BOL. SOC. BRAS. MAT., VOL. 15 Nºs 1 e 2 (1984), 7-24

HAMMING SPACES AND MAXIMAL SELF DUAL CODES OVER GF(q), q = ODD

CHAT YIN HO(*)

Abstract

The group of automorphisms of a Hamming space is determined. Self dual codes over odd characteristic finite field with respect to bilinear forms are treated. Under the subgroup of the monomial group preserving the inner product, we classify the maximal self dual codes over $GF(5)$ with respect to the inner product of dimension ≤ 8. The Hamming weight distribution and the order of the automorphism of the code are given.

0. Introduction

Although coding theory started from an engineering problem in the late 1940, the subject has developed by using more and more mathematical techniques. Besides the application of the error correction, one of its application is using the self dual codes over $GF(2)$ to study the projective plane of order 10. Generalization of this to self dual codes over odd characteristic finite fields turns out to be very successful in obtaining a bound of the order of a group of automorphisms of a finite geometry, and in proving non-existence of various kinds of results for planes (cf. see [3]). This leads to classification of self dual codes of small dimension. In [5], self dual codes over $GF(3)$ of dimension less than 12 have been classified.

* Partially supported by NSERC A8460 and Scarborough College.

Recebido em 11/05/84.

In this note, we first determine the group of automorphisms of a Hamming space in 1.1. Self dual codes over odd characteristic finite fields with respect to bilinear forms are treated in general in section 2. The subgroup H of the monomial group preserving the inner product is shown to be isomorphic to $Z_2 \wr S_n$. As an illustration, in section 3, we classify the maximal self dual codes over $GF(5)$ with respect to the standard inner product of dimension $n \leq 8$ under H. The Hamming weight distribution and the order of the automorphism group of the code are given. Even though H preserves the Hamming weight, it does not preserve the complete weight which is invariant under the subgroup S of the symmetric group on n letters. It is shown that for $n \leq 4$, a H-orbit remains to be a S-orbit in the maximal self dual codes, and for $n = 5$ one of the 2 H-orbits becomes the union of 3 S-orbits with different complete weight distributions.

Most of our results are self contained and notations are standard taken from Dembowski [1], Gorenstein [2], Huppert [4], or MacWilliams and Sloane [7].

I am very grateful for the Mathematical Institute of the University of Tübingen and the Alexander von Humboldt Foundation for their support during my visit to Germany, where most of the work has been developed.

1. Preliminaries

A *discrete metric space* is a set X together with a function d from $X \times X$ into the nonnegative integers such that for $x,y,z \in X$ we have a) $d(x,y) = 0$ if and only if $x = y$; b) $d(x,y) = d(y,x)$; c) $d(x,z) \leq d(x,y)+d(y,z)$. A *code* is a subset of a discrete metric space.

Let (X_1,d_1), (X_2,d_2) be two discrete metric spaces. Their *direct product* is the set $X_1 \times X_2$ together with the functions $d = d_1 \times d_2$ defined by

$$d((x_1,x_2),\ (y_1,y_2)) = d_1(x_1,y_1)+d_2(x_2,y_2).$$

An *isomorphism* between two discrete metric spaces (X_1,d_1) and (X_2,d_2) is a one-to-one and onto map α between the sets such that $d_2(\alpha(x),\alpha(y)) = d_1(x,y)$ for all $x,y \in X_1$. An *automorphism* is an isomorphism such that the two sets are equal. The set of all automorphisms of the discrete metric space (X,d) is denoted by Aut(X,d). It is a group under composition.

Let $\alpha \in \text{Aut}(X_1,d_1)$ and $\beta \in \text{Aut}(X_2,d_2)$. Define $\alpha\times\beta \in \text{Aut}(X_1\times X_2,\ d_1\times d_2)$ by $(\alpha\times\beta)(x_1,x_2) = (\alpha(x_1),\beta(x_2))$ for $x_1 \in X_1$, and $x_2 \in X_2$. This shows that

$$\text{Aut}(X_1,d_1) \times \text{Aut}(X_2,d_2) \subseteq \text{Aut}(X_1\times X_2,\ d_1\times d_2).$$

Let n be a positive integer and let S_n be the symmetric group on n letter. Then $\text{Aut}(\prod_{i=1}^{n} X_i,\ \prod_{i=1}^{n} d_i)$, where $X_i = X$ and $d_i = d$ for $i=1,\ldots,n$, contains a subgroup isomorphic to $\text{Aut}(X,d)\wr S_n$, the wreath product of Aut(X,d) by S_n.

A discrete metric space (X,d) is called an *equal distance space* if $d(x,y) = 1$ whenever $x \neq y$ in X. For simplicity we will just write that X is an equal distance space and Aut(X) for Aut(X,d) when no confusion may be caused. Thus Aut$(X)=S(X)$, the symmetric group on X.

Let Ω and F be two non-empty finite sets and V the set of all functions from Ω into F. For $f,g \in V$ define

$$d(f,g) = |\{x \in \Omega \mid f(x) \neq g(x)\}|.$$

Then (V,d) is called a *Hamming space*. The functional notation or the n-tuple notation for V will be used according to its convenience.

Thus V is the direct product of $|\Omega|$ copies of the equal distance space F. Let $|\Omega| = n$. Then Aut(V,d) contains the group $T = \prod_{x\in\Omega} T_x$, where $T_x \cong S(F)$ for $x \in \Omega$. Define $S = \{S \in \text{Aut}(V,d) \mid$ for $f \in V$ and $x \in \Omega$, we have $(sf)(x) = f(\sigma_s(x))$ where $\sigma_s \in S(\Omega)\}$. Clearly S can be identified as $S(\Omega)$ and is isomorphic to S_n. Also T is normalized by S.

1.1 Theorem. *Using the above notation, we have* $Aut(V,S) = TS \cong S(F)\sim S_n$.

Proof. Clearly $TS \subseteq Aut(V,d)$. Let $\alpha \in Aut(V,d)$. We apply induction on $|\Omega|$ to show $\alpha \in TS$.

