Available online at www.sciencedirect.com

SCIENCE DIRECT®

ELSEVIER

Finite Fields and Their Applications 12 (2006) 232–247

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

Information sets and partial permutation decoding for codes from finite geometries

J.D. Key[a,*,1,2], T.P. McDonough[b,2], V.C. Mavron[b,2]

[a] *Department of Mathematical Sciences, Clemson University, 0-106 Martin Hall, Clemson, SC 29634, USA*

[b] *Institute of Mathematical and Physical Sciences, University of Wales, Aberystwyth, Ceredigion SY23 3BZ, UK*

Received 4 August 2004; revised 28 April 2005

Communicated by Gary L. Mullen

Available online 29 June 2005

Abstract

We determine information sets for the generalized Reed–Muller codes and use these to apply partial permutation decoding to codes from finite geometries over prime fields. We also obtain new bases of minimum-weight vectors for the codes of the designs of points and hyperplanes over prime fields.

PACS: 05; 51; 94

Keywords: Codes; Finite geometries; Designs

[*] Corresponding author. Fax: +1 864 656 5230.

E-mail address: keyj@clemson.edu (J.D. Key).

[1] This work was supported by the DoD Multidisciplinary University Research Initiative (MURI) program administered by the Office of Naval Research under Grant N00014-00-1-0565.

[2] EPSRC grant GR/S95879/01 support acknowledged by all the authors.

1071-5797/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2005.05.007

1. Introduction

In the 1960s, the codes obtained from the row span of the incidence vectors of the blocks of designs obtained from finite geometries were shown to have some useful properties which made them good candidates for practical usage: see [AK92] for references to this work. In particular, the dual codes of those from planes were capable of being used with majority-logic decoding. MacWilliams [Mac64] at this time introduced the notion of permutation decoding and applied it mainly to cyclic codes and the Golay codes. In [KMM], codes from planes were looked at with a view to permutation decoding; here we obtain similar results for the codes of higher dimensional geometries, mostly in the case of those over prime fields.

The codes from finite geometries are the generalized Reed–Muller codes and their subfield subcodes. They have the projective and affine semi-linear groups as automorphism groups. We found in [KMM] that permutation decoding to correct up to the full capability of the code cannot be used for the whole class of codes from planes as the order of the plane increases; this is due to the existence of a lower bound (see Result 1) on the size of the PD-set, which depends on the length, dimension and minimum weight of the code, and which is larger than the size of the full automorphism group above a certain field order. The same will hold for the codes of higher dimensional geometries, for the same reasons. Thus we introduced the notion of s-PD-sets to correct s errors, where s may be lower than the full error-correction capability. We examine these again here in the higher dimensional cases. Also we note that suitable information sets need to be found for the decoding; we were aided in this in the case of planes of prime order through the previously known bases for the codes that were obtained using the geometry of the plane: see Moorhouse [Moo91]. Here we will obtain suitable information sets, at least in the prime case, linked to the polynomial basis for the codes.

Our principle results for information sets and bases are Theorem 1, Corollary 2 and Proposition 5. In Theorem 1 we obtain information sets for a class of polynomial codes that includes the q-ary generalized Reed–Muller codes $\mathcal{R}_{\mathbb{F}_q}(v, m)$, and in Corollary 2 a particularly simple information set is given in the case where q is a prime. This then applies in particular to the codes from the affine geometry designs over fields of prime order, and this leads to information sets for the codes of projective geometry designs (see Section 5). From this we can obtain a simple description for bases of minimum-weight vectors for the codes of the symmetric point-hyperplane designs in the prime case which leads to similar bases of minimum-weight vectors for the affine point-hyperplane designs: see Proposition 5. These bases are different in general from those found in [GK98].

The establishment of information sets is of assistance in the search for s-PD-sets and here our main results are Propositions 1, 2 and 6. In Proposition 1 we show that the translation group will provide an s-PD-set, within certain bounds for s, for $\mathcal{R}_{\mathbb{F}_q}(v, m)$, and we obtain, for q a prime, some relatively small 2-PD-sets for the point-hyperplane designs in the affine case in Proposition 2 and in the projective case in Proposition 6.

The paper is laid out as follows: in Section 2 we give the background notation and definitions; in Section 3 we obtain the information sets; in Section 4 we examine partial permutation decoding in the affine case; in Section 5 we apply the previous results to the projective geometry designs.

2. Background

An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a t-(v, k, λ) design, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks. The design is *symmetric* if it has the same number of points and blocks. The code $C_p(\mathcal{D})$ of $\mathcal{D}$ over the finite field $\mathbb{F}_p$, is the space spanned by the incidence vectors of the blocks over $\mathbb{F}_p$, and is thus a subspace of $\mathbb{F}_p^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to $\mathbb{F}_p$. Its dimension is called the *p-rank of* $\mathcal{D}$.

The notation $[n, k, d]_q$ will denote a linear code C of length n, dimension k, and minimum weight d, over the field $\mathbb{F}_q$. A generator matrix for the code is a $k \times n$ matrix made up of a basis for C. The dual code $C^{\perp}$ is the orthogonal subspace under the standard inner product $(,)$, i.e. $C^{\perp} = \{v \in \mathbb{F}_q^n | (v, c) = 0 \text{ for all } c \in C\}$. A check matrix for C is a generator matrix H for $C^{\perp}$; the *syndrome* of a vector $y \in \mathbb{F}_q^n$ is Hy^T. If $c \in C$ then the *support* of c is the set of non-zero coordinate positions of c, and the *weight* of c is the cardinality of the support. Two linear codes of the same length and over the same field are *isomorphic* if they can be obtained from one another by permuting the coordinate positions. Any linear code is isomorphic to a code with generator matrix in so-called *standard form*, i.e. the form $[I_k \mid A]$; a check matrix then is given by $[-A^T \mid I_{n-k}]$. The first k coordinates are the *information symbols* (or set) and denoted by $\mathcal{I}$, and the last $n - k$ coordinates are the *check symbols*, denoted by $\mathcal{C}$. An *automorphism* of a code C is an isomorphism from C to C. The automorphism group will be denoted by $\mathrm{Aut}(C)$.

For any finite field $\mathbb{F}_q$ of order q, the set of points and r-dimensional subspaces of an m-dimensional projective geometry forms a 2-design which we will denote by $PG_{m,r}(\mathbb{F}_q)$. Similarly, the set of points and r-dimensional flats of an m-dimensional affine geometry forms a 2-design, $AG_{m,r}(\mathbb{F}_q)$. The automorphism groups of these designs (and codes) are the full projective or affine semi-linear groups, $P\Gamma L_{m+1}(\mathbb{F}_q)$ or $A\Gamma L_m(\mathbb{F}_q)$, and are always 2-transitive on points. If $q = p^e$ where p is a prime, the codes of these designs are over $\mathbb{F}_p$ and are subfield subcodes of the generalized Reed–Muller codes: see [AK92, Chapter 5] for a full treatment. The dimension and minimum weight is known in each case: see [AK92, Theorem 5.7.9].

