

Department of Mathematical Sciences, Clemson
University

<http://www.ces.clemson.edu/keyj/>

Codes from finite planes and geometries: an update

J. D. Key

keyj@ces.clemson.edu



Abstract

The error-correcting codes obtained from the span over finite fields of incidence matrices of the designs of points and subspaces of a fixed dimension are members of the larger class of generalized Reed-Muller codes. They have many useful properties and have generated much interest amongst geometers and coding theorists. Similarly, the codes obtained from incidences matrices of projective or affine planes have been studied.

This talk will concern some background on these codes and their duals, and will consider some recent new results and partial answers to some standing conjectures, in particular concerning words of small weight and bases of minimum-weight vectors.

March 16, 2007

Contents

- 1 Background 5**
 - 1.1 Coding theory terminology 5
 - 1.2 Projective planes and codes 7

- 2 Codes from planes 8**
 - 2.1 Planes of order n 8
 - 2.2 Desarguesian planes 9
 - 2.3 Words of small weight in codes from projective planes 10

- 3 Geometries of higher dimension 12**

- 4 Dual codes 13**
 - 4.1 Binary codes 13
 - 4.2 Odd-order planes 15

- 5 Bases of minimum-weight vectors 27**

5.1	Bases for desarguesian planes	27
5.2	Higher dimension	30

6 Bibliography 31

Background

Coding theory terminology

- A **linear code** is a subspace of a finite-dimensional vector space over a finite field.
- The **weight** of a vector is the number of non-zero coordinate entries. If a code has smallest non-zero weight d then the code can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors by nearest-neighbour decoding.
- If a code C over a field of order q is of length n , dimension k , and minimum weight d , then we write $[n, k, d]_q$ to show this information.
- 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 under the standard inner product $(,)$, i.e. $C^\perp = \{v \in F^n \mid (v, c) = 0 \text{ for all } c \in C\}$.
- A **check** matrix for C is a generator matrix H for C^\perp .

Coding theory terminology continued

- 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.
- An **automorphism** of a code C is an isomorphism from C to C .
- If C is the row span over any finite field of an incidence matrix for a plane then every automorphism (bijection that preserves points, lines and incidence) of the plane will give an automorphism of C , i.e. $\text{Aut}(\Pi) \subseteq \text{Aut}(C)$.

Projective planes and codes

Definition 1 An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{L}, \mathcal{I})$, with point set $\mathcal{P} \neq \emptyset$, line set $\mathcal{L} \neq \emptyset$, $\mathcal{P} \cap \mathcal{L} = \emptyset$, and incidence $\mathcal{I} \subset \mathcal{P} \times \mathcal{L}$, is a *projective plane* if

- every set of two points are together incident with exactly one line;
- every set of two lines are together incident with exactly one point (i.e. meet in a point);
- there are four points no three of which are collinear.

If \mathcal{P} or \mathcal{L} are finite, then there is an integer $n \geq 2$ such that $|\mathcal{P}| = |\mathcal{L}| = n^2 + n + 1$ and every line (point) is incident with exactly $n + 1$ points (lines). n is the *order* of the plane.

The *code* C_F of a plane Π over the finite field F is the space spanned by the incidence vectors of the lines over F , i.e. the row span over F of an *incidence matrix* with rows indexed by the lines, columns by the points.

Codes from planes

Planes of order n

Some old results from the folklore, taken from [AK92]:

Result 1 *Let Π be a projective plane of order n and let p be a prime dividing n .*

The minimum-weight vectors of $C_p(\Pi)$, are precisely the scalar multiples of the incidence vectors of the lines, i.e. av^L , where $a \in \mathbb{F}_p$, $a \neq 0$, and L is a line of Π .

The minimum weight of $C_p(\Pi)^\perp$ is at least $n + 2$. If the minimum weight is $n + 2$ then, $p = 2$ and n is even, in which case the minimum-weight vectors are all of the form v^X where X is a hyperoval of Π .

Result 2 *If π is an affine plane of order n and p is a prime dividing n , then the minimum weight of $C_p(\pi)$ is n and all minimum-weight vectors are constant.*

If $n = p$ the minimum-weight vectors of $C_p(\pi)$ are precisely the scalar multiples of the incidence vectors of the lines of π .