Fix $P \in \Omega$. Let V_2 = {all functions from $\Omega-\{P\}$ to F} and V_1 = {all functions from P to F}. Let d_1 and d_2 be the Hamming distances of V_1 and V_2 respectively. Then $V = V_1 \times V_2$. Since $\{\alpha f(P) \mid f \in V\} = F$, there exists $t_P \in T_P$ such that $t_P(\alpha f(P)) = f(P)$ for all $f \in V$. Let $t = t_P \times 1$. Then $t \in T$ and $(t\alpha f)(P) = f(P)$ for all $f \in V$. For $f \in V$, define $f_1 \in V_1$ and $f_2 \in V_2$ by $f_1(P) = f(P)$ and $f_2(x) = f(x)$ for $x \neq P$. These give onto mappings from V to V_1 and V to V_2, and $d_2(g_2,h_2) = d(g,h) - d_1(g_1,h_1)$ for $f,h \in V$. Since $(t\alpha f)_1 = f_1$ for all $f \in V$, we have $d_2((t\alpha g)_2, (t\alpha h)_2) = d(t\alpha g, t\alpha h) - d_1((t\alpha g)_1, (t\alpha h)_1) = d(g,h) - d_1(g_1,h_1) = d_2(g_2,h_2)$. Therefore the function β from V_2 to V_2 defined by $\beta f_2 = (t\alpha f)_2$ for $f \in V$ is well defined and $\beta \in Aut(V_2,d_2)$. By induction we have $\beta \in \left[\prod_{\substack{x\in\Omega \\ x\neq P}} T_x\right] S(\Omega-\{P\}) := G$. Since $1\times G \subseteq TS$ we have $1\times\beta \in TS$. Since $(t\alpha f)_1 = f_1$ for all $f \in V$, $1\times\beta = t\alpha$. Therefore $t\alpha \in TS$ as desired.

Suppose F is a field. Then we can identify V with F^n. A *linear code* of V is a subspace of V. An *affine subspace* of V is a set $v+U$, where U is a subspace of V.

1.2. Corollary. *Suppose* $|F| = 2$. *Two linear codes of* V *are in the same orbit of* $Aut(V,d)$ *on the affine subspaces of* V *if and only if they are in the same orbit of* S *on the subspaces of* V.

Proof. Since $|F| = 2$, T is the group of all translations of V. By 1.1, $Aut(V,d) = TS$, which is a subgroup of the affine transformation group of V. This implies 1.2.

For $v \in V$, define the *Hamming weight* of v to be $w(v) = d(v,0)$. For $C \subseteq V$ and $0 \leq i \leq n$, let $w_i(C) = |\{v \in C \; w(v) = i\}|$. The *Hamming weight distribution* of C is $HW(C) = (w_0(C), w_1(C), w_2(C), \ldots, w_n(C))$.

2. Self dual codes over GF(q), q=odd

In this section let $F = GF(q)$, the finite field of q elements, where q is odd, and let $\{\varepsilon_1,\ldots,\varepsilon_n\}$ be the standard basis for $V = F^n$, and $F^x = F\backslash\{0\}$.

The *monomial group* of V is the set of all non-singular matrices such that each row and each column has exactly one non-zero element. Let S be the subgroup of the monomial group whose non-zero entries are 1. Then S is isomorphic to the symmetric group on n letters, and the monomial group is the product of S with the subgroup consisting of all non-singular diagonal matrices. The monomial group of V preserves the Hamming distance of V.

Let $(,)$ be a non-degenerate symmetric bilinear form of V. By [Huppert, p. 238 Satz 10.9] we see that $V = H_1 \perp \ldots \perp H_m \perp V'$, where H_i is a hyperbolic plane for $i = 1,\ldots,m$ and $\dim V' = \delta \leq 2$. If $V' = \langle v\rangle$, then $(v,v) \neq 0$. If $\delta = 2$, then V' has an orthogonal basis $\{v_1,v_2\}$ such that $(v_1,v_1) = -k(v_2,v_2)$, where k is not a square in F^x.

The maximal totally isotropic subspaces of V have the same dimension m which is called the *index* of V. From a result of Serge [Dembowski, p. 46 Article 45] we have the following.

2.1 Lemma. *The number of maximal totally isotropic subspaces of* V *is* $\prod_{i=1}^{m} (q^{i+\delta-1}+1)$.

For $x = (x_1,\ldots,x_n)$ and $y = (y_1,\ldots,y_n) \in V$, let $B_1(x,y) = x_1y_1+\ldots+x_ny_n$ and $B_2(x,y) = x_1y_1 + \ldots + x_ny_n - x_ny_n$.

Let the discriminant of $B_i(,)$, $i=1,2$ be denoted by Δ_i, $i=1,2$. Then $\Delta_1 \equiv 1$ and $\Delta_2 \equiv -1 \pmod{(F^x)^2}$, where $F^x = F\backslash\{0\}$.

2.2. Lemma. *Concerning* δ *we have the following:*

a) $\delta = 1$ *iff* n *is odd.*

b) *If* $q \equiv 1 \pmod 4$, *then* $\delta \le 1$ *for* $(,) = B_1(,)$ *or* $B_2(,)$.

c) *Suppose* $n \equiv 0 \pmod 4$. *If* $(,) = B_1(,)$, *then* $\delta = 0$. *If* $(,) = B_2(,)$ *and* $q \equiv 3 \pmod 4$, *then* $\delta = 2$.

d) *Suppose* $n \equiv 2 \pmod 4$. *If* $(,) = B_2(,)$, then $\delta=0$. If $(,) = B_1(,)$ and $q \equiv 3 \pmod 4$, then $\delta = 2$.

Proof. a) is obvious.

Let the discriminate of $(,)$ be denoted by Δ. If $\delta = 2$, the decomposition of V into directed sum of hyperbolic planes and V' indicated above implies that $\Delta \equiv (-1)^{m+1}k. \pmod{(F^x)^2}$.

b) Since $q \equiv 1 \pmod 4$, $-1 \equiv 1 \pmod{(F^x)^2}$. If $\delta = 2$, then $k \equiv (-1)^{m+1}k \equiv \Delta \equiv 1 \equiv -1 \pmod{(F^x)^2}$. However this implies that k is a square, a contradiction. Therefore $\delta \le 1$ as asserted.

