# Classification of 2 and 3 dimensional MDS codes for $4 \leq q \leq 32$

Gerzson Kéri *
Computer and Automation Research Institute
Hungarian Academy of Sciences
H-1111 Budapest Kende u. 13-17, Hungary
e-mail: keri@sztaki.hu

**Abstract**

The number of (a) non-equivalent 2 and 3 dimensional MDS codes, (b) non-equivalent 3 dimensional complete MDS codes, (c) 3 dimensional MDS codes that can be described by classical arcs in $\mathrm{PG}(2,q)$, (d) arcs in regular hyperovals, and (e) $2 \times n$ and $3 \times n$ superregular matrices over $\mathrm{GF}(q)$ are established for $q \leq 19$ and for a number of cases when $23 \leq q \leq 32$. The equivalence classes over both $\mathrm{PGL}(k,q)$ and $\mathrm{P\Gamma L}(k,q)$ are considered during the computations. Though, most of the results are reached by the help of a computer, also some general theoretical relations are formulated. A computational result of the paper is that there is no complete $n$-arc in $\mathrm{PG}(2,31)$ for $23 \leq n \leq 30$ and, consequently, the Main Conjecture for MDS Codes is true for arcs in up to 12 dimensional finite projective spaces of order 31, i.e., for MDS codes of up to 13 dimensions over GF(31).

**Keywords:** MDS code, superregular matrix, complete $n$-arc.

*Supported in part by the Hungarian National Research Fund OTKA, Grant No. T043276.

# Introduction

The aim of the present work is to determine the number of equivalence classes regarding three different equivalence relations and to build databases of $k$ dimensional MDS codes over the finite fields GF($q$) which contain one representant from each equivalence class. In the first phase of the project, we draw the limits for the range of these examinations at $k \leq 3$ and $q \leq 32$. As the databases become very huge when $q$ advances towards 32, the aimed classification is impossible to carry out without using a computer. By performing exhaustive computer search, the problem is solved completely for 2 dimensional MDS codes until $q \leq 32$ and for 3 dimensional MDS codes until $q \leq 19$, it is solved partially for 3-dimensional MDS codes when $23 \leq q \leq 32$.

The question about the number and the structure of complete MDS codes is also examined and entirely solved for 3 dimensional MDS codes when $q = 23$, partially solved when $25 \leq q \leq 31$.

Let $Q^n$ denote the set of all $n$-tuples $(x_1, x_2, \ldots, x_n)$, where $Q = \{0, 1, \ldots, q-1\}$. The elements of the set $Q^n$ are often called words, and the Hamming distance $d(x, y)$ between two words $x, y \in Q^n$ is defined as the number of coordinates in which they differ. $Q^n$ is a metric space with respect to the distance $d(x, y)$.

A *code* of length $n$ over $Q$ is defined as an arbitrary non-empty subset of $Q^n$. The elements of $Q$, which are called symbols, might be any $q$ things, in principle. The set of the given symbols $Q$ is often called alphabet, the integer $q$ is called the size of the alphabet.

The *minimum distance* of a code $C \subseteq Q^n$ is defined as

$$\min\{d(x, y) \mid x, y \in C,\ x \neq y\}.$$

*Linear codes* are codes over finite fields $Q = \mathrm{GF}(q)$ (where $q$ is a prime or prime power) with the properties that

– a codeword multiplied by a scalar is also a codeword,

– the sum (and consequently any linear combination) of two codewords is also a codeword.

A linear code over a finite field GF($q$) of length $n$, dimension $k$ and minimum distance $d$ is called *MDS (maximum distance separable)* if $d = n - k + 1$.

MacWilliams and Sloane in [15] describe the theme of MDS codes as *"one of the most fascinating chapters in all of coding theory"*. One of the many

interesting features of MDS codes is that any MDS code over GF($q$) with parameters $[n, k, d = n - k + 1]$ corresponds to an $n$-arc in the projective space PG($k - 1, q$). Therefore, all results of the paper can be interpreted as contributions to the area of projective geometries over finite fields. The points of the arcs that belong to a given MDS code are the column vectors of a generator matrix of the latter.

An *$n$-arc* in PG($k - 1, q$) is a set of $n(\geq k)$ points with at most $k - 1$ in any hyperplane. An $n$-arc in PG($2, q$) is called *oval* if $n$ has the greatest possible value, i.e. if $N > n$ implies that no $N$-arc exists in the same projective space. As it is known, an oval in PG($2, q$), $q$ odd, is a $(q + 1)$-arc, while an oval in PG($2, q$), $q$ even, is a $(q + 2)$-arc, which is often called also *hyperoval.*

In general, *two codes are regarded to be equivalent if either of them can be obtained by permuting the coordinates of the other, and permuting the symbols in each coordinates.*

As regards linear codes, a usual definition of equivalence is as follows: *Two linear codes are equivalent if either of them can be obtained from the other by permuting the coordinates and multiplying the coordinates of the codewords by non-zero elements of* GF($q$)*, using the same multiplier for the same coordinate.*

Since our algorithm uses the generator matrices of the codes, let us interpret the equivalence of linear codes using generator matrices. Two linear codes are equivalent if their generator matrices can be obtained from each other in a finite number of steps by performing the following operations:

*a) a permutation of the rows,*

*b) a permutation of the columns,*

*c) multiplication of a row by a nonzero element of* GF($q$)*,*

*d) multiplication of a column by a nonzero element of* GF($q$)*,*

*e) adding a multiple of a row to another row.*

As regards linear MDS codes, two other kinds of equivalence are introduced by omitting the last operation from the above listing or by adding one more operation: *Weak equivalence is defined by taking a)-d) for generator matrices of canonical form. Strong equivalence is defined by taking a)-f) where the additional operation is as follows:*

*f) performing a field automorphism to each entry of the generator matrix.*

The equivalence and strong eqivalence of linear MDS codes can also be seen as equivalence of the associated $n$-arcs in $\mathrm{PG}(k-1,q)$. In case of the usual equivalence it means that one of the $n$-arcs can be mapped onto the other by using a collineation in $\mathrm{PGL}(k,q)$. In case of strong equivalence, the collineation can be taken from $\mathrm{P\Gamma L}(k,q)$.

