THE UNIVERSITY OF SUSSEX

Arcs in a Finite Projective Plane

G.R. Cook

Submitted for the degree of D.Phil.

July 2011

I hereby declare that this thesis has not and will not be submitted in whole or in part to another university for the award of any other degree.

G.R. Cook

Acknowledgements

I would first like to thank Professor James Hirschfeld for both the excellent level of support and helpful advice that I have received while under his supervision.

I would also like to thank my parents Alan and Gwen, as it was their support and backing that allowed me to pursue my DPhil.

Abstract

The projective plane of order 11 is the dominant focus of this work. The motivation for working in the projective plane of order 11 is twofold. First, it is the smallest projective plane of prime power order such that the size of the largest (n, r)-arc is not known for all $r \in \{2, \ldots, q+1\}$. It is also the smallest projective plane of prime order such that the $(n, 3)$-arcs are not classified. Second, the number of $(n, 3)$-arcs is significantly higher in the projective plane of order 11 than it is in the projective plane of order 7, giving a large number of $(n, 3)$-arcs for study.

The main application of (n, r)-arcs is to the study of linear codes.

As a forerunner to the work in the projective plane of order eleven two algorithms are used to raise the lower bound on the size of the smallest complete n-arc in the projective plane of order thirty-one from 12 to 13.

This work presents the classification up to projective equivalence of the complete $(n, 3)$-arcs in $PG(2, 11)$ and the backtracking algorithm that is used in its construction. This algorithm is based on the algorithm used in [3]; it is adapted to work on $(n, 3)$-arcs as opposed to n-arcs. This algorithm yields one representative from every projectively inequivalent class of $(n, 3)$-arc. The equivalence classes of complete $(n, 3)$-arcs are then further classified according to their stabilizer group.

The classification of all $(n, 3)$-arcs up to projective equivalence in $PG(2, 11)$ is the foundation of an exhaustive search that takes one element from every equivalence class and determines if it can be extended to an $(n', 4)$-arc. This search confirmed that in $PG(2, 11)$ no $(n, 3)$-arc can be extended to a $(33, 4)$-arc and that subsequently $m_4(2, 11) = 32$. This same algorithm is used to determine four projectively inequivalent complete $(32, 4)$-arcs, extended from complete $(n, 3)$-arcs.

Various notions under the general title of symmetry are defined both for an (n, r)-arc and for sets of points and lines. The first of these makes the classification of incomplete $(n, 3)$-arcs in $PG(2, 11)$ practical. The second establishes a symmetry based around the incidence structure of each of the four projectively inequivalent complete $(32, 4)$-arcs in $PG(2, 11)$; this allows the discovery of their duals. Both notions of symmetry are used to analyze the incidence structure of n-arcs in $PG(2, q)$, for $q = 11, 13, 17, 19$.

The penultimate chapter demonstrates that it is possible to construct an (n, r)-arc with a stabilizer group that contains a subgroup of order p, where p is a prime, without reference to an $(m < n, r)$-arc, with stabilizer group isomorphic to $\mathbf{Z}_1$. This method is used to find q-arcs and $(q+1)$-arcs in $PG(2, q)$, for $q = 23$ and 29, supporting Conjecture 6.7.

The work ends with an investigation into the effect of projectivities that are induced by a matrix of prime order p on the projective planes. This investigation looks at the points and subsets of points of order p that are closed under the right action of such matrices and their structure in the projective plane. An application of these structures is a restriction on the size of an (n, r)-arc in $PG(2, q)$ that can be stabilized by a matrix of prime order p.

Contents

List of Tables

Chapter 1

Introduction

1.1 Introduction

The projective plane or order 11 is the dominant focus of this work. The motivation for working in the projective plane of order 11 is twofold. First, it is the smallest projective plane of prime power order such that the size of the largest (n, r)-arc is not known for all $r \in \{2, \ldots, q+1\}$; Table 1.1 shows that in $PG(2, 11)$ the size of the largest $(n, 4)$-arc, $(n, 5)$-arc, $(n, 9)$-arc and $(n, 10)$-arc is unknown. It is also the smallest projective plane of prime order such that the $(n, 3)$-arcs are not classified; in [11] the $(n, 3)$-arcs in $PG(2, 7)$ are classified. Second, the number of $(n, 3)$-arcs is significantly higher in the projective plane of order 11 than it is in the projective plane of order 7, giving a large number of $(n, 3)$-arcs for study; in $PG(2, 7)$ there are only a few thousand classes of projectively equivalent $(n, 3)$-arcs and in $PG(2, 11)$ there are more than 252 million.