In proving c) and d) we have $n = 2m+\delta$, δ is even.

c) Suppose $n \equiv 0 \pmod 4$. First suppose $\delta = 0$. Then $m = \frac{n}{2}$ is even. Hence $\Delta \equiv (-1)^m \equiv 1 \pmod{(F^x)^2}$. If $(,) = B_2(,)$, then $\Delta=\Delta_2 \equiv -1 \pmod{(F^x)^2}$. This implies that -1 is a square in (F^x), which forces $q \equiv 1 \pmod 4$.

Now suppose $\delta = 2$, then $m = \frac{n}{2}+1$ is odd. Hence $\Delta \equiv (-1)^{m+1}k \equiv k \pmod{(F^x)^2}$. If $(,) = B_1(,)$, then $1 \equiv \Delta_1 \equiv \Delta \equiv k \pmod{(F^x)^2}$. This implies that k is square, a contradiction. Therefore $\delta = 0$ when $(,) = B_1(,)$.

Assume $(,) = B_2(,)$. Then $-1 \equiv \Delta_2 \equiv \Delta \equiv (-1)^{m+1}k \equiv k \pmod{(F^x)^2}$. Since k is not a square, -1 is not a square. Therefore $q \equiv 3 \pmod 4$ in this case.

d) Similar argument as in c).

In the rest of this section we assume that $(,) = B_1(,)$. Suppose $\alpha = \mathrm{diag}[1,\ldots,a,\ldots,1]$, where $a \ne 0$ appears at the i-th row. If α preserves $(,)$, then from $(\varepsilon_i,\varepsilon_i) = (\alpha\varepsilon_i, \alpha\varepsilon_i) = a^2(\varepsilon_i,\varepsilon_i)$ we have $a^2 = 1$. This shows that the subgroup H of the monomial group preserving $(,)$ is isomorphic to $\{\pm 1\} \sim S_n$ and is a subgroup of $\{F^x\} \sim S \cong C_{q-1} \sim S$. For $W \subseteq V$, let $W^{\perp} = \{v \in V \mid (w,v)=0$ for all $w \in W\}$. For any linear code C, let $\mathrm{Aut}(C)$ be the subgroup of H leaving C invariant. If $C \subseteq C^{\perp}$, then C is a self dual code. Thus {maximal self dual codes of V} = {maximal totally isotropic subspaces of V}, and we denote this set by M_n. The H-orbits of M gives a classification of the members of M_n.

2.3. Lemma. *Let* $q \equiv 1 \pmod 4$, *and* $n = 2m$. *Let* $\Gamma = \{W \subseteq W^{\perp} \mid \dim W = m-1\}$. *We have the following:*

a) $|\Gamma| = \frac{q^m-1}{q-1} \prod_{i=2}^{m} (q^{i-1}+1)$.

b) *For* $Y \in \Gamma$, *there are exactly two maximal isotropic subspaces containing* Y *and they lie in the same orbit of* H.

Proof. a) This is because

$$|\Gamma| = \prod_{i=2}^{m} (q^i-1)(a^{i-1}+1)q^{\frac{(m-1)(m-2)}{2}} / |GL(m-1,q)|$$

$$= \frac{q^m-1}{q-1} \prod_{i=2}^{m} (q^{i-1}+1).$$

b) For $X = X^{\perp}$ let $m(X) = |\{W\ \Gamma \mid W \subseteq X\}|$. For $W \in \Gamma$ let $n(W) = |\{X \mid X=X^{\perp}$ and $Y \subseteq X\}|$. By Witt's theorem $m(X)$, $n(X)$ are constants. We now count $\Lambda = \{(X,W) \mid X=X^{\perp}$, $W \subseteq X$ and $W \in \Gamma\}$ in two ways. Since $q \equiv 1 \pmod 4$ and $n = 2m$, 2.2 implies $\delta = 0$. By 2.1, there are $\prod_{i=1}^{m} (q^{i-1}+1)$ possibilities for X. Since $m(X) = \frac{q^n-1}{q-1}$,

$|\Lambda| = \left(\prod_{i=1}^{n}(q^{i-1}+1)\right)\left(\frac{q^n-1}{q-1}\right)$. By a) we have $|\Lambda| = n(W)\cdot|\Gamma|$.

Hence $n(W) = |\Lambda|/|\Gamma| = 2$ as asserted.

Let $Y \in \Gamma$. Without loss of generality we may assume that one of the two maximal isotropic subspace X is generated by the row vectors of the following $m\times 2m$ matrix.

$$\begin{bmatrix} 1 & & & a & \dots a_m \\ & & & & \\ & I_{m-1} & & & A \end{bmatrix}$$

and Y is generated by the row vectors except $u=(1,0\dots 0,a_1,\dots a_n)$. Let $X_1 = \langle Y,v\rangle$, where $v=(-1,0,\dots,0,a_1,\dots a_n)$. Since $(u,v) = -1 + \sum_{i=1}^{n} a_i^2$ and $-(u,u) = 1 + \sum_{i=1}^{n} a_i^2 = 0 = (v,v)$, $(u,v) \neq 0$. Hence $X_1 \neq X$ and $X_1^{\perp} = X_1$. Let $\alpha = \mathrm{diag}[-1,1,\dots,1]$. Then $\alpha \in H$. Since $u^{\alpha} = v$ and $Y^{\alpha} = Y$, $X^{\alpha} = X_1$. Therefore they lie in the same orbit of H as desired.

A maximal totally isotropic subspace W is an *x-subspace* if $(e,w) = 0$ for $w \in W$, where $e = (1,1,\dots,1)$. We note that the property of being an x-subspace is invariant under the group H.

2.4. Theorem. *Let the number of x-subspaces of V be $\#$. Let $q = p^a$, and $n = \dim V$.*

a) If $p|n$, then $\# > 0$.

b) Suppose $p\nmid n$ and n is odd. Then $\# = \prod_{i=1}^{\frac{n-1}{2}}(q^{i-1}+1)$. If $q \equiv 1$ (resp. $\equiv 3$) (mod 4), then n (resp. $(-1)^{\frac{n-1}{2}}n$) is a square in $GF(q)$.

c) Suppose $p\nmid n$ and $n \equiv 2$ (mod 4), and $q \equiv 3$ (mod 4). Then $\# = \prod_{i=1}^{n-2}(q^{i}+1)$.

d) In other cases $\# = 0$.