If $C$ is a linear code over $\mathrm{GF}(q)$ then its *dual code* $C^\perp$ is the set of vectors which are orthogonal to all codewords of $C$:

$$C^\perp = \{d \mid c \cdot d = 0 \text{ for all } c \in C\}.$$

If $G = (I_k \mid A)$ is a generator matrix for a linear code $C$ where $A$ is a $k \times (n-k)$ matrix then $G^\perp = \left(-A^T \mid I_{n-k}\right)$ is a generator matrix for $C^\perp$.

As it is known, the dual of an MDS code is also MDS and the duals of equivalent MDS codes are also equivalent.

# 1 The number of non-equivalent 2 and 3 dimensional MDS codes

The computation of the number of non-equivalent 2 and 3 dimensional MDS codes is performed by exhaustive computer search, using the exclusive attribute of MDS codes that all $k \times k$ submatrices of their generator matrices have nonzero determinant, or equivalently, all minors of $A$ in a generator matrix of canonical form are nonzero. A matrix $A$ having this property is called *superregular* [21].

The applied method is based on the ordering of finite field elements, which induces a lexicographic ordering of MDS generator matrices. For a prime $p$, a possibility of ordering in $\mathrm{GF}(p)$ is the natural ordering of non-negative integers less than $p$. In $\mathrm{GF}(7)$, e.g., we have the ordering

$$0 < 1 < 2 < 3 < 4 < 5 < 6.$$

For a prime power $q = p^k, k > 1$, the $k$-tuples of non-negative integers less than $p$ can be ordered according to the natural ordering. In $\mathrm{GF}(9)$, e.g.,

$$0 < 1 < 2 < \alpha < \alpha + 1 < \alpha + 2 < 2\alpha < 2\alpha + 1 < 2\alpha + 2$$

where $\alpha$ is a primitive root for $\mathrm{GF}(9)$.

The ordering can be done, however, according to the powers of a primitive root, too. As 3 is a primitive root for $\mathrm{GF}(7)$, it can be ordered as

$$0 < 1 < 3 < 3^2 (= 2) < 3^3 (= 6) < 3^4 (= 4) < 3^5 (= 5).$$

Similarly, GF(9) can be ordered as

$$0 < 1 < \alpha < \alpha^2 (= 2\alpha + 1) < \alpha^3 (= 2\alpha + 2) < \alpha^4 (= 2) < \alpha^5 < \alpha^6 < \alpha^7.$$

The computer search for the classification with both method of ordering works for arbitrary finite fields GF($q$) where $q$ is a prime power. Actually, we carried out the whole process of classification twice, using the two different alternatives for finite field ordering. The two rounds of these processes constitute also the checking of each other.

When the classification is being performed for $k = 2$, also a database of 2 dimensional MDS codes is created, which is used as input to the classification of 3 dimensional MDS codes. (Similarly, a database of $k$ dimensional MDS codes can be used as input to the classification of $k + 1$ dimensional MDS codes.) The results of the search are summarized in Tables 1–4.

A theoretical approach to the question was published in [9] where some rather complicated formulas and algorithms for the determination of non-equivalent $n$-arcs can be found. As we are interested in finding not only the count numbers, but also the listing of the codes, our methods are mainly of computational nature.

Let $m(k, q)$ denote the maximum number of $n$ for an $n$-arc to exist in PG($k, q$). It is known, e.g. from [11] that

a) $m(1, q) = q + 1$,

b) $m(2, q) = q + 1$ for $q$ odd,

c) $m(2, q) = q + 2$ for $q$ even.

These equalities determine the row size of Tables 1–4. To save space, Table 3 is not shown entirely. The missing rows that would belong to $n > 16$ can be constructed from the given items (cf. Theorem 2), except the last four non-zero items in each column, which are all 1's.

Let $\nu(n, k, q)$ denote the number of non-equivalent linear MDS codes of length $n$ and dimension $k$ up to PGL($k, q$) (simple equivalence). It is the same as $\mathcal{A}(k-1, q, n)$ in the notation applied in [9] which is computed and listed there in the following cases: $k = 2,\ 4 \le n \le 6,\ q \le 31$ and $k = 3,\ n = 6,\ q \le 31$, in the latter case only for primes.

As the duals of equivalent MDS codes are also equivalent, we have the following equality:

**Theorem 1** *$\nu(n, k, q) = \nu(n, n - k, q)$ for $n \ge 4$, $2 \le k \le n - 2$, and any prime or prime power $q$.*

There is another kind of symmetry in the values of $\nu(n,k,q)$, stated in the following assertion.

**Theorem 2** *If $q$ is a prime or prime power and $4 \le n \le q-3$, then*

$$\nu(n,2,q) = \nu(q+1-n,2,q).$$

*In other words: In $\mathrm{PG}(1,q)$, the non-equivalent $n$-arcs and the non-equivalent $(q+1-n)$-arcs are in the same number.*

*Proof.* Clearly, $\nu(n,2,q)$ is also the number of non-equivalent $n$-point sets in the projective line $\mathrm{PG}(1,q)$, and similarly, $\nu(q+1-n,2,q)$ is the number of non-equivalent $(q+1-n)$-point sets. Two $n$-sets $\mathcal{K}_1, \mathcal{K}_2 \in \mathrm{PG}(1,q)$ are equivalent if and only if the complement sets $\mathrm{PG}(1,q) \setminus \mathcal{K}_1, \mathrm{PG}(1,q) \setminus \mathcal{K}_2$ are equivalent. From this observation, the assertion of Theorem 2 immediately follows. □

# 2 The number of non-equivalent 3 dimensional complete MDS codes

An interesting class of $n$-arcs is the class of complete $n$-arcs. The following definition is from [11]. *An $n$-arc in $\mathrm{PG}(k-1,q)$ is complete if it is not contained in an $(n+1)$-arc.*

In harmony with the correspondence between the concepts of MDS codes and $n$-arcs, *we call an MDS code with parameters $[n,k,d=n-k+1]$ complete if it is not a projection of an MDS code with parameters $[n+1,k,d+1=n-k+2]$.*

The number of non-equivalent 3 dimensional complete MDS codes are computed (and arranged into Table 5) either from the set of non-equivalent 3 dimensional MDS codes or – for some parameters – directly from the database of 2 dimensional MDS codes.

