Available online at www.sciencedirect.com
ScienceDirect
Acta Mathematica Scientia 2008,**28B**(3):633–638
Acta Mathematica Scientia 数学物理学报
http://actams.wipm.ac.cn

ON SELF-DUAL PERMUTATION CODES*

Fan Yun (樊恽)
School of Mathematics and Statistics, Central China Normal University, Wuhan 430079, China
E-mail: yunfan@whu.edu.cn
Yuan Yuan (袁媛)
School of Informatics, Guangdong University of Foreign Studies, Guangzhou 510006, China
E-mail: yuanliuyuan79@163.com

Abstract Permutation codes over finite fields are introduced, some conditions for existence or non-existence of self-dual permutation codes are obtained.

Key words Finite field, group code, permutation code, self-dual code

2000 MR Subject Classification 94B15

1 Introduction

Let $\mathbf{F}$ be a finite field of order $q = p^l$, where p is a prime, and X be a finite set; by $\mathbf{F}X$ we denote the $\mathbf{F}$-vector space with basis X; and any subspace C of $\mathbf{F}X$ is said to be a linear code over $\mathbf{F}$. Further, if X is a group, then $\mathbf{F}X$ is an algebra with multiplication induced from the multiplication of X, which is called the group algebra of the group X over $\mathbf{F}$; and any left ideal C of $\mathbf{F}X$ is said to be a group code. On the other hand, with respect to the basis X of the vector space $\mathbf{F}X$, we have a standard inner product on $\mathbf{F}X$, and the orthogonal subspace $C^{\perp}$ of a linear code C is called the dual code of C; we call C a self-dual code if $C = C^{\perp}$. It is an interesting question to find conditions such that a group algebra has self-dual group codes. In general, this question can be extended to the group algebras over finite rings.

In [1], finite abelian groups were considered and some results on the non-existence of self-dual group codes were shown. For direct products of finite 2-groups and finite $2'$-groups, reference [2] showed that the self-dual group codes do not exist. Using the representation theory of finite groups, for group algebras over finite Galois rings reference [3] gave a complete answer for this question.

Extending group codes, in this note we introduce permutation codes of finite groups, and study self-dual permutation codes. We obtain some conditions for the existence or non-existence of the self-dual permutation codes of finite groups. Our results extend the results mentioned above in the case of finite fields. In particular, for direct products of finite 2-groups and finite $2'$-groups, we have a complete answer for the question.

*Received October 30, 2005; Revised June 26, 2006. Project supported by the National Program of Basic Sciences (G19990751)

In the next section we introduce the permutation codes and some general facts. In Section 3 we state and prove the main results.

2 Permutation Codes

Let $\mathbf{F}$ be a finite field of order $q = p^l$, where p is a prime; let G be a finite group. Let X be a finite G-set, that is, X is a finite set and there is a G-action on X, namely, a map $G \times X \to X$, $(s, x) \mapsto sx$, satisfying that $(ss')x = s(s'x)$ for all $s \in G$ and all $x \in X$, and that $1x = x$ for all $x \in X$.

Let $\mathbf{F}X = \{ \sum_{s\in X} a_s\, s \mid a_s \in \mathbf{F} \}$ be the $\mathbf{F}$-vector space with basis X. Extending the G-action on X linearly, $\mathbf{F}X$ becomes an $\mathbf{F}G$-module, called an $\mathbf{F}G$-permutation module, cf. [4, §12].

Definition 1 We say that C is a G-permutation code of $\mathbf{F}X$, denoted by $C \le \mathbf{F}X$, if C is an $\mathbf{F}G$-submodule of the $\mathbf{F}G$-permutation module $\mathbf{F}X$.

Example 1 Any finite group G is a G-set by left multiplication, that is, left translation; and the regular module of the group algebra $\mathbf{F}G$ is an $\mathbf{F}G$-permutation module. A permutation code $C \le \mathbf{F}G$ is just a left ideal of the group algebra $\mathbf{F}G$, which is just the so-called group code in Introduction.

