On sets of vectors of a finite vector space in which every subset of basis size is a basis

Simeon Ball

17 January 2012

Abstract

It is shown that the maximum size of a set S of vectors of a k-dimensional vector space over $\mathbb{F}_q$, with the property that every subset of size k is a basis, is at most $q+1$, if $k \leq p$, and at most $q+k-p$, if $q \geq k \geq p+1 \geq 4$, where $q = p^h$ and p is prime. Moreover, for $k \leq p$, the sets S of maximum size are classified, generalising Beniamino Segre's "arc is a conic" theorem.

These results have various implications. One such implication is that a $k \times (p+2)$ matrix, with $k \leq p$ and entries from $\mathbb{F}_p$, has k columns which are linearly dependent. Another is that the uniform matroid of rank r that has a base set of size $n \geq r+2$ is representable over $\mathbb{F}_p$ if and only if $n \leq p+1$. It also implies that the main conjecture for maximum distance separable codes is true for prime fields; that there are no maximum distance separable linear codes over $\mathbb{F}_p$, of dimension at most p, longer than the longest Reed-Solomon codes. The classification implies that the longest maximum distance separable linear codes, whose dimension is bounded above by the characteristic of the field, are Reed-Solomon codes.

In the autumn of 2008 while I was visiting Budapest, together with Andras Gács, we formulated the coordinate free version of Segre's lemma of tangents (Lemma 2.1) which is fundamental to this article. I dedicate this work to Andras, whose humour, enthusiasm and brilliance I am grateful to have known.

1 Introduction

Let S be a set of vectors of the vector space $\mathbb{F}_q^k$ with the property that every subset of S of size k is a basis.

Departament Matemàtica Aplicada IV, Universitat Politècnica Catalunya, Barcelona, Spain. e-mail: simeon@ma4.upc.edu

Mathematics Subject Classification (2010): 51E21, 15A03, 94B05, 05B35.

In this article we shall prove an upper bound on the size of S and for $k \leq p$, where $q = p^h$ and p is prime, we shall prove that the largest examples are equivalent to the following example.

EXAMPLE 1.1. The set

$$S = \{(1, t, t^2, \ldots, t^{k-1}) \mid t \in \mathbb{F}_q\} \cup \{(0, \ldots, 0, 1)\},$$

is a set of size $q + 1$. It is easily shown that S has the required property by checking that the $k \times k$ Vandermonde matrix formed by k vectors of S, has non-zero determinant.

The following upper bound is easily proved.

LEMMA 1.2. *A set S of vectors of the vector space $\mathbb{F}_q^k$, with the property that every subset of S of size k is a basis, has size at most $q + k - 1$.*

Proof. Consider the $(k-2)$-dimensional subspace U spanned by $k-2$ vectors of S. Each of the $q+1$ hyperplanes containing U contains at most one other vector of S. Thus, $|S| \leq k - 2 + q + 1$. □

In 1947, Bose [3] noted that if $p \geq k = 3$ then $|S| \leq q + 1$ and in the article [18] from 1955, Segre proved that if $p \geq k = 3$ then equality in the bound was only attained by examples equivalent to Example 1.1. In 1952, Bush [4] proved the following lemma.

LEMMA 1.3. *A set of vectors S of the vector space $\mathbb{F}_q^k$, $k \geq q$, with the property that every subset of S of size k is a basis, has size at most $k + 1$. Moreover, a set S which attains the bound is equivalent to*

$$\{(\lambda_1, 0 \ldots, 0), \ldots, (0, \ldots, 0, \lambda_k), (1, 1, \ldots, 1)\}.$$

Proof. After a suitable choice of basis, we can assume that

$$S \supseteq S' = \{(\lambda_1, 0 \ldots, 0), \ldots, (0, \ldots, 0, \lambda_k), (1, 1, \ldots, 1)\},$$

for some $\lambda_i \in \mathbb{F}_q \setminus \{0\}$. Suppose there is an $x \in S \setminus S'$. Since $k \geq q$ either there are two coordinates, the i-th and the j-th say, of x which are the same or one of the coordinates, the i-th say, is zero. In the first case the hyperplane defined by the equation $X_i = X_j$ contains k vectors of S. In the second case, the hyperplane $X_i = 0$ contains k vectors of S. In both cases, this is a contradiction, so $S = S'$. □

The main conjecture for maximum distance separable codes (which we shall define in Section 9) in the terminology of this section is the following. This was essentially proposed by Segre [19] in 1955, although as a question rather than a conjecture; see also MacWilliams and Sloane [14].

CONJECTURE 1.4. *A set S of vectors of the vector space $\mathbb{F}_q^k$, with the property that every subset of S of size $k \leq q$ is a basis, has size at most $q+1$, unless q is even and $k = 3$ or $k = q-1$, in which case it has size at most $q+2$.*

In this article we shall prove the conjecture for all $k \leq p+1$, where $q = p^h$ and p is prime, which will prove the conjecture in its entirety for q prime.

The conjecture is known to be true for all $q \leq 27$, for all $k \leq 5$ and $k \geq q-3$ and for $k = 6, 7, q-4, q-5$ with some exceptions, see [11].

For $p = 2$ and $k = 3$, one can add the vector $(0,1,0)$ to Example 1.1 and obtain an example with $q+2$ vectors. For these parameters, such a set of $q+2$ vectors is called a *hyperoval*, and these have been studied extensively. There are many examples known which are not equivalent (up to change of basis and field automorphisms) to Example 1.1, the first of which were discovered by Segre [20], [21] and subsequently by Glynn [8], Payne [16], Cherowitzo [5], Cherowitzo, Penttila, Pinneri and Royle [7], Cherowitzo, O'Keefe and Penttila [6].

The only other known examples of size $q+1$, which are not equivalent to the previous ones, are the following examples.

EXAMPLE 1.5. *(Glynn [9])* The set

$$S = \{(1, t, t^2 + \eta t^6, t^3, t^4) \mid t \in \mathbb{F}_9\} \cup \{(0, \ldots, 0, 1)\},$$

is a set of 10 vectors of $\mathbb{F}_9^5$ with the required property, if η is chosen such that $\eta^4 = -1$.

EXAMPLE 1.6. *(Hirschfeld [10])* The set

$$S = \{(1, t, t^{2^r}, t^{2^r+1}) \mid t \in \mathbb{F}_q\} \cup \{(0, \ldots, 0, 1)\},$$

is a set of $q+1$ vectors of $\mathbb{F}_q^4$ and has the required property when $q = 2^h$ and $(r,h) = 1$.