For $q \le 19$, the number of non-equivalent 3 dimensional complete MDS codes had been known before, see e.g. [11], so the corresponding columns are not included in Table 5, except for $q = 8$ and 16 when several count numbers can be reduced if also field automorphisms are taken into account. Thus, e.g., the number of complete 6-arcs in $\mathrm{PG}(2,8)$ reduces from 3 to 1 (cf. Theorem 8), the number of complete 9-arcs in $\mathrm{PG}(2,16)$ reduces from 6 to 2.

For $11 \le q \le 32$, the spectrum of the sizes of complete arcs in $\mathrm{PG}(2,q)$ is searched by Chao, Kaneta [2, 3, 4], Faina, Marcugini, Milani and Pambianco

[6, 7, 8, 16, 17, 18, 19]. The summary of the known results that are available about this question are tabulated by Davydov et al. in Table 2 of [5], for larger values of $q$ as well ($25 \leq q \leq 167$); this information is taken into account at some items in the last three columns of Table 5 ($q = 29, 31$ and 32) of the present paper. Our contribution to this question is the following result obtained by exhaustive computer search.

**Theorem 3** *There is no complete $n$-arc in* $\mathrm{PG}(2, q)$ *for the following pairs of $n$ and $q$:*

*a)* 22- *or* 23-*arc in* $\mathrm{PG}(2, 29)$,

*b)* 11-*arc in* $\mathrm{PG}(2, 31)$,

*c)* 23-, 24-, 25-, 26-, 27-, 28-, 29- *or* 30-*arc in* $\mathrm{PG}(2, 31)$,

*d)* 10- *or* 11-*arc in* $\mathrm{PG}(2, 32)$,

*e)* 25- *or* 26-*arc in* $\mathrm{PG}(2, 32)$.

Korchmáros [14] pointed out that assertion (c) of Theorem 3 does not follow from the method of algebraic envelopes of arcs, applied in [11, Chapter 10] and [24].

By the results of Thas [23], Kaneta and Maruta [13] we have the following connection between the length $m'(2, q)$ of the second largest arcs in $\mathrm{PG}(2, q)$ and the length of the largest arcs in $\mathrm{PG}(k, q)$ (cf. Theorem 3.1. of [12] and Theorem 5.3 of [22]):

**Lemma 1**

*a) If $k < 3 + q - m'(2, q)$ then $m(k, q) = q + 1$ and every $(q + 1)$-arc in* $\mathrm{PG}(k, q)$ *is a normal rational curve.*

*b) If every $(q + 1)$-arc in* $\mathrm{PG}(k, q)$ *is a normal rational curve then $m(k + 1, q) = q + 1$.*

As the non-existence of complete $q$-arcs in $\mathrm{PG}(2, q)$ is also known, in general, (see [11]), Theorem 3 implies that $m'(2, 31) = 22$. Now, the application of Lemma 1 for $q = 31$ leads to the following contribution regarding the Main Conjecture for MDS codes.

**Theorem 4** *The longest arc in* $\mathrm{PG}(r, q = 31)$ *has length $q+1 = 32$ if $r \leq 12$ (and any arc of this length is classical if $r < 12$).*

The similar assertion was known only for $r \leq 4$, when $q > 27$ – according to [10], while for $q = 29$, $r \leq 8$ ($r < 8$) follows from the results of Chao and Kaneta in [4].

Our computer search confirms the uniqueness of the second largest complete arc in $\mathrm{PG}(2, 25)$, $\mathrm{PG}(2, 27)$ and $\mathrm{PG}(2, 29)$ that was stated in [4].

# 3 On the number of arcs in ovals and hyperovals

Consider the 3-dimensional generator matrix of the form

$$\begin{pmatrix} 1 & & 1 & 1 & 1 & \dots & 1 & 1 \\ & & 1 & \alpha & \alpha^2 & \dots & \alpha^{q-3} & \alpha^{q-2} \\ & 1 & 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2q-6} & \alpha^{2q-4} \end{pmatrix}.$$

This formula can be extended to specify similar generator matrices in higher dimensions. A generator matrix of this form generates an MDS code (called the extended Reed-Solomon code) and its columns form the points of a *normal rational curve* $\mathcal{C}_{k-1}$. For $q$ odd, any oval in $\mathrm{PG}(2, q)$ is a normal rational curve (Theorem of Segre), and consequently, all ovals are projectively equivalent. For $q$ even, a normal rational curve in $\mathrm{PG}(2, q)$ can be extended to a $(q + 2)$-arc by adding one more point, the nucleus, to it (i.e. by adding another unit vector to the generator matrix of the corresponding MDS code). A $(q + 2)$-arc like this is called a regular hyperoval in $\mathrm{PG}(2, q)$, $q$ even. In both cases, $\alpha$ is a primitive root in $\mathrm{GF}(q)$.

Let $\nu(n, k, q)$ denote the number of non-equivalent linear MDS codes of length $n$ and dimension $k$, i.e. the number of non-equivalent $n$-arcs in $\mathrm{PG}(k - 1, q)$, $\nu'(n, k, q)$ denote the number of non-equivalent $n$-arcs in a normal rational curve of $\mathrm{PG}(k-1, q)$, and $\nu''(n, 3, q)$ denote the number of non-equivalent $n$-arcs in a regular hyperoval of $\mathrm{PG}(2, q)$, $q$ even. (The $n$-arcs that are contained in a normal rational curve are called classical.)

**Theorem 5**

$$\nu'(n, r, q) = \nu(n, 2, q) \tag{1}$$

*for any $q$ prime or prime power, $3 \leq r \leq q - 1$ and $k + 2 \leq n \leq q + 1$. In other words: The non-equivalent $n$-arcs in $\mathrm{PG}(1, q)$ and the non-equivalent classical $n$-arcs in $\mathrm{PG}(r - 1, q)$ are in the same number.*

$$\nu''(5, 3, q) = \nu(5, 2, q) \tag{2}$$

*for any* $q = 2^t, t \geq 2$. *In other words: The non-equivalent* 5*-arcs in* $\mathrm{PG}(1, q)$ *and the non-equivalent* 5*-arcs contained in a regular hyperoval in* $\mathrm{PG}(2, q)$ *are in the same number.*

$$\nu''(n, 3, q) = \nu(n, 2, q) + \nu(n - 1, 2, q) \tag{3}$$

*for any* $q = 2^t, t \geq 3$, *and* $6 \leq n \leq q + 1$. *In other words: For any* $n \geq 6$, *the non-equivalent* $n$*-arcs in a regular hyperoval in* $\mathrm{PG}(2, q)$ *is equal to the number of all non-equivalent* $(n-1)$*-arcs and* $n$*-arcs in* $\mathrm{PG}(1, q)$.

