4-2010

On the non-existence of a projective (75, 4,12, 5) set in PG(3, 7)

Aaron C.S. Chan

James A. Davis
University of Richmond, jdavis@richmond.edu

Jonathan Jedwab

Recommended Citation

Chan, Aaron C.S.; Davis, James A.; and Jedwab, Jonathan, "On the non-existence of a projective (75, 4,12, 5) set in PG(3, 7)" (2010). *Math and Computer Science Faculty Publications*. 152.
http://scholarship.richmond.edu/mathcs-faculty-publications/152

On the non-existence of a projective $(75, 4, 12, 5)$ set in $\mathrm{PG}(3, 7)$

Aaron C.S. Chan James A. Davis Jonathan Jedwab

4 September 2009 (revised 25 October 2009)

Abstract

We show by a combination of theoretical argument and computer search that if a projective $(75, 4, 12, 5)$ set in $\mathrm{PG}(3, 7)$ exists then its automorphism group must be trivial. This corresponds to the smallest open case of a coding problem posed by H. Ward in 1998, concerning the possible existence of an infinite family of projective two-weight codes meeting the Griesmer bound.

Keywords Centraliser, conjugacy class, Griesmer bound, integer linear program, linear code, prescribed automorphism group, projective code, projective set, rational canonical form, two-weight code.

2000 Mathematics Subject Classification 05E20, 05B25, 94B05.

1 Introduction

The Griesmer bound gives a lower bound on the length n of an $[n, k, d]$ code over $\mathrm{GF}(q)$. It was proved originally for the value $q = 2$ [15] and later extended to values $q > 2$ [26]:

Theorem 1 (Griesmer bound). *Suppose there exists an* $[n, k, d]$ *code over* $\mathrm{GF}(q)$. *Then*

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil .$$

Considerable effort has been devoted to constructing linear codes that meet the Griesmer bound; for example, see [3], [13], [17], [18], and [27].

Henceforth, let q be an odd prime power. The following problem was posed in 2001 by H. Ward [28], who had raised the special case $q = p$ in 1998 [27]: determine whether or not there exists

$$\text{a two-weight } \left[\tfrac{3q^2+3}{2}, 4, \tfrac{3q^2-3q}{2}\right] \text{ code } C \text{ over } \mathrm{GF}(q) \text{ with second weight } \tfrac{3q^2-q}{2}. \tag{1}$$

(This problem was also proposed by the same author in a list of open problems, distributed at the *Third EuroWorkshop on Optimal Codes and Related Topics (Sunny Beach, Bulgaria, June 2001)*,

A.C.S. Chan is with Department of Combinatorics and Optimization, University of Waterloo, 200 University Avenue West, Waterloo ON, Canada N2L 3G1. He was supported during Summer 2008 at Simon Fraser University by NSERC of Canada via an Undergraduate Student Research Award. Email: acschan@uwaterloo.ca

J.A. Davis is with Department of Mathematics and Computer Science, University of Richmond, VA 23173, USA, and is supported by NSA Grant # MDA904-03-1-0032. Email: jdavis@richmond.edu

J. Jedwab is with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC, Canada V5A 1S6, and is supported by NSERC of Canada. Email: jed@sfu.ca

but with the condition $k = 4$ accidentally omitted [R. Hill, personal communication, September 2008]; the problem is quoted in [2] in the form given on that list.) At the time the paper [28] was written, the existence of such a code was known for $q = 3$ [24] and for $q = 5$ [1], [11], but not for $q > 5$. Although a full classification is now known for $q = 3$ and $q = 5$ (see below), all cases $q > 5$ remain open. Some necessary conditions on the code C of (1) were obtained by Ferret [12, Appendix A], including Proposition 4 below.

If such a code C exists then it is optimal: for $q > 3$ the code meets the Griesmer bound, while for $q = 3$ it is known that the smallest n for which an $[n, 4, 9]$ code over GF(3) exists is $15 = \frac{3.3^2+3}{2}$ [18]. Furthermore, if C exists then it is necessarily projective, by taking $j = 2$ in Theorem 2.16 of [18] to deal with the case $q > 3$, and by using the complete classification of $[15, 4, 9]$ codes over GF(3) given in [16] to deal with the case $q = 3$.

The existence of such a code C is equivalent to the existence of a projective $\left(\frac{3q^2+3}{2}, 4, \frac{3q+3}{2}, \frac{q+3}{2}\right)$ set O in $\mathrm{PG}(3, q)$ (see Theorem 2), which in turn is equivalent to the existence of a certain partial difference set, or alternatively a certain strongly regular graph [5, Theorem 3.2]. The automorphism group $\mathcal{H}$ of the projective set O is a subgroup of $\mathrm{PGL}(4, q)$. The automorphism group of the code C is isomorphic to the semidirect product of $\mathcal{H}$ with $\mathrm{Gal}(\mathrm{GF}(q)/\mathrm{GF}(p))$ (see Section 2).

The case $q = 3$ of (1) concerns a projective two-weight $[15, 4, 9]$ code over GF(3) with second weight 12. There are exactly two inequivalent such codes: a first [24] for which $\mathcal{H}$ is isomorphic to S_6 [6], and a second [16] for which $\mathcal{H}$ has order 36 [2].

The case $q = 5$ of (1) concerns a projective two-weight $[39, 4, 30]$ code over GF(5) with second weight 35. There are exactly eight inequivalent such codes [3], for which $\mathcal{H}$ has order 1, 3, 4, 6, 6, 12, 12, and 18. Using the generator matrices given in [3], we find by direct checking that the corresponding projective set O in each case has a distinct automorphism group $\mathcal{H}$, which is isomorphic to: the trivial group, $\mathbb{Z}_3$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, S_3, $\mathbb{Z}_6$, A_4, D_6, and $S_3 \times \mathbb{Z}_3$ respectively.

