

# Codes with a certain weight-preserving transitive group of automorphisms

Michael Giudici \*

School of Mathematics and Statistics  
The University of Western Australia  
35 Stirling Highway  
Crawley, WA 6009  
Australia

## Abstract

We determine all linear codes  $C$  containing the constant code  $E$ , for which there is a weight-preserving group of semilinear automorphisms which acts transitively on the set of nontrivial cosets of  $E$  in  $C$ .

**Keywords:** linear codes, weight-preserving automorphism groups, 05E20.

## 1 Introduction

A *linear code*  $C$  of *length*  $n$  over  $\text{GF}(q)$ , where  $q$  is a power of some prime  $p$ , is a subspace of the vector space  $\text{GF}(q)^n$ . We regard  $\text{GF}(q)^n$  as the set of all functions  $f : X \rightarrow \text{GF}(q)$  for some set  $X$  of size  $n$ . If  $X = \{x_1, \dots, x_n\}$  then  $f$  corresponds to the  $n$ -tuple  $(f(x_1), \dots, f(x_n))$  and we often refer to the elements of  $X$  as *coordinates*. Given  $f \in C$ , the *weight* of  $f$  is the number of elements  $x_i \in X$  such that  $f(x_i) \neq 0$ . We call  $C$  a *constant weight code* if all nonzero elements of  $C$  have the same weight. In particular, the 1-dimensional code  $E$  consisting of all the constant functions has constant weight  $n$  and is called the *constant code*.

The *Hamming dual* over  $\text{GF}(q)$  is the code of length  $n = (q^d - 1)/(q - 1)$  given by the restriction of all linear functions  $f : \text{GF}(q)^d \rightarrow \text{GF}(q)$  to a set of representatives for the 1-dimensional subspaces of  $\text{GF}(q)^d$ . If  $f \neq 0$ , the

---

\*The author holds an Australian Postdoctoral Fellowship.

kernel of such a linear function has dimension  $d - 1$  and  $f(\mathbf{a}) \neq 0$  if and only if  $\mathbf{a} \notin \ker(f)$ . Thus all nonzero codewords have weight  $(q^d - 1)/(q - 1) - (q^{d-1} - 1)/(q - 1) = q^{d-1}$ . For each positive integer  $k$  we can construct a constant weight code of weight  $kq^{d-1}$  by taking the restriction of all linear functions  $f : \text{GF}(q)^d \rightarrow \text{GF}(q)$  to some multiset  $X$  of elements of  $\text{GF}(q)^d$  such that  $X$  contains precisely  $k$  elements from each 1-dimensional subspace. Such a code is known as a *replication* of a Hamming dual. In fact, Bonisoli [2] proved that, disregarding coordinates on which every codeword is zero, all constant weight codes over  $\text{GF}(q)^d$  can be constructed in this manner. Bonisoli's proof was combinatorial and inductive, whereas Ward and Wood [10, 11], later derived character theoretic proofs.

A map  $\sigma : \text{GF}(q)^n \rightarrow \text{GF}(q)^n$  is called *semilinear* if  $\sigma$  preserves addition and there exists a field automorphism  $\alpha$  of  $\text{GF}(q)$  such that for all  $\lambda \in \text{GF}(q)$  and  $v \in \text{GF}(q)^n$ , we have  $(\lambda v)^\sigma = \lambda^\alpha v^\sigma$ . Note that, if  $\alpha = 1$  then  $\sigma$  is linear. Let  $\phi$  be the Frobenius automorphism of  $\text{GF}(q)$ , that is,  $\phi$  raises each element of  $\text{GF}(q)$  to its  $p^{\text{th}}$  power, where  $q$  is a power of the prime  $p$ . Then  $\phi$  induces a semilinear automorphism  $\tau_\phi$  of  $\text{GF}(q)^n$  such that  $\tau_\phi$  maps each  $f \in \text{GF}(q)^n$  to the function with evaluation  $(f(x_1)^\phi, f(x_2)^\phi, \dots, f(x_n)^\phi)$ . Any semilinear automorphism is then a combination of some linear automorphism and a power of  $\tau_\phi$ . The *automorphism group* of a linear code  $C \subseteq \text{GF}(q)^n$  is the group of all semilinear transformations of  $\text{GF}(q)^n$  which fix  $C$  setwise and preserve weights. If  $q$  is a prime then all semilinear maps are linear and the automorphism group consists of all monomial transformations fixing  $C$  ([7],[8, p 238]), that is, all transformations of  $\text{GF}(q)^n$  given by monomial matrices. When  $q$  is not a prime, then the automorphism group of  $C$  is a subgroup of the group generated by all monomial transformations and  $\tau_\phi$  (c.f. [8, p 238]).

When studying locally 2-arc transitive graphs with certain properties in [3] it became necessary to know all linear codes  $C$  containing the constant code  $E$ , for which there is a weight-preserving group  $G$  of semilinear automorphisms which acts transitively on the set of nontrivial cosets of  $E$  in  $C$ . The main result of this paper is a determination of all such  $C$  and  $G$ . Before stating our theorem we need the following setup.