The proof of (1) and (2) follows from the geometric fact, that the subgroup of $\mathrm{PGL}(k, q)$ that leaves the normal rational curve $\mathcal{C}_{k-1}$ invariant is the same as $\mathrm{PGL}(2, q)$, and any $n$-set of the normal rational curve is an $n$-arc in $\mathrm{PG}(k - 1, q)$. To prove (3) we have to distinguish two cases: the nucleus can belong to the $n$-set or not.

# 4 The number of matrices with nonzero minors

It is known that a linear code with generator matrix $(I \mid A)$ is MDS if and only if every minor of $A$ is non-zero in $\mathrm{GF}(q)$. This fact suggests studying the matrices with this property, i.e. $k \times (n - k)$ matrices $A$ with entries in $\mathrm{GF}(q)$, all minors of which being non-zero. Two matrices $A$ and $B$ of this type, i.e. *superregular matrices* (see their definition below) are considered to be equivalent if either one can be obtained from the other by multiplying the rows and columns by non-zero elements of $\mathrm{GF}(q)$ and after (or before) the multiplication, permuting the rows and columns.

*A rectangular matrix* $A$ *is called superregular if every submatrix of* $A$ *is non-singular.*

The equivalence of matrices of this type defines the kind of equivalence relation for MDS codes that we called weak equivalence in the introductory part of the paper.

The number of non-equivalent 2 and 3 dimensional MDS codes in the sense of weak equivalence, i.e. the number of non-equivalent superregular matrices can be performed by nearly the same method that was outlined in Section 1 for simple equivalence. There are, however, two essential differences:

1. The exhaustive computer search is 3–5 times faster than before.

2. The number of weakly non-equivalent MDS codes are much higher as it can be seen by comparing the pairing tables (e.g. Table 7 with Table 2 or Table 8 with Table 3).

This means that for these computations, the bottleneck capacity is not only CPU time, but also disk space, when $q$ and $n$ are increasing. Tables 6–9 are analogous to the previous Tables 1–4 for weak equivalence.

Let $\overline{\nu}(n,k,q)$ denote the number of weakly non-equivalent linear MDS codes of length $n$ and dimension $k$. Then, analogously to Theorem 1, we have the following equality:

**Theorem 6** *$\overline{\nu}(n,k,q) = \overline{\nu}(n,n-k,q)$ for $n \geq 4$, $2 \leq k \leq n-2$, and any prime or prime power $q$.*

A columnwise symmetry appears again in Tables 6 and 8, but its centre of gravity moved below to the next place in each column, in comparison to Tables 1 and 3.

By the similar reason as for Table 3 before, also Table 8 is finished in the middle. The missing rows can be constructed from the given items by applying the following Theorem 7. In this case, however, the last two non-zero items are 1's in each column.

**Theorem 7** *For any prime or prime power $q$ and for $4 \leq n \leq q-1$,*

$$\overline{\nu}(n,2,q) = \overline{\nu}(q+3-n,2,q).$$

*Proof.* Let $(S_1,S_2)$ and $(S_1',S_2')$ be two disjoint partitions of the set $\mathrm{GF}(q) \setminus \{0\}$ into subsets of cardinalities $n-2$ and $(q-1)-(n-2)$, respectively:

$$S_1 = \{a_1,a_2,\ldots,a_{n-2}\}, \quad S_2 = \{b_1,b_2,\ldots,b_{(q-1)-(n-2)}\},$$

$$S_1' = \{a_1',a_2',\ldots,a_{n-2}'\}, \quad S_2' = \{b_1',b_2',\ldots,b_{(q-1)-(n-2)}'\},$$

$$S_1 \cap S_2 = S_1' \cap S_2' = \emptyset,$$

$$S_1 \cup S_2 = S_1' \cup S_2' = \mathrm{GF}(q) \setminus \{0\}.$$

Now, the proof can be completed by the reasoning that if the superregular matrices

$$A = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_{n-2} \end{pmatrix} \text{ and } A' = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ a_1' & a_2' & \ldots & a_{n-2}' \end{pmatrix}$$

are equivalent, then also

$$B = \begin{pmatrix} 1 & 1 & \dots & 1 \\ b_1 & b_2 & \dots & b_{(q-1)-(n-2)} \end{pmatrix} \text{ and } B' = \begin{pmatrix} 1 & 1 & \dots & 1 \\ b'_1 & b'_2 & \dots & b'_{(q-1)-(n-2)} \end{pmatrix}$$

are equivalent. □

We note that the following chain of relations holds, in general, for $\underline{\nu}$, $\nu$ and $\overline{\nu}$ where $q = p^h \quad (h \geq 1)$ and $\underline{\nu}$ denotes the number of strongly non-equivalent linear MDS codes of length $n$ and dimension $k$.

$$\frac{1}{h} \cdot \nu(n,k,q) \leq \underline{\nu}(n,k,q) \leq \nu(n,k,q) \leq \overline{\nu}(n,k,q).$$

Finally, it is also worth mentioning that the statements which are analogous to Theorems 1, 2 and 5 are valid also for strong equivalence, i.e. when $\nu$, $\nu'$ and $\nu''$ are replaced by the corresponding underlined variables.

# 5 Examples

The classification of MDS codes, among other results, helps proving the uniqueness of certain types of MDS codes and complete MDS codes. The following four examples, contained in Theorems 8 and 9 are for illustration of this fact.

