Self-dual extended cyclic codes

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

Keywords: extended cyclic codes, Euclidean self-dual codes, Hermitian self-dual codes, divisibility

1 Introduction

In [10] we studied Euclidean self-dual extended group codes over finite fields K of characteristic 2. The groups G involved in the investigations had to be of odd order which means that the corresponding group algebras were semisimple. The situation becomes more subtle if we drop the assumption $\operatorname{char} K = 2$ since in that case KG is no longer semisimple. However, if we stick to self-dual extended cyclic codes - and we will do so - then the usual problems one is faced in modular representation theory do not appear. We will deal the Euclidean and Hermitian case simultanously in this paper. As main results we characterize the existence of Euclidean and Hermitian self-dual extended cyclic codes. It turns out that such codes are extensions of particular duadic codes in the sense of [12]. Its existence can easily described in terms of elementary number theory. Finally, a characterization of t-divisibility of such codes extends the Gleason-Pierce Theorem.

*The author was partially supported by BFM2001-1667-C03-01

†The main part of this paper was written during a stay in Zaragoza in March and September 2004. The author would like to thank the Department of Mathematics for its hospitality and generous support.

Most of the methods we will use are of representation theoretical nature. The readers who are not familiar with that may find the books [6], [4] as good references.

2 Self-dual modules

In this section we collect some elementary facts on Euclidean and Hermitian modules.

Let G be a finite group and let K be a finite field of characteristic r. If V is a KG-module then the dual space $V^* = \mathrm{Hom}_K(V, K)$ becomes a KG-module if we put

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

For a field automorphism α of K we define a G-action on the K-vector space $V^\alpha = V$ in the following way. If $g \in G$ acts on V by the matrix (a_{ij}) with $a_{ij} \in K$ then g acts on V^α by the matrix (a_{ij}^α). With this action V^α becomes a KG-module called the *α-conjugate* of V. In particular, if α maps $x \in K$ onto x^q then we also write V^q for V^α.

Definition 2.1 Let V be a K-vector space.

a) A form $[\cdot\,,\cdot] : V \times V \to K$ is called *Euclidean* if it is K-linear in both components. We call a KG-module V a *Euclidean module* if V carries a non-degenerate G-invariant Euclidean form.

b) Assume that $|K| = q^2$ where q is a power of the prime r. A form $[\cdot,\cdot] : V \times V \to K$ is called *Hermitian* if it is K-linear in the first component, additive in the second and

$$[v, aw] = a^q[v, w] \quad \text{for all } v, w \in V \text{ and all } a \in K.$$

We call a KG-module V a *Hermitian module* if V carries a non-degenerate G-invariant Hermitian form.

To be able to work with both cases simultaneously we use the following notation: We put $\epsilon = 1$ if we are dealing with the Euclidean case and $\epsilon = q$ in the Hermitian case. If $|K| = q\epsilon$ then a Euclidean or Hermitian form satisfies

$$[v, aw] = a^\epsilon[v, w] \quad \text{for all } v, w \in V,\ a \in K.$$

Lemma 2.2 *A KG-module V is Euclidean resp. Hermitian if and only if $V^\epsilon \cong V^*$.*

Proof: If β denotes a KG-isomorphism from V^ϵ to V^* then, for $v, w \in V$, the map $[v, w] = \beta(w)v$ defines a non-degenerate Euclidean resp. Hermitian G-invariant form on V and vice versa.

Definition 2.3 Let $m, q \in \mathbb{N}$ with $\gcd(m, q) = 1$. For $k \in \mathbb{N}$ we denote by $s = s_{q^k}(m)$ the smallest nonnegative integer such that

$$m \mid q^{ks} - 1.$$

Clearly, $s_{q^k}(m)$ is the order of q^k in the group of units of $\mathbb{Z}_m$. This has the following trivial but useful consequences.

Lemma 2.4

a) If $s_q(m)$ is odd then $s_{q^2}(m) = s_q(m)$.

b) If $s_q(m)$ is even then $s_{q^2}(m) = s_q(m)/2$.

Lemma 2.5 *Let $x \in G$ be an element of prime order $p \nmid q \in \mathbb{N}$. Then*

a) $x^{-q} = x^{q^{2k}}$ for a suitable $k \in \mathbb{Z}$ if and only if $s_q(p)$ is even and $s_{q^2}(p)$ is odd.

b) $x^{-1} = x^{q^k}$ for a suitable $k \in \mathbb{Z}$ if and only if $s_q(p)$ is even.

Proof: We have

$$\begin{aligned} x^{-q} = x^{q^{2k}} &\iff p \mid (q^{2k} + q) \\ &\iff p \mid (q^{2k-1} + 1) \qquad \text{since } p \nmid q \\ &\iff \left\{ \begin{array}{l} p \mid (q^{4k-2} - 1) \quad \text{and} \\ p \nmid (q^{2k-1} - 1) \end{array} \right. \\ &\iff 2 \mid s_q(p) \quad \text{and} \quad 2 \nmid s_{q^2}(p) \end{aligned}$$

which yields a). For b) a similar argument which we already used in [10] works along the same lines.

Lemma 2.6 *Let $x \in G$ be a fixed r'-element for a prime r and let q be a power of r. Suppose that $\epsilon = 1$ or $\epsilon = q$. If*

$$L_G(x) = \{g \mid g \in G,\ x^g = x^{(\epsilon q)^k} \text{ for some } k \in \mathbb{Z},\ k \text{ depending on } g\}$$

then $L_G(x) \trianglelefteq N_G(\langle x \rangle)$.

Proof: First we prove that $L_G(x)$ is a subgroup of G. If $x^{g_1} = x^{(\epsilon q)^{k_1}}$ and $x^{g_2} = x^{(\epsilon q)^{k_2}}$ then

$$x^{g_1 g_2} = x^{(\epsilon q)^{k_1+k_2}}.$$

If the order of x divides $(\epsilon q)^t - 1$ and $x^g = x^{(\epsilon q)^k}$ then

$$(x^g)^{(\epsilon q)^{t-k}} = x^{(\epsilon q)^t} = x,$$

hence $x^{g^{-1}} = x^{(\epsilon q)^{t-k}}$. Thus $L_G(x)$ is a subgroup of G. Clearly, $L_G(x)$ is contained in $N_G(\langle x \rangle)$ and it is obviously normal.