As we shall see in Lemma 5.1, every example of a set S in $\mathbb{F}_q^k$ gives an example of a set of size $|S|$, with the required property, in $\mathbb{F}_q^{|S|-k}$. Thus, for example, the hyperovals give rise to examples of size $q+2$ in $\mathbb{F}_q^{q-1}$, subsets of size $q+1$ of the hyperovals give rise to examples of size $q+1$ in $\mathbb{F}_q^{q-2}$ and Example 1.6 gives rise to an example of size $q+1$ in $\mathbb{F}_q^{q-3}$.

There are many upper bounds known on $|S|$, similar to those mentioned below. For a complete list, see [11], see also [12]. Relevant to this article we have from Voloch [24] that if $3 \leq k \leq q/45 + c_1$ and q is prime then $|S| \leq q+1$, where c_1 is a constant. Also relevant is the following from Segre [22] (with an improved constant Thas [23]), which is improved upon here for q the square of a prime. If $3 \leq k \leq \sqrt{q}/4 + c_2$ and q is an odd square then $|S| \leq q+1$, where c_2 is a constant. In Voloch [25], the bound $|S| \leq q+1$ is proven for an odd $q = p^{2e+1}$, $e \geq 1$ and $3 \leq k < \sqrt{pq}/4 - 29p/16 + 4$.

In all of the above if k is one less than the upper bound and $|S| = q + 1$ then S is equivalent to Example 1.1. All classifications of $|S| = q + 1$ use Segre's theorem [18], mentioned before, that states that if $|S| = q + 1$ and $p \geq k = 3$ then S is equivalent to Example 1.1.

In [22] Segre uses the lemma of tangents, which we shall reprove in Section 2, to prove that for $k = 3$ and q even, there is an algebraic curve of degree $t = q + k - 1 - |S|$ which in the dual space contains all the vectors corresponding to tangent hyperplanes. For q odd, he proves that there is an algebraic curve of degree $2t$ which in the dual space contains all the vectors corresponding to tangent hyperplanes, and that the intersection numbers with the hyperplanes, dual to the vectors of S, are 2. This curve extends to an algebraic hypersurface in higher dimensions, as proven in [2].

Let $q = p^h$, where p is a prime.

In Section 6, using the lemmas in the following sections, we shall prove the following theorem.

THEOREM 1.7. *A set S of vectors of the vector space $\mathbb{F}_q^k$, with the property that every subset of S of size k is a basis, has size at most $q + k + 1 - \min(k, p)$, where $k \leq q$.*

Furthermore, in Section 7, we shall prove the following generalisation of Segre's theorem.

THEOREM 1.8. *If $p \geq k$ then a set S of $q + 1$ vectors of the vector space $\mathbb{F}_q^k$, with the property that every subset of S of size k is a basis is equivalent to Example 1.1.*

In Section 8, we shall see that Theorem 1.8 leads to the following slight improvement on Theorem 1.7 in the case $q > k > p$.

THEOREM 1.9. *A set S of vectors of the vector space $\mathbb{F}_q^k$, with the property that every subset of S of size $k \geq 4$ is a basis, where $q > k > p$, has size at most $q + k - p$.*

Finally, we shall prove the following theorem.

THEOREM 1.10. *A set S of vectors of the vector space $\mathbb{F}_q^k$, with the property that every subset of S of size k is a basis, where $3 \leq q - p + 1 \leq k \leq q - 2$, has size at most $q + 1$. Moreover, in the case of equality S is equivalent to Example 1.1.*

2 Segre's Lemma of Tangents

Let S be a set of vectors of $\mathbb{F}_q^k$ with the property that every subset of S of size k is a basis.

In this section we prove a co-ordinate free version of Segre's lemma of tangents [22].

By the proof of Lemma 1.2, for every subset C of S of size $k - 2$, there is a set L_C of

$$t = q + k - 1 - |S|$$

hyperplanes Σ with the property that $\Sigma \cap S = C$.

Let H_C be a set of t linear maps with the property that for each hyperplane $\Sigma \in L_C$, there is a linear map $f \in H_C$ with the property that

$$\Sigma = \{x \in \mathbb{F}_q^k \mid f(x) = 0\}.$$

Let $T_C(u)$, a function from $\mathbb{F}_q^k$ to $\mathbb{F}_q$, called the *tangent function at* C, be defined by

$$T_C(u) = \prod_{f \in H_C} f(u).$$

Note that the tangent function is defined up to scalar factor; it is not important which scalar multiple we use.

LEMMA 2.1. *If* $k = 3$ *and* $x, y, z \in S$ *then*

$$T_{\{x\}}(y)T_{\{y\}}(z)T_{\{z\}}(x) = (-1)^{t+1}T_{\{x\}}(z)T_{\{z\}}(y)T_{\{y\}}(x).$$

Proof. With respect to the basis $\{x, y, z\}$ the tangent function $T_{\{x\}}$ is the evaluation of a polynomial of degree t,

$$\prod(a_{23}X_2 + a_{32}X_3),$$

for some a_{ij}.

For all $d = (d_1, d_2, d_3) \in S \setminus \{x, y, z\}$, the subspace $\langle x, d\rangle$ is defined by the equation $d_3X_2 - d_2X_3 = 0$. The $q - 1$ two-dimensional subspaces containing x, but not containing y or z, are defined by the equations

$$X_2 - \alpha X_3 = 0,$$

where $\alpha \in \mathbb{F}_q \setminus \{0\}$. Since the product of the non-zero elements of $\mathbb{F}_q$ is -1, it follows that

$$\prod \frac{d_2}{d_3} \prod \frac{(-a_{32})}{a_{23}} = -1,$$

where the first product is taken over all $d \in S \setminus \{x, y, z\}$ and the second product is taken over the hyperplanes in $L_{\{x\}}$.

Note that $\prod a_{23} = T_{\{x\}}(y)$ and $\prod a_{32} = T_{\{x\}}(z)$, and so the above implies

$$T_{\{x\}}(z) \prod d_2 = (-1)^{t+1}T_{\{x\}}(y) \prod d_3.$$

Multiplying this equation with the corresponding equations for y and for z gives

$$T_{\{x\}}(z)T_{\{z\}}(y)T_{\{y\}}(x) \prod d_1d_2d_3 = (-1)^{3t+3}T_{\{x\}}(y)T_{\{y\}}(z)T_{\{z\}}(x) \prod d_1d_2d_3$$

and so

$$T_{\{x\}}(y)T_{\{y\}}(z)T_{\{z\}}(x) = (-1)^{t+1}T_{\{x\}}(z)T_{\{z\}}(y)T_{\{y\}}(x).$$

□

This lemma generalises to higher dimensions in the following way.