Let  $M$  be an  $m$ -dimensional vector space over  $\text{GF}(q)$ , where  $q$  is the power of some prime  $p$ . Let  $X$  be a set of size  $n$  and let  $F$  be the vector space of all functions  $f : X \rightarrow M$  with pointwise addition. Then  $F \cong M^n$ . From now on we consider a code to be a subspace of  $F$ ; the classical case is where  $m = 1$ . By the *weight* of  $f \in F$  we mean the number of  $x \in X$  such that  $f(x) \neq 0$ . Each  $g \in \text{Sym}(X)$ , induces a linear automorphism  $\sigma_g$  of  $F$  such that for all

$f \in F$  and  $x \in X$ , we have

$$f^{\sigma_g}(x) = f(x^{g^{-1}}).$$

This is the action of  $\text{Sym}(X)$  on  $M^n$  given by permuting coordinates. Also, for each  $h \in \Gamma\text{L}(m, q)$ ,  $h$  induces a semilinear automorphism  $\tau_h$  of  $F$  via,

$$f^{\tau_h}(x) = (f(x))^h$$

for all  $x \in X$  and  $f \in F$ . Note that if  $h \in \Gamma\text{L}(m, q)$  is scalar multiplication by the field element  $\lambda$  then  $\tau_h$  induces scalar multiplication by  $\lambda$  on  $F$ . Also each automorphism  $\tau_h$  induced by  $\Gamma\text{L}(m, q)$  commutes with each automorphism  $\sigma_g$  induced by  $\text{Sym}(X)$ . Hence  $\text{Aut}(F)$  contains a subgroup

$$W = \langle \tau_h, \sigma_g \mid h \in \Gamma\text{L}(m, q), g \in \text{Sym}(X) \rangle \cong \Gamma\text{L}(m, q) \times S_n.$$

Let  $E$  be the subgroup of  $F$  given by all constant functions. Then  $W$  is the largest weight preserving group of semilinear automorphisms of  $F$ , which fixes  $E$  setwise,

If we take  $X = \text{GF}(q)^d$  for some positive integer  $d$  then  $F \cong M^{q^d}$  and  $\text{A}\Gamma\text{L}(d, q) \leq \text{Sym}(X)$ . The Frobenius automorphism  $\phi$  of  $\text{GF}(q)$ , which raises each element to its  $p^{\text{th}}$  power, induces a semilinear automorphism of  $M$  and of  $\text{GF}(q)^d$ . Hence there is an automorphism  $\sigma_\phi$  of  $F$  such that for all  $f \in F$  and  $x \in \text{GF}(q)^d$ ,

$$f^{\sigma_\phi}(x) = f(x^{\phi^{-1}}),$$

and an automorphism  $\tau_\phi$  such that

$$f^{\tau_\phi}(x) = (f(x))^\phi.$$

Since  $\text{A}\Gamma\text{L}(d, q) = \text{A}\Gamma\text{L}(d, q) \rtimes \langle \phi \rangle$ , this enables us to define a homomorphism  $\Psi : \text{A}\Gamma\text{L}(d, q) \rightarrow W$  such that if  $g \in \text{A}\Gamma\text{L}(d, q)$  then  $\Psi(g) = \sigma_g$ , while  $\Psi(\phi) = \tau_\phi \sigma_\phi$ . In other words,  $\Psi$  embeds  $\text{A}\Gamma\text{L}(d, q)$  in  $\Gamma\text{L}(m, q) \times S_{q^d}$  such that each element  $g \in \text{A}\Gamma\text{L}(d, q)$  with associated field automorphism  $\phi^i$ , induces an action on  $F$  by permuting coordinates in the same way that it acts on  $\text{GF}(q)^d$  and by applying  $\phi^i$  to each entry.

We can now state our theorem.

**Theorem 1.1.** *Let  $M = \text{GF}(q)^m$ ,  $n > 1$ ,  $E$  the subspace of  $M^n$  of all constant functions and  $C \leq M^n$  such that given any two distinct coordinates  $x, y$  there exists  $f \in C$  such that  $f(x) \neq f(y)$ . Let  $G$  be a group with  $\langle \tau_h \mid h \in \Gamma\text{L}(m, q) \rangle \leq G \leq W$  such that  $G$  fixes  $C$  setwise and acts transitively on the set of nontrivial cosets of  $C \cap E$  in  $C$ .*

- (1) If  $E < C$  and  $|C| = (q^m)^{d+1}$  for some  $d \geq 1$  then there exists  $S \subseteq \text{GF}(q)^d$  of size  $n$  such that  $C$  is the restriction to  $S$  of the set of all affine functions  $f : \text{GF}(q)^d \rightarrow \text{GF}(q)^m$ . Moreover, there exists  $K \leq \text{A}\Gamma\text{L}(d, q)$  and a  $K$ -invariant subset  $S$  of  $\text{GF}(q)^d$  such that the projection of  $K$  onto  $\Gamma\text{L}(d, q)$  acts transitively on the set of 1-spaces of  $\text{GF}(q)^d$  and  $G = \langle \tau_h \mid h \in \text{GL}(m, q) \rangle \rtimes \Psi(K)$ .
- (2) If  $E \cap C = \{0\}$  and  $|C| = (q^m)^d$  for some  $d \geq 1$  then there exists  $S \subseteq \text{GF}(q)^d$  of size  $n$  such that  $C$  is the restriction to  $S$  of the set of linear functions  $f : \text{GF}(q)^d \rightarrow \text{GF}(q)^m$ . Moreover, there exists  $J \leq \Gamma\text{L}(d, q)$  and a  $J$ -invariant subset  $S$  of  $\text{GF}(q)^d$  such that  $J$  acts transitively on the set of 1-spaces of  $\text{GF}(q)^d$  and  $G = \langle \tau_h \mid h \in \text{GL}(m, q) \rangle \rtimes \Psi(J)$ .

Furthermore, in both (1) and (2), if  $m > 1$  then  $d = 1$ .

We have the following remarks.