Desarguesian planes

Result 3 Let p be any prime, $q = p^t$, and $\Pi = PG_2(\mathbb{F}_q)$. Then $C_p(\Pi)$ has dimension $\binom{p+1}{2}^t + 1$. The minimum-weight vectors of $C_p(\Pi)$ are the scalar multiples of the incidence vectors of the lines. The minimum weight d^\perp of $C_p(\Pi)^\perp$ satisfies

$$q + p \leq d^\perp \leq 2q,$$

with equality at the lower bound if $p = 2$.

If $\pi = AG_2(\mathbb{F}_q)$, then $C_p(\pi)$ has dimension $\binom{p+1}{2}^t$. The minimum-weight vectors of $C_p(\pi)$ are the scalar multiples of the incidence vectors of the lines of π . The minimum weight d^\perp of $C_p(\pi)^\perp$ satisfies

$$q + p \leq d^\perp \leq 2q,$$

with equality at the lower bound when $p = 2$.

Words of small weight in codes from projective planes

The minimum weight of the p -ary code from a projective plane of order n where p divides n is $n + 1$. The next weight to occur in all known cases is $2n$, the weight of the difference of the incidence vectors of two lines.

Question 1 *Is it true that the p -ary code from a projective plane of order n where p divides n is $n + 1$ has no words in the range $[n + 2, 2n]$?*

Chouinard [Cho00] showed that for desarguesian of prime order there are no words of weight in the range $[p + 2, 2p - 1]$.

For non-prime order, for $n \leq 8$, the weight enumerators are known and the answer to the question is in the affirmative.

There are four planes of order 9, and Chouinard [Cho02] showed that the answer is again in the affirmative for these four planes.

Update

A recently submitted paper by V. Fack, Sz. L. Fancsali, L. Storme, G. Van de Voorde, and J. Winne [FFS⁺] extends the results of Chouinard.

They study codewords of small weight in the codes from desarguesian projective planes and extend the results of Chouinard on codewords of small weight in the p -ary codes arising from $PG_2(p)$, p prime.

Using a Moorhouse basis (see Result 14) for the code, they characterize all the codewords of $C_p(PG_2(\mathbb{F}_p))$, for p prime, of weight up to $2p + \frac{p-1}{2}$ for $p \geq 19$.

They also address Question 1:

[FFS⁺, Theorem 6]: In the p -ary linear code of $PG_2(p^3)$, p prime, $p \geq 7$, there are no codewords with weight in the interval $[p^3 + 2, 2p^3 - 1]$.

Geometries of higher dimension

For dimensions higher than 2, the designs are desarguesian and the codes are various generalized Reed-Muller. We have (see, for example, [AK98, AK92]):

Result 4 *The code over \mathbb{F}_p of the design of points and r -dimensional subspaces of the projective geometry $PG_m(\mathbb{F}_q)$ is the generalized Reed-Muller code $\mathcal{P}_{\mathbb{F}_q/\mathbb{F}_p}(m - r, m + 1)$. It has minimum weight $(q^{r+1} - 1)/(q - 1)$ and the minimum-weight vectors are the multiples of the incidence vectors of the blocks.*

For $r = 1$ we have the designs of points and lines. We ask the same question: are there words in the range $[q + 2, 2q - 1]$?

For $q = 2$ the range is empty; for $q = 3$ and $m = 3, 4, 5$ computation with Magma [CSW06] showed no words of weight 5; for $q = 4$ and $m = 3$ Magma showed no words in the range.

Dual codes

The minimum weight of the dual code of a projective plane is not, in general, known: see Results 1,3. (Even less is known about the higher dimensional cases.) More is known about the binary case than the odd order case.

Binary codes

If a projective plane of even order n does not have hyperovals, the next possible weight in $C_2(\Pi)^\perp$ is $n + 4$.

A non-empty set \mathcal{S} of points in a plane is of **even type** if every line of the plane meets it evenly. Then $|\mathcal{S}|$ and the order n of the plane must be even, and $|\mathcal{S}| = n + 2s$, where $s \geq 1$.

A set has **type** (n_1, n_2, \dots, n_k) if any line meets it in n_i points for some i , and for each i there is at least one line that meets it in n_i points. A set is of even type if all the n_i are even. Such a set of size $n + 4$ in a plane of even order is of type $(0, 2, 4)$.