The following theorem characterizes the situations in which a non-trivial irreducible Euclidean or Hermitian KG-module exists. For char $K = 2$, the Euclidean case was already treated in [10].

Theorem 2.7 *Let $K = \mathbb{F}_{\epsilon q}$ where q is a power of the prime r and let $\epsilon = 1$ or $\epsilon = q$. If G is a finite group of odd order then the following conditions are equivalent.*

a) *There exists a non-trivial irreducible KG-module V with $V^\epsilon \cong V^*$.*

b) *There exists a $y \in G$ and a non-trivial r'-element $x \in G$ such that $x^{-\epsilon} = (x^{(\epsilon q)^k})^y$ for some $k \in \mathbb{Z}$.*

c) *There exists an $x \in G$ of prime order $p \neq r$ with $x^{-\epsilon} = x^{(\epsilon q)^k}$ for some $k \in \mathbb{Z}$.*

d) *If $\epsilon = 1$, then $s_q(p)$ is even for some prime $p \neq r$ with $p \mid |G|$. If $\epsilon = q$, then $s_q(p)$ is even and $s_{q^2}(p)$ is odd for some prime $p \neq r$ with $p \mid |G|$.*

Proof: a) $\Longleftrightarrow$ b) This is Brauer's Permutation Lemma (see [7]) in connection with Berman's Theorem ([6], Chap. VII, 3.11).
b) $\Rightarrow$ c) If

$$x^{-\epsilon} = (x^{(\epsilon q)^k})^y$$

for some $y \in G$ then

$$x^{\epsilon^2} = (x^{(\epsilon q)^{2k}})^{y^2}.$$

Thus $y^2 \in L_G(x)$. Since G is of odd order $N_G(\langle x \rangle)$ is of odd order as well and we obtain $y \in L_G(x)$. If we write $x^y = x^{(\epsilon q)^s}$ for some $s \in \mathbb{Z}$ then

$$x^{-\epsilon} = (x^{(\epsilon q)^k})^y = (x^y)^{(\epsilon q)^k} = x^{(\epsilon q)^{s+k}}.$$

Taking a suitable power of x (to get an element of prime order) the assertion in c) follows.
c) $\Rightarrow$ b) This is obvious.
c) $\Longleftrightarrow$ d) This follows immediately from 2.5.

Definition 2.8 Let $^{-}\colon KG \to KG$ denote the antialgebra automorphism of KG defined by $g \mapsto g^{-1}$ for $g \in G$. In particular,

$$\overline{\sum_{x\in G} a_x x} = \sum_{x\in G} a_x x^{-1}.$$

Furthermore, if $|K| = \epsilon q$ we put $(\sum_{x\in G} a_x x)^{\epsilon} = \sum_{x\in G} a_x^{\epsilon} x$.

Lemma 2.9 *Let $|K| = \epsilon q$ and let G be a finite group of order coprime to q. In particular, KG is semi-simple. Furthermore, let $e_0 = 1/|G| \sum_{g\in G} g$ denote the central idempotent corresponding to the trivial module. Then there is no non-trivial irreducible KG-module V with $V^{\epsilon} \cong V^*$ if and only if $1 \in KG$ has a decomposition*

$$1 = e_0 + e + \bar{e}^{\epsilon}$$

with central and mutually orthogonal idempotents $e_0, e, \bar{e}^{\epsilon}$.

Proof: Since KG is semisimple we may decompose $1 = e_0 + e_1 + \ldots + e_k$ with primitive and mutually orthogonal idempotents e_i. In particular, each $e_i KG$ is an irreducible KG-module. The condition that the trivial module is the only irreducible KG-module V with $V^{\epsilon} \cong V^*$ means that the idempotents e_i can be grouped in such a way that $1 = e_0 + e + f$ with central idempotents e_0, e, f such that $(eKG)^{\epsilon} \cong (fKG)^*$. By a result of Okuyama and Tsushima (see [11]), we have $(fKG)^* \cong \bar{f}KG$. Since the idempotents belong to the center of KG we finally get $f = \bar{e}^{\epsilon}$. The converse is obvious.

The following Lemma is well-known. It follows from ([6], Chap. VII).

Lemma 2.10 *Let G be a finite group and let K be a field of prime characteristic. Furthermore, suppose that L is a splitting field for G. If W is an irreducible KG-module and V an irreducible KL-module which is a component in $W \otimes L$, then the multiplicity of W as composition factor of KG equals the multiplicity of V as composition factor of LG.*

3 Semisimple extended self-dual group codes

Throughout this section let K again be a field with ϵq elements where q is a power of the prime r. As before let $\epsilon = 1$ or $\epsilon = q$ depending on the geometry we are dealing with.

Definition 3.1 A subspace C of the vector space K^n is called a *self-dual Euclidean* resp. *self-dual Hermitian* code if $C = C^\perp$ with respect to the standard Euclidean resp. Hermitian form on K^n.

If G is a finite group then the group algebra KG carries natural non-degenerate G-invariant Euclidean and Hermitian forms defined by

$$[\sum_{x\in G} a_x x, \sum_{g\in G} b_x x] = \sum_{x\in G} a_x b_x^\epsilon.$$

Both forms may be extended to nondegenerate G-invariant Euclidean resp. Hermitian forms on $K \oplus KG$ where G acts trivially on the additional component K.

Definition 3.2 We call C a *group code* if C is an ideal in KG and an *extended group code* if C is a KG- submodule of $K \oplus KG$.