Permutation decoding was first developed by MacWilliams [Mac64] and involves finding a set of automorphisms of a code called a PD-set. The method is described fully in MacWilliams and Sloane [MS83, Chapter 15] and Huffman [Huf98, Section 8]. We extend the definition of PD-sets to s-PD-sets for s-error-correction:

Definition 1. If C is a t-error-correcting code with information set $\mathcal{I}$ and check set $\mathcal{C}$, then a PD-set for C is a set $\mathcal{S}$ of automorphisms of C which is such that every t-set of coordinate positions is moved by at least one member of $\mathcal{S}$ into the check positions $\mathcal{C}$.

For $s \leqslant t$ an s-PD-set is a set $\mathcal{S}$ of automorphisms of C which is such that every s-set of coordinate positions is moved by at least one member of $\mathcal{S}$ into $\mathcal{C}$.

That a PD-set will fully use the error-correction potential of the code follows easily and is proved in Huffman [Huf98, Theorem 8.1], and that an s-PD-set will correct s errors follows in a similar manner.

The algorithm for permutation decoding is as follows: we have a t-error-correcting $[n, k, d]_q$ code C with check matrix H in standard form. Thus the generator matrix $G = [I_k|A]$ and $H = [-A^T|I_{n-k}]$, for some A, and the first k coordinate positions correspond to the information symbols. Any vector v of length k is encoded as vG. Suppose x is sent and y is received and at most s errors occur, where $s \leqslant t$. Let $\mathcal{S} = \{g_1, \ldots, g_m\}$ be an s-PD-set. Compute the syndromes $H(yg_i)^T$ for $i = 1, \ldots, m$ until an i is found such that the weight of this vector is s or less. Compute the codeword c that has the same information symbols as yg_i and decode y as cg_i^{-1}.

Such sets might not exist at all, and the property of having a PD-set will not, in general, be invariant under isomorphism of codes, i.e. it depends on the choice of $\mathcal{I}$ and $\mathcal{C}$. Furthermore, there is a bound on the minimum size of $\mathcal{S}$ (see [Gor82,Sch64], or [Huf98]):

Result 1. *If $\mathcal{S}$ is a PD-set for a t-error-correcting $[n, k, d]_q$ code C, and $r = n - k$, then* $|\mathcal{S}| \geqslant \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil$.

This result can be adapted to s-PD-sets for $s \leqslant t$ by replacing t by s in the formula.

To obtain PD-sets, a generator matrix for the code needs to be in standard form, and thus the question of what points to take as information symbols arises.

We use the notation of [AK92, Chapter 5] or [AK98] for generalized Reed–Muller codes. Let $q = p^t$, where p is a prime, and let V be the vector space $\mathbb{F}_q^m$ of m-tuples, with standard basis. The codes will be q-ary codes with ambient space the function space $\mathbb{F}_q^V$, with the usual basis of characteristic functions of the vectors of V. We can denote the elements f of $\mathbb{F}_q^V$ by functions of the m-variables denoting the coordinates of a variable vector in V, i.e. if $\mathbf{x} = (x_1, x_2, \ldots, x_m) \in V$, then $f \in \mathbb{F}_q^V$ is given by $f = f(x_1, x_2, \ldots, x_m)$ and the x_i take values in $\mathbb{F}_q$. Since $a^q = a$ for $a \in \mathbb{F}_q$, the polynomial functions can be reduced modulo $x_i^q - x_i$. Furthermore, every polynomial can be written uniquely as a linear combination of the q^m monomial functions

$$\mathcal{M} = \{x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m} \mid 0 \leqslant i_k \leqslant q-1, \text{ for } 1 \leqslant k \leqslant m\}.$$

For any such monomial the degree ρ is the total degree, i.e. $\rho = \sum_{k=1}^m i_k$ and clearly $0 \leqslant \rho \leqslant m(q-1)$.

The generalized Reed–Muller codes are defined as follows (see [AK92, Definition 5.4.1]):

Definition 2. Let $V = \mathbb{F}_q^m$ be the vector space of m-tuples, for $m \geqslant 1$, over $\mathbb{F}_q$, where $q = p^t$ and p is a prime. For any ρ such that $0 \leqslant \rho \leqslant m(q-1)$, the ρth-order generalized

Reed–Muller code $\mathcal{R}_{\mathbb{F}_q}(\rho, m)$ is the subspace of $\mathbb{F}_q^V$ (with basis the characteristic functions of vectors in V) of all m-variable polynomial functions (reduced modulo $x_i^q - x_i$) of degree at most ρ. Thus

$$\mathcal{R}_{\mathbb{F}_q}(\rho, m) = \left\langle x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m} | 0 \leqslant i_k \leqslant q-1, \text{ for } 1 \leqslant k \leqslant m, \ \sum_{k=1}^{m} i_k \leqslant \rho \right\rangle.$$

These codes are thus codes of length q^m and the codewords are obtained by evaluating the m-variable polynomials in the subspace at all the points of the vector space $V = \mathbb{F}_q^m$. From [AK92, Theorem 5.4.2] we know that $\mathcal{R}_{\mathbb{F}_q}(v, m)^{\perp} = \mathcal{R}_{\mathbb{F}_q}(\mu, m)$ for $v < m(q-1)$ and where $v + \mu + 1 = m(q-1)$.

The code $\mathcal{R}_{\mathbb{F}_p}((m-r)(p-1), m)$ is the p-ary code of the affine geometry design $AG_{m,r}(\mathbb{F}_p)$: see [AK92, Theorem 5.7.9].

3. Information sets

In this section we determine some useful information sets for the generalized Reed–Muller codes that will be used in later sections to obtain some small 2-PD-sets for some of the codes from geometries, and also to obtain bases of minimum-weight vectors for the codes from affine and projective point-hyperplane designs in the prime case.

The set of monomial functions of degree at most v,

$$\mathcal{B} = \left\{ x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m} \mid 0 \leqslant i_k \leqslant q-1, \text{ for } 1 \leqslant k \leqslant m, \ \sum_{k=1}^{m} i_k \leqslant v \right\},$$

is an $\mathbb{F}_q$-basis of $\mathcal{R}_{\mathbb{F}_q}(v, m)$. A subset $S \subseteq V = \mathbb{F}_q^m$ will be an information set of the code if, and only if, the subspace of $\mathbb{F}_q^S$ spanned by the restriction of $\mathcal{B}$ to S has dimension $|\mathcal{B}|$.