Proof. Let $f_1 = \varepsilon_1-\varepsilon_n$, $f_2 = \varepsilon_2-\varepsilon_n,\dots,f_{n-1} = \varepsilon_{n-1}-\varepsilon_n$. Then $\{f_1,\dots,f_{n-1}\}$ is a basis for $\langle\varepsilon\rangle^{\perp} = U$. Each diagonal entry of the matrix $((f_i,f_j))$ is 2, while the other entries are 1. Therefore $\det((f_i,f_j)) = n$.

Suppose $p|n$. Then $e \in U$ and the radical of U is just $\langle e\rangle$. Also $V = V_1 \perp \langle e,v\rangle$ where $V_1 \perp \langle e\rangle = U$ and $\langle e,v\rangle$ is a hyperbolic plane. Let W_1 be a maximal totally isotropic subspace of V_1. Then $\langle W_1,e\rangle$ is an x-subspace of V. This yields a).

Suppose $p\nmid n$ in the rest of this proof. Then $\det((f_i,f_j)) \not\equiv 0 \pmod q$. Hence the restriction of $(,)$ on U is non-degenerate, and $V = \langle e\rangle \perp U$.

Let W be an x-subspace. Then $W \subseteq U$ and assume that n is odd. Hence $\dim W = \frac{1}{2}(n-1)$ by 2.2. Since $W \subseteq W^{\perp} \cap U$, W is a maximal totally isotropic subspace of U and the discriminant of the restriction of $(,)$ to U is congruent to $(-1)^{\frac{n-1}{2}}$.

Therefore $(-1)^{\frac{n-1}{2}} = \det((f_i,f_j)) \equiv n \pmod{(F^x)^2}$. Since $V = \langle e\rangle \perp U$, U has the same index as V, which is $\frac{1}{2}(n-1)$. Applying 2.2 to the restriction of $(,)$ to U, we see that U has a maximal totally isotropic subspace of dimension $\frac{1}{2}(n-1)$. Therefore the number of x-subspaces of V equals the number of maximal totally isotropic subspaces of U, which is the number stated in b). From $(-1)^{\frac{n-1}{2}} \equiv n \pmod{(F^x)^2}$, we see that if $q \equiv 1 \pmod 4$, then n is a square, and if $q \equiv 3 \pmod 4$, then $(-1)^{\frac{n-1}{2}}n$ is a square. This yields b).

c) Suppose $n \equiv 2 \pmod 4$ and $q \equiv 3 \pmod 4$. Thus $\delta = 2$ by 2.2. Since $\dim U = n-1$, $\dim U$ is odd in this case. Again by applying 2.2 to U we see that U has maximal totally isotropic subspace of dimension $\frac{1}{2}(\dim U - 1) = \frac{1}{2}(n-2)$ = index of V. Hence U contains a x-subspace of V. So # equals the number of maximal totally isotropic subspaces of U, which is $\prod_{i=1}^{\frac{n-2}{2}} (q^i+1)$ by 2.1.

d) By the proof of b) we may assume that n is even. Hence $\dim U = n-1$ is odd, and the index of U is $\frac{1}{2}(n-2)$. If $n \equiv 0 \pmod 4$ 2.2. c) implies that the index of V is $\frac{1}{2}n$. Therefore # = 0 in this case. If $n \equiv 2 \pmod 4$ but $q \equiv 1 \pmod 4$, then the index of V is $\frac{1}{2}n$ by 2.2 b) and again # = 0 as asserted.

We say that a linear code C is *decomposable* if $\{\varepsilon_1, \ldots, \varepsilon_n\} = \bigcup_{j=1}^{k} B_j$ is a partition with $k \geq 2$ and $C = \bigoplus_{j=1}^{k} (C \cap \langle B_j \rangle)$. Otherwise C is called *indecomposable*.

3. Maximal self dual codes over GF(5)

In this section, under the group H we classify the maximal self dual codes over $F = GF(5)$ with respect to $(,) = B(,)$ for $\dim V = n \leq 8$.

Let $X \in M_n$. The orbit containing X is X^H and $|X^H| = [H:\mathrm{Aut}(X)]$. For any subset L of $\mathrm{Aut}(X)$ and $v \in X$, set $C_L(v) = \{\ell \in L \,|\, v^\ell = v\}$ and $L_{\langle v \rangle} = \{\ell \in L \,|\, \langle v \rangle^\ell = \langle v \rangle\}$.

For $a,b,c \in F^x$, we have $a^2+b^2+c^2 \neq 0$. as a consequence we have the following.

3.1. Lemma. *If* $X \in M_n$, *then* $w_3(X) = 0$.

3.2. Theorem. *The following holds, where* * *means that the code is indecomposable. Also the code is generated by the row vector of the matrix when this matrix is given in the description of the code.*