- Remark 1.1.** 1. The codes in part (2) of Theorem 1.1 are constant weight codes and are replications of Hamming duals.
2. If  $d = 1$  then Theorem 1.1 only requires that  $S$  is a  $K$ - or  $J$ -invariant subset of  $\text{GF}(q)$ .
3. Suppose that  $J \leq \Gamma\text{L}(d, q)$  acts transitively on the set of 1-spaces of  $\text{GF}(q)^d$ . Letting  $Z$  be the group of scalars in  $\text{GL}(d, q)$  it follows that  $JZ$  is transitive on the set of nonzero vectors, that is,  $JZ$  is the point stabiliser in an affine 2-transitive group. All such groups are known (see [4, 5, 6]).

**Acknowledgements** The author would like to thank Cai Heng Li for bringing to his attention the work of Bonisoli, Ward and Wood, and Cheryl Praeger for helpful discussions.

## 2 Proof of Theorem 1.1

We begin by constructing the codes  $C$  and groups  $G$  stated in Theorem 1.1 and show that they have the desired properties.

Let  $M = \text{GF}(q)^m$  and let  $d$  be a positive integer such that if  $m > 1$  then  $d = 1$ . Let  $F$  be the vector space of all functions  $f : \text{GF}(q)^d \rightarrow M$ , let  $L$  be the subspace of all linear functions,  $E$  be the subspace of all constant functions and  $A = L \oplus E$  be the subspace of all affine functions.

Given  $S \subseteq \text{GF}(q)^d$  and  $f \in F$  we denote the restriction of  $f$  to  $S$  by  $f|_S$ . We have corresponding vector spaces  $F|_S, L|_S, E|_S$  and  $A|_S$ . Note that if  $S$  spans  $\text{GF}(q)^d$  then  $L \cong L|_S$  and  $A \cong A|_S$ . Recall the automorphisms  $\sigma_g$  and  $\tau_h$  of  $F$ .

We have the following lemma.

**Lemma 2.1.** *The subspace  $L$  is fixed setwise by each  $\tau_h$  such that  $h \in \text{GL}(m, q)$ , by each  $\sigma_g$  such that  $g \in \text{GL}(d, q)$  and by  $\tau_\phi \sigma_\phi$ . Moreover, if  $J \leq \Gamma\text{L}(d, q)$  acts transitively on the set of 1-spaces of  $\text{GF}(q)^d$  then  $\langle \tau_h \mid h \in \text{GL}(m, q) \rangle \rtimes \Psi(J)$  acts transitively on the set of nontrivial elements of  $L$ .*

*Proof.* Each  $\tau_h$  such that  $h \in \text{GL}(m, q)$  clearly fixes  $L$  setwise and  $L$  is a well known submodule for the permutation module of  $\text{GL}(d, q)$  and so each  $\sigma_g$  such that  $g \in \text{GL}(d, q)$  fixes  $L$  setwise. Hence the only nontrivial part is to prove that  $\tau_\phi \sigma_\phi$  fixes  $L$  setwise.

Let  $f : \text{GF}(q)^d \rightarrow M$  be a linear function. Then for all  $\mathbf{a}, \mathbf{b} \in \text{GF}(q)^d$ ,

$$\begin{aligned} f^{\tau_\phi \sigma_\phi}(\mathbf{a} + \mathbf{b}) &= (f((\mathbf{a} + \mathbf{b})^{\phi^{-1}}))^\phi \\ &= (f(\mathbf{a}^{\phi^{-1}} + \mathbf{b}^{\phi^{-1}}))^\phi \\ &= (f(\mathbf{a}^{\phi^{-1}}))^\phi + (f(\mathbf{b}^{\phi^{-1}}))^\phi \\ &= f^{\tau_\phi \sigma_\phi}(\mathbf{a}) + f^{\tau_\phi \sigma_\phi}(\mathbf{b}) \end{aligned}$$

and for all  $\lambda \in \text{GF}(q)$ ,

$$\begin{aligned} f^{\tau_\phi \sigma_\phi}(\lambda \mathbf{a}) &= (f((\lambda \mathbf{a})^{\phi^{-1}}))^\phi \\ &= (f(\lambda^{\phi^{-1}} \mathbf{a}^{\phi^{-1}}))^\phi \\ &= (\lambda^{\phi^{-1}} (f(\mathbf{a}^{\phi^{-1}})))^\phi \\ &= \lambda f^{\tau_\phi \sigma_\phi}(\mathbf{a}). \end{aligned}$$

Hence  $f^{\tau_\phi \sigma_\phi}$  is linear and so  $L$  is fixed setwise by  $\langle \tau_h \mid h \in \text{GL}(m, q) \rangle \rtimes \Psi(\Gamma\text{L}(d, q))$ .

Let  $J \leq \Gamma\text{L}(d, q)$  which acts transitively on the set of 1-spaces of  $\text{GF}(q)^d$ . By Block's Lemma [1],  $J$  also acts transitively on the set of hyperplanes of  $\text{GF}(q)^d$ . Let  $f_1, f_2 \in L$  be linear functions. Suppose first that  $d = 1$ . Then there exists  $h \in \text{GL}(m, q)$  such that  $f_1^{\tau_h} = f_2$  and so  $\langle \tau_h \mid h \in \text{GL}(m, q) \rangle \rtimes \Psi(J)$  acts transitively on the set of nontrivial elements of  $L$ .

