Des. Codes Cryptogr. (2012) 62:19–29
DOI 10.1007/s10623-011-9487-z

On the existence of self-dual permutation codes of finite groups

Yun Fan · Guanghui Zhang

Received: 6 September 2010 / Revised: 21 January 2011 / Accepted: 26 January 2011 /
Published online: 20 February 2011

Abstract Motivated by a research on self-dual extended group codes, we consider permutation codes obtained from submodules of a permutation module of a finite group of odd order over a finite field, and demonstrate that the condition "the extension degree of the finite field extended by n'th roots of unity is odd" is sufficient but not necessary for the existence of self-dual extended transitive permutation codes of length $n+1$. It exhibits that the permutation code is a proper generalization of the group code, and has more delicate structure than the group code.

Keywords Group code · Permutation code · Self-dual code · Self-dual module · Extension degree

Mathematics Subject Classification (2000) 94B05 · 11T71

1 Introduction

Let F be a finite field of order q which is a power of a prime integer, and let X be a finite set with cardinality n. By FX we denote the F-vector space with the basis X, and with the usual scalar product as its standard inner product. Any subspace C of FX is just the usual *linear code over F of length n*, and the orthogonal subspace $C^\perp$ of C is called the *dual code* of C. A linear code C is said to be *self-orthogonal* if $C \subseteq C^\perp$, and C is said to be *self-dual* if $C = C^\perp$.

Communicated by P. Charpin.

Y. Fan · G. Zhang
Department of Mathematics, Central China Normal University, Wuhan 430079, China
e-mail: yunfan02@yahoo.com.cn

G. Zhang (✉)
Department of Mathematics, Luoyang Normal University, Luoyang 471022, China
e-mail: zgh09@yahoo.com.cn

Further, if X is a multiplicative group, then FX is an algebra with multiplication induced by the multiplication of the group X, and any left ideal C of the algebra FX, i.e. any FX-submodule of the regular FX-module, is called a *group code* of the group X over the field F. The study on group codes has been there since many years, e.g. [2]. In recent years it has attracted attentions to explore the conditions for the existence of self-dual group codes.

In [9], finite abelian groups were considered and some results on the non-existence of self-dual group codes were shown. For the direct product of a finite 2-group and a finite $2'$-group, reference [5] showed a condition for the nonexistence of self-dual group codes. With the help of the representation theory of finite groups, Willems in [10] gave a necessary and sufficient condition for the existence of self-dual group codes; in particular, it follows that there are no self-dual group codes for finite groups of odd order. One obvious obstruction for the existence of the self-dual group codes of the finite groups of odd order is that the length of the codes is odd.

Thus, Martinez-Pérez and Willems in [7] considered the so-called extended group codes. Assume that X is a finite group of odd order, and extend the set X to $\hat{X}$ which is the union set of X and a single point set, then the vector space $F\hat{X}$ is a module over the algebra FX with the additional single point corresponding to a trivial submodule of dimension 1, and any submodule C of $F\hat{X}$ is called an *extended group code* of the group X. When the characteristic of F is even, Martinez-Pérez and Willems in [7] showed that any one of the following two conditions is necessary and sufficient for the existence of self-dual extended group codes.

- **(C1)**. Every self-dual (in module-theoretical sense) composition factor of the FX-module $F\hat{X}$ has even multiplicity.
- **(C2)**. The extension field of F generated by n'th roots of unity has odd degree over F.

Further, they in [8] demonstrated that, for odd characteristic, the existence of self-dual extended group codes is equivalent to the condition (C2) with an additional condition "$-n$ is a square element in F".

Extending group codes, Y. Fan and Y. Yuan in [3] discussed the so-called *permutation codes* of finite groups. Let G be any finite group and X be any finite G-set. Then FX is an FG-module, called a *permutation module*; any FG-submodule C of FX is said to be a *permutation code* of the G-set X over F. If X is a transitive G-set, then the permutation codes are said to be *transitive*. Group codes are obviously permutation codes since the base set of the group G is a left regular G-set. Some important codes, for example *multiple-cyclic code*, are permutation codes in a natural way but may not be group codes; see [3] for details. Moreover, the research of permutation codes is interesting in a perspective to automorphism groups of linear codes, for: any permutation automorphism of a linear code is just a permutation of the standard basis of the linear code. In [3] some conditions were obtained for the non-existence of the self-dual transitive permutation codes. And, it is also an easy consequence that, for a transitive G-set X with odd length, there is no self-dual transitive permutation codes. Thus, similar to what did in [7], it is reasonable to consider the *extended transitive permutation codes* of X, i.e. the permutation codes of the extended G-set $\hat{X}$ which is the union set of X and a single point set.

Motivated by the research in [7], we are interested in the performance of the two conditions (C1) and (C2) mentioned above for the permutation codes. In an early version of this work we obtained that, when q is even, there exists a self-dual permutation code C of a G-set X over F if and only if every self-dual composition factor of the permutation FG-module FX has even multiplicity. Thanks are given to an anonymous reviewer who suggested that this result has been published in [4, Theorem 2.1], and also suggested us to pay attention to the reference [8].