In [10] we proved that $(K \oplus KG)/C^\perp \cong C^*$ as G-modules if C is an extended group code. The proof works similarily in case of a Hermitian geometry. Thus we have

Lemma 3.3 *If C is an extended group code then*

$$(K \oplus KG)/(C^\perp)^\epsilon \cong C^*$$

as KG-modules. In particular, if C is self-dual then

$$(K \oplus KG)/C^\epsilon \cong C^*,$$

and every non-trivial self-dual irreducible KG-module with $V^\epsilon \cong V^*$ has even multiplicity in KG.

Proof: Let $[\cdot\,,\cdot]$ denote the canonical Euclidean resp. Hermitian form on the space $K \oplus KG$. Then α with $\alpha(a)c = [c, a^\epsilon]$ for $c \in C$ and $a \in K \oplus KG$ defines a KG-epimorphism from $K \oplus KG$ onto C^* with kernel

$$\{a \mid a \in K \oplus KG,\ [c, a^\epsilon] = 0 \text{ for all } c \in C\} = (C^\perp)^\epsilon.$$

So far we have proved the first part of the lemma from which the others follow easily.

Definition 3.4 A vector $v \in \mathbb{F}_{\epsilon q}^n$ is called *isotropic* if $[v,v] = 0$. Thus, if $v = (a_1, \ldots, a_n)$ then $[v,v] = \sum_{i=1}^n a_i^{1+\epsilon} = 0$.

Lemma 3.5 *Let q be a power of an odd prime r and let $v = (a, 1, \ldots, 1)$ be a vector in K^{n+1} with $n+1 \geq 2$.*

a If $K = \mathbb{F}_{q^2}$, then there exists an $a \in K$ such that v is Hermitian isotropic.

b) If $K = \mathbb{F}_q$, then there exists an $a \in K$ such that v is Euclidean isotropic if and only if $a^2 = -n$ has a solution in K.

Proof: a) We have to solve the equation $[v,v] = a^{q+1} + n = 0$ in K. Since

$$\{a^{q+1} \mid a \in \mathbb{F}_{q^2}\} = \mathbb{F}_q$$

such a solution always exists.
b) This is obvious.

Lemma 3.6 *Let $k \in \mathbb{Z}$ and let K be a finite field of characteristic r with $r \nmid k$. Then the equation $x^2 = k$ has a solution in K if and only if either $(\frac{k}{r}) = 1$ (this includes the case $r = 2$) or $\log_r |K|$ is even.*

Proof: Put $t = \log_r |K|$. $k \in K^2$ means $k \in K^{*2} \cap \mathbb{F}_r^*$ since $r \nmid k$. This is obviously true for $r = 2$. For r odd, note that the squares in K^* form a subgroup of index two. Since

$$r - 1 \mid q - 1 = r^t - 1 = (r-1)(1 + r + \ldots r^{t-1})$$

we get $K^{*2} \cap \mathbb{F}_r^* = \mathbb{F}_r^*$ for t even and $K^{*2} \cap \mathbb{F}_r^* = \mathbb{F}_r^{*2}$ for t odd. Hence the latter condition forces $(\frac{k}{r}) = 1$ if t is odd.

If C is a self-dual code in $K \oplus KG$ then $2 \dim C = 1 + |G|$. Thus G is of odd order. Since we are always dealing with self-dual group codes we may assume $2 \nmid |G|$ in the sequel.

Lemma 3.7 *Let G be a finite group of odd order. Then, over any field K with $\operatorname{char} K \nmid |G|$, an irreducible KG-module has odd multiplicity in KG.*

Proof: According to 2.10 we may assume that K is algebraically closed. Since $\operatorname{char} K \nmid |G|$ the group algebra KG is semisimple, and the multiplicity of an irreducible module M as a composition factor of KG equals $\dim M$. But $\dim M$ is odd as G is of odd order and K is algebraically closed.

Lemma 3.8 *Suppose that* $\operatorname{char} K \nmid |G|$. *If* C *is an extended self-dual Euclidean or Hermitian group code for* G *then the trivial module is the only irreducible* KG*-module* V *with* $V^\epsilon \cong V^*$.

Proof: By 3.3 each non-trivial self-dual irreducible KG-module has even multiplicity in KG. Thus the assertion follows immediately by 3.7.

Theorem 3.9 *Let* K *be a finite field with* ϵq *elements where* q *is a power of the prime* r. *If* G *is a finite group with* $\gcd(|G|, 2r) = 1$ *then the following conditions are equivalent.*

a) *There are extended self-dual Euclidean resp. Hermitian group codes for the group* G.

b) *In case* $\epsilon = 1$ *(i.e. Euclidean geometry)* $s_q(p)$ *is odd for all primes* $p \mid |G|$ *and either* $(\frac{-|G|}{r}) = 1$ *or* $\log_{\mathrm{r}}|\mathrm{K}|$ *is even.*
In case $\epsilon = q$ *(i.e. Hermitian geometry) either* $s_q(p)$ *is odd or* $s_{q^2}(p)$ *is even for all primes* $p \mid |G|$.

Proof: a) $\Rightarrow$ b) Let $C = C^\epsilon \leq K \oplus KG$. By 3.8, the trivial module is the only irreducible KG-module V with $V^\epsilon \cong V^*$. Therefore, by 2.7, the conditions on s_q and s_{q^2} follow immediately. Moreover, since

$$K \oplus KG = K \oplus e_0 KG \oplus (1 - e_0)KG = K^{1+|G|}$$

the code C must contain an isotropic vector v of the form

$$v = (a, 0, \ldots, 0) + (0, |G|e_0) = (a, 1, \ldots, 1).$$

Thus b) follows from 3.5 and 3.6.
b) $\Rightarrow$ a) Now, by 2.7 and 2.9, there is a decomposition $1 = e_0 + e + \bar{e}^\epsilon$ with mutually orthogonal and central idempotents $e_0 = 1/|G| \sum_{g \in G} g$, e and $\bar{e}^\epsilon$. We put

$$v = (a, 1, \ldots, 1) = (a, 0, \ldots, 0) + (0, |G|e_0)$$

and choose a (as in 3.5) such that v is isotropic and $C = vK + eKG$. With this notation we get

$$[e, v] = [e, e_0] = [ee_0, e_0] = [0, e_0] = 0.$$

Finally we have

$$[eKG, eKG] = [e^2 KG, eKG] = [eKG, (\overline{e})^\epsilon eKG] = [eKG, 0] = 0.$$

We would like to mention that part b) of the above theorem can easily be checked if $|G|$ and $|K|$ are given. Also note that, by 2.4, both possibilities in the Hermitian case of b) exclude each other and that the existence of a Euclidean self-dual extended cyclic code over $\mathbb{F}_q$ implies that of a Hermitian over $\mathbb{F}_{q^2}$. The latter is also a consequence of the fact that by extending scalars in a code of the first type one gets a code of the second.