**Theorem 8** *The complete MDS code with parameters $q = 8, k = 3, n = 6$ is unique. (In other words: The complete 6-arc in $\mathrm{PG}(2,8)$ is unique.)*

*Proof.* There are 3 non-equivalent complete MDS codes with the given parameters. Their generator matrices are

$$\begin{pmatrix} 1 & & & 1 & 1 & 1 \\ & 1 & & 1 & \alpha & \alpha^3 \\ & & 1 & 1 & \alpha^3 & \alpha \end{pmatrix}, \quad \begin{pmatrix} 1 & & & 1 & 1 & 1 \\ & 1 & & 1 & \alpha^2 & \alpha^6 \\ & & 1 & 1 & \alpha^6 & \alpha^2 \end{pmatrix}, \quad \begin{pmatrix} 1 & & & 1 & 1 & 1 \\ & 1 & & 1 & \alpha^4 & \alpha^5 \\ & & 1 & 1 & \alpha^5 & \alpha^4 \end{pmatrix}.$$

These 3 codes are strongly equivalent, because appropriate automorphisms of GF(8) brings their generator matrices (and consequently, the codes itself) into each other. □

The unique 6-arc in PG$(2, 8)$ (deduced from the first form of the generator matrix) consists of the points

$$(1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 1), (1, \alpha, \alpha^3), (1, \alpha^3, \alpha).$$

It is known that the four longest arcs in PG(1,32) is unique. By performing the classification for strong equivalence, we can extend this result to the five longest arcs.

**Theorem 9** *The MDS codes with parameters $q = 32, k = 2, n = 4$ or $n = 29$ are unique. (In other words: The 4-arc and the 29-arc in* PG$(1, 32)$ *are unique.) Consequently, the dual code of the latter, the MDS code with parameters $q = 32, k = 27, n = 29$ is also unique. (In other words: The 29-arc in* PG$(26, 32)$ *is unique.)*

The proof is similar to that of Theorem 8. For each part of this theorem, the 5 non-equivalent codes (as regards simple equivalence) become all equivalent (as regards strong equivalence). Generator matrices of codes of length 4 like this are

$$\begin{pmatrix} 1 & & 1 & 1 \\ & 1 & 1 & \alpha^k \end{pmatrix}, \quad k = 1, 2, 4, 8, 16.$$

As a last example, we give a short remark to the hyperovals in PG$(2, 32)$. It is proved [20] that there are precisely 6 isomorphism classes of the hyperovals in this plane, which are listed as

- the regular hyperoval,
- the irregular translation hyperoval,
- the Segre hyperoval,
- the Payne hyperoval,
- the Cherowitzo hyperoval,
- the O'Keefe–Penttila hyperoval.

It can be shown that performing field automorphisms to each of these hyperovals, with the exception of the last one, keeps them in the initial equivalence class, for simple equivalence of linear codes. As regards the last case, the 5 field automorphisms map this hyperoval into 5 non-equivalent hyperovals according to the simple equivalence of linear codes. Naturally, these non-equivalent variants of the O'Keefe–Penttila hyperoval are all strongly equivalent.

# 6 Tables

The results of the accomplished classification of 2 and 3 dimensional MDS codes are summarized in the Tables given in this section. Where the count numbers determined for simple (i.e. PGL) equivalence differ from the ones given for strong (i.e. PΓL) equivalence, the latter ones are included in parentheses in Tables 1–5. According to Theorem 5, the items of Tables 1 and 3 present also the number of non-equivalent (strongly non-equivalent) classical $n$-arcs in $\mathrm{PG}(r-1,q)$ where $r+2 \leq n \leq q+1$.

In Table 5, '.' is standing for an unknown (positive or zero) value, '.P.' for an unknown positive value, '.M.' and '.MM.' for not exactly determined large values (greater than a million), where '.MM.' is the maximum for a given $q$.

Consider now the items of Tables 2 and 4 that belong to even $q \geq 8$ and $n = q+1$ showing that the number of non-equivalent $(q+1)$-arcs is 2, 3, 35 when $q = 8$, 16, 32. According to Theorem 5, two of these $(q+1)$-arcs are contained in the regular hyperoval. Thus, exactly one 17-arc is contained in the non-regular hyperoval of PG(2,16) and just *thirty-three* 33-*arcs* are contained in the five non-regular hyperovals in PG(2,32).

From Tables 3 and 8 the omitted lines for $n > 16\,(17)$ can be reconstructed according to the notes taken in the appropriate sections, mainly by using Theorems 2 and 7. As regards Tables 4 and 9, the missing items are not yet determined because they would require far too much CPU time.

As regards the number of non-equivalent superregular matrices (Tables 6–9), we make only one comment to the case when $q = 16$. From the 30 non-equivalent superregular $3 \times 15$ matrices only 2 can be derived from the doubly extended Reed-Solomon code (so they belong to the regular hyperoval), while the other 28 matrices belong to the alternative MDS code having the same parameters (i.e. to the non-regular hyperoval).

We should like to mention, finally, that the number of non-equivalent superregular matrices is surprisingly huge for $n = q+1$ and $n = q+2$ when $q = 32$. (See in Table 9.) This fact suggests that the computational approach for the classification of MDS codes is extremely difficult for $q = 32$ and seems to be unrealizable for any greater $q$ in the even case.

| $n\backslash q$ | 3 | 4 | 5 | 7 | 8 | 9 | 11 | 13 | 16 | 17 | 19 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 1 | 1 | 1 | 2 | 1 | 2 | 2 | 3 | 3(2) | 3 | 4 |
| 5 | - | 1 | 1 | 1 | 1 | 2 | 2 | 3 | 4(3) | 4 | 5 |
| 6 | - | - | 1 | 1 | 1 | 2 | 4 | 5 | 8(4) | 10 | 13 |
| 7 | - | - | - | 1 | 1 | 1 | 2 | 5 | 10(5) | 10 | 18 |
| 8 | - | - | - | 1 | 1 | 1 | 2 | 5 | 11(6) | 17 | 31 |
| 9 | - | - | - | - | 1 | 1 | 1 | 3 | 11(6) | 17 | 33 |
| 10 | - | - | - | - | - | 1 | 1 | 3 | 10(5) | 17 | 44 |
| 11 | - | - | - | - | - | - | 1 | 1 | 8(4) | 10 | 33 |
| 12 | - | - | - | - | - | - | 1 | 1 | 4(3) | 10 | 31 |
| 13 | - | - | - | - | - | - | - | 1 | 3(2) | 4 | 18 |
| 14 | - | - | - | - | - | - | - | 1 | 1 | 3 | 13 |
| 15 | - | - | - | - | - | - | - | - | 1 | 1 | 5 |
| 16 | - | - | - | - | - | - | - | - | 1 | 1 | 4 |
| 17 | - | - | - | - | - | - | - | - | 1 | 1 | 1 |
| 18 | - | - | - | - | - | - | - | - | - | 1 | 1 |
| 19 | - | - | - | - | - | - | - | - | - | - | 1 |
| 20 | - | - | - | - | - | - | - | - | - | - | 1 |