LEMMA 2.2. *For all $x_1, x_2, x_3, y_1, \ldots, y_{k-3}$ distinct vectors of S*

$$T_{\{x_1\}\cup Y}(x_2)T_{\{x_2\}\cup Y}(x_3)T_{\{x_3\}\cup Y}(x_1) = (-1)^{t+1}T_{\{x_1\}\cup Y}(x_3)T_{\{x_3\}\cup Y}(x_2)T_{\{x_2\}\cup Y}(x_1),$$

where $Y = \{y_1, \ldots, y_{k-3}\}$.

Proof. It suffices to apply Lemma 2.1 in the quotient space $\mathbb{F}_q^k/\langle Y\rangle$. Alternatively, this can be proved in the same way as Lemma 2.1, working with respect to the basis $\{x_1, x_2, x_3, y_1, \ldots, y_{k-3}\}$. □

3 Interpolation of the tangent function

In this section an equation involving the function T_Y is obtained by interpolation.

LEMMA 3.1. *If $|S| \geq k + t > k$ then for any $Y = \{y_1, \ldots, y_{k-2}\}$ and E of size $t + 2$, disjoint subsets of S,*

$$0 = \sum_{a\in E} T_Y(a) \prod_{z\in E\setminus\{a\}} \det(a, z, y_1, \ldots, y_{k-2})^{-1}.$$

Proof. Suppose $E = \{a_1, \ldots, a_{t+2}\}$. With respect to the basis $B = \{a_1, a_2, y_1, \ldots, y_{k-2}\}$, the tangent function T_Y is the evaluation of a homogeneous polynomial in two variables of degree t.

Since $\{a_j, a_\ell, y_1, \ldots, y_{k-2}\}$ is a basis for all $j \neq \ell$, by interpolation at $a_1, a_2, \ldots, a_{t+1}$,

$$T_Y(x) = \sum_{j=1}^{t+1} T_Y(a_j) \prod_{\substack{\ell=1\\ \ell\neq j}}^{t+1} \frac{\det(x, a_\ell, y_1, \ldots, y_{k-2})}{\det(a_j, a_\ell, y_1, \ldots, y_{k-2})},$$

which gives

$$T_Y(a_{t+2}) \prod_{m=1}^{t+1} \det(a_{t+2}, a_m, y_1, \ldots, y_{k-2})^{-1} = -\sum_{j=1}^{t+1} T_Y(a_j) \prod_{\substack{\ell=1\\ \ell\neq j}}^{t+2} \det(a_j, a_\ell, y_1, \ldots, y_{k-2})^{-1}.$$

□

4 Combinations of the interpolation equation

The aim in this section is to combine the equation in Lemma 3.1 for $E' = (E \setminus E_1) \cup Y_1$, and $Y' = (Y \setminus Y_1) \cup E_1$ for various $Y_1 \subseteq Y$ and $E_1 \subseteq E$, to prove the following.

LEMMA 4.1. *If $|S| \geq k+t > k$ then for any $Y = \{y_1, \ldots, y_{k-2}\}$ and E of size $t+2$, disjoint subsets of S and $r \leq \min(k-1, t+2)$,*

$$0 = \sum_{a_1,\ldots,a_r \in E} \left(\prod_{i=1}^{r-1} \frac{T_{\theta_i}(a_i)}{T_{\theta_{i+1}}(y_i)} \right) T_{\theta_r}(a_r) \prod_{z \in (E \cup Y) \setminus (\theta_r \cup \{a_r\})} \det(a_r, z, \theta_r)^{-1},$$

where $\theta_i = (a_1, \ldots, a_{i-1}, y_i, \ldots, y_{k-2})$ is an ordered sequence and the sum is over each ordered sequence $a_1, \ldots, a_r$ of distinct elements of E.

Moreover, the $r!$ terms in the sum for which $\{a_1, \ldots, a_r\} = A$, for some r element subset A of E, are the same.

Proof. We prove the final claim first by showing that transposing a_j and a_{j+1}, $j = 1, \ldots, r-1$, does not affect the expression in the sum. Since all permutations on r letters are generated by transpositions $(1\ 2)$, $(2\ 3)$,..., $(r-1\ r)$, this will suffice.

For $j = 1, \ldots, r-2$, writing $L_r = (E \cup Y) \setminus (\theta_r \cup \{a_r\})$, the expression in the sum is

$$\left(\prod_{i=1}^{j-1} \frac{T_{\theta_i}(a_i)}{T_{\theta_{i+1}}(y_i)} \right) \left(\prod_{i=j+2}^{r} \frac{T_{\theta_i}(a_i)}{T_{\theta_i}(y_{i-1})} \right) \left(\frac{T_{\theta_j}(a_j) T_{\theta_{j+1}}(a_{j+1})}{T_{\theta_{j+1}}(y_j)} \right) \prod_{z \in L_r} \det(a_r, z, \theta_r)^{-1}$$

which is equal to

$$\left(\prod_{i=1}^{j-1} \frac{T_{\theta_i}(a_i)}{T_{\theta_{i+1}}(y_i)} \right) \left(\prod_{i=j+2}^{r} \frac{T_{\theta_i}(a_i)}{T_{\theta_i}(y_{i-1})} \right) \left((-1)^{t+1} \frac{T_{\theta_j}(a_{j+1}) T_{\{a_1,\ldots,a_{j-1},a_{j+1},y_{j+1},\ldots,y_{k-2}\}}(a_j)}{T_{\{a_1,\ldots,a_{j-1},a_{j+1},y_{j+1},\ldots,y_{k-2}\}}(y_j)} \right)$$

$$\times (-1)^{t+1} \prod_{z \in L_r} \det(a_r, z, a_1, \ldots, a_{j-1}, a_{j+1}, a_j, a_{j+2}, \ldots, a_{r-1}, y_r, y_{r+1}, \ldots, y_{k-2})^{-1},$$

by Lemma 2.2, and this is precisely the term in the sum corresponding to the sequence $(a_1, \ldots, a_{j-1}, a_{j+1}, a_j, a_{j+2}, \ldots, a_r)$. For $j = r-1$, exactly the same argument works, the only difference being the position of a_r in the determinants.