Examples 3.10 Let $K = \mathbb{F}_4$.
a) Let G be a cyclic group of order $p = 5$. Since $s_4(5) = 2$ there exists an extended self-dual Hermitian group code C for G, by Theorem 3.9. Let ξ be a primitive 5-th root of unity in $\mathbb{F}_{16}$. If $\alpha = \xi + \xi^4$ and $\beta = \xi^2 + \xi^3$ then a generator matrix for C is given by

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & \alpha & \beta & \beta & \alpha \\ 0 & \alpha & 0 & \alpha & \beta & \beta \end{pmatrix}.$$

One easily checks that $\mathrm{d}(C) \geq 4$. Thus C is an extended cyclic self-dual Hermitian $[6, 3, 4]$ MDS code over $\mathbb{F}_4$.
b) Let $p = 13$ and let G be a cyclic group of order 13. Since $s_4(13) = 6$ there exists a self-dual Hermitian group code C for G, again by Theorem 3.9. Note that $x^2 = x^{-1}$ for $x \in K^*$. Thus, by 3.3, the group algebra decomposes as $KG = K \oplus M \oplus M^2$. In particular, up to Galois conjugation, the code C is unique. It must be the extended quadratic residue code Q_{14} (see [9], Table VI). Hence C is an extended cyclic self-dual Hermitian $[14, 7, 6]_4$ code which is optimal (see [2] or [9], Corollary 15).
c) Along the same lines as in b) we find a $[30, 15, 12]_4$ extended cyclic self-dual Hermitian code. This code is also optimal (see [2]).
d) By 3.9, there exists an extended self-dual cyclic $[26, 13]$ code over K. Theorem 6 of [12] shows that such a code has minimum distance $\mathrm{d} \leq 5$ so that the code is far away from being optimal. Observe that in contrast to a), b) and c) the corresponding group algebra has more than 3 irreducible components.

Lemma 3.11 *Let p be an odd prime and let $p \nmid q \in \mathbb{N}$. Then $(\frac{q}{p}) = 1$ if and only if $s_q(p) \mid \frac{p-1}{2}$.*

Proof: Let $L = \mathbb{F}_p^*$ and $L^2 = \{a^2 \mid a \in L\}$. Clearly, L^2 is of index two in L. Since L is cyclic it is in fact the only subgroup of order $\frac{p-1}{2}$ and the claim follows.

Remark 3.12 We collect some trivial consequences of the previous lemma.

a) If $s_q(p)$ is odd, then $(\frac{q}{p}) = 1$, i.e., q is a square modulo p.

b) If $p \equiv -1 \bmod 4$ and $(\frac{q}{p}) = 1$, then $s_q(p)$ is odd.

c) If $p \equiv -1 \bmod 4$, then $s_{q^2}(p)$ is odd.

Proposition 3.13 *Let $|K| = \epsilon q$ and $n \in \mathbb{N}$ with $\gcd(n, |K|) = 1$. Let C_0 be a cyclic code over K of length n. Suppose that the extended code C is self-dual Euclidean or Hermitian. Then $|K|$ is a square modulo n and C_0 is a duadic code in the sense of* [12].

Proof: The assertion on $|K|$ is trivial if $\epsilon = q$, and a consequence of 3.9 and 3.12 a) in other case. The existence of a self-dual code of length $n+1$ forces n to be odd. Let G be a cyclic group of order n. By Lemma 3.8, the trivial KG-module is the only irreducible KG-module V with $V^\epsilon \cong V^*$. and by 3.3, the code C_0 does not contain with some non-trivial irreducible module V also its dual $V^{\epsilon *}$. Furthermore note, that an irreducible KG-module corresponds uniquely to a cyclotomic class modulo n, i.e., to

$$\{i(\epsilon q)^j \mid j = 1, 2, \ldots\}$$

for some $0 \leq i < n$. Let S_1 resp. S_2 denote the union of all cyclotomic classes which correspond to non-trivial irreducible composition factors of C_0 resp. $C_0^{\epsilon q}$. Clearly, $i \in S_1$ if and only if $-iq \in S_2$ Since $V \not\cong V^{\epsilon q}$ for a non-trivial irreducible V we have $S_1 \cap S_2 = \emptyset$. Moreover, by 3.3,

$$S_1 \cup S_2 = \{1, 2, \ldots, n-1\}.$$

This shows that

$$\mu_{-q} : S_1 \to S_2$$

defined by $i \mapsto -iq$ is a splitting modulo n in the sense of [12]. Thus C_0 is a duadic code.

Note that part of 3.13 can also be found in [12].

Let $n \in \mathbb{N}$ be odd and let r be a prime with $r \nmid n$. Let $\mathcal{Q} = \{a^2 \bmod n \mid a \in \mathbb{Z}, n \nmid a\}$ be the set of squares modulo n. Similarily, let $\mathcal{N}$ denote the set of nonsquares modulo n. We put $q = r^t$ and suppose that ϵq is a square modulo n. Let α be a primitive n-th root of unity in an extention field of $K = \mathbb{F}_{\epsilon q}$. Under these conditions the polynomial

$$\prod_{i \in \mathcal{Q}} (x - \alpha^i)$$

generates a cyclic code over K of length n and dimension $\frac{n-1}{2}$, a so-called quadratic residue code which we denote by Q_n. If n is a power of a prime then Q_n has a canonical extension which we denote by $\hat{Q}_n$ (see [5], section 6 or [14], section 6). Note that this definition coincides with the usual definition of a quadratic residue code over a prime field.

