The Geometry of the Plane of Order Seventeen and its Application to Error-Correcting Codes

Najm Abdulzahra Makhrib Al-Seraji

A thesis submitted for the degree of Doctor of Philosophy

University of Sussex

August 2010

DECLARATION

I hereby declare that the work presented in this thesis is entirely my own, unless otherwise stated, and has not been presented for examination, in whole or in part, to this or any other university or institution.

Signature:

ABSTRACT

The aim of the thesis is to classify certain geometric structures, called arcs, in a particular setting, namely the projective plane of order seventeen. The main computing tool is the mathematical programming language GAP.

First, subsets of the line $PG(1,17)$ are classified. The results on the line $PG(1,17)$ classify sets of points on the conic on $PG(2,17)$, since there is a one-to-one correspondence between a set of points on $PG(1,17)$ and a set of the same size on a conic in $PG(2,17)$.

In the plane $PG(2,17)$ the important arcs are called complete and are those that cannot be increased to a larger arc. So far, all arcs up to and including size eight have been classified, as have complete 10-arcs, 11-arcs, 12-arcs, 13-arcs and 14-arcs. In the plane of order seventeen, the maximum size is eighteen.

Each of these arcs gives rise to an error-correcting code that corrects the maximum possible number of errors for its length.

Cubic curves and the related $(k;3)$-arcs in $PG(2,17)$ are also considered. A classification of both complete and incomplete curves is determined.

CONTENTS

LIST OF TABLES

To my Parents

ACKNOWLEDGMENTS

I am most indebted to my supervisor, Professor J.W.P. Hirschfeld for his help, time and patience. Without his guidance and support, this work would not have been completed.

I would like to thank the staff in the Department of Mathematics at University of Sussex, with special thanks to Mr Tom Armour, Dr Ali Taheri, Dr Omar Lakkis, Mr Tristan Pryer, Mrs Uduak George, Miss Louise Wintes, Mr Chandrashekar Venkataraman.

Also I would like to thank my friends in UK, with special thanks to Mr Ebrahim, and Mr Mohd Faizul Iqmal with their families.

Finally, I want to thank my family and relatives, and express my most sincere and unlimited thanks to my mother, the most important person in my life and the most effective person in any success that I have achieved, for her support and help.

Thanks are extended to Ministry of Higher Education and Research in my country Iraq for the grant.

1. INTRODUCTION

A projective plane is an incidence structure of points and lines with the following properties.

($P1$) Every two points are incident with a unique line.

($P2$) Every two lines are incident with a unique point.

($P3$) There are four points, no three collinear.

A *Desarguesian* projective plane $PG(2, q)$ has as points one-dimensional subspaces and as lines two-dimensional subspaces of a three-dimensional vector space over the finite field $\mathbb{F}_q$ of q elements. A k*-arc* in $PG(2, q)$ is a set of k points no three of which are collinear. A k-arc is *complete* if it is not contained in a $(k + 1)$-arc. A $(k; 3)$*-arc* in $PG(2, q)$ is a set of k points in which no four points but some three points are collinear.

The main aims of this thesis

(1) To classify arcs of all sizes in projective plane $PG(2, 17)$.

(2) To classify those arcs which are contained in a *conic*.

(3) To classify cubic curves in $PG(2, 17)$, to determine which of them are complete as $(k; 3)$-arcs, and for each incomplete $(k; 3)$-arc to find the largest complete $(k; 3)$-arc which contains it.

(4) Each of these arcs gives rise to an error-correcting code that corrects the maximum possible number of errors for its length.

Arcs in $PG(2, q)$ for $q = 2, 3, 4, 5, 7, 8, 9, 11, 13$ have been classified; see [10, chapter 14]. We are looking at the plane of order seventeen, as it is the next in the sequence.

Outline of the Chapters

Chapter 2 is devoted to basic definitions and well-known results on finite fields, roots of an element, projective spaces, the fundamental theorem of projective geometry, conics, cubics, B-points, useful results from group theory and links with coding theory.

Chapter 3 contains the classification of all subsets of the projective line of order seventeen. The basic tool is the fundamental theorem of projective geometry; there is a unique projectivity of the projective line transforming three points to any three other points.

Chapter 4 contains the classification of complete k-arcs in $PG(2, 17)$. The main theme of chapter 4 is to classify subsets that are k-arcs. In particular, we are interested in the values of k for which the arcs are complete. For $k = 4, 5, 6, 7, 8$, the k-arcs are completely classified. For all k with $k \leq 18$ there is a classification of complete k-arcs. The basic tool is the fundamental theorem of projective geometry; there is a unique projectivity of $PG(2,17)$ transforming four points no three on a line to any other four no three on a line. The parameters of the corresponding codes C are found; for each C, the length n, the dimension k and the minimum distance d are found.

Chapter 5 contains the classification of cubic curves in $PG(2,q)$ and for $PG(2,17)$ in particular. The expression "complete cubic curve" means that the associated $(k;3)$-arc is complete. We answer the question of which non-singular cubic curves in $PG(2,17)$ are complete as $(k;3)$-arcs.

Appendix 1 contains a list of the programs written in GAP.

Appendix 2 contains the tables of the points of $PG(2,17)$ written in numeral and vector forms.

A brief history

Associated to any topic in mathematics is its history. Arcs were first introduced by Bose (1947) in connection with designs in statistics. Further development began with Segre in (1954); he showed that every $(q+1)$-arc in $PG(2,q)$ is a conic. An important result is that of Ball, Blokhuis and Mazzocca showing that maximal arcs cannot exist in a plane of odd order. In 1981 Goppa found important applications of curves over finite fields to coding theory. As to geometry over a finite field, it has been thoroughly studied in the major treatise of Hirschfeld 1979-1985 and of Hirschfeld−Thas 1991.

2. BACKGROUND

2.1 Finite fields

Definition 2.1. A *field* is a set K closed under two operations $+$, $\times$ such that

(1) $(K, +)$ is an abelian group with identity 0;

(2) $(K^*, \times)$ is an abelian group with identity 1, where $K^* = K \setminus \{0\}$;

(3) $x \times (y + z) = x \times y + x \times z$, $(x + y) \times z = x \times z + y \times z$ for all x, y, z in K.

Definition 2.2. A *finite field* is a field with only a finite number of elements.

The characteristic of a finite field K is the least positive integer p, and hence a prime, such that

$$pz = \underbrace{z + \cdots + z}_{p} = 0$$

for all z in K.

Definition 2.3. The set denoted by $\mathbb{F}_p$, with p prime, consists of the residue classes of the integers modulo p under the natural addition and multiplication.

Theorem 2.4. *The set $\mathbb{F}_p$ is a finite field with p elements.*

Proof See [10, chapter 1].

Definition 2.5. Given an irreducible polynomial $F(t)$ of degree h over $\mathbb{F}_p$, we define the set $\mathbb{F}_q$, $q = p^h$ with p prime, as

$$\begin{aligned} \mathbb{F}_q &= \mathbb{F}_p[t]/(F) \\ &= \{a_0 + a_1 t + \cdots + a_{h-1} t^{h-1} \mid a_i \in \mathbb{F}_p, F(t) = 0\}. \end{aligned}$$

Theorem 2.6. *For any given q, the set $\mathbb{F}_q$ satisfies the following properties* :

(1) *the set $\mathbb{F}_q$, where $q = p^h$, is a field of characteristic p;*

(2) *the elements x of $\mathbb{F}_q$ satisfy $x^q - x = 0$;*

(3) *there exists s in $\mathbb{F}_q$ such that $s^{q-1} = 1$ and*

$$\mathbb{F}_q = \{0, 1, \ldots, s^{q-2}\};$$

such an s is called a primitive element *or* primitive root *of $\mathbb{F}_p$;*

(4) *the additive structure of* $\mathbb{F}_q$ *is given by the group isomorphism*

$$\mathbb{F}_q \cong \underbrace{Z_p \times \cdots \times Z_p}_{h};$$

(5) *the multiplicative structure of* $\mathbb{F}_q$ *is given by the group isomorphism*

$$\mathbb{F}_q \setminus \{0\} \cong Z_{q-1}.$$

Proof See [10, chapter 1].

Definition 2.7. Let $\mathbf{f}(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_0$ be a polynomial of degree n over $\mathbb{F}_q$. Then its *companion matrix* $\mathbf{C}(\mathbf{f})$ is the $n \times n$ matrix given by

$$\mathbf{C}(\mathbf{f}) = \begin{pmatrix} 0 & & & \\ \vdots & & I_{n-1} & \\ 0 & & & \\ a_0 & a_1 & \dots & a_{n-1} \end{pmatrix}$$

Definition 2.8. Let λ be a root of $\mathbf{f}$. Then $\mathbf{f}$ is *primitive* if the smallest power s of λ such that $\lambda^s = 1$ is $s = q^n - 1$. It is *subprimitive* if the smallest power s of λ such that $\lambda^s \in \mathbb{F}_q$ is $s = q^{n-1} + \cdots + q + 1$.

Definition 2.9. An *automorphism* σ of $\mathbb{F}_q$ is a permutation of the elements of $\mathbb{F}_q$ such that

(1) $(x + y)\sigma = x\sigma + y\sigma$,

(2) $(xy)\sigma = (x\sigma)(y\sigma)$

for all x, y in $\mathbb{F}_q$.

2.2 Roots of an element

To solve the equation $x^n = c$ in $\mathbb{F}_q$, let $d = (n, q-1)$, $e = (q-1)/d$ and let s be a primitive element of $\mathbb{F}_q$.

(1) $x^n = 1$ has d solutions in $\mathbb{F}_q$ namely $x = 1, s^e, s^{2e}, \dots, s^{(d-1)e}$.

(2) $x^n = 1$ has the unique solution $x = 1$ when $d = 1$.

(3) $x^n = 1$ has n solutions when $n|(q-1)$; these are $x = 1, s^{(q-1)/n}, \dots, s^{(n-1)(q-1)/n}$.

(4) $x^n = c$ has a unique solution when $d = 1$; this is $x = c^r$ where $r, r' \in Z$ and

$$rn + r'(q-1) = 1.$$

(5) $x^n = c$ has n solutions when $n|(q-1)$ and $c^{(q-1)/n} = 1$.

2.3 Projective Spaces

Let K be a field and V be *the* $(n+1)$*-dimensional vector space* K^{n+1} *over* K, with origin O. Let $V_0 = V \setminus \{O\}$. Two elements $X, Y \in V_0$ are *related* if X and Y belong to the same one-dimensional subspace of V. This relation defines an equivalence relation on V_0. Let (X) be the equivalence class of $X \in V_0$, which is the set of tX where $t \in K \setminus \{0\}$. The set of equivalence classes, denoted by $PG(n, K)$, is the n*-dimensional projective space over* K. If $K = \mathbb{F}_q$, then we will use the notation $PG(n, q)$.

The equivalence class (X), which is also denoted by $\mathbf{P}(X)$, is called a *point* of $PG(n, K)$, and X is called a *vector representing* $\mathbf{P}(X)$. If $X = (x_0, \ldots, x_n)$, and x_i is the first nonzero coordinate of X, then $\mathbf{P}(X)$ will be written as

$$(\underbrace{0, \ldots, 0}_{i}, 1, x_{i+1}/x_i, \ldots, x_n/x_i).$$

Let $W(m+1, K)$ be an $(m+1)$-dimensional subspace of V; then the set

$$\pi_m = \{\mathbf{P}(X) \mid X \in W\}$$

is an m-dimensional subspace, or m-space, of $PG(n, K)$. A 1-dimensional subspace π_1 is a *line*; a π_2 is a *plane* and a π_3 is a *solid*. The largest proper subspaces π_{n-1} are *hyperplanes* or *primes*.

Let $u = (u_0, \ldots, u_n) \in K^{n+1} \setminus \{0\}$; therefore there exists i, where $0 \leq i \leq n$, such that $u_i \neq 0$. Hence the solutions of the equation

$$u_0 x_0 + u_1 x_1 + \cdots + u_n x_n = 0$$

form a prime, which is denoted by $\pi(u)$. The vector $u = (u_0, \ldots, u_n)$ is called *the coordinate vector of the prime.*

Definition 2.10. In $PG(n, q)$, consider the points $U_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, and $U = (1, \ldots, 1)$. The set $\{U_0, \ldots, U_n\}$ is *the simplex of reference* which together with U forms the frame $\{U_0, \ldots, U_n, U\}$, where a frame is a set of $n+2$ points in $PG(n, q)$, no $n+1$ in a prime.

In this work we mainly consider the case where $n = 2$ and $q = p = 17$.

2.4 The fundamental theorem of projective geometry

Denote by S and S' two spaces $PG(n, K)$.

Definition 2.11. A *collineation* $\xi : S \to S'$ is a bijection which preserves incidence; that is, if $\Pi_r \subset \Pi_s$, then $\Pi_r \xi \subset \Pi_s \xi$. where Π_r and Π_s are subspaces of $PG(n, K)$. The group of collineations of $PG(n, K)$ is denoted by $P\Gamma L(n+1, K)$.

Definition 2.12. A *projectivity* $\beta : S \to S'$ is a bijection given by a matrix $\mathbf{T}$, necessarily nonsingular, where $\mathbf{P}(X') = \mathbf{P}(X)\beta$ if $tX' = X\mathbf{T}$, with $t \in K^*$. Write $\beta = \mathbf{M}(\mathbf{T})$; then $\beta = \mathbf{M}(\lambda \mathbf{T})$ for any λ in K^*. The group of projectivities of $PG(n, K)$ is denoted by $PGL(n+1, K)$.

Definition 2.13. With respect to a fixed basis of $V(n+1, K)$, an automorphism σ of K can be extended to an automorphic collineation σ of $PG(n, K)$; this is given by $\mathbf{P}(X)\sigma = \mathbf{P}(X\sigma)$ where $X\sigma = (x_0\sigma, x_1\sigma, \ldots, x_n\sigma)$.

Note the following properties.

(1) If $\xi : S \to S$ is a *collineation*, then $\xi = \sigma\beta$, where σ is an *automorphic collineation*, given by a field automorphism σ, and β is a projectivity.

(2) If $\{\mathbf{P}_0, \ldots, \mathbf{P}_{n+1}\}$ and $\{\mathbf{P}'_0, \ldots, \mathbf{P}'_{n+1}\}$ are both subsets of $PG(n, K)$ such that no $n+1$ points chosen from the same set lie on a prime, then there exists a unique projectivity β such that $\mathbf{P}'_i = \mathbf{P}_i\beta$ for all $i = 0, \ldots, n+1$.

(3) For $n = 1$, the previous statement simplifies: there is a unique projectivity transforming any three distinct points on a line to any other three.

(4) When $K = \mathbb{F}_2$, it suffices to give the images of $\mathbf{P}_0, \ldots, \mathbf{P}_n$ to determine β. Similarly, for the case $n = 1$, the images of two points determine the projectivity.

2.5 Conics

Definition 2.14. Given a homogenous polynomial F in three variables x_0, x_1, x_2 over $\mathbb{F}_q$, a *curve* $\mathcal{F}$ is the set

$$\mathcal{F} = \nu(F) = \{\mathbf{P}(X) \mid F(X) = 0\}$$

where $\mathbf{P}(X)$ is the point of $PG(2, q)$ represented by $X = (x_0, x_1, x_2)$.

If F has degree two, that is,

$$F = a_0x_0^2 + a_1x_1^2 + a_2x_2^2 + b_2x_0x_1 + b_1x_0x_2 + b_0x_1x_2,$$

then $\mathcal{F}$ is called a *quadric*. For q odd, the *discriminant* of a quadric $\mathcal{F}$ is the determinant

$$D = \begin{vmatrix} 2a_0 & b_2 & b_1 \\ b_2 & 2a_1 & b_0 \\ b_1 & b_0 & 2a_2 \end{vmatrix}$$

A quadric $\mathcal{F}$ is *non-singular* if its discriminant D is non-zero.

Definition 2.15. For q even, a conic $\mathbf{C}$ in $PG(2, q)$ has a canonical form

$$\nu(x_0^2 + x_1x_2),$$

that is

$$\mathbf{C} = \{\mathbf{P}(t, -1, t^2) \mid t \in \mathbb{F}_q \cup \mathbf{P}(0, 0, 1)\}.$$

Definition 2.16. A *conic* $\mathbf{C}$ is a non-singular quadric $\mathcal{F}$.

Lemma 2.17. *Every conic in $PG(2, q)$ is a $(q+1)$-arc.*

Proof See [10, chapter 7].

Corollary 2.18. *A conic in $PG(2,q)$ has other canonical forms as follows:*

(1) $\nu(x_0^2 + x_1x_2)$, *all q;*

(2) $\nu(x_0^2 - x_1x_2)$, *all q;*

(3) $\nu(a_0x_0^2 + a_1x_1^2 + a_2x_2^2)$, *with $a_0a_1a_2 \neq 0$, q odd;*

(4) $\nu(x_0^2 + x_1^2 + x_2^2)$, *$q$ odd.*

Proof See [10, chapter 7].

Corollary 2.19. *The projective group $PGO(3,q)$ of a conic has order*

$$\begin{aligned} \mid PGO(3,q) \mid &= \mid PGL(3,q) \mid /(q^5 - q^2) \\ &= q(q^2-1) \\ &= \mid PGL(2,q) \mid . \end{aligned}$$

Proof See [10, chapter 7].

Corollary 2.20. *In $PG(2,q)$ with $q \geq 4$, there is a unique conic through a 5-arc.*

Proof See [10, chapter 7].

Corollary 2.21. $PGO(3,q) \cong PGL(2,q)$.

Proof See [10, chapter 7].

2.6 Cubics

Definition 2.22. Given a homogenous polynomial F in three variables x_0, x_1, x_2 over $\mathbb{F}_q$, a *curve* $\mathcal{F}$ is the set

$$\mathcal{F} = \nu(F) = \{\mathbf{P}(X) : F(X) = 0\}$$

where $\mathbf{P}(X)$ is the point of $PG(2,q)$ represented by $X = (x_0, x_1, x_2)$.

If F has degree three, that is,

$$F = a_0x_0^3 + a_1x_1^3 + a_2x_2^3 + a_3x_0^2x_1 + a_4x_0^2x_2 + a_5x_1^2x_0 + a_6x_1^2x_2 + a_7x_2^2x_0 + a_8x_2^2x_1 + a_9x_0x_1x_2,$$

then $\mathcal{F}$ is called a *cubic*. The multiplicity of P on $\mathcal{F}$, denoted $m_P(\mathcal{F})$, is the minimum of intersection multiplicities of the line ℓ and $\mathcal{F}$ at P, denoted $m_P(\ell, \mathcal{F})$, for all lines ℓ through P. Then P is a singular point of $\mathcal{F}$ if $m_P(\mathcal{F}) > 1$ and a non-singular point of $\mathcal{F}$ if $m_P(\mathcal{F}) = 1$. The cubic $\mathcal{F}$ is called *singular* or *non-singular* (smooth) according as $\mathcal{F}$ does or does not have a singular point.

Definition 2.23. A non-singular point P of $\mathcal{F}$ is *a point of inflexion of $\mathcal{F}$* if

$$I(P, \ell_P \cap \mathcal{F}) \geq 3.$$

Here, P is also called *an inflexion*; the tangent ℓ_P at P is *the inflexional tangent.*

2.7 B-points

Definition 2.24. Let K be a k-arc and P a point of $PG(2,q)\backslash K$. Then if exactly i bisecants of K pass through P it is said to be a point of index i. The number of these points is denoted by c_i.

Lemma 2.25. *The constants c_i of a k-arc K in $PG(2,q)$ satisfy the following equations with the summation taken 0 to n for which $c_i \neq 0$:*

$$\begin{aligned} \sum c_i &= q^2+q+1-k, && (2.1)\\ \sum ic_i &= k(k-1)(q-1)/2, && (2.2)\\ \sum i(i-1)c_i/2 &= k(k-1)(k-2)(k-3)/8. && (2.3) \end{aligned}$$

Proof See [10, chapter 9].

Definition 2.26. Let K be a 6-arc and P a point of $PG(2,q)\setminus K$. Then, if exactly 3 bisecants of K pass through P, it is said to be a *B-point* or *point of index* 3.

Definition 2.27. The maximum value of k for a k-arc to exist is denoted by $m(2,q)$, and a k-arc with this number of points is an *oval.*

2.8 Useful results from group theory

Definition 2.28. A group G acts on a set Λ if there is a map $\Lambda \times G \rightarrow \Lambda$ such that given g, g' elements in G and 1 its identity, then

(1) $x1 = x$,

(2) $(xg)g' = x(gg')$
for any x in Λ.

Definition 2.29. The orbit of x in Λ under the action of G is the set

$$xG = \{xg \mid g \in G\}.$$

Definition 2.30. The stabilizer of x in Λ under the action of G is the group

$$G_x = \{g \in G \mid xg = x\}.$$

Remark 2.31. The orbit of x is a subset of Λ, whereas the stabilizer of x is a subset of G.

Definition 2.32. The action of G on Λ is *transitive* if given any two elements x, y in Λ there exists g in G such that $y = xg$. In that case, there is only one orbit. The action is *regular* if it is transitive and $G_x = \{1\}$ for all x in Λ.

The action of G on Λ is *k-transitive* if there is some element of G transforming any ordered k-tuple of distinct elements of Λ to any other such k-tuple.

Definition 2.33. Let the group G act on the set Λ.

(1) If $y = xg$, for x, y in G, then

   (a) $yG = xG$;

   (b) $G_y = g^{-1}G_x g$.

(2) $|G_x| = |G|/|xG|$.

In Table 2.1 a list of groups of order up to 24 is given.

Tab. 2.1: Group of order up to 24

Order	Number	Groups
1	1	I
2	1	$\mathbf{Z}_2$
3	1	$\mathbf{Z}_3$
4	2	$\mathbf{Z}_4, \mathbf{Z}_2 \times \mathbf{Z}_2$
5	1	$\mathbf{Z}_5$
6	2	$\mathbf{Z}_6, \mathbf{S}_3$
7	1	$\mathbf{Z}_7$
8	5	$\mathbf{Z}_8, \mathbf{Z}_4 \times \mathbf{Z}_2, \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2, \mathbf{D}_4, \mathbf{Q}_4$
9	2	$\mathbf{Z}_9, \mathbf{Z}_3 \times \mathbf{Z}_3$
10	2	$\mathbf{Z}_{10}, \mathbf{D}_5$
11	1	$\mathbf{Z}_{11}$
12	5	$\mathbf{Z}_{12}, \mathbf{Z}_6 \times \mathbf{Z}_2, \mathbf{D}_6, \mathbf{Q}_6, \mathbf{A}_4$

13	1	$\mathbf{Z}_{13}$
14	2	$\mathbf{Z}_{14}, \mathbf{D}_7$
15	1	$\mathbf{Z}_{15}$
16	14	$\mathbf{Z}_{16}, \mathbf{Z}_8 \times \mathbf{Z}_2, (\mathbf{Z}_4)^2, \mathbf{Z}_4 \times (\mathbf{Z}_2)^2, (\mathbf{Z}_2)^4, \mathbf{D}_8, \mathbf{Q}_8$
		$\mathbf{D}_4 \times \mathbf{Z}_2, \mathbf{Q}_4 \times \mathbf{Z}_2, H_1 \cong \mathbf{Z}_8 \rtimes \mathbf{Z}_2, H_2 \cong \mathbf{Z}_8 \rtimes \mathbf{Z}_2$
		$\mathbf{Z}_4 \rtimes \mathbf{Z}_4, H_3 \cong (\mathbf{Z}_4 \times \mathbf{Z}_2) \rtimes \mathbf{Z}_2, H_4 \cong (\mathbf{Z}_4 \times \mathbf{Z}_2) \rtimes \mathbf{Z}_2$
17	1	$\mathbf{Z}_{17}$
18	5	$\mathbf{Z}_{18}, \mathbf{Z}_6 \times \mathbf{Z}_3, \mathbf{D}_9, \mathbf{S}_3 \times \mathbf{Z}_3, (\mathbf{Z}_3 \times \mathbf{Z}_3) \rtimes \mathbf{Z}_2$
19	1	$\mathbf{Z}_{19}$
20	5	$\mathbf{Z}_{20}, \mathbf{Z}_{10} \times \mathbf{Z}_2, \mathbf{D}_{10}, \mathbf{Q}_{10}, \mathbf{Z}_5 \rtimes \mathbf{Z}_4$
21	2	$\mathbf{Z}_{21}, \mathbf{Z}_7 \rtimes \mathbf{Z}_3$
22	2	$\mathbf{Z}_{22}, \mathbf{D}_{11}$
23	1	$\mathbf{Z}_{23}$
24	15	$\mathbf{Z}_{24}, \mathbf{Z}_{12} \times \mathbf{Z}_2, \mathbf{Z}_6 \times (\mathbf{Z}_2)^2, \mathbf{S}_4, \mathbf{D}_{12}, \mathbf{Q}_{12}, \mathbf{D}_6 \times \mathbf{Z}_2$
		$\mathbf{A}_4 \times \mathbf{Z}_2, \mathbf{Q}_6 \times \mathbf{Z}_2, \mathbf{D}_4 \times \mathbf{Z}_3, \mathbf{Q}_4 \times \mathbf{Z}_3, \mathbf{S}_3 \times \mathbf{Z}_4$
		$SL(2,3), \mathbf{Z}_3 \rtimes \mathbf{Z}_8, \mathbf{Z}_3 \rtimes \mathbf{D}_4$

The types of group that occurs are listed below.

$$\begin{aligned}
\mathbf{Z}_n &= \text{cyclic group of order } n;\\
\mathbf{S}_n &= \text{symmetric group of degree } n;\\
\mathbf{A}_n &= \text{alternating group of degree } n;\\
\mathbf{D}_n &= \text{dihedral group of order } 2n\\
&= \langle r, s \mid r^n = s^2 = (rs)^2 = 1\rangle;\\
\mathbf{Q}_n &= \text{dicyclic group of order } 2n\\
&= \langle r, s \mid r^n = 1, r^{n/2} = s^2 = (sr^{-1})^2\rangle;\\
G \times H &= \text{the direct product of } G \text{ and } H;\\
G \rtimes H &= \text{a semi-direct product of } G \text{ with } H, \text{where } H\\
& \text{ is a normal subgroup.}
\end{aligned}$$

Lemma 2.34. *Subgroups of order* 16 *in Table 2.1 are distinguished in pairs as follows:*

(1) H_1 *has three elements of order* 2*;*

(2) H_2 *has five elements of order* 2*;*

(3) *the subgroup of squares in* H_3 *is isomorphic to* $\mathbf{Z}_2$*;*

(4) *the subgroup of squares in* H_4 *is isomorphic to* $\mathbf{Z}_2 \times \mathbf{Z}_2$*.*

Proof See [10, chapter 2].

2.9 Links with Coding Theory

The geometrical objects considered in this work can be viewed and studied as linear codes defined over a finite field. Hence, results on their geometry can be translated to results in Coding Theory. In order to understand these results, we introduce the basic concepts and results concerning this theory.

An $(n, M, d)_q$ code C is a set of M words, each with n symbols taken from an alphabet of size q, such that any two words differ in at least d places. A code $(n, M, d)_q$ has the following desirable properties:

(1) small n: fast transmission;

(2) large M: many messages;

(3) large d: correct many errors.

If the code is *linear*, it can more easily be used for encoding and decoding; in this case, $M = q^k$ for some positive integer k, the dimension of the code, and C is called an $[n, k, d]_q$ code. The Main Coding Theory problem is to find codes optimising one parameter with the other two fixed. Mathematically, such a code can also be viewed as a set of n points in $PG(k-1, q)$ with at most $n-d$ points in a subspace of dimension $k-2$.

Definition 2.35. An (n, M) *code* C over $\mathbb{F}_q$ is a subset of $\mathbb{F}_q^n$ of size M. A *linear* $[n,k]_q$ *code* over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$ and size $M = q^k$. The vectors in the linear code C arc called *codewords* and we denote them by $\mathbf{x} = x_1 x_2 \dots x_n$, where $x_i \in \mathbb{F}_q$.

Definition 2.36. A *generator matrix* G for an $[n,k]_q$ code C is any $k \times n$ matrix G whose rows form a basis for C. For any set of k independent columns of a generator matrix G, the corresponding set of coordinates forms an information set for G. If the first k coordinates form an information set, the code has a unique generator matrix of the form $[I_k|A]$ where I_k is the $k \times k$ identity matrix; such a generator matrix is in *standard form.*

Definition 2.37. The ordinary *inner product* of vectors $\mathbf{u} = u_1 \dots u_n$,$\mathbf{v} = v_1 \dots v_n$ in $\mathbb{F}_q^n$ is defined by

$$\mathbf{u} \cdot \mathbf{v} = \sum_{i=1}^{n} u_i v_i.$$

Definition 2.38. The *dual* of the code C is the $[n, n-k]_q$ linear code $C^\perp$ defined as

$$C^\perp = \{\mathbf{v} \in \mathbb{F}_q^n \mid \mathbf{u} \cdot \mathbf{v} = 0 \ \forall \mathbf{u} \in C\}.$$

Definition 2.39. A *parity check matrix* H of a linear $[n,k]_q$ code C is defined to be an $(n-k) \times n$ generator matrix of $C^\perp$.

Remark 2.40. From the previous definition, we deduce that

$$C = \{\mathbf{x} \in \mathbb{F}_q^n \mid H\mathbf{x}^T = 0\}.$$

Theorem 2.41. *If* $G = [I_k|A]$ *is a generator matrix for* C *in standard form, then* $H = [-A^T|I_{n-k}]$ *is a* parity check matrix for $C^\perp$*.*

Proof See [10, chapter 2].