The performance of the condition (C2) for permutation codes is not so straightforward. In this paper we exhibit its peculiar role for the existence of self-dual extended transitive permutation codes. The outline is as follows.

In Sect. 2 we explain our notation precisely and state some related known results as our preliminaries.

The main purpose of Sect. 3 is to prove that, for a group G of odd order and a transitive G-set X with length n coprime to the order q of F, the condition (C2), and with the additional condition "$-n$ is a square element of F" if q is odd, is sufficient for the existence of self-dual extended transitive permutation codes. This is a generalization of the sufficiency part of the corresponding result for group codes in the references [7,8], but our argument is different from that in [7,8]. An analysis of idempotents takes an important part in [7,8], but it is not applicable to our case.

In Sect. 4 we present some examples to show that the condition (C2) is not necessary for the existence of self-dual extended transitive permutation codes.

The peculiar behavior of the condition (C2) for permutation codes exhibits that the notion of permutation codes is a deeply extensive generalization of the group codes, and the structure of permutation codes is more delicate than that of group codes.

2 Preliminaries

In this section we explain the necessary notation and state some related known results as a preparation.

Let X be a finite set and $n := |X|$, the cardinality of the set X. Let FX be the vector space over F with basis X. Any vector $\mathbf{w} = \sum_{x\in X} w_x\, x$ with $w_x \in F$ of FX is also called a *word* of length n over F. The *standard inner product* on FX with respect to the basis X is defined as follows:

$$\langle \mathbf{w},\ \mathbf{w}'\rangle = \sum_{x\in X} w_x w'_x, \quad \forall\, \mathbf{w} = \sum_{x\in X} w_x x,\ \ \mathbf{w}' = \sum_{x\in X} w'_x x \in FX.$$

In the following we assume that G is a finite group and there is a group homomorphism $G \to \mathrm{Sym}(X)$, where $\mathrm{Sym}(X)$ denotes the group consisting of all permutations of X; in that case, X is called a *G-set*. Then any $g \in G$ is mapped to a permutation of X, denoted by g again in short. With the linear extension of the G-action on X, the F-vector space FX becomes an FG-module, called a *permutation FG*-module with permutation basis X; see [1, §12].

We say that C is a *permutation code* of the G-set X over F, or a *permutation code* of FX in short, if C is an FG-submodule of the permutation FG-module FX; in that case we denote $C \le FX$. Further, if X is a transitive G-set, then any $C \le FX$ is said to be a *transitive permutation code*.

Moreover, the standard inner product on the vector space FX is *G-invariant*, since it is easy to check that

$$\langle g(\mathbf{w}),\ g(\mathbf{w}')\rangle = \langle \mathbf{w},\ \mathbf{w}'\rangle, \qquad \forall\, g \in G,\ \forall\, \mathbf{w}, \mathbf{w}' \in FX;$$

or equivalently,

$$\langle g(\mathbf{w}),\ \mathbf{w}'\rangle = \langle \mathbf{w},\ g^{-1}(\mathbf{w}')\rangle, \qquad \forall\, g \in G,\ \forall\, \mathbf{w}, \mathbf{w}' \in FX.$$

As a consequence, the dual code $C^{\perp} := \{\mathbf{w} \in FX \mid \langle \mathbf{c}, \mathbf{w}\rangle = 0,\ \forall\, \mathbf{c} \in C\}$ of the permutation code C is G-invariant hence a permutation code too.

Remark 2.1 As a diversion, we recall some notation from the module theory over the algebra FG, and emphasize that the words “dual”, “self-dual” have different explanations in module theory.

(i) A bilinear form $f(u, v)$ on an FG-module V is said to be *G-invariant* if $f(gu, gv) = f(u, v)$, $\forall u, v \in V$, $\forall g \in G$. Any pair (V, f) of an FG-module V and a G-invariant non-degenerate bilinear form f on V is called a *metric FG-module*; further, (V, f) is called a *symmetric FG*-module if f is symmetric. A map α between two metric FG-modules (V, f) and (V', f') is said to be an *isometry* if α is an FG-isomorphism and $f'(\alpha u, \alpha v) = f(u, v)$, $\forall u, v \in V$.

(ii) For any FG-module V, the dual space $V^* := \mathrm{Hom}_F(V, F)$, which denotes the F-space of all linear forms on V, becomes an FG-module in a natural way: for $g \in G$ and $\lambda \in V^*$, the $g\lambda \in V^*$ is defined by $(g\lambda)(v) = \lambda(g^{-1}v)$ for all $v \in V$; the FG-module V^* is called the *dual module* of V. If the FG-module V is isomorphic to its dual module V^*, then we say that V is a *self-dual module*. It is known that an FG-module V is self-dual if and only if V can become a metric FG-module (V, f); see [6, Chap. VII, §8] for details.