Korchmáros and Mazzocca [KM90] consider $(n+t)$ -sets of type $(0, 2, t)$ in the desarguesian plane of order n . They show that sets of size $n+4$ that are of type $(0, 2, 4)$ always exist in the desarguesian plane for $n = 4, 8, 16$, but have no existence results for size $n+4$ for $n > 16$.

From Key and de Resmini [KdR98]:

Result 5 *Let Π be any of the known planes of order 16. Then Π has a 20-set of even type.*

(Two of these planes do not have hyperovals.)

Incorrect exercise from [AK92, page 214]:

If $\Pi = PG_2(\mathbf{F}_{2^m})$, where $m \geq 3$ and $C = C_2(\Pi)$, show that if $c \in C^\perp$ satisfies $\text{wt}(c) > 2^m + 2$, then $\text{wt}(c) \geq 2^m + 8$. (Probably true for $m \geq 5$.)

Blokhuis, Szőnyi and Weiner [BSW03], Gács and Weiner [GW03], and Limbupasiriporn [Lim05], further explore sets of even type.

Odd-order planes

The minimum weight of the dual code of planes of odd order is only known in general for desarguesian planes of prime order p (when it is $2p$), and for some planes of small order.

The following results appeared in Clark and Key [CK99], and part of them much earlier in Sachar [Sac79]:

Result 6 *If \mathcal{D} is a projective plane of odd order $q = p^t$, then*

1. $d^\perp \geq \frac{4}{3}q + 2$;
2. if $p \geq 5$ then $d^\perp \geq \frac{3}{2}q + 2$.

(This is better than the bound $p + q$ for desarguesian planes.)

Result 7 *A projective plane of square order q^2 that contains a Baer subplane has words of weight $2q^2 - q$ in its p -ary dual code, where $p|q$.*

Translation planes

From Clark, Key and de Resmini [CKdR02]:

Result 8 *Let Π be a projective translation plane of order q^m (e.g. $PG_2(\mathbb{F}_q^m)$) where $m = 2$ or 3 , $q = p^t$, and p is a prime. If C is its p -ary code then C^\perp has words of weight*

$$2q^m - (q^{m-1} + q^{m-2} + \cdots + q).$$

If Π is desarguesian, this also holds for $m = 4$.

We really want this for all $m \geq 2$ to get an upper bound for the minimum weight of C^\perp better than $2q^m$. But, we couldn't verify our construction for $m \geq 5$.

For the desarguesian plane of order p^m , where p is a prime, in all cases where the minimum weight of the dual p -ary code is known, and in particular for $p = 2$, or for $m = 1$, the minimum weight is precisely as given in this formula,

$$2p^m - (p^{m-1} + p^{m-2} + \cdots + p).$$

Question 2 *Is the minimum weight of the dual code of the p -ary code of the desarguesian plane of order p^m given by the formula*

$$2p^m - (p^{m-1} + p^{m-2} + \cdots + p) = 2p^m + 1 - \frac{p^m - 1}{p - 1}$$

for all primes p and all $m \geq 1$?

Figuerola planes

A similar construction as that used in Result 8 applies to Figuerola planes: see Key and de Resmini [KdR03].

Result 9 Let Φ be the Figuerola plane $\text{Fig}(q^3)$ of order q^3 where $q = p^t$ and p is any prime. Let C denote the p -ary code of Φ . Then C^\perp contains words of weight $2q^3 - q^2 - q$. Furthermore, if d^\perp denotes the minimum weight of C^\perp then

1. $d^\perp = q + 2$ if $p = 2$;
2. $\frac{4}{3}q + 2 \leq d^\perp \leq 2q^3 - q^2 - q$ if $p = 3$;
3. $\frac{3}{2}q + 2 \leq d^\perp \leq 2q^3 - q^2 - q$ if $p > 3$.

Planes of order 9

The other odd orders for which the minimum weight is known in the desarguesian case are $q = 9$ (see [KdR01]) and $q = 25$ (see [Cla00, CHKW03]).

From Key and de Resmini [KdR01]:

Result 10 *Let Π be a projective plane of order 9. The minimum weight of the dual ternary code of Π is 15 if Π is Φ , Ω , or Ω^D , and 14 if Π is Ψ .*

The four projective planes of order 9 are: the desarguesian plane, Φ , the translation (Hall) plane, Ω , the dual translation plane, Ω^D , and the Hughes plane, Ψ . The weight-15 vectors are from the Baer subplane construction; the weight-14 are from two totally disjoint (share no points nor lines) Fano planes.