Table 1. The number of non-equivalent (strongly non-equivalent) linear 2-dimensional MDS codes (the number of $n$-sets in $\mathrm{PG}(1,q)$) for $3 \le q \le 19$

| $n\backslash q$ | 4 | 5 | 7 | 8 | 9 | 11 | 13 | 16 | 17 | 19 |
|---|---|---|---|---|---|---|---|---|---|---|
| 5 | 1 | 1 | 1 | 1 | 2 | 2 | 3 | 4(3) | 4 | 5 |
| 6 | 1 | 1 | 3 | 5(3) | 7(6) | 15 | 26 | 61(22) | 74 | 117 |
| 7 | - | - | 1 | 2 | 4(3) | 21 | 80 | 454(125) | 733 | 1768 |
| 8 | - | - | 1 | 2 | 2 | 21 | 181 | 2633(685) | 5441 | 20361 |
| 9 | - | - | - | 2 | 1 | 5 | 110 | 6014(1534) | 17633 | 115492 |
| 10 | - | - | - | 1 | 1 | 2 | 27 | 4899(1262) | 21064 | 280104 |
| 11 | - | - | - | - | - | 1 | 2 | 1171(300) | 6814 | 235320 |
| 12 | - | - | - | - | - | 1 | 2 | 587(159) | 629 | 55708 |
| 13 | - | - | - | - | - | - | 1 | 260(70) | 15 | 2733 |
| 14 | - | - | - | - | - | - | 1 | 100(30) | 4 | 83 |
| 15 | - | - | - | - | - | - | - | 30(9) | 1 | 5 |
| 16 | - | - | - | - | - | - | - | 9(5) | 1 | 4 |
| 17 | - | - | - | - | - | - | - | 3 | 1 | 1 |
| 18 | - | - | - | - | - | - | - | 2 | 1 | 1 |
| 19 | - | - | - | - | - | - | - | - | - | 1 |
| 20 | - | - | - | - | - | - | - | - | - | 1 |

Table 2. The number of non-equivalent (strongly non-equivalent) linear 3-dimensional MDS codes (the number of $n$-arcs in $\mathrm{PG}(2,q)$) for $4 \le q \le 19$

| $n\backslash q$ | 23 | 25 | 27 | 29 | 31 | 32 |
|---|---|---|---|---|---|---|
| 4 | 4 | 5(4) | 5(3) | 5 | 6 | 5(1) |
| 5 | 6 | 8(7) | 8(4) | 10 | 11 | 11(3) |
| 6 | 22 | 28(19) | 34(14) | 42 | 51 | 53(13) |
| 7 | 36 | 54(34) | 73(29) | 97 | 132 | 148(32) |
| 8 | 83 | 131(79) | 196(72) | 289 | 415 | 481(97) |
| 9 | 125 | 225(132) | 382(134) | 629 | 992 | 1240(248) |
| 10 | 196 | 398(223) | 745(257) | 1339 | 2318 | 2964(596) |
| 11 | 227 | 531(293) | 1142(390) | 2314 | 4442 | 6049(1217) |
| 12 | 268 | 692(379) | 1665(565) | 3732 | 7856 | 11099(2227) |
| 13 | 227 | 714(391) | 1976(670) | 5026 | 11854 | 17759(3555) |
| 14 | 196 | 692(379) | 2170(738) | 6194 | 16218 | 25370(5074) |
| 15 | 125 | 531(293) | 1976(670) | 6502 | 19234 | 32054(6414) |
| 16 | 83 | 398(223) | 1665(565) | 6194 | 20636 | 36045(7217) |
| . | . | . | . | . | . | . |

Table 3. The number of non-equivalent (strongly non-equivalent) linear 2-dimensional MDS codes (the number of $n$-sets in $\mathrm{PG}(1, q)$) for $23 \leq q \leq 32$

| $n\backslash q$ | 23 | 25 | 27 | 29 | 31 | 32 |
|---|---|---|---|---|---|---|
| 5 | 6 | 8(7) | 8(4) | 10 | 11 | 11(3) |
| 6 | 257 | 365(205) | 504(174) | 682 | 905 | 1037(213) |
| 7 | 7613 | 14114(7163) | 24725(8261) | 41301 | 66272 | 82881(16593) |
| 8 | 172416 | 419385 (210299) | 933733 (311313) | 1933469 | 3768298 | 5158638 (1031750) |
| 9 | 2235523 | 7490938 (3747561) | . | . | . | . |
| . | . | . | . | . | . | . |
| $q-8$ | 64773 | 1493(789) | 515(183) | 646 | 992 | . |
| $q-7$ | 692 | 222(135) | 218(82) | 293 | 415 | . |
| $q-6$ | 41 | 58(38) | 76(32) | 98 | 132 | . |
| $q-5$ | 22 | 29(20) | 35(15) | 43 | 51 | . |
| $q-4$ | 6 | 9(8) | 8(4) | 10 | 11 | . |
| $q-3$ | 4 | 5(4) | 5(3) | 5 | 6 | . |
| $q-2$ | 1 | 1 | 1 | 1 | 1 | . |
| $q-1$ | 1 | 1 | 1 | 1 | 1 | . |
| $q$ | 1 | 1 | 1 | 1 | 1 | 1798(374) |
| $q+1$ | 1 | 1 | 1 | 1 | 1 | 119(35) |
| $q+2$ | - | - | - | - | - | 10(6) |