Definition 2.42. The (*Hamming*) *distance* $d(\mathbf{x}, \mathbf{y})$ between two *vectors* $\mathbf{x}, \mathbf{y}$ in $\mathbb{F}_q^n$ is defined to be the number of coordinates in which $\mathbf{x}$ and $\mathbf{y}$ differ. The distance d is a *metric.* The *minimum distance* d of a code C is the smallest distance between any pair of distinct codewords.

Definition 2.43. The (*Hamming*) weight $\mathrm{w}(\mathbf{x})$ of a vector $\mathbf{x}$ in $\mathbb{F}_q^n$ is the number of its nonzero coordinates.

Therefore, if C is a linear code, the minimum distance d is the same as the minimum weight of a nonzero codeword. When the minimum distance d of an $[n,k]_q$ code C is known, we refer to C as a linear $[n,k,d]_q$ code.

Let A_i be the number of codewords of weight i in a code C.

Definition 2.44. The list A_i for $0 \leq i \leq n$ is called *the weight distribution of* C.

Theorem 2.45. *A linear code has minimum distance d if and only if its parity check matrix has a set of d linearly dependent columns but no set of $d-1$ linearly dependent columns.*

Proof See [10, chapter 2].

Corollary 2.46. *For any $[n,k,d]_q$ code we have*

$$d \leq n - k + 1.$$

Proof See [10, chapter 2].

Definition 2.47. A code is *maximum distance separable (MDS)* when

$$d = n - k + 1.$$

3. THE PROJECTIVE LINE $PG(1,17)$

3.1 Introduction

The 18 points of $PG(1,17)$ are $\mathbf{P}(x_0,x_1)$, $x_i \in \mathbb{F}_{17}$. So

$$PG(1,17) = \{U_0 = \mathbf{P}(1,0)\} \cup \{\mathbf{P}(x,1) \mid x \in \mathbb{F}_{17}\}.$$

Each point $\mathbf{P}(x_0,x_1)$ with $x_1 \neq 0$ is determined by the non-homogeneous coordinate x_0/x_1; the coordinate for U_0 is ∞. Then, with $\mathbb{F}_{17} \cup \{\infty\}$, each point of $PG(1,17)$ is represented by a single element of $\mathbb{F}_{17} \cup \{\infty\}$. Thus

$$PG(1,17) = \{\mathbf{P}(t,1) \mid t \in \mathbb{F}_{17} \cup \{\infty\};$$

here, $\mathbf{P}(\infty,1) = \mathbf{P}(1,0)$. A projectivity $\xi = \mathbf{M}(\mathbf{T})$ of $PG(1,17)$ is given by $Y = X\mathbf{T}$, where $X = (x_0,x_1), Y = (y_0,y_1)$ and

$$\mathbf{T} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Let $s = y_0/y_1$ and $t = x_0/x_1$; then $s = (at+c)/(bt+d)$. If $Q_i = P_i\xi$ for $i = 2,3,4$ and P_i and Q_i have the respective coordinates t_i and s_i, then ξ is given by

$$\frac{(s-s_3)(s_2-s_4)}{(s-s_4)(s_2-s_3)} = \frac{(t-t_3)(t_2-t_4)}{(t-t_4)(t_2-t_3)}.$$

3.2 The tetrads

There are 18 points on the line $PG(1,17)$ and they have non-homogeneous coordinates

$$\infty, 0, 1, -1, 2, -2, 3, -3, 4, -4, 5, -5, 6, -6, 7, -7, 8, -8.$$

The cross-ratio of four ordered points P_1, P_2, P_3, P_4 with coordinates t_1, t_2, t_3, t_4 is

$$\{P_1, P_2; P_3, P_4\} = \{t_1, t_2; t_3, t_4\} = \frac{(t_1-t_3)(t_2-t_4)}{(t_1-t_4)(t_2-t_3)}.$$

If P_1, P_2, P_3, P_4 are distinct points, then P_1 and P_2 separate P_3 and P_4 harmonically, written $h(P_1, P_2; P_3, P_4)$, if

$$\{t_1, t_2; t_3, t_4\} = -1.$$

So,

$$h(P_1, P_2; P_3, P_4) \Longleftrightarrow h(P_2, P_1; P_3, P_4).$$

In this case, the permutations of the points only give three values of the cross-ratio, $-1, 2, 1/2$. Let ω be the cross-ratio of a tetrad in a given order. The tetrad is called *harmonic* (H) if $\omega = 1-\omega$, $\omega = \omega/(\omega-1)$ or $\omega = 1/\omega$. It is called *equianharmonic* (E) if $\omega = 1/(1-\omega)$ or $\omega = (\omega-1)/\omega$, and it is neither harmonic nor equianharmonic (N) if the cross-ratio is another value. Consider the tetrad $\{\infty, 0, 1, t\}$ with $t \in \mathbb{F}_{17} \setminus \{0,1\}$. Let

$$\begin{aligned} X_1 &= \{ \text{ class of } H \text{ tetrads}\},\\ X_2 &= \{ \text{ class of } E \text{ tetrads}\},\\ X_3 &= \{ \text{ class of } N \text{ tetrads}\}. \end{aligned}$$

Since $17 \not\equiv 0,1 (\text{mod } 3)$, there are no equianharmonic tetrads. So X_2 is empty. The tetrad $\{\infty, 0, 1, a\} \in X_1$ for $a = -1, 2, -8$. The tetrad $\{\infty, 0, 1, c\} \in X_3$ for

$$c = -2, 3, -3, 4, -4, 5, -5, 6, -6, 7, -7, 8.$$

As a tetrad of type N has six possible values of its cross-ratio, the class X_3 is partitioned into two subclasses C_2 with

$$c = -2, 3, -5, 6, -7, 8.$$

and the other C_3 with

$$c = -3, 4, -4, 5, -6, 7.$$

If we now call the three classes C_1, C_2 and C_3 where $C_1 = X_1$, $C_2 \cup C_3 = X_3$, then the tetrads within each class C_i are projectively equivalent. So there are three projectively distinct tetrads : one of type H and two of type N, called N_1 and N_2.

1. Consider the tetrad $H = \{\infty, 0, 1, -1\}$ chosen from the class C_1. Then the projective group of H is isomorphic to dihedral group of order 8.

2. The tetrad $N_1 = \{\infty, 0, 1, -2\}$ chosen from the class C_2. Then the projective group of N_1 is isomorphic to the direct product of $\mathbf{Z_2}$ and $\mathbf{Z_2}$.

3. The tetrad $N_2 = \{\infty, 0, 1, -3\}$ chosen from the class C_3. Then the projective group of N_2 is isomorphic to the direct product of $\mathbf{Z_2}$ and $\mathbf{Z_2}$.

3.3 The pentads

Under the group $G(H) = \langle b, d \rangle$, where $b = \frac{1}{x}, d = \frac{x-1}{x+1}$, the points of $PG(1,17) \setminus H$ are partitioned into three orbits; they are

$$\{2, -2, 3, -3, 6, -6, 8, -8\}, \{4, -4\}, \{5, -5, 7, -7\}.$$

Under the group $G(N_1) = \langle f, h \rangle$, where $f = \frac{x+2}{x-1}, h = \frac{-2}{x}$, the points of $PG(1,17) \setminus N_1$ are partitioned into four orbits; they are

$$\{-1, 2, 4, 8\}, \{3, 5, 6, -6\}, \{-3, -4, -5, -8\}, \{7, -7\}.$$

Finally $G(N_2) = \langle k, l \rangle$, where $k = \frac{x+3}{x-1}, l = \frac{-3}{x}$, and the points of $PG(1,17) \setminus N_2$ are partitioned into four orbits; they are

$$\{-1, 3\}, \{2, -4, 5, 7\}, \{-2, -6, -7, -8\}, \{4, -5, 6, 8\}.$$

Adding one point from each orbit to the corresponding tetrad gives eleven pentads to be

$$\{a_1,a_2,a_3,a_4\},\{a_1,a_2,a_3,a_5\},\{a_1,a_2,a_4,a_5\},\{a_1,a_3,a_4,a_5\},\{a_2,a_3,a_4,a_5\}.$$

So we get Table 3.1.

Tab. 3.1: The pentads

No.	The pentads	CR of tetrads	Types of tetrad	Stabilizer
1	$\{\infty,0,1,-1,2\}$	$-1,2,-2,8,-4$	$H\,H\,N_1\,N_1\,N_2$	$\mathbf{Z_2}=\langle\frac{1-x}{1}\rangle$
2	$\{\infty,0,1,-1,4\}$	$-1,4,-4,7,-6$	$H\,N_2\,N_2\,N_2\,N_2$	$\mathbf{Z_4}=\langle\frac{x-1}{x+1}\rangle$
3	$\{\infty,0,1,-1,5\}$	$-1,5,-5,-2,-3$	$H\,N_2\,N_1\,N_1\,N_2$	$\mathbf{Z_2}=\langle\frac{1-x}{1+x}\rangle$
4	$\{\infty,0,1,-2,-1\}$	$-2,-1,-8,-5,7$	$N_1\,H\,H\,N_1\,N_2$	$\mathbf{Z_2}=\langle\frac{-x-1}{1}\rangle$
5	$\{\infty,0,1,-2,3\}$	$-2,3,7,5,8$	$N_1\,N_1\,N_2\,N_2\,N_1$	$\mathbf{Z_2}=\langle\frac{1-x}{1}\rangle$
6	$\{\infty,0,1,-2,-3\}$	$-2,-3,-7,7,-1$	$N_1\,N_2\,N_1\,N_2\,H$	$\mathbf{Z_2}=\langle\frac{-x-2}{1}\rangle$
7	$\{\infty,0,1,-2,7\}$	$-2,7,5,-2,3$	$N_1\,N_2\,N_2\,N_1\,N_1$	$\mathbf{Z_2}=\langle\frac{-2}{x}\rangle$
8	$\{\infty,0,1,-3,-1\}$	$-3,-1,6,-8,-7$	$N_2\,H\,N_1\,H\,N_1$	$\mathbf{Z_2}=\langle\frac{x+3}{x-1}\rangle$
9	$\{\infty,0,1,-3,2\}$	$-3,2,5,4,-6$	$N_2\,H\,N_2\,N_2\,N_2$	$\mathbf{Z_4}=\langle\frac{2x-2}{x}\rangle$
10	$\{\infty,0,1,-3,-2\}$	$-3,-2-5,5,-1$	$N_2\,N_1\,N_1\,N_2\,H$	$\mathbf{Z_2}=\langle\frac{-x-2}{1}\rangle$
11	$\{\infty,0,1,-3,4\}$	$-3,4,-7,-5,8$	$N_2\,N_2\,N_1\,N_1\,N_1$	$\mathbf{Z_2}=\langle\frac{1-x}{1}\rangle$

According to the types of the five tetrads, the pentads fall into four sets,

$$\{1,4,8\},\{2,9\},\{3,6,10\},\{5,7,11\}.$$

The pentads 6 and 10 are the same. Transformations can be carried out as follows:

(1) $1\longrightarrow 4$ by $\frac{-x}{1}$,

(2) $1\longrightarrow 8$ by $\frac{1+x}{1-x}$,

(3) $2\longrightarrow 9$ by $\frac{x+1}{x}$,

(4) $3 \longrightarrow 6$ by $\frac{x+1}{8x-6}$,

(5) $5 \longrightarrow 7$ by $\frac{x+2}{5x+2}$,

(6) $5 \longrightarrow 11$ by $\frac{7x-3}{1}$.

This gives the following conclusion.

Theorem 3.1. *On $PG(1, 17)$ there are precisely four projectively distinct pentads, given in Table 3.2.*

Tab. 3.2: The distinct pentads

No.	New symbol	Canonical form	Stabilizer
1	P_1	$\{\infty, 0, 1, -1, 2\}$	$G(P_1) \cong \mathbf{Z_2} = \langle \frac{1-x}{1} \rangle$
2	P_2	$\{\infty, 0, 1, -1, 4\}$	$G(P_2) \cong \mathbf{Z_4} = \langle \frac{x-1}{x+1} \rangle$
3	P_3	$\{\infty, 0, 1, -1, 5\}$	$G(P_3) \cong \mathbf{Z_2} = \langle \frac{1-x}{1+x} \rangle$
5	P_4	$\{\infty, 0, 1, -2, 3\}$	$G(P_4) \cong \mathbf{Z_2} = \langle \frac{1-x}{1} \rangle$

3.4 The hexads

1. The group $G(P_1)$ partitions the set $PG(1, 17) \setminus P_1$ into seven orbits; they are
$$\{-2, 3\}, \{-3, 4\}, \{-4, 5\}, \{-5, 6\}, \{-6, 7\}, \{-7, 8\}, \{-8\}.$$
2. The group $G(P_2)$ partitions the set $PG(1, 17) \setminus P_2$ into four orbits; they are
$$\{-2, 3, -6, -8\}, \{2, 6, -3, -8\}, \{-4\}, \{5, -5, -7, 7\}.$$
3. The group $G(P_3)$ partitions the set $PG(1, 17) \setminus P_3$ into seven orbits; they are
$$\{2, -6\}, \{-2, -3\}, \{3, 8\}, \{4, -4\}, \{-5, 7\}, \{6, -8\}, \{-7\}.$$
4. The group $G(P_4)$ partitions the set $PG(1, 17) \setminus P_4$ into seven orbits; they are
$$\{-1, 2\}, \{-3, 4\}, \{-4, 5\}, \{-5, 6\}, \{-6, 7\}, \{-7, 8\}, \{-8\}.$$

Therefore, 25 hexads can be formed (the total number of all orbits) by adding one point from each orbit to the corresponding pentad.

Remark 3.2. The numbers of hexads and their stabilizers are given in Table 3.3.

Tab. 3.3: The stabilizers of hexads

Stabilizer	I	$\mathbf{Z_2}\times\mathbf{Z_2}$	$\mathbf{Z_2}$	$\mathbf{S_3}$	$\mathbf{D_4}$	$\mathbf{S_4}$
Number	6	4	12	1	1	1

According to the types of the six pentads, the hexads fall into ten sets. This gives the following conclusion.

Theorem 3.3. *On $PG(1,17)$ there are precisely 10 projectively distinct hexads, given in Table 3.4.*

Tab. 3.4: The distinct hexads

Symbol	Canonical form	Types of pentad	Stabilizer
H_1	$\{\infty,0,1,-1,2,-2\}$	$P_1P_1P_1P_1P_3P_3$	$\mathbf{Z_2}\times\mathbf{Z_2}=\langle\frac{-x}{1},\frac{2}{x}\rangle$
H_2	$\{\infty,0,1,-1,2,-3\}$	$P_1P_1P_2P_4P_3P_4$	$I=\langle x\rangle$
H_3	$\{\infty,0,1,-1,2,-4\}$	$P_1P_2P_3P_1P_3P_2$	$\mathbf{Z_2}=\langle\frac{2x+2}{x-2}\rangle$
H_4	$\{\infty,0,1,-1,2,-6\}$	$P_1P_1P_3P_4P_4P_3$	$\mathbf{Z_2}=\langle\frac{1-x}{1+x}\rangle$
H_5	$\{\infty,0,1,-1,2,-7\}$	$P_1P_3P_1P_4P_3P_4$	$\mathbf{Z_2}=\langle\frac{x-2}{x-1}\rangle$
H_6	$\{\infty,0,1,-1,2,-8\}$	$P_1P_1P_1P_1P_1P_1$	$\mathbf{D_6}=\langle\frac{1+x}{2-x},\frac{2-x}{x+1}\rangle$
H_7	$\{\infty,0,1,-1,4,-4\}$	$P_2P_2P_2P_2P_2P_2$	$\mathbf{S_4}=\langle\frac{1+x}{4-4x},\frac{x+1}{1-x}\rangle$
H_8	$\{\infty,0,1,-1,4,5\}$	$P_2P_3P_2P_4P_4P_3$	$\mathbf{Z_2}=\langle\frac{1-x}{1+4x}\rangle$

Symbol	Canonical form	Types of pentad	Stabilizer
H_9	$\{\infty, 0, 1, -1, 5, -5\}$	$P_3P_3P_3P_3P_4P_4$	$\mathbf{Z_2} \times \mathbf{Z_2} = \langle \frac{-x}{1}, \frac{5}{x} \rangle$
H_{10}	$\{\infty, 0, 1, -2, 3, -6\}$	$P_4P_4P_4P_4P_4P_4$	$\mathbf{S_3} = \langle \frac{x+2}{x-1}, \frac{x+6}{6x-1} \rangle$

3.5 The heptads

1. The group $G(H_1)$ partitions the set $PG(1,17) \setminus H_1$ into four orbits; they are
$$\{3, -3, 5, -5\}, \{4, -4, 8, -8\}, \{6, -6\}, \{7, -7\}.$$
2. The group $G(H_2)$ partitions the set $PG(1,17) \setminus H_2$ into 12 orbits; they are
$$\{-2\}, \{3\}, \{4\}, \{-4\}, \{5\}, \{-5\}, \{6\}, \{-6\}, \{7\}, \{-7\}, \{8\}, \{-8\}.$$
3. The group $G(H_3)$ partitions the set $PG(1,17) \setminus H_3$ into six orbits; they are
$$\{-2, -8\}, \{3, 8\}, \{-3, -6\}, \{4, 5\}, \{-5, 6\}, \{7, -7\}.$$
4. The group $G(H_4)$ partitions the set $PG(1,17) \setminus H_4$ into seven orbits; they are
$$\{-2, -3\}, \{3, 8\}, \{4, -4\}, \{5\}, \{-5, 7\}, \{6, -8\}, \{-7\}.$$
5. The group $G(H_5)$ partitions the set $PG(1,17) \setminus H_5$ into seven orbits; they are
$$\{-2, 7\}, \{3, -8\}, \{-3\}, \{4, -5\}, \{-4, 8\}, \{5\}, \{6, -6\}.$$
6. The group $G(H_6)$ fixes the set $PG(1,17) \setminus H_6$.
7. The group $G(H_7)$ fixes the set $PG(1,17) \setminus H_7$.
8. The group $G(H_8)$ partitions the set $PG(1,17) \setminus H_8$ into six orbits; they are
$$\{2, -2\}, \{3, -8\}, \{-3, -5\}, \{-4, -6\}, \{6, -7\}, \{7, 8\}.$$
9. The group $G(H_9)$ partitions the set $PG(1,17) \setminus H_9$ into three orbits; they are
$$\{2, -2, 6, -6\}, \{3, -3, 4, -4\}, \{7, -7, 8, -8\}.$$
10. The group $G(H_{10})$ partitions the set $PG(1,17) \setminus H_{10}$ into two orbits; they are
$$\{-1, -5, 5, 6, 8, -8\}, \{2, -3, 4, -4, 7, -7\}.$$

Therefore, 49 heptads can be formed (the total number of all orbits) by adding one point from each orbit to the corresponding hexad. In Tables 3.5 we list the additional points to the hexads.

Tab. 3.5: The additional points to the hexads

Symbol	Types of pentad	The additional points
H_1	$P_1P_1P_1P_1P_3P_3$	$-3, -8, 6, -7$
H_2	$P_1P_1P_2P_4P_3P_4$	$[-2], 3, 4, -4, 5, -5, 6, -6, 7, -7, 8, -8$
H_3	$P_1P_2P_3P_1P_3P_2$	$-2, 3, -6, 4, -5, -7$
H_4	$P_1P_1P_3P_4P_4P_3$	$[-3], 3, [-4], 5, -5, 6, -7$
H_5	$P_1P_3P_1P_4P_3P_4$	$[-2], 3, [-3], 4, [-4], 5, [-6]$
H_6	$P_1P_1P_1P_1P_1P_1$	$[-2]$
H_7	$P_2P_2P_2P_2P_2P_2$	5
H_8	$P_2P_3P_2P_4P_4P_3$	$2, 3, -5, [-4], 6, 7$
H_9	$P_3P_3P_3P_3P_4P_4$	$2, [4], 7$
H_{10}	$P_4P_4P_4P_4P_4P_4$	$-1, 2$

So far, the number of heptads constructed is 39, since each point in square brackets gives an identical heptad to one already included.

Remark 3.4. The numbers of heptads and their stabilizers are given in Table 3.6.

Tab. 3.6: The stabilizers of heptads

Stabilizer	I	$\mathbf{Z_2}$
Number	17	22

According to the types of the seven hexads, the heptads fall into ten sets. This gives the following conclusion.

Theorem 3.5. *On $PG(1,17)$ there are precisely 10 projectively distinct heptads, given in Table 3.7.*

Tab. 3.7: The distinct heptads

Symbol	Canonical form	Types of hexad	Stabilizer
T_1	$\{\infty,0,1,-1,2,-2,-3\}$	$H_1H_2H_1H_3H_2H_3H_4$	$\mathbf{Z_2}=\langle -x-1\rangle$
T_2	$\{\infty,0,1,-1,2,-2,-8\}$	$H_1H_6H_4H_2H_3H_2H_4$	$I=\langle x\rangle$
T_3	$\{\infty,0,1,-1,2,-2,6\}$	$H_1H_2H_4H_2H_4H_8H_8$	$\mathbf{Z_2}=\langle \frac{2}{x}\rangle$
T_4	$\{\infty,0,1,-1,2,-2,-7\}$	$H_1H_4H_4H_4H_4H_9H_9$	$\mathbf{Z_2}=\langle \frac{-2}{x}\rangle$
T_5	$\{\infty,0,1,-1,2,-3,4\}$	$H_2H_2H_2H_2H_4H_4H_4$	$\mathbf{Z_2}=\langle 1-x\rangle$
T_6	$\{\infty,0,1,-1,2,-3,-4\}$	$H_2H_3H_3H_8H_4H_9H_2$	$I=\langle x\rangle$
T_7	$\{\infty,0,1,-1,2,-3,5\}$	$H_2H_3H_2H_7H_8H_3H_8$	$\mathbf{Z_2}=\langle \frac{x+3}{x-1}\rangle$
T_8	$\{\infty,0,1,-1,2,-3,6\}$	$H_2H_2H_4H_8H_{10}H_9H_8$	$I=\langle x\rangle$

Symbol	Canonical form	Types of hexad	Stabilizer
T_9	$\{\infty, 0, 1, -1, 2, -3, -7\}$	$H_2H_4H_4H_2H_{10}H_4H_{10}$	$\mathbf{Z_2} = \langle \frac{x-2}{x-1} \rangle$
T_{10}	$\{\infty, 0, 1, -1, 2, -4, -7\}$	$H_3H_4H_8H_4H_4H_3H_8$	$\mathbf{Z_2} = \langle \frac{2x-3}{x-2} \rangle$

3.6 The octads

1. The group $G(T_1)$ partitions the set $PG(1,17) \setminus T_1$ into six orbits; they are
$$\{3, -4\}, \{4, -5\}, \{5, -6\}, \{6, -7\}, \{7, -8\}, \{8\}.$$
2. The group $G(T_2)$ partitions the set $PG(1,17) \setminus T_2$ into eleven orbits; they are
$$\{3\}, \{-3\}, \{4\}, \{-4\}, \{5\}, \{-5\}, \{6\}, \{-6\}, \{7\}, \{-7\}, \{8\}.$$
3. The group $G(T_3)$ partitions the set $PG(1,17) \setminus T_3$ into six orbits; they are
$$\{3, -5\}, \{-3, 5\}, \{4, -8\}, \{-4, 8\}, \{-6\}, \{7, -7\}.$$
4. The group $G(T_4)$ partitions the set $PG(1,17) \setminus T_4$ into six orbits; they are
$$\{3, 5\}, \{-3, -5\}, \{4, 8\}, \{-4, -8\}, \{6, -6\}, \{7\}.$$
5. The group $G(T_5)$ partitions the set $PG(1,17) \setminus T_5$ into six orbits; they are
$$\{-2, 3\}, \{-4, 5\}, \{-5, 6\}, \{-6, 7\}, \{-7, 8\}, \{-8\}.$$
6. The group $G(T_6)$ partitions the set $PG(1,17) \setminus T_6$ into eleven orbits; they are
$$\{-2\}, \{3\}, \{4\}, \{5\}, \{-5\}, \{6\}, \{-6\}, \{7\}, \{-7\}, \{8\}, \{-8\}.$$
7. The group $G(T_7)$ partitions the set $PG(1,17) \setminus T_7$ into six orbits; they are
$$\{-2, -6\}, \{3\}, \{4, 8\}, \{-4, 7\}, \{-5, 6\}, \{-7, -8\}.$$
8. The group $G(T_8)$ partitions the set $PG(1,17) \setminus T_8$ into eleven orbits; they are
$$\{-2\}, \{3\}, \{4\}, \{-4\}, \{5\}, \{-5\}, \{-6\}, \{7\}, \{-7\}, \{8\}, \{-8\}.$$

9. The group $G(T_9)$ partitions the set $PG(1,17) \setminus T_9$ into six orbits; they are

$$\{-2,7\}, \{3,-8\}, \{4,-5\}, \{-4,8\}, \{5\}, \{6,-6\}.$$

10. The group $G(T_{10})$ partitions the set $PG(1,17) \setminus T_{10}$ into six orbits; they are

$$\{-2,6\}, \{3\}, \{-3,-5\}, \{4,-6\}, \{5,8\}, \{7,-8\}.$$

Therefore, 75 octads can be formed (the total number of all orbits) by adding one point from each orbit to the corresponding heptad. In Tables 3.8 we list the additional points to the heptads.

Tab. 3.8: The additional points to the heptads

Symbol	Canonical form	The additional points
T_1	$\{\infty,0,1,-1,2,-2,-3\}$	$-4,4,5,-7,-8,8$
T_2	$\{\infty,0,1,-1,2,-2,-8\}$	$3,[-3],4,-4,5,-5,6,-6,7,-7,8$
T_3	$\{\infty,0,1,-1,2,-2,6\}$	$3,-3,[-8],-4,-6,-7$
T_4	$\{\infty,0,1,-1,2,-2,-7\}$	$3,[-3],4,[-8],[6],7$
T_5	$\{\infty,0,1,-1,2,-3,4\}$	$[-2],5,6,-6,-7,-8$
T_6	$\{\infty,0,1,-1,2,-3,-4\}$	$[-2],3,4,5,-5,6,-6,7,-7,8,-8$
T_7	$\{\infty,0,1,-1,2,-3,5\}$	$[-2],3,[4],[-4],6,-7$
T_8	$\{\infty,0,1,-1,2,-3,6\}$	$[-2],3,[4],[-4],[5],-5,-6,7,-7,8,-8$
T_9	$\{\infty,0,1,-1,2,-3,-7\}$	$[-2],3,[4],[-4],[5],[6]$
T_{10}	$\{\infty,0,1,-1,2,-4,-7\}$	$-2,3,[-3],4,5,7$

The number of octads constructed is 55, since each point in square brackets gives an identical octad to one already included.

Remark 3.6. The numbers of octads and their stabilizers are given in Table 3.9.

Tab. 3.9: The stabilizers of octads

Stabilizer	I	$\mathbf{Z_2} \times \mathbf{Z_2}$	$\mathbf{Z_2}$	$\mathbf{D_4}$
Number	20	6	27	2

According to the types of the eight heptads, the octads fall into 17 sets. This gives the following conclusion.