Suppose now that  $d \geq 2$ . Note that this implies that  $M = \text{GF}(q)$  and so  $W_1 = \ker(f_1)$  and  $W_2 = \ker(f_2)$  both have dimension  $d - 1$ . Since  $J$  acts transitively on hyperplanes, there exists  $g \in J$  such that  $(W_1)^{g^{-1}} = W_2$ . Hence  $f_1^{\Psi(g)} = \lambda f_2$  for some  $\lambda \in \text{GF}(q)$ . Now there exists  $h \in \text{GL}(1, q)$  such

that  $\tau_h$  induces the automorphism of  $F$  corresponding to scalar multiplication by  $\lambda^{-1}$  and hence  $f_1^{\Psi(\sigma)\tau_h} = f_2$ . Thus  $\langle \tau_h \mid h \in \text{GL}(1, q) \rangle \rtimes \Psi(J)$  acts transitively on the set of nonzero elements of  $L$ .  $\square$

**Lemma 2.2.** *Let  $J \leq \Gamma L(d, q)$  which acts transitively on the set of 1-spaces of  $\text{GF}(q)^d$  and let  $S$  be a nontrivial  $J$ -invariant subset of  $\text{GF}(q)^d$ . Then  $\langle \tau_h \mid h \in \text{GL}(m, q) \rangle \rtimes \Psi(J)$  acts transitively on the set of nonzero elements of  $L|_S$ .*

*Proof.* Since  $J$  acts transitively on the set of 1-spaces of  $\text{GF}(q)^d$  it follows that  $S$  spans  $\text{GF}(q)^d$  and so  $L|_S \cong L$ . Let  $g \in J$ . As  $\Psi(g) \in \text{Aut}(F)$  and  $g$  fixes  $S$  setwise, it follows that  $\Psi(g)$  induces an automorphism of  $F|_S$  such that  $(f|_S)^{\Psi(g)} = (f^{\Psi(g)})|_S$ . Moreover,  $\langle \tau_h \mid h \in \text{GL}(m, q) \rangle \rtimes \Psi(J)$  fixes  $L|_S$  setwise. Since restriction to  $S$  intertwines the action of  $\Psi(J)$  on  $L$  and the action of  $\Psi(J)$  on  $L|_S$  it follows from Lemma 2.1 that  $\langle \tau_h \mid h \in \text{GL}(m, q) \rangle \rtimes \Psi(J)$  acts transitively on the set of nonzero elements of  $L|_S$ .  $\square$

We now look at the subspace  $A$  of all affine functions  $f : \text{GF}(q)^d \rightarrow M$ . We let  $\pi$  denote the projection map of  $\text{AGL}(d, q)$  onto  $\Gamma L(d, q)$ .

**Lemma 2.3.** *The subspace  $A$  is fixed setwise by each  $\tau_h$  such that  $h \in \text{GL}(m, q)$ , by each  $\sigma_g$  such that  $g \in \text{AGL}(d, q)$  and by  $\tau_\phi\sigma_\phi$ . Moreover, if  $K \leq \text{AGL}(d, q)$  such that  $\pi(K)$  acts transitively on the set of 1-spaces of  $\text{GF}(q)^d$ , then  $\langle \tau_h \mid h \in \text{GL}(m, q) \rangle \rtimes \Psi(K)$  acts transitively on the set of nonzero cosets of  $E$  in  $A$ .*

*Proof.* Clearly  $A$  is fixed setwise by  $\langle \tau_h \mid h \in \text{GL}(m, q) \rangle$ . It is also a well known submodule of the permutation module for  $\text{AGL}(d, q)$ , see for example [9, Section 3(B)]. Since  $\tau_\phi\sigma_\phi$  fixes  $E$  setwise and by Lemma 2.1 fixes  $L$  setwise, it follows that  $\tau_\phi\sigma_\phi$  fixes  $A = E \oplus L$  setwise.

Note that  $L$  provides a set of coset representatives for  $E$  in  $A$ . Let  $f_1, f_2 \in L$  be nontrivial linear functions. Suppose first that  $d = 1$ . Then  $f_1 = f_2^{\tau_h}$  for some  $h \in \text{GL}(m, q)$  and  $\langle \tau_h \mid h \in \text{GL}(m, q) \rangle \rtimes \Psi(K)$  acts transitively on the set of nontrivial cosets of  $E$  in  $A$ .

Suppose next that  $d \geq 2$ . Then  $M = \text{GF}(q)$  and  $W_1 = \ker(f_1)$  and  $W_2 = \ker(f_2)$  both have dimension  $d - 1$ . Since  $\pi(K)$  acts transitively on 1-spaces, by Block's Lemma [1] it also acts transitively on hyperplanes and so there exists  $g = g_1g_2 \in K$  such that  $g_1$  is a translation,  $g_2 \in \Gamma L(d, q)$ , and  $(W_1)^{g_2^{-1}} = W_2$ . Hence  $(E + f_1)^{\Psi(g)} = E + \lambda f_2$  for some  $\lambda \in \text{GF}(q)$ . Now there exists  $h \in \text{GL}(1, q)$  such that  $\tau_h$  induces the automorphism of  $F$  corresponding to scalar multiplication by  $\lambda^{-1}$  and hence  $(E + f_1)^{\Psi(g)\tau_h} = E + f_2$ . Thus  $\langle \tau_h \mid h \in \text{GL}(1, q) \rangle \rtimes \Psi(K)$  acts transitively by conjugation on the set of nontrivial cosets of  $E$  in  $A$ .  $\square$

**Lemma 2.4.** *Let  $K \leq \text{AGL}(d, q)$  such that  $\pi(K)$  acts transitively on the set of 1-spaces of  $\text{GF}(q)^d$  and let  $S$  be a nontrivial  $K$ -invariant subset of  $\text{GF}(q)^d$ . Then  $\langle \tau_h \mid h \in \text{GL}(m, q) \rangle \rtimes \Psi(K)$  acts transitively on the set of nontrivial cosets of  $E|_S$  in  $A|_S$ .*

*Proof.* This follows from Lemma 2.3 in the same manner that Lemma 2.2 follows from Lemma 2.1.  $\square$

We now determine all  $C$  satisfying the hypotheses of Theorem 1.1.