(iii) Let (V, f) be a symmetric FG-module and U be a submodule of V. From the G-invariance of f, it follows that the orthogonal subspace $U^\perp := \{v \in V \mid f(u, v) = 0, \forall\, u \in U\}$ is a submodule too. If $U \cap U^\perp = 0$ (equivalently, the restriction of f on U is non-degenerate) then we say that U is a *non-degenerate* submodule; in that case we have an orthogonal direct sum $V = U \oplus U^\perp$. On the other hand, if $U \subseteq U^\perp$ (equivalently, the restriction of f on U is zero) then we say that U is an *isotropic* submodule. If $U = U^\perp$ then we say that U is a *hyperbolic submodule*. If V has a hyperbolic submodule then we say that V is a *hyperbolic FG*-module. We mention two related known conclusions.

Proposition 2.1 *Let (V, f) be a symmetric FG-module.*

(i) If any composition factor of V is not self-dual, then V is hyperbolic.
(ii) Assume that $q = |F|$ is even. Then V is hyperbolic if and only if any self-dual composition factor of V has even multiplicity.

A key idea for the proof is that for any submodule W of V we have the following exact sequence of FG-homomorphisms

$$0 \longrightarrow W^\perp \longrightarrow V \longrightarrow W^* \longrightarrow 0,$$

where the third arrow maps $v \in V$ to the linear form $f(-, v)$ in W^*. The above conclusion (i) follows from it by taking W to be an irreducible submodule of V and by induction on the composition length. The conclusion (ii) is proved as the same as [4, Theorem 2.1], i.e. it can be shown that an isotropic irreducible submodule W exists, and then the same argument for (i) works well.

Return to the permutation codes of the G-set X over F. The following is just [4, Theorem 2.1].

Corollary 2.1 *Assume that $q = |F|$ is even. Then there exists a self-dual permutation code of FX if and only if any self-dual composition factor of the FG-module FX has even multiplicity.*

Next, we always denote ξ_n a primitive n'th root of unity, and denote $F(\xi_n)$ the extension over F generated by ξ_n. We restate [8, Theorem 3.9] (which covers the even characteristic version [7, Theorem 3.3]) as follows.

Proposition 2.2 *Assume that the order $n := |G|$ is odd and coprime to $q = |F|$. Then there exists a self-dual extended group code of G over F if and only if the degree $|F(\xi_n) : F|$ is odd and $-n$ is a square element in F.*

Remark 2.2 (i) When the integer n is odd and coprime to q, the extension degree $|F(\xi_n) : F|$ is just the order of q in $(\mathbf{Z}/n\mathbf{Z})^\times$, which denotes the multiplicative group consisting of the reduced residue classes of the integer ring $\mathbf{Z}$ modulo n; from Chinese Remainder Theorem it is easy to check that $|F(\xi_n) : F|$ *is odd if and only if for any prime factor p of n the order of q in $(\mathbf{Z}/p\mathbf{Z})^\times$ is odd*. There are related discussions in [7].

(ii) Assume that r is the prime such that $q = r^l$, i.e. the integer residual ring $\mathbf{Z}/r\mathbf{Z}$ modulo r is the unique minimal subfield of F. It follows from Galois theory that $-n$ is a square element in F if and only if either $-n$ is a square residue in $\mathbf{Z}/r\mathbf{Z}$ or the degree $|F : (\mathbf{Z}/r\mathbf{Z})|$ is even. See [8, Lemma 3.6]. In particular, this condition is trivial (i.e. always holds) if $r = 2$.

We will cite two special conclusions for group codes.

Lemma 2.1 *Let G be an abelian p-group where p is a prime coprime to q.*

(i) If $|F(\xi_p) : F|$ is even, then any irreducible FG-module is self-dual.
(ii) If $|F(\xi_p) : F|$ is odd, then any non-trivial irreducible FG-module is not self-dual.

Proof The conclusions are essentially included in [8]. One can also check them straightforwardly from the following two points:

- Any non-trivial irreducible representation of G over F can be realized as a homomorphism from a cyclic quotient group $G/H = \langle gH \rangle$ to an extension field $F(\xi_\ell)$, where $\ell = |G/H|$, by mapping the generator gH of the cyclic quotient group to ξ_ℓ.
- This representation is self-dual if and only if $|F(\xi_\ell) : F|$ is even; in that case, the unique Galois transformation of order 2 of $F(\xi_\ell)$ over F induces the isomorphism between the representation and its dual representation. □

3 Self-dual extended transitive permutation codes

In this section we show a sufficient condition for the existence of self-dual extended transitive permutation codes. We need a general elementary result on induced permutation codes.