Theorem 3.7. *On $PG(1,17)$ there are precisely 17 projectively distinct octads, given in Table 3.10.*

Tab. 3.10: The distinct octads

Symbol	Canonical form	Type of heptad	Stabilizer
O_1	$\{\infty,0,1,-1,2,-2,-3,-4\}$	$T_1T_2T_6T_1T_{10}T_2T_6T_5$	$\mathbf{Z_2}=\langle\frac{-x-2}{1}\rangle$
O_2	$\{\infty,0,1,-1,2,-2,-3,4\}$	$T_1T_2T_5T_1T_2T_5T_2T_2$	$\mathbf{Z_2}=\langle\frac{x+3}{-x-1}\rangle$
O_3	$\{\infty,0,1,-1,2,-2,-3,5\}$	$T_1T_1T_7T_3T_7T_3T_{10}T_{10}$	$\mathbf{Z_2}=\langle\frac{2}{x}\rangle$
O_4	$\{\infty,0,1,-1,2,-2,-3,-7\}$	$T_1T_4T_9T_3T_6T_8T_6T_8$	$I=\langle x\rangle$
O_5	$\{\infty,0,1,-1,2,-2,-3,-8\}$	$T_1T_2T_2T_4T_6T_6T_1T_4$	$\mathbf{Z_2}=\langle\frac{2x-1}{x-2}\rangle$
O_6	$\{\infty,0,1,-1,2,-2,-3,8\}$	$T_1T_2T_8T_2T_7T_8T_7T_9$	$\mathbf{Z_2}=\langle\frac{-x-1}{1}\rangle$
O_7	$\{\infty,0,1,-1,2,-2,-8,-4\}$	$T_2T_2T_2T_9T_9T_2T_9T_9$	$\mathbf{Z_2}\times\mathbf{Z_2}=\langle\frac{-x+2}{x+1},\frac{x+1}{-8x-1}\rangle$
O_8	$\{\infty,0,1,-1,2,-2,-8,6\}$	$T_2T_3T_2T_4T_5T_6T_6T_{10}$	$I=\langle x\rangle$
O_9	$\{\infty,0,1,-1,2,-2,-8,-6\}$	$T_2T_3T_2T_8T_6T_6T_8T_3$	$\mathbf{Z_2}=\langle\frac{-x+2}{-2x+1}\rangle$
O_{10}	$\{\infty,0,1,-1,2,-2,-8,7\}$	$T_2T_4T_2T_{10}T_8T_{10}T_8T_4$	$\mathbf{Z_2}=\langle\frac{x+1}{2x-1}\rangle$
O_{11}	$\{\infty,0,1,-1,2,-2,-8,8\}$	$T_2T_2T_2T_2T_7T_7T_3T_3$	$\mathbf{Z_2}\times\mathbf{Z_2}=\langle\frac{1}{x},\frac{-1}{x}\rangle$
O_{12}	$\{\infty,0,1,-1,2,-2,6,-7\}$	$T_3T_4T_5T_9T_9T_5T_8T_8$	$I=\langle x\rangle$
O_{13}	$\{\infty,0,1,-1,2,-2,-7,7\}$	$T_4T_4T_4T_4T_4T_4T_4T_4$	$\mathbf{D_8}=\langle\frac{-x+7}{5x+1},\frac{x+2}{x+1}\rangle$
O_{14}	$\{\infty,0,1,-1,2,-3,4,5\}$	$T_5T_7T_6T_8T_7T_8T_{10}T_6$	$I=\langle x\rangle$
O_{15}	$\{\infty,0,1,-1,2,-3,-4,5\}$	$T_6T_7T_7T_6T_7T_6T_6T_7$	$\mathbf{Z_2}\times\mathbf{Z_2}=\langle\frac{x-5}{-x-1},\frac{-x+1}{-4x+1}\rangle$
O_{16}	$\{\infty,0,1,-1,2,-3,-4,-7\}$	$T_6T_9T_{10}T_{10}T_8T_9T_6T_8$	$\mathbf{Z_2}=\langle\frac{x+7}{-x-1}\rangle$
O_{17}	$\{\infty,0,1,-1,2,-3,6,8\}$	$T_8T_8T_8T_8T_8T_8T_8T_8$	$\mathbf{D_4}=\langle\frac{x+1}{-x+1},\frac{2x+1}{x-2}\rangle$

3.7 The nonads

1. The group $G(O_1)$ partitions the set $PG(1,17) \setminus O_1$ into five orbits; they are
$$\{3,-5\},\{4,-6\},\{5,-7\},\{6,-8\},\{7,8\}.$$
2. The group $G(O_2)$ partitions the set $PG(1,17) \setminus O_2$ into six orbits; they are
$$\{3,7\},\{-4,-6\},\{5,-7\},\{-5,8\},\{6\},\{8\}.$$
3. The group $G(O_3)$ partitions the set $PG(1,17) \setminus O_3$ into six orbits; they are
$$\{3,-5\},\{4,-8\},\{-4,8\},\{6\},\{-6\},\{7,-7\}.$$
4. The group $G(O_6)$ partitions the set $PG(1,17) \setminus O_6$ into ten orbits; they are
$$\{3\},\{4\},\{-4\},\{5\},\{-5\},\{6\},\{-6\},\{7\},\{8\},\{-8\}.$$
5. The group $G(O_5)$ partitions the set $PG(1,17) \setminus O_5$ into five orbits; they are
$$\{3,5\},\{4,-5\},\{-4,-7\},\{6,7\},\{-6,8\}.$$
6. The group $G(O_5)$ partitions the set $PG(1,17) \setminus O_5$ into five orbits; they are
$$\{3,-4\},\{4,-5\},\{5,-6\},\{6,-7\},\{7,-8\}.$$
7. The group $G(O_7)$ partitions the set $PG(1,17) \setminus O_7$ into three orbits; they are
$$\{-3,-5,6,-6\},\{3,4,5,8\},\{7,-7\}.$$
8. The group $G(O_8)$ partitions the set $PG(1,17) \setminus O_8$ into ten orbits; they are
$$\{-3\},\{3\},\{4\},\{-4\},\{5\},\{-5\},\{-6\},\{7\},\{-7\},\{8\}.$$
9. The group $G(O_9)$ partitions the set $PG(1,17) \setminus O_9$ into five orbits; they are
$$\{-3,8\},\{3,7\},\{4,-7\},\{-4,-5\},\{5,6\}.$$
10. The group $G(O_{10})$ partitions the set $PG(1,17) \setminus O_{10}$ into five orbits; they are
$$\{-3,-7\},\{3,-6\},\{4,8\},\{-4,6\},\{5,-5\}.$$
11. The group $G(O_{11})$ partitions the set $PG(1,17) \setminus O_{11}$ into three orbits; they are
$$\{3,-3,6,-6\},\{4,-4\},\{5,-5,7,-7\}.$$

12. The group $G(O_{12})$ partitions the set $PG(1,17) \setminus O_{12}$ into ten orbits; they are

$$\{3\}, \{-3\}, \{4\}, \{-4\}, \{5\}, \{-5\}, \{-6\}, \{7\}, \{8\}, \{-8\}.$$

13. The group $G(O_{13})$ partitions the set $PG(1,17) \setminus O_{13}$ into two orbits; they are

$$\{3, -3, 4, -4, 5, -5, 8, -8\}, \{6, -6\}.$$

14. The group $G(O_{14})$ partitions the set $PG(1,17) \setminus O_{14}$ into ten orbits; they are

$$\{-2\}, \{3\}, \{-4\}, \{-5\}, \{6\}, \{-6\}, \{7\}, \{-7\}, \{8\}, \{-8\}.$$

15. The group $G(O_{15})$ partitions the set $PG(1,17) \setminus O_{15}$ into three orbits; they are

$$\{-2, -5, 6, -7\}, \{3, -6, 8, -8\}, \{4, 7\}.$$

16. The group $G(O_{16})$ partitions the set $PG(1,17) \setminus O_{16}$ into five orbits; they are

$$\{-2, 5\}, \{3, 6\}, \{4, 8\}, \{-5, -8\}, \{-6, 7\}.$$

17. The group $G(O_{17})$ partitions the set $PG(1,17) \setminus O_{17}$ into two orbits; they are

$$\{-2, 3, 5, -5, -6, 7, -7, -8\}, \{4, -4\}.$$

Therefore, 95 nonads can be formed (the total number of all orbits) by adding one point from each orbit to the corresponding octad. In Tables 3.11 we list the additional points to the octads.

Tab. 3.11: The additional points to the octads

Symbol	Canonical form	The additional points
O_1	$\{\infty,0,1,-1,2,-2,-3,-4\}$	$3,[4],[5],[-8],[8]$
O_2	$\{\infty,0,1,-1,2,-2,-3,4\}$	$3,[-4],[5],[8],6,[-8]$
O_3	$\{\infty,0,1,-1,2,-2,-3,5\}$	$3,[-8],[8],6,-6,[-7]$
O_4	$\{\infty,0,1,-1,2,-2,-3,-7\}$	$3,4,[-4],5,-5,[6],-6,[7],[8],[-8]$
O_5	$\{\infty,0,1,-1,2,-2,-3,-8\}$	$3,-5,-7,[6],[8]$
O_6	$\{\infty,0,1,-1,2,-2,-3,8\}$	$[-4],4,-6,-7,[-8]$
O_7	$\{\infty,0,1,-1,2,-2,-8,-4\}$	$[6],4,[7]$
O_8	$\{\infty,0,1,-1,2,-2,-8,6\}$	$-3,3,4,-4,5,-5,[-6],[7],[-7],8$
O_9	$\{\infty,0,1,-1,2,-2,-8,-6\}$	$8,[7],-7,-4,6$
O_{10}	$\{\infty,0,1,-1,2,-2,-8,7\}$	$-7,-6,[8],6,-5$
O_{11}	$\{\infty,0,1,-1,2,-2,-8,8\}$	$-3,-4,7$
O_{12}	$\{\infty,0,1,-1,2,-2,6,-7\}$	$3,-3,4,-4,5,-5,-6,[7],8,-8$
O_{13}	$\{\infty,0,1,-1,2,-2,-7,7\}$	$-3,6$
O_{14}	$\{\infty,0,1,-1,2,-3,4,5\}$	$-2,3,[-4],-5,6,-6,7,-7,8,-8$
O_{15}	$\{\infty,0,1,-1,2,-3,-4,5\}$	$[-7],8,4$
O_{16}	$\{\infty,0,1,-1,2,-3,-4,-7\}$	$5,6,4,-5,-6$
O_{17}	$\{\infty,0,1,-1,2,-3,6,8\}$	$-5,4$

The number of nonads constructed is 65, since each point in square brackets gives an identical nomad to one already included.

Remark 3.8. The numbers of nonads and their stabilizers are given in Table 3.12.

Tab. 3.12: The stabilizers of nonads

Stabilizer	I	$\mathbf{Z_2}$	$\mathbf{Z_3}$	$\mathbf{Z_4}$	$\mathbf{Z_8}$	$\mathbf{S_3}$	$\mathbf{D_9}$
Number	34	24	2	2	1	1	1

According to the types of the nine octads, the nonads fall into 17 sets. This gives the following conclusion.

Theorem 3.9. *On $PG(1, 17)$ there are precisely* 17 *projectively distinct nonads.*

Remark 3.10. The distinct nonads and the classification of complementary nonads are given in Tables 3.13 and 3.14.

Tab. 3.13: The distinct nonads

Symbol	Canonical form	Types of octad	Stabilizer
S_1	$\{\infty,0,1,-1,2,-2,-3,-4,3\}$	$O_1O_1O_2O_5O_2O_8O_5O_8O_2$	$\mathbf{Z_2}=\langle\frac{-x-1}{1}\rangle$
S_2	$\{\infty,0,1,-1,2,-2,-3,4,6\}$	$O_2O_4O_8O_{12}O_4O_9O_{12}O_8O_9$	$\mathbf{Z_2}=\langle\frac{x+3}{-x-1}\rangle$
S_3	$\{\infty,0,1,-1,2,-2,-3,5,3\}$	$O_3O_1O_2O_{11}O_8O_{14}O_9O_{10}O_8$	$I=\langle x\rangle$
S_4	$\{\infty,0,1,-1,2,-2,-3,5,6\}$	$O_3O_4O_4O_{14}O_{12}O_{14}O_{12}O_{16}O_{16}$	$\mathbf{Z_2}=\langle\frac{2}{x}\rangle$
S_5	$\{\infty,0,1,-1,2,-2,-3,5,-6\}$	$O_3O_3O_3O_3O_3O_3O_3O_3O_3$	$\mathbf{D_9}=\langle\frac{x-2}{x+2},\frac{-x-1}{1}\rangle$
S_6	$\{\infty,0,1,-1,2,-2,-3,-7,3\}$	$O_4O_1O_5O_7O_9O_8O_4O_{16}O_{12}$	$I=\langle x\rangle$
S_7	$\{\infty,0,1,-1,2,-2,-3,-7,4\}$	$O_4O_2O_{10}O_{12}O_3O_1O_{14}O_5O_6$	$I=\langle x\rangle$
S_8	$\{\infty,0,1,-1,2,-2,-3,-7,5\}$	$O_4O_3O_5O_6O_{11}O_{15}O_9O_8O_{14}$	$I=\langle x\rangle$
S_9	$\{\infty,0,1,-1,2,-2,-3,8,4\}$	$O_6O_2O_7O_{12}O_2O_{11}O_{12}O_6O_7$	$\mathbf{Z_2}=\langle\frac{-3x-5}{x+3}\rangle$
S_{10}	$\{\infty,0,1,-1,2,-2,-3,8,-6\}$	$O_6O_3O_8O_4O_1O_{14}O_{14}O_{15}O_{16}$	$I=\langle x\rangle$
S_{11}	$\{\infty,0,1,-1,2,-2,-3,8,-7\}$	$O_6O_4O_{10}O_{16}O_9O_{14}O_{17}O_{14}O_{12}$	$I=\langle x\rangle$
S_{12}	$\{\infty,0,1,-1,2,-2,-8,6,-3\}$	$O_8O_5O_4O_{10}O_{13}O_8O_4O_5O_{10}$	$\mathbf{Z_2}=\langle\frac{-2x-5}{x+2}\rangle$
S_{13}	$\{\infty,0,1,-1,2,-2,-8,7,6\}$	$O_{10}O_8O_{12}O_7O_8O_{12}O_{16}O_{16}O_{10}$	$\mathbf{Z_2}=\langle\frac{x-1}{3x-1}\rangle$
S_{14}	$\{\infty,0,1,-1,2,-2,6,-7,-3\}$	$O_{12}O_4O_4O_{12}O_{12}O_4O_{12}O_4O_{17}$	$\mathbf{Z_4}=\langle\frac{4x-7}{1}\rangle$
S_{15}	$\{\infty,0,1,-1,2,-2,6,-7,-8\}$	$O_{12}O_8O_8O_8O_{12}O_{12}O_{14}O_{14}O_{14}$	$\mathbf{Z_3}=\langle\frac{1}{-x+1}\rangle$
S_{16}	$\{\infty,0,1,-1,2,-2,-7,7,6\}$	$O_{13}O_{12}O_{12}O_{12}O_{12}O_{12}O_{12}O_{12}O_{12}$	$\mathbf{Z_8}=\langle\frac{x+2}{x+1}\rangle$
S_{17}	$\{\infty,0,1,-1,2,-3,-4,5,4\}$	$O_{15}O_{14}O_{14}O_{15}O_{14}O_{14}O_{14}O_{14}O_{15}$	$\mathbf{S_3}=\langle\frac{x+1}{-6x+7},\frac{-x+2}{6x+1}\rangle$

Tab. 3.14: The classification of complementary nonads

Symbol	Canonical form	Types of octad complement	Stabilizer
S'_1	$\{4,5,-5,6,-6,7,-7,8,-8\}$	$O_5O_2O_1O_5O_8O_1O_2O_8O_2$	$\mathbf{Z_2} = \langle \frac{-x-1}{1} \rangle$
S'_2	$\{3,-4,5,-5,-6,7,-7,8,-8\}$	$O_2O_4O_{12}O_8O_9O_4O_{12}O_9O_8$	$\mathbf{Z_2} = \langle \frac{x+3}{-x-1} \rangle$
S'_3	$\{4,-4,-5,6,-6,7,-7,8,-8\}$	$O_{10}O_1O_8O_9O_3O_{14}O_{11}O_8O_2$	$I = \langle x \rangle$
S'_4	$\{3,4,-4,-5,-6,7,-7,8,-8\}$	$O_{12}O_{16}O_4O_4O_3O_{14}O_{16}O_{12}O_{14}$	$\mathbf{Z_2} = \langle \frac{2}{x} \rangle$
S'_5	$\{3,4,-4,-5,6,7,-7,8,-8\}$	$O_3O_3O_3O_3O_3O_3O_3O_3O_3$	$\mathbf{D_9} = \langle \frac{x-2}{x+2}, \frac{-x-1}{1} \rangle$
S'_6	$\{4,-4,5,-5,6,-6,7,8,-8\}$	$O_4O_{12}O_7O_{16}O_4O_9O_8O_1O_5$	$I = \langle x \rangle$
S'_7	$\{3,-4,5,-5,6,-6,7,8,-8\}$	$O_1O_{10}O_2O_{14}O_{12}O_4O_6O_3O_5$	$I = \langle x \rangle$
S'_8	$\{3,4,-4,-5,6,-6,7,8,-8\}$	$O_5O_{14}O_{11}O_3O_4O_9O_{15}O_6O_8$	$I = \langle x \rangle$
S'_9	$\{3,-4,5,-5,6,-6,7,-7,-8\}$	$O_5O_{10}O_8O_8O_4O_{13}O_4O_{10}O_5$	$\mathbf{Z_2} = \langle \frac{-3x-5}{x+3} \rangle$
S'_{10}	$\{3,4,-4,5,-5,6,7,-7,-8\}$	$O_{15}O_{16}O_{14}O_{14}O_4O_3O_1O_8O_6$	$I = \langle x \rangle$
S'_{11}	$\{3,4,-4,5,-5,6,-6,7,-8\}$	$O_9O_6O_{16}O_{17}O_4O_{14}O_{14}O_{10}O_{12}$	$I = \langle x \rangle$
S'_{12}	$\{3,4,-4,5,-5,-6,7,-7,8\}$	$O_6O_{12}O_7O_{11}O_2O_{12}O_7O_2O_6$	$\mathbf{Z_2} = \langle \frac{-2x-5}{x+2} \rangle$
S'_{13}	$\{3,-3,4,-4,5,-5,-6,-7,8\}$	$O_8O_{12}O_{10}O_{10}O_{12}O_{16}O_8O_7O_{16}$	$\mathbf{Z_2} = \langle \frac{x-1}{3x-1} \rangle$
S'_{14}	$\{3,4,-4,5,-5,-6,7,8,-8\}$	$O_{12}O_{17}O_{12}O_4O_{12}O_4O_4O_{12}O_4$	$\mathbf{Z_4} = \langle \frac{4x-7}{1} \rangle$
S'_{15}	$\{3,-3,4,-4,5,-5,-6,7,8\}$	$O_{14}O_{12}O_8O_{14}O_8O_{12}O_8O_{12}O_{14}$	$\mathbf{Z_3} = \langle \frac{1}{-x+1} \rangle$
S'_{16}	$\{3,-3,4,-4,5,-5,-6,8,-8\}$	$O_{12}O_{12}O_{13}O_{12}O_{12}O_{12}O_{12}O_{12}O_{12}$	$\mathbf{Z_8} = \langle \frac{x+2}{x+1} \rangle$
S'_{17}	$\{-2,3,-5,6,-6,7,-7,8,-8\}$	$O_{15}O_{15}O_{14}O_{15}O_{14}O_{14}O_{14}O_{14}O_{14}$	$\mathbf{S_3} = \langle \frac{x+1}{-6x+7}, \frac{-x+2}{6x+1} \rangle$

3.8 The partitions of $PG(1,17)$

The stabilizer $G(S_i)$ of S_i also fixes the complement S_i'. The nonad S_i is projectively equivalent to its complement S_i', except that S_9 is not equivalent to S_9' and S_{12} is inequivalent to S_{12}'.

This gives the following result on partitions into nonads.

Theorem 3.11. *The projective line $PG(1,17)$ has 17 projectively distinct partitions into two equivalent nonads given by Table 3.15.*

Tab. 3.15: Partitions of $PG(1,17)$ into two nonads

No.	Symbol	Stabilizer of partition
1	$\{S_1; S'_1\}$	$\mathbf{Z_2} \times \mathbf{Z_2} = \langle \frac{8x-6}{x-8}, \frac{-x-1}{1} \rangle$
2	$\{S_2; S'_2\}$	$\mathbf{Z_2} \times \mathbf{Z_2} = \langle \frac{x-3}{4x-1}, \frac{x+3}{-x-1} \rangle$
3	$\{S_3; S'_3\}$	$\mathbf{Z_2} = \langle \frac{-x-8}{5x+1} \rangle$
4	$\{S_4; S'_4\}$	$\mathbf{Z_2} \times \mathbf{Z_2} = \langle \frac{-x-4}{2x+1}, \frac{2}{x} \rangle$
5	$\{S_5; S'_5\}$	$\mathbf{D_{18}} = \langle \frac{5x+2}{7x-5}, \frac{-x-1}{1} \rangle$
6	$\{S_6; S'_6\}$	$\mathbf{Z_2} = \langle \frac{-x-6}{2x+1} \rangle$
7	$\{S_7; S'_7\}$	$\mathbf{Z_2} = \langle \frac{x-3}{7x-1} \rangle$
8	$\{S_8; S'_8\}$	$\mathbf{Z_2} = \langle \frac{-x+3}{2x+1} \rangle$
9	$\{S_9; S'_{12}\}$	$\mathbf{Z_2} = \langle \frac{x-3}{4x-1} \rangle$
10	$\{S_{10}; S'_{10}\}$	$\mathbf{Z_2} = \langle \frac{-x-8}{5x+1} \rangle$
11	$\{S_{11}; S'_{11}\}$	$\mathbf{Z_2} = \langle \frac{3x+2}{x-3} \rangle$
12	$\{S_{12}; S'_9\}$	$\mathbf{Z_2} = \langle \frac{x-3}{4x-1} \rangle$
13	$\{S_{13}; S'_{13}\}$	$\mathbf{Z_2} \times \mathbf{Z_2} = \langle \frac{-x+3}{7x+1}, \frac{x-1}{3x-1} \rangle$
14	$\{S_{14}; S'_{14}\}$	$\mathbf{D_4} = \langle \frac{8x-6}{x-8}, \frac{4x-7}{1} \rangle$
15	$\{S_{15}; S'_{15}\}$	$\mathbf{S_3} = \langle \frac{-x+3}{2x+1}, \frac{1}{-x+1} \rangle$
16	$\{S_{16}; S'_{16}\}$	$\mathbf{D_8} = \langle \frac{4x+2}{-x-4}, \frac{x+2}{x+1} \rangle$
17	$\{S_{17}; S'_{17}\}$	$\mathbf{D_6} = \langle \frac{4x+8}{3x+1}, \frac{-x+2}{6x+1} \rangle$

In Table 3.15, we note that, for the stabilizer groups which are generated by two elements, the first generator transforms the nonad to its complement, while the second generator fixes the nonad and its complement.

3.9 Transformations between the nonads and their complements

1. $S_1 \longrightarrow S'_1$ by $\frac{8x-6}{x-8}$,
2. $S_2 \longrightarrow S'_2$ by $\frac{x-3}{4x-1}$,
3. $S_3 \longrightarrow S'_3$ by $\frac{-x-8}{5x+1}$,
4. $S_4 \longrightarrow S'_4$ by $\frac{-x-4}{2x+1}$,
5. $S_5 \longrightarrow S'_5$ by $\frac{3x+4}{-2x+1}$,
6. $S_6 \longrightarrow S'_6$ by $\frac{-x-6}{2x+1}$,
7. $S_7 \longrightarrow S'_7$ by $\frac{x-3}{7x-1}$,
8. $S_8 \longrightarrow S'_8$ by $\frac{-x+3}{2x+1}$,
9. $S_9 \longrightarrow S'_{12}$ by $\frac{x-3}{4x-1}$,
10. $S_{10} \longrightarrow S'_{10}$ by $\frac{-x-8}{5x+1}$,
11. $S_{11} \longrightarrow S'_{11}$ by $\frac{3x+2}{x-3}$,
12. $S_{12} \longrightarrow S'_9$ by $\frac{x-3}{4x-1}$,
13. $S_{13} \longrightarrow S'_{13}$ by $\frac{-x+3}{7x+1}$,
14. $S_{14} \longrightarrow S'_{14}$ by $\frac{8x-6}{x-8}$,
15. $S_{15} \longrightarrow S'_{15}$ by $\frac{-x+3}{2x+1}$,
16. $S_{16} \longrightarrow S'_{16}$ by $\frac{4x+2}{-x-4}$,
17. $S_{17} \longrightarrow S'_{17}$ by $\frac{4x+8}{3x+1}$.

3.10 Links with Coding Theory

From Definition 2.47, an $[n, k, d]$ code is *maximum distance separable (MDS)* when

$$d = n - k + 1.$$

In the case that $k = 2$ and $d = n - 1$ of an $[n, k, d]$ code, the code C converts to a set K of n points on the line $PG(1, q)$.

The parameters n, k and d for tetrads, pentads, hexads, heptads, octads, and nonads in $PG(1, q)$ and the number e of errors that can be corrected are given in Table 3.16.

Tab. 3.16: The parameters n, k, d and e on $PG(1, 17)$

Type	n	k	d	e
tetrad	4	2	3	1
pentad	5	2	4	1
hexad	6	2	5	2
heptad	7	2	6	2
octad	8	2	7	3
nonad	9	2	8	3

4. THE PROJECTIVE PLANE $PG(2, 17)$

4.1 Introduction

In $PG(2, 17)$, the projective plane of order 17, $\theta_1 = 18$, $\theta_2 = 307$, where

$$\theta_n = |PG(n, q)| = (q^{n+1} - 1)/(q - 1);$$

hence we have 307 points, 307 lines, 18 points on each line and 18 lines passing through each point.

From Table 7.1, we may choose the points with the third coordinate equal to zero. They form the following difference set:

$$1 \quad 2 \quad 4 \quad 46 \quad 59 \quad 63 \quad 74 \quad 97 \quad 111 \quad 123 \quad 143 \quad 150 \quad 179 \quad 197 \quad 268 \quad 278 \quad 287 \quad 303$$

Hence a regular array giving the lines of $PG(2, 17)$ is as follows:

$$\begin{array}{cccccccccccccccccc}
1 & 2 & 4 & 46 & 59 & 63 & 74 & 97 & 111 & 123 & 143 & 150 & 179 & 197 & 268 & 278 & 287 & 303 \\
2 & 3 & 5 & 47 & 60 & 64 & 75 & 98 & 112 & 124 & 144 & 151 & 180 & 198 & 269 & 279 & 288 & 304 \\
3 & 4 & 6 & 48 & 61 & 65 & 76 & 99 & 113 & 125 & 145 & 152 & 181 & 199 & 270 & 280 & 289 & 305 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
307 & 1 & 3 & 45 & 58 & 62 & 73 & 96 & 110 & 122 & 142 & 149 & 178 & 196 & 267 & 277 & 286 & 302
\end{array}$$

Each row represents one of the 307 lines of $PG(2, 17)$.

By the Fundamental Theorem of Projective Geometry, any four points, no three collinear, can be mapped projectively to any other four points, no three collinear.

4.2 Stabilizer of the frame

The stabilizer of any 4-arc is the group of 24 projectivities found by shifting the 4-arc to its 24 permutations. Table 4.1 contains the stabilizer (it is isomorphic to $\mathbf{S_4}$) of the frame for $PG(2,q)$.

The matrix determining each elements of the $\mathbf{S_4}$ is given by its rows. Let the numeral form of the frame for $PG(2,q)$ be a,b,c and d; that is $a=(1,0,0)$, $b=(0,1,0)$, $c=(0,0,1)$ and $d=(1,1,1)$. The stabilizer of the frame are given in Table 4.1.

Tab. 4.1: The stabilizer of the frame

$\{a\,b\,c\,d\}$	1	0	0	0	1	0	0	0	1	
$\{b\,a\,c\,d\}$	0	1	0	1	0	0	0	0	1	g_1
$\{c\,b\,a\,d\}$	0	0	1	0	1	0	1	0	0	
$\{d\,b\,c\,a\}$	1	1	1	0	-1	0	0	0	-1	
$\{a\,c\,b\,d\}$	1	0	0	0	0	1	0	1	0	
$\{a\,d\,c\,b\}$	-1	0	0	1	1	1	0	0	-1	
$\{a\,b\,d\,c\}$	-1	0	0	0	-1	0	1	1	1	
$\{c\,a\,b\,d\}$	0	1	0	0	0	1	1	0	0	
$\{d\,a\,c\,b\}$	0	-1	0	1	1	1	0	0	-1	
$\{b\,c\,a\,d\}$	0	0	1	1	0	0	0	1	0	
$\{d\,b\,a\,c\}$	0	0	-1	0	-1	0	1	1	1	
$\{b\,d\,c\,a\}$	1	1	1	-1	0	0	0	0	-1	
$\{c\,b\,d\,a\}$	1	1	1	0	-1	0	-1	0	0	
$\{a\,d\,b\,c\}$	-1	0	0	0	0	-1	1	1	1	
$\{a\,c\,d\,b\}$	-1	0	0	1	1	1	0	-1	0	

$\{d\,a\,b\,c\}$	0	-1	0	0	0	-1	1	1	1	g_2
$\{c\,a\,d\,b\}$	0	-1	0	1	1	1	-1	0	0	
$\{d\,c\,a\,b\}$	0	0	-1	1	1	1	0	-1	0	
$\{b\,d\,a\,c\}$	0	0	-1	-1	0	0	1	1	1	
$\{c\,d\,b\,a\}$	1	1	1	0	0	-1	-1	0	0	
$\{b\,c\,d\,a\}$	1	1	1	-1	0	0	0	-1	0	
$\{b\,a\,d\,c\}$	0	-1	0	-1	0	0	1	1	1	
$\{c\,d\,a\,b\}$	0	0	-1	1	1	1	-1	0	0	
$\{d\,c\,b\,a\}$	1	1	1	0	0	-1	0	-1	0	

The frame points in $PG(2,17)$ are $1,2,3,254$. The two projectivities g_1 and g_2 which generate $\mathbf{S_4}$, the stabilizer of the frame, partitions the points in $PG(2,17)$ into 21 disjoint orbits as follows.

(1) $111, 112, 122$.

(2) $1, 2, 3, 254$.

(3) $90, 145, 155, 171, 214, 253$.

(4) $107, 197, 198, 221, 274, 307$.

(5) $4, 5, 63, 64, 73, 74, 132, 133, 211, 222, 230, 286$.

(6) $6, 17, 91, 92, 96, 123, 124, 208, 228, 278, 279, 302$.

(7) $9, 23, 49, 94, 106, 114, 131, 152, 169, 173, 245, 248$.

(8) $19, 28, 41, 50, 81, 147, 184, 210, 227, 233, 262, 289$.

(9) $21, 59, 60, 86, 93, 157, 170, 178, 242, 267, 303, 304$.

(10) $40, 46, 47, 54, 72, 149, 177, 185, 196, 268, 269, 281$.

(11) $44, 52, 71, 153, 156, 159, 191, 207, 225, 260, 294, 301$.

(12) $45, 66, 74, 75, 82, 179, 180, 190, 194, 234, 246, 277$.

(13) $58, 62, 97, 98, 115, 127, 135, 140, 150, 151, 261, 296$.