Theorem 3.14

a) There exists an extension of Q_n which is Euclidean if and only if $p \equiv -1 \bmod 4$ for at least one prime $p \mid n$ and if $r \neq 2$ and $\log_r |K|$ is odd, $(\frac{-n}{r}) = 1$.

b) There exists an extension of Q_n which is Hermitian if and only if $(\frac{-q}{p}) = -1$ for at least one prime $p \mid n$.

Proof: a) Clearly, Q_n has an Euclidean extension if and only if $\mu_{-1} : \mathcal{Q} \to \mathcal{N}$ (multiplication by -1) is a bijection and $-n \in K^2$. The first condition means that $-1 \in \mathcal{N}$ which, by the Chinese Reminder Theorem, is equivalent to $(\frac{-1}{p}) = -1$ for at least one prime $p \mid n$. Thus $p \equiv -1 \bmod 4$ for at least one prime divisor p of n. The latter condition follows from Lemma 3.6.
b) The proof runs similarly to that of part a).

Next we prove some number theoretical results which we need in the rest of this section. For simplicity we stick to the case $q = r$.

Proposition 3.15 *Let $2 \neq p$ and r be primes. Suppose that $(\frac{r}{p}) = 1$.*

a) For $r \neq 2$, $s_r(p)$ is odd and $(\frac{-p}{r}) = 1$ if and only if either $p \equiv -1 \bmod 4$ or $s_r(p)$ is odd and $r \equiv 1 \bmod 4$.

b) $(\frac{-p}{r}) = -1$ if and only if $p \equiv 1 \bmod 4$ and $r \equiv -1 \bmod 4$.

c) If $s_{r^2}(p)$ is even, then $p \equiv 1 \bmod 8$.

Proof: Before proceeding with the proof note that for $r \neq 2$ the quadratic reciprocity law yields

$$\left(\frac{-p}{r}\right) = \left(\frac{-1}{r}\right)\left(\frac{p}{r}\right) = (-1)^{\frac{r-1}{2}}(-1)^{\frac{r-1}{2}\frac{p-1}{2}}\left(\frac{r}{p}\right) = (-1)^{\frac{r-1}{2}\frac{p+1}{2}}.$$

a) Observe that

$$1 = \left(\frac{-p}{r}\right) = (-1)^{\frac{r-1}{2}\frac{p+1}{2}}$$

if and only if either $\frac{p+1}{2}$ is even (i.e., $p \equiv -1 \bmod 4$) or $\frac{r-1}{2}$ is odd (i.e., $r \equiv 1 \bmod 4$). Finally, by 3.12 b), if $p \equiv -1 \bmod 4$ then $s_r(p)$ is odd.
b) Clearly, both sides of the equivalence force r to be odd. Now,

$$-1 = \left(\frac{-p}{r}\right) = (-1)^{\frac{r-1}{2}\frac{p+1}{2}}$$

if and only if both $\frac{p+1}{2}$ and $\frac{r-1}{2}$ are odd.
c) By 2.4, we have $4 \mid s_r(p)$ and by 3.11, we get $s_r(p) \mid \frac{p-1}{2}$. Thus the claim follows.

Proposition 3.16 *Let $2 \neq p$ and r be primes. If $(\frac{r}{p}) = -1$ then*

a) $s_r(p)$ is even.

b) $s_{r^2}(p)$ is even if and only if $p \equiv 1 \bmod 4$.

Proof: a) According to 3.12 a) the condition $(\frac{r}{p}) = -1$ implies that $s_r(p)$ is even.
b) By 3.12 c), we obtain $p \equiv 1 \bmod 4$ if $s_{r^2}(p)$ is even. To prove the converse, note that, by 2.4,

$$s_{r^2}(p) = s_r(p)/2$$

as $s_r(p)$ is even, by part a). Furthermore, by 3.11, we have $s_r(p) = p - 1$. Thus, if $4 \mid p - 1$ then $2 \mid s_{r^2}(p)$.

Remark 3.17 Let p, r be different primes with $p \neq 2$ and $(\frac{r}{p}) = 1$. Let $\hat{Q}_p$ denote the canonical extended quadratic residue code over the prime field $\mathbb{F}_r$ with parameters $[p+1, \frac{p+1}{2}]$. It is well known that $\hat{Q}_p$ carries a Euclidean geometry if and only if $p \equiv -1 \bmod 4$ (see for instance [15], 6.3.5). The only if part follows immediately from 3.14. For the if part, note that if $p \equiv -1 \bmod 4$ the condition $(\frac{-p}{r}) = 1$ holds true by 3.15 b). This implies the existence of an isotropic vector as in 3.5 and such a vector is precisely what is used in the construction of $\hat{Q}_p$ (see [15], 6.3.5).

We also deduce from 3.14 that the canonical extended quadratic residue code over $\mathbb{F}_{r^2}$ with parameters $[p+1, \frac{p+1}{2}]$ carries a Hermitian geometry only if either $(\frac{r}{p}) = 1$ and $p \equiv -1 \bmod 4$ or $(\frac{r}{p}) = -1$ and $p \equiv 1 \bmod 4$. As in the previous case these conditions are also sufficient for the existence of a Hermitian geometry on $\hat{Q}_p$.