n	$\|M_n\|$	$\|H\|$	R(Representative from each orbit of M_n under H)	$\|\mathrm{Aut}(R)\|$	$\|R^H\|$	$HW(R)$
1	0	1				
2	2	8	$X_2 = \langle (1,2) \rangle$	4	2	(1,0,4)
3	6	$2^4.3$	$X_3 = X_2 \oplus \langle 0 \rangle = \{(x,0) \,\|\, x \in X_2\}$	8	6	(1,0,4,0)
4	12	$2^7.3$	$X_4 = X_2 \oplus X_2$	2^5	6	(1,0,8,0,16)
5	$2^2.3.13$	$2^8.3.5$	$X_5 = X_2 \oplus X_2 \oplus \langle 0 \rangle$	2^6	$2^2.3.5$	(1,0,8,0,16,0)
			$U_5 = \begin{pmatrix} 1&1&1&1&1 \\ 0&1&2&3&4 \end{pmatrix}^*$	$2^3.5$	$2^5.3$	(1,0,0,0,20,4)
6	$2^3.3.13$	$2^6.6!$	$X_6 = X_2 \oplus X_2 \oplus X_2$	$2^7.3$	$2^3.3.5$	(1,12,0,48,0,64)
			$U_6 = \begin{pmatrix} 1&0&0&1&2&2 \\ 0&1&0&2&1&3 \\ 0&0&1&2&3&1 \end{pmatrix}^*$	$2^4.3.5$	$2^6.3$	(1,0,0,60,24,40)
7	$2^3.3^3.7.13$	$2^7.7!$	$X_7 = X_6 \oplus \langle 0 \rangle$	$2^8.3$	$2^3.3.5.7$	(1,12,0,48,0,64,0)
			$C_2 = U_6 \oplus \langle 0 \rangle$	$2^5.3.5$	$2^6.3.7$	(1,0,0,62,24,40,0)
			$C_3 = U_5 \oplus X_2$	$2^5.5$	$2^6.3^2.7$	(1,4,0,20,4,80,16)
			$U_7 = \begin{pmatrix} 1&0&0&1&0&2&2 \\ 0&1&0&1&2&0&2 \\ 0&0&1&1&2&2&0 \end{pmatrix}^*$	$2^4.3$	$2^7.3.5.7$	(1,0,0,24,12,72,16)
8	$2^4.3^3.7.13$	$2^8.8!$	$X_8 = X_2 \oplus X_2 \oplus X_2 \oplus X_2$	$2^{11}.3$	$2^4.3.5.7$	(1,16,0,96,0,256,0,256)
			$T_2 = U_6 \oplus X_2$	$2^6.3.5$	$2^9.3.7$	(1,4,0,60,24,280,96,160)
			$U_8 = \begin{pmatrix} 1&0&0&0&1&1&1&1 \\ 0&1&0&0&1&0&2&2 \\ 0&0&1&0&1&2&0&2 \\ 0&0&0&1&1&2&2&0 \end{pmatrix}^*$	$2^7.3$	$2^8.3.5.7$	(1,0,0,48,32,288,128,128)

Proof. If $n = 1$, then $|M_1| = 0$. For $n > 1$, by 2.1 and 2.2 we see that $|M_n| = \prod_{i=1}^{\frac{n}{2}} (5^{i-1}+1)$ when n is even, and $|M_n| = \prod_{i=1}^{\frac{n-1}{2}} (5^{i-1}+1)$ when n is odd.

Suppose $n = 2$. Then $|M_2| = 2$ and $|H| = 2^2.2 = 8$. Let $X_2 = \langle(1,2)\rangle$. Then $\mathrm{Aut}(X_2) = \langle\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\rangle$ has order 4. Hence $M_2 = X_2^H$.

Suppose $n = 3$. Then $|M_3| = 6$ and $|H| = |Z_2 \sim S_3| = 2^4.3$. Let $X_3 = X_2 \oplus \langle 0\rangle = \{(x,0) | x \in X_2\}$. Then $|\mathrm{Aut}(X_3)| = 8$ and $M_3 = X_3^H$.

Suppose $n = 4$. Then $|M_4| = 12$ and $|H| = 2^4.4! = 2^7.3$. Let $X_4 = X_2 \oplus X_2$. Thus $\mathrm{Aut}(X_4) \cong \mathrm{Aut}(X_2) \sim S_2$ has order 2^5 and $M_4 = X_4^H$.

Suppose $n = 5$. Then $|M_5| = 2^2.3.13$ and $|H| = 2^8.3.5$. Let $X_5 = X_2 \oplus X_2 \oplus \langle 0\rangle$. Thus $|\mathrm{Aut}(X_5)| = |(\mathrm{Aut}(X_2) \sim S_2) X Z_2| = 2^6$. So $|X_5^H| = 2^2.3.5$. Let $U_5 = \langle u_1, u_2 | u_1 = (1,1,1,1,1)$ and $u_2 = (0,1,2,3,4)\rangle$. Then $U_5 \in M$. Let $k \in \mathrm{Aut}(U_5) = K$ be such that $u_2^k = u_2$. The corresponding permutation on the coordinates induced by k must be the identity and the corresponding scalars not 1 can only appear possibly in the first coordinate. Thus $|C_K(u_2)| \le 2$. Since there are 4 nonzero vectors in $\langle u_2\rangle$, $[K_{\langle u_2\rangle} : C_K(u_2)] \le 4$. Since there are 6 1-dimensional subspaces in U_5 and $w(u_1) \ne w(u_2)$, $[K : K_{\langle u_2\rangle}] \le 5$. Therefore $|K| \le 5.4.2$ and so $|U_5^H| = \frac{|H|}{|K|} \ge \frac{2^8.3.5}{2^3.5} = 2^5.3$. Hence $M_5 = X_5^H \cup U_5^H$ and $|U_5^H| = 2^5.3$.

Suppose $n = 6$. Then $|M_6| = 2^3.3.13$ and $|H| = 2^6.6!$

Let $X_6 = X_2 \oplus X_2 \oplus X_2$. Thus $\mathrm{Aut}(X_6) = \mathrm{Aut}(X_2) \sim S_3$ has order $2^7.3$ and $|X_6^H| = 2^3.3.5$.