Let G be any finite group and H be a subgroup of G, and let Y be a finite H-set. Then FY is a permutation FH-module. We have the *induced FG-module*

$$\mathrm{Ind}_H^G(FY) = FG \bigotimes_{FH} FY = \bigoplus_{t\in T} t \otimes FY,$$

where T is a representative set of the left cosets of G over H, and $\mathrm{Ind}_H^G(FY)$ is a vector space with basis

$$X := \mathrm{Ind}_H^G(Y) = \bigcup_{t\in T} t \otimes Y = \bigcup_{t\in T} \{t \otimes y \mid y \in Y\},$$

which is a G-set with G-action as follows:

$$g(t \otimes y) = t_g \otimes t_g^{-1} gty, \qquad \forall\, g \in G,\ t \in T,\ y \in Y,$$

where t_g is the representative of the unique left coset $t_g H$ such that $gt \in t_g H$, or equivalently $t_g^{-1} gt \in H$. We say that $\mathrm{Ind}_H^G(FY)$ is the *induced permutation FG-module* with the *induced G-set* $\mathrm{Ind}_H^G(Y)$.

Lemma 3.1 *Notation as above, and let D be any permutation code of the FH-permutation module FY. Then*

$$\mathrm{Ind}_H^G(D)^\perp = \mathrm{Ind}_H^G(D^\perp).$$

Proof It is obvious that the induced module $C := \mathrm{Ind}_H^G(D)$ is a submodule of $\mathrm{Ind}_H^G(FY) = \bigoplus_{t\in T} t \otimes FY$, and we have a direct decomposition of F-spaces:

$$\mathrm{Ind}_H^G(D) = \bigoplus_{t\in T} t \otimes D,$$

with each $t \otimes D$ being an F-subspace of $t \otimes FY$. Each $t \otimes FY$ is an F-space with bases $t \otimes Y$, hence with the standard inner product:

$$\left\langle \sum_{y\in Y} a_y(t \otimes y), \sum_{y\in Y} b_y(t \otimes y) \right\rangle = \sum_{y\in Y} a_y b_y,$$

and

$$FY \longrightarrow t \otimes FY, \quad \sum_{y\in Y} a_y y \longmapsto \sum_{y\in Y} a_y(t \otimes y),$$

is an isometric F-isomorphism. With respect to the isometries, it is clear that $(t \otimes D)^\perp = t \otimes D^\perp$; hence

$$\mathrm{Ind}_H^G(D)^\perp = \bigoplus_{t\in T}(t \otimes D)^\perp = \bigoplus_{t\in T} t \otimes D^\perp = \mathrm{Ind}_H^G(D^\perp).$$

□

Remark 3.1 By the same argument, we can get that, if (U, f) is a metric FH-module, then $V := \mathrm{Ind}_H^G(U)$ is a metric FG-module with the "induced metric" $\tilde{f}(t\otimes u, t'\otimes u') = f(u, u')$ if $t = t'$, and $= 0$ otherwise. In particular, the induced module of a self-dual module is self-dual too.

Next, we convert the question on self-dual extended transitive permutation codes into a question on transitive permutation codes itself.

Let G be any finite group, and let X be a transitive G-set with length $n := |X|$ coprime to q. In the permutation module FX, the element $e_X := \sum_{x\in X} x$ is G-fixed and non-isotropic, hence the subspace Fe_X is a non-degenerate trivial FG-submodule; so the orthogonal subspace $(Fe_X)^\perp$ is a non-degenerate FG-submodule, and we have an orthogonal direct sum $FX = (Fe_X) \oplus (Fe_X)^\perp$.

Remark 3.2 For any transitive G-set X, it is known that

$$\mathrm{Hom}_{FG}(FX, F) \cong F, \tag{1}$$

where F denotes the trivial FG-module and $\mathrm{Hom}_{FG}(FX, F)$ denotes the F-space of all FG-homomorphisms from FX to F. Noting that FX may be not semisimple, we sketch a proof for reference. Let H be the stabilizer in G of $x_1 \in X$; then the permutation module $FX \cong FG \otimes_{FH} F$ and

$$\mathrm{Hom}_{FG}(FG \otimes_{FH} F, F) \cong \mathrm{Hom}_{FH}(F, \mathrm{Hom}_{FG}(FG, F));$$

further, $\mathrm{Hom}_{FG}(FG, F) \cong F$ since F appears in $FG/J(FG)$ exactly once, where $J(FG)$ denotes the radical of FG; thus we get the formula (1).

Return to our case where $n := |X|$ is coprime to q, we have that

$$\mathrm{Hom}_{FG}\Big((Fe_X)^{\perp},\ F\Big) = 0. \tag{2}$$

Further, let $\hat{X} = X \cup \{x_0\}$ be the extended G-set, where $x_0 \notin X$ and x_0 is G-fixed. At these contexts, FX is a non-degenerate submodule of $F\hat{X}$, and the above notation $(Fe_X)^{\perp}$ should be replaced by $\mathrm{Ann}_{FX}(Fe_X)$, which denotes the subspace of all the vectors in FX (with the vectors outside FX excluded) which are orthogonal to Fe_X.