Existence for each case $q > 5$ of (1) is currently unknown. The smallest open case, having $q = 7$, concerns the existence of a projective two-weight $[75, 4, 63]$ code over GF(7) with second weight 70. We shall show by a combination of theoretical argument and computer search that if any such code exists then the automorphism group $\mathcal{H}$ of the corresponding projective $(75, 4, 12, 5)$ set O in $\mathrm{PG}(3, 7)$ must be trivial.

In principle, this could be achieved by prescribing each possible non-trivial subgroup $\mathcal{H}$ of $\mathrm{PGL}(4, 7)$ in turn as being contained in the automorphism group of O, and then showing by exhaustive search that such a projective set O does not exist. However, there are a great many subgroups of $\mathrm{PGL}(4, 7)$, and for some of those having small order a simple exhaustive search is beyond computational reach. We shall show how to reduce drastically the number of subgroups of $\mathrm{PGL}(4, 7)$ that need be prescribed, and furthermore how to simplify the search in the case of subgroups of small order. Each search is then cast as an integer linear program, and solved using open source software. This method is sufficiently powerful to handle all subgroups of $\mathrm{PGL}(4, 7)$ except the trivial subgroup, for which the search space remains unfeasibly large.

The integer linear programs described in this paper were implemented in 2008 using the CBC (COIN-OR branch and cut) solver [8] and Ubuntu 7.10 running on a computational cluster, and verified in 2009 using GLPK (GNU Linear Programming Kit) [14] and Ubuntu 9.04 running on a PS3 gaming machine.

A possible alternative analysis of the case $q = 7$ of (1) is suggested by van Eupen and Hill's nonexistence proof [10] for a $[70, 6, 45]$ projective two-weight code C over GF(3) with second weight 54. They showed that if such a code C exists then it can be shortened to a $[69, 5, 45]$ two-weight code C' over GF(3) with second weight 54, and classified all such codes C'; they then showed by exhaustive search that no such code C' can be a shortened code of the desired code C. Ferret [12, Theorem A.2.8] likewise proved that if the code C of (1) exists then it can be shortened to a $\left[\frac{3q^2+1}{2}, 3, \frac{3q^2-3q}{2}\right]$ two-weight code C' over $\mathrm{GF}(q)$ with second weight $\frac{3q^2-q}{2}$, and characterised the structure of such all such codes C' by reference to a dual $(q+3)/2$-cap. However, for the case $q=7$ we found it computationally unfeasible to determine by exhaustive search whether a $[74, 3, 63]$ code C' with the specified structure can be a shortened code of the desired $[75, 4, 63]$ code C.

2 Definitions and notation

This section introduces definitions and notation used in the rest of the paper. For general background on coding theory, see [20] or [25]; for background on projective geometry, see [7] or [19]. An $[n, k, d]$ code over $\mathrm{GF}(q)$ is *projective* if no two columns of a generator matrix are scalar multiples of each other. The code is *two-weight with weights* w_1 *and* w_2 if every non-zero codeword has weight w_1 or w_2.

We will represent points of the projective space $\mathrm{PG}(k-1, q)$ either in the form p (without angle brackets), or else in the form $\langle v\rangle$ for some non-zero column vector $v \in \mathrm{GF}(q)^k$. Given a non-zero vector $v \in \mathrm{GF}(q)^k$, we write

$$v^\perp := \{x \in \mathrm{GF}(q)^k \mid v^T x = 0\} \tag{2}$$

for the set of vectors orthogonal to v, and

$$\langle v\rangle^\perp := \{\langle x\rangle \mid x \in v^\perp \setminus \{0\}\} \tag{3}$$

for the corresponding set of projective points of $\mathrm{PG}(k-1, q)$; this set forms the hyperplane that is dual to the projective point $\langle v\rangle$.

A *projective* (n, k, h_1, h_2) *set* O *in* $\mathrm{PG}(k-1, q)$ is a proper non-empty subset of the points of the projective space $\mathrm{PG}(k-1, q)$ having $|O| = n$, such that every hyperplane of $\mathrm{PG}(k-1, q)$ contains exactly h_1 or h_2 points of O. Given such a set O with $k = 4$, we shall call the hyperplanes containing exactly $\min(h_1, h_2)$ points of O *small planes*, and the hyperplanes containing exactly $\max(h_1, h_2)$ points of O *large planes*. The following correspondence between projective sets and projective two-weight codes is a slight modification of that given by Calderbank and Kantor [5], based on a result due to Delsarte [9]:

Theorem 2. *Let $y_1, \ldots, y_n$ be distinct non-zero vectors in $\mathrm{GF}(q)^k$. Then the following are equivalent:*

1. *The $k \times n$ matrix having columns $y_1, \ldots, y_n$ generates a projective two-weight $[n, k]$ code over $\mathrm{GF}(q)$ with weights w_1 and w_2 (and therefore minimum distance $\min(w_1, w_2)$)*

2. *$\{\langle y_1\rangle, \ldots, \langle y_n\rangle\}$ is a projective $(n, k, n-w_1, n-w_2)$ set in $\mathrm{PG}(k-1, q)$ with $w_1, w_2 \neq 0$.*

Proof. Let v be any non-zero vector in $\mathrm{GF}(q)^k$. Then the weight of the codeword $(v^T y_1, \ldots, v^T y_n)$ is $n - |\langle v\rangle^\perp \cap \{y_1, \ldots, y_n\}|$. This gives a correspondence between a projective two-weight code C of length n over $\mathrm{GF}(q)$ with weights w_1 and w_2, and a projective $(n, k, n-w_1, n-w_2)$ set O in $\mathrm{PG}(k-1, q)$ with $w_1, w_2 \neq 0$. It remains to show that the existence of O implies that $\dim(C) = k$. Suppose, for a contradiction, that $\dim(C) < k$ so that there is a non-zero $v \in \mathrm{GF}(q)^k$ for which $(v^T y_1, \ldots, v^T y_n) = (0, \ldots, 0)$. Then $|\langle v\rangle^\perp \cap \{y_1, \ldots, y_n\}| = n$, contradicting $w_1, w_2 \neq 0$. □

By Theorem 2, the existence of the projective two-weight code C of (1) is equivalent to the existence of

$$\text{a projective } \left(\tfrac{3q^2+3}{2}, 4, \tfrac{3q+3}{2}, \tfrac{q+3}{2}\right) \text{ set } O \text{ in } \mathrm{PG}(3,q). \tag{4}$$

In particular, in the case $q = 7$, the existence of a projective $(75, 4, 12, 5)$ set in $\mathrm{PG}(3, 7)$ is equivalent to the existence of a projective two-weight $[75, 4, 63]$ code over $\mathrm{GF}(7)$ with second weight 70.