The main application of (n, r)-arcs is to the study of linear codes, as an $(n, n-d)$-arc in $PG(k-1, q)$ is equivalent to an $[n, k, d]_q$-code; details are given in Section 1.9.

In Chapters 2, 3, 4, 5, 6, 7 and 8, the research on which this thesis is based is described as it evolved over time. The remainder of Chapter 1 introduces all those ideas from Group Theory, Finite Field Theory and Projective Geometry that are needed for a full understanding of later chapters.

Chapters 2 and 3 feature the classification of (n, r)-arcs in the projective plane up to projective equivalence. In Chapter 2, n-arcs are classified in $PG(2, 29)$. In Chapter 3, $(n, 3)$-arcs are classified in $PG(2, 11)$. In both Chapters 2 and 3, an adapted version of the algorithm that is introduced in [3] is used for implementing the classification. This algorithm is described fully in Chapter 3 including ideas for its improvement that developed during its implementation.

In Chapter 2, n-arcs are classified up to projective equivalence, for $n \leq 8$ and a new algorithm is used to expand these 8-arcs to 12-arcs and 13-arcs, for the purpose of determining the existence of complete 12-arcs and complete 13-arcs; the previously known smallest complete n-arc in $PG(2, 29)$ consisted of 14 points. This was partially successful as this algorithm determined the non-existence of complete 12-arcs but it is too inefficient to determine the non-existence of complete 13-arcs on a single PC in a reasonable amount of time.

Chapter 3 features the full classification of $(n, 3)$-arcs in $PG(2, 11)$ up to projective equivalence and a further classification of complete $(n, 3)$-arcs as determined by their stabilizer

group. Sections 1.2.3 - 1.2.10 give a description of all groups of order less than or equal to 24 up to isomorphism and all the groups of larger order that are present in this classification.

In Chapter 4, the classification of $(n, 3)$-arcs in $PG(2, 11)$ up to projective equivalence, as presented in Chapter 3, is used in a new algorithm to determine that no $(n, 3)$-arc can be extended to a $(33, 4)$-arc. By the existence of a $(32, 4)$-arc, the largest $(n, 4)$-arcs in $PG(2, 11)$ consists of 32 points. This same algorithm is used to determine that there are 4 classes of projectively equivalent complete $(32, 4)$-arcs that are attainable by extending complete $(n, 3)$-arcs and these are described in Section 4.2.

From an investigation into the equations of Lemma 1.62, an idea called symmetry has been developed together with supporting notation; this idea of symmetry is a relationship between lines as described by the points with which they are incident and points as described by the lines with which they are incident, all in relation to a given (n, r)-arc in $PG(2, q)$. This relationship is described fully in Chapter 5 together with an extended example showing the symmetry between the first of the four $(32, 4)$-arcs in $PG(2, 11)$ and its duals; brief descriptions of the duals of the other three $(32, 4)$-arcs in $PG(2, 11)$ are also given.

A link between the symmetrical properties of (n, r)-arcs in $PG(2, q)$ and their stabilizer groups is explored in Chapter 6, with a number of questions posed and conjectures formulated. This link is used to finish the work of classifying $(n, 3)$-arcs in $PG(2, 11)$ by classifying all incomplete $(n, 3)$-arcs by their stabilizer group as described in Chapter 6. Information linking the symmetrical properties of n-arcs with their stabilizer group is displayed, for $q = 11, 13, 17, 19$. Conjectures are formulated about the continuation of these links to higher values of q.

The ideas in Chapter 7 demonstrate that it is possible to classify all (n, r)-arcs in $PG(2, q)$ that possess a stabilizer group with a subgroup that is isomorphic to $\mathbf{Z}_p$, where p is a prime, without the need to calculate every $(m < n, r)$-arc with stabilizer group isomorphic to $\mathbf{Z}_1$, which constitutes the majority of cases. Tests have demonstrated that q-arcs and $q+1$-arcs in $PG(2, 23)$ and $PG(2, 29)$ as well as $(23, 3)$-arcs in $PG(2, 13)$ can be very quickly constructed using this method.

The final chapter determines the effect of projectivities induced by a matrix of prime order p on the projective planes. In particular it determines how many points are closed under the right action of such a matrix and their structure; all other points are in a subset of order p that is closed under the right action of this matrix. This information is determined, for all $p > 3$, with $p = 2$ and $p = 3$ handled as special cases. The structure of the points in $PG(2, q)$ that are closed under the right action of such prime order matrices, for differing instances of p and q are interesting in their right, but it is studied here as it provides a good starting point from which to work on the symmetrical properties described in Chapters 5 and 6. An application of these structures is a restriction on the size of an (n, r)-arc in $PG(2, q)$ that can be stabilized by a matrix of prime order p.

