Partial permutation decoding for codes from affine geometry designs

J. D. Key*
Department of Mathematical Sciences
Clemson University
Clemson SC 29634, U.S.A.

T. P. McDonough and V. C. Mavron
Institute of Mathematical and
Physical Sciences
University of Wales, Aberystwyth
Ceredigion SY23 3BZ, U.K.

September 7, 2006

Abstract

We find explicit PD-sets for partial permutation decoding of the generalized Reed-Muller codes $\mathcal{R}_{\mathbb{F}_p}(2(p-1),3)$ from the affine geometry designs $AG_{3,1}(\mathbb{F}_p)$ of points and lines in dimension 3 over the prime field of order p, using the information sets found in [8].

Mathematics Subject Classification (2000): 05, 51, 94
Key words: Codes, finite geometries, designs, decoding

1 Introduction

In [7] we found s-PD-sets (see Definition 1) for $s = 2$ and 3 for partial permutation decoding for the p-ary codes of affine planes of prime order p; this was extended to projective planes. Since PD-sets are dependent on specific information sets for the codes, we were able to deal with the plane case by using information sets deduced from the bases found by Moorhouse [12]. Using new information sets found in [8],

*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

we extended these results to the codes from the designs of points and hyperplanes of affine and projective geometries of prime order, obtaining 2-PD-sets. We now use these information sets to find s-PD-sets for $s = 2$ and 3 for the p-ary codes of the affine geometry designs $AG_{3,1}(\mathbb{F}_p)$ of points and lines in 3-dimensional affine space $AG_3(\mathbb{F}_p)$ over the field $\mathbb{F}_p$. We prove the following theorem:

Theorem 1 *Let $\mathcal{D}$ be the 2-$(p^3, p, 1)$ design $AG_{3,1}(\mathbb{F}_p)$ of points and lines in the affine space $AG_3(\mathbb{F}_p)$, where p is a prime, and let $C = \mathcal{R}_{\mathbb{F}_p}(2(p-1), 3)$ be the p-ary code of $\mathcal{D}$. Then C is a $[p^3, \frac{1}{6}p(5p^2+1), p]_p$ code with information set*

$$\mathcal{I} = \{(i_1, i_2, i_3) \mid i_k \in \mathbb{F}_p,\ 1 \leq k \leq 3,\ \sum_{k=1}^{3} i_k \leq 2(p-1)\}. \tag{1}$$

Let T be the translation group of $AG_3(\mathbb{F}_p)$, let D be the group of invertible diagonal 3×3 matrices, and let Z be the group of scalar matrices. For each $d \in \mathbb{F}_p$ with $d \neq 0$, let $\mu(d)$ be the associated dilatation. Corresponding to the information set $\mathcal{I}$, the code C has a 2-PD-set of the form $T \cup T\mu(d)$ of size $2p^3$ for $p \geq 5$ and for some $d \in \mathbb{F}_p^*$, and the group TD is a 3-PD-set for C of size $p^3(p-1)^3$ for $p \geq 7$. (In fact, for the 2-PD-set, we can choose $d = (p-1)/2$.)

It should be noted that, when elements of $\mathbb{F}_p$ occur in an inequality, they are being treated as integers in the interval $[0, p-1]$.

The proof of the theorem will follow in Section 3, after a section on some basic results, definitions and background. In Section 4 we obtain a new 3-PD-set for the p-ary code $AG_{2,1}(\mathbb{F}_p)$ of points and lines in the affine plane $AG_2(\mathbb{F}_p)$ over the field $\mathbb{F}_p$.

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 $\boldsymbol{t}$**-**$\boldsymbol{(v, k, \lambda)}$ **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 **code** $\boldsymbol{C_p(\mathcal{D})}$ 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 $\mathbb{F}_p$.

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. $C^\perp = \{v \in \mathbb{F}_q^n | (v, c) = 0$ 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. 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. (See Huffman [6] for related, more general, concepts of isomorphisms of codes.) 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 $\mathbf{Aut(C)}$.

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 $\boldsymbol{PG_{m,r}(\mathbb{F}_q)}$. Similarly, the set of points and r-dimensional flats of an m-dimensional affine geometry forms a 2-design, $\boldsymbol{AG_{m,r}(\mathbb{F}_q)}$. 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 [1, Chapter 5] for a full treatment. The dimension and minimum weight is known in each case: see [1, Theorem 5.7.9].