Table 4. The number of non-equivalent (strongly non-equivalent) linear 3-dimensional MDS codes (the number of $n$-arcs in $\mathrm{PG}(2, q)$) for $23 \leq q \leq 32$

| $n\backslash q$ | 8 | 16 | 23 | 25 | 27 | 29 | 31 | 32 |
|---|---|---|---|---|---|---|---|---|
| 6 | 3(1) | - | - | - | - | - | - | - |
| 7 | - | - | - | - | - | - | - | - |
| 8 | - | - | - | - | - | - | - | - |
| 9 | - | 6(2) | - | - | - | - | - | - |
| 10 | 1 | 1944(501) | 1 | - | - | - | - | - |
| 11 | - | 113(30) | - | - | - | - | - | - |
| 12 | - | 32(9) | 112449 | 1156(606) | 21(7) | - | . | . |
| 13 | - | 1 | 4341514 | .M. | .P. | .P. | . | . |
| 14 | - | - | 1828196 | .MM. | .M. | .P. | .P. | .P. |
| 15 | - | - | 58361 | .M. | .MM | .P. | .P. | .P. |
| 16 | - | - | 564 | 246446(124577) | .M. | .P. | .P. | .P. |
| 17 | - | - | 5 | 843(434) | .P. | .P. | .P. | .P. |
| 18 | - | 2 | - | 65(41) | .P. | .P. | .P. | .P. |
| 19 | - | - | - | - | 13(5) | .P. | .P. | .P. |
| 20 | - | - | - | - | - | .P. | .P. | .P. |
| 21 | - | - | - | 1 | - | 2 | .P. | .P. |
| 22 | - | - | - | - | 1 | - | 11 | .P. |
| 23 | - | - | - | - | - | - | - | .P. |
| 24 | - | - | 1 | - | - | 1 | - | 95(19) |
| 25 | - | - | - | - | - | - | - | - |
| 26 | - | - | - | 1 | - | - | - | - |
| 27 | - | - | - | - | - | - | - | - |
| 28 | - | - | - | - | 1 | - | - | - |
| 29 | - | - | - | - | - | - | - | - |
| 30 | - | - | - | - | - | 1 | - | - |
| 31 | - | - | - | - | - | - | - | - |
| 32 | - | - | - | - | - | - | 1 | - |
| 33 | - | - | - | - | - | - | - | - |
| 34 | - | - | - | - | - | - | - | 10(6) |

Table 5. The number of non-equivalent (strongly non-equivalent) complete linear 3-dimensional MDS codes (the number of complete $n$-arcs in $\mathrm{PG}(3, q)$) for $q = 8, 16$ and $23 \leq q \leq 32$

| $n\backslash q$ | 3 | 4 | 5 | 7 | 8 | 9 | 11 | 13 | 16 | 17 | 19 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 1 | 1 | 2 | 3 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 5 | - | 1 | 1 | 3 | 4 | 5 | 8 | 12 | 19 | 21 | 27 |
| 6 | - | - | 1 | 3 | 4 | 8 | 16 | 29 | 56 | 72 | 104 |
| 7 | - | - | - | 1 | 3 | 5 | 16 | 38 | 111 | 147 | 252 |
| 8 | - | - | - | 1 | 1 | 4 | 16 | 50 | 185 | 280 | 561 |
| 9 | - | - | - | - | 1 | 1 | 8 | 38 | 232 | 375 | 912 |
| 10 | - | - | - | - | - | 1 | 5 | 29 | 232 | 440 | 1282 |
| 11 | - | - | - | - | - | - | 1 | 12 | 185 | 375 | 1387 |
| 12 | - | - | - | - | - | - | 1 | 6 | 111 | 280 | 1282 |
| 13 | - | - | - | - | - | - | - | 1 | 56 | 147 | 912 |
| 14 | - | - | - | - | - | - | - | 1 | 19 | 72 | 561 |
| 15 | - | - | - | - | - | - | - | - | 7 | 21 | 252 |
| 16 | - | - | - | - | - | - | - | - | 1 | 8 | 104 |
| 17 | - | - | - | - | - | - | - | - | 1 | 1 | 27 |
| 18 | - | - | - | - | - | - | - | - | - | 1 | 9 |
| 19 | - | - | - | - | - | - | - | - | - | - | 1 |
| 20 | - | - | - | - | - | - | - | - | - | - | 1 |

Table 6. The number of non-equivalent superregular $2 \times (n-2)$ matrices for $3 \leq q \leq 19$

| $n\backslash q$ | 4 | 5 | 7 | 8 | 9 | 11 | 13 | 16 | 17 | 19 |
|---|---|---|---|---|---|---|---|---|---|---|
| 5 | 1 | 1 | 3 | 4 | 5 | 8 | 12 | 19 | 21 | 27 |
| 6 | 1 | 1 | 9 | 21 | 36 | 107 | 257 | 737 | 983 | 1683 |
| 7 | - | - | 2 | 12 | 49 | 446 | 2290 | 14530 | 24137 | 59586 |
| 8 | - | - | 1 | 8 | 15 | 585 | 8024 | 137277 | 293606 | 1118523 |
| 9 | - | - | - | 3 | 2 | 125 | 7144 | 487980 | 1457246 | 9644076 |
| 10 | - | - | - | 2 | 1 | 13 | 1258 | 536580 | 2458911 | 33376322 |
| 11 | - | - | - | - | - | 2 | 62 | 178909 | 1097510 | 38665103 |
| 12 | - | - | - | - | - | 1 | 19 | 116574 | 108343 | 11976301 |
| 13 | - | - | - | - | - | - | 3 | 68788 | 2109 | 746106 |
| 14 | - | - | - | - | - | - | 1 | 31322 | 288 | 13958 |
| 15 | - | - | - | - | - | - | - | 10448 | 81 | 1047 |
| 16 | - | - | - | - | - | - | - | 2437 | 21 | 414 |
| 17 | - | - | - | - | - | - | - | 349 | 3 | 119 |
| 18 | - | - | - | - | - | - | - | 30 | 1 | 27 |
| 19 | - | - | - | - | - | - | - | - | - | 4 |
| 20 | - | - | - | - | - | - | - | - | - | 1 |