Let U_6 be the subspace generated by the $u_1 = (1,0,0,1,2,2)$, $u_2 = (0,1,0,2,1,3)$ and $u_3 = (0,0,1,2,3,1)$. Then $U_6 \in M$ and is indecomposable. So $U_6 \notin X_6^H$. Note that $U_6 = \{(a,b,c,a+2b+2c, 2a+b-2c, 2a-2b+c) | a,b,c \in F\}$. Let $K = \mathrm{Aut}(U_6)$. Then K induces a permutation group $\bar{K}$ on the 6 coordinate places $\bar{1}, \bar{2}, \ldots, \bar{6}$. Since $\{\pm 2\} \cap \{\pm 1\} = \emptyset$ in F, $\bar{K}_{\langle u\rangle}$ leaves invariant $\{\bar{2}, \bar{3}\}$, $\{\bar{1}, \bar{4}\}$, $\{\bar{5}, \bar{6}\}$. Let $(Y_1, \ldots, Y_6)$ be a vector in V. If $k \in C_K(u_1)$, then k permutes Y_2, Y_3 with possible multiplication by a factor ± 1, and permutes Y_1, Y_4, and permutes Y_5, Y_6. Suppose $\bar{2}^{\bar{k}} = \bar{2}$. Then $\bar{3}^{\bar{k}} = \bar{3}$. If $Y_1^k = Y_1$, then $Y_4^k = Y_4$. This implies $u_2^k = u_2$ which forces $Y_2^k = Y_2$. Also $u_3^k = u_3$ under the present assumption on k. Hence $Y_t^k = Y_t$, for $t = 3,5,6$. Therefore k is the identity linear transformation in this case. If $Y_1^k = Y_4$, then $Y_4^k = Y_1$. Thus $u_2^k = (2, \pm 1, 0, 0, *, *) \in U_6$ which implies $u_2^k = (2,-1,0,0,3,1)$ by the description of the vectors in U_6. Hence k interchanges Y_5 and Y_6, and $Y_2^k = -Y_2$. Since $u_3^k = (2,0,\pm 1,0,1,-2) \in U_6$, $u_3^k = (2,0,-1,0,1,-2)$. Hence $Y_3^k = -Y_3$. Therefore if $\bar{2}^{\bar{k}} = \bar{2}$, then either k is the identity linear transformation or $Y_1^k = Y_4$, $Y_4^k = Y_1$, $Y_2^k = -Y_2$, $Y_3^k = -Y_3$, $Y_5^k = Y_6$, and $Y_6^k = Y_5$. Next suppose $\bar{2}^{\bar{k}} = \bar{3}$. If $Y_1^k = Y_4$, then $Y_4^k = Y_1$ and so $u_2^k = (2,0,\pm 1,0,**) \in U_6$. This implies $u_2^k = (2,0,-1,0,1,3)$ which shows $Y_5^k = Y_5$ and $Y_6^k = Y_6$. Hence $u_3^k = (2,\pm 1,0,0,-2,1)$ which forces $Y_3^k = -Y_2$. If $Y_1^k = Y_1$, then $Y_4^k = Y_4$. Thus $u_2^k = (0,0,\pm 1,2,*,*)$ which implies $u_2^k = u_3$ Hence $Y_2^k = Y_3$, $Y_5^k = Y_6$ and $Y_6^k = Y_5$. So

$u_3^k = (0,\pm1,0,2,1,-2)$ which implies $Y_3^k = Y_2$. This whows that $C_K(u_1) = \langle\pi,\delta\rangle$ is an elementary abelian 2-group of order 4, where π interchanges Y_1 and Y_4, Y_5 and Y_6, also $Y_2^\pi = -Y_2$ and $Y_3^\pi = -Y_3$; and δ fixes Y_1, Y_4, interchanges Y_2 and Y_3, Y_5 and Y_6. Define α in the following way: it interchanges Y_1 and Y_2, Y_4 and Y_5, also $Y_3^\alpha = -Y_3$, $Y_6^\alpha = -Y_6$. Since $u_1^\alpha = u_2$, $u_2^\alpha = u_1$ and $u_3^\alpha = -u_3$, we have $\alpha \in K$. Let $\beta = \alpha\delta$. Then $\beta^3 = -I$ and β has order 6. Let $g \in K$ such that g induces identity on U_6. Then $g \in C_K(u_1)$. From $u_2^g = u_2$ and $u_3^g = u_3$, we see that $g = 1$. Therefore K is isomorphic to a subgroup of $GL(U_6) \cong GL(3,5)$. Hence $|K|$ divides $5^3.31.3.2^7$. Since $|K|\,\big|\,|H| = 2^6.6!$, $|K|$ divides $5.3.2^7$. Let $\Gamma = \{1\text{-dimensional subspaces of } U_6\}$. Then $|\Gamma| = 31$ and K acts on Γ. Let $e_1 = u_1+u_2+u_3 = (1,1,1,0,1,1)$, $e_2 = e_1^\beta = (1,-1,1,1,-1,0)$, $e_3 = e_2^\beta = (-1,-1,1,-1,0,1)$, and $e_4 = e_1^\pi = (0,-1,-1,1,1,1)$. Since $\beta \notin K_{\langle e_4\rangle}$, $|\langle e_1\rangle^K| \geq 6$. Let $f_1 = u_1-u_2-u_3 = (1,-1,-1,-3,3,3)$. Let $f_2 = f_1^\pi = (-3,1,1,1,3,3)$. Then $(f_2)^{\beta^2} = (-1,3,1,-3,-1,3) \notin \{\langle f_1\rangle,\langle f_2\rangle\}$. It is easy to see that $|\langle f_1\rangle^K| \geq 6$. From $w(u_1) = 4$, $w(e_1) = 5$, $w(f_1) = 6$, we get $\langle u_1\rangle^K \neq \langle e_1\rangle^K \neq \langle f_1\rangle^K \neq \langle u_1\rangle^K$. Thus $[K:K_{\langle u_1\rangle}] = |\langle u_1\rangle^K| \leq 31-(6+6) = 19$. Combining the facts that 3 divides $|K|$ to the first power, $|K|\,\big|\,5.3.2^7$, and $K_{\langle u_1\rangle}$ is a 2-group, we see that $15\,|\,[K:K_{\langle u_1\rangle}]$. Therefore $[K:K_{\langle u_1\rangle}] = 15$. Since $K_{\langle u_1\rangle}$ acts on the 4 non-zero vectors of $\langle u_1\rangle$, $[K_{\langle u_1\rangle}:C_K(u_1)] \leq 4$. Hence $|K| = 15\cdot|K_{\langle u_1\rangle}| \leq 15.2^4$. Thus $|U_6^H| = \frac{|H|}{|K|} \geq \frac{2^6.6!}{15.2^4} = 3.2^6 = |M\setminus X_6^H|$. Therefore $M_6 = X_6^H \cup U_6^H$ and $|K| = 2^4.3.5$. Define θ by $Y_1^\theta = -Y_6$, $Y_6^\theta = Y_1$, $Y_4^\theta = -Y_5$,

$Y_5^\theta = Y_4$, $Y_2^\theta = -Y_3$, $Y_3^\theta = Y_2$. Then $\theta \in K$ and $\theta^2 = -I$. Since $\langle\theta\rangle$ acts transitively on the 4 non-zero vectors of $\langle u_1\rangle$, $K_{\langle u_1\rangle} = \langle\theta\rangle\cdot C_K(u_1)$. This shows that $\bar{K} = K/\langle -I\rangle$. Since $\bar{K}$ acts transitively on $\{\bar{1},\ldots,\bar{6}\}$ and $|\bar{K}| = 120$ and $\bar{\theta} = (16)(23)(45)$, we have $\bar{K} \cong S_5$. This completes the analysis for $n = 6$.