Example 2 Let $G = \{1, s, \cdots, s^{n-1}\} \cong \mathbf{Z}_n$ be a cyclic group of order n. Let $X = \overbrace{G \cup \cdots \cup G}^{m}$ which is a G-set by left translation. Then,

$$\begin{aligned}\mathbf{F}X &= \overbrace{\mathbf{F}G \oplus \cdots \oplus \mathbf{F}G}^{m} \\ &= \Big\{ (a_{00} + a_{01}s + \cdots + a_{0,n-1}s^{n-1}, \cdots, a_{n-1,0} + a_{n-1,1}s + \cdots + a_{n-1,n-1}s^{n-1}) \\ &\qquad \Big| a_{ij} \in \mathbf{F} \Big\}.\end{aligned}$$

Then, a subset $C \subseteq \mathbf{F}X$ is a permutation code if and only if for any

$$(c_{00}, c_{01}, \cdots, c_{0,n-1},\ \cdots,\ c_{n-1,0}, c_{n-1,1}, \cdots, c_{n-1,n-1}) \in C,$$

we have

$$(c_{0,n-1}, c_{00}, \cdots, c_{0,n-2},\ \cdots,\ c_{n-1,n-1}, c_{n-1,0}, \cdots, c_{n-1,n-2}) \in C,$$

that is, if and only if C is a so-called m-cyclic code.

This example shows that, though group codes can be recognized as permutation codes, the permutation codes may be not group codes.

The $\mathbf{F}$-vector space $\mathbf{F}X$ is equipped with a non-degenerate symmetric bilinear form

$$\Big\langle \sum_{x\in X} a_x x,\ \sum_{x\in X} b_x x \Big\rangle = \sum_{x\in X} a_x b_x, \quad \forall\, \mathbf{a} = \sum_{x\in X} a_x x,\ \mathbf{b} = \sum_{x\in X} b_x x \in \mathbf{F}X,$$

we call it the classical inner product on $\mathbf{F}X$. For any $s \in G$ and any $\mathbf{a} = \sum_{x\in X} a_x x$ and $\mathbf{b} = \sum_{x\in X} b_x x \in \mathbf{F}X$, we have

$$\langle s(\mathbf{a}),\ s(\mathbf{b})\rangle = \Big\langle s\Big(\sum_{x\in X} a_x x\Big),\ s\Big(\sum_{x\in X} b_x x\Big)\Big\rangle$$

$$= \left\langle \sum_{x\in X} a_x sx,\ \sum_{x\in X} b_x sx \right\rangle = \sum_{x\in X} a_x b_x$$
$$= \langle \mathbf{a},\ \mathbf{b}\rangle.$$

That is, the classical inner product on $\mathbf{F}X$ is G-invariant in the following sense:

$$\langle s(\mathbf{a}),\ s(\mathbf{b})\rangle = \langle \mathbf{a},\ \mathbf{b}\rangle, \qquad \forall\ s\in G\,,\ \forall\ \mathbf{a},\mathbf{b}\in \mathbf{F}X.$$

For any $U\le \mathbf{F}X$, denote $U^{\perp}=\{\mathbf{a}\in\mathbf{F}X \mid \langle \mathbf{u},\ \mathbf{a}\rangle = 0\,,\ \forall\ \mathbf{u}\in U\}$. If C is an $\mathbf{F}G$-submodule of $\mathbf{F}X$, then for any $s\in G$ and $\mathbf{c}'\in C^{\perp}$, and for any $\mathbf{c}\in C$, by the G-invariance of the inner product we have that

$$\langle s\mathbf{c}'\,,\ \mathbf{c}\rangle = \langle s\mathbf{c}'\,,\ ss^{-1}\mathbf{c}\rangle = \langle \mathbf{c}'\,,\ s^{-1}\mathbf{c}\rangle = 0,$$

so $s\mathbf{c}'\in C^{\perp}$, that is, $C^{\perp}$ is G-invariant. Hence, $C^{\perp}$ is an $\mathbf{F}G$-submodule too.

Definition 2 A permutation code $C\le \mathbf{F}X$ is said to be self-dual if $C^{\perp}=C$.