Lemma 3.2 *Let notation be as above. The following two are equivalent:*

(i) There is a permutation code C of FX such that $C^{\perp} = C \oplus Fe_X$ and $-n$ is a square element of F.

(ii) There is a self-dual permutation code $\hat{C}$ of $F\hat{X}$.

Proof Note that we have an orthogonal direct sum:

$$F\hat{X} = \mathrm{Ann}_{FX}(Fe_X) \oplus Fe_X \oplus Fx_0.$$

(i) $\Rightarrow$ (ii) It is clear that $C \subseteq \mathrm{Ann}_{FX}(Fe_X)$. By [8, Lemma 3.5] there is an isotropic element $e_0 \in Fe_X \oplus Fx_0$, hence $C \oplus Fe_0$ is a self-dual permutation code of $F\hat{X}$; cf. the proof in [8, Theorem 3.9].

(ii) $\Rightarrow$ (i) Set $C = \hat{C} \cap \mathrm{Ann}_{FX}(Fe_X)$. By the formula (2) we have

$$\hat{C} = \hat{C} \cap (\mathrm{Ann}_{FX}(Fe_X) \oplus (Fe_X \oplus Fx_0)) = C \oplus \Big(\hat{C} \cap (Fe_X \oplus Fx_0)\Big).$$

So C is a hyperbolic submodule of $\mathrm{Ann}_{FX}(Fe_X)$, hence $\mathrm{Ann}_{FX}(C) = C \oplus Fe_X$; and $\hat{C} \cap (Fe_X \oplus Fx_0)$ is a hyperbolic submodule of $Fe_X \oplus Fx_0$, hence $-n$ is a square element of F (see [8, Lemma 3.5]). □

As mentioned in Introduction, the permutation code $\hat{C}$ is called an *extended permutation code of X over F*.

We come to the main result of this section.

Theorem 3.1 *Let G be a finite group of odd order, and let X be a transitive G-set with length n coprime to $q = |F|$. If the extension degree $|F(\xi_n) : F|$ is odd, then there exists a permutation code C of FX such that $C^{\perp} = C \oplus Fe_X$.*

Proof We prove it by induction on the order of G. It is trivial for $|G| = 1$. Assume $|G| > 1$. Let $x_1 \in X$ and H be the stabilizer of x_1 in G. Then H is a subgroup and $FX = \mathrm{Ind}_H^G(F)$. Since G is solvable by Feit-Thompson Odd Order Theorem, a minimal normal subgroup A of G is an elementary abelian p-group, where p is a prime. Since A is normal, the product AH is a subgroup of G. There are three cases.

Case 1: $AH = H$. Then $A \subseteq H$, and hence A is contained in every conjugate of H. Thus A acts trivially on X, and X is a G/A-set and FX is a permutation module over G/A. Since $|G/A| < |G|$, the conclusion follows by induction.

Case 2: $AH = G$. Since $A \cap H$ is both normal in H and in A, we have that $A \cap H$ is normal in $AH = G$; but A is a minimal normal subgroup of G, so either $A \cap H = A$ or $A \cap H = 1$. If $A \cap H = A$, then $H \subseteq A$ and $FX \cong F(A/H)$ is a regular module of the group algebra

$F(A/H)$, the conclusion is known in [8] (one can also deduce it by Lemma 2.1 directly). Thus we assume that $A \cap H = 1$. Then we have a bijection

$$\beta : A \longrightarrow X, \quad a \longmapsto a(x_1).$$

Let A act on A by left translation, and let H act on A by conjugation, hence $G = AH$ is mapped into the group $\mathrm{Sym}(A)$ of all permutations of A:

$$(bh)(a) = bhah^{-1}, \qquad \forall\, a, b \in A,\ h \in H.$$

Noting that H stabilizes x_1, we have that

$$\beta\left((bh)(a)\right) = (bhah^{-1})(x_1) = bha(x_1) = (bh)\beta(a).$$

Thus, mapping $bh \in G$ to the permutation $a \mapsto bhah^{-1}$ of A is an action of G on A, and β is an isomorphism of G-sets. Then $n = |A|$ hence $p|n$, so p is coprime to q. By Lemma 2.1(ii), the regular FA-module

$$FA = F \oplus W_1 \oplus \cdots \oplus W_m,$$

where $W_1, \ldots, W_m$ are non-self-dual irreducible FA-modules. Then taking dual $W_j \mapsto W_j^*$ is a permutation of $W_1, \ldots, W_m$. The action of H on FA permutes the irreducible summands of FA, and any H-orbit $\{W_{i_1}, \ldots, W_{i_k}\}$ forms exactly an irreducible FG-submodule $W_{i_1} + \cdots + W_{i_k}$, which is self-dual if and only if $\{W_{i_1}^*, \ldots, W_{i_k}^*\} = \{W_{i_1}, \ldots, W_{i_k}\}$, in particular, k is even. However, H has odd order, hence the length k of the H-orbit is odd. In conclusion, FX is a direct sum of irreducible FG-submodules and any irreducible FG-summand other than F is not self-dual; hence, by Proposition 2.1(i), there is an FG-submodule C of FX such that $C^\perp = C \oplus F$.