**Proposition 2.1.** *Let  $E < C \leq M^n$  such that  $|C| = |M|^{d+1}$  for some positive integer  $d \geq 1$  and for any two distinct coordinates  $x, y$ , there exists  $f \in C$  such that  $f(x) \neq f(y)$ . Suppose that there exists  $G$  with  $\langle \tau_h \mid h \in \text{GL}(m, q) \rangle \leq G \leq W$  such that  $G$  acts transitively on the set of nontrivial cosets of  $E$  in  $C$ . Then there exists a spanning subset  $S \subseteq \text{GF}(q)^d$  such that  $C$  is the restriction to  $S$  of all affine functions from  $f : \text{GF}(q)^d \rightarrow M$ . Moreover, if  $m > 1$  then  $d = 1$ .*

*Proof.* Suppose first that  $m = 1$ , that is  $M = \text{GF}(q)$ . Let  $D$  be a  $(d+1) \times n$  matrix over  $\text{GF}(q)$  whose rows form a basis for  $C$  as a  $\text{GF}(q)$ -space, such that the first row is  $(1, 1, \dots, 1) \in E$ , and let  $S$  be the set of column vectors of  $D$  with the first coordinate removed, so  $S \subseteq \text{GF}(q)^d$ . If two of the column vectors of  $D$  were equal then we would have a pair of distinct coordinates  $x, y$  such that  $f(x) = f(y)$  for all  $f \in C$ , a contradiction. Thus  $D$  has no repeated columns and so there are at most  $q^d$  choices for the columns of  $D$ . Hence  $n = |S| \leq q^d$ . Furthermore, as the rank of  $D$  with the first row removed is  $d$ , it follows that  $S$  spans  $\text{GF}(q)^d$ . For  $1 \leq i \leq d$ , the  $(i+1)^{\text{th}}$  row of  $D$  gives the  $i^{\text{th}}$  coordinate of each element of  $S$ , and hence is the evaluation of the  $i^{\text{th}}$  projection map from  $\text{GF}(q)^d$  to  $M$  at the vectors in  $S$ . Thus the last  $d$  rows of  $D$  provide a basis for the group of all linear functions  $f : \text{GF}(q)^d \rightarrow M$  restricted to  $S$ , where we think of each vector of length  $n$  in the space generated by the last  $d$  rows of  $D$  as the evaluation of some linear map on  $S$ . In addition, the first row is the restriction of a constant function to  $S$  and so  $C$  is the set of restrictions to  $S$  of all affine functions  $f : \text{GF}(q)^d \rightarrow M$ .

Now suppose that  $m \geq 2$ . In this case  $C$  is invariant under  $\langle \tau_h \mid h \in \text{GL}(m, q) \rangle$ . Since  $\text{GL}(m, q)$  contains a subgroup isomorphic to  $\text{GL}(1, q^m)$ ,  $G$  contains a subgroup  $\{\tau_h \mid h \in \text{GL}(1, q^m)\}$  which preserves a  $\text{GF}(q^m)$ -structure on  $M$ . However, since  $\langle \tau_h \mid h \in \text{GL}(m, q) \rangle \leq G$ , it follows that  $G$  does not preserve such a structure. Thinking of  $M$  as the additive group of  $\text{GF}(q^m)$  and  $C$  as a  $\text{GF}(q^m)$ -space, we can find  $d+1$  linearly independent functions which generate  $C$ , the first of which can be taken to be the constant function

$(1, 1, \dots, 1)$ , which lies in  $E$ . Let  $D$  be the  $(d+1) \times n$  matrix whose rows are given by the evaluation of these  $d+1$  functions and note that  $n \geq d+1$  since  $C \cong M^{d+1} \leq M^n$ . As  $C$  has dimension  $d+1$  over  $\text{GF}(q^m)$  we can echelonize  $D$  so that it is of the form

$$\begin{pmatrix} 1 & 1 \dots 1 & 1 \dots 1 \\ 0 & & \\ \vdots & I_{d \times d} & B \\ 0 & & \end{pmatrix}$$

where  $B$  is a  $d \times (k-d-1)$  matrix whose entries lie in  $\text{GF}(q^m)$ .

Suppose that  $B$  contains an entry  $x$  which does not belong to the subfield  $\text{GF}(q)$  and let  $\mathbf{v}$  be the row of  $D$  containing such an element. Now  $\text{GL}(m, q)$  contains a subgroup isomorphic to  $\Gamma\text{L}(1, q^m)$ , and hence  $G$  contains an element  $\tau_h$  such that  $h \in \text{GL}(m, q)$  centralises 1 but does not centralise  $x$ . Then  $\tau_h$  maps  $\mathbf{v}$  to a vector whose first  $d+1$  entries agree with  $\mathbf{v}$  but at least one of the last  $n-d-1$  entries does not agree with  $\mathbf{v}$ . However,  $G$  preserves  $C$  and any element of  $C$  agreeing with  $\mathbf{v}$  in the first  $d+1$  coordinates must be equal to  $\mathbf{v}$ . This contradicts  $\mathbf{v}^{\tau_h} \neq \mathbf{v}$ . Hence all the entries of  $B$  lie in the subfield  $\text{GF}(q)$ .