Suppose $n = 7$. Then $|M_7| = 2^3.3^3.7.13$ and $|H| = 2^7.7!$ Let $X_7 = X_6 \oplus \langle 0\rangle$, $C_2 = U_6 \oplus \langle 0\rangle$, $C_3 = U_5 \oplus X_2$. Then $|\mathrm{Aut}(X_7)| = 2^8.3$, $|\mathrm{Aut}(C_2)| = 2^5.3.5$, $|\mathrm{Aut}(C_3)| = 2^5.5$ and so $|X_7^H| = 2^3.3.5.7$, $|C_2^H| = 2^6.3.7$, $|C_3^H| = 2^6.3^2.7$. Let U_7 be the linear code generated by $t_1 = (1,0,0,1,0,2,2)$, $t_2 = (0,1,0,1,2,0,2)$ and $t_3 = (0,0,1,1,2,2,0)$. Then $U_7 \in M$. Let $G = \mathrm{Aut}(U_7)$ and $\bar{G}$ the permutation group induced by G on the 7 coordinate places $\{\bar{1},\ldots,\bar{7}\}$. Let $g \in G_{\langle t_1\rangle}$. Since g permutes the 3 zero coordinates of v_1, $\{\bar{2},\bar{3},\bar{5}\}$ is $\bar{g}$ invariant. If $g \in G_{\langle t_2\rangle} \cap G_{\langle t_3\rangle}$, then $\{\bar{1},\bar{3},\bar{6}\}$ and $\{\bar{1},\bar{2},\bar{7}\}$ are $\bar{g}$ invariant by the same argument. Hence $\bar{g}$ fixes $\bar{1} = \{\bar{1},\bar{2},\bar{7}\} \cap \{\bar{1},\bar{3},\bar{6}\}$, $\bar{2} = \{\bar{1},\bar{2},\bar{7}\} \cap \{\bar{2},\bar{3},\bar{5}\}$, and $\bar{3} = \{\bar{2},\bar{3},\bar{5}\} \cap \{\bar{1},\bar{3},\bar{6}\}$. This implies that $\bar{g}$ also fixes $\bar{7},\bar{6},\bar{5}$ which forces $\bar{g}$ to be the identity permutation. Easy calculation shows that $g = \pm I_7$. Note that U_7 is indecomposable. A typical vector in U_7 has the form $(a,b,c,a+b+c,2(b+c),2(a+c),2(a+b))$. In finding $\langle v\rangle$ with $w(v) = 7$, we may assume the first coordinate of v to be 1. A direct calculation shows that there are 4 possibilities: $v_1 = (1,1,1,3,4,4,4)$, $v_2 = (1,1,2,4,1,1,4)$, $v_3 = (1,2,1,4,1,4,1)$ and $v_4 = (1,3,3,2,2,3,3)$. Therefore $w_7(U_7) = 16$ and G acts on $\{\langle v_i\rangle \mid i=1,2,3,4\}$. If $g \in G$ and $\langle v_i\rangle^g = \langle v_i\rangle$ for $i=1,2,3$, then $\langle t_i\rangle^g = \langle t_i\rangle$ for $i=1,2,3$. This implies $g=\pm I_7$

and so $|G| \,\big|\, |S_4| \cdot 2 = 2^4.3$. Hence $|U_7^H| \geq 2^7.7!/2^4.3 = 2^7.3.5.7 = |M_7 \backslash \{X_7^H \cup C_2^H \cup C_3^H\}|$. Therefore $M_7 = X_7^H \cup C_2^H \cup C_3^H \cup U_7^H$ and $|\mathrm{Aut}(U_7)| = 2^4.3$.

Suppose $n = 8$. Then $|M_8| = 2^4.3^3.7.13$, and $|H| = 2^8.8!$ Let $X \in M_8$. In finding X^H we may assume that X is generated by $(1,0,0,0,a_1)$, $(0,1,0,0,a_2)$, $(0,0,1,0,a_3)$, $(0,0,0,1,a_4)$ where $a_i \in F^4$, for $1 \leq i \leq 4$. Let $Y = \langle(1,0,0,a_2), (0,1,0,a_3), (0,0,1,a_4)\rangle$. Then $Y \in M_7$. Without loss of generality, we may assume that $Y = X_7$, C_2, C_3 or U_7. By 2.3, there are at most 4 orbits of H in M_7. If $Y = X_7$, then $X \in X_8^H$, where $X_8 = X_2 \oplus X_2 \oplus X_2 \oplus X_2$. Since $\mathrm{Aut}(X_8) = 2^8.2^3.3$, $|X_8^H| = 2^4.3.5.7$. Let $T_2 = U_6 \oplus X_2$. Since $w_2(U_6) = 0$, $|\mathrm{Aut}(T_2)| = (2^4.3.5).4$. Hence $|T_2^H| = 2(2^6.3.7(1+3))$. Clearly C_2 can be embedded in T_2. Now U_6 contains $z_1 = (1,1,1,0,1,1)$ and $z_2 = (0,1,4,0,3,2)$. As $\langle(z_1,0,0), (z_2,0,0)\rangle \cong U_5$ and $\langle(0,0,0,0,0,0,1,2)\rangle \cong X_2$, $C_3 = U_5 \oplus X_2$ can be embedded in T_2. Hence M_8 has at most 3 orbits of H. Let $U_8 = \langle(1,0,0,0,1,1,1,1), (0,1,0,0,1,0,2,2), (0,0,1,0,1,2,0,2), (0,0,0,1,1,2,2,0)\rangle$. Then $U_8 \in M_8$ and U_7 can be embedded in U_8. Also U_8 is indecomposable. Hence $M_8 = X_8^H \cup T_2^H \cup U_8^H$, and $|U_8^H| = 2^8.3.5.7$ and $|\mathrm{Aut}(U_8)| = 2^7.3$.