Now we prove the main part of the lemma by induction.

For $r = 1$, this is Lemma 3.1.

For $r = 2$, the equation in Lemma 3.1 for $E' = (E \setminus \{b\}) \cup \{y_1\}$ and $Y' = (Y \setminus \{y_1\}) \cup \{b\}$, for some $b \in E$, is

$$0 = T_{\phi_1}(y_1) \prod_{z \in E \setminus \{b\}} \det(y_1, z, \phi_1)^{-1} + \sum_{a_1 \in E \setminus \{b\}} T_{\phi_1}(a_1) \prod_{z \in E' \setminus \{a_1\}} \det(a_1, z, \phi_1)^{-1},$$

where $\phi_1 = (b, y_2, \ldots, y_{k-2})$.

Multiply this equation by

$$\frac{T_Y(b)}{T_{\phi_1}(y_1)}$$

and note that when we sum over $b \in E$ the sum of the first terms, after rearranging the order of the vectors in the determinants, is zero by Lemma 3.1.

Hence

$$0 = \sum_{b\in E} \sum_{a_1\in E\setminus\{b\}} \frac{T_Y(b)}{T_{\phi_1}(y_1)} T_{\phi_1}(a_1) \prod_{z\in(E\setminus\{b,a_1\})\cup\{y_1\}} \det(a_1, z, \phi_1)^{-1}.$$

Letting b play the role of a_1 and replacing a_1 by a_2 we have

$$0 = \sum_{a_1,a_2\in E} \frac{T_{\theta_1}(a_1)}{T_{\theta_2}(y_1)} T_{\theta_2}(a_2) \prod_{z\in(E\setminus\{a_1,a_2\})\cup\{y_1\}} \det(a_2, z, \theta_2)^{-1},$$

which is what we wanted to prove.

Now assume that the equation holds for some r, where $2 \le r \le \min(k-2, t+1)$, and consider this equation for $E' = (E \setminus \{b\}) \cup \{y_r\}$ and $Y' = (Y \setminus \{y_r\}) \cup \{b\}$, for some $b \in E$.

Defining

$$\phi_i = (a_1, \ldots, a_{i-1}, y_i, \ldots, y_{r-1}, b, y_{r+1}, \ldots, y_{k-2})$$

for $i \ge 1$, and

$$\psi_i = (y_r, a_2, \ldots, a_{i-1}, y_i, \ldots, y_{r-1}, b, y_{r+1}, \ldots, y_{k-2})$$

for $i \ge 2$, the equation is

$$0 = \sum_{a_1,\ldots,a_r\in E\setminus\{b\}} \left(\prod_{i=1}^{r-1} \frac{T_{\phi_i}(a_i)}{T_{\phi_{i+1}}(y_i)}\right) T_{\phi_r}(a_r) \prod_{z\in(E\cup Y)\setminus(\phi_r\cup\{a_r\})} \det(a_r, z, \phi_r)^{-1}$$

$$+r \sum_{a_2,\ldots,a_r\in E\setminus\{b\}} \frac{T_{\phi_1}(y_r)}{T_{\psi_2}(y_1)} \left(\prod_{i=2}^{r-1} \frac{T_{\psi_i}(a_i)}{T_{\psi_{i+1}}(y_i)}\right) T_{\psi_r}(a_r) \prod_{z\in(E\cup Y)\setminus(\psi_r\cup\{a_r\})} \det(a_r, z, \psi_r)^{-1},$$

where in the second sum we have combined the terms corresponding to

$$(y_r, a_2, \ldots, a_r), (a_1, y_r, a_3, \ldots, a_r), \ldots, (a_1, \ldots, a_{r-1}, y_r),$$

since they are all equal, as proved in the first part of the proof.

Now multiply this equation by

$$\frac{T_{\theta_1}(b)}{T_{\phi_1}(y_r)},$$

and note that if we sum over $b \in E$ then the second sum, after changing the order of the vectors in the determinants, is the original equation which, by induction, is zero.

Hence

$$0 = \sum_{b\in E} \frac{T_{\theta_1}(b)}{T_{\phi_1}(y_r)} \sum_{a_1,\ldots,a_r\in E\setminus\{b\}} \left(\prod_{i=1}^{r-1} \frac{T_{\phi_i}(a_i)}{T_{\phi_{i+1}}(y_i)}\right) T_{\phi_r}(a_r) \prod_{z\in(E\cup Y)\setminus(\phi_r\cup\{a_r\})} \det(a_r, z, \phi_r)^{-1}.$$

Now let b play the role of a_1, replace $(y_r, y_1, \ldots, y_{r-1})$ by $(y_1, y_2, \ldots, y_r)$ and $(a_1, \ldots, a_r)$ by $(a_2, \ldots, a_{r+1})$.

This gives

$$0 = \sum_{a_1,\ldots,a_{r+1}\in E} \frac{T_{\theta_1}(a_1)}{T_{\theta_2}(y_1)} \left(\prod_{i=1}^{r-1} \frac{T_{\theta_{i+1}}(a_{i+1})}{T_{\theta_{i+2}}(y_{i+1})} \right) T_{\theta_{r+1}}(a_{r+1})$$

$$\times \prod_{z\in(E\cup Y)\setminus(\theta_{r+1}\cup\{a_{r+1}\})} \det(a_{r+1}, z, a_2, \ldots, a_r, a_1, y_{r+1}, \ldots, y_{k-2})^{-1}$$

which, rearranging the order of the vectors in the determinant, implies

$$0 = \sum_{a_1,\ldots,a_{r+1}\in E} \left(\prod_{i=1}^{r} \frac{T_{\theta_i}(a_i)}{T_{\theta_{i+1}}(y_i)} \right) T_{\theta_{r+1}}(a_{r+1}) \prod_{z\in(E\cup Y)\setminus(\theta_{r+1}\cup\{a_{r+1}\})} \det(a_{r+1}, z, \theta_{r+1})^{-1}.$$

□

LEMMA 4.2. *If $|S| \geq k + t > k$ then for any $Y = \{y_1, \ldots, y_{k-2}\}$ and ordered sequence E of length $t + 2$, disjoint subsets of S and $r \leq \min(k - 1, t + 2)$,*

$$0 = r! \sum_{a_1<\ldots<a_r\in E} \left(\prod_{i=1}^{r-1} \frac{T_{\theta_i}(a_i)}{T_{\theta_{i+1}}(y_i)} \right) T_{\theta_r}(a_r) \prod_{z\in(E\cup Y)\setminus(\theta_r\cup\{a_r\})} \det(a_r, z, \theta_r)^{-1}.$$

Proof. This simply combines the two claims in Lemma 4.1. □

We are now in a position to prove Theorem 1.7 for $|S| \geq k + t$. In the next section, we prove Lemma 5.1, which we shall need for the case $|S| \leq k + t - 1$.