Planes of order 25

From Clark, Hatfield, Key and Ward [CHKW03]:

Result 11 *If Π is a projective plane of order 25 and C is the code of Π over F_5 , then the minimum weight d^\perp of C^\perp is either 42 or 44, or $45 \leq d^\perp \leq 50$.*

- *If Π has a Baer subplane, then the minimum weight is either 42, 44 or 45.*
- *If the minimum weight is 42, then a minimum-weight word has support that is the union of two projective planes, π_1 and π_2 , of order 4 that are totally disjoint (share no points nor lines) and the word has the form $\mathbf{v}^{\pi_1} - \mathbf{v}^{\pi_2}$.*
- *If the minimum weight is 44 then the support of a minimum-weight word is the union of two disjoint complete 22-arcs that have eleven 2-secants in common.*
- *If the minimum weight is 45 then $\mathbf{v}^\beta - \mathbf{v}^l$, where β is a Baer subplane of Π and l is a line of Π that is a line of the subplane, is a minimum-weight word.*

Corollary 1 *The dual 5-ary code of the desarguesian projective plane $PG_2(\mathbb{F}_{25})$ has minimum weight 45.*

All the known planes of order 25 have Baer subplanes. Czerwinski and Oakden [C092] found the 21 translation planes of order 25.

Planes of order 49

Work for masters project of Fidele Ngwane [KN] at Clemson:

Result 12 *If C is the 7-ary code of a projective plane of order 49, then the minimum weight of the dual code C^\perp is at least 88. Thus, the minimum weight d^\perp of C^\perp satisfies*

$$88 \leq d^\perp \leq 98.$$

Further, $88 \leq d^\perp \leq 91$ if the projective plane contains a Baer subplane.

Note that a word of weight 86 that consists of two totally disjoint 2-(43,6,1) designs (i.e. planes of order 6), a combinatorial possibility, cannot exist by Bruck-Ryser.

Mathon and Royle [MR95] find that there are 1347 translation planes of order 49.

Totally disjoint sets

Let Π be a projective plane of order n , and let $p|n$, where p is a prime.

Let \mathcal{S}_i for $i \in \{1, 2\}$ be a set of s_i points of Π that is a $(0, 1, h_i)$ -set, where $h_i > 1$, i.e. lines meet \mathcal{S}_i in 0, 1 or h_i points.

\mathcal{S}_1 and \mathcal{S}_2 are **totally disjoint** if for $\{i, j\} = \{1, 2\}$,

- they have no points in common;
- the h_i -secants to \mathcal{S}_i are exterior to \mathcal{S}_j ;
- every 1-secant to \mathcal{S}_i is a 1-secant to \mathcal{S}_j .

Result 13 *If Π is a projective plane of order n , p a prime dividing n , and \mathcal{S}_i for $i = 1, 2$ are a pair of totally disjoint $(0, 1, h_i)$ -sets, respectively, where $p|h_i$, then $v^{\mathcal{S}_1} - v^{\mathcal{S}_2}$ is a word of weight $s_1 + s_2$ in $C_p(\Pi)^\perp$ where $|\mathcal{S}_i| = s_i$. Further*

$$n + 1 = \frac{s_1 - 1}{h_1 - 1} + s_2 = \frac{s_2 - 1}{h_2 - 1} + s_1.$$

The following special cases are feasible:

1. $s_1 = s_2 = h_1 = h_2$: the configuration consists of two lines with the point of intersection omitted.
2. If $n = q^r = p^t$ and $s_2 = h_2$, then $p|h_1$ and $(h_1 - 1)|(q^r - 1)$ is possible if $h_1 = q$, which will give a word of weight $2q^r - (q^{r-1} + q^{r-2} + \dots + q)$. This is the construction of our Result 8.