Next we introduce the dual modules. Let $\mathbf{F}X$ be the $\mathbf{F}G$-permutation module as above. Let $C\le\mathbf{F}X$ be a permutation code, i.e., a submodule of $\mathbf{F}X$. Define

$$C^* = \mathrm{Hom}_{\mathbf{F}}(C,\ \mathbf{F}) = \{\ \gamma : C\to\mathbf{F} \mid \gamma \text{ is linear }\}.$$

It is well-known that $C^*\cong C$ as vector spaces, in particular

$$\dim C^* = \dim C.$$

Further, define a natural G-action as follows:

$$s\gamma(\mathbf{c}) = \gamma(s^{-1}\mathbf{c}), \qquad \forall\ s\in G,\ \gamma\in C^*,\ \mathbf{c}\in C.$$

Then, C^* is an $\mathbf{F}G$-module, called the dual module of C, cf. [4, §12]. Note that this is different from the dual code in the coding theoretical sense. Recall from the representation theory of finite groups that an $\mathbf{F}G$-module M is said to be self-dual if $M\cong M^*=\mathrm{Hom}(M,\mathbf{F})$. For example, the trivial module $\mathbf{F}$, which is a one-dimensional $\mathbf{F}$-vector space with trivial G-action, is a self-dual $\mathbf{F}G$-module.

Lemma 1 Let $C\le\mathbf{F}X$ be an $\mathbf{F}G$-permutation code. Then, the classical inner product induces a homomorphism $\beta:\mathbf{F}X\to C^*$ such that the following is an exact sequence of $\mathbf{F}G$-modules

$$0\longrightarrow C^{\perp}\longrightarrow \mathbf{F}X \xrightarrow{\beta} C^*\longrightarrow 0.$$

Proof For any $\mathbf{a}\in\mathbf{F}X$, define $\beta(\mathbf{a}) : C\to\mathbf{F}$ by $\beta(\mathbf{a})(\mathbf{c}) = \langle\mathbf{a},\ \mathbf{c}\rangle$, $\forall\ \mathbf{c}\in C$, then, from the usual linear algebra, we have a surjective linear homomorphism

$$\beta:\quad \mathbf{F}X\longrightarrow C^*,\quad \mathbf{a}\longmapsto\beta(\mathbf{a}).$$

For $s\in G$ and $\mathbf{a}\in\mathbf{F}X$ and $\mathbf{c}\in C$, by the G-invariance of the inner product we have

$$\beta(s\mathbf{a})(\mathbf{c}) = \langle s\mathbf{a},\mathbf{c}\rangle = \langle s\mathbf{a}, ss^{-1}\mathbf{c}\rangle = \langle \mathbf{a}, s^{-1}\mathbf{c}\rangle = \beta(\mathbf{a})(s^{-1}\mathbf{c}) = s\beta(\mathbf{a})(\mathbf{c}),$$

that is, $\beta(s\mathbf{a}) = s\beta(\mathbf{a})$, $\forall\ s\in G$ and $\mathbf{a}\in\mathbf{F}X$. Thus, β is an $\mathbf{F}G$-homomorphism. It is clear that the kernel $\mathrm{Ker}(\beta) = \{\ \mathbf{a}\in\mathbf{F}X \mid \langle\mathbf{a},\mathbf{c}\rangle = 0,\ \forall\ \mathbf{c}\in C\ \} = C^{\perp}$. Hence, we have the desired exact sequence of $\mathbf{F}G$-modules.

Corollary 1 If $C \le \mathbf{F}X$ is a permutation code such that $C \subseteq C^{\perp}$, then C is self-dual if and only if $\dim C = |X|/2$. In particular, if $\mathbf{F}X$ has a self-dual code, then $|X|$ is even.

Proof As a consequence of the exact sequence of the lemma, we get that $|X| = \dim C^{\perp} + \dim C^{*}$, but $\dim C^{*} = \dim C$, so we have $\dim C + \dim C^{\perp} = |X|$.

Thus, $C = C^{\perp}$ if and only if $|X| = 2\dim C$.