The following theorem holds for a wider class of codes spanned by monomials and we state and prove it in the more general form

Theorem 1. *Let $V = \mathbb{F}_q^m$ be the vector space of m-tuples, for $m \geqslant 1$, over the finite field $\mathbb{F}_q$ of order q, where $q = p^t$ and p is a prime. Let $\alpha_0, \ldots, \alpha_{q-1}$ be the elements of $\mathbb{F}_q$ and let*

$$\mathcal{S} = \{[i_1, i_2, \ldots, i_m] | i_k \in \mathbb{Z}, \ 0 \leqslant i_k \leqslant q-1, \ 1 \leqslant k \leqslant m\}.$$

Let $\leqslant$ denote the partial order defined on S by $[i_1, i_2, \ldots, i_m] \leqslant [j_1, j_2, \ldots, j_m]$ if and only if $i_k \leqslant j_k$ for all k such that $1 \leqslant k \leqslant m$.

Let $\mathcal{X} \subseteq \mathcal{S}$ have the property that $y \in \mathcal{X}$ if $y \in \mathcal{S}$ and $y \leqslant x$ for some $x \in \mathcal{X}$, and let $C = \langle x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m} \mid [i_1, i_2, \ldots, i_m] \in \mathcal{X} \rangle$. Then the set of vectors

$$\mathcal{I} = \{(\alpha_{i_1}, \ldots, \alpha_{i_m}) \mid [i_1, i_2, \ldots, i_m] \in \mathcal{X}\}$$

is an information set for C.

In particular, if $\mathcal{X} = \{[i_1, i_2, \ldots, i_m] \in \mathcal{S} \mid \sum_{k=1}^{m} i_k \leqslant v\}$, *then* $\mathcal{I}$ *is an information set for the* v*th-order generalized Reed–Muller code* $\mathcal{R}_{\mathbb{F}_q}(v, m)$.

The proof depends on some identities involving polynomials and these will be stated and proved through a series of lemmas. Let $u_0, u_1, \ldots, u_{q-1}$ be independent commuting indeterminates, and for $0 \leqslant i, j \leqslant q-1$, let $a_{i,j} = u_i - u_j$. For $q-1 \geqslant t \geqslant 0$, let $s_{r,t} = \displaystyle\sum_{0 \leqslant i_1 \leqslant i_2 \leqslant \cdots \leqslant i_r \leqslant t} u_{i_1} u_{i_2} \ldots u_{i_r}$ for $r \geqslant 1$ and let $s_{0,t} = 1$.

Lemma 1. *For* $0 \leqslant r, t \leqslant q-1$, $s_{r,t} = \displaystyle\sum_{0 \leqslant i \leqslant t} \frac{u_i^{r+t}}{\prod_{0 \leqslant \ell \leqslant t,\ \ell \neq i} a_{i,\ell}}$.

Proof. If $t = 0$, $s_{r,0} = u_0^r$ which is also the only term occurring in the right-hand sum.

If $r = 0$ and $t \geqslant 1$, consider the first term of the right-hand sum and obtain partial fractions. $\dfrac{u_0^{r+t}}{\prod_{1 \leqslant k \leqslant t} (u_0 - u_k)} = 1 + \displaystyle\sum_{1 \leqslant k \leqslant t} \frac{b_k}{u_0 - u_k}$, where $b_k = \dfrac{u_k^{r+t}}{\prod_{1 \leqslant \ell \leqslant t,\ \ell \neq k} (u_k - u_\ell)}$. Hence $\dfrac{u_0^{r+t}}{\prod_{1 \leqslant k \leqslant t} (u_0 - u_k)} = 1 - \displaystyle\sum_{1 \leqslant k \leqslant t} \frac{u_k^{r+t}}{\prod_{0 \leqslant \ell \leqslant t,\ \ell \neq k} (u_k - u_\ell)}$, which establishes the identity in this case as $s_{0,t} = 1$.

Now use induction on $r + t$. If $r, t \geqslant 1$,

$$s_{r,t} = s_{r,t-1} + s_{r-1,t} u_t = \sum_{0 \leqslant i \leqslant t-1} \frac{u_i^{r+t-1}}{\prod_{0 \leqslant \ell \leqslant t-1,\ \ell \neq i} a_{i,\ell}} + \sum_{0 \leqslant i \leqslant t} \frac{u_i^{r+t-1} u_t}{\prod_{0 \leqslant \ell \leqslant t,\ \ell \neq i} a_{i,\ell}}$$

$$= \sum_{0 \leqslant i \leqslant t-1} \frac{u_i^{r+t-1}}{\prod_{0 \leqslant \ell \leqslant t-1,\ \ell \neq i} a_{i,\ell}} \left(1 + \frac{u_t}{a_{i,t}}\right) + \frac{u_t^{r+t}}{\prod_{0 \leqslant \ell \leqslant t-1} a_{i,\ell}} = \sum_{0 \leqslant i \leqslant t} \frac{u_i^{r+t}}{\prod_{0 \leqslant \ell \leqslant t,\ \ell \neq i} a_{i,\ell}}$$

since $a_{i,t} + u_t = u_i$. □

Lemma 2. *Let* y *be an indeterminate which commutes with* $u_0, u_1, \ldots, u_{q-1}$. *For* $0 \leqslant t \leqslant r$ *and* $t \leqslant q-1$,

$$\sum_{0 \leqslant k \leqslant t} \left(s_{r-k,k} \prod_{0 \leqslant \ell \leqslant k-1} (y - u_\ell) \right) = \sum_{0 \leqslant i \leqslant t} u_i^r \left(\prod_{0 \leqslant \ell \leqslant t,\ \ell \neq i} \frac{y - u_\ell}{a_{i,\ell}} \right).$$

Proof. We use induction on t. If $t = 0$, the left-hand side is $s_{r,0}$ and the right-hand side is u_0^r. Now suppose $t \geqslant 1$. Then the left-hand side is

$$\sum_{0\leqslant i\leqslant t-1} u_i^r \left(\prod_{0\leqslant \ell\leqslant t-1,\ \ell\neq i} \frac{y-u_\ell}{a_{i,\ell}} \right) + s_{r-t,t} \prod_{0\leqslant \ell\leqslant t-1} (y-u_\ell)$$

$$= \sum_{0\leqslant i\leqslant t-1} u_i^r \left(\prod_{0\leqslant \ell\leqslant t-1,\ \ell\neq i} \frac{y-u_\ell}{a_{i,\ell}} \right) + \left(\sum_{0\leqslant i\leqslant t} \frac{u_i^r}{\prod_{0\leqslant \ell\leqslant t,\ \ell\neq i} a_{i,\ell}} \right)$$

$$\times \prod_{0\leqslant \ell\leqslant t-1} (y-u_\ell)$$

$$= \sum_{0\leqslant i\leqslant t-1} u_i^r \left(\prod_{0\leqslant \ell\leqslant t-1,\ \ell\neq i} \frac{y-u_\ell}{a_{i,\ell}} \right) \left(1 + \frac{y-u_i}{a_{i,t}} \right) + u_t^r \prod_{0\leqslant \ell\leqslant t-1} \frac{y-u_\ell}{a_{t,\ell}}$$

$$= \sum_{0\leqslant i\leqslant t} u_i^r \left(\prod_{0\leqslant \ell\leqslant t,\ \ell\neq i} \frac{y-u_\ell}{a_{i,\ell}} \right). \quad \square$$

Replacing y by u_t in Lemma 2 and setting $c_{i,j} = \prod_{0\leqslant \ell\leqslant j-1} a_{i,\ell}$, for $0\leqslant j\leqslant i\leqslant q-1$, we get the following result.