Permutation decoding was first developed by MacWilliams [10] and involves finding a set of automorphisms of a code called a PD-set. The method is described fully in MacWilliams and Sloane [11, Chapter 15] and Huffman [6, Section 8]. We extend the concept of PD-sets to s-PD-sets for s-error-correction in [7], as in the following definition. This coincides with the use of the term s-PD-set in Kroll and Vincenti [9].

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 $\mathcal{C}$.*

*For $s \leq t$ 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 [6, Theorem 8.1], and that an s-PD-set will correct s errors follows in a similar manner. The algorithm for permutation decoding is given in [6, 11] or see [7]. 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 [5],[13], or [6]). This bound can be adapted to one for s-PD-sets by replacing in the formula for the bound, the variable t, that denotes full error-correction, by $s < t$ for correction of s errors.

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 [1, Chapter 5] or [2] for generalized Reed-Muller codes: (see [1, Definition 5.4.1]):

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

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

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 $V = \mathbb{F}_q^m$.

The code $\mathcal{R}_{\mathbb{F}_p}((m-1)(p-1), m)$ is the p-ary code of the affine geometry design $AG_{m,1}(\mathbb{F}_p)$ of points and lines in affine space $AG_m(\mathbb{F}_p)$: see [1, Theorem 5.7.9]. Here we take $m = 3$, in which case $\mathcal{R}_{\mathbb{F}_p}(2(p-1), 3)$ is a $[p^3, \frac{1}{6}p(5p^2+1), p]_p$ code over $\mathbb{F}_p$.

The information set we will be using was found in [8, Theorem 1,Corollary 2]:

Result 1 *If p is a prime, the code $\mathcal{R}_{\mathbb{F}_p}(\nu, m)$ has information set*

$$\mathcal{I} = \{(i_1, \ldots, i_m) \mid i_k \in \mathbb{F}_p, \, 1 \leq k \leq m, \, \sum_{k=1}^{m} i_k \leq \nu\}. \tag{2}$$

3 Proof of theorem

Before proving the theorem, we establish some notation. We will use τ with an appropriate argument to denote translations in $\mathbb{F}_p$ and $AG_3(\mathbb{F}_p)$. Thus, $\tau(w) : v \mapsto v + w$. If $w = (w_1, w_2, w_3)$, where $w_1, w_2, w_3 \in \mathbb{F}_p$, we will also write $\tau(w)$ as $\tau(w_1, w_2, w_3)$. For $d_1, d_2, d_3 \in \mathbb{F}_p \backslash \{0\}$, let $\delta(d_1)$ denote the mapping $v_1 \mapsto d_1 v_1$, for $v_1 \in \mathbb{F}_p$ and let $\delta(d_1, d_2, d_3)$ denote the mapping $(v_1, v_2, v_3) \mapsto (d_1 v_1, d_2 v_2, d_3 v_3)$, for $v_1, v_2, v_3 \in \mathbb{F}_p$.

We begin the proof of Theorem 1 by establishing that there is a 2-PD-set of the stated form. Let $\mathcal{C}$ denote the check set of C corresponding to the information set $\mathcal{I}$, where

$$\mathcal{I} = \{(i_1, i_2, i_3) \mid i_k \in \mathbb{F}_p, \, 1 \leq k \leq 3, \, \sum_{k=1}^{3} i_k \leq 2(p-1)\}$$

as in Equation (1). Let P' and Q' be two points. By a translation τ', we can take Q' to $Q = (0,0,0)$ and P' to $P = (a, b, c)$.

If $a, b \leq (p-3)/2$, let $w = (p-1-a, p-1-b, e)$ where $e = p-1$ or $p-2$ according as $c \neq 1$ or $c = 1$. Clearly, $P\tau(w) = (p-1, p-1, c+e) \in \mathcal{C}$ as $c + e \neq 0$. Also, $p - 1 - a + p - 1 - b \geq p + 1$ and $e \geq p - 2$. So, $Q\tau(w) \in \mathcal{C}$.

If $a, b \geq (p+3)/2$, let $w = (p-1, p-1, e)$ where $e = p-1-c$ or $p-2-c$ according as $c \neq p-1$ or $c = p-1$. Then, $Q\tau(w) = (p-1, p-1, e) \in \mathcal{C}$ as $e \neq 0$. Since $P\tau(w) = (a-1, b-1, c+e)$ and $a+b-2 \geq p+1$ and $c+e \geq p-2$, $P\tau(w) \in \mathcal{C}$.