(14) $102, 110, 113, 142, 143, 144, 205, 251, 252, 287, 288, 290$.

(15) $7, 33, 39, 55, 68, 85, 95, 119, 125, 126, 128, 139, 175, 192,$
$193, 213, 218, 235, 255, 270, 276, 280, 293, 299$.

(16) $8, 16, 20, 22, 26, 27, 48, 51, 57, 65, 67, 77, 78, 83, 87, 116,$
$161, 195, 217, 240, 241, 256, 272, 300$.

(17) $10, 11, 15, 29, 36, 43, 61, 100, 108, 117, 118, 134, 148, 160,$
$162, 165, 166, 212, 236, 243, 244, 271, 295, 298$.

(18) $12, 14, 32, 42, 53, 70, 89, 104, 120, 146, 167, 176, 183, 187,$
$188, 200, 219, 247, 259, 263, 264, 283, 291, 305$.

(19) $13, 31, 38, 69, 79, 80, 101, 121, 129, 138, 154, 158, 172, 199,$
$203, 215, 216, 231, 232, 237, 239, 266, 285, 306$.

(20) $18, 24, 34, 35, 37, 56, 84, 99, 130, 163, 164, 181, 189, 202, 209,$
$223, 224, 226, 229, 249, 250, 273, 275, 297$.

(21) $25, 30, 76, 88, 103, 105, 109, 136, 137, 141, 168, 182, 186, 201,$
$204, 206, 220, 238, 257, 258, 265, 282, 284, 292$.

The first orbit consists of *diagonal points* and the second orbit is the set of the *frame points*.

4.3 The 5-arcs

Let K be a k-arc in $PG(2, q)$. For $k = 4$, the equations in Lemma 2.25 become

$$\begin{aligned} c_0 &= (q-2)(q-3), \\ c_1 &= 6(q-2), \\ c_2 &= 3; \end{aligned}$$

Another way of calculating c_0 is by listing the points not on the bisecants of the 4-arc. The points represented by the number c_0 are separated into orbits. Then 5-arcs are constructed by adding one point from each orbit. This gives the following result.

Theorem 4.1. *In $PG(2, 17)$ there are precisely four projectively distinct 5-arcs, given in Table 4.2.*

Tab. 4.2: The distinct 5-arcs

Symbol	5-arc	Stabilizer
A_1	$\{1, 2, 3, 254, 7\}$	$\mathbf{Z_4}$
A_2	$\{1, 2, 3, 254, 8\}$	$\mathbf{Z_2}$
A_3	$\{1, 2, 3, 254, 10\}$	$\mathbf{Z_2}$
A_4	$\{1, 2, 3, 254, 12\}$	$\mathbf{Z_2}$

4.4 The 6-arcs

The number of the points on the bisecant of any 5-arc is $L(5, q) = 10q - 20$; that is, 150 for $q = 17$. Hence there are $307 - 150 = 157$ points of the plane not on the bisecants of any of the four 5-arcs. Let K be a k-arc in $PG(2, q)$. For $k = 5$, the equations in Lemma 2.25 become

$$\begin{aligned} c_0 &= (q-4)(q-5)+1, \\ c_1 &= 10(q-4), \\ c_2 &= 15; \end{aligned}$$

Another way of calculating c_0 is by listing the points not on the bisecants of the 5-arc. The points represented by the number c_0 are separated into orbits. Then 6-arcs are constructed by adding one point from each orbit. For a specific 5-arc, points of index zero are divided into orbits by the stabilizer of that 5-arc. The points of index zero for every 5-arc as a number of orbits with the size of the orbits in brackets are given in Table 4.3.

Tab. 4.3: The orbits

5-arc	c_0	Orbits
A_1	157	$36(4), 6(2), 1(1)$
A_2	157	$72(2), 13(1)$
A_3	157	$72(2), 13(1)$
A_4	157	$72(2), 13(1)$

We list in Table 4.4 the four distinct 5-arcs and the points added to the corresponding 5-arc chosen from each orbit to construct 6-arcs.

Tab. 4.4: The points of index zero

5-arc	The additional points
A_1	$11, 12, 13, 14, 16, 19, 20, 22, 23, 24, 25, 26, 28, 29, 30, 31, 35, 37, 39, 42, 43, 48, 56, 71,$ $76, 77, 85, 88, 95, 100, 101, 105, 120, 121, 130, 139, 158, 159, 160, 164, 165, 233, 270.$
A_2	$12, 13, 14, 15, 16, 18, 20, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 41, 44, 48, 49,$ $50, 51, 61, 71, 76, 77, 78, 79, 84, 87, 89, 90, 94, 99, 101, 105, 106, 114, 116, 125, 128, 137, 138,$ $139, 141, 146, 147, 148, 152, 153, 154, 155, 158, 162, 163, 168, 171, 172, 176, 181, 182, 184,$ $188, 189, 191, 192, 200, 201, 209, 210, 212, 214, 219, 227, 229, 235, 244, 247, 299.$
A_3	$9, 11, 12, 13, 15, 16, 18, 19, 20, 22, 23, 24, 27, 28, 29, 30, 33, 35, 37, 38, 41, 43, 44, 49, 51, 55, 56$ $61, 67, 68, 70, 71, 77, 79, 81, 83, 84, 87, 95, 99, 100, 106, 109, 114, 118, 121, 125, 126, 131, 134$ $137, 152, 154, 155, 158, 159, 160, 161, 162, 164, 165, 167, 172, 175, 176, 181, 183, 184, 187, 188$ $189, 193, 204, 210, 215, 224, 225, 236, 249, 250, 253, 256, 263, 275, 292.$
A_4	$[7], [8], 9, [10], 11, 13, 14, 15, 16, 18, 19, 20, 23, 25, 26, 27, 29, 30, 31, 38, 39, 41, 48, 50, 52, 53, 56$ $57, 65, 67, 68, 69, 70, 76, 77, 79, 83, 85, 89, 90, 94, 99, 101, 105, 108, 109, 114, 116, 120, 130, 131$ $134, 136, 137, 139, 141, 145, 148, 153, 154, 162, 166, 167, 171, 172, 176, 181, 183, 203, 213, 215$ $217, 218, 219, 224, 226, 227, 235, 237, 243, 255, 258, 259, 264, 265.$

So far, the number of 6-arcs constructed is 295, since each point in square brackets gives an identical 6-arc to one already included. The method to compute the transformations between the 6-arcs is the following; By use of The Fundamental Theorem of Projective Geometry there is a unique projectivity of $PG(2, q)$ transforming four points no three on a line to any other four points no three on a line. Two 6-arcs K_1 and K_2 are equivalent if $K_1\beta = K_2$ and β is given by a matrix $\mathbf{T}$ and $\beta = \mathbf{M}(\mathbf{T})$ with

$$\mathbf{M}(\lambda\mathbf{T}) = \mathbf{M}(\mathbf{T}),\ \lambda \in \mathbb{F}_{17} \setminus \{0\}.$$

This gives the following result.

Theorem 4.2. *In $PG(2, 17)$ there are precisely 74 projectively distinct 6-arcs, given in Table 4.5.*

Tab. 4.5: Distinct 6-arcs

No.	6-arc	Stabilizer	No.	6-arc	Stabilizer
B_1	$\{1,2,3,254,7,14\}$	$\mathbf{Z_2}$	B_{19}	$\{1,2,3,254,7,24\}$	I
B_2	$\{1,2,3,254,7,42\}$	I	B_{20}	$\{1,2,3,254,7,25\}$	I
B_3	$\{1,2,3,254,7,85\}$	$\mathbf{Z_2}$	B_{21}	$\{1,2,3,254,7,26\}$	I
B_4	$\{1,2,3,254,7,270\}$	$\mathbf{S_4}$	B_{22}	$\{1,2,3,254,7,29\}$	I
B_5	$\{1,2,3,254,8,24\}$	$\mathbf{Z_2}$	B_{23}	$\{1,2,3,254,7,30\}$	$\mathbf{Z_2}$
B_6	$\{1,2,3,254,8,34\}$	$\mathbf{Z_2}\times\mathbf{Z_2}$	B_{24}	$\{1,2,3,254,7,31\}$	$\mathbf{Z_2}$
B_7	$\{1,2,3,254,8,99\}$	$\mathbf{Z_2}$	B_{25}	$\{1,2,3,254,7,37\}$	$\mathbf{Z_2}$
B_8	$\{1,2,3,254,8,154\}$	$\mathbf{Z_2}\times\mathbf{Z_2}$	B_{26}	$\{1,2,3,254,7,39\}$	I
B_9	$\{1,2,3,254,10,236\}$	$\mathbf{D_6}$	B_{27}	$\{1,2,3,254,7,43\}$	I
B_{10}	$\{1,2,3,254,12,183\}$	$\mathbf{S_3}$	B_{28}	$\{1,2,3,254,7,48\}$	$\mathbf{Z_2}$
B_{11}	$\{1,2,3,254,7,11\}$	I	B_{29}	$\{1,2,3,254,7,56\}$	I
B_{12}	$\{1,2,3,254,7,12\}$	I	B_{30}	$\{1,2,3,254,7,71\}$	I
B_{13}	$\{1,2,3,254,7,13\}$	$\mathbf{Z_3}$	B_{31}	$\{1,2,3,254,7,76\}$	$\mathbf{Z_3}$
B_{14}	$\{1,2,3,254,7,16\}$	I	B_{32}	$\{1,2,3,254,7,88\}$	I
B_{15}	$\{1,2,3,254,7,19\}$	I	B_{33}	$\{1,2,3,254,7,100\}$	I
B_{16}	$\{1,2,3,254,7,20\}$	I	B_{34}	$\{1,2,3,254,7,101\}$	$\mathbf{Z_2}$
B_{17}	$\{1,2,3,254,7,22\}$	I	B_{35}	$\{1,2,3,254,7,105\}$	I
B_{18}	$\{1,2,3,254,7,23\}$	I	B_{36}	$\{1,2,3,254,7,120\}$	$\mathbf{Z_2}$

B_{37}	$\{1,2,3,254,7,121\}$	I	B_{56}	$\{1,2,3,254,8,105\}$	$\mathbf{A_4}$
B_{38}	$\{1,2,3,254,7,130\}$	$\mathbf{S_3}$	B_{57}	$\{1,2,3,254,8,106\}$	$\mathbf{Z_3}$
B_{39}	$\{1,2,3,254,7,139\}$	$\mathbf{S_3}$	B_{58}	$\{1,2,3,254,8,141\}$	I
B_{40}	$\{1,2,3,254,7,158\}$	I	B_{59}	$\{1,2,3,254,8,152\}$	$\mathbf{Z_3}$
B_{41}	$\{1,2,3,254,7,159\}$	I	B_{60}	$\{1,2,3,254,8,176\}$	I
B_{42}	$\{1,2,3,254,7,160\}$	$\mathbf{Z_2}$	B_{61}	$\{1,2,3,254,8,181\}$	$\mathbf{S_3}$
B_{43}	$\{1,2,3,254,7,165\}$	I	B_{62}	$\{1,2,3,254,8,182\}$	$\mathbf{Z_3}$
B_{44}	$\{1,2,3,254,7,233\}$	$\mathbf{Z_2}$	B_{63}	$\{1,2,3,254,8,210\}$	$\mathbf{Z_4}$
B_{45}	$\{1,2,3,254,8,16\}$	I	B_{64}	$\{1,2,3,254,8,212\}$	I
B_{46}	$\{1,2,3,254,8,18\}$	I	B_{65}	$\{1,2,3,254,8,219\}$	I
B_{47}	$\{1,2,3,254,8,20\}$	I	B_{66}	$\{1,2,3,254,10,18\}$	$\mathbf{Z_3}$
B_{48}	$\{1,2,3,254,8,27\}$	$\mathbf{S_3}$	B_{67}	$\{1,2,3,254,10,43\}$	I
B_{49}	$\{1,2,3,254,8,35\}$	$\mathbf{Z_2}$	B_{68}	$\{1,2,3,254,10,81\}$	$\mathbf{Z_3}$
B_{50}	$\{1,2,3,254,8,36\}$	$\mathbf{Z_3}$	B_{69}	$\{1,2,3,254,10,121\}$	$\mathbf{Z_4}$
B_{51}	$\{1,2,3,254,8,50\}$	I	B_{70}	$\{1,2,3,254,10,164\}$	$\mathbf{Z_2}$
B_{52}	$\{1,2,3,254,8,76\}$	$\mathbf{Z_3}$	B_{71}	$\{1,2,3,254,10,172\}$	$\mathbf{A_4}$
B_{53}	$\{1,2,3,254,8,77\}$	$\mathbf{S_3}$	B_{72}	$\{1,2,3,254,10,263\}$	$\mathbf{S_3}$
B_{54}	$\{1,2,3,254,8,94\}$	$\mathbf{Z_2}$	B_{73}	$\{1,2,3,254,12,19\}$	$\mathbf{Z_2}$
B_{55}	$\{1,2,3,254,8,101\}$	$\mathbf{Z_4}$	B_{74}	$\{1,2,3,254,12,224\}$	$\mathbf{A_4}$

4.5 The 6-arcs on a conic

The ten distinct hexads on $PG(1,17)$ can be mapped to ten distinct 6-arcs on a conic. If the points $U_0=(1,0,0), U_1=(0,1,0), U_2=(0,0,1)$ are on the conic, then the general equation of the conic reduces to the following:

$$x_0x_1+a_0x_0x_2+a_1x_1x_2=0.$$

Therefore, $(a_0,a_1)=(-7,6),(-3,2),(-2,1),(-5,4)$ are the coefficients of the equations of the conics containing the respective four 5-arcs

$$\{U_0,U_1,U_2,U_3,U_4\},\{U_0,U_1,U_2,U_3,U_5\},\{U_0,U_1,U_2,U_3,U_6\},\{U_0,U_1,U_2,U_3,U_7\},$$

where

$$U_3=(1,1,1),U_4=(-8,-6,1),U_5=(-8,4,1),U_6=(-8,-5,1),U_7=(-7,6,1).$$

Substituting the point of each 6-arc in the corresponding conic shows the ten 6-arcs on a conic as given in Table 4.6.

Tab. 4.6: The distinct 6-arcs on a conic

New symbol	Conic	6-arcs	Stabilizers
B_1	$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$\{1, 2, 3, 254, 7, 14\}$	$\mathbf{Z_2}$
B_2	$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$\{1, 2, 3, 254, 7, 42\}$	I
B_3	$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$\{1, 2, 3, 254, 7, 85\}$	$\mathbf{Z_2}$
B_4	$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$\{1, 2, 3, 254, 7, 270\}$	$\mathbf{S_4}$
B_5	$x_0x_1 - 3x_0x_2 + 2x_1x_2$	$\{1, 2, 3, 254, 8, 24\}$	$\mathbf{Z_2}$
B_6	$x_0x_1 - 3x_0x_2 + 2x_1x_2$	$\{1, 2, 3, 254, 8, 34\}$	$\mathbf{Z_2} \times \mathbf{Z_2}$
B_7	$x_0x_1 - 3x_0x_2 + 2x_1x_2$	$\{1, 2, 3, 254, 8, 99\}$	$\mathbf{Z_2}$
B_8	$x_0x_1 - 3x_0x_2 + 2x_1x_2$	$\{1, 2, 3, 254, 8, 154\}$	$\mathbf{Z_2} \times \mathbf{Z_2}$
B_9	$x_0x_1 - 2x_0x_2 + x_1x_2$	$\{1, 2, 3, 254, 10, 236\}$	$\mathbf{D_6}$
B_{10}	$x_0x_1 - 5x_0x_2 + 4x_1x_2$	$\{1, 2, 3, 254, 12, 183\}$	$\mathbf{S_3}$

Remark 4.3. For the 74 distinct 6-arcs the B-points are given in Table 4.7.

Tab. 4.7: The B-points

6-arcs	B-points	c_3	6-arcs	B-points	c_3
B_1	63	1	B_{18}	–	0
B_2	–	0	B_{19}	111	1
B_3	122	1	B_{20}	–	0
B_4	$6, 64, 111, 222, 274, 302$	6	B_{21}	64	1
B_5	124	1	B_{22}	–	0
B_6	$211, 288$	2	B_{23}	$64, 112$	2
B_7	4	1	B_{24}	$222, 302$	2
B_8	$142, 228$	2	B_{25}	$63, 288$	2
B_9	$74, 93, 180, 230$	4	B_{26}	–	0
B_{10}	$45, 112, 246$	3	B_{27}	185	1
B_{11}	–	0	B_{28}	$6, 102$	2
B_{12}	122	1	B_{29}	112	1
B_{13}	$64, 122, 185$	3	B_{30}	149	1
B_{14}	102	1	B_{31}	$6, 112, 149$	3

B_{15}	252	1	B_{32}	185	1
B_{35}	185	1	B_{16}	111	1
B_{36}	$222, 302$	2	B_{17}	185	1
B_{37}	105	1	B_{33}	252	1
B_{38}	$112, 222, 252, 302$	4	B_{34}	$185, 274$	2
B_{39}	$123, 185, 222, 302$	4	B_{57}	$124, 150, 211$	3
B_{40}	111	1	B_{58}	112	1
B_{41}	$-$	0	B_{59}	$4, 66, 288$	3
B_{42}	$222, 302$	2	B_{60}	$-$	0
B_{43}	185	1	B_{61}	$4, 122, 142, 228$	4
B_{44}	$222, 302$	2	B_{62}	$157, 211, 274$	3
B_{45}	$-$	0	B_{63}	$142, 228$	2
B_{46}	66	1	B_{64}	247	1
B_{47}	$-$	0	B_{65}	$-$	0
B_{48}	$142, 228, 274, 288$	4	B_{66}	$111, 180, 290$	3
B_{49}	$142, 228$	2	B_{67}	185	1
B_{50}	$112, 149, 211$	3	B_{68}	$122, 290, 304$	3
B_{51}	124	1	B_{69}	$122, 149$	2
B_{52}	$4, 149, 157$	3	B_{70}	$111, 278$	2
B_{53}	$124, 142, 149, 228$	4	B_{71}	$74, 93, 112, 149, 274, 290$	6
B_{54}	$142, 228$	2	B_{72}	$74, 93, 122, 127$	4

B_{55}	$185, 274$	2	B_{73}	$135, 267$	2
B_{56}	$66, 112, 142, 150, 185, 228$	6	B_{74}	$112, 115, 135, 143, 211, 267$	6

4.6 The 7-arcs

Let K be a k-arc in $PG(2,q)$. For $k = 6$, the equations in Lemma 2.25 become

$$\begin{aligned} c_0 &= (q-7)^2 + 6 - c_3, \\ c_1 &= 3\{5(q-7) + c_3\}, \\ c_2 &= 3\{15 - c_3\}; \end{aligned}$$

The constant c_3 and hence c_0, c_1 and c_2 are calculated. Another way of calculating c_0 is by listing the points not on the bisecants of the 6-arc. The points represented by the number c_0 are separated into orbits. Then 7-arcs are constructed by adding one point from each orbit. The 6-arcs for each pair (c_0, c_3) are given in Table 4.8.

Tab. 4.8: (c_0, c_3)

6-arcs	c_3	c_0
$B_2, B_{11}, B_{18}, B_{20}, B_{22}, B_{26}, B_{33}, B_{41}, B_{45}, B_{47}, B_{60}, B_{65}$	0	106
$B_1, B_3, B_5, B_7, B_{12}, B_{14}, B_{15}, B_{16}, B_{17}, B_{19}, B_{21}, B_{27}, B_{29}, B_{30}, B_{32}, B_{35}, B_{37}, B_{40}, B_{43}, B_{46}, B_{49}, B_{51}, B_{58}, B_{64}, B_{67}$	1	105
$B_6, B_8, B_{23}, B_{24}, B_{25}, B_{28}, B_{34}, B_{36}, B_{42}, B_{44}, B_{54}, B_{55}, B_{63}, B_{69}, B_{70}, B_{73}$	2	104
$B_{10}, B_{13}, B_{31}, B_{50}, B_{52}, B_{57}, B_{59}, B_{62}, B_{66}, B_{68}$	3	103
$B_9, B_{38}, B_{39}, B_{48}, B_{53}, B_{61}, B_{72}$	4	102
$B_4, B_{56}, B_{71}, B_{74}$	6	100

For a specific 6-arc, points of index zero are divided into orbits by the stabilizer of that 6-arc. The points of index zero for every 6-arc as a number of orbits with the size of the orbits in brackets are given in Table 4.9.

Tab. 4.9: The size of orbits

6-arc	Orbits	6-arc	Orbits	6-arc	Orbits
1	$8(1), 49(2)$	21	$105(1)$	41	$106(1)$
2	$106(1)$	22	$106(1)$	42	$52(2)$
3	$9(1), 48(2)$	23	$52(2)$	43	$105(1)$
4	$1(4), 4(12), 2(24)$	24	$52(2)$	44	$52(2)$
5	$9(1), 48(2)$	25	$52(2)$	45	$106(1)$
6	$10(2), 21(4)$	26	$106(1)$	46	$105(1)$
7	$9(1), 48(2)$	27	$105(1)$	47	$106(1)$
8	$10(2), 21(4)$	28	$52(2)$	48	$17(6)$
9	$7(6), 5(12)$	29	$105(1)$	49	$52(2)$
10	$1(1), 8(3), 13(6)$	30	$105(1)$	50	$1(1), 34(3)$
11	$106(1)$	31	$1(1), 34(3)$	51	$105(1)$
12	$105(1)$	32	$105(1)$	52	$1(1), 34(3)$
13	$1(1), 34(3)$	33	$105(1)$	53	$17(6)$
14	$105(1)$	34	$52(2)$	54	$52(2)$
15	$105(1)$	35	$105(1)$	55	$26(4)$
16	$105(1)$	36	$52(2)$	56	$1(4), 8(12)$
17	$105(1)$	37	$105(1)$	57	$1(1), 34(3)$
18	$106(1)$	38	$17(6)$	58	$105(1)$
19	$105(1)$	39	$17(6)$	59	$1(1), 34(3)$

20	106(1)	40	105(1)	60	106(1)
61	17(6)	67	105(1)	73	52(2)
62	1(1), 34(3))	68	1(1), 34(3)	74	1(4), 8(12)
63	26(4)	69	26(4)		
64	105(1)	70	52(2)		
65	106(1)	71	1(4), 8(12)		
66	1(1), 34(3)	72	17(6)		

The number of 7-arcs constructed by adding one point from each orbit is

$$4848 - 604 = 4244.$$

This gives the following result.

Theorem 4.4. *In $PG(2,17)$ there are precisely 733 projectively distinct 7-arcs.*

Remark 4.5. The numbers of 7-arcs and their stabilizers are given in Table 4.10.

Tab. 4.10: The stabilizers of 7-arcs

Stabilizer	I	$\mathbf{Z_2}$	$\mathbf{S_3}$	$\mathbf{Z_3}$
Number	644	75	2	12

4.7 The 7-arcs on a conic

The ten distinct heptads on $PG(1,17)$ can be mapped to ten distinct 7-arcs on a conic.

Substituting the points of each 7-arc in the corresponding conic shows the ten 7-arcs on a conic as given in Table 4.11.

Tab. 4.11: The distinct 7-arcs on a conic

New simple	7-arc	Conic	Stabilizer
C_1	$B_1 \cup \{42\}$	$x_0x_1 - 7x_0x_2 + 6x_1x_2$	I
C_2	$B_1 \cup \{85\}$	$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$\mathbf{Z_2}$
C_3	$B_1 \cup \{153\}$	$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$\mathbf{Z_2}$
C_4	$B_1 \cup \{168\}$	$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$\mathbf{Z_2}$
C_5	$B_1 \cup \{176\}$	$x_0x_1 - 7x_0x_2 + 6x_1x_2$	I
C_6	$B_2 \cup \{85\}$	$x_0x_1 - 7x_0x_2 + 6x_1x_2$	I
C_7	$B_2 \cup \{168\}$	$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$\mathbf{Z_2}$
C_8	$B_2 \cup \{176\}$	$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$\mathbf{Z_2}$
C_9	$B_2 \cup \{206\}$	$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$\mathbf{Z_2}$
C_{10}	$B_5 \cup \{34\}$	$x_0x_1 - 3x_0x_2 + 2x_1x_2$	$\mathbf{Z_2}$

4.8 The 8-arcs

Let K be a k-arc in $PG(2, q)$. For $k = 7$, the equations in Lemma 2.25 become:

$$\begin{aligned} c_0 &= (q-10)^2 + 20 - c_3, \\ c_1 &= 3\{7(q-11) + c_3\}, \\ c_2 &= 3(35 - c_3); \end{aligned}$$

The constant c_3 and hence c_0, c_1 and c_2 is calculated. Another way of calculating c_0 is by listing the points not on the bisecant of the 7-arc. The points represented by the number c_0 are separated into orbits. Then 8-arcs are constructed by adding one point from each orbit. This gives the following result.

Theorem 4.6. *In* $PG(2, 17)$ *there are precisely* 5441 *projectively distinct* 8*-arcs.*

Remark 4.7. The numbers of 8-arcs and their stabilizers are given in Table 4.12.

Tab. 4.12: The stabilizers of 8-arcs

Stabilizer	I	$\mathbf{Z_2}$	$\mathbf{Z_4}$	$\mathbf{D_8}$	$\mathbf{D_4}$	$\mathbf{Z_2 \times Z_2}$	$\mathbf{Z_8 \rtimes Z_2}$
Number	5027	389	4	1	3	16	1

4.9 The 8-arcs on a conic

The seventeen distinct octads on $PG(1,17)$ can be mapped to seventeen distinct 8-arcs on a conic. The 8-arcs in $PG(2,17)$ on a conic are given in Tables 4.13.

Tab. 4.13: The distinct 8-arcs on a conic

Conic	8-arc	Stabilizer
$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$C_1 \cup \{85\}$	I
$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$C_1 \cup \{136\}$	$\mathbf{Z_2}$
$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$C_1 \cup \{153\}$	I
$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$C_1 \cup \{176\}$	$\mathbf{Z_2}$
$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$C_1 \cup \{186\}$	I
$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$C_1 \cup \{206\}$	$\mathbf{Z_2}$

Conic	8-arc	Stabilizer
$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$C_1 \cup \{270\}$	$\mathbf{Z_2} \times \mathbf{Z_2}$
$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$C_2 \cup \{168\}$	$\mathbf{Z_2}$
$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$C_2 \cup \{176\}$	$\mathbf{Z_2}$
$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$C_3 \cup \{168\}$	$\mathbf{Z_2} \times \mathbf{Z_2}$
$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$C_3 \cup \{176\}$	$\mathbf{Z_2}$
$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$C_4 \cup \{176\}$	I
$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$C_4 \cup \{186\}$	$\mathbf{Z_2}$
$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$C_5 \cup \{299\}$	$\mathbf{D_4}$
$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$C_6 \cup \{136\}$	$\mathbf{Z_2}$
$x_0x_1 - 7x_0x_2 + 6x_1x_2$	$C_6 \cup \{176\}$	$\mathbf{Z_2} \times \mathbf{Z_2}$
$x_0x_1 - 3x_0x_2 + 2x_1x_2$	$C_{10} \cup \{241\}$	$\mathbf{D_8}$

4.10 The 9-arcs on a conic

The seventeen distinct nonads on $PG(1,17)$ can be mapped to seventeen distinct 9-arcs on a conic as given in Table 4.14. The 9-arcs all lie on the conic $\nu(x_0x_1 - 7x_0x_2 + 6x_1x_2)$.

Tab. 4.14: The distinct 9-arcs on a conic

9-arc	Stabilizer
$\{1,2,3,254,7,14,42,85,136\}$	$\mathbf{Z_2}$
$\{1,2,3,254,7,14,42,85,153\}$	$\mathbf{Z_3}$
$\{1,2,3,254,7,14,42,85,168\}$	I
$\{1,2,3,254,7,14,42,85,176\}$	$\mathbf{Z_2}$
$\{1,2,3,254,7,14,42,85,186\}$	$\mathbf{Z_2}$
$\{1,2,3,254,7,14,42,85,188\}$	$\mathbf{Z_2}$
$\{1,2,3,254,7,14,42,85,206\}$	I
$\{1,2,3,254,7,14,42,85,270\}$	I
$\{1,2,3,254,7,14,42,85,301\}$	I
$\{1,2,3,254,7,14,42,136,188\}$	I

9-arc	Stabilizer
$\{1,2,3,254,7,14,42,153,176\}$	I
$\{1,2,3,254,7,14,42,153,188\}$	$\mathbf{Z_2}$
$\{1,2,3,254,7,14,42,153,270\}$	$\mathbf{S_3}$
$\{1,2,3,254,7,14,42,186,188\}$	$\mathbf{Z_4}$
$\{1,2,3,254,7,14,85,168,270\}$	$\mathbf{D_9}$
$\{1,2,3,254,7,14,153,168,176\}$	$\mathbf{Z_2}$
$\{1,2,3,254,7,14,168,176,301\}$	$\mathbf{Z_8}$

Remark 4.8. It was computationally too difficult to classify all 9-arcs. It would have taken approximately $3,000$ hours.

4.11 The algorithm to calculate k-arcs, $k \leq 18$

The strategy to compute the complete k-arcs is the following.

(1) The way of calculating c_0 for $(k-1)$-arcs is by listing the points not on the bisecants of the $(k-1)$-arcs.

(2) The points represented by the number c_0 are separated into orbits.

(3) The k-arcs are constructed by adding one point from each orbit.

(4) For a given k-arc K, the set S of points not on the bisecants of K is found.