5 Construction of S'

In this section, we construct a set S', of $|S|$ vectors of $\mathbb{F}_q^{|S|-k}$, with the property that every subset of S' of size $|S| - k$ is a basis. This we shall need to prove Theorem 1.7 in the case $|S| \leq k + t - 1$.

The following is well-known and is included only for the sake of completeness.

LEMMA 5.1. *Given a set S of vectors of $\mathbb{F}_q^k$ with the property that every subset of S of size k is a basis, we can construct a set S', of $|S|$ vectors of $\mathbb{F}_q^{|S|-k}$, with the property that every subset of S' of size $|S| - k$ is a basis.*

Proof. Let G be a $k \times n$ matrix whose columns are the vectors of S, where $n = |S|$. For any non-zero $y \in \mathbb{F}_q^k$, the row vector y^tG has at most $k - 1$ zero coordinates since no hyperplane contains k vectors of S. Hence y^tG has at least $n-k+1$ non-zero coordinates.

Let H be a $(n-k) \times n$ matrix of rank $n-k$ with the property that $HG^t = 0$. The kernel of H has dimension k and so is $\{G^t y \mid y \in \mathbb{F}_q^k\}$. Hence, all non-zero vectors in the kernel of H have at least $n-k+1$ non-zero coordinates.

Suppose that H has $n-k$ columns that are linearly dependent. Then there is an non-zero $x \in \mathbb{F}_q^n$ with at most $n-k$ non-zero coordinates with the property that $Hx = 0$, a contradiction.

Thus, we can define S' to be the columns of H. □

If S is taken to be Example 1.1 then it is an exercise to show that

$$S' = \{(1, t, t^2, \ldots, t^{q-k}) \mid t \in \mathbb{F}_q\} \cup \{(0, \ldots, 0, 1)\}.$$

6 Proof of Theorem 1.7

Proof. (of Theorem 1.7)

The case $k = 2$ is trivial and so we can assume $k \geq 3$.

By Lemma 5.1 we can construct a subset S' of $\mathbb{F}_q^{k'}$ of size $|S|$, where $k' = |S| - k$, with the property that every subset of S' of size k' is a basis.

If both $|S| \leq k + t$ and $|S'| \leq k' + t'$ then, since $k + k' = |S| = |S'|$, we have $k' \leq t$ and $k \leq t'$, which implies

$$|S| \leq q - 1 + \min(t' - t, t - t') \leq q - 1.$$

If not then, without loss of generality, we can assume $|S| \geq k+t$ and apply Lemma 4.2. Assume that $t \leq k-3$ and consider the equation in Lemma 4.2 with $r = t+2$.

The sum has just one term, and the equation becomes

$$0 = (t+2)! \left(\prod_{i=1}^{t+1} \frac{T_{\theta_i}(a_i)}{T_{\theta_{i+1}}(y_i)} \right) T_{\theta_{t+2}}(a_{t+2}) \prod_{z \in Y \setminus (\theta_{t+2} \cup \{a_{t+2}\})} \det(a_{t+2}, z, \theta_{t+2})^{-1}.$$

With the possible exception of the $(t+2)!$ all the expressions in this product are non-zero. Hence $(t+2)! = 0$, which gives $t \geq p-2$.

Therefore $t \geq \min(k-2, p-2)$ and since $|S| = q + k - 1 - t$ it follows that

$$|S| \leq q + k + 1 - \min(k, p).$$

□

7 Classification of the largest subsets for $k \leq p$

In Theorem 1.7 we proved the bound $|S| \leq q+1$ for $k \leq p$. In this section, we prove that if $|S| = q+1$ and $k \leq p$ then S is equivalent to Example 1.1.

LEMMA 7.1. *If $p \geq k \geq 3$ and $q \geq 2k-2$, then for any ordered basis $E = (e_1, \ldots, e_k) \subset S$, where $|S| = q+1$, and $Y \subseteq S \setminus E$ of size $k-2$,*

$$0 = \sum_{j=1}^{k-1} T_{E\setminus\{e_j,e_k\}}(e_k) T_{E\setminus\{e_j,e_k\}}(e_j)^{-1} \prod_{z\in Y} z_j^{-1} + (-1)^{k-1} \prod_{z\in Y} z_k^{-1},$$

where $z = (z_1, z_2, \ldots, z_k)$ are the coordinates of z with respect to E.

Proof. By Lemma 4.2, with $r = t+1 = k-1$,

$$0 = (k-1)! \sum_{a_1<\ldots<a_{k-1}\in E} \left(\prod_{i=1}^{k-2} \frac{T_{\theta_i}(a_i)}{T_{\theta_{i+1}}(y_i)} \right) T_{\theta_{k-1}}(a_{k-1}) \prod_{z\in(E\cup Y)\setminus(\theta_{k-1}\cup\{a_{k-1}\})} \det(a_{k-1}, z, \theta_{k-1})^{-1}.$$

Let

$$c_j = \left(\prod_{i=1}^{k-2} \frac{T_{\theta_i}(a_i)}{T_{\theta_{i+1}}(y_i)} \right) T_{\theta_{k-1}}(a_{k-1}),$$

where $(a_1, \ldots, a_{k-1}) = E \setminus \{e_j\}$.