1.2 Group Theory

Definitions 1.1, 1.2 and 1.3 describe three different types of map from a group G into a group H that preserve the structure of G in H.

1.2.1 Mappings and the Automorphism Group

Let S and T be finite sets that are closed under some binary operations; possibly groups or fields.

Definition 1.1. A map $f : S \to T$ is called a *homomorphism* of S into T if and only if

$$(s_1 s_2)f = (s_1)f(s_2)f,$$

for all $s_1, s_2 \in S$.

Definition 1.2. A homomorphism $f : S \to T$ is called an *isomorphism* of S into T if and only if f is a bijection. Two sets S and T are called *isomorphic* if and only if there exists an isomorphism between them; such a relationship is denoted $S \cong T$.

Definition 1.3. An isomorphism of S into S is called an *automorphism* of S.

The *automorphism group of* S $\mathrm{aut}(S)$ is the set of all automorphisms of S together with the operation of composition of maps. So, for $f_1, f_2 \in \mathrm{aut}(S)$, $(s)f_1 f_2 = ((s)f_1)f_2$, $\forall s \in S$. The identity of $\mathrm{aut}(S)$ is i, where $(s)i = s$, $\forall s \in S$ and for every $f \in \mathrm{aut}(S)$ there exists an $f^{-1} \in \mathrm{aut}(S)$ such that $((s)f)f^{-1} = ((s)f^{-1})f = s$, $\forall s \in S$.

1.2.2 Cyclic groups

Let G be a finite group that contains an element g of order m. The subgroup $\mathbf{C}_m$ is generated by a single element of G; that is,

$$\mathbf{C}_m = \langle g \rangle = \{1, g, g^2, \ldots, g^{m-1}\}.$$

Multiplication is determined by the rule

$$g^a g^b = g^{(a+b) \pmod m}, \ \forall a, b \in \overline{\mathbf{N}}_{m-1}.$$

The identity is 1 and $(g^a)^{-1} = g^{m-a}$, $\forall a \in \mathbf{N}_{\mathrm{m-1}}$.

The group G is called the *cyclic group of order* m if and only if $G = \mathbf{C}_m$. The cyclic group of order m is isomorphic to the additive group of integers modulo m; that is, $\mathbf{C}_m \cong \mathbf{Z}_m$.

Notation 1.4. Throughout this work $\mathbf{N}_n = \{1, \ldots, n\}$ and $\overline{\mathbf{N}}_n = \{0, 1, \ldots, n\}$.

1.2.3 Permutation groups

Definition 1.5. A *permutation* of the set $\mathbf{N}_n$ is a bijection $\alpha : \mathbf{N}_n \to \mathbf{N}_n$. The set of all permutations of degree n is denoted $\mathbf{S}_n$.

Proposition 1.6. *The set* $\mathbf{S}_{\mathrm{n}}$ *together with the operation of composition of maps is a non-Abelian group and is called the symmetric group of degree* n.

Definition 1.7. The alternating group of degree n, denoted $\mathbf{A}_n$, is the subgroup of $\mathbf{S}_n$ consisting of all even permutations.

The permutation group $\mathbf{S}_n$ has order $n!$. The alternating group $\mathbf{A}_n$ has order $\frac{1}{2}n!$. The groups $\mathbf{S}_3$, $\mathbf{A}_4$ and $\mathbf{S}_4$ are used in the Chapter 3 and Chapter 5 classifications.

Note 1.8. For a full description of the symmetric group and the alternating group see [9, Chapter 4].

1.2.4 The Direct Product

Definition 1.9. The *exterior direct product* of the set of groups $G_1, G_2, \ldots, G_n$, denoted $G = G_1 \times G_2 \times \ldots \times G_n$ is the set

$$\{(g_1, g_2, \ldots, g_n) : g_i \in G_i\}.$$

The set G together with the composition law

$$(g_1, g_2, \ldots, g_n)(h_1, h_2, \ldots, h_n) = (g_1h_1, g_2h_2, \ldots, g_nh_n)$$

form a group with identity element

$$(1_{G_1}, 1_{G_2}, \ldots, 1_{G_n})$$

and inverse

$$(g_1, g_2, \ldots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}).$$

Proposition 1.10. *Let $H_1, H_2, \ldots, H_n$ be subgroups of the group G such that*

(i) *$h_ih_j = h_jh_i$, where $h_i \in H_i$, $h_j \in H_j$ and $i \neq j$,*

(ii) *$G = H_1H_2 \ldots H_n$,*

(iii) *$H_i \cap H_1H_2 \ldots H_{i-1}H_{i+1} \ldots H_n = 1$.*

Then G is isomorphic to $H_1 \times H_2 \times \cdots \times H_n$.