(5) If S is empty, then K is complete. Otherwise K is incomplete.

(6) All possible k-arcs from a given $(k-1)$-arcs are listed.

(7) The next step is to select the non-identical complete k-arcs among the total number constructed.

(8) Calculate the transformations between them. By use of The Fundamental Theorem of Projective Geometry, there is a unique projectivity of $PG(2,q)$ transforming four points no three on a line to any other four points no three on a line. Two k-arcs K_1 and K_2 are equivalent if $K_1\beta = K_2$ and β is given by a matrix $\mathbf{T}$ and $\beta = \mathbf{M}(\mathbf{T})$ with

$$\mathbf{M}(\lambda\mathbf{T}) = \mathbf{M}(\mathbf{T}),\ \lambda \in \mathbb{F}_{17} \setminus \{0\}.$$

A non-singular matrix $\mathbf{T}$ can be determined as follows.

Let $\mathbf{T} = (t_{ij})$, $i,j = 0,1,2$, $t_{ij} \in \mathbb{F}_q$. As $\mathbf{T}$ is determined up to a constant, so dividing the matrix by one of its entries leaves us needing only eight conditions to determine the whole matrix. If $x = (x_0\, x_1\, x_2), y = (y_0\, y_1\, y_2)$, then the matrix $\mathbf{T}$ which transforms x into y should satisfy the matrix equation $x\mathbf{T} = \lambda y$, where λ is a constant; that is,

$$\begin{aligned} x_0t_{00} + x_1t_{10} + x_2t_{20} &= \lambda y_0, && (4.1)\\ x_0t_{01} + x_1t_{11} + x_2t_{21} &= \lambda y_1, && (4.2)\\ x_0t_{02} + x_1t_{12} + x_2t_{22} &= \lambda y_1. && (4.3) \end{aligned}$$

By eliminating λ from equations (1) and (2), and from (2) and (3) we get two homogeneous equations for each pair x and y:

$$\begin{aligned} y_1(x_0t_{00} + x_1t_{10} + x_2t_{20}) - y_0(x_0t_{01} + x_1t_{11} + x_2t_{21}) &= 0,\\ y_2(x_0t_{01} + x_1t_{11} + x_2t_{21}) - y_1(x_0t_{02} + x_1t_{12} + x_2t_{22}) &= 0. \end{aligned}$$

The four points give us eight equations in the unknown t_{ij}. They form a system of homogeneous equations. There is always a unique solution of the system which gives the entries of the matrix $\mathbf{T}$. The solution of the system of homogeneous equations is a solution over $\mathbb{F}_q$. The calculations for finding such solution can be simplified by inserting one middle step; that is, instead of shifting the 4-arc

$$\{(a_0\,a_1\,a_2),\ (b_0\,b_1\,b_2),\ (c_0\,c_1\,c_2),\ (d_0\,d_1\,d_2)\}$$

to the 4-arc

$$\{(a'_0\,a'_1\,a'_2),\ (b'_0\,b'_1\,b'_2),\ (c'_0\,c'_1\,c'_2),\ (d'_0\,d'_1\,d'_2)\},$$

we can use the points of the frame

$$\{(1\,0\,0),\ (0\,1\,0),\ (0\,0\,1),\ (1\,1\,1)\}.$$

In general the procedure to find a matrix $\mathbf{T}$ which transforms the frame, in the above order, to any given 4-arc, say

$$\{(a_0\,a_1\,a_2),\ (b_0\,b_1\,b_2),\ (c_0\,c_1\,c_2),\ (d_0\,d_1\,d_2)\},$$

is as follows:

$$\begin{aligned}(1\,0\,0)\mathbf{T} &= \lambda(a_0\,a_1\,a_2),\\ (0\,1\,0)\mathbf{T} &= \mu(b_0\,b_1\,b_2),\\ (0\,0\,1)\mathbf{T} &= \nu(c_0\,c_1\,c_2),\end{aligned}$$

where $\lambda, \mu, \nu \in \mathbb{F}_q$. So

$$\mathbf{T} = \begin{pmatrix} \lambda a_0 & \lambda a_1 & \lambda a_2 \\ \mu b_0 & \mu b_1 & \mu b_2 \\ \nu c_0 & \nu c_1 & \nu c_2 \end{pmatrix}.$$

Also $(1\,1\,1)\mathbf{T} = \rho.(d_0\,d_1\,d_2), \rho \in \mathbb{F}_q$, which implies that

$$\begin{pmatrix} a_0 & b_0 & c_0 & d_0 \\ a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \end{pmatrix} . \begin{pmatrix} \lambda \\ \mu \\ \nu \\ -\rho \end{pmatrix} = 0.$$

The unique solution of the above system is.

$$\frac{\lambda}{A} = \frac{\mu}{B} = \frac{\nu}{C} = \frac{\rho}{D},$$

where $ABCD \neq 0$ and

$$A = \begin{vmatrix} d_0 & b_0 & c_0 \\ d_1 & b_1 & c_1 \\ d_2 & b_2 & c_2 \end{vmatrix},\ B = \begin{vmatrix} a_0 & d_0 & c_0 \\ a_1 & d_1 & c_1 \\ a_2 & d_2 & c_2 \end{vmatrix},\ C = \begin{vmatrix} a_0 & b_0 & d_0 \\ a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \end{vmatrix},\ D = \begin{vmatrix} a_0 & b_0 & c_0 \\ a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{vmatrix}.$$

Therefore,

$$\lambda = A\frac{\rho}{D},\ \ \mu = B\frac{\rho}{D},\ \ \nu = C\frac{\rho}{D},$$

$$\mathbf{T} = \begin{pmatrix} Aa_0 & Aa_1 & Aa_2 \\ Bb_0 & Bb_1 & Bb_2 \\ Cc_0 & Cc_1 & Cc_2 \end{pmatrix}.$$

This gives the following result.

Theorem 4.9. *The numbers of projectively distinct complete k-arcs in $PG(2,17)$ for $k \geq 10$ are given in Table 4.15.*

Tab. 4.15: The numbers of the complete k-arcs

k	10	11	12	13	14	15	16	17	18
Number	560	2644	553	8	1	–	–	–	1

Remark 4.10. The numbers of the complete k-arcs, $k = 10, 11, 12, 13, 14$ and their stabilizers are given in Tables 4.16, 4.17, 4.18, 4.19, 4.20.

Tab. 4.16: The stabilizers of the complete 10-arcs

Stabilizer	I	$\mathbf{Z_2}$	$\mathbf{A_4}$	$\mathbf{D_9}$	$\mathbf{Z_3}$	$\mathbf{Z_2} \times \mathbf{Z_2}$	$\mathbf{S_3}$	$\mathbf{Z_4}$	$\mathbf{Z_8} \rtimes \mathbf{Z_2}$	$\mathbf{Q_4}$	$\mathbf{S_4}$
Number	343	178	2	1	9	8	9	7	1	1	1

Let K_1 be the complete 10-arc with group isomorphic to $\mathbf{D_9}$ in Table 4.16. Then $G(K_1)$ is generated by g_1, g_2 where

$$g_1 = \begin{pmatrix} 0 & 0 & 16 \\ 0 & 11 & 0 \\ 15 & 0 & 0 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 13 & 13 & 13 \\ 6 & 13 & 12 \\ 6 & 15 & 13 \end{pmatrix}.$$

Then $G(K_1)$ has the following orbits on K_1: one orbit M_1 of size 9 and one orbit $M_2 = \{p\}$ of size 1. Then K_1 consists of M_1 on a conic $\mathbf{C}$ and P not on $\mathbf{C}$. The number of the points on no bisecant of M_1 is $c_0 = 19$. So P is not unique and we can select it from any of these ten points not on $\mathbf{C}$.

Let K_2 be the complete 10-arc with group isomorphic to $\mathbf{Z_8} \rtimes \mathbf{Z_2}$ in Table 4.16. Then $G(K_2)$ is generated by g_1, g_2 where

$$g_1 = \begin{pmatrix} 0 & 0 & 1 \\ 15 & 0 & 0 \\ 13 & 3 & 4 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 8 & 0 & 0 \\ 14 & 5 & 16 \\ 12 & 12 & 12 \end{pmatrix}.$$

Then $G(K_2)$ has the following orbits on K_2: one orbit of size 8 and one orbit of size 2. The group $G(K_2)$ stabilizes a line containing the orbit of size two, and partitions the line into one orbit of size 8, two of size 4, and one orbit of size 2.

Let K_3 be the complete 10-arc with group isomorphic to $\mathbf{S_4}$ in Table 4.16. Then $G(K_3)$ is generated by g_1, g_2 where

$$g_1 = \begin{pmatrix} 0 & 12 & 0 \\ 16 & 2 & 8 \\ 8 & 8 & 8 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 16 & 0 & 0 \\ 0 & 16 & 0 \\ 10 & 12 & 1 \end{pmatrix}.$$

Then $G(K_3)$ has the following orbits on K_3: one orbit of size 6 and one orbit of size 4.

Tab. 4.17: The stabilizers of the complete 11-arcs

Stabilizer	I	$\mathbf{Z_2}$
Number	2569	75

Tab. 4.18: The stabilizers of the complete 12-arcs

Stabilizer	I	$\mathbf{Z_2}$	$\mathbf{Z_3}$	$\mathbf{Z_2} \times \mathbf{Z_2}$	$\mathbf{Z_4}$	$\mathbf{S_3}$	$\mathbf{D_4}$	$\mathbf{D_6}$	$\mathbf{S_4}$
Number	337	152	17	18	1	20	2	3	3

Tab. 4.19: The stabilizers of the complete 13-arcs

Stabilizer	I	$\mathbf{Z_2}$	$\mathbf{Z_3}$	$\mathbf{Z_4}$	$\mathbf{S_3}$
Number	1	4	1	1	1

Tab. 4.20: The stabilizer of the complete 14-arc

Stabilizer	$\mathbf{D_4}$
Number	1

Let K_4 be the complete 14-arc with group isomorphic to $\mathbf{D_4}$ in Table 4.20. Then $G(K_4)$ is generated by g_1, g_2 where

$$g_1 = \begin{pmatrix} 0 & 6 & 0 \\ 3 & 0 & 0 \\ 2 & 12 & 16 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 11 & 1 & 15 \\ 12 & 12 & 12 \\ 0 & 0 & 2 \end{pmatrix}.$$

Then $G(K_4)$ has the following orbits on K_4: one orbit O_4 of size 8, one orbit O_5 of size 4 and one orbit O_1 of size 2. The group $G(K_4)$ stabilizes a line ℓ containing O_1 on a conic $\mathbf{C}$, and partitions the line ℓ into three orbits of size 4 and three orbits O_1, O_2, O_3 of size 2. Then K_4 consists of ten points on $\mathbf{C}$, two of them on ℓ, and eight points in $O_4 = \{R_1, R_2, R_3, R_4, R_5, R_6, R_7, R_8\}$ on $\mathbf{C}$. Let Q_1, Q_2, Q_3, Q_4 be the four points in O_5 not on $\mathbf{C}$. Let $O_1 = \{P_1, P_1'\}, O_2 = \{P_2, P_2'\}, O_3 = \{P_3, P_3'\}$ on ℓ, where

$$P_2 = Q_1Q_3 \cap \ell = Q_2Q_4 \cap \ell,\ P_2' = Q_1Q_4 \cap \ell = Q_2Q_3 \cap \ell,\ P_3 = Q_1Q_2 \cap \ell,\ P_3' = Q_3Q_4 \cap \ell.$$

The tetrad $O_1 \cup O_2$ is a *harmonic* and the tetrads $O_1 \cup O_3, O_2 \cup O_3$ are neither *harmonic* nor *equianharmonic*. The tangents at P_1 and P_1' to $\mathbf{C}$ meet at R. The lines

$$R_1R,\ R_2R,\ R_3R,\ R_4R,\ R_5R,\ R_6R,\ R_7R,\ R_8R,\ P_1R,\ P_1'R;$$

are part of a *pencil* . However $O_4' = \mathbf{C} \backslash (O_2 \cup O_4)$ is inequivalent to O_4. The other eight lines of the pencil meet $\mathbf{C}$ in O_4.

4.12 Links with Coding Theory

From Definition 2.47, an $[n, k, d]$ code is *maximum distance separable (MDS)* when

$$d = n - k + 1.$$

in the case that $k = 3$ and $d = n - 2$ of an $[n, k, d]$ code, the code C converts to a set K of n points on the projective plane $PG(2, q)$.

The parameters n, k and d for k-arcs in $PG(2, q)$ up to 14 and the number e of errors that can be corrected are given in Table 4.21.

Tab. 4.21: The parameters n, k, d and e for k-arcs

k-arc	n	k	d	e	k-arc	n	k	d	e
4-arc	4	3	2	1	10-arc	10	3	8	3
5-arc	5	3	3	1	11-arc	11	3	9	4
6-arc	6	3	4	1	12-arc	12	3	10	4
7-arc	7	3	5	2	13-arc	13	3	11	5
8-arc	8	3	6	2	14-arc	14	3	12	5
9-arc	9	3	7	3	18-arc	18	3	16	7

5. CUBIC CURVES OVER A FINITE FIELD

5.1 Introduction

The main goal of this chapter is to answer the question:

Which non-singular cubic curves in $PG(2,17)$ are complete as $(k;3)$-arcs?

Over $\mathbb{F}_q$, plane cubic curves have properties familiar from the classical theory over the real and complex numbers. When $q \equiv 1 \pmod 3$, their properties resemble those of cubics over the complex numbers; when $q \equiv -1 \pmod 3$, the real numbers are the better analogy. When $q \equiv 0 \pmod 3$, there is no suitable classical model.

Cubics with $3, 1, 0$ rational inflexions are treated in this order. The main difference from some other treatments is that here two curves are equivalent if there is a projectivity over $\mathbb{F}_q$ between them.

Let P_q be the total number of projectively inequivalent cubics. Let n_i for $i = 0, 1, 3, 9$ be the number of projectively inequivalent cubics with exactly i rational inflexions.

Hence,

$$P_q = n_9 + n_3 + n_1 + n_0.$$

Theorem 5.1.

$$P_q = 3q + 2 + \left(\frac{-4}{q}\right) + \left(\frac{-3}{q}\right)^2 + 3\left(\frac{-3}{q}\right).$$

Proof See [10, chapter 11, section 11].

Put

$$\left(\frac{x}{3}\right) = \begin{cases} 1 & \text{if } x \equiv 1 \pmod 3, \\ 0 & \text{if } x \equiv 0 \pmod 3, \\ -1 & \text{if } x \equiv -1 \pmod 3; \end{cases}$$

$$\left(\frac{-4}{c}\right) = \begin{cases} 1 & \text{if } c \equiv 1 \pmod 4, \\ 0 & \text{if } c \equiv 0 \pmod 2, \\ -1 & \text{if } c \equiv -1 \pmod 4; \end{cases}$$

$$\left(\frac{-3}{c}\right) = \begin{cases} 1 & \text{if } c \equiv 1 \pmod 3, \\ 0 & \text{if } c \equiv 0 \pmod 3, \\ -1 & \text{if } c \equiv -1 \pmod 3; \end{cases}$$

From the above formulas and Theorem 5.1, the total number of projectively inequivalent cubics over $\mathbb{F}_{17}$ is 52; that is, $P_{17} = 52$.

Theorem 5.2. *There exists a non-singular plane cubic curve over $\mathbb{F}_q$ with nine rational inflexions if and only if $q \equiv 1 \pmod 3$.*

Proof See [10, chapter 11, section 5].

Remark 5.3. From Theorem 5.2, since $17 \not\equiv 1 \pmod 3$, the number of projective inequivalent curves with exactly nine rational inflexions is zero; that is, $n_9 = 0$.

Lemma 5.4. *There are $(q-1,3)$ projectively distinct cubic curves with three collinear rational inflexions such that the inflexional tangents are concurrent. The polynomials are as follows:*

(1) $(q-1,3) = 1$,
$$F = XY(X+Y) + Z^3;$$

(2) $(q-1,3) = 3$,
$$\begin{aligned} F &= XY(X+Y) + Z^3, \\ F &= XY(X+Y) + \alpha Z^3, \\ F &= XY(X+Y) + \alpha^2 Z^3, \end{aligned}$$

where α is a primitive element of $\mathbb{F}_q$.

Proof See [10, chapter 11, section 5].

Corollary 5.5. *Over $\mathbb{F}_{17}$, the polynomial $F = XY(X+Y)+Z^3$ has three rational inflexions.*

Remark 5.6. When $q \equiv 0 \pmod 3$ the cubic curve $\mathcal{F} = \nu(F)$ in Lemma 5.4 is singular. When $q \equiv 1 \pmod 3$, the cubic curve $\mathcal{F} = \nu(F)$ has nine rational inflexions when $e = 1$ and three rational inflexions when $e = \alpha, \alpha^2$, where α is a primitive element of $\mathbb{F}_q$.

Theorem 5.7. *A non-singular plane cubic over $\mathbb{F}_q$ with three collinear rational inflexions and non-concurrent inflexional tangents has three or nine rational inflexions and polynomial*
$$F = XYZ + e(X+Y+Z)^3,$$
$e \neq 0, -1/27$.

Proof See [10, chapter 11, section 5].

Lemma 5.8. *The polynomial $F = XYZ + e(X+Y+Z)^3$ is*

(1) *singular and irreducible if $e = -1/27$;*

(2) *equianharmonic if $e = -1/24$;*

(3) *harmonic if $216e^2 + 36e + 1 = 0$, which has two roots when 3 is a square.*

Corollary 5.9. *Over $\mathbb{F}_{17}$, the polynomial $F = XYZ + e(X+Y+Z)^3$ is*

(1) *singular and irreducible if $e = 5$;*

(2) *equianharmonic if $e = -5$.*

5.2 Non-singular cubics with three rational inflexions

The classification of non-singular cubics with exactly three rational inflexions can be completed on the basis of the previous theorems. From Lemma 5.4, Corollary 5.5, Theorem 5.7, Lemme 5.8 and Corollary 5.9, such a cubic F has polynomial

$$F = XY(X+Y) + Z^3 \quad \text{or} \quad F = XYZ + e(X+Y+Z)^3$$

as the three inflexional tangents are concurrent or not.

For a non-singular cubic curve $\mathcal{F} = \nu(F)$, let K_F be a complete $(k_F;3)$-arc of largest size containing the points of $\mathcal{F}$. Table 5.1 lists, for each projectively distinct curve, the polynomial of $\mathcal{F}$, the size k_F of K_F, the completeness or incompleteness of $\mathcal{F}$ as a $(k;3)$-arc, and the type of $\mathcal{F}$, where G, E, H are respectively the general, equianharmonic, harmonic types when the inflexional tangents are not concurrent, and $\bar{E}$ the type when they are concurrent as described in Table 5.1.

Tab. 5.1: The canonical forms with three rational inflexions

No.	F	k	Description	Type	k_F
1	$XY(X+Y)+Z^3$	18	incomplete	$\bar{E}$	22
2	$XYZ+(X+Y+Z)^3$	12	incomplete	G	25
3	$XYZ-(X+Y+Z)^3$	21	complete	G	21
4	$XYZ+2(X+Y+Z)^3$	21	complete	G	21
5	$XYZ-2(X+Y+Z)^3$	15	incomplete	G	20
6	$XYZ+3(X+Y+Z)^3$	15	incomplete	G	21
7	$XYZ-3(X+Y+Z)^3$	12	incomplete	G	22
8	$XYZ+4(X+Y+Z)^3$	24	incomplete	G	25
9	$XYZ-4(X+Y+Z)^3$	12	incomplete	G	22
10	$XYZ-5(X+Y+Z)^3$	18	incomplete	E	24
11	$XYZ+6(X+Y+Z)^3$	15	incomplete	G	21
12	$XYZ-6(X+Y+Z)^3$	18	complete	G	18
13	$XYZ+7(X+Y+Z)^3$	21	complete	G	21
14	$XYZ-7(X+Y+Z)^3$	18	incomplete	G	22
15	$XYZ+8(X+Y+Z)^3$	24	complete	G	24
16	$XYZ-8(X+Y+Z)^3$	24	complete	G	24

So, the number of projectively inequivalent cubics with exactly three rational inflexions is 16; that is, $n_3 = 16$.

5.3 Non-singular cubics with one rational inflexion

The classification of non-singular cubics with exactly one rational inflexions can be completed on the basis of the next theorem.

Theorem 5.10. *A non-singular, plane, cubic curve defined over $\mathbb{F}_q$, with at least one inflexion has the polynomial.*

$$F = Z^2Y + X^3 + cXY^2 + dY^3,$$

where $4c^3 + 27d^2 \neq 0$.

Proof See [10, chapter 11, section 8].

Remark 5.11. The curve $\mathcal{F}$ in Theorem 5.10 is general when $cd \neq 0$, harmonic when $c \neq 0$ and $d = 0$, equinanharmonic when $c = 0$ and $d \neq 0$, and singular when $4c^3 + 27d^2 = 0$.

From Theorem 5.10 and Remark 5.11, Table 5.2 lists, for each projectively distinct curve, the polynomial of $\mathcal{F}$, the size k_F of K_F, the completeness or incompleteness of $\mathcal{F}$ as a $(k;3)$-arc, and the type of $\mathcal{F}$ as described in Table 5.2.

Tab. 5.2: The canonical forms with one rational inflexion

No.	F	k	Description	Type	k_F
1	$Z^2Y + X^3 + XY^2 + Y^3$	18	incomplete	G	22
2	$Z^2Y + X^3 + XY^2 - Y^3$	18	incomplete	G	22
3	$Z^2Y + X^3 + XY^2 + 2Y^3$	24	incomplete	G	25
4	$Z^2Y + X^3 + XY^2 - 2Y^3$	24	incomplete	G	25
5	$Z^2Y + X^3 + XY^2 + 3Y^3$	17	incomplete	G	20
6	$Z^2Y + X^3 + XY^2 - 3Y^3$	17	incomplete	G	20
7	$Z^2Y + X^3 + XY^2 + 4Y^3$	14	incomplete	G	21

No.	F	k	Description	Type	k_F
8	$Z^2Y + X^3 + XY^2 - 4Y^3$	14	incomplete	G	23
9	$Z^2Y + X^3 + XY^2 + 5Y^3$	15	incomplete	G	22
10	$Z^2Y + X^3 + XY^2 - 5Y^3$	15	incomplete	G	21
11	$Z^2Y + X^3 + XY^2 + 6Y^3$	20	incomplete	G	21
12	$Z^2Y + X^3 + XY^2 - 6Y^3$	20	incomplete	G	21
13	$Z^2Y + X^3 + XY^2 + 7Y^3$	12	incomplete	G	23
14	$Z^2Y + X^3 + XY^2 - 7Y^3$	12	incomplete	G	22
15	$Z^2Y + X^3 + XY^2 + 8Y^3$	25	complete	G	25
16	$Z^2Y + X^3 + XY^2 - 8Y^3$	25	complete	G	25
17	$Z^2Y + X^3 + XY^2$	16	incomplete	H	20
18	$Z^2Y + X^3 + 2XY^2$	20	complete	H	20
19	$Z^2Y + X^3 + 3XY^2$	26	complete	H	26
20	$Z^2Y + X^3 + 6XY^2$	10	incomplete	H	22

So, the number of projectively inequivalent cubics with exactly one rational inflexion is 20; that is, $n_1 = 20$.

5.4 Non-singular cubics with no rational inflexions

In this section, a summary of the results for cubics with no rational inflexions is given.

Lemma 5.12. *Over $\mathbb{F}_q$, $q \equiv -1 \ (mod\ 3)$, a non-singular cubic with no rational inflexions has polynomial*

$$F = Z^3 - 3c(X^2 - dXY + Y^2)Z - (X^3 - 3XY^2 + dY^3),$$

where $X^3 - 3X + d$ is irreducible.

Proof See [10, chapter 11, section 9].

Lemma 5.13. *The curve $\mathcal{F}$ in Lemma* 5.12 *is equianharmonic for $c = 0, 2/e$, harmonic for $c = (-1 \pm \sqrt{3})/e$, where $e^3 = d^2 - 4$.*

Corollary 5.14. *Over $\mathbb{F}_{17}$, the curve $\mathcal{F}$ in Lemma* 5.12 *is equianharmonic for $c = 0, -6$.*

Remark 5.15. The polynomial $X^3 - 3X + d$ of degree 3 is irreducible over $\mathbb{F}_{17}$, where $d = \pm 3, \pm 4, \pm 7$.

From Lemma 5.12, Lemma 5.13, Corollary 5.14 and Remark 5.15, Table 5.3 lists, for each projectively distinct curve, the polynomial of $\mathcal{F}$, the size k_F of K_F, the completeness or incompleteness of $\mathcal{F}$ as a $(k;3)$-arc, and the type of $\mathcal{F}$ as described in Table 5.3.

Tab. 5.3: The canonical forms with no rational inflexions

No.	F	k	Description	Type	k_F
1	$Z^3 - 3(X^2 - 3XY + Y^2)Z - (X^3 - 3XY^2 + 3Y^3)$	15	incomplete	G	22
2	$Z^3 + 3(X^2 - 3XY + Y^2)Z - (X^3 - 3XY^2 + 3Y^3)$	24	complete	G	24
3	$Z^3 - 6(X^2 - 3XY + Y^2)Z - (X^3 - 3XY^2 + 3Y^3)$	15	incomplete	G	21
4	$Z^3 + 6(X^2 - 3XY + Y^2)Z - (X^3 - 3XY^2 + 3Y^3)$	21	complete	G	21
5	$Z^3 - 8(X^2 - 3XY + Y^2)Z - (X^3 - 3XY^2 + 3Y^3)$	18	complete	G	18
6	$Z^3 + 5(X^2 - 3XY + Y^2)Z - (X^3 - 3XY^2 + 3Y^3)$	24	complete	G	24
7	$Z^3 - 5(X^2 - 3XY + Y^2)Z - (X^3 - 3XY^2 + 3Y^3)$	12	incomplete	G	23
8	$Z^3 + 2(X^2 - 3XY + Y^2)Z - (X^3 - 3XY^2 + 3Y^3)$	24	complete	G	24
9	$Z^3 - 2(X^2 - 3XY + Y^2)Z - (X^3 - 3XY^2 + 3Y^3)$	21	complete	G	21
10	$Z^3 - (X^2 - 3XY + Y^2)Z - (X^3 - 3XY^2 + 3Y^3)$	15	incomplete	G	22
11	$Z^3 + (X^2 - 3XY + Y^2)Z - (X^3 - 3XY^2 + 3Y^3)$	18	complete	E	18
12	$Z^3 - 4(X^2 - 3XY + Y^2)Z - (X^3 - 3XY^2 + 3Y^3)$	18	complete	G	18

No.	F	k	Description	Type	k_F
13	$Z^3+4(X^2-3XY+Y^2)Z-(X^3-3XY^2+3Y^3)$	21	complete	G	21
14	$Z^3-7(X^2-3XY+Y^2)Z-(X^3-3XY^2+3Y^3)$	12	incomplete	G	23
15	$Z^3+7(X^2-3XY+Y^2)Z-(X^3-3XY^2+3Y^3)$	12	incomplete	G	23
16	$Z^3-X^3+3XY^2-3Y^3$	18	incomplete	E	22

So, the number of projectively inequivalent cubics with no rational inflexions is 16; that is, $n_0 = 16$.

5.5 Number of rational points on a non-singular cubics

Let $N_q(1)$ be the maximum number of points on a non-singular cubic over $\mathbb{F}_q$. From [10], the range of the number N_1 of points on a cubic is

$$q+1-2\sqrt{q} \leq N_1 \leq q+1+2\sqrt{q}.$$

From Tables 5.1, 5.2, 5.3,

$$N_{17}(1) = 26, M_{17}(1) = 10,$$

where $M_{17}(1)$ is the minimum number of points on a non-singular cubic over $\mathbb{F}_{17}$. So $m_3(2,17) \geq N_{17}(1)$ where $m_3(2,17)$ is the maximum number of points on a $(k;3)$-arc in $PG(2,17)$.

Theorem 5.16. *In $PG(2,17)$ there are precisely 19 projectively distinct complete non-singular cubic curves.*

The numbers of the complete non-singular cubic curves and their stabilizer are given in Table 5.4.

Tab. 5.4: The stabilizers of the complete non-singular cubic curves

Stabilizer	$\mathbf{Z_2}$	$\mathbf{Z_3}$	$\mathbf{Z_4}$	$\mathbf{S_3}$
Number	2	9	2	6

5.6 Links with Coding Theory

A linear $[n, k, d]$ code C is called *near-MDS*, or simply *NMDS*, if

$$d = n - k.$$

in the case that $k = 3$ and $d = n - 3$ of an $[n, k, d]$ code, the code C converts to a set K of n points on the projective plane $PG(2, q)$ with at least one line of the plane containing three points of K.

The parameters n, k and d for k-arcs in $PG(2, q)$ up to 26 and the number e of errors that can be corrected are given in Table 5.5.