If $a \leq (p-3)/2$, $b \geq (p-1)/2$, and $c = (p-1)/2$, let $w = (p-1-a, p-1, (p-1)/2)$. Clearly, $Q\tau(w) \in \mathcal{C}$. Also, $P\tau(w) = (p-1, b-1, p-1) \in \mathcal{C}$.

If $a \leq (p+1)/2$, $b \geq (p+3)/2$, and $c = (p+1)/2$, let $w = (p-1-a, p-1, p-1)$. Clearly, $Q\tau(w) \in \mathcal{C}$. Also, $P\tau(w) = (p-1, b-1, (p-1)/2)$. Since $b-1 \geq (p+1)/2$, $P\tau(w) \in \mathcal{C}$.

If $a \geq (p+5)/2$ and $b = c = (p-1)/2$ let $w = (p-1, p-1, p+2-a)$. Clearly, $Q\tau(w) \in \mathcal{C}$. Also, $P\tau(w) = (a-1, (p-3)/2, 3(p+1)/2 - a) \in \mathcal{C}$.

If $a \leq (p-5)/2$ and $b = c = (p+1)/2$ let $w = ((p+3)/2, (p-3)/2, p-1)$. Clearly, $Q\tau(w) \in \mathcal{C}$. Also, $P\tau(w) = (a+(p+3)/2, p-1, (p-1)/2)$. Since $(p+3)/2 \leq a \leq p-1$, $P\tau(w) \in \mathcal{C}$.

These arguments can be applied to any permutation of the coordinates. So, in these cases, we can find a translation τ'' so that $P'\tau'\tau'', Q'\tau'\tau'' \in \mathcal{C}$. Hence, the only cases that remain are when at least two of a, b and c are in $\{(p-1)/2, (p+1)/2\}$ and, if there is a remaining one, it is in $\{(p-3)/2, (p+3)/2\}$.

If $p > 7$, then none of $2a$, $2b$ and $2c$ are in $\{(p-3)/2, (p-1)/2, (p+1)/2, (p+3)/2\}$. The preceding arguments show the existence of a translation τ'' for which $P'\tau'\delta(2)\tau''$ and $Q'\tau'\delta(2)\tau''$ are in $\mathcal{C}$. If $p = 5$ or $p = 7$, we can apply the same argument to $a(p-1)/2$, $b(p-1)/2$, and $c(p-1)/2$, even though the sets $\{a(p-1)/2, b(p-1)/2, c(p-1)/2\}$ and $\{(p-3)/2, (p-1)/2, (p+1)/2, (p+3)/2\}$ overlap. Hence, in these cases, there is a translation τ'' for which $P'\tau'\delta((p-1)/2)\tau'', Q'\tau'\delta((p-1)/2)\tau'' \in \mathcal{C}$.

Since the translations form a normal subgroup of the automorphism group of $AG_3(\mathbb{F}_p)$, we can write $\tau'\delta(d)\tau'' = \tau\delta(d)$, for some translation τ. Hence, we have shown that $T \cup T\delta(d)$ is a 2-PD-set for C with d chosen as in the preceding paragraph. In fact, we could take $d = (p-1)/2$ in all cases; the details are straightforward but would lengthen the proof. This completes the proof of the first part of the theorem.

Next, we show that TD, the group generated by T and D, where $D = \{\delta(d_1, d_2, d_3) \mid d_1, d_2, d_3 \in \mathbb{F}_p \backslash \{0\}\}$, is a 3-PD-set for C.

A translation can take any three points to the triple $X = (0,0,0)$, $P = (a,b,c)$, $Q = (d,e,f)$ where not all of a,b,c,d,e,f are 0 and $(a,b,c) \neq (d,e,f)$. A point (a,b,c) is in the check set $\mathcal{C}$ if, and only if, $a+b+c \geq 2p-1$. The theme of the proof is to show that, by a non-zero multiplication and an addition on each coordinate position, the three entries (either $[0,a,d]$, $[0,b,e]$ or $[0,c,f]$) in that position can be moved to three elements of $\mathbb{F}_p$ corresponding to integers in the interval $[(2p-1)/3, p-1]$. If, in the i-th coordinate position, the multiplication is by d_i and the addition is w_i, then this mapping as effected by an element $\delta(d_1, d_2, d_3)\tau(w_1, w_2, w_3)$ of DT $(= TD)$ necessarily maps the triple X, P and Q into $\mathcal{C}$.