Lemma 3. *For* $0\leqslant t\leqslant r$ *and* $t\leqslant q-1$, $\sum_{0\leqslant k\leqslant t} s_{r-k,k} c_{t,k} = u_t^r$.

We also derive an identity for certain polynomials in y using Lemma 2.

Lemma 4. *For* $0\leqslant r\leqslant q-1$, $\sum_{0\leqslant k\leqslant r} \left(s_{r-k,k} \prod_{0\leqslant \ell\leqslant k-1} (y-u_\ell) \right) = y^r$.

Proof. The left-hand side of the equation in Lemma 2 with $t = r$, is equal to the polynomial

$$\sum_{0\leqslant i\leqslant r} u_i^r \left(\prod_{0\leqslant \ell\leqslant r,\ \ell\neq i} \frac{y-u_\ell}{a_{i,\ell}} \right)$$

in y of degree r. Replacing y by u_j, for each j with $0\leqslant j\leqslant r$, we get u_j^r. Hence this polynomial coincides with y^r for $r+1$ values. Consequently, these polynomials are identical. $\square$

From this we derive an identity similar to that of Lemma 3 by substituting u_t for y in Lemma 4:

Lemma 5. *For* $0 \leqslant r \leqslant t$ *and* $t \leqslant q-1$, $\sum_{0 \leqslant k \leqslant r} s_{r-k,k} c_{t,k} = u_t^r$.

We denote the lexicographic order on $\mathcal{X}$ by $\prec$, i.e. $[i_1, \ldots, i_m] \prec [j_1, \ldots, j_m]$ if, and only if, for some k with $1 \leqslant k \leqslant m$, $i_k < j_k$ and $i_\ell = j_\ell$ for $\ell < k$. We use $\preceq$ to denote the corresponding non-strict order; that is, the union of $\prec$ and $=$. Note that $\preceq$ is a total order. We use $\leqslant$ for the partial order on $\mathcal{X}$, as defined in the statement of the theorem.

We define three matrices M, L and R whose rows and columns are indexed by $\mathcal{X}$, ordered by $\prec$. Let $x, y \in \mathcal{X}$ and write $x = [i_1, \ldots, i_m]$ and $y = [j_1, \ldots, j_m]$. We set $M_{x,y} = u_y^x = u_{j_1}^{i_1} \cdots u_{j_m}^{i_m}$. We set $L_{x,y} = s_{i_1-j_1,j_1} \ldots s_{i_m-j_m,j_m}$ if $y \leqslant x$ and $L_{x,y} = 0$ otherwise. We set $R_{x,y} = c_{j_1,i_1} \ldots c_{j_m,i_m}$ if $x \leqslant y$ and $R_{x,y} = 0$ otherwise. Note that $x \prec y$ implies that $y \nleqslant x$. So, L is lower triangular and R is upper triangular.

Lemma 6. $M = LR$ *and* $\det M = \prod_{0 \leqslant j < i \leqslant q-1} a_{i,j}^{n_i}$ *where* n_i *is the number of occurrences of* i *among the coordinates of elements of* $\mathcal{X}$.

Proof. We calculate the (x, y)-entry in the product LR. For $1 \leqslant k \leqslant m$, let $h_k = \min\{i_k, j_k\}$ and $z = [h_1, \ldots, h_m]$. Then $z \leqslant x$ and $z \leqslant y$ implies $z \in \mathcal{X}$ and every $w \in \mathcal{S}$ for which $w \leqslant z$ is also in $\mathcal{X}$, by the assumed properties of $\mathcal{X}$. Now $(LR)_{x,y} = \sum_{w \in \mathcal{X}} L_{x,w} R_{w,y}$. Since $L_{x,w} = 0$ if $w \nleqslant x$ and $R_{w,y} = 0$ if $w \nleqslant y$, we may take the sum over all $w \in \mathcal{X}$ such that $w \leqslant z$. Thus we have

$$
\begin{aligned}
(LR)_{x,y} &= \sum_{w \leqslant z} L_{x,w} R_{w,y} \\
&= \sum_{0 \leqslant g_k \leqslant h_k,\ 1 \leqslant k \leqslant m} s_{i_1-g_1,g_1} \ldots s_{i_m-g_m,g_m} c_{j_1,g_1} \ldots c_{j_m,g_m} \\
&= \prod_{1 \leqslant k \leqslant m} \left(\sum_{0 \leqslant g_k \leqslant h_k} s_{i_k-g_k,g_k} c_{j_k,g_k} \right) = \prod_{1 \leqslant k \leqslant m} u_{j_k}^{i_k} = M_{x,y},
\end{aligned}
$$

using Lemmas 3 and 5.

To compute $\det M$, we only need to determine the diagonal entries of L and R. The diagonal entry of L at position $[i_1, \ldots, i_m]$ is $s_{0,i_1} \ldots s_{0,i_m} = 1$. The diagonal entry of R at position $[i_1, \ldots, i_m]$ is $c_{i_1,i_1} \ldots c_{i_m,i_m}$ and $c_{i,i} = \prod_{0 \leqslant \ell \leqslant i-1} a_{i,\ell}$. This completes the proof. □

We now return to the proof of Theorem 1.

Proof of Theorem 1. We determine explicitly a spanning set of size $|\mathcal{X}|$ for the subspace of $\mathbb{F}_q^{\mathcal{I}}$ spanned by the restriction of $\mathcal{B}$ to $\mathcal{I}$. The $(\alpha_{j_1}, \ldots, \alpha_{j_m})$-coordinate of the polynomial function $x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m}$ is $\alpha_{j_1}^{i_1} \alpha_{j_2}^{i_2} \ldots \alpha_{j_m}^{i_m}$. The dimension of the spanning set is thus the rank of the $|\mathcal{X}| \times |\mathcal{X}|$ matrix N with $N_{x,y} = \alpha_{j_1}^{i_1} \alpha_{j_2}^{i_2} \ldots \alpha_{j_m}^{i_m}$ where $x = [i_1, \ldots, i_m]$ and $y = [j_1, \ldots, j_m]$. For $0 \leqslant j < i \leqslant q-1$, we write $\beta_{i,j} = \alpha_i - \alpha_j$ and note that $\beta_{i,j} \neq 0$. Hence, from Lemma 6, $\det N = \prod_{0 \leqslant j < i \leqslant q-1} \beta_{i,j}^{n_i} \neq 0$. So, we conclude that $\mathcal{I}$ is an information set for $\mathcal{R}_{\mathbb{F}_q}(v, m)$. □

In dealing with the field $\mathbb{F}_p$, where p is prime, it is frequently convenient to describe the elements by $0, 1, \ldots, p-1$ while at the same time using $0, 1, \ldots, p-1$ to denote integers. We will use this notation ambiguously below since the context will clearly determine whether these symbols refer to finite field elements or to integers.