Tab. 5.5: The parameters n, k, d and e for $(k;3)$-arcs

$(k;3)$-arc	n	k	d	e	$(k;3)$-arc	n	k	d	e
(11;3)-arc	11	3	8	3	(19;3)-arc	19	3	16	7
(12;3)-arc	12	3	9	4	(20;3)-arc	20	3	17	8
(13;3)-arc	13	3	10	4	(21;3)-arc	21	3	18	8
(14;3)-arc	14	3	11	5	(22;3)-arc	22	3	19	9
(15;3)-arc	15	3	12	5	(23;3)-arc	23	3	20	9
(16;3)-arc	16	3	13	6	(24;3)-arc	24	3	21	10
(17;3)-arc	17	3	14	6	(25;3)-arc	25	3	22	10
(18;3)-arc	18	3	15	7	(26;3)-arc	26	3	23	11

6. APPENDIX 1

Programming

The programs are written in GAP for use on a Windows machine. We classified the types of heptads in $PG(1,17)$ to compute the projectivities between them. So far, all arcs up to and including size eight on projective plane $PG(2,17)$ have been classified, as have complete k-arcs, where $k \leq 18$. The complete non-singular cubic curves in $PG(2,17)$ as $(k;3)$-arcs have been classified as well. We checked the programs on the case $q = 7$.

6.1 Computing the points of $PG(2,17)$

```
t:=[[0,1,0],[0,0,1],[14,1,0]];;
    u:=[1,0,0];;
    for i in [0..306] do
    p := u * t^i mod 17;
    if p[3] <> 0 mod 17 then z := p * p[3]^-1 mod 17;
    elif p[2] <> 0 mod 17 then z := p * p[2]^-1 mod 17;
    elif p[1] <> 0 mod 17 then z := p * p[1]^-1 mod 17;
    fi;
    Print(i+1,p,"\n");
    od;
```

6.2 Classifying heptads in $PG(1,17)$

```
a := [3,4,5,-5,6,-6,-8];;
    A := a[1,2,3,4,5,6];;
    B := a[1,2,3,4,5,7];;
    C := a[1,2,3,4,6,7];;
    D := a[1,2,3,5,6,7];;
    K := a[1,2,4,5,6,7];;
    F := a[1,3,4,5,6,7];;
    G := a[2,3,4,5,6,7];;
    wa := [A,B,C,D,K,F,G];;
    A51 := A[1,2,3,4,5];;
    A52 := A[1,2,3,4,6];;
    A53 := A[1,2,3,5,6];;
    A54 := A[1,2,4,5,6];;
    A55 := A[1,3,4,5,6];;
```

$A56 := A[2,3,4,5,6];;$
$WA5 := [A51, A52, A53, A54, A55, A56];;$
$A51-41 := A51\{[1,2,3,4]\};;$
$A51-42 := A51\{[1,2,3,5]\};;$
$A51-43 := A51\{[1,2,4,5]\};;$
$A51-44 := A51\{[1,3,4,5]\};;$
$A51-45 := A51\{[2,3,4,5]\};;$
$WA51-4 := [A51-41, A51-42, A51-43, A51-44, A51-45];;$
$A52-41 := A52\{[1,2,3,4]\};;$
$A52-42 := A52\{[1,2,3,5]\};;$
$A52-43 := A52\{[1,2,4,5]\};;$
$A52-44 := A52\{[1,3,4,5]\};;$
$A52-45 := A52\{[2,3,4,5]\};;$
$WA52-4 := [A52-41, A52-42, A52-43, A52-44, A52-45];;$
$A53-41 := A53\{[1,2,3,4]\};;$
$A53-42 := A53\{[1,2,3,5]\};;$
$A53-43 := A53\{[1,2,4,5]\};;$
$A53-44 := A53\{[1,3,4,5]\};;$
$A53-45 := A53\{[2,3,4,5]\};;$
$WA53-4 := [A53-41, A53-42, A53-43, A53-44, A53-45];;$
$A54-41 := A54\{[1,2,3,4]\};;$
$A54-42 := A54\{[1,2,3,5]\};;$
$A54-43 := A54\{[1,2,4,5]\};;$
$A54-44 := A54\{[1,3,4,5]\};;$
$A54-45 := A54\{[2,3,4,5]\};;$
$WA54-4 := [A54-41, A54-42, A54-43, A54-44, A54-45];;$
$A55-41 := A55\{[1,2,3,4]\};;$
$A55-42 := A55\{[1,2,3,5]\};;$
$A55-43 := A55\{[1,2,4,5]\};;$
$A55-44 := A55\{[1,3,4,5]\};;$
$A55-45 := A55\{[2,3,4,5]\};;$
$WA55-4 := [A55-41, A55-42, A55-43, A55-44, A55-45];;$
$A56-41 := A56\{[1,2,3,4]\};;$
$A56-42 := A56\{[1,2,3,5]\};;$
$A56-43 := A56\{[1,2,4,5]\};;$
$A56-44 := A56\{[1,3,4,5]\};;$
$A56-45 := A56\{[2,3,4,5]\};;$
$WA56-4 := [A56-41, A56-42, A56-43, A56-44, A56-45];;$
$WA-4 := [WA51-4, WA52-4, WA53-4, WA54-4, WA55-4, WA56-4];;$
$Print("A-", A, "\backslash n");$
$for\ l\ in\ [1..6]\ do$
$Print(l, "-", WA5[l], "\backslash n");$
$od;$
$for\ i\ in\ [1..6]\ do$
$Print(i, "=", WA5[i]);$

$AA := WA-4[i];$
$for\ j\ in\ [1..5]\ do$
$AAA := AA[j];$
$if\ AAA[1] = "infinity"\ then$
$CR := (AAA[2]-AAA[4])/(AAA[2]-AAA[3]) mod 17;$
$Print(j, " = ", AAA, "CR = ", "\backslash n");$
$else$
$CR := ((AAA[1]-AAA[3])*(AAA[2]-AAA[4]))/((AAA[1]-AAA[4])*(AAA[2]-AAA[3])) mod 17;$
$Print(j, " = ", AAA, "CR = ", "\backslash n");$
$fi;$
$od;$
$Print(******************************, "\backslash n");$
$od;$

6.3 Computing the transformations between the 5-arcs

```
s:=[[ [ 0, 0, 1 ], [ 0, 1, 0 ], [ 1, 0, 0 ], [ 1, 1, 1 ], [ 3, 8, 1 ]],
[ [ 0, 0, 1 ], [ 0, 1, 0 ], [ 1, 0, 0 ], [ 1, 1, 1 ], [ 2, 4, 1 ]]];;
w:=Size(s);;
for h in [1 . . w-1] do
for j in [h+1 . . w] do
v:=[ ];;
for i1 in [1 . . 5] do
for i2 in [1 . . 5] do
for i3 in [1 . . 5] do
for i4 in [1 . . 5] do
if i1 <> i2 and i1 <> i3 and i1 <> i4 and i2 <> i3 and i2 <> i4 and
i3 <> i4 then
n := [s[j][i1], s[j][i2], s[j][i3], s[j][i4]]; ;
Add(v,n);
fi;
od;od;od;od;
for i in [1 . . Length(v)] do
t := v[i];
a1 := t[4][1] * (t[2][2] * t[3][3] - t[3][2] * t[2][3]);
a2 := t[2][1] * (t[4][2] * t[3][3] - t[3][2] * t[4][3]);
a3 := t[3][1] * (t[4][2] * t[2][3] - t[2][2] * t[4][3]);
b1 := t[1][1] * (t[4][2] * t[3][3] - t[3][2] * t[4][3]);
b2 := t[4][1] * (t[1][2] * t[3][3] - t[3][2] * t[1][3]);
b3 := t[3][1] * (t[1][2] * t[4][3] - t[4][2] * t[1][3]);
c1 := t[1][1] * (t[2][2] * t[4][3] - t[4][2] * t[2][3]);
c2 := t[2][1] * (t[1][2] * t[4][3] - t[4][2] * t[1][3]);
c3 := t[4][1] * (t[1][2] * t[2][3] - t[2][2] * t[1][3]);
a := (a1 - a2 + a3) mod 17;
```

$b := (b1 - b2 + b3)$ mod 17;
$c := (c1 - c2 + c3)$ mod 17;
$T := [[a * t[1][1]$ mod 17, $a * t[1][2]$ mod 17, $a * t[1][3]$ mod 17],
$[b * t[2][1]$ mod 17, $b * t[2][2]$ mod 17,$b * t[2][3]$ mod 17],
$[c * t[3][1]$ mod 17, $c * t[3][2]$ mod 17,$c * t[3][3]$ mod 17]];
r1:=(s[h][1]*T) mod 17;
r2:=(s[h][2]* T) mod 17;
r3:=(s[h][3]* T) mod 17;
r4:=(s[h][4]*T) mod 17;
r5:=(s[h][5]* T) mod 17;
if $r1[3] <> 0$ mod 17 then $x1 := r1 * r1[3]^-1$ mod 17;
elif $r1[2] <> 0$ mod 17 then $x1 := r1 * r1[2]^-1$ mod 17;
elif $r1[1] <> 0$ mod 17 then $x1 := r1 * r1[1]^-1$ mod 17;
fi;
if $r2[3] <> 0$ mod 17 then $x2 := r2 * r2[3]^-1$ mod 17;
elif $r2[2] <> 0$ mod 17 then $x2 := r2 * r2[2]^-1$ mod 17;
elif $r2[1] <> 0 mod 17 then x2 := r2 * r2[1]^-1$ mod 17;
fi;
if $r3[3] <> 0$ mod 17 then $x3 := r3 * r3[3]^-1$ mod 17;
elif $r3[2] <> 0$ mod 17 then $x3 := r3 * r3[2]^-1$ mod 17;
elif $r3[1] <> 0$ mod 17 then $x3 := r3 * r3[1]^-1$ mod 17;
fi;
if $r4[3] <> 0$ mod 17 then $x4 := r4 * r4[3]^-1$ mod 17;
elif $r4[2] <> 0$ mod 17 then $x4 := r4 * r4[2]^-1$ mod 17;
elif $r4[1] <> 0$ mod 17 then $x4 := r4 * r4[1]^-1$ mod 17;
fi;
if $r5[3] <> 0$ mod 17 then $x5 := r5 * r5[3]^-1$ mod 17;
elif $r5[2] <> 0$ mod 17 then $x5 := r5 * r5[2]^-1$ mod 17;
elif $r5[1] <> 0$ mod 17 then $x5 := r5 * r5[1]^-1$ mod 17;
fi;
if Set($[x1, x2, x3, x4, x5]$)=Set($s[j]$) mod 17 then
Print($h, T, j, "\backslash n"$);
fi;
od;od;od;

In above programme $|s| = 2$, but we can choose $|s| = n$ for any positive integer number n.

6.4 Computing the transformations between the 6-arcs

s:=[[[0, 0, 1], [0, 1, 0], [1, 0, 0], [1, 1, 1], [9, 11, 1],[3,8,1]],
[[0, 0, 1], [0, 1, 0], [1, 0, 0], [1, 1, 1], [9, 11, 1],[10,15,1]]];;
w:=Size(s);;
for h in [1 . . w-1] do
for j in [h+1 . . w] do
v:=[ ];;

```
for i1 in [1 . . 6] do
for i2 in [1 . . 6] do
for i3 in [1 . . 6] do
for i4 in [1 . . 6] do
if i1 <> i2 and i1 <> i3 and i1 <> i4 and i2 <> i3 and i2 <> i4 and
i3 <> i4 then
n := [s[j][i1], s[j][i2], s[j][i3], s[j][i4]]; ;
Add(v,n);
fi;
od;od;od;od;
for i in [1 . . Length(v)] do
t := v[i];
a1 := t[4][1] * (t[2][2] * t[3][3] − t[3][2] * t[2][3]);
a2 := t[2][1] * (t[4][2] * t[3][3] − t[3][2] * t[4][3]);
a3 := t[3][1] * (t[4][2] * t[2][3] − t[2][2] * t[4][3]);
b1 := t[1][1] * (t[4][2] * t[3][3] − t[3][2] * t[4][3]);
b2 := t[4][1] * (t[1][2] * t[3][3] − t[3][2] * t[1][3]);
b3 := t[3][1] * (t[1][2] * t[4][3] − t[4][2] * t[1][3]);
c1 := t[1][1] * (t[2][2] * t[4][3] − t[4][2] * t[2][3]);
c2 := t[2][1] * (t[1][2] * t[4][3] − t[4][2] * t[1][3]);
c3 := t[4][1] * (t[1][2] * t[2][3] − t[2][2] * t[1][3]);
a := (a1 − a2 + a3) mod 17;
b := (b1 − b2 + b3) mod 17;
c := (c1 − c2 + c3) mod 17;
T := [[a * t[1][1] mod 17, a * t[1][2] mod 17, a * t[1][3] mod 17],
[b * t[2][1] mod 17, b * t[2][2] mod 17,b * t[2][3] mod 17],
[c * t[3][1] mod 17, c * t[3][2] mod 17,c * t[3][3] mod 17]];
r1:=(s[h][1]*T) mod 17;
r2:=(s[h][2]* T ) mod 17;
r3:=(s[h][3]* T ) mod 17;
r4:=(s[h][4]*T) mod 17;
r5:=(s[h][5]* T ) mod 17;
r6:=(s[h][6]* T ) mod 17;
if r1[3] <> 0 mod 17 then x1 := r1 * r1[3]^−1 mod 17;
elif r1[2] <> 0 mod 17 then x1 := r1 * r1[2]^−1 mod 17;
elif r1[1] <> 0 mod 17 then x1 := r1 * r1[1]^−1 mod 17;
fi;
if r2[3] <> 0 mod 17 then x2 := r2 * r2[3]^−1 mod 17;
elif r2[2] <> 0 mod 17 then x2 := r2 * r2[2]^−1 mod 17;
elif r2[1] <> 0mod17thenx2 := r2 * r2[1]^−1 mod 17;
fi;
if r3[3] <> 0 mod 17 then x3 := r3 * r3[3]^−1 mod 17;
elif r3[2] <> 0 mod 17 then x3 := r3 * r3[2]^−1 mod 17;
elif r3[1] <> 0 mod 17 then x3 := r3 * r3[1]^−1 mod 17;
fi;
```

if $r4[3] <> 0$ mod 17 then $x4 := r4 * r4[3]^{-}1$ mod 17;
elif $r4[2] <> 0$ mod 17 then $x4 := r4 * r4[2]^{-}1$ mod 17;
elif $r4[1] <> 0$ mod 17 then $x4 := r4 * r4[1]^{-}1$ mod 17;
fi;
if $r5[3] <> 0$ mod 17 then $x5 := r5 * r5[3]^{-}1$ mod 17;
elif $r5[2] <> 0$ mod 17 then $x5 := r5 * r5[2]^{-}1$ mod 17;
elif $r5[1] <> 0$ mod 17 then $x5 := r5 * r5[1]^{-}1$ mod 17;
fi;
if $r6[3] <> 0$ mod 17 then $x6 := r6 * r6[3]^{-}1$ mod 17;
elif $r6[2] <> 0$ mod 17 then $x6 := r6 * r6[2]^{-}1$ mod 17;
elif $r6[1] <> 0$ mod 17 then $x6 := r6 * r6[1]^{-}1$ mod 17;
fi;
if Set($[x1, x2, x3, x4, x5, x6]$)=Set($s[j]$) mod 17 then
Print$(h, T, j, "\backslash n")$;
fi;
od;od;od;
Here in above programme $|s| = 2$, but in fact $|s| = 74$.

6.5 *Computing the transformations between the 7-arcs*

s:=[[[0, 0, 1], [0, 1, 0], [1, 0, 0], [1, 1, 1], [9, 11, 1],[3,8,1],[10,15,1]],
[[0, 0, 1], [0, 1, 0], [1, 0, 0], [1, 1, 1], [9, 11, 1],[10,15,1],[5,14,1]]];;
w:=Size(s);;
for h in [1 . . w-1] do
for j in [h+1 . . w] do
v:=[ ];;
for i1 in [1 . . 7] do
for i2 in [1 . . 7] do
for i3 in [1 . . 7] do
for i4 in [1 . . 7] do
if $i1 <> i2$ and $i1 <> i3$ and $i1 <> i4$ and $i2 <> i3$ and $i2 <> i4$ and
$i3 <> i4$ then
$n := [s[j][i1], s[j][i2], s[j][i3], s[j][i4]];;$
Add(v,n);
fi;
od;od;od;od;
for i in [1 . . Length(v)] do
$t := v[i];$
$a1 := t[4][1] * (t[2][2] * t[3][3] - t[3][2] * t[2][3]);$
$a2 := t[2][1] * (t[4][2] * t[3][3] - t[3][2] * t[4][3]);$
$a3 := t[3][1] * (t[4][2] * t[2][3] - t[2][2] * t[4][3]);$
$b1 := t[1][1] * (t[4][2] * t[3][3] - t[3][2] * t[4][3]);$
$b2 := t[4][1] * (t[1][2] * t[3][3] - t[3][2] * t[1][3]);$
$b3 := t[3][1] * (t[1][2] * t[4][3] - t[4][2] * t[1][3]);$
$c1 := t[1][1] * (t[2][2] * t[4][3] - t[4][2] * t[2][3]);$

$c2 := t[2][1] * (t[1][2] * t[4][3] - t[4][2] * t[1][3]);$
$c3 := t[4][1] * (t[1][2] * t[2][3] - t[2][2] * t[1][3]);$
$a := (a1 - a2 + a3)$ mod 17;
$b := (b1 - b2 + b3)$ mod 17;
$c := (c1 - c2 + c3)$ mod 17;
$T := [[a * t[1][1]$ mod 17, $a * t[1][2]$ mod 17, $a * t[1][3]$ mod 17],
$[b * t[2][1]$ mod 17, $b * t[2][2]$ mod 17,$b * t[2][3]$ mod 17],
$[c * t[3][1]$ mod 17, $c * t[3][2]$ mod 17,$c * t[3][3]$ mod 17]];
r1:=(s[h][1]*T) mod 17;
r2:=(s[h][2]* T) mod 17;
r3:=(s[h][3]* T) mod 17;
r4:=(s[h][4]*T) mod 17;
r5:=(s[h][5]* T) mod 17;
r6:=(s[h][6]* T) mod 17;
r7:=(s[h][7]* T) mod 17;
if $r1[3] <> 0$ mod 17 then $x1 := r1 * r1[3]^{-}1$ mod 17;
elif $r1[2] <> 0$ mod 17 then $x1 := r1 * r1[2]^{-}1$ mod 17;
elif $r1[1] <> 0$ mod 17 then $x1 := r1 * r1[1]^{-}1$ mod 17;
fi;
if $r2[3] <> 0$ mod 17 then $x2 := r2 * r2[3]^{-}1$ mod 17;
elif $r2[2] <> 0$ mod 17 then $x2 := r2 * r2[2]^{-}1$ mod 17;
elif $r2[1] <> 0 mod 17 then x2 := r2 * r2[1]^{-}1$ mod 17;
fi;
if $r3[3] <> 0$ mod 17 then $x3 := r3 * r3[3]^{-}1$ mod 17;
elif $r3[2] <> 0$ mod 17 then $x3 := r3 * r3[2]^{-}1$ mod 17;
elif $r3[1] <> 0$ mod 17 then $x3 := r3 * r3[1]^{-}1$ mod 17;
fi;
if $r4[3] <> 0$ mod 17 then $x4 := r4 * r4[3]^{-}1$ mod 17;
elif $r4[2] <> 0$ mod 17 then $x4 := r4 * r4[2]^{-}1$ mod 17;
elif $r4[1] <> 0$ mod 17 then $x4 := r4 * r4[1]^{-}1$ mod 17;
fi;
if $r5[3] <> 0$ mod 17 then $x5 := r5 * r5[3]^{-}1$ mod 17;
elif $r5[2] <> 0$ mod 17 then $x5 := r5 * r5[2]^{-}1$ mod 17;
elif $r5[1] <> 0$ mod 17 then $x5 := r5 * r5[1]^{-}1$ mod 17;
fi;
if $r6[3] <> 0$ mod 17 then $x6 := r6 * r6[3]^{-}1$ mod 17;
elif $r6[2] <> 0$ mod 17 then $x6 := r6 * r6[2]^{-}1$ mod 17;
elif $r6[1] <> 0$ mod 17 then $x6 := r6 * r6[1]^{-}1$ mod 17;
fi;
if $r7[3] <> 0$ mod 17 then $x7 := r7 * r7[3]^{-}1$ mod 17;
elif $r7[2] <> 0$ mod 17 then $x7 := r7 * r7[2]^{-}1$ mod 17;
elif $r7[1] <> 0$ mod 17 then $x7 := r7 * r7[1]^{-}1$ mod 17;
fi;
if Set($[x1, x2, x3, x4, x5, x6, x7]$)=Set($s[j]$) mod 17 then
Print($h, T, j,$ "\n");

fi;
od;od;od;
Here $|s| = 2$, but in fact $|s| = 733$.

6.6 Computing the transformations between the 8-arcs

```
m:=[ [0,1,0],[0,0,1],[14,1,0] ];;
u:=[1,0,0];;
f:=[ ];;
for q in [0 . . 306] do
p := u * m^q mod 17;
if p[3] <> 0 mod 17 then z := p * p[3]^-1 mod 17;
elif p[2] <> 0 mod 17 then z := p * p[2]^-1 mod 17;
elif p[1] <> 0 mod 17 then z := p * p[1]^-1 mod 17;
fi;
Add(f,z);
od;
s:=[[f[1],f[2],f[3],f[254],f[7],f[14],f[28],f[11]],
[f[1],f[2],f[3],f[254],f[7],f[14],f[28],f[13]]
[f[1],f[2],f[3],f[254],f[7],f[14],f[28],f[15]],
[f[1],f[2],f[3],f[254],f[7],f[14],f[28],f[19]],
[f[1],f[2],f[3],f[254],f[7],f[14],f[28],f[20]],
[f[1],f[2],f[3],f[254],f[7],f[14],f[28],f[22]],
[f[1],f[2],f[3],f[254],f[7],f[14],f[28],f[24]],
[f[1],f[2],f[3],f[254],f[7],f[14],f[28],f[26]]];;
w:=Size(s);;
for h in [1 . . w-1] do
for j in [h+1 . . w] do
v:=[ ];;
for i1 in [1 . . 8] do
for i2 in [1 . . 8] do
for i3 in [1 . . 8] do
for i4 in [1 . . 8] do
if i1 <> i2 and i1 <> i3 and i1 <> i4 and i2 <> i3 and i2 <> i4 and
i3 <> i4 then
n := [s[j][i1], s[j][i2], s[j][i3], s[j][i4]];;
Add(v,n);
fi;
od;od;od;od;
for i in [1 . . Length(v)] do
t := v[i];
a1 := t[4][1] * (t[2][2] * t[3][3] - t[3][2] * t[2][3]);
a2 := t[2][1] * (t[4][2] * t[3][3] - t[3][2] * t[4][3]);
a3 := t[3][1] * (t[4][2] * t[2][3] - t[2][2] * t[4][3]);
b1 := t[1][1] * (t[4][2] * t[3][3] - t[3][2] * t[4][3]);
```

$b2 := t[4][1] * (t[1][2] * t[3][3] - t[3][2] * t[1][3]);$
$b3 := t[3][1] * (t[1][2] * t[4][3] - t[4][2] * t[1][3]);$
$c1 := t[1][1] * (t[2][2] * t[4][3] - t[4][2] * t[2][3]);$
$c2 := t[2][1] * (t[1][2] * t[4][3] - t[4][2] * t[1][3]);$
$c3 := t[4][1] * (t[1][2] * t[2][3] - t[2][2] * t[1][3]);$
$a := (a1 - a2 + a3) \bmod 17;$
$b := (b1 - b2 + b3) \bmod 17;$
$c := (c1 - c2 + c3) \bmod 17;$
$T := [[a * t[1][1] \bmod 17,\ a * t[1][2] \bmod 17,\ a * t[1][3] \bmod 17],$
$[b * t[2][1] \bmod 17,\ b * t[2][2] \bmod 17, b * t[2][3] \bmod 17],$
$[c * t[3][1] \bmod 17,\ c * t[3][2] \bmod 17, c * t[3][3] \bmod 17]];$
r1:=(s[h][1]*T) mod 17;
r2:=(s[h][2]* T) mod 17;
r3:=(s[h][3]* T) mod 17;
r4:=(s[h][4]*T) mod 17;
r5:=(s[h][5]* T) mod 17;
r6:=(s[h][6]* T) mod 17;
r7:=(s[h][7]* T) mod 17;
r8:=(s[h][8]* T) mod 17;
if $r1[3] <> 0 \bmod 17$ then $x1 := r1 * r1[3]^{-}1 \bmod 17;$
elif $r1[2] <> 0 \bmod 17$ then $x1 := r1 * r1[2]^{-}1 \bmod 17;$
elif $r1[1] <> 0 \bmod 17$ then $x1 := r1 * r1[1]^{-}1 \bmod 17;$
fi;
if $r2[3] <> 0 \bmod 17$ then $x2 := r2 * r2[3]^{-}1 \bmod 17;$
elif $r2[2] <> 0 \bmod 17$ then $x2 := r2 * r2[2]^{-}1 \bmod 17;$
elif $r2[1] <> 0 mod 17 then x2 := r2 * r2[1]^{-}1 \bmod 17;$
fi;
if $r3[3] <> 0 \bmod 17$ then $x3 := r3 * r3[3]^{-}1 \bmod 17;$
elif $r3[2] <> 0 \bmod 17$ then $x3 := r3 * r3[2]^{-}1 \bmod 17;$
elif $r3[1] <> 0 \bmod 17$ then $x3 := r3 * r3[1]^{-}1 \bmod 17;$
fi;
if $r4[3] <> 0 \bmod 17$ then $x4 := r4 * r4[3]^{-}1 \bmod 17;$
elif $r4[2] <> 0 \bmod 17$ then $x4 := r4 * r4[2]^{-}1 \bmod 17;$
elif $r4[1] <> 0 \bmod 17$ then $x4 := r4 * r4[1]^{-}1 \bmod 17;$
fi;
if $r5[3] <> 0 \bmod 17$ then $x5 := r5 * r5[3]^{-}1 \bmod 17;$
elif $r5[2] <> 0 \bmod 17$ then $x5 := r5 * r5[2]^{-}1 \bmod 17;$
elif $r5[1] <> 0 \bmod 17$ then $x5 := r5 * r5[1]^{-}1 \bmod 17;$
fi;
if $r6[3] <> 0 \bmod 17$ then $x6 := r6 * r6[3]^{-}1 \bmod 17;$
elif $r6[2] <> 0 \bmod 17$ then $x6 := r6 * r6[2]^{-}1 \bmod 17;$
elif $r6[1] <> 0 \bmod 17$ then $x6 := r6 * r6[1]^{-}1 \bmod 17;$
fi;
if $r7[3] <> 0 \bmod 17$ then $x7 := r7 * r7[3]^{-}1 \bmod 17;$
elif $r7[2] <> 0 \bmod 17$ then $x7 := r7 * r7[2]^{-}1 \bmod 17;$

elif $r7[1] <> 0$ mod 17 then $x7 := r7 * r7[1]^{-}1$ mod 17;
fi;
if $r8[3] <> 0$ mod 17 then $x8 := r8 * r8[3]^{-}1$ mod 17;
elif $r8[2] <> 0$ mod 17 then $x8 := r8 * r8[2]^{-}1$ mod 17;
elif $r8[1] <> 0$ mod 17 then $x8 := r8 * r8[1]^{-}1$ mod 17;
fi;
if Set($[x1, x2, x3, x4, x5, x6, x7, x8]$)=Set($s[j]$) mod 17 then
Print($h, T, j,$ "\n");
fi;
od;od;od;

Here in above programme $|s| = 8$, but in fact $|s| = 5441$.