It can be shown that the set of points comprising the duals of the small planes of the projective set O of (4) forms another projective set with the same parameters as O; in the terminology of [2], it follows that the code C is *formally projective self-dual* (see also [27, p. 92]). We state and prove the following consequence of this result:

Lemma 3. *Suppose there exists a projective* $\left(\frac{3q^2+3}{2}, 4, \frac{3q+3}{2}, \frac{q+3}{2}\right)$ *set* O *in* $\mathrm{PG}(3, q)$*. Then the number of small planes is* $\frac{3q^2+3}{2}$*.*

Proof. Let j be the number of small planes. By counting each point of O in each plane of $\mathrm{PG}(3, q)$, we obtain the relation

$$j\left(\frac{q+3}{2}\right) + \left(\frac{q^4-1}{q-1} - j\right)\left(\frac{3q+3}{2}\right) = \left(\frac{3q^2+3}{2}\right)\left(\frac{q^3-1}{q-1}\right),$$

and so $j = \frac{3q^2+3}{2}$. □

Furthermore, given the projective set O of (4), we can constrain the number of small planes containing a given line of $\mathrm{PG}(3, q)$:

Proposition 4 ([12, Lemma A.2.5])**.** *Suppose there exists a projective* $\left(\frac{3q^2+3}{2}, 4, \frac{3q+3}{2}, \frac{q+3}{2}\right)$ *set* O *in* $\mathrm{PG}(3, q)$*, and let* L *be a line of* $\mathrm{PG}(3, q)$ *that intersects* O *in exactly* i *points. Then the number of small planes containing* L *is* $3 - i$*.*

Proof. Let j be the number of small planes containing L. By counting each point of $O \setminus L$ in each plane through L, we obtain the relation

$$j\left(\frac{q+3}{2} - i\right) + (q + 1 - j)\left(\frac{3q+3}{2} - i\right) = \frac{3q^2+3}{2} - i,$$

and so $j = 3 - i$. □

In particular, Proposition 4 implies that no four points of O are collinear.

Given a non-zero vector $v \in \mathrm{GF}(q)^k$ and a matrix $M \in \mathrm{PGL}(k, q)$, we define the action of M on the projective point $\langle v\rangle$ to be $M\langle v\rangle := \langle Mv\rangle$. For a set P of projective points of $\mathrm{PG}(k-1, q)$, we then define $MP := \{Mp \mid p \in P\}$. The *automorphism group* of P is

$$\mathrm{Aut}(P) := \{M \in \mathrm{PGL}(k, q) \mid MP = P\},$$

namely the group of matrices of $\mathrm{PGL}(k, q)$ under whose action the set P maps to itself. If P is a projective set then, by Theorem 2, we can interpret the points of P as the columns of a generator matrix for a projective two-weight code C. The automorphism group of C is isomorphic to the semidirect product of $\mathrm{Aut}(P)$ with $\mathrm{Gal}(\mathrm{GF}(q)/\mathrm{GF}(p))$ (where the Galois group takes account of the action of a field automorphism applied to all co-ordinate positions of the codewords; see [2] for further discussion). In the case $q = p$, which is our primary interest here, the automorphism group of C is isomorphic to $\mathrm{Aut}(P)$.

Given a matrix $A \in \mathrm{PGL}(k,q)$, the *centraliser* of A is

$$C(A) := \{M \in \mathrm{PGL}(k,q) \mid MAM^{-1} = A\},$$

namely the group of matrices of $\mathrm{PGL}(k,q)$ which fix A under the action of conjugacy. It is straightforward to prove:

Lemma 5. *Let P be a set of projective points in $\mathrm{PG}(k-1,q)$ and let $A \in \mathrm{Aut}(P)$. Then $A \in \mathrm{Aut}(MP)$ for all $M \in C(A)$.*

We will make use of the following result on the action of a matrix of $\mathrm{PGL}(k,q)$ on a hyperplane of $\mathrm{PG}(k-1,q)$.

Lemma 6. *Let p be a point of $\mathrm{PG}(k-1,q)$ and let $M \in \mathrm{PGL}(k,q)$. Then $Mp^{\perp} = \left(\left(M^T\right)^{-1} p\right)^{\perp}$.*

Proof. Write $p = \langle v \rangle$ for some non-zero $v \in \mathrm{GF}(q)^k$, By (2) and (3),

$$p^{\perp} = \langle v \rangle^{\perp} = \left\{ \langle x \rangle \mid x \in \mathrm{GF}(q)^k \setminus \{0\},\, v^T x = 0 \right\}.$$

Therefore we have

$$\begin{aligned}
Mp^{\perp} &= \{\langle Mx \rangle \mid x \in \mathrm{GF}(q)^k \setminus \{0\},\, v^T x = 0\} \\
&= \left\{ \langle Mx \rangle \mid x \in \mathrm{GF}(q)^k \setminus \{0\},\, \left(\left(M^T\right)^{-1} v\right)^T Mx = 0 \right\} \\
&= \left\{ \langle y \rangle \mid y \in \mathrm{GF}(q)^k \setminus \{0\},\, \left(\left(M^T\right)^{-1} v\right)^T y = 0 \right\} \\
&= \left\langle \left(M^T\right)^{-1} v \right\rangle^{\perp} \\
&= \left(\left(M^T\right)^{-1} \langle v \rangle\right)^{\perp} \\
&= \left(\left(M^T\right)^{-1} p\right)^{\perp}.
\end{aligned}$$