Proposition 3.18 *Let p, r be primes with $p \neq 2$ and $(\frac{r}{p}) = 1$. Then, over the prime field $\mathbb{F}_r$, the canonical extended QR code $\hat{Q}_p$ is not self-dual Euclidean but there is a self-dual Euclidean extended cyclic code of the same length precisely in the following cases:*

a) $r = 2$, $p \equiv 1 \bmod 8$ *and* $s_2(p)$ *odd.*

b) $p \equiv 1 \bmod 4$, $r \equiv 1 \bmod 4$ *and* $s_r(p)$ *odd.*

Proof: If a) or b) holds then $p \equiv 1 \bmod 4$ and $\hat{Q}_p$ is not Euclidian, by 3.17. According to 3.15 a), the condition in b) yields $(\frac{-p}{r}) = 1$. Thus, by 3.6, the equation $a^2 \equiv -p \bmod r$ has a solution and the existence of a self-dual Euclidean extended cyclic code of length $p+1$ follows by 3.9. Conversely, if $\hat{Q}_p$ is not Euclidean then $p \equiv 1 \bmod 4$. In case $r = 2$ the condition $(\frac{2}{p}) = 1$ implies $p \equiv 1 \bmod 8$. The existence of an extended Euclidean cyclic code of length $p+1$ forces $s_r(p)$ odd, by 3.9. Furthermore, for r odd, we have $r \equiv 1 \bmod 4$, by 3.15 a).

Proposition 3.19 *Let p, r be primes with $p \neq 2$ and $K = \mathbb{F}_{r^2}$ be the underlying field. The canonical extended QR code $\hat{Q}_p$ is not self-dual Hermitian but there is a self-dual Euclidean extended cyclic of the same length if and only if $(\frac{r}{p}) = 1$ and one of the following cases holds:*

a) $r = 2$, $p \equiv 1 \bmod 8$ *and* $s_2(p)$ *odd.*

b) $p \equiv 1 \bmod 4$, $r \equiv 1 \bmod 4$ *and* $s_r(p)$ *odd.*

c) $p \equiv 1 \bmod 4, r \equiv -1 \bmod 4$ *and* $s_r(p)$ *odd.*

d) $p \equiv 1 \bmod 8$ *and* $s_{r^2}(p)$ *even.*

Proof: If $(\frac{r}{p}) = -1$ then $s_r(p)$ is even, by 3.16 a). Thus if there exists an extended self-dual Hermitian cyclic code over $\mathbb{F}_{r^2}$ of length $p+1$ then $s_{r^2}(p)$ must be even. Hence $p \equiv 1 \bmod 4$, by 3.16 b). But in this case the code $\hat{Q}_p$ is Hermitian according to 3.17.

Clearly, in a) - d) we have $p \equiv 1 \bmod 4$. Thus $\hat{Q}_p$ is not Hermitian, by 3.17. According to 3.9 there exists an extended self-dual Hermitian cyclic code over $\mathbb{F}_{r^2}$ of length $p+1$ if and only if $s_r(p)$ is odd or $s_{r^2}(p)$ is even.

If $r = 2$ then $p \equiv \pm 1 \bmod 8$ since by assumption $(\frac{r}{p}) = 1$. Since $\hat{Q}_p$ is not Hermitian, we get $p \equiv 1 \bmod 8$, by 3.17. Thus have case a). Suppose that r is odd. Applying 3.15 a) we obtain case b), and applying 3.15 b) yields case c). Finally we may suppose that $s_{r^2}(p)$ is even. Thus, by 3.15 c), we get $p \equiv 1 \bmod 8$ which is case d).

Remark 3.20 If there is some self-dual Euclidean or Hermitian extended QR code, then it is $\hat{Q}_p$, by 3.17. Therefore the previous results characterize the cases in which there is no self-dual Euclidean or Hermitian extended QR code but there is some duadic code.

Note that for simplicity we have reduced ourselves in 3.18 and 3.19 to the case of prime length and $q = \epsilon r$. One can easily deduce similar results in the general situation.

4 Modular extended self-dual cyclic codes

In the previous section we considered extended self-dual codes for groups G in case that the characteristic r of the underlying field does not divide the order of G. In this section we assume that r divides $|G|$. Hence KG is no longer semisimple and its algebraic structure may become quite complicated. However, in case of cyclic groups one is not faced with hard representation theoretical problems which usually arise in many questions. On the other hand cyclic codes, i.e. group codes for cyclic groups, are of particular interest. Therefore we will deal here only with cyclic codes and extended versions. In this case we may split $G = R \times Q$ with R an r-group and Q an r'-group. Thus we are in a situation in which we can apply the results of section 3 to the semisimple group algebra KQ while the group algebra KR is uniserial with the only ideals the powers of the radical $J = J(KR)$.

Proposition 4.1 *Let $|K| = \epsilon q$ where q is a power of the prime r and let H be any finite group. If C is an ideal in KH then the dual $C^{\perp_\epsilon}$ of C is given by*

$$C^{\perp} = \overline{\mathcal{L}}(C)^{\epsilon}$$

where $\mathcal{L}(C)$ denotes the left annihilator of C in KH. In particular, if J is the radical of KH and $J^{N-1} > J^N = 0$ then

$$(J^k)^{\perp} = J^{N-k}$$

for $0 \leq k \leq N$.

Proof: One easily checks that $C^{\perp} = \overline{\mathcal{L}}(C)^{\epsilon}$. Since $\overline{J}^{\epsilon} = J$ the rest of the assertion follows by ([15], 7.1.16).

Proposition 4.2 *Let K be a field with ϵq elements where q is a power of a prime r and let G be a cyclic group of order r^n. Furthermore, let J denote the radical of the group algebra KG. Then there exists $C = C^{\perp_\epsilon} \leq K \oplus KG$ if and only if there is an isotropic vector $v = a1_K + w$ with $a1_K$ in the first component of $K \oplus KG$ and $w \in J^m \setminus J^{m+1}$ where $m = \frac{r^n-1}{2}$. In that case*

$$C = J^{m+1} \oplus \langle v \rangle.$$

Proof: Clearly, for $k \geq m+1$ we have $J^k \leq (J^k)^\perp$. Therefore, if there is an isotropic vector v as described in the proposition then the code

$$C = J^{m+1} \oplus \langle v \rangle$$

is Euclidean or Hermitian self-dual.

To prove the converse note that $C \leq K \oplus J^m$ since KG is a uniserial algebra and $\dim C = \frac{r^n+1}{2} = m+1$.

Suppose that $b1_K + x \in C = C^{\perp_\epsilon}$ with $x \in J^k$ and $k \geq m+1$. Then

$$0 = [b1_K + x, b1_K + x] = b^{\epsilon+1} + [x,x] = b^{\epsilon+1}.$$

This shows that $J^{m+1} \leq C$ and the assertion follows since $\dim J^{m+1} = m$.