Case 3: $H \lneqq AH \lneqq G$. In this case,

$$FX \cong \mathrm{Ind}_H^G(F) = \mathrm{Ind}_{AH}^G \mathrm{Ind}_H^{AH}(F).$$

Let $Y = \{gx_1 \mid g \in AH\}$, then Y is an AH-set and the permutation $F(AH)$-module $FY \cong \mathrm{Ind}_H^{AH}(F)$. By induction, there is a code $D \le FY$ such that $D^\perp = D \oplus Fe_Y$ where $e_Y = \sum_{y \in Y} y$. Turn to the permutation module $FX = \mathrm{Ind}_{AH}^G(FY)$, by Lemma 3.1, we have

$$\mathrm{Ind}_{AH}^G(D)^\perp = \mathrm{Ind}_{AH}^G(D^\perp) = \mathrm{Ind}_{AH}^G(D \oplus Fe_Y) = \mathrm{Ind}_{AH}^G(D) \oplus \mathrm{Ind}_{AH}^G(Fe_Y).$$

Noting that Fe_Y is a trivial $F(AH)$-module, by induction again, there is a code $E \le \mathrm{Ind}_{AH}^G(Fe_Y)$ such that

$$\mathrm{Ann}_{\mathrm{Ind}_{AH}^G(Fe_Y)}(E) = E \oplus Fe_X,$$

where $e_X = \sum_{x \in X} x$. So we can write $\mathrm{Ind}_{AH}^G(Fe_Y) = E' \oplus E \oplus Fe_X$ and

$$\mathrm{Ind}_{AH}^G(D)^\perp = \mathrm{Ind}_{AH}^G(D) \oplus \mathrm{Ind}_{AH}^G(Fe_Y) = \mathrm{Ind}_{AH}^G(D) \oplus E' \oplus E \oplus Fe_X.$$

Let

$$C = \mathrm{Ind}_{AH}^G(D) \oplus E.$$

Then C is a permutation code of FX and

$$\begin{aligned} C^{\perp} &= \mathrm{Ind}_{AH}^{G}(D)^{\perp} \bigcap E^{\perp} = \mathrm{Ann}_{FX}\left(\mathrm{Ind}_{AH}^{G}(D)\right) \bigcap \mathrm{Ann}_{FX}(E) \\ &= \left(\mathrm{Ind}_{AH}^{G}(D) \oplus E' \oplus E \oplus Fe_X\right) \bigcap \mathrm{Ann}_{\mathrm{Ind}_{AH}^{G}(D)\oplus E'\oplus E\oplus Fe_X}(E) \\ &= \left(\mathrm{Ind}_{AH}^{G}(D) \oplus E' \oplus E \oplus Fe_X\right) \bigcap \left(\mathrm{Ind}_{AH}^{G}(D) \oplus E \oplus Fe_X\right) \\ &= \mathrm{Ind}_{AH}^{G}(D) \oplus E \oplus Fe_X \\ &= C \oplus Fe_X. \end{aligned}$$

□

As a consequence of Theorem 3.1 and Lemma 3.2, we have the following at once.

Corollary 3.1 *Let notation be as in Theorem 3.1. If $|F(\xi_n) : F|$ is odd and $-n$ is a square element of F, then there is a self-dual extended transitive permutation code of X over F.* □

Taking X to be the regular G-set, we get the sufficiency part of [8, Theorem 3.9] again. If $q = |F|$ is even, by Remark 2.2(ii) we have the following consequence.

Corollary 3.2 *Let notation be as in Theorem 3.1; further assume that $q = |F|$ is even. If $|F(\xi_n) : F|$ is odd, then there is a self-dual extended transitive permutation code of X over F.* □

Taking X to be the regular G-set, we get the sufficiency part of [7, Theorem 3.3] again.

4 Examples

In this section, we present some examples to show that the condition "$|F(\xi_n) : F|$ is odd" in Theorem 3.1 is not necessary for the existence of self-dual extended transitive permutation codes. It exhibits that the notion of permutation codes is a deeply extensive generalization of the group codes, and the structure of permutation codes is more delicate than that of group codes.