□

This paper rules out the existence of a projective $(75, 4, 12, 5)$ set O in $\mathrm{PG}(3, 7)$ whose automorphism group $\mathcal{H}$ is a non-trivial subgroup of $\mathrm{PGL}(4, 7)$. By Theorem 2, this implies there is no projective two-weight [75,4,63] code over GF(7) with second weight 70 whose automorphism group is non-trivial. Section 3 describes how to cast the search problem for a projective set, whose automorphism group contains a specified group $\mathcal{H}$, as an integer linear program. In Section 4, we note that to search for O we need examine only groups $\mathcal{H}$ of prime order having the form $\langle M \rangle$, as M ranges over a set of representatives for the conjugacy classes of $\mathrm{PGL}(4, 7)$. This is sufficient to eliminate all but six matrices M from consideration, having order 2 or 3. Section 5 calculates the form of the centraliser of these six matrices, and constrains the positions of the points of O contained in a single large plane. Section 6 uses an equivalence relation on the elements of $\mathrm{PGL}(3, 7)$, by reference to the known form of the centraliser, to bring the search within computational reach.

3 Conversion of the search problem to an integer linear program

In this section we describe how to cast the search problem for a projective (n, k, h_1, h_2) set O in $\mathrm{PG}(k-1, q)$, whose automorphism group contains a specified subgroup $\mathcal{H}$ of $\mathrm{PGL}(k, q)$, as an integer linear program. This follows the treatment of the papers [4], [21], and [22], which are based on the method of Kramer and Mesner [23] for constructing designs with a prescribed automorphism group. We begin with the simpler (but less efficient) case where no subgroup $\mathcal{H}$ is specified.

Proposition 7. *The existence of a projective* (n, k, h_1, h_2) *set* O *in* $\mathrm{PG}(k-1, q)$ *is equivalent to the existence of a solution to an integer linear program having* $\frac{2(q^k-1)}{q-1}$ *variables.*

Proof. We assign a variable $x_i \in \{0, 1\}$ to each point $p_i \in \mathrm{PG}(k-1, q)$, where $x_i = 1$ if and only if $p_i \in O$. We assign a variable $y_j \in \{0, 1\}$ to each hyperplane $p_j^\perp \in \mathrm{PG}(k-1, q)$, where $y_j = 1$ if and only if the hyperplane $p_j^\perp$ contains exactly h_1 points of O. The conditions on O are then equivalent to the following system of linear equations governing the $\frac{2(q^k-1)}{q-1}$ variables $\{x_i, y_j\}$:

$$\begin{aligned} \sum_i x_i &= n, \\ (h_2 - h_1)y_j + \sum_{i:\, p_i \in p_j^\perp} x_i &= h_2 \quad \text{for each } j. \end{aligned}$$

(The first equation fixes the number of points of O as n. The second equation states that the number of points of O contained in the hyperplane $p_j^\perp$ is h_1 in the case that $y_j = 1$, and h_2 in the case that $y_j = 0$.) □

In the case where the automorphism group of the projective set contains a specified non-trivial subgroup $\mathcal{H}$ of $\mathrm{PGL}(k, q)$, the efficiency of the integer linear program of Proposition 7 can be improved:

Proposition 8. *The existence of a projective* (n, k, h_1, h_2) *set* O *in* $\mathrm{PG}(k-1, q)$ *for which* $\mathrm{Aut}(O)$ *contains a given non-trivial subgroup* $\mathcal{H}$ *of* $\mathrm{PGL}(k, q)$ *is equivalent to the existence of a solution to an integer linear program having fewer than* $\frac{2(q^k-1)}{q-1}$ *variables.*

Proof. For each point p_i of $\mathrm{PG}(k-1, q)$ and for any $M \in \mathcal{H}$, the point Mp_i is contained in O if and only if p_i is contained in O. Therefore we can merge the variables x_i of a given orbit of points under the action of $\mathcal{H}$ into a single variable $\overline{x_i}$. Similarly, for each hyperplane $p_j^\perp$ and for any $M \in \mathcal{H}$, the hyperplane $Mp_j^\perp$ contains the same number of points of O as $p_j^\perp$, so we can merge the variables y_j of a given orbit of hyperplanes under the action of $\mathcal{H}$ into a single variable $\overline{y_j}$.

We therefore assign a variable $\overline{x_i} \in \{0, 1\}$ to each distinct point orbit

$$r_i := \{Mp_i \mid M \in \mathcal{H}\}$$

as p_i ranges over the points of $\mathrm{PG}(k-1, q)$, where $\overline{x_i} = 1$ if and only if the point orbit $r_i \subseteq O$. We also assign a variable $\overline{y_j} \in \{0, 1\}$ to each distinct hyperplane orbit

$$s_j := \{Mp_j^\perp \mid M \in \mathcal{H}\} \tag{5}$$

as $p_j^\perp$ ranges over the hyperplanes of $\mathrm{PG}(k-1, q)$, where $\overline{y_j} = 1$ if and only if the hyperplane $p_j^\perp$ contains exactly h_1 points of O. By a similar argument to that used in the proof of Proposition 7, the conditions on O are then equivalent to the following system of linear equations governing the fewer than $\frac{2(q^k-1)}{q-1}$ variables $\{\overline{x_i}, \overline{y_j}\}$:

$$\begin{aligned} \sum_i |r_i|\, \overline{x_i} &= n, \\ (h_2 - h_1)\overline{y_j} + \sum_i |r_i \cap p_j^\perp|\, \overline{x_i} &= h_2 \quad \text{for each } j. \end{aligned}$$

□

The number of variables required in the integer linear program of Proposition 8 can be significantly fewer than $\frac{2(q^k-1)}{q-1}$, giving substantially improved performance compared with the integer linear program of Proposition 7. To find the hyperplane orbits s_j of (5) efficiently, note that by Lemma 6 we can write $s_j = \left\{ \left(\left(M^T\right)^{-1} p_j \right)^{\perp} \mid M \in \mathcal{H} \right\}$ for any point p_j of $\mathrm{PG}(k-1,q)$, which simplifies to $s_j = \left\{ \left(M^T p_j\right)^{\perp} \mid M \in \mathcal{H} \right\}$.