3 Transitive Permutation Codes

In this section we consider transitive permutation codes, that is, X is a transitive G-set, and study self-dual permutation codes.

Let G be a finite group, and X be a transitive G-set, and $x \in X$. Denote $G_x = \{s \in G \mid sx = x\}$, called the stabilizer of x in G, and let G/G_x denote the set of all the left cosets sG_x. Then, G acts on G/G_x by left multiplication, and the stabilizer in G of the coset G_x is just G_x. Moreover, the G-action on X is equivalent to the G-action on G/G_x. In particular, if G_x is normal in G, then the permutation module $\mathbf{F}X$ is equivalent to the regular module of the quotient group G/G_x.

Thus, we have the following from Corollary 1 at once.

Corollary 2 Let X be a transitive G-set and $x \in X$. If there is a self-dual code in $\mathbf{F}X$, then $|G : G_x|$ is even.

Let us recall an elementary fact from representation theory of finite groups. For any $\mathbf{F}G$-module V there is a series of submodules $V = V_0 \ge V_1 \ge \cdots \ge V_r = 0$ such that every quotient module V_{i-1}/V_i is a simple $\mathbf{F}G$-module, and the collection V_{i-1}/V_i, $i = 1, \cdots, r$, are independent, up to isomorphism, of the choice of the series. Thus, for a simple $\mathbf{F}G$-module S, we can speak of the multiplicity in V of the simple module S.

If $\mathbf{F}G$ is a semisimple algebra, then it is a direct sum $\mathbf{F}G = \bigoplus_{i=1}^{h} \mathrm{M}_{n_i}(D_i)$ of matrix algebras $\mathrm{M}_{n_i}(D_i)$ of degree n_i over D_i, which corresponds to exactly one simple module S_i, and D_i is the endomorphism algebra of S_i, and n_i is just the multiplicity of S_i appeared in the regular module $\mathbf{F}G$; in particular, the trivial $\mathbf{F}G$-module $\mathbf{F}$ appears in the regular module exactly once [4, §13]. Further, we have

Lemma 2 Let X be a transitive G-set. If the characteristic p of $\mathbf{F}$ is prime to the order of G, then the trivial $\mathbf{F}G$-module $\mathbf{F}$ appears in $\mathbf{F}X$ exactly once.

Proof This is somewhat known. We sketch a proof for convenience. Let $x \in X$, then $\mathbf{F}X$ is the induced module $\mathrm{Ind}_{G_x}^{G}(\mathbf{F})$ of the trivial $\mathbf{F}G_x$-module $\mathbf{F}$. On the other hand, the regular $\mathbf{F}G_x$-module $\mathbf{F}G_x = \mathrm{Ind}_{1}^{G_x}(\mathbf{F})$ is an induced module. Under the present condition, both $\mathbf{F}G_x$ and $\mathbf{F}G$ are semisimple, see [4, §12 Cor 8]. So $\mathbf{F}G_x = \mathbf{F} \oplus \cdots$, and

$$\mathbf{F}G = \mathrm{Ind}_{G_x}^{G}(\mathbf{F}G_x) = \mathrm{Ind}_{G_x}^{G}(\mathbf{F}) \oplus \cdots \cong \mathbf{F}X \oplus \cdots$$

which is semisimple with the trivial module $\mathbf{F}$ appeared exactly once. Hence, the trivial $\mathbf{F}G$-module $\mathbf{F}$ appears in $\mathbf{F}X$ exactly once.

Proposition 1 Assume that $\mathbf{F}$ is of odd characteristic. Let X be a transitive G-set and $x \in X$. If the intersection of the stabilizer G_x of x with any Sylow 2-subgroup of G is a Sylow 2-subgroup of G_x, then there is no self-dual code in $\mathbf{F}X$.