Example 4.1 Let $F = F_2 := \mathbf{Z}/2\mathbf{Z}$ be the binary field and P be the elementary abelian 5-group of order 5^3, hence P can be viewed as a 3-dimensional vector space over $F_5 := \mathbf{Z}/5\mathbf{Z}$ (the finite field of order 5). Since $5^3 - 1 = 124 = 4 \cdot 31$, the extension $F_5(\xi_{31})$ generated by a primitive 31'st root of unity has degree 3 over F_5; hence $F_5(\xi_{31}) \cong P$ as F_5-vector spaces. Multiplying by ξ_{31}, we get an F_5-linear automorphism of order 31 of the F_5-vector space $F_5(\xi_{31})$; correspondingly, we have an automorphism σ of order 31 of the elementary 5-group P, and there is no proper subspace which is σ-invariant; cf. the proof of Lemma 2.1. Let $S = \langle\sigma\rangle$ be the cyclic group generated by σ, and let $G = P \rtimes S$ be the semidirect product. Take a subgroup H of order 5 of P, and let X be the set of all left cosets of G over H. Then we have that $|S| = 31$, $|G| = 5^3 \cdot 31$ and X is a transitive G-set of length $5^2 \cdot 31$. Consider permutation codes of the transitive G-set X over the binary field F_2. It is clear that $|F_2(\xi_5) : F_2| = 4$ is even, consequently, $|F_2(\xi_{5^2\cdot 31}) : F_2|$ is even (see Remark 2.2); but we have the orthogonal direct sum $F_2X = (F_2e_X)^{\perp} \oplus F_2e_X$, where $e_X := \sum_{x\in X} x$ as before, and we can show that

(∗) *any self-dual composition factor of $(F_2e_X)^{\perp}$ has even multiplicity.*

By Proposition 2.1 and Lemma 3.2, this implies that there is a self-dual extended transitive permutation code of X over F_2.

Proof of the conclusion $(*)$ Since the number of maximal subgroups (i.e. the subgroups of order 5^2) of P is $(5^3-1)/(5-1)=31$ and the stabilizer in S of any maximal subgroup of P is trivial, we see that all the maximal subgroups form exactly one S-orbit. For the given subgroup H of order 5, the number of the maximal subgroups of P which contain H is $(5^2-1)/(5-1)=6$; by M_i, $1\le i\le 6$, we denote the 6 maximal subgroups. Then for any $1\le i, j\le 6$ there is an element of S which permutes M_i by conjugation to M_j.

Note that F_2X is isomorphic to the induced module:

$$F_2X \cong \mathrm{Ind}_H^G(F_2) = \mathrm{Ind}_P^G\left(\mathrm{Ind}_H^P(F_2)\right),$$

and $\mathrm{Ind}_H^P(F_2)$ is just the regular module of the algebra $F_2(P/H)$; hence each M_i, $1\le i\le 6$, contributes to $\mathrm{Ind}_H^P(F_2)$ the direct summand $F_2(P/M_i)=F_2\oplus W_i$ with W_i being a self-dual irreducible factor (recall that $|F_2(\xi_5):F_2|=4$ is even and W_i is corresponding to the representation by mapping a generator of the cyclic group P/W_i of order 5 to the 5'th root ξ_5 of unity in $F_2(\xi_5)$, see Lemma 2.1 and its proof). So we get $\mathrm{Ind}_H^P(F_2)=F_2\bigoplus\left(\bigoplus_{i=1}^6 W_i\right)$, and

$$F_2X \cong \mathrm{Ind}_P^G(F_2)\bigoplus\left(\bigoplus_{i=1}^{6}\mathrm{Ind}_P^G(W_i)\right).$$

Since the stabilizer in S of W_i is trivial, $\mathrm{Ind}_P^G(W_i)$ is an irreducible F_2G-module. Since W_i is self-dual (see Lemma 2.1(i)), $\mathrm{Ind}_P^G(W_i)$ is self-dual (see Remark 3.1). And, since M_i for $1\le i\le 6$ are conjugate to each other by S, we conclude that $\mathrm{Ind}_P^G(W_i)$ for $1\le i\le 6$ are isomorphic to each other. Finally, $\mathrm{Ind}_P^G(F_2)$ is isomorphic to the regular module of the algebra $F_2(G/P)\cong F_2S$, and the degree $|F_2(\xi_{31}):F_2|=5$ is odd, by Lemma 2.1 (ii), $\mathrm{Ind}_P^G(F_2)=F_2\oplus U$ and any composition factor of U is not self-dual. □

In fact, by a similar argument we can obtain a collection of examples, including the odd characteristic case. We state it and sketch a proof.

Example 4.2 Take three positive integers q, p, k satisfying the following three conditions:

(i) q is a power of a prime, and p is an odd prime coprime to q;
(ii) $s:=(p^k-1)/(p-1)$ is an odd prime coprime to q (so k must be odd);
(iii) q has even order modulo p, while has odd order modulo s.

Let $F=F_q$ be the finite field with q elements, P be an elementary abelian p-group of order p^k, and S be a Sylow s-subgroup of the automorphism group of P. Let $G=P\rtimes S$ be the semidirect product of P by S, let H be a subgroup of P of order p, and let X be the set of all left cosets of G over H. Then G is a finite group of odd order, X is a transitive G-set with length $|X|=p^{k-1}s$ which is odd, and $|F(\xi_p):F|$ is even (while $|F(\xi_s):F|$ is odd); but we have that

$(**)$ *any non-trivial self-dual composition factor of the permutation FG-module FX has even multiplicity.*

Proof of the conclusion $(**)$ Since s is a prime, s does not divide p^j-1 for any $j<k$; hence $S=\langle\sigma\rangle$ is a cyclic group of order s, where σ is constructed similarly to that in Example 4.1; and S acts on P irreducibly and permutes all maximal subgroups of P transitively.