This approach needs to be modified for $p = 13$ and fails to work for $p = 7$. In the case $p = 7$, we have checked the result with simple computer programs using Magma [3] and GAP [4].

We deal first with some easy cases. If all three entries are 0, then $\tau(p-1)$ has the desired effect; that is, $\tau(p-1)$ acting on the entries maps $[0,0,0]$ to $[p-1,p-1,p-1]$. If two entries are 0 and one is nonzero, say $[0,0,d]$, then $\delta(d^{-1})\tau(p-2)$ has the desired effect. Thus, we need only consider triples with one 0 and two nonzero elements. These may be mapped, by a suitable nonzero multiplication, to $[0,1,g]$, where $1 \leq g \leq p-1$.

We now subdivide the proof into two cases, according as $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$. We write $p = 6m+1$ in the former case and $p = 6m+5$ in the latter. Note that $m \geq 1$ in both cases, since $p \geq 7$.

Case 1: $p = 6m+1$. In this case, $(2p-1)/3 < 4m+1$. Since we do not consider $p = 7$ here, $m \geq 2$.

If $1 \leq g \leq 2m-1$, $[0,1,g]\tau(4m+1) = [4m+1, 4m+2, 4m+1+g]$ and $4m+1 < 4m+1+g \leq 6m$. If $4m+3 \leq g \leq 6m$, $[0,1,g]\tau(6m-1) = [6m-1, 6m, g-2]$ and $4m+1 \leq g-2 \leq 6m-2$.

If $2m+2 \leq g \leq 3m$, $[0,1,g]\delta(2)\tau(6m-2) = [6m-2, 6m, 2g-3]$ and $4m+1 \leq 2g-3 \leq 6m-3$. If $3m+1 \leq g \leq 4m$, $[0,1,g]\delta(2)\tau(4m+1) = [4m+1, 4m+3, 2g-2m]$ and $4m+2 \leq 2g-2m \leq 6m$.

This leaves just four values of g to consider, *viz.* $g = 2m, 2m+1, 4m+1, 4m+2$. Noting that $4m+4 \leq 6m$, for $g = 2m+1$, $[0,1,g]\delta(3)\tau(4m+1) = [4m+1, 4m+4, 4m+3]$ and for $g = 4m+1$, $[0,1,g]\delta(3)\tau(4m+1) = [4m+1, 4m+4, 4m+2]$. For the other two values of g, we require $6m-4 \geq 4m+1$; that is, $m \geq 3$, i.e. $p \geq 19$. If $g = 2m$, $[0,1,g]\delta(3)\tau(6m-3) = [6m-3, 6m, 6m-4]$. If $g = 4m+2$, $[0,1,g]\delta(3)\tau(6m-4) = [6m-4, 6m-1, 6m]$.

We now deal with the last two values of g when $p = 13$ ($m = 2$). For $g = 4$, note that $[0,1,4]\tau(8) = [8,9,12]$, $[0,1,4]\delta(9)\tau(12) = [12,8,9]$ and $[0,1,4]\delta(3)\tau(8) = [9,12,8]$. For any coordinate column of this type, we can choose a mapping in which one of the entries is 8 ($= 4m$) while the others are $\geq 4m+1$. Moreover, the $4m$ entry can be made to appear in the image of any one of our triple of points X, P and Q. Similarly, for $g = 10$, $[0,1,10]\delta(3)\tau(8) = [8,11,12]$, $[0,1,10]\delta(12)\tau(9) = [9,8,12]$ and $[0,1,10]\tau(11) = [11,12,8]$.

We can thus arrange that the image of each of the points X, P and Q has at most one entry equal to $4m$ while the others are $\geq 4m+1$. Hence, these images lie in $\mathcal{C}$. This completes the proof of Case 1.

Case 2: $p = 6m+5$. In this case, $(2p-1)/3 = 4m+3$ and $m \geq 1$.