4 Conjugacy classes of $\mathrm{PGL}(4,7)$

Henceforth, suppose that $\widehat{O}$ is a projective $(75,4,12,5)$ set in $\mathrm{PG}(3,7)$. We wish to show that

> *the integer linear program (described in the statement and proof) of Proposition* 8 *for* $O = \widehat{O}$ *has no solution, as* $\mathcal{H}$ *ranges over the non-trivial subgroups of* $\mathrm{PGL}(4,7)$.

In this section, we show that it is instead sufficient for $\mathcal{H}$ to range over a much smaller set of subgroups.

Since Proposition 8 specifies that $\mathrm{Aut}(\widehat{O})$ should contain (but not necessarily equal) $\mathcal{H}$, it is sufficient for $\mathcal{H}$ to range over the cyclic subgroups of $\mathrm{PGL}(4,7)$ of prime order. Furthermore, for any $M \in \mathrm{Aut}(\widehat{O})$ and $N \in \mathrm{PGL}(4,7)$, we have $NMN^{-1} \in \mathrm{Aut}(N\widehat{O})$. Therefore, given a set S of representatives for the 407 conjugacy classes of $\mathrm{PGL}(4,7)$, it is sufficient to show that

> *the integer linear program of Proposition* 8 *for* $O = \widehat{O}$ *has no solution, as* $\mathcal{H}$ *ranges over* $\{\langle M\rangle \mid M \in S$ *and* M *has prime order*$\}$.

We next summarise the method described in [19, p. 42–43] for determining the required set S. We firstly find a set of representatives for the $7^4 - 7 = 2394$ conjugacy classes of $\mathrm{GL}(4,7)$, using the following well-known result:

Theorem 9. *Given a non-constant monic polynomial* $f(\lambda) = f_0 + f_1\lambda + \cdots + f_{m-1}\lambda^{m-1} + \lambda^m$ *of degree* m*, write* $L(f)$ *for the* $m \times m$ companion matrix

$$\begin{bmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ & & & & \ddots & \\ 0 & 0 & 0 & 0 & \dots & 1 \\ -f_0 & -f_1 & -f_2 & -f_3 & \dots & -f_{m-1} \end{bmatrix}.$$

The rational canonical form *of a* $k \times k$ *matrix* A *over a field* F *is the unique matrix of the form* $\mathrm{diag}(L(\psi_1), \dots, L(\psi_\ell))$*, belonging to the same conjugacy class as* A *over* F*, such that* $\psi_1, \dots, \psi_\ell$ *are non-constant monic polynomials in* λ *whose degrees sum to* k *and which satisfy*

$$\psi_i \mid \psi_{i+1} \quad \text{for } i = 1, \dots, \ell - 1. \tag{6}$$

By Theorem 9, the set of 4×4 invertible rational canonical forms over $\mathrm{GF}(7)$ provides a set of representatives for the 2394 conjugacy classes of $\mathrm{GL}(4,7)$. To compute these rational canonical forms, it is sufficient to factor each degree 4 monic polynomial $g(\lambda)$ over $\mathrm{GF}(7)$ that is not divisible by λ, and then to use each assignment of non-constant monic polynomials $\psi_1, \dots, \psi_\ell$ satisfying (6) and $\prod_{i=1}^{\ell} \psi_i = g(\lambda)$ to form the rational canonical form $\mathrm{diag}(L(\psi_1), \dots, L(\psi_\ell))$. We then reduce the 2394 rational canonical forms to the desired set S by retaining a single element of each set $\{R(cA) \mid c \in \mathrm{GF}(7)^*\}$, where $R(M)$ represents the rational canonical form over $\mathrm{GF}(7)$ of the matrix M (which can be calculated using the Maple function `Frobenius`). This retains exactly one of at most six matrices that are conjugate in $\mathrm{PGL}(4,7)$ but not in $\mathrm{GL}(4,7)$.

The specified integer linear program runs quickly for all groups $\langle M \rangle$ of order greater than 3, leaving just seven groups to be checked. Four of these seven groups have order 3, and are generated by

$$A_1 = \begin{bmatrix} 3 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 6 & 0 & 0 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 5 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 5 & 4 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 3 & 2 \end{bmatrix}, \quad A_4 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 5 & 4 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 5 & 4 \end{bmatrix},$$

and the other three have order 2, and are generated by

$$A_5 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad A_6 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad A_7 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 6 & 0 \end{bmatrix}.$$

The matrix A_7 can be excluded by noting that it has order 2 but no fixed points, and so cannot fix a set of size 75. It therefore remains to show that

> *the integer linear program of Proposition* 8 *for* $O = \widehat{O}$ *has no solution when* $\mathcal{H} = \langle A_i \rangle$, *as* i *ranges over* $1 \leq i \leq 6$.

5 Potential base plane sets

In this section, we simplify the required computations for the six remaining groups $\langle A_1 \rangle, \ldots, \langle A_6 \rangle$, by constraining the positions of the points of the projective set $\widehat{O}$ that are contained in a single large plane.