In the special case where $q = p$ is a prime we have the following corollary to Theorem 1:

Corollary 2. *If p is a prime, the code $\mathcal{R}_{\mathbb{F}_p}(v, m)$ has information set*

$$\mathcal{I} = \left\{ (i_1, \ldots, i_m) \mid i_k \in \mathbb{F}_p,\ 1 \leqslant k \leqslant m,\ \sum_{k=1}^{m} i_k \leqslant v \right\}. \tag{1}$$

Proof. The choice $\alpha_i = i$ for the elements of $\mathbb{F}_p$ will produce this information set from the theorem, recalling of course that the sum is taken in $\mathbb{Z}$, not in $\mathbb{F}_p$. □

Note: The theorem applies not only to the generalized Reed–Muller codes: for example, if $m = 2$, $q > 2$, and $\mathcal{X} = \{[0,0], [0,1], [1,0], [1,1]\}$, then $C = \langle 1, x_1, x_2, x_1 x_2 \rangle$, $\{(0,0), (0,1), (1,0), (1,1)\}$ is an information set for C, and C is not a generalized Reed–Muller code.

Definition 3. For $\mathcal{R}_{\mathbb{F}_p}(v, m)$, when p is a prime, we call $\mathcal{I}$ of Eq. (1) the *standard* information set for C if $\alpha_i = i \in \mathbb{F}_p$ for all i. More generally, the information set using the particular ordering $[\alpha_0, \ldots, \alpha_{p-1}]$ of $\mathbb{F}_p$ will be said to be *based on* that ordering.

4. Partial PD-sets

We now look for s-PD-sets for the generalized Reed–Muller codes, and in particular, for those that are the codes of finite geometry designs. First we obtain a general lemma that finds a number s such that a code C with an automorphism group G will have G as an s-PD-set.

Lemma 7. *Let C be a code with minimum distance d, $\mathcal{I}$ an information set, $\mathcal{C}$ the corresponding check set and $\mathcal{P} = \mathcal{I} \cup \mathcal{C}$. Let G be an automorphism group of C, and n*

the maximum of $|\mathcal{O}\cap\mathcal{I}|/|\mathcal{O}|$, *where* $\mathcal{O}$ *is a G-orbit. If* $s=\min(\lceil\frac{1}{n}\rceil-1, \lfloor\frac{d-1}{2}\rfloor)$, *then G is an s-PD-set for C.*

Proof. For each $a\in\mathcal{P}$, let $G^{(a)}=\{g\in G \mid ag\in\mathcal{I}\}$. Then $|G^{(a)}|=|\mathcal{O}_a\cap\mathcal{I}|\,|G|/|\mathcal{O}_a|$, where $\mathcal{O}_a$ denotes the G-orbit of a.

Let $a_1,\dots,a_s$ be s distinct elements in $\mathcal{P}$ and assume that exactly t of them are in G-orbits meeting $\mathcal{I}$. We may assume that these t elements are $a_1,\dots,a_t$. Then

$$\left|\bigcup_{1\leqslant i\leqslant t} G^{(a_i)}\right| \leqslant |G| \sum_{1\leqslant i\leqslant s} |\mathcal{O}_{a_i}\cap\mathcal{I}|/|\mathcal{O}_a| \leqslant |G|sn < |G|,$$

since $s<\frac{1}{n}$. Hence there is an element $g\in G\setminus\bigcup_{1\leqslant i\leqslant s}G^{(a_i)}$. Since $g\notin G^{(a_i)}$, $a_ig\notin\mathcal{I}$ for each i. That is, $a_ig\in\mathcal{C}$ for each i.

Hence, for each s-tuple in $\mathcal{P}$, there is an element in G mapping the s-tuple into $\mathcal{C}$. Since $s\leqslant\lfloor\frac{d-1}{2}\rfloor$, C can correct s errors. Thus G is an s-PD-set for C with respect to the information set $\mathcal{I}$. □

Note that this lemma depends only on the size of the information set. Thus, when the parameters satisfy the inequality, G will be an s-PD-set with respect to all information sets. The lemma is a generalization of the observation in [Mac64] for cyclic codes for the number of errors that the cyclic group will correct by permutation decoding.

Now turning to the generalized Reed–Muller codes, here $C=\mathcal{R}_{\mathbb{F}_q}(v,m)$ where $q=p^t$, p is a prime and $0\leqslant v\leqslant m(q-1)$, $\mathcal{P}=\mathbb{F}_q^m$ and an information set $\mathcal{I}$ has size $|\mathcal{I}|=f_{v,m,q}=\sum_{i=0}^{\ell}(-1)^i\binom{m}{i}\binom{m+v-iq}{m}$ where $\ell=\min(m,\lfloor(m+v)/q\rfloor)$ (see [AK92, Theorem 5.4.1, p.154] for an expression of this number as a double sum). Moreover, the automorphism group of $\mathcal{R}_{\mathbb{F}_q}(v,m)$ contains the translation group $T_m(\mathbb{F}_q)$, whose order is q^m, and the minimum distance of the code is $d_{v,m,q}=(q-b)q^{m-a-1}$, where $v=a(q-1)+b$, $0\leqslant b<q-1$ (see [AK92, Theorem 5.4.3, Corollary 5.5.4]).

Applying Lemma 7, we have immediately:

Proposition 1. *Let* $f_{v,m,q}$ *denote the dimension and* $d_{v,m,q}$ *the minimum weight of* $\mathcal{R}_{\mathbb{F}_q}(v,m)$. *If* $s=\min(\lfloor(q^m-1)/f_{v,m,q}\rfloor, \lfloor(d_{v,m,q}-1)/2\rfloor$, *then the translation group* $T_m(\mathbb{F}_q)$ *is an s-PD-set for* $\mathcal{R}_{\mathbb{F}_q}(v,m)$.

In the special case, $q=p$ and $v=(m-r)(p-1)$, $\mathcal{R}_{\mathbb{F}_p}((m-r)(p-1),m)=C_p(AG_{m,r}(\mathbb{F}_p))$, i.e. the code of the affine geometry design of points and r-flats. If $r=m-1$, we have points and hyperplanes and $|\mathcal{I}|=\binom{m+p-1}{m}$. We have a general construction for smaller 2-PD-sets for these designs for $p\geqslant3$ and $m\geqslant3$ (except for $p=3$ when we will need $m\geqslant4$).