If $1 \leq g \leq 2m+1$, $[0,1,g]\tau(4m+3) = [4m+3, 4m+4, 4m+3+g]$ and $4m+3 < 4m+3+g \leq 6m+4$. If $4m+5 \leq g \leq 6m+4$, $[0,1,g]\tau(6m+3) = [6m+3, 6m+4, g-2]$ and $4m+3 \leq g-2 \leq 6m+2$.

If $2m+3 \leq g \leq 3m+2$, $[0,1,g]\delta(2)\tau(6m+2) = [6m+2, 6m+4, 2g-3]$ and $4m+3 \leq 2g-3 \leq 6m+1$. If $3m+3 \leq g \leq 4m+3$, $[0,1,g]\delta(2)\tau(4m+3) = [4m+3, 4m+5, 2g-2m-2]$ and $4m+4 \leq 2g-2m-2 \leq 6m+4$.

This leaves just two values of g to consider. If $g = 2m+2$, $[0,1,g]\delta(3)\tau(4m+3) = [4m+3, 4m+6, 4m+4]$. If $g = 4m+4$, $[0,1,g]\delta(3)\tau(4m+3) = [4m+3, 4m+6, 4m+5]$. This completes the proof of Case 2 and the proof of the theorem. ■

We illustrate the method of proof for the 3-PD-sets with an example for $p = 19 = 6m+1$ where $m = 3$ and $4m+1 = 13$. Suppose our three points have been mapped by a translation τ' to the points $(0,0,0)$, $(2,11,5)$, $(3,10,7)$. For the first coordinate triple $[0,2,3]$, the map $\delta(10)$ takes this to the standard form $[0,1,11]$ and the map $\delta(2)\tau(13)$ takes this to the triple to $[13,15,16]$. For the second coordinate triple $[0,11,10]$, the map $\delta(7)$ takes it to $[0,1,13]$ and the map $\delta(3)\tau(13)$ to this to the triple $[13,16,14]$. For the third coordinate triple $[0,5,7]$, the map $\delta(4)$ takes this to $[0,1,9]$ and the map $\delta(2)\tau(16)$ to this to the triple $[16,18,15]$. Note that $\delta(10)\delta(2) = \delta(1)$, $\delta(7)\delta(3) = \delta(2)$ and $\delta(4)\delta(2) = \delta(8)$. Thus, the the element $\tau'\delta(1,2,8)\tau(13,13,16)$ of TD will take our original three points to the points $(13,13,16)$,$(15,16,18)$,$(16,14,15)$, all of which are in the check set $\mathcal{C}$.

Note: These codes have high rate $\geq .83$. The worst-case time-complexity for the decoding algorithm using an s-PD-set of size z on a code of length n and dimension k is $\mathcal{O}(nkz)$, as a simple counting argument shows.

4 Affine planes

In [7, Proposition 4.5] we found 3-PD-sets of size $2p^2(p-1)$ for the codes from the affine planes $AG_{2,1}(\mathbb{F}_p)$, using an information set different from the one we have used in Theorem 1. We show that this can be improved to $p^2(p-1)$ using the set $\mathcal{I}$ of Equation 1. This further leads to $(m+1)$-PD-sets for the codes of the designs $AG_{m,m-1}(\mathbb{F}_p)$, using [8, Proposition 4]

Proposition 1 *Let p be a prime. Let $\mathcal{D}$ be the design $AG_{2,1}(\mathbb{F}_p)$ of points and lines in the affine plane $AG_2(\mathbb{F}_p)$ and let $C = \mathcal{R}_{\mathbb{F}_p}(p-1,2)$ be the p-ary code of $\mathcal{D}$. With information set*

$$\mathcal{I} = \{(i_1, i_2) \mid i_k \in \mathbb{F}_p,\ 1 \leq k \leq 2,\ \sum_{k=1}^{2} i_k \leq p-1\},$$

the group TZ, where T is the translation group and Z is the group of scalar matrices, is a 3-PD-set for C for $p \geq 7$, of size $p^2(p-1)$.

Proof: We extend our notation τ and μ for translations and dilatations, as used in Theorem 1, to affine planes. Thus $Z = \{\mu(a) \mid a \in \mathbb{F}_p,\ a \neq 0\}$. Let $H = TZ$.