6.7 Computing the transformations between the 9-arcs

```
m:=[ [0,1,0],[0,0,1],[14,1,0] ];;
u:=[1,0,0];;
f:=[ ];;
for q in [0 . . 306] do
p := u * m^q mod 17;
if p[3] <> 0 mod 17 then z := p * p[3]^-1 mod 17;
elif p[2] <> 0 mod 17 then z := p * p[2]^-1 mod 17;
elif p[1] <> 0 mod 17 then z := p * p[1]^-1 mod 17;
fi;
Add(f,z);
od;
s:=[[f[1],f[2],f[3],f[254],f[7],f[14],f[42],f[85],f[136]],
[f[1],f[2],f[3],f[254],f[7],f[14],f[42],f[85],f[153]],
[f[1],f[2],f[3],f[254],f[7],f[14],f[42],f[85],f[168]],
[f[1],f[2],f[3],f[254],f[7],f[14],f[42],f[85],f[176]],
[f[1],f[2],f[3],f[254],f[7],f[14],f[42],f[85],f[186]],
[f[1],f[2],f[3],f[254],f[7],f[14],f[42],f[85],f[188]],
[f[1],f[2],f[3],f[254],f[7],f[14],f[42],f[85],f[206]],
[f[1],f[2],f[3],f[254],f[7],f[14],f[42],f[85],f[270]],
[f[1],f[2],f[3],f[254],f[7],f[14],f[42],f[85],f[299]],
[f[1],f[2],f[3],f[254],f[7],f[14],f[42],f[85],f[301]],
[f[1],f[2],f[3],f[254],f[7],f[14],f[42],f[136],f[85]],
[f[1],f[2],f[3],f[254],f[7],f[14],f[42],f[136],f[153]]];;
w:=Size(s);;
for h in [1 . . w-1] do
for j in [h+1 . . w] do
v:=[ ];;
for i1 in [1 . . 9] do
for i2 in [1 . . 9] do
for i3 in [1 . . 9] do
for i4 in [1 . . 9] do
```

if $i1 <> i2$ and $i1 <> i3$ and $i1 <> i4$ and $i2 <> i3$ and $i2 <> i4$ and $i3 <> i4$ then
$n := [s[j][i1], s[j][i2], s[j][i3], s[j][i4]];;$
Add(v,n);
fi;
od;od;od;od;
for i in [1 . . Length(v)] do
$t := v[i];$
$a1 := t[4][1] * (t[2][2] * t[3][3] - t[3][2] * t[2][3]);$
$a2 := t[2][1] * (t[4][2] * t[3][3] - t[3][2] * t[4][3]);$
$a3 := t[3][1] * (t[4][2] * t[2][3] - t[2][2] * t[4][3]);$
$b1 := t[1][1] * (t[4][2] * t[3][3] - t[3][2] * t[4][3]);$
$b2 := t[4][1] * (t[1][2] * t[3][3] - t[3][2] * t[1][3]);$
$b3 := t[3][1] * (t[1][2] * t[4][3] - t[4][2] * t[1][3]);$
$c1 := t[1][1] * (t[2][2] * t[4][3] - t[4][2] * t[2][3]);$
$c2 := t[2][1] * (t[1][2] * t[4][3] - t[4][2] * t[1][3]);$
$c3 := t[4][1] * (t[1][2] * t[2][3] - t[2][2] * t[1][3]);$
$a := (a1 - a2 + a3)$ mod 17;
$b := (b1 - b2 + b3)$ mod 17;
$c := (c1 - c2 + c3)$ mod 17;
$T := [[a * t[1][1]$ mod 17, $a * t[1][2]$ mod 17, $a * t[1][3]$ mod 17],
$[b * t[2][1]$ mod 17, $b * t[2][2]$ mod 17,$b * t[2][3]$ mod 17],
$[c * t[3][1]$ mod 17, $c * t[3][2]$ mod 17,$c * t[3][3]$ mod 17]];
r1:=(s[h][1]*T) mod 17;
r2:=(s[h][2]* T) mod 17;
r3:=(s[h][3]* T) mod 17;
r4:=(s[h][4]*T) mod 17;
r5:=(s[h][5]* T) mod 17;
r6:=(s[h][6]* T) mod 17;
r7:=(s[h][7]* T) mod 17;
r8:=(s[h][8]* T) mod 17;
r9:=(s[h][9]* T) mod 17;
if $r1[3] <> 0$ mod 17 then $x1 := r1 * r1[3]^-1$ mod 17;
elif $r1[2] <> 0$ mod 17 then $x1 := r1 * r1[2]^-1$ mod 17;
elif $r1[1] <> 0$ mod 17 then $x1 := r1 * r1[1]^-1$ mod 17;
fi;
if $r2[3] <> 0$ mod 17 then $x2 := r2 * r2[3]^-1$ mod 17;
elif $r2[2] <> 0$ mod 17 then $x2 := r2 * r2[2]^-1$ mod 17;
elif $r2[1] <> 0 mod 17 then x2 := r2 * r2[1]^-1$ mod 17;
fi;
if $r3[3] <> 0$ mod 17 then $x3 := r3 * r3[3]^-1$ mod 17;
elif $r3[2] <> 0$ mod 17 then $x3 := r3 * r3[2]^-1$ mod 17;
elif $r3[1] <> 0$ mod 17 then $x3 := r3 * r3[1]^-1$ mod 17;
fi;
if $r4[3] <> 0$ mod 17 then $x4 := r4 * r4[3]^-1$ mod 17;

```
elif r4[2] <> 0 mod 17 then x4 := r4 * r4[2]^-1 mod 17;
elif r4[1] <> 0 mod 17 then x4 := r4 * r4[1]^-1 mod 17;
fi;
if r5[3] <> 0 mod 17 then x5 := r5 * r5[3]^-1 mod 17;
elif r5[2] <> 0 mod 17 then x5 := r5 * r5[2]^-1 mod 17;
elif r5[1] <> 0 mod 17 then x5 := r5 * r5[1]^-1 mod 17;
fi;
if r6[3] <> 0 mod 17 then x6 := r6 * r6[3]^-1 mod 17;
elif r6[2] <> 0 mod 17 then x6 := r6 * r6[2]^-1 mod 17;
elif r6[1] <> 0 mod 17 then x6 := r6 * r6[1]^-1 mod 17;
fi;
if r7[3] <> 0 mod 17 then x7 := r7 * r7[3]^-1 mod 17;
elif r7[2] <> 0 mod 17 then x7 := r7 * r7[2]^-1 mod 17;
elif r7[1] <> 0 mod 17 then x7 := r7 * r7[1]^-1 mod 17;
fi;
if r8[3] <> 0 mod 17 then x8 := r8 * r8[3]^-1 mod 17;
elif r8[2] <> 0 mod 17 then x8 := r8 * r8[2]^-1 mod 17;
elif r8[1] <> 0 mod 17 then x8 := r8 * r8[1]^-1 mod 17;
fi;
if r9[3] <> 0 mod 17 then x9 := r9 * r9[3]^-1 mod 17;
elif r9[2] <> 0 mod 17 then x9 := r9 * r9[2]^-1 mod 17;
elif r9[1] <> 0 mod 17 then x9 := r9 * r9[1]^-1 mod 17;
fi;
if Set([x1, x2, x3, x4, x5, x6, x7, x8, x9])=Set(s[j]) mod 17 then
Print(h, T, j, "\n");
fi;
od;od;od;
```

6.8 Computing the transformations between the 10-arcs

```
m:=[ [0,1,0],[0,0,1],[14,1,0] ];;
u:=[1,0,0];;
f:=[ ];;
for q in [0 . . 306] do
p := u * m^q mod 17;
if p[3] <> 0 mod 17 then z := p * p[3]^-1 mod 17;
elif p[2] <> 0 mod 17 then z := p * p[2]^-1 mod 17;
elif p[1] <> 0 mod 17 then z := p * p[1]^-1 mod 17;
fi;
Add(f,z);
od;
s:=[[ [ 0, 0, 1 ], [ 0, 1, 0 ], [ 1, 0, 0 ], [ 1, 1, 1 ], [ 5, 4, 1 ],
[ 6, 12, 1 ], [ 7, 10, 1 ], [ 9, 11, 1 ], [ 10, 15, 1 ], [ 13, 3, 1 ] ],
[ [ 0, 0, 1 ], [ 0, 1, 0 ], [ 1, 0, 0 ], [ 1, 1, 1 ], [ 3, 12, 1 ],
[ 5, 8, 1 ], [ 8, 7, 1 ], [ 9, 4, 1 ], [ 13, 15, 1 ], [ 16, 5, 1 ] ]];;
```

```
w:=Size(s);;
for h in [1 . . w-1] do
for j in [h+1 . . w] do
v:=[ ];;
for i1 in [1 . . 10] do
for i2 in [1 . . 10] do
for i3 in [1 . . 10] do
for i4 in [1 . . 10] do
if i1 <> i2 and i1 <> i3 and i1 <> i4 and i2 <> i3 and i2 <> i4 and
i3 <> i4 then
n := [s[j][i1], s[j][i2], s[j][i3], s[j][i4]]; ;
Add(v,n);
fi;
od;od;od;od;
for i in [1 . . Length(v)] do
t := v[i];
a1 := t[4][1] * (t[2][2] * t[3][3] - t[3][2] * t[2][3]);
a2 := t[2][1] * (t[4][2] * t[3][3] - t[3][2] * t[4][3]);
a3 := t[3][1] * (t[4][2] * t[2][3] - t[2][2] * t[4][3]);
b1 := t[1][1] * (t[4][2] * t[3][3] - t[3][2] * t[4][3]);
b2 := t[4][1] * (t[1][2] * t[3][3] - t[3][2] * t[1][3]);
b3 := t[3][1] * (t[1][2] * t[4][3] - t[4][2] * t[1][3]);
c1 := t[1][1] * (t[2][2] * t[4][3] - t[4][2] * t[2][3]);
c2 := t[2][1] * (t[1][2] * t[4][3] - t[4][2] * t[1][3]);
c3 := t[4][1] * (t[1][2] * t[2][3] - t[2][2] * t[1][3]);
a := (a1 - a2 + a3) mod 17;
b := (b1 - b2 + b3) mod 17;
c := (c1 - c2 + c3) mod 17;
T := [[a * t[1][1] mod 17, a * t[1][2] mod 17, a * t[1][3] mod 17],
[b * t[2][1] mod 17, b * t[2][2] mod 17,b * t[2][3] mod 17],
[c * t[3][1] mod 17, c * t[3][2] mod 17,c * t[3][3] mod 17]];
r1:=(s[h][1]*T) mod 17;
r2:=(s[h][2]* T ) mod 17;
r3:=(s[h][3]* T ) mod 17;
r4:=(s[h][4]*T) mod 17;
r5:=(s[h][5]* T ) mod 17;
r6:=(s[h][6]* T ) mod 17;
r7:=(s[h][7]* T ) mod 17;
r8:=(s[h][8]* T ) mod 17;
r9:=(s[h][9]* T ) mod 17;
r10:=(s[h][10]* T ) mod 17;
if r1[3] <> 0 mod 17 then x1 := r1 * r1[3]^-1 mod 17;
elif r1[2] <> 0 mod 17 then x1 := r1 * r1[2]^-1 mod 17;
elif r1[1] <> 0 mod 17 then x1 := r1 * r1[1]^-1 mod 17;
fi;
```

```
if r2[3] <> 0 mod 17 then x2 := r2 * r2[3]^-1 mod 17;
elif r2[2] <> 0 mod 17 then x2 := r2 * r2[2]^-1 mod 17;
elif r2[1] <> 0 mod 17 then x2 := r2 * r2[1]^-1 mod 17;
fi;
if r3[3] <> 0 mod 17 then x3 := r3 * r3[3]^-1 mod 17;
elif r3[2] <> 0 mod 17 then x3 := r3 * r3[2]^-1 mod 17;
elif r3[1] <> 0 mod 17 then x3 := r3 * r3[1]^-1 mod 17;
fi;
if r4[3] <> 0 mod 17 then x4 := r4 * r4[3]^-1 mod 17;
elif r4[2] <> 0 mod 17 then x4 := r4 * r4[2]^-1 mod 17;
elif r4[1] <> 0 mod 17 then x4 := r4 * r4[1]^-1 mod 17;
fi;
if r5[3] <> 0 mod 17 then x5 := r5 * r5[3]^-1 mod 17;
elif r5[2] <> 0 mod 17 then x5 := r5 * r5[2]^-1 mod 17;
elif r5[1] <> 0 mod 17 then x5 := r5 * r5[1]^-1 mod 17;
fi;
if r6[3] <> 0 mod 17 then x6 := r6 * r6[3]^-1 mod 17;
elif r6[2] <> 0 mod 17 then x6 := r6 * r6[2]^-1 mod 17;
elif r6[1] <> 0 mod 17 then x6 := r6 * r6[1]^-1 mod 17;
fi;
if r7[3] <> 0 mod 17 then x7 := r7 * r7[3]^-1 mod 17;
elif r7[2] <> 0 mod 17 then x7 := r7 * r7[2]^-1 mod 17;
elif r7[1] <> 0 mod 17 then x7 := r7 * r7[1]^-1 mod 17;
fi;
if r8[3] <> 0 mod 17 then x8 := r8 * r8[3]^-1 mod 17;
elif r8[2] <> 0 mod 17 then x8 := r8 * r8[2]^-1 mod 17;
elif r8[1] <> 0 mod 17 then x8 := r8 * r8[1]^-1 mod 17;
fi;
if r9[3] <> 0 mod 17 then x9 := r9 * r9[3]^-1 mod 17;
elif r9[2] <> 0 mod 17 then x9 := r9 * r9[2]^-1 mod 17;
elif r9[1] <> 0 mod 17 then x9 := r9 * r9[1]^-1 mod 17;
fi;
if r10[3] <> 0 mod 17 then x10 := r10 * r10[3]^-1 mod 17;
elif r10[2] <> 0 mod 17 then x10 := r10 * r10[2]^-1 mod 17;
elif r10[1] <> 0 mod 17 then x10 := r10 * r10[1]^-1 mod 17;
fi;
if Set([x1,x2,x3,x4,x5,x6,x7,x8,x9,x10])=Set(s[j]) mod 17 then
Print(h,T,j,"\n");
fi;
od;od;od;
```

6.9 Computing the transformations between the 11-arcs

```
m:=[ [0,1,0],[0,0,1],[14,1,0] ];;
    u:=[1,0,0];;
```

```
f:=[ ];;
for q in [0 . . 306] do
p := u * m^q mod 17;
if p[3] <> 0 mod 17 then z := p * p[3]^-1 mod 17;
elif p[2] <> 0 mod 17 then z := p * p[2]^-1 mod 17;
elif p[1] <> 0 mod 17 then z := p * p[1]^-1 mod 17;
fi;
Add(f,z);
od;
s:=[[ [ 0, 0, 1 ], [ 0, 1, 0 ], [ 1, 0, 0 ], [ 1, 1, 1 ], [ 3, 8, 1 ],
[ 9, 11, 1 ], [ 10, 15, 1 ], [ 11, 10, 1 ], [ 13, 4, 1 ], [ 14, 16, 1 ],
[ 16, 14, 1 ] ],
[ [ 0, 0, 1 ], [ 0, 1, 0 ], [ 1, 0, 0 ], [ 1, 1, 1 ], [ 3, 8, 1 ],
[ 5, 4, 1 ], [ 9, 11, 1 ], [ 10, 5, 1 ], [ 10, 15, 1 ], [ 11, 10, 1 ],
[ 16, 14, 1 ] ]];;
w:=Size(s);;
for h in [1 . . w-1] do
for j in [h+1 . . w] do
v:=[ ];;
for i1 in [1 . . 11] do
for i2 in [1 . . 11] do
for i3 in [1 . . 11] do
for i4 in [1 . . 11] do
if i1 <> i2 and i1 <> i3 and i1 <> i4 and i2 <> i3 and i2 <> i4 and
i3 <> i4 then
n := [s[j][i1], s[j][i2], s[j][i3], s[j][i4]];;
Add(v,n);
fi;
od;od;od;od;
for i in [1 . . Length(v)] do
t := v[i];
a1 := t[4][1] * (t[2][2] * t[3][3] - t[3][2] * t[2][3]);
a2 := t[2][1] * (t[4][2] * t[3][3] - t[3][2] * t[4][3]);
a3 := t[3][1] * (t[4][2] * t[2][3] - t[2][2] * t[4][3]);
b1 := t[1][1] * (t[4][2] * t[3][3] - t[3][2] * t[4][3]);
b2 := t[4][1] * (t[1][2] * t[3][3] - t[3][2] * t[1][3]);
b3 := t[3][1] * (t[1][2] * t[4][3] - t[4][2] * t[1][3]);
c1 := t[1][1] * (t[2][2] * t[4][3] - t[4][2] * t[2][3]);
c2 := t[2][1] * (t[1][2] * t[4][3] - t[4][2] * t[1][3]);
c3 := t[4][1] * (t[1][2] * t[2][3] - t[2][2] * t[1][3]);
a := (a1 - a2 + a3) mod 17;
b := (b1 - b2 + b3) mod 17;
c := (c1 - c2 + c3) mod 17;
T := [[a * t[1][1] mod 17, a * t[1][2] mod 17, a * t[1][3] mod 17],
[b * t[2][1] mod 17, b * t[2][2] mod 17,b * t[2][3] mod 17],
```

[$c*t$[3][1] mod 17, $c*t$[3][2] mod 17,$c*t$[3][3] mod 17]];
r1:=(s[h][1]*T) mod 17;
r2:=(s[h][2]* T) mod 17;
r3:=(s[h][3]* T) mod 17;
r4:=(s[h][4]*T) mod 17;
r5:=(s[h][5]* T) mod 17;
r6:=(s[h][6]* T) mod 17;
r7:=(s[h][7]* T) mod 17;
r8:=(s[h][8]* T) mod 17;
r9:=(s[h][9]* T) mod 17;
r10:=(s[h][10]* T) mod 17;
r11:=(s[h][11]* T) mod 17;
if $r1[3] <> 0$ mod 17 then $x1 := r1*r1[3]^{-}1$ mod 17;
elif $r1[2] <> 0$ mod 17 then $x1 := r1*r1[2]^{-}1$ mod 17;
elif $r1[1] <> 0$ mod 17 then $x1 := r1*r1[1]^{-}1$ mod 17;
fi;
if $r2[3] <> 0$ mod 17 then $x2 := r2*r2[3]^{-}1$ mod 17;
elif $r2[2] <> 0$ mod 17 then $x2 := r2*r2[2]^{-}1$ mod 17;
elif $r2[1] <> 0 mod 17 then x2 := r2*r2[1]^{-}1$ mod 17;
fi;
if $r3[3] <> 0$ mod 17 then $x3 := r3*r3[3]^{-}1$ mod 17;
elif $r3[2] <> 0$ mod 17 then $x3 := r3*r3[2]^{-}1$ mod 17;
elif $r3[1] <> 0$ mod 17 then $x3 := r3*r3[1]^{-}1$ mod 17;
fi;
if $r4[3] <> 0$ mod 17 then $x4 := r4*r4[3]^{-}1$ mod 17;
elif $r4[2] <> 0$ mod 17 then $x4 := r4*r4[2]^{-}1$ mod 17;
elif $r4[1] <> 0$ mod 17 then $x4 := r4*r4[1]^{-}1$ mod 17;
fi;
if $r5[3] <> 0$ mod 17 then $x5 := r5*r5[3]^{-}1$ mod 17;
elif $r5[2] <> 0$ mod 17 then $x5 := r5*r5[2]^{-}1$ mod 17;
elif $r5[1] <> 0$ mod 17 then $x5 := r5*r5[1]^{-}1$ mod 17;
fi;
if $r6[3] <> 0$ mod 17 then $x6 := r6*r6[3]^{-}1$ mod 17;
elif $r6[2] <> 0$ mod 17 then $x6 := r6*r6[2]^{-}1$ mod 17;
elif $r6[1] <> 0$ mod 17 then $x6 := r6*r6[1]^{-}1$ mod 17;
fi;
if $r7[3] <> 0$ mod 17 then $x7 := r7*r7[3]^{-}1$ mod 17;
elif $r7[2] <> 0$ mod 17 then $x7 := r7*r7[2]^{-}1$ mod 17;
elif $r7[1] <> 0$ mod 17 then $x7 := r7*r7[1]^{-}1$ mod 17;
fi;
if $r8[3] <> 0$ mod 17 then $x8 := r8*r8[3]^{-}1$ mod 17;
elif $r8[2] <> 0$ mod 17 then $x8 := r8*r8[2]^{-}1$ mod 17;
elif $r8[1] <> 0$ mod 17 then $x8 := r8*r8[1]^{-}1$ mod 17;
fi;
if $r9[3] <> 0$ mod 17 then $x9 := r9*r9[3]^{-}1$ mod 17;

```
elif r9[2] <> 0 mod 17 then x9 := r9 * r9[2]^-1 mod 17;
elif r9[1] <> 0 mod 17 then x9 := r9 * r9[1]^-1 mod 17;
fi;
if r10[3] <> 0 mod 17 then x10 := r10 * r10[3]^-1 mod 17;
elif r10[2] <> 0 mod 17 then x10 := r10 * r10[2]^-1 mod 17;
elif r10[1] <> 0 mod 17 then x10 := r10 * r10[1]^-1 mod 17;
fi;
if r11[3] <> 0 mod 17 then x11 := r11 * r11[3]^-1 mod 17;
elif r11[2] <> 0 mod 17 then x11 := r11 * r11[2]^-1 mod 17;
elif r11[1] <> 0 mod 17 then x11 := r11 * r11[1]^-1 mod 17;
fi;
if Set([x1, x2, x3, x4, x5, x6, x7, x8, x9, x10, x11])=Set(s[j]) mod 17 then
Print(h, T, j, "\n");
fi;
od;od;od;
```

6.10 Computing the transformations between the 12-arcs

```
m:=[ [0,1,0],[0,0,1],[14,1,0] ];;
u:=[1,0,0];;
f:=[ ];;
for q in [0 . . 306] do
p := u * m^q mod 17;
if p[3] <> 0 mod 17 then z := p * p[3]^-1 mod 17;
elif p[2] <> 0 mod 17 then z := p * p[2]^-1 mod 17;
elif p[1] <> 0 mod 17 then z := p * p[1]^-1 mod 17;
fi;
Add(f,z);
od;
s:=[[ [ 0, 0, 1 ], [ 0, 1, 0 ], [ 1, 0, 0 ], [ 1, 1, 1 ], [ 2, 3, 1 ],
[ 3, 8, 1 ], [ 4, 2, 1 ], [ 6, 5, 1 ], [ 8, 7, 1 ], [ 9, 11, 1 ],
[ 10, 12, 1 ], [ 16, 4, 1 ] ]];;
w:=Size(s);;
for h in [1 . . w-1] do
for j in [h+1 . . w] do
v:=[ ];;
for i1 in [1 . . 12] do
for i2 in [1 . . 12] do
for i3 in [1 . . 12] do
for i4 in [1 . . 12] do
if i1 <> i2 and i1 <> i3 and i1 <> i4 and i2 <> i3 and i2 <> i4 and
i3 <> i4 then
n := [s[j][i1], s[j][i2], s[j][i3], s[j][i4]];;
Add(v,n);
fi;
```

od;od;od;od;
for i in [1 . . Length(v)] do
$t := v[i]$;
$a1 := t[4][1] * (t[2][2] * t[3][3] - t[3][2] * t[2][3])$;
$a2 := t[2][1] * (t[4][2] * t[3][3] - t[3][2] * t[4][3])$;
$a3 := t[3][1] * (t[4][2] * t[2][3] - t[2][2] * t[4][3])$;
$b1 := t[1][1] * (t[4][2] * t[3][3] - t[3][2] * t[4][3])$;
$b2 := t[4][1] * (t[1][2] * t[3][3] - t[3][2] * t[1][3])$;
$b3 := t[3][1] * (t[1][2] * t[4][3] - t[4][2] * t[1][3])$;
$c1 := t[1][1] * (t[2][2] * t[4][3] - t[4][2] * t[2][3])$;
$c2 := t[2][1] * (t[1][2] * t[4][3] - t[4][2] * t[1][3])$;
$c3 := t[4][1] * (t[1][2] * t[2][3] - t[2][2] * t[1][3])$;
$a := (a1 - a2 + a3)$ mod 17;
$b := (b1 - b2 + b3)$ mod 17;
$c := (c1 - c2 + c3)$ mod 17;
$T := [[a * t[1][1]$ mod 17, $a * t[1][2]$ mod 17, $a * t[1][3]$ mod 17],
[$b * t[2][1]$ mod 17, $b * t[2][2]$ mod 17,$b * t[2][3]$ mod 17],
[$c * t[3][1]$ mod 17, $c * t[3][2]$ mod 17,$c * t[3][3]$ mod 17]];
r1:=(s[h][1]*T) mod 17;
r2:=(s[h][2]* T) mod 17;
r3:=(s[h][3]* T) mod 17;
r4:=(s[h][4]*T) mod 17;
r5:=(s[h][5]* T) mod 17;
r6:=(s[h][6]* T) mod 17;
r7:=(s[h][7]* T) mod 17;
r8:=(s[h][8]* T) mod 17;
r9:=(s[h][9]* T) mod 17;
r10:=(s[h][10]* T) mod 17;
r11:=(s[h][11]* T) mod 17;
r12:=(s[h][12]* T) mod 17;
if $r1[3] <> 0$ mod 17 then $x1 := r1 * r1[3]^-1$ mod 17;
elif $r1[2] <> 0$ mod 17 then $x1 := r1 * r1[2]^-1$ mod 17;
elif $r1[1] <> 0$ mod 17 then $x1 := r1 * r1[1]^-1$ mod 17;
fi;
if $r2[3] <> 0$ mod 17 then $x2 := r2 * r2[3]^-1$ mod 17;
elif $r2[2] <> 0$ mod 17 then $x2 := r2 * r2[2]^-1$ mod 17;
elif $r2[1] <> 0 mod 17 then x2 := r2 * r2[1]^-1$ mod 17;
fi;
if $r3[3] <> 0$ mod 17 then $x3 := r3 * r3[3]^-1$ mod 17;
elif $r3[2] <> 0$ mod 17 then $x3 := r3 * r3[2]^-1$ mod 17;
elif $r3[1] <> 0$ mod 17 then $x3 := r3 * r3[1]^-1$ mod 17;
fi;
if $r4[3] <> 0$ mod 17 then $x4 := r4 * r4[3]^-1$ mod 17;
elif $r4[2] <> 0$ mod 17 then $x4 := r4 * r4[2]^-1$ mod 17;
elif $r4[1] <> 0$ mod 17 then $x4 := r4 * r4[1]^-1$ mod 17;

```
fi;
if r5[3] <> 0 mod 17 then x5 := r5 * r5[3]^-1 mod 17;
elif r5[2] <> 0 mod 17 then x5 := r5 * r5[2]^-1 mod 17;
elif r5[1] <> 0 mod 17 then x5 := r5 * r5[1]^-1 mod 17;
fi;
if r6[3] <> 0 mod 17 then x6 := r6 * r6[3]^-1 mod 17;
elif r6[2] <> 0 mod 17 then x6 := r6 * r6[2]^-1 mod 17;
elif r6[1] <> 0 mod 17 then x6 := r6 * r6[1]^-1 mod 17;
fi;
if r7[3] <> 0 mod 17 then x7 := r7 * r7[3]^-1 mod 17;
elif r7[2] <> 0 mod 17 then x7 := r7 * r7[2]^-1 mod 17;
elif r7[1] <> 0 mod 17 then x7 := r7 * r7[1]^-1 mod 17;
fi;
if r8[3] <> 0 mod 17 then x8 := r8 * r8[3]^-1 mod 17;
elif r8[2] <> 0 mod 17 then x8 := r8 * r8[2]^-1 mod 17;
elif r8[1] <> 0 mod 17 then x8 := r8 * r8[1]^-1 mod 17;
fi;
if r9[3] <> 0 mod 17 then x9 := r9 * r9[3]^-1 mod 17;
elif r9[2] <> 0 mod 17 then x9 := r9 * r9[2]^-1 mod 17;
elif r9[1] <> 0 mod 17 then x9 := r9 * r9[1]^-1 mod 17;
fi;
if r10[3] <> 0 mod 17 then x10 := r10 * r10[3]^-1 mod 17;
elif r10[2] <> 0 mod 17 then x10 := r10 * r10[2]^-1 mod 17;
elif r10[1] <> 0 mod 17 then x10 := r10 * r10[1]^-1 mod 17;
fi;
if r11[3] <> 0 mod 17 then x11 := r11 * r11[3]^-1 mod 17;
elif r11[2] <> 0 mod 17 then x11 := r11 * r11[2]^-1 mod 17;
elif r11[1] <> 0 mod 17 then x11 := r11 * r11[1]^-1 mod 17;
fi;
if r12[3] <> 0 mod 17 then x12 := r12 * r12[3]^-1 mod 17;
elif r12[2] <> 0 mod 17 then x12 := r12 * r12[2]^-1 mod 17;
elif r12[1] <> 0 mod 17 then x12 := r12 * r12[1]^-1 mod 17;
fi;
if Set([x1, x2, x3, x4, x5, x6, x7, x8, x9, x10, x11, x12])=Set(s[j]) mod 17 then
Print(h, T, j, "\n");
fi;
od;od;od;
```