The above equation, rearranging the order of the vectors in the determinant, is

$$0 = (k-1)! \sum_{j=1}^{k} c_j \prod_{z\in Y\cup\{e_j\}} \det(E \setminus \{e_j\}, z)^{-1},$$

It is a simple matter to check that

$$c_{k-1} c_k^{-1} = T_{\{e_1,\ldots,e_{k-2}\}}(e_k) T_{\{e_1,\ldots,e_{k-2}\}}(e_{k-1})^{-1}.$$

To calculate $c_j c_k^{-1}$, note that according to Lemma 4.1, we can arrange the sequence $(e_1, \ldots, e_{k-1})$ as $(e_1, \ldots, e_{j-1}, e_{j+1}, \ldots, e_{k-1}, e_j)$, which changes the value of the determinants by $(-1)^{(k-1)(k-1-j)}$, by does not alter the overall expression in the sum corresponding to this sequence. Therefore, replacing $k-1$ by j in the above, gives

$$c_j c_k^{-1} = (-1)^{(k-1)(k-1-j)} T_{E\setminus\{e_j,e_k\}}(e_k) T_{E\setminus\{e_j,e_k\}}(e_j)^{-1}.$$

Let $z = (z_1, \ldots, z_k)$ be the coordinates of z with respect to the basis $E = (e_1, \ldots, e_k)$ and note that

$$\det(E \setminus \{e_j\}, z)^{-1} = (-1)^{k-j} z_j^{-1}.$$

Dividing the equation above through by $(k-1)! c_k$, we have that for $p \geq k$,

$$0 = \sum_{j=1}^{k-1} T_{E\setminus\{e_j,e_k\}}(e_k) T_{E\setminus\{e_j,e_k\}}(e_j)^{-1} (-1)^{k-1} \prod_{z\in Y} z_j^{-1} + \prod_{z\in Y} z_k^{-1}.$$

□

We are now in a position to prove Theorem 1.8.

Proof. (of Theorem 1.8)

The case $k = 2$ is trivial and so we can assume $k \geq 3$.

By Lemma 5.1 and the comment immediately thereafter, we can assume that $q + 1 \geq 2k$.

Suppose that S contains the basis $E = \{e_1, \ldots, e_k\}$. Let U be a subset of $S \setminus E$ of size $k - 2$ and suppose that $x \in S \setminus (U \cup E)$.

For $u_i \in U$, apply Lemma 7.1 with $Y = (U \cup \{x\}) \setminus \{u_i\}$. This gives

$$0 = \sum_{j=1}^{k-1} T_{E\setminus\{e_j,e_k\}}(e_k) T_{E\setminus\{e_j,e_k\}}(e_j)^{-1} (-1)^{k-1} \prod_{z\in U\setminus u_i} z_j^{-1} x_j^{-1} + \prod_{z\in U\setminus u_i} z_k^{-1} x_k^{-1}.$$

Define a $(k-2) \times k$ matrix A whose ij-th entry is

$$\prod_{z\in U\setminus u_i} z_j^{-1}.$$

The matrix obtained from A by multiplying the j-th column of A by $\prod_{z\in U} z_j$ is the matrix whose i-th row is u_i. Since $\{u_1, \ldots, u_{k-2}\}$ is a subset of S these vectors are linearly independent, and so this matrix, and hence the matrix A, has rank $k - 2$. Therefore, the solution to this system of equations has a two dimensional kernel and there is an n and an ℓ such that for all other m

$$x_m^{-1} = \beta_m x_n^{-1} + \epsilon_m x_\ell^{-1},$$

for some β_m and an ϵ_m.

The solutions to this equation for $i = m, n, \ell$ are

$$x_i = \gamma_i (y - \alpha_i)^{-1},$$

for some γ_i and α_i, where $y \in \mathbb{F}_q \setminus \{\alpha_m, \alpha_n, \alpha_\ell\}$, and $x_i = \gamma_i$.

We conclude that, after the change of coordinates in which x_i replaced by $\gamma_i^{-1} x_i$, and replacing the vectors $\lambda_i^{-1} e_i$ by e_i, for $i = 1, \ldots, k$,

$$S = \{e_1, \ldots, e_k\} \cup \{((x-\alpha_1)^{-1}, \ldots, (x-\alpha_k)^{-1}) \mid x \in \mathbb{F}_q \setminus \{\alpha_1, \ldots, \alpha_k\}\} \cup \{(1, 1, \ldots, 1)\}.$$

This implies S is equivalent to the set

$$\{(g(x)(x - \alpha_1)^{-1}, \ldots, g(x)(x - \alpha_k)^{-1}) \mid x \in \mathbb{F}_q \cup \{\infty\}\},$$

where $g(x) = \prod_{i=1}^{k} (x - \alpha_i)$, which is equivalent to Example 1.1, since the polynomials $g(x)/(x - \alpha_i)$ generate the vector space of polynomials of degree at most $k - 1$, as do the monomials in Example 1.1.

□

8 Proofs of Theorem 1.9 and Theorem 1.10

Now, using Theorem 1.8, we can prove Theorem 1.9.

Proof. (of Theorem 1.9) For $k = p + 1$ this follows immediately from Theorem 1.8 and Kaneta-Maruta's theorem [13], which states that if every S of size $q + 1$ in $\mathbb{F}_q^k$, $k < q$, with the property that every subset of S of size k is a basis, is equivalent to Example 1.1, then a set S' of vectors of the vector space $\mathbb{F}_q^{k+1}$, with the property that every subset of S of size $k + 1$ is a basis, has size at most $q + 1$.

For $k \geq p + 2$, let $Y = \{y_1, \ldots, y_{k-p-1}\}$ be distinct elements of S and note that $S' = S/\langle Y \rangle$ is a set of $|S| - k + p + 1$ vectors in $\mathbb{F}_q^{p+1}$ with the property that every subset of S' of size $p + 1$ is a basis. □

Finally, we prove Theorem 1.10.

Proof. (of Theorem 1.10) Suppose that S is a set of $q+2$ vectors of $\mathbb{F}_q^k$, where $q-p+1 \leq k \leq q-2$, with the property that every subset of S of size k is a basis. By Lemma 5.1, we can construct a set S' of vectors of $\mathbb{F}_q^{q+2-k}$ with the property that every subset of size $q + 2 - k$ is a basis. This contradicts Theorem 1.9, since $4 \leq q + 2 - k \leq p + 1$. Hence $|S| \leq q + 1$.

Suppose that S is a set of $q + 1$ vectors of $\mathbb{F}_q^k$, where $q - p + 1 \leq k \leq q - 2$, with the property that every subset of S of size k is a basis. By Lemma 5.1, we can construct a set S' of vectors of $\mathbb{F}_q^{q+1-k}$ with the property that every subset of size $q + 1 - k$ is a basis. By Theorem 1.8, since $3 \leq q + 1 - k \leq p$, S' is equivalent to Example 1.1, which implies, by the comment after Lemma 5.1, that S is equivalent to Example 1.1. □

9 Consequences for maximum distance separable codes

In this section we shall list the consequences of the previous theorems for maximum distance separable codes.