The number of the maximal subgroups of P which contain H is $m = \frac{p^{k-1}-1}{p-1}$; by M_i, $1 \leq i \leq m$, we denote the m maximal subgroups. Since $k-1$ is even, m is even too. Since $|F(\xi_p) : F|$ is even, $F(P/M_1) = F \bigoplus \left(\bigoplus_{j=1}^{l} W_{1j}\right)$ with any W_{1j} being a self-dual irreducible module, see Lemma 2.1(i). For any M_i with $1 \leq i \leq m$ there is a $\sigma_i \in S$ such that $M_i = \sigma_i(M_1)$, thus the module $F(P/M_i) = F \bigoplus \left(\bigoplus_{j=1}^{l} W_{ij}\right)$ with $W_{ij} = \sigma_i(W_{1j})$.

Therefore $\mathrm{Ind}_H^P(F) = F \bigoplus \left(\bigoplus_{i=1}^{m} \bigoplus_{j=1}^{l} W_{ij}\right)$, and

$$FX \cong \mathrm{Ind}_H^G(F) = \mathrm{Ind}_P^G(F) \bigoplus \left(\bigoplus_{j=1}^{l} \bigoplus_{i=1}^{m} \mathrm{Ind}_P^G(W_{ij}) \right).$$

Similar to Example 4.1, any non-trivial composition factor of $\mathrm{Ind}_P^G(F)$ is not self-dual, while any $\mathrm{Ind}_P^G(W_{ij})$ is a self-dual irreducible module; and for any j, the factors $\mathrm{Ind}_P^G(W_{1j}), \ldots, \mathrm{Ind}_P^G(W_{mj})$ are isomorphic to each other.

However, $W_{1j'}$ is not S-conjugate to W_{1j} for $1 \leq j' \neq j \leq l$; otherwise $\sigma'(W_{1j'}) \cong W_{1j}$ for a non-identity $\sigma' \in S$ and, considering the kernel of $\sigma'(W_{1j'})$ which is $\sigma'(M_1)$, we get an impossible equality $\sigma'(M_1) = M_1$. Thus, $\mathrm{Ind}_P^G(W_{ij'})$ is not isomorphic to $\mathrm{Ind}_P^G(W_{ij})$ provided $j' \neq j$ (this is the only key point which does not appear in Example 4.1).

To sum up, any non-trivial self-dual composition factor of the permutation FG-module FX has multiplicity m which is even. □

Example 4.1 is just one member of the collection of Example 4.2 for $q = 2$, $p = 5$, $k = 3$ (hence $s = 31$). Also, we can take $q = 53$, $p = 3$, $k = 3$ (hence $s = 13$), that is an example for odd characteristic.

Acknowledgments The authors are grateful to Professor Ping Jin from Shanxi University for many useful discussions. Many thanks are given to the anonymous reviewers for their valuable comments which have helped us to renew and improve this paper. This work is supported by Natural Science Foundation of China, Grant No. 10871079.

References

1. Alperin J.L., Bell R.B.: Groups and representations, GTM 13. Springer-Verlag, Berlin (1995).
2. Bernhardt F., Landrock P., Manz O.: The extended Golay codes considered as ideals. J. Comb. Theory Ser. A **55**(2), 235–246 (1990).
3. Fan Y., Yuan Y.: On self-dual permutation codes. Acta Math. Sci. 28B **3**, 633–638 (2008).
4. Günther A., Gabriele N.: Automorphisms of doubly even self-dual codes. Bull. Lond. Math. Soc. **41**, 769–778 (2009).
5. Hughes G.: Structure theorems for group ring codes with an application to self-dual codes. Des. Codes Cryptogr. **24**, 5–14 (2001).
6. Huppert B., Blackburn N.: Finite Groups II. Springer-Verlag, Berlin (1982).
7. Martinez-Pérez C., Willems W.: Self-dual codes and modules for finite groups in characteristic two. IEEE Trans. Inform. Theory **50**(8), 1798–1803 (2004).
8. Martinez-Pérez C., Willems W.: Self-dual extended cyclic codes. Appl. Algebra Eng. Com. Comp. **17**, 1–16 (2006).
9. Rajan B.S., Siddiqi M.U.: A generalized DFT for abelian codes over $\mathbf{Z}_m$. IEEE Trans. Inform. Theory **40**, 2082–2090 (1994).
10. Willems W.: A note on self-dual group codes. IEEE Trans. Inform. Theory **48**, 3107–3109 (2002).