6.11 Computing the transformations between the 13-arcs

```
m:=[ [0,1,0],[0,0,1],[14,1,0] ];;
u:=[1,0,0];;
f:=[ ];;
for q in [0 . . 306] do
p := u * m^q mod 17;
```

```
if p[3] <> 0 mod 17 then z := p * p[3]^-1 mod 17;
elif p[2] <> 0 mod 17 then z := p * p[2]^-1 mod 17;
elif p[1] <> 0 mod 17 then z := p * p[1]^-1 mod 17;
fi;
Add(f,z);
od;
s:=[[ [ 0, 0, 1 ], [ 0, 1, 0 ], [ 1, 0, 0 ], [ 1, 1, 1 ], [ 2, 3, 1 ],
[ 3, 8, 1 ], [ 4, 10, 1 ], [ 7, 4, 1 ], [ 7, 6, 1 ], [ 9, 11, 1 ],
[ 9, 16, 1 ], [ 10, 12, 1 ], [ 16, 15, 1 ] ],
[ [ 0, 0, 1 ], [ 0, 1, 0 ], [ 1, 0, 0 ], [ 1, 1, 1 ], [ 2, 3, 1 ],
[ 3, 8, 1 ], [ 4, 12, 1 ], [ 5, 14, 1 ], [ 6, 5, 1 ], [ 7, 15, 1 ],
[ 9, 11, 1 ], [ 11, 10, 1 ], [ 14, 16, 1 ] ]];;
w:=Size(s);;
for h in [1 . . w-1] do
for j in [h+1 . . w] do
v:=[ ];;
for i1 in [1 . . 13] do
for i2 in [1 . . 13] do
for i3 in [1 . . 13] do
for i4 in [1 . . 13] do
if i1 <> i2 and i1 <> i3 and i1 <> i4 and i2 <> i3 and i2 <> i4 and
i3 <> i4 then
n := [s[j][i1], s[j][i2], s[j][i3], s[j][i4]]; ;
Add(v,n);
fi;
od;od;od;od;
for i in [1 . . Length(v)] do
t := v[i];
a1 := t[4][1] * (t[2][2] * t[3][3] − t[3][2] * t[2][3]);
a2 := t[2][1] * (t[4][2] * t[3][3] − t[3][2] * t[4][3]);
a3 := t[3][1] * (t[4][2] * t[2][3] − t[2][2] * t[4][3]);
b1 := t[1][1] * (t[4][2] * t[3][3] − t[3][2] * t[4][3]);
b2 := t[4][1] * (t[1][2] * t[3][3] − t[3][2] * t[1][3]);
b3 := t[3][1] * (t[1][2] * t[4][3] − t[4][2] * t[1][3]);
c1 := t[1][1] * (t[2][2] * t[4][3] − t[4][2] * t[2][3]);
c2 := t[2][1] * (t[1][2] * t[4][3] − t[4][2] * t[1][3]);
c3 := t[4][1] * (t[1][2] * t[2][3] − t[2][2] * t[1][3]);
a := (a1 − a2 + a3) mod 17;
b := (b1 − b2 + b3) mod 17;
c := (c1 − c2 + c3) mod 17;
T := [[a * t[1][1] mod 17, a * t[1][2] mod 17, a * t[1][3] mod 17],
[b * t[2][1] mod 17, b * t[2][2] mod 17,b * t[2][3] mod 17],
[c * t[3][1] mod 17, c * t[3][2] mod 17,c * t[3][3] mod 17]];
r1:=(s[h][1]*T) mod 17;
r2:=(s[h][2]* T ) mod 17;
```

r3:=(s[h][3]* T) mod 17;
r4:=(s[h][4]*T) mod 17;
r5:=(s[h][5]* T) mod 17;
r6:=(s[h][6]* T) mod 17;
r7:=(s[h][7]* T) mod 17;
r8:=(s[h][8]* T) mod 17;
r9:=(s[h][9]* T) mod 17;
r10:=(s[h][10]* T) mod 17;
r11:=(s[h][11]* T) mod 17;
r12:=(s[h][12]* T) mod 17;
r13:=(s[h][13]* T) mod 17;
if $r1[3] <> 0$ mod 17 then $x1 := r1 * r1[3]^{-}1$ mod 17;
elif $r1[2] <> 0$ mod 17 then $x1 := r1 * r1[2]^{-}1$ mod 17;
elif $r1[1] <> 0$ mod 17 then $x1 := r1 * r1[1]^{-}1$ mod 17;
fi;
if $r2[3] <> 0$ mod 17 then $x2 := r2 * r2[3]^{-}1$ mod 17;
elif $r2[2] <> 0$ mod 17 then $x2 := r2 * r2[2]^{-}1$ mod 17;
elif $r2[1] <> 0mod17thenx2 := r2 * r2[1]^{-}1$ mod 17;
fi;
if $r3[3] <> 0$ mod 17 then $x3 := r3 * r3[3]^{-}1$ mod 17;
elif $r3[2] <> 0$ mod 17 then $x3 := r3 * r3[2]^{-}1$ mod 17;
elif $r3[1] <> 0$ mod 17 then $x3 := r3 * r3[1]^{-}1$ mod 17;
fi;
if $r4[3] <> 0$ mod 17 then $x4 := r4 * r4[3]^{-}1$ mod 17;
elif $r4[2] <> 0$ mod 17 then $x4 := r4 * r4[2]^{-}1$ mod 17;
elif $r4[1] <> 0$ mod 17 then $x4 := r4 * r4[1]^{-}1$ mod 17;
fi;
if $r5[3] <> 0$ mod 17 then $x5 := r5 * r5[3]^{-}1$ mod 17;
elif $r5[2] <> 0$ mod 17 then $x5 := r5 * r5[2]^{-}1$ mod 17;
elif $r5[1] <> 0$ mod 17 then $x5 := r5 * r5[1]^{-}1$ mod 17;
fi;
if $r6[3] <> 0$ mod 17 then $x6 := r6 * r6[3]^{-}1$ mod 17;
elif $r6[2] <> 0$ mod 17 then $x6 := r6 * r6[2]^{-}1$ mod 17;
elif $r6[1] <> 0$ mod 17 then $x6 := r6 * r6[1]^{-}1$ mod 17;
fi;
if $r7[3] <> 0$ mod 17 then $x7 := r7 * r7[3]^{-}1$ mod 17;
elif $r7[2] <> 0$ mod 17 then $x7 := r7 * r7[2]^{-}1$ mod 17;
elif $r7[1] <> 0$ mod 17 then $x7 := r7 * r7[1]^{-}1$ mod 17;
fi;
if $r8[3] <> 0$ mod 17 then $x8 := r8 * r8[3]^{-}1$ mod 17;
elif $r8[2] <> 0$ mod 17 then $x8 := r8 * r8[2]^{-}1$ mod 17;
elif $r8[1] <> 0$ mod 17 then $x8 := r8 * r8[1]^{-}1$ mod 17;
fi;
if $r9[3] <> 0$ mod 17 then $x9 := r9 * r9[3]^{-}1$ mod 17;
elif $r9[2] <> 0$ mod 17 then $x9 := r9 * r9[2]^{-}1$ mod 17;

```
elif r9[1] <> 0 mod 17 then x9 := r9 * r9[1]^-1 mod 17;
fi;
if r10[3] <> 0 mod 17 then x10 := r10 * r10[3]^-1 mod 17;
elif r10[2] <> 0 mod 17 then x10 := r10 * r10[2]^-1 mod 17;
elif r10[1] <> 0 mod 17 then x10 := r10 * r10[1]^-1 mod 17;
fi;
if r11[3] <> 0 mod 17 then x11 := r11 * r11[3]^-1 mod 17;
elif r11[2] <> 0 mod 17 then x11 := r11 * r11[2]^-1 mod 17;
elif r11[1] <> 0 mod 17 then x11 := r11 * r11[1]^-1 mod 17;
fi;
if r12[3] <> 0 mod 17 then x12 := r12 * r12[3]^-1 mod 17;
elif r12[2] <> 0 mod 17 then x12 := r12 * r12[2]^-1 mod 17;
elif r12[1] <> 0 mod 17 then x12 := r12 * r12[1]^-1 mod 17;
fi;
if r13[3] <> 0 mod 17 then x13 := r13 * r13[3]^-1 mod 17;
elif r13[2] <> 0 mod 17 then x13 := r13 * r13[2]^-1 mod 17;
elif r13[1] <> 0 mod 17 then x13 := r13 * r13[1]^-1 mod 17;
fi;
if Set([x1, x2, x3, x4, x5, x6, x7, x8, x9, x10, x11, x12, x13])=Set(s[j]) mod 17 then
Print(h, T, j, "\n");
fi;
od;od;od;
```

6.12 Computing the transformations between the 14-arcs

```
m:=[ [0,1,0],[0,0,1],[14,1,0] ];;
u:=[1,0,0];;
f:=[ ];;
for q in [0 . . 306] do
p := u * m^q mod 17;
if p[3] <> 0 mod 17 then z := p * p[3]^-1 mod 17;
elif p[2] <> 0 mod 17 then z := p * p[2]^-1 mod 17;
elif p[1] <> 0 mod 17 then z := p * p[1]^-1 mod 17;
fi;
Add(f,z);
od;
s:=[[ [ 0, 0, 1 ], [ 0, 1, 0 ], [ 1, 0, 0 ], [ 1, 1, 1 ], [ 2, 16, 1 ],
[ 5, 2, 1 ], [ 8, 9, 1 ], [ 9, 10, 1 ], [ 9, 11, 1 ], [ 10, 5, 1 ],
[ 10, 15, 1 ], [ 13, 8, 1 ], [ 14, 12, 1 ], [ 15, 3, 1 ] ],
[ [ 0, 0, 1 ], [ 0, 1, 0 ], [ 1, 0, 0 ], [ 1, 1, 1 ], [ 3, 16, 1 ],
[ 5, 13, 1 ], [ 6, 7, 1 ], [ 8, 2, 1 ], [ 9, 11, 1 ], [ 9, 12, 1 ],
[ 10, 4, 1 ], [ 10, 15, 1 ], [ 11, 6, 1 ], [ 13, 8, 1 ] ]];;
w:=Size(s);;
for h in [1 . . w-1] do
for j in [h+1 . . w] do
```

```
v:=[ ];;
for i1 in [1 . . 14] do
for i2 in [1 . . 14] do
for i3 in [1 . . 14] do
for i4 in [1 . . 14] do
if i1 <> i2 and i1 <> i3 and i1 <> i4 and i2 <> i3 and i2 <> i4 and
i3 <> i4 then
n := [s[j][i1], s[j][i2], s[j][i3], s[j][i4]]; ;
Add(v,n);
fi;
od;od;od;od;
for i in [1 . . Length(v)] do
t := v[i];
a1 := t[4][1] * (t[2][2] * t[3][3] - t[3][2] * t[2][3]);
a2 := t[2][1] * (t[4][2] * t[3][3] - t[3][2] * t[4][3]);
a3 := t[3][1] * (t[4][2] * t[2][3] - t[2][2] * t[4][3]);
b1 := t[1][1] * (t[4][2] * t[3][3] - t[3][2] * t[4][3]);
b2 := t[4][1] * (t[1][2] * t[3][3] - t[3][2] * t[1][3]);
b3 := t[3][1] * (t[1][2] * t[4][3] - t[4][2] * t[1][3]);
c1 := t[1][1] * (t[2][2] * t[4][3] - t[4][2] * t[2][3]);
c2 := t[2][1] * (t[1][2] * t[4][3] - t[4][2] * t[1][3]);
c3 := t[4][1] * (t[1][2] * t[2][3] - t[2][2] * t[1][3]);
a := (a1 - a2 + a3) mod 17;
b := (b1 - b2 + b3) mod 17;
c := (c1 - c2 + c3) mod 17;
T := [[a * t[1][1] mod 17, a * t[1][2] mod 17, a * t[1][3] mod 17],
[b * t[2][1] mod 17, b * t[2][2] mod 17,b * t[2][3] mod 17],
[c * t[3][1] mod 17, c * t[3][2] mod 17,c * t[3][3] mod 17]];
r1:=(s[h][1]*T) mod 17;
r2:=(s[h][2]* T ) mod 17;
r3:=(s[h][3]* T ) mod 17;
r4:=(s[h][4]*T) mod 17;
r5:=(s[h][5]* T ) mod 17;
r6:=(s[h][6]* T ) mod 17;
r7:=(s[h][7]* T ) mod 17;
r8:=(s[h][8]* T ) mod 17;
r9:=(s[h][9]* T ) mod 17;
r10:=(s[h][10]* T ) mod 17;
r11:=(s[h][11]* T ) mod 17;
r12:=(s[h][12]* T ) mod 17;
r13:=(s[h][13]* T ) mod 17;
r14:=(s[h][14]* T ) mod 17;
if r1[3] <> 0 mod 17 then x1 := r1 * r1[3]^-1 mod 17;
elif r1[2] <> 0 mod 17 then x1 := r1 * r1[2]^-1 mod 17;
elif r1[1] <> 0 mod 17 then x1 := r1 * r1[1]^-1 mod 17;
```

fi;
if $r2[3] <> 0$ mod 17 then $x2 := r2 * r2[3]^{-}1$ mod 17;
elif $r2[2] <> 0$ mod 17 then $x2 := r2 * r2[2]^{-}1$ mod 17;
elif $r2[1] <> 0mod17thenx2 := r2 * r2[1]^{-}1$ mod 17;
fi;
if $r3[3] <> 0$ mod 17 then $x3 := r3 * r3[3]^{-}1$ mod 17;
elif $r3[2] <> 0$ mod 17 then $x3 := r3 * r3[2]^{-}1$ mod 17;
elif $r3[1] <> 0$ mod 17 then $x3 := r3 * r3[1]^{-}1$ mod 17;
fi;
if $r4[3] <> 0$ mod 17 then $x4 := r4 * r4[3]^{-}1$ mod 17;
elif $r4[2] <> 0$ mod 17 then $x4 := r4 * r4[2]^{-}1$ mod 17;
elif $r4[1] <> 0$ mod 17 then $x4 := r4 * r4[1]^{-}1$ mod 17;
fi;
if $r5[3] <> 0$ mod 17 then $x5 := r5 * r5[3]^{-}1$ mod 17;
elif $r5[2] <> 0$ mod 17 then $x5 := r5 * r5[2]^{-}1$ mod 17;
elif $r5[1] <> 0$ mod 17 then $x5 := r5 * r5[1]^{-}1$ mod 17;
fi;
if $r6[3] <> 0$ mod 17 then $x6 := r6 * r6[3]^{-}1$ mod 17;
elif $r6[2] <> 0$ mod 17 then $x6 := r6 * r6[2]^{-}1$ mod 17;
elif $r6[1] <> 0$ mod 17 then $x6 := r6 * r6[1]^{-}1$ mod 17;
fi;
if $r7[3] <> 0$ mod 17 then $x7 := r7 * r7[3]^{-}1$ mod 17;
elif $r7[2] <> 0$ mod 17 then $x7 := r7 * r7[2]^{-}1$ mod 17;
elif $r7[1] <> 0$ mod 17 then $x7 := r7 * r7[1]^{-}1$ mod 17;
fi;
if $r8[3] <> 0$ mod 17 then $x8 := r8 * r8[3]^{-}1$ mod 17;
elif $r8[2] <> 0$ mod 17 then $x8 := r8 * r8[2]^{-}1$ mod 17;
elif $r8[1] <> 0$ mod 17 then $x8 := r8 * r8[1]^{-}1$ mod 17;
fi;
if $r9[3] <> 0$ mod 17 then $x9 := r9 * r9[3]^{-}1$ mod 17;
elif $r9[2] <> 0$ mod 17 then $x9 := r9 * r9[2]^{-}1$ mod 17;
elif $r9[1] <> 0$ mod 17 then $x9 := r9 * r9[1]^{-}1$ mod 17;
fi;
if $r10[3] <> 0$ mod 17 then $x10 := r10 * r10[3]^{-}1$ mod 17;
elif $r10[2] <> 0$ mod 17 then $x10 := r10 * r10[2]^{-}1$ mod 17;
elif $r10[1] <> 0$ mod 17 then $x10 := r10 * r10[1]^{-}1$ mod 17;
fi;
if $r11[3] <> 0$ mod 17 then $x11 := r11 * r11[3]^{-}1$ mod 17;
elif $r11[2] <> 0$ mod 17 then $x11 := r11 * r11[2]^{-}1$ mod 17;
elif $r11[1] <> 0$ mod 17 then $x11 := r11 * r11[1]^{-}1$ mod 17;
fi;
if $r12[3] <> 0$ mod 17 then $x12 := r12 * r12[3]^{-}1$ mod 17;
elif $r12[2] <> 0$ mod 17 then $x12 := r12 * r12[2]^{-}1$ mod 17;
elif $r12[1] <> 0$ mod 17 then $x12 := r12 * r12[1]^{-}1$ mod 17;
fi;

```
if r13[3] <> 0 mod 17 then x13 := r13 * r13[3]^-1 mod 17;
elif r13[2] <> 0 mod 17 then x13 := r13 * r13[2]^-1 mod 17;
elif r13[1] <> 0 mod 17 then x13 := r13 * r13[1]^-1 mod 17;
fi;
if r14[3] <> 0 mod 17 then x14 := r14 * r14[3]^-1 mod 17;
elif r14[2] <> 0 mod 17 then x14 := r14 * r14[2]^-1 mod 17;
elif r14[1] <> 0 mod 17 then x14 := r14 * r14[1]^-1 mod 17;
fi;
if Set([x1,x2,x3,x4,x5,x6,x7,x8,x9,x10,x11,x12,x13,x14])=Set(s[j]) mod 17 then
Print(h,T,j,"\n");
fi;
od;od;od;
```

6.13 Computing the complete $(k;2)$-arcs

```
m:=[ [0,1,0],[0,0,1],[14,1,0] ];;
u:=[1,0,0];;
f:=[ ];;
for q in [0 . . 306] do
p := u * m^q mod 17;
if p[3] <> 0 mod 17 then z := p * p[3]^-1 mod 17;
elif p[2] <> 0 mod 17 then z := p * p[2]^-1 mod 17;
elif p[1] <> 0 mod 17 then z := p * p[1]^-1 mod 17;
fi;
Add(f,z);
od;
l:= the set of lines
s:=[[ [ 0, 0, 1 ], [ 0, 1, 0 ], [ 1, 0, 0 ], [ 1, 1, 1 ], [ 2, 16, 1 ],
[ 5, 4, 1 ], [ 6, 2, 1 ], [ 7, 12, 1 ], [ 9, 11, 1 ], [ 11, 7, 1 ],
[ 16, 13, 1 ] ]];;
o:=[];;
for i in [1..1] do
10a:=s[i]; vv:=[];;
w:=Difference(f,10a);
for jj in w do
ch:=[];;
11a:=[f[1],f[2],f[3],f[254],10a[5],10a[6],10a[7],10a[8],10a[9],10a[10],10a[11],jj];
for j in [1..307] do
l3:=l[j];
if Size(Intersection(11a,l3))=3 then
Add(ch,j);
fi;
od;
if Size(ch) = 0 then Add(vv,jj); fi;
od; if Size(vv)=0 then Add(o,10a); fi; od;
```

6.14 Computing the complete $(k;3)$-arcs

```
m:=[ [0,1,0],[0,0,1],[14,1,0] ];;
u:=[1,0,0];;
f:=[ ];;
for q in [0 . . 306] do
p := u * m^q mod 17;
if p[3] <> 0 mod 17 then z := p * p[3]^-1 mod 17;
elif p[2] <> 0 mod 17 then z := p * p[2]^-1 mod 17;
elif p[1] <> 0 mod 17 then z := p * p[1]^-1 mod 17;
fi;
Add(f,z);
od;
l:= the set of lines
s:=[ [ [ 0, 3, 1 ], [ 0, 11, 1 ], [ 5, 0, 1 ], [ 10, 5, 1 ], [ 14, 11, 1 ],
[ 10, 2, 1 ], [ 10, 11, 1 ], [ 3, 16, 1 ], [ 14, 7, 1 ], [ 15, 6, 1 ],
[ 14, 4, 1 ], [ 7, 9, 1 ],[0,0,1],[1,1,0],[1,4,1],[1,8,1],[2,4,1],[3,1,0],
[3,9,1],[3,12,1],[5,13,1],[6,6,1],[7,13,1] ]];;
o:=[];;
for i in [1..1] do
10a:=s[i]; vv:=[];;
w:=Difference(f,10a);
for jj in w do
ch:=[];;
11a:=[ [ 0, 3, 1 ], [ 0, 11, 1 ], [ 5, 0, 1 ], [ 10, 5, 1 ], [ 14, 11, 1 ],
[ 10, 2, 1 ], [ 10, 11, 1 ], [ 3, 16, 1 ], [ 14, 7, 1 ], [ 15, 6, 1 ],
[ 14, 4, 1 ], [ 7, 9, 1 ],[0,0,1],[1,1,0],[1,4,1],[1,8,1],[2,4,1],[3,1,0],
[3,9,1],[3,12,1],[5,13,1],[6,6,1],[7,13,1] ,jj];
for j in [1..307] do
l3:=l[j];
if Size(Intersection(11a,l3))=4 then
Add(ch,j);
fi;
od;
if Size(ch) = 0 then Add(vv,jj); fi;
od; if Size(vv)=0
then Add(o,10a);
fi;
od;
```

7. APPENDIX 2

The points of $PG(2,17)$ in numeral and vector forms

Tab. 7.1: The points of $PG(2,17)$ generated by $(010, 001, -310)$

1	$1\,0\,0$	2	$0\,1\,0$	3	$0\,0\,1$	4	$-3\,1\,0$	5	$0\,-3\,1$	6	$1\,-6\,1$
7	$-8\,-6\,1$	8	$-8\,4\,1$	9	$-5\,-6\,1$	10	$-8\,-5\,1$	11	$4\,-2\,1$	12	$-7\,6\,1$
13	$8\,-1\,1$	14	$3\,8\,1$	15	$6\,-8\,1$	16	$-6\,-3\,1$	17	$1\,-4\,1$	18	$5\,8\,1$
19	$6\,5\,1$	20	$-4\,-2\,1$	21	$-7\,-7\,1$	22	$-2\,-4\,1$	23	$5\,-4\,1$	24	$5\,7\,1$
25	$2\,-4\,1$	26	$5\,-5\,1$	27	$4\,-8\,1$	28	$-6\,-7\,1$	29	$-2\,8\,1$	30	$6\,2\,1$
31	$7\,-5\,1$	32	$4\,-5\,1$	33	$4\,-1\,1$	34	$3\,-5\,1$	35	$4\,6\,1$	36	$8\,-2\,1$
37	$-7\,4\,1$	38	$-5\,7\,1$	39	$2\,-3\,1$	40	$1\,-1\,1$	41	$3\,-2\,1$	42	$-7\,-2\,1$
43	$-7\,3\,1$	44	$-1\,-2\,1$	45	$-7\,0\,1$	46	$1\,2\,0$	47	$0\,-8\,1$	48	$-6\,2\,1$
49	$7\,6\,1$	50	$8\,7\,1$	51	$2\,-6\,1$	52	$-8\,8\,1$	53	$6\,-3\,1$	54	$1\,-8\,1$
55	$-6\,4\,1$	56	$-5\,3\,1$	57	$-1\,-7\,1$	58	$-2\,0\,1$	59	$3\,1\,0$	60	$0\,3\,1$
61	$-1\,6\,1$	62	$8\,0\,1$	63	$-6\,1\,0$	64	$0\,-6\,1$	65	$-8\,-3\,1$	66	$1\,8\,1$
67	$6\,-4\,1$	68	$5\,-6\,1$	69	$-8\,-1\,1$	70	$3\,7\,1$	71	$2\,3\,1$	72	$-1\,1\,1$
73	$-3\,0\,1$	74	$-7\,1\,0$	75	$0\,-7\,1$	76	$-2\,-5\,1$	77	$4\,7\,1$	78	$2\,8\,1$
79	$6\,-6\,1$	80	$-8\,-4\,1$	81	$5\,6\,1$	82	$8\,1\,1$	83	$-3\,-8\,1$	84	$-6\,-4\,1$
85	$5\,-3\,1$	86	$1\,-2\,1$	87	$-7\,-1\,1$	88	$3\,6\,1$	89	$8\,-5\,1$	90	$4\,5\,1$
91	$-4\,1\,1$	92	$-3\,-3\,1$	93	$1\,-5\,1$	94	$4\,3\,1$	95	$-1\,-4\,1$	96	$5\,0\,1$

97	8 1 0	98	0 8 1	99	6 −2 1	100	−7 5 1	101	−4 −8 1	102	−6 −6 1
103	−8 −2 1	104	−7 −5 1	105	4 8 1	106	6 7 1	107	2 1 1	108	−3 3 1
109	−1 5 1	110	−4 0 1	111	1 1 0	112	0 1 1	113	−3 1 1	114	−3 −2 1
115	−7 1 1	116	−3 −6 1	117	−8 6 1	118	8 −4 1	119	5 2 1	120	7 3 1
121	−1 −3 1	122	1 0 1	123	1 5 0	124	0 7 1	125	2 5 1	126	−4 4 1
127	−5 −5 1	128	4 −6 1	129	−8 2 1	130	7 5 1	131	−4 5 1	132	−4 −4 1
133	5 5 1	134	−4 8 1	135	6 6 1	136	8 4 1	137	−5 −2 1	138	−7 2 1
139	7 −3 1	140	1 3 1	141	−1 −5 1	142	4 0 1	143	−4 1 0	144	0 −4 1
145	5 4 1	146	−5 −7 1	147	−2 3 1	148	−1 −6 1	149	−8 0 1	150	−2 1 0
151	0 −2 1	152	−7 8 1	153	6 −5 1	154	4 2 1	155	7 −6 1	156	−8 −7 1
157	−2 1 1	158	−3 −1 1	159	3 2 1	160	7 2 1	161	7 4 1	162	−5 2 1
163	7 −2 1	164	−7 −4 1	165	5 −7 1	166	−2 4 1	167	−5 4 1	168	−5 −1 1
169	3 4 1	170	−5 1 1	171	−3 −4 1	172	5 −8 1	173	−6 −5 1	174	4 1 1
175	−3 5 1	176	−4 3 1	177	−1 −1 1	178	3 0 1	179	−5 1 0	180	0 −5 1
181	4 −7 1	182	−2 −8 1	183	−6 −2 1	184	−7 −6 1	185	−8 1 1	186	−3 −7 1
187	−2 −7 1	188	−2 5 1	189	−4 −7 1	190	−2 −2 1	191	−7 −8 1	192	−6 5 1
193	−4 −1 1	194	3 3 1	195	−1 7 1	196	2 0 1	197	1 −1 0	198	0 −1 1
199	3 −1 1	200	3 −4 1	201	5 −1 1	202	3 −6 1	203	−8 5 1	204	−4 2 1
205	7 7 1	206	2 6 1	207	8 −8 1	208	−6 1 1	209	−3 −5 1	210	4 −3 1

211	1 4 1	212	−5 − 8 1	213	−6 − 8 1	214	−6 7 1	215	2 − 8 1	216	−6 6 1
217	8 2 1	218	7 − 4 1	219	5 − 2 1	220	−7 − 3 1	221	1 2 1	222	7 1 1
223	−3 8 1	224	6 4 1	225	−5 6 1	226	8 5 1	227	−4 − 5 1	228	4 4 1
229	−5 − 3 1	230	1 7 1	231	2 − 7 1	232	−2 2 1	233	7 8 1	234	6 1 1
235	−3 7 1	236	2 7 1	237	2 − 2 1	238	−7 7 1	239	2 4 1	240	−5 5 1
241	−4 6 1	242	8 8 1	243	6 − 1 1	244	3 − 7 1	245	−2 − 3 1	246	1 6 1
247	8 6 1	248	8 − 7 1	249	−2 6 1	250	8 − 3 1	251	1 − 3 1	252	1 5 1
253	−4 − 3 1	254	1 1 1	255	−3 2 1	256	7 − 1 1	257	3 − 8 1	258	−6 8 1
259	6 − 7 1	260	−2 − 1 1	261	3 1 1	262	−3 4 1	263	−5 8 1	264	6 8 1
265	6 3 1	266	−1 8 1	267	6 0 1	268	2 1 0	269	0 2 1	270	7 − 8 1
271	−6 − 1 1	272	3 5 1	273	−4 − 6 1	274	−8 − 8 1	275	−6 3 1	276	−1 4 1
277	−5 0 1	278	5 1 0	279	0 5 1	280	−4 7 1	281	2 2 1	282	7 − 7 1
283	−2 − 6 1	284	−8 3 1	285	−1 − 8 1	286	−6 0 1	287	3 5 0	288	0 4 1
289	−5 − 4 1	290	5 1 1	291	−3 6 1	292	8 − 6 1	293	−8 7 1	294	2 − 1 1
295	3 − 3 1	296	1 − 7 1	297	−2 7 1	298	2 − 5 1	299	4 − 4 1	300	5 3 1
301	−1 2 1	302	7 0 1	303	2 6 0	304	0 6 1	305	8 3 1	306	−1 3 1
307	−1 0 1										

BIBLIOGRAPHY

[1] A.H. Ali, Classification of Arcs in Galois Plane of Order Thirteen, Ph.D. Thesis, University of Sussex, 1993.

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

[3] M. Aghaei, Near Maximum Distance Separable Codes Over The Field of Eleven Elements, Ph.D. Thesis, University of Sussex, 2005.

[4] S.M. Ball, On Sets of Points in Finite Planes, Ph.D. Thesis, University of Sussex, 1994.

[5] M.E. Contreras, Arcs and Curves Over a Finite Field and Their Points, Ph.D. Thesis, University of Sussex, 2003.

[6] V.D. Goppa. Codes on algebraic curves, *Soviet Math. Dokl.*, 24 (1981), 170-172.

[7] L. Giuzzi, Hermitian Varieties Over a Finite Field, Ph.D. Thesis, University of Sussex, 2000.

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

[9] J.W.P. Hirschfeld, G. Korchmáros and F.Torres, *Algebraic Curves Over a Finite Field*, Oxford University Press, Oxford, 2007.

[10] J.W.P. Hirschfeld, *Projective Geometries Over Finite Fields, Second Edition*, Oxford University Press, Oxford, 555 + xiv pp., 1998.

[11] J.W.P. Hirschfeld, Complete Arcs, *Discrete Math.*, 174 (1997), 177-184.

[12] J.W.P. Hirschfeld and A. Sadeh, The Projective Plane Over The Field of Eleven Elements, *Mitt. Math. Sem. Giessen*, 164 (1984), 245-257.

[13] R. Hill, *A First Course in Coding Theory*, Clarendon Press, Oxford 1986.

[14] S. Packer, On Sets of Odd Type and Caps in Galois Geometries of Order Four, Ph.D. Thesis, University of Sussex, 1995.

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

[16] A. Sonnino, Ovals and Arcs in Finite Projective Planes, Ph.D. Thesis, University of Sussex, 2004.

[17] A.D. Thomas and G.V. Wood, *Group Tables*, Shiva Publishing Limited, 1980.

[18] H.M. Tabrizi, Pencils of Conics in The Galois Planes of Order q, Ph.D. Thesis, University of Sussex, 1990.

[19] S.K. Vereecke, Some Properties of Arcs, Caps and Quadrics in Projective Spaces of Finite Order, Ph.D. Thesis, University of Sussex, 1998.

[20] A.L. Yasin, Cubic Arcs in The Projective Plane of Order Eight, Ph.D. Thesis, University of Sussex, 1986.

[21] M.O. Yazdi, The Classification of $(k;3)$-arcs Over The Galois Field of Order Five, Ph.D. Thesis, University of Sussex, 1983.