Given that the automorphism group of $\widehat{O}$ contains some group $\langle A \rangle$, Lemma 5 shows that we can replace $\widehat{O}$ by $M\widehat{O}$, for any $M \in C(A)$, and the automorphism group of the replacement projective set $M\widehat{O}$ will still contain $\langle A \rangle$. It is therefore of interest to determine $C(A)$ explicitly for each $A \in \{A_1, \ldots, A_6\}$. To do so, we solve the equation

$$MA = tAM$$

(interpreted in $\mathrm{GL}(4,7)$) as a set of linear equations in the entries of a 4×4 matrix M over $\mathrm{GF}(7)$, for each $A \in \{A_1, \ldots, A_6\}$ and each $t \in \mathrm{GF}(7)^*$ in turn. Each solution set can be expressed in terms of a number of free variables $a, b, c, \ldots$. Since M must be invertible, we then impose the condition $\det(M) \neq 0$. For $A \in \{A_1, \ldots, A_5\}$, it turns out that the determinant condition forces $t = 1$; for $A = A_6$, it forces $t \in \{1, -1\}$. The form of $C(A)$ corresponding to these values of t, but neglecting the determinant condition, is shown in Table 1. Using these explicit forms, we now show that we can make the simplifying assumption that $\langle [0,0,0,1]^T \rangle^\perp$ is a large plane:

Lemma 10. *Suppose that* $\mathrm{Aut}(\widehat{O})$ *contains the group* $\langle A_i \rangle$ *for some* $i \in \{1, \ldots, 6\}$. *Then we can assume without loss of generality that* $\langle [0,0,0,1]^T \rangle^\perp$ *is a large plane.*

Proof. By Lemma 3, the projective set $\widehat{O}$ defines exactly 75 small planes. We claim there are 76 hyperplanes $p^\perp$ of $\mathrm{PG}(3,7)$ such that $Mp^\perp = \langle [0,0,0,1]^T \rangle^\perp$ for some $M = M_p \in C(A_i)$. Therefore we can replace $\widehat{O}$ by $M\widehat{O}$, for some $M \in C(A_i)$, so that $\langle [0,0,0,1]^T \rangle^\perp$ is a large plane; and by Lemma 5, $\mathrm{Aut}(M\widehat{O})$ contains $\langle A_i \rangle$.

	Representative A_i of a conjugacy class of PGL$(4,7)$	$C(A_i)$ has the form
A_i with order 3	$A_1 = \begin{bmatrix} 3 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 6 & 0 & 0 \end{bmatrix}$	$\begin{bmatrix} a & 2b & 3b & b \\ 4c & d & e & f \\ 5c & 6f & d & e \\ c & 6e & 6f & d \end{bmatrix}$
	$A_2 = \begin{bmatrix} 5 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 5 & 4 \end{bmatrix}$	$\begin{bmatrix} a & b & c & c \\ d & e & f & f \\ 3g & 3h & 3i+j & i \\ g & h & 5i & j \end{bmatrix}$
	$A_3 = \begin{bmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 3 & 2 \end{bmatrix}$	$\begin{bmatrix} a & b & c & c \\ d & e & f & f \\ 5g & 5h & 5i+j & i \\ g & h & 3i & j \end{bmatrix}$
	$A_4 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 5 & 4 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 5 & 4 \end{bmatrix}$	$\begin{bmatrix} 3a+b & a & 3c+d & c \\ 5a & b & 5c & d \\ 3e+f & e & 3g+h & g \\ 5e & f & 5g & h \end{bmatrix}$
A_i with order 2	$A_5 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} a & b & c & c \\ d & e & f & f \\ g & h & i & j \\ g & h & j & i \end{bmatrix}$
	$A_6 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} a & b & c & d \\ b & a & d & c \\ e & f & g & h \\ f & e & h & g \end{bmatrix}$ or $\begin{bmatrix} a & b & c & d \\ 6b & 6a & 6d & 6c \\ e & f & g & h \\ 6f & 6e & 6h & 6g \end{bmatrix}$

Table 1: The form of $C(A)$ for each $A \in \{A_1, \ldots, A_6\}$. The centraliser $C(A_i)$ comprises all invertible matrices having the specified form, as $a, b, c, \ldots$ range over GF(7), up to multiplication by a non-zero scalar.

To prove the claim, we use Lemma 6 to replace the condition $Mp^\perp = \langle [0,0,0,1]^T \rangle^\perp$ by $(M^T)^{-1}p = \langle [0,0,0,1]^T \rangle$, or equivalently $\langle M^T [0,0,0,1]^T \rangle = p$. It is therefore sufficient to exhibit 76 distinct points p of $\mathrm{PG}(3,7)$, each of the form $\langle M^T [0,0,0,1]^T \rangle$ for some $M = M_p \in C(A_i)$. This is easily done by computer for each A_i, since $C(A_i)$ is known from Table 1. □

Henceforth, assume that $\langle [0,0,0,1]^T \rangle$ is a large plane, which we shall call the *base plane*.

The base plane is isomorphic to $\mathrm{PG}(2,7)$. By the definition of projective set, the base plane contains exactly 12 points of $\widehat{O}$, and by Proposition 4 no four of these points are collinear. We shall call a set of 12 points of $\mathrm{PG}(2,7)$, no four of which are collinear, a *potential base plane set*. The set of points of $\widehat{O}$ contained in the base plane must be the canonical embedding of some potential base plane set B in $\mathrm{PG}(3,7)$ (meaning the subset $\left\{ \left\langle \left[\begin{smallmatrix} v \\ 0 \end{smallmatrix} \right] \right\rangle \mid \langle v \rangle \in B \right\}$ of $\mathrm{PG}(3,7)$).

(The set $\widehat{O} \cap \langle [0,0,0,1]^T \rangle^\perp$ of points of $\widehat{O}$ contained in the base plane is related to the well-known concept of a residual code in the following way. The matrix G, whose columns $y_1, \ldots, y_{75}$ correspond to the points of $\widehat{O}$, generates a two-weight $[75,4,63]$ code C over $\mathrm{GF}(7)$ with second weight 70, as described in Theorem 2. The submatrix G' of G, whose columns y_i satisfy $[0,0,0,1]y_i = 0$, generates the *residual code* of C with respect to the codeword $[0,0,0,1]G$. The projective points of $\mathrm{PG}(3,7)$ corresponding to the columns of G' form the set $\{\langle y_i \rangle \mid \langle y_i \rangle \in \langle [0,0,0,1]^T \rangle^\perp\} = \widehat{O} \cap \langle [0,0,0,1]^T \rangle^\perp$. Projective two-weight codes have previously been constructed by reference to the structure of certain residual codes, for example in [2].)