Proposition 4.3 *Let the notation be as in* 4.2. *Then $C = C^\perp$ is an* MDS *code if and only if $|G| = r$.*

Proof: If $|G| = r$ then, using ([15], 7.2.5), one easily checks that C is an MDS code. Conversely suppose that $|G| = r^n$ with $n > 1$. Then

$$r^n - 1 \geq r^{n-1}(r-1) \geq m+1 = \frac{r^n-1}{2}$$

since $r > 2$. If $k = r^{n-1}(r-1)$ then $c = (g-1)^k \in C$ where g is a generator of G. Furthermore

$$(g-1)^k = (g^{r^{n-1}} - 1)^{r-1}.$$

Thus $\mathrm{wt}(c) \leq r < \frac{r^n+3}{2}$ which shows that C is not an MDS code.

Examples 4.4 There are two inequivalent $[10,5,6]$ MDS codes over $\mathbb{F}_9$. One of them is Euclidean the other Hermitian self-dual (see [1]). By 4.3, both codes are not extended cyclic codes since the underlying group has order $r^n = 3^2$.

To state one of the main results in this section we need a lemma from elementary number theory.

Lemma 4.5 *Let r be an odd prime and $n \in \mathbb{N}$. If $m = \frac{r^n-1}{2}$ then*

a) $\sum_{i=0}^{m} \binom{m}{i}^2 = \binom{2m}{m}$.

b) $\binom{2m}{m} \equiv (-1)^{n\frac{r-1}{2}} \bmod r$.

Proof: a) This is a formula well-known in combinatorics.
b) We write

$$2m = r^n - 1 = (r-1) + (r-1)r + \ldots + (r-1)r^{n-1}$$

and

$$m = \frac{(r-1)}{2} + \frac{(r-1)}{2}r + \ldots + \frac{(r-1)}{2}r^{n-1}.$$

Thus, by Lucas' Theorem (see [13], 4.5.1), we obtain

$$\begin{aligned}
\binom{2m}{m} &\equiv \prod_{i=0}^{n-1} \binom{r-1}{\frac{r-1}{2}} \bmod r \\
&\equiv \prod_{i=0}^{n-1} \frac{(r-1)(r-2)\ldots(r-\frac{(r-1)}{2})}{1\cdot 2 \ldots \frac{(r-1)}{2}} \bmod r \\
&\equiv \prod_{i=0}^{n-1} (-1)^{\frac{r-1}{2}} \equiv (-1)^{n\frac{r-1}{2}} \bmod r.
\end{aligned}$$

Theorem 4.6 *Let r be an odd prime, $n \in \mathbb{N}$, and let q be a power of r. Furthermore, suppose that $r \nmid l \in \mathbb{N}$.*

a) For $K = \mathbb{F}_q$, the following two conditions are equivalent.

(i) There exists a Euclidean self-dual extended cyclic code of length $1 + r^n l$.

(ii) $s_q(l)$ is odd and either $(\frac{k}{r}) = 1$ where $k = l(-1)^{n(\frac{r-1}{2})+1}$ or $\log_{\mathrm{r}}|\mathrm{K}|$ is even.

b) For $K = \mathbb{F}_{q^2}$, the following two conditions are equivalent.

(i) There exists an Hermitian self-dual extended cyclic code of length $1 + r^n l$.

(ii) For all primes p with $p \mid l$ either $s_q(p)$ is odd or $s_{q^2}(p)$ is even.

Proof: Let G be a cyclic group of order $r^n l$ and write $G = R \times H$ with $|R| = r^n$ and $|H| = l$. Then, as vector spaces, we may identify $KG = KR \otimes KH$ via the map $g \to x \otimes y$ if $g = xy$ with $x \in R$ and $y \in H$.

Since $e_0 = 1/|H| \sum_{h \in H} h$ resp. 1 is the principal block idempotent of KH resp. KR the principal block idempotent of KG is $f_0 = 1 \otimes e_0$. Furthermore, we have

$$f_0 KG = (1 \otimes e_0)(KR \otimes KH) = KR \otimes e_0$$

and

$$K \oplus KG = K \oplus f_0 KG \oplus (1 - f_0)KG = (K \oplus f_0 KG) \perp_\epsilon (1 - f_0)KG.$$

Therefore there exists a Euclidean resp. Hermitian self-dual KG-submodule in $K \oplus KG$ if and only if there are Euclidean resp. Hermitian self-dual KG-submodules $D_1 \leq K \oplus f_0 KG$ and $D_2 \leq (1 - f_0)KG$. In order to prove the theorem we have to find neccessary and sufficient conditions for the existence of D_1 and D_2.

First we deal with the Euclidean case. To determine the existence of D_1 note that $f_0 KG = KR \otimes e_0 \cong KR$. Therefore we may apply 4.2 and deduce that there is such a code if and only if there exists an isotropic vector $v = a1_K + w$ with $w \in J(f_0 KG)^{\frac{r^n - 1}{2}}$. So we need a solution a of the equation

$$0 = [v, v] = a^2 + [w, w].$$

If x is a generator of R then w must be (up to a scalar) of the form $(1 - x)^{\frac{r^n - 1}{2}} \otimes e_0$. Therefore, by 4.5, we have

$$[w, w] = l(-1)^{n \frac{r-1}{2}}.$$

Thus we are forced to solve the equation

$$a^2 + l(-1)^{n(\frac{r-1}{2})} = 0$$

for $a \in K = \mathbb{F}_q$. By 3.6, a solution exists if and only if $(\frac{k}{r}) = 1$ with $l(-1)^{n(\frac{r-1}{2})+1}$ or $\mathrm{log_r|K|}$ is even and the result follows by 3.6. In the Hermitian case there is no such restriction as shown in Lemma 3.5.