Proposition 2. *Let* $C=\mathcal{R}_{\mathbb{F}_p}(p-1,m)$ *where p is a prime and* $p\geqslant3$ *and let* $T_m(\mathbb{F}_p)$ *be its translation group. For the vector* $z=(1,1,\dots,1)\in\mathbb{F}_p^m$ *let* τ *denote the translation* *by z and let $Z = \langle \tau \rangle$. Using the standard information set*

$$\mathcal{I} = \left\{ (i_1, \ldots, i_m) \mid i_k \in \mathbb{F}_p,\ 1 \leqslant k \leqslant m,\ \sum_{k=1}^{m} i_k \leqslant p-1 \right\}, \tag{2}$$

Z is a 2-PD-set of size p for C for $m \geqslant 3$ and $p \geqslant 5$, and for $m \geqslant 4$ when $p = 3$.

Proof. We need to show that any two vectors v and w can be moved by some multiple of z into the check positions, $\mathcal{C} = \{(i_1, i_2, \ldots, i_m) \mid i_k \in \mathbb{F}_p,\ \sum_{k=1}^{m} i_k > p-1\}$. Notice that if, for a given prime p, we can prove this for $m = t$ then it will follow for $m \geqslant t$. To shorten the exposition, we will omit consideration of primes $\leqslant 11$ and prove the result for $p \geqslant 13$ and $m = 3$. This leaves $m = 3$ for the primes $p = 5$, 7 and 11 and $m = 4$ for $p = 3$. These involve a proliferation of subdivisions which need to be considered but no essential difficulty.

We consider the various types of pairs of vectors $(a, b, c) \in \mathbb{F}_p^3$ and for each pair we write down an element k of $\mathbb{F}_p$ so that the corresponding element in S that will move that pair into $\mathcal{C}$. We can always translate such a pair of vectors into one of the form (a, b, c), $(0, d, e)$. As membership of $\mathcal{C}$ depends only on the sum of the coordinates, we may assume that $0 \leqslant a \leqslant b \leqslant c \leqslant p-1$ and $0 \leqslant d \leqslant e \leqslant p-1$. Let $\ell = \lfloor p/3 \rfloor + 1$.

First, suppose $d = e = 0$. If $p-1-a \geqslant \ell$, let $k = p-1-a$ unless $b = c = a+1$. In this case, if $p-2-a \geqslant \ell$ let $k = p-2-a$, and if $p-1-a = \ell$ let $k = 2\ell+1$. If $p-1-a < \ell$ let $k = p-1$.

Next, suppose $d = 0$ and $e \neq 0$. If $a+b+c > p+2$, let $k = p-1$. If $a+b+c \leqslant p+2$ and $p \geqslant 11$, let $k = p-1-a$ unless $b = c = a+1$. In this case, let $k = p-2-a$ if $p \geqslant 13$.

Finally, suppose a, b and c are distinct and 0, d and e are distinct. If $a+b+c > p+2$, let $k = p-1$. Now suppose $a+b+c \leqslant p+2$. We may choose $k = p-1-a$ if $d \leqslant a$ or if $a < d$ and $d+e \geqslant 3a+3$. Now suppose additionally that $a < d$ and $d+e < 3a+3$. If $e \leqslant b$ let $k = p-1-b$ and if $b < e$ let $k = p-e$.

This completes the proof for $p \geqslant 13$ and $m \geqslant 3$. □

For the case $m = 2$ and planes of prime order, Proposition 1 does not prove that the translation group is a 2-PD-set. However, this is easily done:

Proposition 3. *Let $C = \mathcal{R}_{\mathbb{F}_p}(p-1, m)$ where p is a prime and $p \geqslant 3$. Using the standard information set $\mathcal{I}$ of Eq.* (2), *the translation group is a* 2*-PD-set for C for $m \geqslant 2$ and $p \geqslant 5$, and for $m \geqslant 3$ when $p = 3$.*

Proof. First take $p > 5$ and $m \geqslant 2$. As in Proposition 2, if we can prove the result for $m = 2$, it will follow for all $m \geqslant 2$. We need to show that any two vectors can be moved by some translation into the check positions $\mathcal{C}$. If the vectors are already all in $\mathcal{C}$, then the identity map, corresponding to translation by $(0, 0)$ is used. If not, we can translate the vectors so that one of them is the zero vector. Suppose they are $A = (a, b)$

p	2					2						3				5			7		
m	5					6						4				3			3		
s	2	3	4	5	6	2	3	4	5	6	7	2	3	4	5	2	3	4	2	3	4
size	4	8	13	19	26	3	9	10	13	15	26	6	11	17	30	8	21	43	11	22	47

Fig. 1. Sizes of some s-PD-sets in the translation group $T_m(\mathbb{F}_p)$.

and $B = (0, 0)$. We first translate by $(p - 1 - a, p - 1)$ to obtain $(p - 1, p - 1 + b)$ and $(p - 1 - a, p - 1)$, which are in $\mathcal{C}$ unless (i) $b = 1$ or (ii) $a = p - 1$.

If (i), $b = 1$, translate A and B by $(p - 1, p - 1 - b)$ to give $(p - 1 + a, p - 1)$ and $(p - 1, p - 1 - b)$, which are in $\mathcal{C}$ unless $a = 1$. In that case the two vectors are $(1, 1)$ and $(0, 0)$ and translation by $(p - 2, p - 2)$ yields the vectors $(p - 1, p - 1)$ and $(p - 2, p - 2)$, which are in $\mathcal{C}$ since $2(p - 2) > p - 1$ for $p \geqslant 5$.

If (ii), $a = p - 1$ the vectors are $(p - 1, b)$ and $(0, 0)$ and translation by $(p - 1, p - 1 - b)$ gives $(p - 2, p - 1)$ and $(p - 1, p - 1 - b)$, which are in $\mathcal{C}$ unless $b = 1$. In this case the vectors are $(p - 1, 1)$ and $(0, 0)$ and translation by $(p - 2, p - 2)$ gives $(p - 3, p - 1)$ and $(p - 2, p - 2)$, which are again in $\mathcal{C}$ for $p \geqslant 5$.

For $p = 3$, $m = 3$, a direct simple computation gives the result. □

In Fig. 1 we list the sizes of some s-PD-sets for codes of points and hyperplanes ($v = p - 1$) of $PG_m(\mathbb{F}_p)$, found using Magma [BC94] and GAP [GAP]. In these cases we used the information sets described in Definition 3, observing that different information sets of this type for a given code produced partial PD-sets of comparable sizes. In addition, in the affine group $AGL_5(\mathbb{F}_2)$, we found a 7-PD-set of size 51 and an 8-PD-set of size 74.