We now determine all potential base plane sets that are inequivalent under multiplication by an element of $\mathrm{PGL}(3,7)$. To do so, we recursively generate all inequivalent sets of i points of $\mathrm{PG}(2,7)$, no four of which are collinear, for $i = 1, 2, \ldots, 12$. This requires repeated testing of whether there exists an element of $\mathrm{PGL}(3,7)$ that transforms a set B of i points of $\mathrm{PG}(2,7)$ to another such set B'. In most cases we can avoid the full test by first comparing the number of lines of $\mathrm{PG}(2,7)$ containing 0, 1, 2, and 3 points of B and B', then similarly comparing $B \cup \{p_1\}$ and $B' \cup \{p_1\}$ for all points p_1 of $\mathrm{PG}(2,7)$, and then comparing $B \cup \{p_1, p_2\}$ and $B' \cup \{p_1, p_2\}$ for all distinct points p_1, p_2 of $\mathrm{PG}(2,7)$. If any of the line counts for these pairs of sets disagree, the sets B and B' must be inequivalent. The time and space complexity of these comparisons can be reduced by hashing all the line intersection data for each set B.

In this way, we find that there are exactly 395 inequivalent potential base plane sets $B_1, \ldots, B_{395}$. The canonical embedding in $\mathrm{PG}(3,7)$ of each potential base plane set can therefore be represented in the form $\left\{ \left\langle \left[\begin{smallmatrix} Nv \\ 0 \end{smallmatrix} \right] \right\rangle \mid \langle v \rangle \in B_j \right\}$, for some $N \in \mathrm{PGL}(3,7)$ and for some j in the range $1 \le j \le 395$. It is now sufficient to show that

> *the integer linear program of Proposition* 8 *for* $O = \widehat{O}$ *has no solution when* $\mathcal{H} = \langle A_i \rangle$ *and* $\widehat{O}$ *contains the* 12 *points* $\left\{ \left\langle \left[\begin{smallmatrix} Nv \\ 0 \end{smallmatrix} \right] \right\rangle \mid \langle v \rangle \in B_j \right\}$, *as* N *ranges over* $\mathrm{PGL}(3,7)$ *and as* i *and* j *range over* $1 \le i \le 6$ *and* $1 \le j \le 395$.

6 Equivalence classes of $\mathrm{PGL}(3,7)$

According to the current problem statement, we need to run the integer linear program a total of $|\mathrm{PGL}(3,7)| = 5{,}630{,}688$ times for each pair of values (i,j). In this section, we show how to use the known form of $C(A_i)$ to reduce this number and so make the search computationally feasible.

Fix $A \in \{A_1, \ldots, A_6\}$, and suppose that $\mathrm{Aut}(\widehat{O})$ contains $\langle A \rangle$. Define an equivalence relation on the elements of $\mathrm{PGL}(3,7)$ by $N_1 \sim N_2$ if and only if

$$\left[\begin{array}{ccc|c} & & & w \\ & N_2N_1^{-1} & & x \\ & & & y \\ \hline 0 & 0 & 0 & z \end{array}\right] \in C(A) \text{ for some } w,x,y \in \mathrm{GF}(7),\ z \in \mathrm{GF}(7)^* \tag{7}$$

(interpreting the matrix product $N_2N_1^{-1}$ in $\mathrm{PGL}(3,7)$), where the form of $C(A)$ is known from Table 1.

Now fix $B \in \{B_1, \ldots, B_{395}\}$, and suppose that $\widehat{O}$ contains the 12 points $\left\{\left\langle\begin{bmatrix} N_1v \\ 0 \end{bmatrix}\right\rangle \mid \langle v\rangle \in B\right\}$ for some $N_1 \in \mathrm{PGL}(3,7)$. Let $N_2 \in \mathrm{PGL}(3,7)$ belong to the same equivalence class as N_1, so that (7) holds for some w,x,y,z, and write the 4×4 matrix appearing in (7) as $M = M(N_2)$. Then

$$\begin{aligned}\left\{\left\langle\begin{bmatrix} N_2v \\ 0 \end{bmatrix}\right\rangle \mid \langle v\rangle \in B\right\} &= \left\{\left\langle\left[\begin{array}{ccc|c} & & & w \\ & N_2N_1^{-1} & & x \\ & & & y \\ \hline 0 & 0 & 0 & z \end{array}\right]\left[\begin{array}{c} \\ N_1v \\ \\ \hline 0 \end{array}\right]\right\rangle \mid \langle v\rangle \in B\right\} \\ &= M\left\{\left\langle\begin{bmatrix} N_1v \\ 0 \end{bmatrix}\right\rangle \mid \langle v\rangle \in B\right\}.\end{aligned}$$

So, for any $N_2 \in \mathrm{PGL}(3,7)$ in the same equivalence class as N_1, there is a matrix $M = M(N_2) \in C(A)$ such that $M\widehat{O}$ contains the 12 points $\left\{\left\langle\begin{bmatrix} N_2v \\ 0 \end{bmatrix}\right\rangle \mid \langle v\rangle \in B\right\}$ and, by Lemma 5, such that $\mathrm{Aut}(M\widehat{O})$ contains $\langle A\rangle$. It is therefore sufficient to test just one representative N of each equivalence class of $\mathrm{PGL}(3,7)$. The resulting search procedure, in pseudocode form, is:

```
for $i$ from 1 to 6 do
     $T \leftarrow$ a set of representatives for the equivalence classes of
          $\mathrm{PGL}(3,7)$ with respect to $C(A_i)$
     for $j$ from 1 to 395 do
          for $N$ ranging over $T$ do
               run the integer linear program of Proposition 8 with
               $O \leftarrow \widehat{O}$, $\mathcal{H} \leftarrow \langle A_i\rangle$, and $\widehat{O} \supset \left\{\left\langle\begin{bmatrix} Nv \\ 0 \end{bmatrix}\right\rangle \mid \langle v\rangle \in B_j\right\}$
          end do
     end do
end do
```

It is now computationally feasible to complete this search, establishing:

Theorem 11. *There is no projective* $(75,4,12,5)$ *set in* $\mathrm{PG}(3,7)$ *whose automorphism group is a non-trivial subgroup of* $\mathrm{PGL}(4,7)$.