Other numerical possibilities

1. $n = 9$, $s_1 = s_2 = 7$, $h_1 = h_2 = 3$: two totally disjoint Fano planes, weight 14 (see [KdR01]).
2. $n = 25$, $s_1 = s_2 = 21$, $h_1 = h_2 = 5$: two totally disjoint planes of order 4, weight 42; in general it is unknown if a plane of order 25 can have an embedded plane of order 4 (see the note below).
3. $n = 27$, $s_1 = s_2 = 19$, $h_1 = h_2 = 3$: two totally disjoint Steiner triple systems, weight 38; it is not known if this is possible.
4. $n = 27$, $s_1 = 25$, $s_2 = 16$, $h_1 = 3$, $h_2 = 6$: $2-(25, 3, 1)$ and $2-(16, 6, 1)$ designs, weight 41; no design with the latter parameters can exist by Fisher's inequality.
5. $n = 49$, $s_1 = s_2 = 43$, $h_1 = h_2 = 7$: two totally disjoint $2-(43, 7, 1)$ designs, i.e. planes of order 6, weight 86; planes of order 6 do not exist, by the Bruck-Ryser theorem (see, for example, [AK92, Chapter 4]).
6. $n = 81$, $s_1 = 73$, $s_2 = 46$, $h_1 = 3$, $h_2 = 6$: $2-(73, 3, 1)$ and $2-(46, 6, 1)$ designs, weight 119; it is unknown if a design with the latter parameters exists.

- The desarguesian plane $PG_{2,1}(F_q)$ does not contain subplanes of orders other than those from subfields of F_q , so the configurations for $n = 9$ or 25 (1. and 2. of previous page) cannot exist for the desarguesian case.
- It is conjectured that any non-desarguesian plane contains a Fano plane (see Neumann [Neu55]).
- Not all the known planes of order 25 have been checked for subplanes of order 4, but some are known **not** to have any; Clark [Cla00] has a survey of the known results.
- All known planes of square order have Baer subplanes.

Bases of minimum-weight vectors

Bases for desarguesian planes

There are several nice constructions of bases of incidence vectors of lines for the desarguesian planes of prime order:

Result 14 (Moorhouse[Moo91]) *Let $\Pi = PG_2(\mathbb{F}_p)$ where p is prime. A basis for the code $C_p(\Pi)$ can be found by taking the incidence vectors of the following lines: choose any one line L ; then take all the other p lines through any one point; any $p - 1$ lines from a second point on L ; and so on, until a single line is chosen from one of the final two points, and no lines are chosen through the last point. This gives*

$$1 + p + (p - 1) + (p - 2) + \cdots + 1 = p(p + 1)/2 + 1 = \binom{p + 1}{2} + 1$$

lines, whose incidence vectors form a basis for $C_p(\Pi)$.

Result 15 (Blokhuis and Moorhouse[BM95]) *Let $\Pi = PG_2(\mathbb{F}_p)$ of prime order p , and let \mathcal{C} denote a conic in Π . Then a basis for the code $C_p(\Pi)$ can be found by taking the incidence vectors of all nonsecants to \mathcal{C} , i.e. all tangents and exterior lines.*

Using a result concerning information sets for generalized Reed-Muller codes:

Result 16 (Key, McDonough, Mavron[KMM06]) *If p is a prime,*

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

is an information set for the p -ary code for the affine geometry design of points and r -dimensional subspaces in $AG_m(\mathbb{F}_p)$.

the following basis is derived:

Result 17 (Key, McDonough, Mavron[KMM06]) *If $C = C_p(PG_2(\mathbb{F}_p))$, where p is a prime, then, using homogeneous coordinates, the incidence vectors of the set of lines*

$$\{(1, a_1, a_2)' \mid a_i \in \mathbb{F}_p, a_1 + a_2 \leq p-1\} \cup \{(0, 0, 1)'\}$$

form a basis for C .

Similarly, a basis of lines for $C_p(AG_2(\mathbb{F}_p))$ for p prime is the set of incidence vectors of the lines with equation $a_1X_1 + a_2X_2 = p-1$ with $a_1 + a_2 \leq p-1$, where $a_i \in \mathbb{F}_p$ for $1 \leq i \leq 2$, and not all the a_i are 0, along with the line with equation $X_m = 0$.

Higher dimension

Tentative basis for the p -ary code of the design of points and lines in $AG_3(\mathbb{F}_p)$, where p is a prime:

for $a, b \in \mathbb{F}^3$ let $[a, b]$ denote the line $a\mathbb{F}_p + b$. Let

$$\mathcal{L} = \{[a, b] \mid a_1 + a_2 + a_3 \geq p - 1, b_1 = 0, b_2 = a_2, b_3 = a_2 + a_3\}$$

where $a = (a_1, a_2, a_3)$. The claim is that the incidence vectors of \mathcal{L} form a basis for the code.