We now show how the existence of s-PD-sets for $\mathcal{R}_{\mathbb{F}_q}(v, m)$ leads to the existence of $(s + 1)$-PD-sets for $\mathcal{R}_{\mathbb{F}_q}(v, m + r)$. If $\mathbb{F}_q = \{\alpha_0, \ldots, \alpha_{q-1}\}$, consider the information set for $\mathcal{R}_{\mathbb{F}_q}(v, m)$,

$$\mathcal{I}_{m,v} = \left\{ (\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_m}) \mid 0 \leqslant i_k \leqslant q - 1,\ 1 \leqslant k \leqslant m,\ \sum_{k=1}^{m} i_k \leqslant v \right\}$$

based on the ordering $[\alpha_0, \ldots, \alpha_{q-1}]$ of $\mathbb{F}_q$. If $\mathcal{P}^{(m)} = \mathbb{F}_q^m$ is embedded in $\mathcal{P}^{(m+r)} = \mathbb{F}_q^{m+r}$ by $v \mapsto (v, 0)$ where $r \geqslant 1$, then clearly $\mathcal{I}_{m,v}$ embeds in $\mathcal{I}_{m+r,v}$ and $AGL_m(\mathbb{F}_q)$ embeds in $AGL_{m+r}(\mathbb{F}_q)$ naturally. We use these embeddings to show how an $(s + 1)$-PD-set for $\mathcal{R}_{\mathbb{F}_q}(v, m + r)$ with respect to $\mathcal{I}_{m+r,v}$ can be constructed from an s-PD-set for $\mathcal{R}_{\mathbb{F}_q}(v, m)$ with respect to $\mathcal{I}_{m,v}$.

Proposition 4. *Let P be an s-PD-set in $AGL_m(\mathbb{F}_q)$ for $\mathcal{R}_{\mathbb{F}_q}(v, m)$ with respect to $\mathcal{I}_{m,v}$. Let P^* be the image of P under the natural embedding of $AGL_m(\mathbb{F}_q)$ in $AGL_{m+r}(\mathbb{F}_q)$,* *where $r \geqslant 1$. Let U be the set of q translations of $\mathbb{F}_q^{m+r}$ which fix the first m coordinates, and let $Q = P^*U$. If $v < r(q-1)$, then Q is an $(s+1)$-PD-set in $AGL_{m+r}(\mathbb{F}_q)$ for $\mathcal{R}_{\mathbb{F}_q}(v, m+r)$ with respect to $\mathcal{I}_{m+r,v}$.*

In particular, if $P \subseteq T_m(\mathbb{F}_q)$ then $Q \subseteq T_{m+r}(\mathbb{F}_q)$.

Proof. Let $a_1, \ldots, a_{s+1} \in \mathcal{P}^{(m+r)}$. For each i, let a_i' be the projection of a_i on the first m coordinates. Choose $g \in P$ so that $a_i'g \notin \mathcal{I}_{m,v}$ for $i = 1, \ldots, s$. If $g \mapsto g^* \in P^*$, then $a_i g^* \notin \mathcal{I}_{m+r,v}$ for $i = 1, \ldots, s$. Indeed, $a_i g^* u \notin \mathcal{I}_{m+r,v}$ for $i = 1, \ldots, s$ and $u \in U$. We may choose $u \in U$ so that $a_{s+1}g^*u$ has α_{q-1} as its j-th coordinate, for all $j > m$. Since $r(q-1) > v$, $a_{s+1}g^*u \notin \mathcal{I}_{m+r,v}$. □

5. Projective geometries

The codes of the projective geometries over finite fields are the non-primitive generalized Reed–Muller codes (see [AK92, Chapter 5]). We can obtain some results about these codes in the prime order case by using some of the facts we have established for the affine case, and the usual embeddings. We can also apply Lemma 7 to the projective (non-primitive) generalized Reed–Muller codes to obtain similar results for s for an automorphism group to be an s-PD-set, using the known facts about the dimension and minimum weight.

Firstly, we can construct information sets for the code $C_p(PG_{m,r}(\mathbb{F}_p))$ in the following way: represent a point of $PG_m(\mathbb{F}_p)$ by a vector in $\mathbb{F}_p^{m+1}$ whose first non-zero coordinate is 1. Let $\beta_{m,r} = \dim(C_p(AG_{m,r}(\mathbb{F}_p)))$ and $\gamma_{m,r} = \dim(C_p(PG_{m,r}(\mathbb{F}_p)))$. Then $\gamma_{m,r} = \gamma_{m-1,r} + \beta_{m,r}$ (see [AK92, Corollary 5.7.3]). Note that $\beta_{m,r} = |\{(i_1, \ldots, i_m) \mid \sum_{1 \leqslant j \leqslant m} i_j \leqslant (m-r)(p-1)\}|$ and thus $\gamma_{m,r} = 1 + \sum_{1 \leqslant i \leqslant m-r} \beta_{r+i,r}$.

If $\mathcal{I}$ is an information set for $C_p(AG_{m,m-1}(\mathbb{F}_p))$, then $\mathcal{I}^* \cup \{(0, \ldots, 0, 1)\}$ is an information set for $C_p(PG_{m,m-1}(\mathbb{F}_p))$, where

$$\mathcal{I}^* = \{(1, x_1, \ldots, x_m) \mid (x_1, \ldots, x_m) \in \mathcal{I}\}.$$

More generally, if $\mathcal{I}$ is an information set for $C_p(AG_{m,r}(\mathbb{F}_p))$ and $\mathcal{J}$ is an information set for $C_p(PG_{m-1,r}(\mathbb{F}_p))$, then $\mathcal{I}^* \cup \mathcal{J}^\dagger$ is an information set for $C_p(PG_{m,r}(\mathbb{F}_p))$, where $\mathcal{J}^\dagger = \{(0, x_1, \ldots, x_m) \mid (x_1, \ldots, x_m) \in \mathcal{J}\}$.

Using this inductive construction, we see that $\{(0, \ldots, 0, 1)\} \cup \bigcup_{1 \leqslant i \leqslant r} \mathcal{K}_i$ is an information set for $C_p(PG_{m,r}(\mathbb{F}_p))$, where $\mathcal{K}_i$ is the set of vectors

$$\left\{ (\underbrace{0, \ldots, 0}_{r-i}, 1, \underbrace{a_{r-i+1}, \ldots, a_m}_{m-r+i}) \mid 0 \leqslant a_j \leqslant p-1, r-i+1 \leqslant j \leqslant m, \sum_{j=r-i+1}^{m} a_j \leqslant i(p-1) \right\}.$$

As a by-product of this construction of information sets for the projective geometry designs, in the case of the design of points and hyperplanes we can use homogeneous coordinates to obtain a set of hyperplanes whose incidence vectors will form a basis for the code in the prime case. This construction can be compared with the basis found in [GK98], where a basis of hyperplanes for the affine prime case was constructed and this then applied to the projective case.

Proposition 5. *If $C = C_p(PG_{m,m-1}(\mathbb{F}_p))$, where p is a prime and $m \geqslant 2$, then, using homogeneous coordinates, the incidence vectors of the set*

$$\left\{(1, a_1, \ldots, a_m)' \mid a_i \in \mathbb{F}_p, \sum_{i=1}^{m} a_i \leqslant p-1\right\} \cup \{(0, \ldots, 0, 1)'\}$$

of hyperplanes form a basis for C.