Recall that for each  $\bar{g} \in G$ , there exists  $h \in \Gamma\text{L}(m, q)$  and  $g \in S_n$  such that for all  $f \in C$  and  $x \in X$  we have  $f^{\bar{g}}(x) = (f(x^{g^{-1}}))^h$ . It follows that the number  $r(f)$  of distinct values in  $\text{GF}(q)^m$  taken by the values of  $f$  is constant over  $G$ -orbits in  $C$ . Also  $r(f)$  is constant over all vectors in  $E + f$ . Since  $G$  acts transitively on the set of nontrivial cosets of  $C/E$  it follows that  $r(f)$  is constant on  $C \setminus E$ , equal to  $r$  say. Suppose that  $d \geq 2$  and let  $\mathbf{v}_1$  and  $\mathbf{v}_2$  be the last two rows of the matrix  $D$ . Let  $\lambda \in \text{GF}(q^m) \setminus \text{GF}(q)$  and let  $\mathbf{w} = \mathbf{v}_1 + \lambda \mathbf{v}_2 \in C \setminus E$ . We need to determine the number of values in  $\text{GF}(q^m)$  taken by  $\mathbf{w}$ . We have already seen that the entries in  $\mathbf{v}_1$  and in  $\mathbf{v}_2$  lie in  $\text{GF}(q)$  and so the entries of  $\mathbf{w}$  are of the form  $a + \lambda b$  for some  $a, b \in \text{GF}(q)$ . Now if  $a_1 + \lambda b_1 = a_2 + \lambda b_2$  for some  $a_1, b_1, a_2, b_2 \in \text{GF}(q)$  then  $1(a_1 - a_2) + \lambda(b_1 - b_2) = 0$ . Then as 1 and  $\lambda$  are  $\text{GF}(q)$ -linearly independent in  $\text{GF}(q^m)$ , it follows that  $a_1 = a_2$  and  $b_1 = b_2$ . Hence  $\mathbf{w}$  takes on precisely  $r$  values in  $\text{GF}(q^m)$  if and only if, whenever the  $i^{\text{th}}$  and  $j^{\text{th}}$  coordinates of  $\mathbf{v}_1$  are equal then so are the  $i^{\text{th}}$  and  $j^{\text{th}}$  coordinates of  $\mathbf{v}_2$ . However, since  $d \geq 2$ , we see that the  $(d-1)^{\text{th}}$  and  $(d+1)^{\text{th}}$  coordinates of  $\mathbf{v}_1$  are both equal to 0 but the  $(d-1)^{\text{th}}$  coordinate of  $\mathbf{v}_2$  is equal to 0 while the  $(d+1)^{\text{th}}$  coordinate is equal to 1. Hence  $d = 1$ .

Now let  $S$  be the set of  $n$  columns of  $D$  with the first entry removed. There is no repetition amongst the elements of  $S$ , and so  $n = |S|$  and we can regard  $S$  as a subset of  $\text{GF}(q)$ . Furthermore, the first row is the evaluation of

a constant function from  $\text{GF}(q)$  to  $M$  restricted to  $S$ , while the second row is the evaluation of a linear function from  $\text{GF}(q)$  to  $M$  restricted to  $S$ . Hence  $C$  is the restriction to  $S$  of the set of all affine functions  $f : \text{GF}(q) \rightarrow M$ . Thus the proposition is proved.  $\square$

**Corollary 2.1.** *Let  $C' \leq M^n$  such that  $|C'| = |M|^d$  for some positive integer  $d \geq 1$  and for any two coordinates  $x, y \in X$ , there exists  $f \in C'$  such that  $f(x) \neq f(y)$ . Suppose that there exists a group  $G$  with  $\langle \tau_h \mid h \in \text{GL}(m, q) \rangle \leq G \leq W$  which acts transitively on the set of nonzero vectors of  $C'$ . Then there exists a spanning subset  $S \subseteq \text{GF}(q)^d$  such that  $C$  is the restriction to  $S$  of all linear functions from  $\text{GF}(q)^d$  to  $M$ . Moreover, if  $m > 1$  then  $d = 1$ .*

*Proof.* Since  $E \cap C' = \{0\}$  and  $E$  is fixed setwise by  $G$  it follows that  $C = E \oplus C'$ , which has size  $|M|^{d+1}$ , is determined by Proposition 2.1. The result then follows by taking the last  $d$  rows of the generator matrix in the proof of Proposition 2.1 to be a set of generators for  $C'$ .  $\square$

We now turn our attention to finding  $G$ .

**Proposition 2.2.** *Let  $d \geq 1$  and  $S$  be a spanning subset of  $\text{GF}(q)^d$  such that  $C \leq M^n$  is the restriction to  $S$  of the set of all affine functions from  $\text{GF}(q)^d$  to  $M$ . Suppose that there exists  $\langle \tau_h \mid h \in \text{GL}(m, q) \rangle \leq G \leq W$  which acts transitively on the set of nontrivial cosets of  $E$  in  $C$ . Then there exists  $K \leq \text{AFL}(d, q)$  such that  $S$  is a  $K$ -invariant subset,  $\pi(K)$  acts transitively on the set of 1-spaces of  $\text{GF}(q)^d$  and  $G = \langle \tau_h \mid h \in \text{GL}(m, q) \rangle \rtimes \Psi(K)$ .*