A direct computation using computer's help in the case $n = 7,8$ yields the Hamming weight distribution of the representative of each orbit of M_n under H. This completes the proof of 3.2.

3.3. Remark. Even though H preserves the Hamming weight, it does not preserve the complete weight of a vector $\mathrm{comp}(v) = (\xi_0, \xi_1, \xi_2, \xi_3, \xi_4)$ for $v = (v_1, \ldots, v_n)$, where $\xi_i = |\{j \mid v_j = i\}|$ for $0 \leq i \leq 4$ [See p. 142, 6]. The symmetric subgroup S of H does preserve the complete weight. Note that $S \cong S_n$.

It is easy to see that for $2 \leq n \leq 4$, M_n is still an orbit of S. Also $X_5^H = X_5^S$.

Let $R = S_{U_5}$. Then $C_R(u_2) = 1$, and so $|R| = [R:R_{\langle u_2\rangle}][R_{\langle u_2\rangle}] \leq 5.4$. Therefore $|U_5^S| \geq \frac{5!}{5.4} = 6$.

Let $W = \langle\alpha_1, \alpha_2\rangle$, where $\alpha_1 = (1,-1,1,1,1)$ and $\alpha_2 = (0,4,2,3,4)$. Then $W \in U_5^H$. Any image of α_2 under S will have exactly 2 coordinates equal to 4. Since $U_5 = \{(x, x+y, x+2y, x+3y, x+4y) \mid x, y \in F\}$, $\alpha_2^S \notin U_5$. Hence $W \notin U_5^S$. Let $A = S_W$. If $\sigma \in A$, then $(\alpha_1, \alpha_1^\sigma) = 0$, which implies that $\bar{2}^\sigma = \bar{2}$ (the second coordinate place). Suppose $\sigma \in A_{\langle\alpha_2\rangle}$. Then from $\bar{2}^\sigma = \bar{2}$ we get $\sigma \in C_A(\alpha_2)$ which implies that $\sigma = I$. Hence $|A_{\langle\alpha_2\rangle}| = 1$. Since $\bar{2}^A = \bar{2}$, $5 \nmid |A|$. As A acts on the 6 1-dimensional subspaces of W and $w(\alpha_2) \neq w(\alpha_1)$, $|A| = |A : A_{\langle\alpha_2\rangle}| = |\langle\alpha_2\rangle^A| \leq 4$, as $5 \nmid |A|$. Therefore $|W^S| \geq \frac{5!}{4} = 2.3.5$.

Let $Z = \langle\beta_1, \beta_2\rangle$, where $\beta_1 = (1,-1,-1,1,1)$ and $\beta_2 = (0,4,3,3,4)$. Then $Z \in U_5^H$. As in the case of α_1, we see that $\beta_2^S \notin U_5$. Hence $Z \notin U_5^S$. Since $W_2 = \{(x, -x+4y, x+2y, x+3y, x+4y) \mid x, y \in F\}$, $\beta_2^S \notin W_2$ as β_2 has 2 distinct pairs of equal coordinates. Hence $Z \notin W_2^S$. Let $B = S_Z$. Since $(\beta_1^B, \beta_1) = 0$, B fixes $\{\bar{2}, \bar{3}\}$. Suppose $b \in B_{\langle\beta_2\rangle}$. Then $\bar{1}^b = \bar{1}$. Assume that $\bar{2}^b = \bar{3}$. So $\bar{3}^b = \bar{2}$. Then $\beta_2^b = (0,3,4,*,*) = \lambda\beta_2$ implies that $3 = \lambda 4$ or $\lambda = 4.3 = 2$. Hence $\beta_2^b = (0,3,1,1,3)$ which is impossible as no coordinate of β_2 equals to 1. Hence $\bar{2}^b = \bar{2}$ and $\bar{3}^b = \bar{3}$. Thus $b \in C_B(\beta_2)$, and this implies that $b = I$. Therefore

$|B_{\langle\beta_2\rangle}| = 1$. Now $Z = \{(x,-x-y,-x-2y,x+3y,x+4y) \mid x,y \in F\}$ contains $(1,0,1,3,2) = z_2$, $(1,2,0,2,4) = z_3$ and $(1,3,2,4,0)=z_5$. By inspection $\langle\beta_2\rangle^B \not\in \langle\beta_1\rangle \bigcup_{i=2}^{5} \langle z_i\rangle$. Hence $|B|=[B:B_{\langle\beta_2\rangle}]=|\langle\beta_2\rangle^B|\leq 2$.

Therefore $|Z^S| \geq \frac{5!}{2} = 2^2.3.5$. Since $|U_5^S \cup W^S \cup Z^S| \geq 6+2.3.5+2^2.3.5 = 2^5.3 = |U_5^H|$, we have $U_5^H = U_5^S \cup W^S \cup Z^S$, $|U_5^S| = 6$, $|W^S|=2.3.5$, $|Z^S|=2^2.3.5$, $|S_{U_5}| = 20$, $|S_W| = 4$ and $|S_Z| = 2$. Note also that the complete weight distribution of U_5 and W are different.

References

1. P. Dembowski, *Finite Geometries*, Springer 1972.
2. D. Gorenstein, *Finite groups*, Harper and Row 1968.
3. C. Ho, *On finite projective planes*, to appear.
4. B. Huppert, *Endliche Gruppen I*, Springer, 1967.
5. C. Mallows, V. Pless, N. Sloane, *Self dual codes over GF(3)*, SIAM J. of apply Math. 31 (1976) p. 649-666.
6. F. MacWilliams, N. Sloane, *The theory of error correcting codes*, North Holland, 1977.

Chat Yin Ho
Department of Mathematics
University of Toronto
Scarborough College
Toronto, Ontario
Canada