Similarly, a basis for $C_p(AG_{m,m-1}(\mathbb{F}_p))$ for $m \geqslant 2$, p prime, is the set of incidence vectors of the hyperplanes with equation

$$\sum_{i=1}^{m} a_i X_i = p-1 \text{ with } \sum_{i=1}^{m} a_i \leqslant p-1,$$

where $a_i \in \mathbb{F}_p$ for $1 \leqslant i \leqslant m$, and not all the a_i are 0, along with the hyperplane with equation $X_m = 0$.

Proof. This follows from the above discussion of the progression from projective to affine, and vice-versa, and of the dual nature of the projective case, noting that if a set of projective points in homogeneous coordinates is an information set, then the set of hyperplanes with these coordinates will give a basis. □

Finally we derive some partial PD-sets for these codes from partial PD-sets for the corresponding affine geometry codes. In Proposition 2, using the information set $\mathcal{I}$ of Eq. (2), we obtained a 2-PD-set $R = \{\tau_i \mid 0 \leqslant i \leqslant p-1\}$ for $C_p(AG_{m,m-1}(\mathbb{F}_p))$, where τ_i is the translation $\tau_i : v \mapsto v + iz$ and $z = (1, \ldots, 1)$. Using the embedding of $AG_m(\mathbb{F}_p)$ into $PG_m(\mathbb{F}_p)$ described above, each τ_i corresponds to a collineation

$$\hat{\tau}_i : (x_0, x_1, \ldots, x_m) \mapsto (x_0, x_1 + i, \ldots, x_m + i)$$

of $PG_m(\mathbb{F}_p)$. Let $Z = \{\hat{\tau}_i \mid 0 \leqslant i \leqslant p-1\}$. We define two further collineations:

$$\mu : (x_0, \ldots, x_{m-2}, x_{m-1}, x_m) \mapsto (x_0, \ldots, x_{m-2}, x_m, x_{m-1}),$$

$$\nu : (x_0, x_1, \ldots, x_{m-1}, x_m) \mapsto (x_0, x_1, \ldots, x_{m-1} + x_m, x_m),$$

where the images are normalized further if necessary.

Using these collineations we find a ‘small’ 2-PD-set for $C_p(PG_{m,m-1}(\mathbb{F}_p))$.

Proposition 6. *For $m\geqslant 3$, $p\geqslant 5$, the set $S=Z\cup\mu Z\cup\{v\}$ of collineations of $PG_m(\mathbb{F}_p)$ is a 2-PD-set of size $2p+1$ of the code $C_p(PG_{m,m-1}(\mathbb{F}_p))$ with respect to the information set $\mathcal{I}^*\cup\{(0,\ldots,0,1)\}$.*

Proof. In this case, the check set

$$\mathcal{C}=\left\{(1,a_1,\ldots,a_m)\mid 0\leqslant a_j\leqslant p-1 \text{ for } 1\leqslant j\leqslant m,\ \sum_{1\leqslant j\leqslant m} a_j>p-1\right\}$$

$$\cup\ \{(0,a_1,\ldots,a_m)\mid 0\leqslant a_j\leqslant p-1 \text{ for } 1\leqslant j\leqslant m, a_m \text{ not the leading entry}\}.$$

Clearly a pair of points of the form $(1,a_1,\ldots,a_m)$ and $(1,b_1,\ldots,b_m)$ can be mapped into $\mathcal{C}$ by an element of Z by Proposition 2. Also, since $m\geqslant 3$, a pair of points of the form $(1,a_1,\ldots,a_m)$ and $(0,\ldots,0,1)$ can be mapped into $\mathcal{C}$ by an element of μZ, again by Proposition 2.

Since Z fixes all points with first coordinate 0, a pair of points of the form $(1,a_1,\ldots,a_m)$ and $(0,\ldots,0,1,a_j,\ldots,a_m)\neq(0,\ldots,0,1)$ can be mapped into $\mathcal{C}$ by an element of Z by Proposition 2.

A pair of points of the form $(0,\ldots,0,1,a_j,\ldots,a_m)$ and $(0,\ldots,0,1,b_k,\ldots,b_m)$, neither equal to $(0,\ldots,0,1)$, can be mapped into $\mathcal{C}$ by the identity mapping.

A pair of points of the form $(0,\ldots,0,1,a_j,\ldots,a_m)$ and $(0,\ldots,0,1)$, where either $j\leqslant m-1$ or $j=m$ and $a_m\neq 0$, can be mapped into $\mathcal{C}$ by μ. The pair of points $(0,\ldots,0,1,0)$ and $(0,\ldots,0,1)$ can be mapped into $\mathcal{C}$ by v. □

Acknowledgements

J.D. Key thanks the Institute of Mathematical and Physical Sciences at the University of Wales at Aberystwyth for their hospitality, and the Institute of Mathematics and its Applications for an award under its Small Grant Scheme.

References

[AK92] E.F. Assmus Jr., J.D. Key, Designs and their Codes, Cambridge Tracts in Mathematics, vol. 103, Cambridge University Press, Cambridge, 1992 (Second printing with corrections, 1993).

[AK98] E.F. Assmus Jr., J.D. Key, Polynomial codes and finite geometries, in: V.S. Pless, W.C. Huffman, (Eds.), Handbook of Coding Theory, vol. 2, part 2, Elsevier, Amsterdam, 1998, pp. 1269–1343 (Chapter 16).

[BC94] W. Bosma, J. Cannon, Handbook of Magma Functions, Department of Mathematics, University of Sydney, November 1994, http://magma.maths.usyd.edu.au/magma/.

[GAP] The GAP Group, GAP–Groups, Algorithms, and Programming, Version 4.4, 2004, http://www.gap-system.org.

[GK98] S. Gao, J.D. Key, Bases of minimum-weight vectors for codes from designs, Finite Fields Appl. 4 (1998) 1–15.

[Gor82] D.M. Gordon, Minimal permutation sets for decoding the binary Golay codes, IEEE Trans. Inform. Theory 28 (1982) 541–543.

[Huf98] W.C. Huffman, Codes and groups, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, vol. 2, part 2, Elsevier, Amsterdam, 1998, pp. 1345–1440 (Chapter 17).

[KMM] J.D. Key, T.P. McDonough, V.C. Mavron, Partial permutation decoding of codes from finite planes, European J. Combin. 26 (2005) 665–682.

[Mac64] F.J. MacWilliams, Permutation decoding of systematic codes, Bell System Tech. J. 43 (1964) 485–505.

[MS83] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1983.

[Moo91] G.E. Moorhouse, Bruck nets, codes, and characters of loops, Des. Codes Cryptogr. 1 (1991) 7–29.

[Sch64] J. Schönheim, On coverings, Pacific J. Math. 14 (1964) 1405–1411.