Table 7. The number of non-equivalent superregular $3 \times (n-3)$ matrices for $4 \leq q \leq 19$

| $n\backslash q$ | 23 | 25 | 27 | 29 | 31 | 32 |
|---|---|---|---|---|---|---|
| 4 | 11 | 12 | 13 | 14 | 15 | 15 |
| 5 | 40 | 48 | 56 | 65 | 75 | 80 |
| 6 | 195 | 256 | 328 | 413 | 511 | 560 |
| 7 | 621 | 913 | 1298 | 1794 | 2421 | 2793 |
| 8 | 1782 | 2920 | 4576 | 6916 | 10133 | 12103 |
| 9 | 3936 | 7293 | 12760 | 21287 | 34112 | 42640 |
| 10 | 7440 | 15581 | 30415 | 56021 | 98254 | 127920 |
| 11 | 11410 | 27407 | 60335 | 123695 | 238957 | 325845 |
| 12 | 14938 | 41272 | 102817 | 235378 | 502303 | 716859 |
| 13 | 16159 | 52234 | 148976 | 384111 | 911456 | 1367184 |
| 14 | 14938 | 56822 | 186616 | 544802 | 1444147 | 2278640 |
| 15 | 11410 | 52234 | 200474 | 669468 | 1997499 | 3329165 |
| 16 | 7440 | 41272 | 186616 | 718146 | 2427036 | 4280355 |
| 17 | 3936 | 27407 | 148976 | 669468 | 2587018 | 4850640 |
| . | . | . | . | . | . | . |

Table 8. The number of non-equivalent superregular $2 \times (n-2)$ matrices for $23 \leq q \leq 32$

| $n\backslash q$ | 23 | 25 | 27 | 29 | 31 | 32 |
|---|---|---|---|---|---|---|
| 5 | 40 | 48 | 56 | 65 | 75 | 80 |
| 6 | 4141 | 6087 | 8652 | 11957 | 16133 | 18605 |
| 7 | 261738 | 487691 | 857044 | 1434842 | 2306134 | 2884900 |
| 8 | 9594801 | 23391022 | 52150380 | 108075860 | 210747351 | 288524138 |
| 9 | 187548579 | 628815516 | . | . | . | . |
| . | . | . | . | . | . | . |
| $q-6$ | 21160 | . | . | . | . | . |
| $q-5$ | 9111 | . | . | . | . | . |
| $q-4$ | 3414 | . | 8888 | 13494 | . | . |
| $q-3$ | 1020 | 1508 | 2144 | 2964 | 4010 | . |
| $q-2$ | 229 | 303 | 392 | 497 | 619 | . |
| $q-1$ | 40 | 48 | 56 | 65 | 75 | . |
| $q$ | 4 | 5 | 5 | 5 | 6 | . |
| $q+1$ | 1 | 1 | 1 | 1 | 1 | 589679 |
| $q+2$ | - | - | - | - | - | 19084 |

Table 9. The number of non-equivalent superregular $3 \times (n-3)$ matrices for $23 \leq q \leq 32$

# Acknowledgment

The author wishes to thank to Tamás Szőnyi for discussions and for his useful advices, also to Patrick Govaerts for his valuable remarks on the paper.


# References


[1] A. H. Ali, J. W. P. Hirschfeld and H. Kaneta, On the size of arcs in projective spaces, IEEE Trans. Inform. Theory, 41 (1995), 1649–1656.

[2] J. M. Chao and H. Kaneta, A complete 24-arc in PG(2,29) with the automorphism group PSL(2,7), Rend. Math. Appl. (7), 16 (1996), 537–544.

[3] J. M. Chao and H. Kaneta, Classical arcs in PG$(r, q)$ for $11 \leq q \leq 19$, Discrete. Math., 174 (1997), 87–94.

[4] J. M. Chao and H. Kaneta, Classical arcs in PG$(r, q)$ for $23 \leq q \leq 29$, Discrete. Math., 226 (2001), 377–385.

[5] A. A. Davydov, G. Faina, S. Marcugini and F. Pambianco, Computer search in projective planes for the sizes of complete arcs, J. Geom., to appear.

[6] G. Faina, S. Marcugini, A. Milani and F. Pambianco, The spectrum of the values $k$ for which there exists a complete $k$-arc in PG$(2, q)$ for $q \leq 23$, Ars Combin., 47 (1997) 3–11.

[7] G. Faina and F. Pambianco, On the spectrum of the values $k$ for which a complete $k$-cap in PG$(n, q)$ exists, J. Geom., 62 (1998) 84–98.

[8] G. Faina and F. Pambianco, On some 10-arcs for deriving the minimum order for complete arcs in small projective planes, Discrete Math., 208–209 (1999) 261–271.

[9] C. E. Gordon, Orbits of arcs in PG$(N, K)$ under projectivities, Geom. Dedicata, 42 (1992), no. 2, 187–203.

[10] J. W. P. Hirschfeld, The main conjecture for MDS codes, Cryptography and Coding, 5th IMA Conference, Cirencester, UK, 1995, (C. Boyd ed.), Springer, 44–52.

[11] J. W. P. Hirschfeld, Projective Geometries over Finite Fields, 2nd ed., Clarendon, Oxford (1998).

[12] J. W. P. Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces, Journal of Statistical Planning and Inference, 72 (1998), 355–380.

[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] G. Korchmáros, private communication.

[15] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam (1977).

[16] S. Marcugini, A. Milani and F. Pambianco, A computer search for complete arcs in $\mathrm{PG}(2,q)$, $q \leq 128$, Rapporto Tecnico n. 18/95, Università degli Studi di Perugia, 1995.

[17] S. Marcugini, A. Milani and F. Pambianco, A computer search for small and large complete arcs in $\mathrm{PG}(2,q)$, Rapporto Tecnico n. 5/98, Università degli Studi di Perugia, 1998.

[18] S. Marcugini, A. Milani and F. Pambianco, Complete arcs in $\mathrm{PG}(2,25)$: the spectrum of the sizes and the classification of the smallest complete arcs, submitted.

[19] S. Marcugini, A. Milani and F. Pambianco, Minimal complete arcs in $\mathrm{PG}(2,q)$, $q \leq 29$, J. Combin. Math. Combin. Comput., 47 (2003) 19–29.

[20] T. Penttila and G. F. Royle, Classification of hyperovals in $\mathrm{PG}(2,32)$, J. Geom., 50 (1994) 151–158.

[21] R.M. Roth and A. Lempel, On MDS codes via Cauchy matrices, IEEE Trans. Inform. Theory, 35 (1989) 1314–1319.

[22] T. Szőnyi, Arcs, caps, codes and 3-independent subsets, Giornate di Geometrie Combinatorie (Proc. International Conference Univ. Perugia 1992, G. Faina and G. Tallini, eds.), Università degli studi di Perugia, 1993, 57-80.

[23] J. A. Thas, Normal rational curves and $k$-arcs in Galois spaces, Rend. Math. Appl. (6), 1 (1968), 331–334.

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