Let U be the k-dimensional subspace of $\mathbb{F}_q^{|S|}$ generated by the rows of the matrix whose columns are the vectors of S and let u be a non-zero vector of U. Since no hyperplane contains k vectors of S, at most $k - 1$ of the coordinates of u are zero.

Define the *weight* of a vector u, with respect to the basis, to be the number of coordinates of u that are non-zero. All the non-zero vectors of the subspace U have weight at least $|S| - k + 1$.

A *linear code* of length n and minimum distance d, is a k-dimensional subspace U of $\mathbb{F}_q^n$, in which every non-zero vector has weight at least d, with respect to a fixed basis.

Thus, we have seen that S gives rise to a linear code of length $|S|$, dimension k and minimum distance $|S| - k + 1$, and vice-versa.

Let U be any linear code of length n, dimension k and minimum distance d. Fix any $n-d+1$ coordinates and consider two vectors x, y of U. If x and y agree on the $n-d+1$ coordinates then $x-y$ has weight $d-1$, which does not occur since $x-y \in U$. Thus, any two vectors of U disagree on any $n-d+1$ coordinates and therefore $|U| \leq q^{n-d+1}$. Since $|U| = q^k$, it follows that $k \leq n-d+1$. This is the *Singleton bound* for linear codes. If $k = n-d+1$ then the code is called *maximum distance separable*.

Thus, we have seen that S gives rise to a maximum distance separable linear code of length $|S|$ and dimension k. By this construction Example 1.1 gives rise to a Reed-Solomon code.

Suppose that $q = p^h$ and that p is prime.

The following corollary is an immediate consequence of Theorem 1.7.

COROLLARY 9.1. *A linear maximum distance separable code of dimension k over $\mathbb{F}_q$ has length at most*

$$q + k + 1 - \min(k, p),$$

where $k \leq q$.

The following is an immediate consequence of Theorem 1.8.

COROLLARY 9.2. *If $p \geq k$ then a linear maximum distance separable code over $\mathbb{F}_q$ of dimension k and length $q+1$ is a Reed-Solomon code.*

The following is an immediate consequence of Theorem 1.9.

COROLLARY 9.3. *If $p < k < q$ then a linear maximum distance separable code of dimension k over $\mathbb{F}_q$ has length at most $q + k - p$.*

The following is an immediate consequence of Theorem 1.10.

COROLLARY 9.4. *If $2 < q-p+1 < k < q-2$ then a linear maximum distance separable code of dimension k over $\mathbb{F}_q$ has length at most $q+1$. Moreover, in the case of equality the code is a Reed-Solomon code.*

REMARK 9.5. One can also consider codes that are not necessarily linear, see [14, Chapter 2]. A recent result from Alderson and Gács [1] states that if a linear code can be extended (i.e. we can extend the code to a subset of $\mathbb{F}_q^{n+1}$ with minimum distance $d+1$) then there is a linear extension of the code. This implies that if the maximum distance separable code can be extended then we can add a vector to the set S, while preserving the property that every subset of size k is a basis.

10 Consequences for projective spaces

An *arc* in the projective space PG$(k-1,q)$ is a set A of points with the property that every k points of A span the whole space. Clearly from S we can construct an arc of size $|S|$ by defining

$$A = \{\langle x\rangle \mid x \in S\},$$

and vice-versa, given an arc A one can construct a set S of vectors of $\mathbb{F}_q^k$ of size $|A|$ with the property that every subset of S of size k is a basis.

Suppose that $q = p^h$ and that p is prime.

The following corollary is an immediate consequence of Theorem 1.7.

COROLLARY 10.1. *An arc in PG$(k-1,q)$ has at most $q+k+1-\min(k,p)$ points, where $k \leq q$.*

The following is an immediate consequence of Theorem 1.8.

COROLLARY 10.2. *If $p \geq k$ then an arc in PG$(k-1,q)$ of size $q+1$ is a normal rational curve.*

The following is an immediate consequence of Theorem 1.9.

COROLLARY 10.3. *If $p < k < q$ then an arc in PG$(k-1,q)$ has at most $q+k-p$ points.*

The following is an immediate consequence of Theorem 1.10.

COROLLARY 10.4. *If $2 < q-p+1 < k < q-2$ then an arc in PG$(k-1,q)$ has at most $q+1$ points. Moreover, in the case of equality, the arc is a normal rational curve.*

11 Consequences for matrices and matroids

Let p be a prime.

Theorem 1.7 has the following immediate corollaries.

COROLLARY 11.1. *For any $k \times (p+2)$ matrix, with $2 \leq k \leq p$ and entries from $\mathbb{F}_p$, there is a set of k columns which are linearly dependent.*

Example 1.1 gives an example of a $k \times (p+1)$ matrix which does not have the above property, and Lemma 1.3 implies that the bound $k \leq p$ is essential.

A *matroid* $M = (E, F)$ is a pair in which E is a set and F is a set of subsets of E, called *independent sets*, such that (1) every subset of an independent set is an independent subset; and (2) for all $A \subseteq E$, all maximal independent subsets of A have the same cardinality, called the *rank* of A and denoted $r(A)$. A *basis* B of M is a maximal independent set.

If E can be mapped to a subset of vectors of a vector space over a field $\mathbb{K}$ so that $I \subseteq E$ is an independent set if and only if the vectors of I are linearly independent, then the matroid is said to be *representable over* $\mathbb{K}$.

The following follows immediately from Theorem 1.7.

COROLLARY 11.2. *If, for a matroid $M = (E, F)$ and prime $p \geq r(E)$, there is a subset $S \subseteq E$ of size $p + 2$, in which every subset of S of size $r(E)$ is a basis, then M is not representable over $\mathbb{F}_p$.*

The maximal independent sets of the *uniform matroid* of rank r are all the r element subsets of the set E. Theorem 1.7 implies the following, which is the prime case of Conjecture 14.1.5 from Oxley [15]. Note that the reverse implication holds since we can map the elements of E to a subset of the columns of the matrix in Example 1.1.

COROLLARY 11.3. *The uniform matroid of rank r, with $|E| \geq r + 2$, is representable over $\mathbb{F}_p$, p prime, if and only if $|E| \leq p + 1$.*

12 Further consequences of the interpolation equation

Lemma 3.1 can be manipulated to give an equation of rational functions ϕ_R, for any subset R of S of size $k + t$, such that for any $x \in S \setminus R$, $\phi_R(x) = 0$.