Proof Let T be a Sylow 2-subgroup of G. Assume that $|T| = 2^a$ and $|T \cap G_x| = 2^b$ and $|G_x| = 2^b n$, then $|G| = 2^a nm$ and mn is an odd integer. Consider the action of T on X, and let $Y \subset X$ be a T-orbit, and take $y \in Y$. By the transitivity of X, there is an $s \in G$ such that $sx = y$, hence, $sG_x s^{-1} = G_y$. So,

$$T \bigcap G_y = T \bigcap sG_x s^{-1} = s\Big(s^{-1}Ts \bigcap G_x\Big)s^{-1},$$

in particular, $|T_y| = |T \bigcap G_y| = 2^b$, hence the length $|Y| = |T : T_y| = 2^{a-b}$. Thus the total number of the T-orbits is

$$|X|/|Y| = |G : G_x|/2^{a-b} = 2^a mn/2^b n 2^{a-b} = m,$$

which is an odd integer. Therefore, as $\mathbf{F}T$-modules we have

$$\mathbf{F}X \cong \overbrace{\mathbf{F}Y \oplus \cdots \oplus \mathbf{F}Y}^{m}.$$

By Lemma 2, the trivial $\mathbf{F}T$-module $\mathbf{F}$ appears in $\mathbf{F}Y$ exactly once, thus, the multiplicity of the trivial $\mathbf{F}T$-module $\mathbf{F}$ in $\mathbf{F}X$ is the odd number m.

Suppose that the $\mathbf{F}G$-permutation module $\mathbf{F}X$ has a self-dual code C, that is, C is a submodule and $C^\perp = C$, then by Lemma 1 we have an exact sequence of $\mathbf{F}G$-modules:

$$0 \longrightarrow C \longrightarrow \mathbf{F}X \longrightarrow C^* \longrightarrow 0,$$

which is of course also an $\mathbf{F}T$-module sequence. Assume that the multiplicity of the trivial $\mathbf{F}T$-module $\mathbf{F}$ in C is m', then the multiplicity of the dual of the trivial $\mathbf{F}T$-module $\mathbf{F}$ in C^* is m'. But, the trivial module $\mathbf{F}$ is self-dual, the multiplicity of the trivial $\mathbf{F}T$-module $\mathbf{F}$ in C^* is also m'. Thus, the multiplicity of the trivial $\mathbf{F}T$-module $\mathbf{F}$ in $\mathbf{F}X$ is $2m'$, which contradicts that this multiplicity is odd.

Corollary 3 Assume that $\mathbf{F}$ is of odd characteristic. Let X be a transitive G-set and $x \in X$. Then, there is no self-dual code in $\mathbf{F}X$ if one of the following holds:

(1) $|G_x|$ is odd.

(2) G_x is normal.

(3) G has a normal Sylow 2-subgroup.

Proof In any one of the three cases, the intersection of G_x with any Sylow 2-subgroup of G is a Sylow 2-subgroup of G_x, so the conclusion is proved.

If take $X = G$ to be the regular G-set and take $x = 1$, then $\mathbf{F}X = \mathbf{F}G$, and $G_1 = 1$, so both (1) and (2) of the corollary are satisfied, and we get [3, Prop. 3.1] again for the case of finite fields.

Proposition 2 Assume that $\mathbf{F}$ is of characteristic 2. Let X be a finite transitive G-set and $x \in X$. If there is a subgroup H of G such that $H \supseteq G_x$ and $|H : G_x| = 2$, then there is a self-dual permutation code in $\mathbf{F}X$.

Proof By the condition, we can assume that $H = G_x \cup hG_x$ where $h \in H - G_x$ and $h^2 \in G_x$, and assume that $|G : H| = n$ and $G = s_1 H \cup \cdots \cup s_n H$ with $s_1 = 1$. Let $Y = \{x, hx\} \subset X$. Then, $X = Y \cup s_2 Y \cup \cdots \cup s_n Y$ is a disjoint union, and as $\mathbf{F}$-vector space we have the following orthogonal direct sum:

$$\mathbf{F}X = \mathbf{FY} \oplus \mathbf{F}(s_2 Y) \oplus \cdots \oplus \mathbf{F}(s_n Y).$$