By Theorem 2, this implies:

Corollary 12. *There is no projective two-weight* $[75,4,63]$ *code over* $\mathrm{GF}(7)$ *with second weight* 70, *whose automorphism group is non-trivial.*

7 Comments

The projective two-weight code C of (1) exists for $q = 3$ and $q = 5$ (see Section 1): there are two inequivalent two-weight $[15, 4, 9]$ codes over GF(3) with second weight 12, and there are eight inequivalent two-weight $[39, 4, 30]$ codes over GF(5) with second weight 35. Furthermore, nine of these ten codes have a non-trivial automorphism group.

Does the code C of (1) exist for infinitely many prime powers q? The work described in this paper was motivated by the hypothesis that an example of such a code could be found for $q = 7$ by assuming the existence of a non-trivial automorphism group; we have shown, using an equivalent formulation involving a projective set, that this is not the case. While it is possible that there are examples of such codes for $q > 7$, a complete search for $q = 9$ or $q = 11$ remains well out of computational reach using the methods of this paper. We might instead ask whether one or more of the above nine codes (having a non-trivial automorphism group and $q = 3$ or $q = 5$) belongs to an infinite family of optimal or near-optimal projective two-weight codes different from that specified in (1).

Acknowledgements

We are grateful to Harold (Thann) Ward and to Ray Hill for several interesting and helpful discussions.

References

[1] I. Boukliev. Some new optimal linear codes over $\mathbb{F}_5$. In *Proc. 25th Spring Conf. of the Union of Bulgarian Mathematicians (Kazanlak, Bulgaria, April 1996)*, pages 81–85, 1996.

[2] I. Bouyukliev, V. Fack, W. Willems, and J. Winne. Projective two-weight codes with small parameters and their corresponding graphs. *Designs, Codes and Cryptography*, **41**:59–78, 2006.

[3] I. Bouyukliev and J. Simonis. Some new results on optimal codes over $\mathbb{F}_5$. *Designs, Codes and Cryptography*, **30**:97–111, 2003.

[4] M. Braun, A. Kohnert, and A. Wassermann. Optimal linear codes from matrix groups. *IEEE Trans. Inform. Theory*, **51**:4247–4251, 2005.

[5] R. Calderbank and W.M. Kantor. The geometry of two-weight codes. *Bull. London Math. Soc.*, **18**:97–122, 1986.

[6] P.J. Cameron and J.H. van Lint. On the partial geometry pg(6,6,2). *J. Combin. Theory (A)*, **32**:252–255, 1982.

[7] R. Casse. *Projective Geometry: An Introduction.* Oxford University Press, Oxford, UK, 2006.

[8] COmputational INfrastructure for Operations Research. Available online: `http://www.coin-or.org`, 2008.

[9] P. Delsarte. Weights of linear codes and strongly regular normed spaces. *Discrete Math.*, **3**:47–64, 1972.

[10] M. van Eupen and R. Hill. An optimal ternary $[69, 5, 45]$ code and related codes. *Designs, Codes and Cryptography*, **4**:271–282, 1994.

[11] M. van Eupen and V.D. Tonchev. Linear codes and the existence of a reversible Hadamard difference set in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5^4$. *J. Combin. Theory (A)*, **79**:161–167, 1997.

[12] S. Ferret. *Projective Spaces and Linear Codes.* PhD thesis, Ghent University, 2003.

[13] S. Ferret and L. Storme. Minihypers and linear codes meeting the Griesmer bound: Improvements to results of Hamada, Helleseth and Maekawa. *Designs, Codes and Cryptography*, **25**:143–162, 2002.

[14] GLPK (GNU Linear Programming Kit). Available online: `http://www.gnu.org/software/glpk`, 2009.

[15] J.H. Griesmer. A bound for error-correcting codes. *IBM J. Res. Develop.*, **4**:532–542, 1960.

[16] N. Hamada and T. Helleseth. A characterization of some $\{3v_2+v_3, 3v_1+v+2; 3, 3\}$-minihypers and some $[15, 4, 9; 3]$-codes with $B_2 = 0$. *J. Stat. Planning Inf.*, **56**:129–146, 1996.

[17] T. Helleseth. Projective codes meeting the Griesmer bound. *Discrete Math.*, **106/107**:265–271, 1992.

[18] R. Hill and D.E. Newton. Optimal ternary linear codes. *Designs, Codes and Cryptography*, **2**:137–157, 1992.

[19] J.W.P. Hirschfeld. *Projective Geometries over Finite Fields.* Clarendon Press, Oxford, UK, 2nd edition, 1998.

[20] W.C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes.* Cambridge University Press, Cambridge, UK, 2003.

[21] A. Kohnert. Constructing two-weight codes with prescribed groups of automorphisms. *Discrete Applied Math.*, **155**:1451–1457, 2007.

[22] A. Kohnert and J. Zwanzger. New linear codes with prescribed group of automorphisms found by heuristic search. *Adv. Math. Commun.*, **3**:157–166, 2009.

[23] E.S. Kramer and D.M. Mesner. t-designs on hypergraphs. *Discrete Math.*, **15**:263–296, 1976.

[24] J.H. van Lint and A. Schrijver. Construction of strongly regular graphs, two-weight codes and partial geometries by finite fields. *Combinatorica*, **1**:63–73, 1981.

[25] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland, Amsterdam, 1986.

[26] G. Solomon and J.J. Stiffler. Algebraically punctured cyclic codes. *Info. and Control*, **8**:170–179, 1965.

[27] H.N. Ward. Divisibility of codes meeting the Griesmer bound. *J. Combin. Theory (A)*, **83**:79–93, 1998.

[28] H.N. Ward. Divisible codes — a survey. *Serdica Math. J.*, **27**:263–278, 2001.