In earlier versions of this manuscript Theorem 12.1 was used in place of Lemma 3.1. I am indebted to Aart Blokhuis for suggesting the weaker version Lemma 3.1, which is sufficient to prove Theorem 1.7. Theorem 12.1 is more useful in general because the tangent functions do not depend on the tangent functions T_X, for any X containing x.

THEOREM 12.1. *If $|S| \geq k+t+1$ then for any $Y = \{y_1, \ldots, y_{k-3}\}$ and $E = \{a_1, \ldots, a_{t+2}\}$, disjoint subsets of S, and distinct d and $x \in S \setminus \{Y \cup E\}$,*

$$0 = \sum_{j=1}^{t+2} T_{Y\cup\{d\}}(a_j) T_{Y\cup\{a_j\}}(d)^{-1} T_{Y\cup\{a_j\}}(x) \prod_{m\neq j} \det(a_j, a_m, y_1, \ldots, y_{k-3}, x)^{-1}.$$

Proof. By Lemma 3.1, with $y_{k-2} = x$ we have

$$0 = \sum_{j=1}^{t+2} T_{Y\cup\{x\}}(a_j) \prod_{m\neq j} \det(a_j, a_m, y_1, \ldots, y_{k-3}, x)^{-1}.$$

Multiply through by $(-1)^{t+1} T_{Y\cup\{d\}}(x) T_{Y\cup\{x\}}(d)^{-1}$ and apply Lemma 2.2. □

Note that the equation does not depend on the choice of d, since we could multiply by

$$T_{Y\cup\{d\}}(a_1)^{-1} T_{Y\cup\{a_1\}}(d)$$

and apply Lemma 2.2 to eliminate any mention of d.

Acknowledgments. I would like to thank Peter Sziklai and Zsuzsa Weiner, who were there when we proved Lemma 2.1, and were involved in the initial work on possible applications. I would also like to thank Jack Edmonds, for being enthusiastic about Theorem 1.7 and encouraging me to rework and rewrite the proof. Thanks also to my colleagues Eulalia Tramuns for her careful reading of the manuscript and Anna de Mier for drawing my attention to Conjecture 14.1.5 from [15], which led to Corollary 11.3. Above all, I would like to thank Aart Blokhuis and David Glynn for suggestions and comments which led to various improvements.

The author acknowledges the support of the project MTM2008-06620-C03-01 of the Spanish Ministry of Science and Education and the project 2009-SGR-01387 of the Catalan Research Council.

References

[1] T. Alderson and A. Gács, If a linear code has an extension, then it also has a linear extension, *Des. Codes Cryptogr.*, **53** (2009) 59-68.

[2] A. Blokhuis, A. A. Bruen and J. A. Thas, Arcs in $PG(n, q)$, MDS-codes and three fundamental problems of B. Segre - some extensions, *Geom. Dedicata*, **35** (1990) 1–11.

[3] R. C. Bose, Mathematical theory of the symmetrical factorial design, *Sankhyā*, **8** (1947), 107–166.

[4] K. A. Bush, Orthogonal arrays of index unity, *Ann. Math. Statist.*, **23** (1952) 426–434.

[5] W. E. Cherowitzo, α-flocks and hyperovals, *Geom. Dedicata*, **72** (1998) 221–246.

[6] W. E. Cherowitzo, C. M. O'Keefe and T. Penttila, A unified construction of finite geometries in characteristic two, *Adv. Geom.*, **3** (2003) 1–21.

[7] W. E. Cherowitzo, T. Penttila, I. Pinneri and G. F. Royle, Flocks and ovals, *Geom. Dedicata*, **60** (1996) 17–37.

[8] D. G. Glynn, Two new sequences of ovals in finite Desarguesian planes of even order, *Combinatorial Mathematics X* (ed. L. R. A. Casse), Lecture Notes in Mathematics **1036**, Springer, 1983, pp. 217–229.

[9] D. G. Glynn, The non-classical 10-arc of $PG(4, 9)$, *Discrete Math.*, **59** (1986) 43–51.

[10] J. W. P. Hirschfeld, Rational curves on quadrics over finite fields of characteristic two, *Rend. Mat.*, **3** (1971) 772-795.

[11] J. W. P. Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces: update 2001, in *Developments in Mathematics*, **3**, Kluwer Academic Publishers. *Finite Geometries*, Proceedings of the *Fourth Isle of Thorns Conference*, pp. 201–246.

[12] J. W. P. Hirschfeld and J. A. Thas, *General Galois Geometries*, Clarendon Press, Oxford, 1991.

[13] H. Kaneta and T. Maruta, An elementary proof and an extension of Thas' theorem on k-arcs, *Math. Proc. Cambridge Philos. Soc.*, **105** (1989) 459–462.

[14] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[15] J. Oxley, *Matroid Theory*, Oxford University Press, New York, 1992.

[16] S. E. Payne, A new infinite family of generalized quadrangles, *Congr. Numer.*, **49** (1985) 115–128.

[17] B. Segre, Sulle ovali nei piani lineari finiti, *Atti Accad. Naz. Lincei Rend.*, **17** (1954) 1–2.

[18] B. Segre, Ovals in a finite projective plane, *Canad. J. Math.*, **7** (1955) 414-416.

[19] B. Segre, Curve razionali normali e k-archi negli spazi finiti, *Ann. Mat. Pura Appl.*, **39** (1955) 357–379.

[20] B. Segre, Sui k-archi nei piani finiti di caratteristica due, *Rev. Math. Pures Appl.*, **2** (1957) 289–300.

[21] B. Segre, Ovali e curve σ nei piani di Galois di caratteristica due, *Atti dell' Accad. Naz. Lincei Rend.*, **32** (1962) 785–790.

[22] B. Segre, Introduction to Galois geometries, *Atti Accad. Naz. Lincei Mem.*, **8** (1967) 133–236.

[23] J. A. Thas, Normal rational curves and k-arcs in Galois spaces, *Rend. Mat.*, **1** (1968) 331–334.

[24] J. F. Voloch, Arcs in projective planes over prime fields, *J. Geom.*, **38** (1990) 198–200.

[25] J. F. Voloch, Complete arcs in Galois planes of non-square order, in: *Advances in Finite Geometries and Designs*, Oxford University Press, Oxford, 1991, pp. 401–406.