Consider the $\mathbf{F}H$-permutation module $\mathbf{F}Y$, and take

$$C_1 = \mathbf{F} \cdot (x + hx) = \{\, ax + a(hx) \mid a \in \mathbf{F} \,\}.$$

Then, it is clear that C_1 is an $\mathbf{F}H$-submodule of $\mathbf{FY}$, and $C_1 \subseteq C_1^{\perp}$. Since $\dim C_1 = 1$ and $\dim \mathbf{FY} = 2$, by Corollary 1 we have that $C_1 = C_1^{\perp}$ which is a self-dual code of $\mathbf{F}Y$. For $i = 1, 2, \cdots, n$, it is clear that s_iC_1 is a subspace of $\mathbf{F}(s_iY)$ such that $s_iC_1 = (s_iC_1)^{\perp}$, and

$$C = C_1 \oplus s_2C_1 \oplus \cdots \oplus s_nC_1$$

is an $\mathbf{F}G$-submodule of $\mathbf{F}X$, which is in fact the induced $\mathbf{F}G$-module form the $\mathbf{F}H$-module C_1, and it is clear that $C = C^{\perp}$. That is, C is a self-dual permutation code in $\mathbf{F}X$. The proof is completed.

If take $X = G$ to be the regular G-set and take $x = 1$, then $\mathbf{F}X = \mathbf{F}G$, and $G_1 = 1$. By Sylow Theorem, there is an $H \le G$ such that $|H : 1| = 2$ if and only if $|G|$ is even. Thus we deduce [3, Prop. 3.2] again for the case of finite fields.

Theorem 1 Let $\mathbf{F}$ be a finite field and $G = T \times S$ be a direct product of a finite 2-group T and a finite $2'$-group S, let X be a finite transitive G-set. Then, the permutation $\mathbf{F}G$-module $\mathbf{F}X$ has a self-dual code if and only if both the characteristic of the field $\mathbf{F}$ and the length of X are even.

Proof If $|X|$ is odd, by Corollary 2, $\mathbf{F}X$ has no self-dual code. If the characteristic p of $\mathbf{F}$ is odd, by Corollary 3(3), $\mathbf{F}X$ has no self-dual code. The necessity is proved.

Assume that both p and $|X|$ are even. Take $x \in X$, and G_x denotes the stabilizer of x. Then, $G_x \cap S$ is a normal Hall $2'$-subgroup of G_x, and $G_x \cap T$ is a normal Sylow 2-subgroup of G_x. Hence,

$$G_x = (G_x \cap S) \times (G_x \cap T),$$

and $|G : G_x| = |S : G_x \cap S| \cdot |T : G_x \cap T|$. Since $|X| = |G : G_x|$ is even, $|T : G_x \cap T| = 2^b$ with $b \ge 1$, and there is a subgroup $R \le T$ such that $R \supset G_x \cap T$ and $|R : G_x \cap T| = 2$. Set

$$H = (G_x \cap S) \times R \le S \times T = G,$$

then $H \supset G_x$ and $|H : G_x| = 2$, thus, by Proposition 2, the permutation $\mathbf{F}G$-module $\mathbf{F}X$ has a self-dual code.

References

1 Rajan B S, Siddiqi M U. A generalized DFT for abelian codes over $\mathbf{Z}_m$. IEEE Trans Inform Theory, 1994, **40**: 2082–2090

2 Hughes G. Structure theorems for group ring codes with an application to self-dual codes. Des, Codes Cryptogr, 2001, **24**: 5–14

3 Williems W. A note on self-dual group codes. IEEE Trans Inform Theory, 2002, **48**: 3107–3109

4 Alperin J L, Bell R B. Groups and Representations. GTM 13. Heidelberg, New York: Springer-Verlag, 1995

5 Bernhardt F, Landrock P, Sloane N J A. The extended Golay codes considered as ideals. J Comb Theory Ser A, 1990, **55**: 235–246

6 McDonald B R. Finite Rings with Identity. New York: Marcel Dekker, 1974

7 Graham H, Norton, Ana Salagean. On the hamming distance of linear codes over a finite chain ring. IEEE Trans Inform Theory, 2000, **46**: 1060–1067