*Proof.* Let  $\bar{g} \in G$ . Since  $\langle \tau_h \mid h \in \text{GL}(m, q) \rangle \leq G$  and  $\Gamma\text{L}(m, q) = \text{GL}(m, q) \rtimes \langle \phi \rangle$ , we may assume that  $\bar{g} = \tau_{\phi^i} \sigma_g \in G$ , where  $g \in S_n$  and  $0 \leq i \leq |\phi| - 1$ . Then  $\bar{g}$  is a semilinear map of the vector space  $M^n$ , where  $(\lambda f)^{\bar{g}} = \lambda^{\phi^i} f^{\bar{g}}$  for each  $f \in M^n$  and  $\lambda \in \text{GF}(q)$ . Also  $\bar{g}$  fixes setwise  $C \leq M^n$  and so  $\bar{g}^C$  is a semilinear map with associated field automorphism  $\phi^i$ . Hence if  $\phi^i \neq 1$  then  $\bar{g}^C \neq 1$ . If  $\bar{g} = \sigma_g \in S_n$  with  $g \neq 1$ , then we also have  $\bar{g}^C \neq 1$ , as otherwise there would exist distinct  $x, y \in X$  such that  $f(x) = f(y)$  for all  $f \in C$ , a contradiction.

Recall the  $(d+1) \times n$  matrix  $D$  which generates  $C$  (as a  $\text{GF}(q^m)$ -space) and the set  $S \subseteq \text{GF}(q)^d \subseteq \text{GF}(q^m)^d$  of column vectors of  $D$  with their first entry removed. Let  $S = \{\mathbf{a}_1, \dots, \mathbf{a}_n\}$  such that  $\mathbf{a}_j$  corresponds to the  $j^{\text{th}}$  column of  $D$  and note that  $g \in S_n$  gives a permutation of  $S$  such that  $(\mathbf{a}_j)^g = \mathbf{a}_{jg}$ . We aim to construct from  $\bar{g} = \tau_{\phi^i} \sigma_g \in G$ , an element  $g' \in \text{AFL}(d, q)$  such that  $g'$  fixes  $S$  setwise,  $(g')^S = g^S$  and the associated field automorphism of  $g'$  is  $\phi^i$ .

Let  $f \in C$  be a row of  $D$ , that is, the  $i^{\text{th}}$  entry of  $f$  is  $f(\mathbf{a}_i)$ , where  $\mathbf{a}_i \in S$  corresponds to the  $i^{\text{th}}$  column of  $D$ . Then  $f^{\bar{g}} \in C$  as  $G$  fixes  $C$  setwise. If

$m = 1$  then  $M = \text{GF}(q)$  and so  $f^{\bar{g}}$  is a  $\text{GF}(q)$ -linear combination of the rows of  $D$ . On the other hand, if  $m \geq 2$  then  $M = \text{GF}(q)^m$ . However, since the rows of  $D$  lie in  $\text{GF}(q)^n$  and  $\bar{g} = \tau_{\phi^i} \sigma_g$  fixes  $\text{GF}(q)^n$  setwise, we also have that  $f^{\bar{g}}$  is a  $\text{GF}(q)$ -linear combination of the rows of  $D$ . As this is true for each row of  $D$ , there is a matrix  $Q \in \text{GL}(d+1, q)$  such that for each  $j$ , the  $j^{\text{th}}$  row of  $QD$  is the image of the  $j^{\text{th}}$  row of  $D$  under  $\bar{g}$ . Moreover, as  $\bar{g}$  centralises the first row  $(1, \dots, 1)$  of  $D$  and  $S$  spans  $\text{GF}(q)^d$ , it follows that

$$Q = \begin{pmatrix} 1 & \mathbf{0}_{1 \times d} \\ \mathbf{b} & P \end{pmatrix}$$

where  $\mathbf{b} \in \text{GF}(q)^d$  and  $P \in \text{GL}(d, q)$ .

Now for each  $\mathbf{a}_j \in S$  we have that  $f^{\bar{g}}(\mathbf{a}_j) = (f(\mathbf{a}_{jg^{-1}}))^{\phi^i}$ . On the other hand,  $f^{\bar{g}}$  corresponds to the same row of  $QD$  as  $f$  corresponds to in  $D$ , and  $f^{\bar{g}}(\mathbf{a}_j)$  is the  $j^{\text{th}}$  entry of the row of  $QD$  associated with  $f^{\bar{g}}$ . Hence as,

$$Q \begin{bmatrix} 1 \\ \mathbf{a}_j \end{bmatrix} = \begin{bmatrix} 1 \\ \mathbf{b} + P\mathbf{a}_j \end{bmatrix}$$

it follows that

$$\mathbf{b} + P\mathbf{a}_j = (\mathbf{a}_{jg^{-1}})^{\phi^i}.$$

Hence  $\mathbf{a}_{jg^{-1}} = (\mathbf{b} + P\mathbf{a}_j)^{\phi^{-i}}$ . Thus we can define an element  $g' \in \text{AFL}(d, q)$  by  $\mathbf{a}^{(g')^{-1}} = (\mathbf{b} + P\mathbf{a})^{\phi^{-i}}$ , for all  $\mathbf{a} \in \text{GF}(q)^d$ , such that  $g'$  fixes  $S$  setwise and  $(g')^S = g^S$ . Let

$$K = \langle g' \mid \tau_{\phi^i} \sigma_g \in G \rangle \leq \text{AFL}(d, q).$$

Then  $S$  is a  $K$ -invariant subset of  $\text{GF}(q)^d$  and  $G^{\{1, 2, \dots, n\}} = K^S$ . Note also, that  $\bar{g} = \tau_{\phi^i} \sigma_g = \Psi(g')$ , and so  $G = \langle \tau_h \mid h \in \text{GL}(m, q) \rangle \rtimes \Psi(K)$ .

