C$ where eC is a self-dual ideal in $eKG = eKT$. Let J denote the Jacobson radical of KT. Since $eKT \cong KT$ as KT-modules we get $eC = eJ^{2^{m-1}}$. Finally the weight of

$$c = e(1-t)^{2^{m-1}} = e(1-t^{2^{m-1}}) \in eJ^{2^{m-1}} = eC \subseteq C$$

is $2\,|H|$ which is congruent $2 \bmod 4$ as $|H|$ is odd.

Example 4.3 Let G be a finite group with Sylow 2-subgroup T which has at least three generators, say, x, y, z. Put

$$a = (1-x) + (1-y) + (1-z) = 1 - (x+y+z).$$

Then $a \in J \setminus J^2$ where J denotes the Jacobson radical of KT. By a result of Charpin [4], the ideal $C = \langle a \rangle$ of KT generated by a is self-dual and doubly even. Inducing C up to KG (see [13], Proposition 2.5) we obtain a self-dual doubly even group code in KG. Thus only groups of a small 2-rank may prove the non-existence of self-dual doubly even codes.

Theorem 4.4 *Let G be a finite group with Sylow 2-subgroup T. Then KG contains a self-dual doubly even group code if and only if T is not cyclic nor a Klein four group.*

Proof: If T is cyclic, then by 4.2, there do not exist self-dual doubly even group codes in KG. If T is a Klein four group then $8 \nmid |G|$ and by Gleason's theorem there are no self-dual doubly even codes of length $|G|$.

Thus in order to prove the Theorem we may assume that T is not cyclic nor a Klein four group. In particular $|T| \geq 8$ and we have to show that in this case KG contains a self-dual doubly even group code. Note that by 2.5 of [13] it is enough to show that KH contains a self-dual doubly even group code for some $H \leq G$.

Now let H be a subgroup of G of order 8 and let C_n denote a cyclic group of order n. Since T is not cyclic we may find an H not cyclic as well. Thus H is one of the following groups.

(i) $H = C_2 \times C_2 \times C_2$,

(ii) $H = C_2 \times C_4$,

(iii) $H = D_8$ *is a dihedral group,*

(iv) $H = Q_8$ *is a quaternion group.*

We shall prove that in each case KH contains a selfdual doubly even group code. Let J denote the Jacobson radical of the group algebra KH.
(i) This case follows already by Example 4.3. We give here a more direct proof.
Let $H = \langle x, y, z \rangle$ be elementary abelian of order 8. For C we may take the Reed-Muller code $C = RM(3,1) = J^2$ which is generated as a K-vector space by

$$(1-x)(1-y),\ (1-x)(1-z),\ (1-y)(1-z) \text{ and } \sum_{h \in H} h.$$

Note that all generaters have weights divisible by 4. Thus, by ([12], 3.1.7), the code C which is obviously an ideal in KH is doubly even.
(ii) Let $H = \langle x, y \mid x^4 = y^2 = 1,\, [x,y] = 1 \rangle$. For C we now take the K-vector space generated by the elements

$$(1-x)(1-y),\ (1-x)(1-y)^2,\ (1-y)^3 \text{ and } \sum_{h \in H} h.$$

Note that C is equal to the self-dual ideal $J^3 \oplus \langle (1-x)(1-y) \rangle$. Again all generators have weights divisible by 4 and we are done again.
(iii) Let $H = D_8 = \langle x, y \mid x^4 = y^2 = 1,\, x^y = x^{-1} \rangle$ be a dihedral group. In this case C is generated in the same way as in (ii).
(iv) Let $H = Q_8 = \langle x, y \mid x^4 = y^4 = 1,\, x^y = x^{-1} \rangle$ be a quaternion group. Now we take for C the K-vector space generated by

$$(1-x)(1-y),\ (1-x)^3,\ (1-y)^3 \text{ and } \sum_{h \in H} h.$$

Thus C is the self-dual ideal $J^3 \oplus \langle (1-x)(1-y) \rangle$ and all generators have again weights divisible by 4.

Finally we would like to mention that Theorem 4.4 is rather of theoretical nature. It does not say anything about the existence of good self-dual doubly even group codes; even worse all codes we have constructed have minimum distance 4. But there may exist self-dual doubly even group codes which perform better. For instance, if $G = \mathrm{S}_4$ we can realize the binary $[24, 12, 8]$ self-dual doubly even Golay code as an ideal in KG as shown in [2]. Note that this code is extremal. It remains an open question which groups give raise to extremal self-dual doubly even group codes.

Furthermore, as the known examples show and contrary to the extended group code case there does not seem to exist a handy criteria to decide whether a given self-dual group code is doubly even or not.

References

[1] J.L. Alperin and R.B.Bell, Groups and representations. Graduate Text in Math., Springer, New York, Heidelberg 1995.

[2] F. Bernhardt, P. Landrock and O. Manz, The extended Golay codes considered as ideals. J. Comb. Theory, Series A 55, 235-246 (1990).

[3] P. Charpin and F.Levy-dit-Vehel, On self-dual affine-invariant codes. J. Comb. Theory Ser. A 67, 223-244 (1994).

[4] P. Charpin, Self-dual codes which are principal ideals of the group algebra $\mathbb{F}_2[\{\mathbb{F}_{2^m}, +\}]$. J. Statistical Planning and Interference 56, 79-92 (1996).

[5] B. Huppert, Endliche Gruppen, Springer, Berlin, Heidelberg, New York 1967.

[6] B. Huppert and N. Blackburn, Finite groups II, Springer, Berlin, Heidelberg, New York 1982.

[7] L.G. Kovacs, The permutation lemma of Richard Brauer. Bull. Lond. Math. Soc. 14, 127-128 (1982).

[8] P. Landrock, Finite group algebras and their modules. Lecture Note Series 84, Cambridge University Press, 1983.

[9] F.J. MacWilliams and N.J.A. Sloane, The theory of error-correcting codes. North-Holland, Amsterdam 1977.

[10] T. Okuyama and Y. Tsushima, On a conjecture of P. Landrock. J. Algebra 104, 203-208 (1986).

[11] N.J.A. Sloane and J.G. Thompson, Cyclic self-dual codes. IEEE Trans. Inform. Theory 29, 364-366 (1983).

[12] W. Willems, Codierungstheorie, deGruyter, Berlin, New York 1999.

[13] W. Willems, A note on self-dual group codes. IEEE Trans. Inform. Theory 48 (12), 3107-3109.