Bibliography



References

- [AK92] E. F. Assmus, Jr and J. D. Key. *Designs and their Codes*. Cambridge: Cambridge University Press, 1992. Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).
- [AK98] E. F. Assmus, Jr and J. D. Key. Polynomial codes and finite geometries. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, pages 1269–1343. Amsterdam: Elsevier, 1998. Volume 2, Part 2, Chapter 16.
- [BM95] Aart Blokhuis and G. Eric Moorhouse. Some p -ranks related to orthogonal spaces. *J. Algebraic Combin.*, 4:295–316, 1995.
- [BSW03] Aart Blokhuis, Tamás Szőny, and Zsuzsa Weiner. On sets without tangents in Galois planes of even order. *Des. Codes Cryptogr.*, 29:91–98, 2003.
- [CHKW03] K. L. Clark, L.D. Hatfield, J. D. Key, and H. N. Ward. Dual codes of projective planes of order 25. *Advances in Geometry*, 3:140–152, 2003.

- [Cho00] K. Chouinard. *Weight distributions of codes from planes*. PhD thesis, University of Virginia, 2000.
- [Cho02] K. Chouinard. On weight distributions of codes of planes of order 9. *Ars Combin.*, 63:3–13, 2002.
- [CK99] K. L. Clark and J. D. Key. Geometric codes over fields of odd prime power order. *Congr. Numer.*, 137:177–186, 1999.
- [CKdR02] K. L. Clark, J. D. Key, and M. J. de Resmini. Dual codes of translation planes. *European J. Combin.*, 23:529–538, 2002.
- [Cla00] K. L. Clark. *Improved bounds for the minimum weight of the dual codes of some classes of designs*. PhD thesis, Clemson University, 2000.
- [CO92] Terry Czerwinski and David Oakden. The translation planes of order twenty-five. *J. Combin. Theory, Ser. A*, 59:193–217, 1992.
- [CSW06] J. Cannon, A. Steel, and G. White. Linear codes over finite fields. In J. Cannon and W. Bosma, editors, *Handbook of Magma Functions*, pages 3951–4023. Computational Algebra Group, Department of Mathematics, University of Sydney, 2006. V2.13,

<http://magma.maths.usyd.edu.au/magma>.

- [FFS⁺] V. Fack, Sz. L. Fancsali, L. Storme, G. Van de Voorde, and J. Winne. Small weight codewords in the codes arising from Desarguesian projective planes. Submitted.
- [GW03] A. Gács and Zs. Weiner. On $(q + t, t)$ -arcs of type $(0, 2, t)$. *Des. Codes Cryptogr.*, 29:131–139, 2003.
- [KdR98] J. D. Key and M. J. de Resmini. Small sets of even type and codewords. *J. Geom.*, 61:83–104, 1998.
- [KdR01] J. D. Key and M. J. de Resmini. Ternary dual codes of the planes of order nine. *J. Statist. Plann. Inference*, 95:229 – 236, 2001.
- [KdR03] J. D. Key and M. J. de Resmini. An upper bound for the minimum weight of dual codes of Figueroa planes. *J. Geom.*, 77:102–107, 2003.
- [KM90] Gábor Korchmáros and Francesco Mazzocca. On $(q + t)$ -arcs of type $(0, 2, t)$ in a Desarguesian plane of order q . *Math. Proc. Cambridge Philos. Soc.*, 108:445–459, 1990.

- [KMM06] J. D. Key, T. P. McDonough, and V. C. Mavron. Information sets and partial permutation decoding of codes from finite geometries. *Finite Fields Appl.*, 12:232–247, 2006.
- [KN] J. D. Key and F. Ngwane. The minimum weight of the dual 7-ary code of a projective plane of order 49. Submitted.
- [Lim05] J. Limbupasiriporn. *Partial permutation decoding for codes from designs and finite geometries*. PhD thesis, Clemson University, 2005.
- [Moo91] G. Eric Moorhouse. Bruck nets, codes, and characters of loops. *Des. Codes Cryptogr.*, 1:7–29, 1991.
- [MR95] Rudolf Mathon and Gordon F. Royle. The translation planes of order 49. *Des. Codes Cryptogr.*, 5:57–72, 1995.
- [Neu55] H. Neumann. On some finite non-desarguesian planes. *Arch. Math.*, VI:36–40, 1955.
- [Sac79] H. Sachar. The F_p span of the incidence matrix of a finite projective plane. *Geom. Dedicata*, 8:407–415, 1979.