All that remains to prove is that  $\pi(K)$  acts transitively on the set of 1-spaces of  $\text{GF}(q)^d$ . Now  $G$  acts transitively on  $C/E \cong M^d$ . If  $d = 1$  then we trivially have that  $\pi(K)$  acts transitively on 1-spaces and so we assume that  $d \geq 2$ . Thus by Proposition 2.1,  $m = 1$  and  $G = \langle \tau_h \mid h \in \text{GL}(1, q) \rangle \rtimes \Psi(K)$ . As  $\langle \tau_h \mid h \in \text{GL}(1, q) \rangle$  induces scalar multiplication on  $C$ , it follows that  $\Psi(K)$  acts transitively on the set of 1-dimensional subspaces of  $C/E$ . Let  $W_1$  and  $W_2$  be distinct hyperplanes of  $\text{GF}(q)^d$ . Then there exist linear functions  $f_1, f_2 : \text{GF}(q)^d \rightarrow M$  such that  $\ker(f_1) = W_1$  and  $\ker(f_2) = W_2$ . Moreover,  $(f_1)|_S, (f_2)|_S \in C$  and lie in different  $E$ -cosets. Hence there exists  $\bar{g} \in \Psi(K)$  such that  $(E + f_1)^{\bar{g}} = E + \lambda f_2$ . Then  $\bar{g} = \tau_{\phi^i} \sigma_g$  for some  $g \in K$ . Let  $g = g_1 g_2$  such that  $g_1$  is a translation and  $g_2 \in \Gamma\text{L}(d, q)$ . All functions in  $E + f_1$  are constant on  $W_1$  (since  $W_1 = \ker(f_1)$ ) and so are all functions of  $(E + f_1)^{\tau_{\phi^i} g_1}$ . Meanwhile all functions of  $E + \lambda f_2$  are constant on  $W_2$  and so  $W_1^{g_2^{-1}} = W_2$ .

Thus  $\pi(K)$  acts transitively on the set of hyperplanes of  $\text{GF}(q)^d$ . Hence by Block's Lemma,  $\pi(K)$  acts transitively on the set of 1-spaces and the proof is complete.  $\square$

**Corollary 2.2.** *Let  $d \geq 1$  and  $S$  be a spanning subset  $\text{GF}(q)^d$  such that  $C' \leq M^n$  is the restriction to  $S$  of the set of all linear functions from  $\text{GF}(q)^d$  to  $M$ . Suppose that there exists  $G$  with  $\langle \tau_h \mid h \in \text{GL}(m, q) \rangle \leq G \leq W$  which acts transitively on the set of nonzero vectors of  $C'$ . Then there exists  $J \leq \Gamma\text{L}(d, q)$  such that  $S$  is  $J$ -invariant,  $J$  is transitive on the set of 1-spaces of  $\text{GF}(q)^d$  and  $G = \langle \tau_h \mid h \in \text{GL}(m, q) \rangle \rtimes \Psi(J)$ .*

*Proof.* Since  $E \cap C' = \{0\}$  and  $E$  is fixed setwise by  $G$  it follows that  $G$  acts transitively on the set of nontrivial cosets of  $E$  in  $C = E \oplus C'$ . Thus  $G$  is determined by Proposition 2.2 and so there exists  $K \leq \text{A}\Gamma\text{L}(d, q)$  such that  $G = \langle \tau_h \mid h \in \text{GL}(m, q) \rangle \rtimes \Psi(K)$ . Since each  $\bar{g} = \tau_{\phi^i} \sigma_g \in G$  fixes both  $E$  and  $C'$  setwise, it follows that the matrix  $Q$  obtained in the proof of Proposition 2.2 is completely decomposable and so the permutation  $g'$  obtained in  $\text{A}\Gamma\text{L}(d, q)$  actually lies in  $\Gamma\text{L}(d, q)$ . Letting  $J = K = \pi(K)$ , the result follows.  $\square$

## References

- [1] R. E. Block, On automorphism groups of block designs, *J. Combinatorial Theory*, 5 (1968), 293–301.
- [2] A. Bonisoli, Every equidistant linear code is a sequence of dual Hamming codes, *Ars Combinatoria*, 18 (1983), 181–186.
- [3] M. Giudici, C. H. Li, and C. E. Praeger, Locally  $s$ -arc transitive graphs with two different quasiprimitive actions, submitted.
- [4] C. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order, *Geometriae Dedicata*, 2 (1974), 425–460.
- [5] C. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order. II, *J. Algebra*, 93 (1985), no. 1, 151–164.
- [6] M. W. Liebeck, The affine permutation groups of rank three, *Proceedings of the London Mathematical Society* (3), 54 (1987), 477–516.

- [7] F. J. MacWilliams, Combinatorial properties of elementary abelian groups, (Ph.D. thesis, Radcliffe College, Cambridge, Massachusetts, 1962).
- [8] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes. I, (North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977).
- [9] B. Mortimer, The modular permutation representations of the known doubly transitive groups, Proc. London Math. Soc. (3), 41 (1980), 1–20.
- [10] H. N. Ward, A bound for divisible codes, IEEE Trans. Inform. Theory, 38 (1992), 191–194.
- [11] H. N. Ward and J. A. Wood, Characters and the equivalence of codes, J. Combin. Theory Ser. A, 73 (1996), 348–352.