To find the condition for the existence of D_2 we first assume that the conditions on s_q and s_{q^2} hold true. That means that there is no non-trivial irreducible KH-module V with $V^\epsilon \cong V^*$ (see Theorem 2.7). By 2.9, we may decompose $1 \in KH$ as $1 = e_0 + e + \bar{e}^\epsilon$ where e is an idempotent with

$e\bar{e}^\epsilon = 0$. For $f = 1 \otimes e \in KR \otimes KH$ one easily checks that $D_2 = fKG$ is a Euclidean resp. Hermitian self-dual KG-submodule of $(1 - f_0)KG$

It remains to prove that the conditions on s_q and s_{q^2} are necessary. Note that (i) of a) or b) forces l to be odd. Therefore, by 3.7, the composition factors of KG have odd multplicity. Thus $K \oplus KG/C^\epsilon \cong C^*$ imlies that the trivial module is the only irreducible self-dual KG-module and the conditions on s_q and s_{q^2} follow from 2.7.

Corollary 4.7 *Let K be a field with $q = r^s$ elements where r is an odd prime. Furthermore, let $G = \langle g \rangle$ be a cyclic group of order r^n. Then there exists a Euclidean $C = C^\perp \leq K \oplus KG$ if and only if one of the following conditions holds.*

(i) $r \equiv 1 \bmod 4$.

(ii) *n is odd.*

(iii) *s is even.*

Proof: We may apply 4.6 with $l = 1$. Thus there exists a Euclidean self-dual extended cyclic code of length $1 + r^n$ if and only if either $(-1)^{n(\frac{r-1}{2})+1}$ is a square mod r or s is even. Now, the assertion of the corollary follows easily.

The Hermitian case turns out to be much simpler. Here we get immediately by 4.6

Corollary 4.8 *Let K be a field with $q^2 = r^{2s}$ elements where r is an odd prime number. Let $G = \langle g \rangle$ be cyclic of order r^n. Then there always exists a Hermitian $C = C^\perp \leq K \oplus KG$.*

Let t be a positive integer. A code C is called *t-divisible* if all codewords in C have a weight which is a multiple of t. Unless $t = q = 2$, the dimension of a t-divisible code over $\mathbb{F}_q$ of length n is bounded by $n/2$ (see [15], 4.5.5).

Corollary 4.9 *Let K be a field with q elements. Let t and n be positive integers with $n \geq 3$ odd. Assume that $(t, q) \neq (2, 2)$. Then there exists an extended cyclic t-divisible code of length $n+1$ and dimension $\frac{n+1}{2}$ over K if and only if one of the following conditions hold true.*

a) *$t = 2$, $q = 4$ and for any prime $p \mid n$ either $s_2(p)$ is odd or $s_4(p)$ is even.*

b) *$t = 4$, $q = 2$ and $n \equiv -1 \bmod 8$ with $s_2(n)$ odd.*

c) $t = 3$, $q = 3$ and $n = 3^m l$ with $3 \nmid l$, $s_3(l)$ odd, $(-1)^{m+1} l \equiv 1 \bmod 3$.

Proof: By the Gleason-Pierce Theorem (see [15] 4.5.7), the existence of a code as stated in the Corollary implies that one of the following conditions hold.

i) $t = 2$, $q = 4$ and C is Hermitian self-dual.

ii) $t = 4$, $q = 2$ and C is Euclidean self-dual. In this case we have $n \equiv -1 \bmod 8$, by Gleason's Theorem (see [15], 6.3.8).

iii) $t = 3$, $q = 3$ and C is Euclidean self-dual.

iv) $t = 2$ and C is equivalent to a 2-fold repetition code.

Clearly, a code in iv) can not be extended cyclic as $n \geq 3$ and the remaining conditions (i) - (iii) follow immediately from 4.6.
To prove the converse, note that, again by 4.6, we have the following.

If a) holds then there exists a Hermitian self-dual extended cyclic code C of length $n + 1$. Let $c = (c_0, c_1, \ldots, c_n) \in C = C^{\perp_2}$. Then

$$0 = [c, c] = \sum_{i=0}^{n} c_i^3 = \sum_{\text{supp}(c)} 1 = \text{wt}(c)$$

implies that $2 \mid \text{wt}(c)$. Thus C is 2-divisible.

If b) holds then there exists a Euclidean self-dual extended cyclic code of length $n + 1$. As $n \equiv -1 \bmod 8$ the code is 4-divisible, by Theorem 3.8 of [10].

If c) holds then there is a Euclidean self-dual extended cyclic code of length $n + 1$. By ([15], 3.1.6), the code is 3-divisible.

References

[1] T. Baicheva, I. Bouyukliev, S. Dodunekov and W. Willems. On the $[10, 5, 6]_9$ Reed-Solomon and Glynn codes. Mathematica Balkanica, New Series, Vol. 18, 67-78 (2004).

[2] `http://www.win.tue.nl/ aeb/voorlincod.html`

[3] W. Feit and J.G. Thompson. Solvability of groups of odd order. Pac. J. Math. 13, 775-1029 (1963).

[4] W. Feit. The representation theory of finite groups, North Holland, Amsterdam 1982.

[5] W.C. Huffman. Codes and groups. Chap. 17 in *Handbook of Coding Theory*, Elsevier, Amsterdam (1998), 1345-1440.

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

[9] F.J. MacWilliams, A.M. Odlyzko, N.J.A. Sloane and H.N. Ward. Self-dual codes over GF(4). J. Combinatorial Theory, Ser. A 25 (1978), 288-318.

[10] Martínez-Pérez and W. Willems. Self-dual codes and modules for finite groups in characteristc two. IEEE Trans. Inform Theory 50 (8) (2004), 1798-1803.

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

[12] M.H.M. Smid. Duadic codes. IEEE Trans. Inform. Theory 33 (3) (1987), 432-433.

[13] J.H. van Lint. Introduction to coding theory. Springer, New York, Heidelberg, Berlin 1982.

[14] H.N. Ward. Quadratic residue codes and divisibility. Chap. 9 in *Handbook of Coding Theory*, Elsevier, Amsterdam (1998), 827-870.

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