Any three distinct points may be mapped by a translation to a triple of the form $X = (0,0)$, $P = (q,r)$, $Q = (s,t)$ where $(q,r) \neq (0,0)$, $(s,t) \neq (0,0)$ and $(q,r) \neq (s,t)$; in particular, $q \neq s$ or $r \neq t$. We may assume that $q \neq s$. The case $r \neq t$ may be dealt with in a similar manner. We will show how to find maps in TZ that move such triples into the check set $\mathcal{C}$.

Since $q \neq s$, some element of Z will fix X and map P and Q into a pair P' and Q' of the form (a,b), $(a+1,d)$, for some a, b, d, where $0 \leq a \leq p-2$. If $a \geq (p+1)/2$, $\mu(p-1)$ will fix X and map (a,b) to $(p-a, p-b)$ and $(a+1,d)$ to $(p-a-1, p-d)$; that is, to a similar triple with $a \leq (p-3)/2$. Hence, we may assume that $a \leq (p-1)/2$.

In this case, $p-a-2 \geq (p-3)/2$. The mapping $\tau(p-a-2,u)$ maps X, P' and Q' to $(p-a-2,u)$, $(p-2,u+b)$ and $(p-1,u+d)$, which are in $\mathcal{C}$ if $a+2 \leq u \leq p-1$ and $u \notin \{p-b, p-b+1, p-d\}$. Since $a+2 \leq (p+3)/2$, there are at least $(p-3)/2$ integers in the interval $[a+2, p-1]$ of which at most 3 must be excluded. If $p \geq 11$, there is at least one value of u meeting these constraints.

The only case that remains is $p = 7$. We can apply the argument of the preceding paragraph if $a = 0$ or $a = 1$. We are left with $a = 2$ and $a = 3$.

The triple X, P' and Q' is mapped by $\tau(5-a,6)$ into $\mathcal{C}$ if $b \neq 1$ or 2 and $d \neq 1$. If $d = 1$, $\tau(5-a,5)$ or $\tau(6,4)$ maps the triple into $\mathcal{C}$ according as $b \neq 2$ or $b = 2$. If $b = 1$, $\tau(5-a,5)$, $\tau(3,4)$ or $\tau(6,4)$ maps the triple into $\mathcal{C}$ according as $d \neq 2$, $d = 2$ and $a = 2$ or $d = 2$ and $a = 3$. If $b = 2$ and $a = 2$, $\tau(3,4)$ or $\mu(6)\tau(1,6)$ maps the triple into $\mathcal{C}$ according as $d \neq 3$ or $d = 3$. If $b = 2$ and $a = 3$, $\mu(3)\tau(1,6)$ or $\mu(3)\tau(3,5)$ maps the triple into $\mathcal{C}$ according as $d \neq 5$ or $d = 5$.

This completes the proof of the proposition. ■

Note: 1. We exclude $p = 5$ since the code is only 2-error-correcting.
2. Using [8, Proposition 4], we can now construct $(m+1)$-PD-sets of size $p^m(p-1)$ for $AG_{m,m-1}(\mathbb{F}_p)$, the design of points and hyperplanes in $AG_m(\mathbb{F}_p)$, for $m \geq 2$, p prime.

Acknowledgement

J. D. Key thanks the Institute of Mathematical and Physical Sciences at the University of Wales at Aberystwyth for their hospitality, and the London Mathematical Society for financial support.

References

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

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

[3] Wieb Bosma and John Cannon. Handbook of Magma Functions, Department of Mathematics, University of Sydney, November 1994, http://magma.maths.usyd.edu.au/magma/.

[4] GAP. Groups, Algorithms and Programming, Version 4. The GAP Group, Lehrstuhl D für Mathematik, RWTH Aachen, Germany and School of Mathematical and Computational Sciences, University of St. Andrews, Scotland. http://www-gap.dcs.st-and.ac.uk/ gap/.

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

[6] W. Cary Huffman. Codes and groups, in Handbook of Coding Theory, V. S. Pless and W. C. Huffman, Eds., Volume 2, Part 2, Chapter 17, Elsevier, Amsterdam, 1998. pp. 1345–1440.

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

[8] J. D. Key, T. P. McDonough, and V. C. Mavron. Information sets and partial permutation decoding of codes from finite geometries. Finite Fields Appl. **12** (2006) 232–247.

[9] Hans-Joachim Kroll and Rita Vincenti. PD-sets related to the codes of some classical varieties. Discrete Math. **301** (2005) 89–105.

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

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

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

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