Proof See [9, 2.7.3 Proposition 9]. □

Definition 1.11. If G is a group that satisfies the conditions of Proposition 1.10, then G is called the *interior direct product* of the groups $H_1, H_2, \ldots, H_n$.

The order of the direct product is given by

$$|H_1 \times H_2 \times \cdots \times H_n| = \prod_{n}^{i=1} |H_i| .$$

1.2.5 The Semidirect Product

Definition 1.12. A group G with subgroups N and H such that

(i) $N \triangleleft G$,

(ii) $G = NH$,

(iii) $N \cap H = 1$,

is called a *semidirect product* of N by H, denoted $N \rtimes H$. The order of G is $|N| \times |H|$.

The operation of multiplication of elements in the semidirect product is now constructed. Consider a map φ from the subgroup H to $\mathrm{aut}(N)$ that is defined by $\varphi(h) = \varphi_h$, where $\varphi_h(n) = hnh^{-1}$, $\forall h \in H, n \in N$.

Definition 1.13. For given N, H and $\varphi : H \to \mathrm{aut}(N)$, a semidirect product G of N by H is said to *realize* φ if and only if

$$\varphi_h(n) = hnh^{-1}, \forall n \in N.$$

Definition 1.14. For N, H and $\varphi : H \to \mathrm{aut}(N)$ given, $N \rtimes_\varphi H$ is the set $N \times H$ together with the operation of multiplying elements $(n_1, h_1), (n_2, h_2) \in N \rtimes_\varphi H$ that is defined by

$$(n_1, h_1)(n_2, h_2) = (n_1\varphi_{h_1}(n_2), h_1h_2),$$

where $\varphi_{h_1}(n_2) = h_1n_2h_1^{-1} \in N$.

Theorem 7.12 in [12] proves that $N \rtimes_\varphi H$ is a semidirect product of N by H that realizes φ and Theorem 7.13 in [12] proves that if G is a semidirect product of N by H, then G is isomorphic to $N \rtimes_\varphi H$, for some $\varphi : H \to \mathrm{aut}(N)$.

Hence, Definition 1.13 and Definition 1.14 combine to show that N, H and φ determine G up to isomorphism.

Notation 1.15. Using the notation nh in place of (n, h), the multiplication in Definition 1.14 is expressed as

$$n_1h_1n_2h_2 = n_1h_1n_2h_1^{-1}h_1h_2 = n_1\varphi_{h_1}(n_2)h_1h_2.$$

Note 1.16. If G is the semidirect product of N by H that realizes φ, then G is either non-Abelian or $\varphi_h(n) = hnh^{-1} = n$, in which case G is the interior direct product of the subgroups N and H.

Example 1.17. The modular group, denoted $\mathbf{H}_1$ in the classification, is the semidirect product of $\mathbf{Z}_8$ by $\mathbf{Z}_2$ that realizes φ and is generated by

$$\left\langle (n, h) \mid n^8 = h^2 = 1,\ \varphi_h(n) = n^5 \right\rangle,$$

where $n \in \mathbf{Z}_8$ and $h \in \mathbf{Z}_2$.

The group $\mathbf{H}_1$ has order 16. The element 1 has order 1, the elements n^4, h and n^4h have order 2, the elements n^2, n^6, n^2h and n^6h have order 4 and the elements n, n^3, n^5, n^7, nh, n^3h, n^5h and n^7h, have order 8.

Example 1.18. The quasihedral group, denoted $\mathbf{H}_2$ in the classification, is the semidirect product of $\mathbf{Z}_8$ by $\mathbf{Z}_2$ that realizes φ and is generated by

$$\left\langle (n, h) \mid n^8 = n^2 = 1,\ \varphi_h(n) = n^3 \right\rangle,$$

where $n \in \mathbf{Z}_8$ and $h \in \mathbf{Z}_2$.

The group $\mathbf{H}_2$ has order 16. The element 1 has order 1, the elements n^4h, h, n^2h, n^4h and n^6h have order 2, the elements n^2, n^6, nh, n^3h, n^5h and n^7h have order 4 and the elements n, n^3, n^5 and n^7 have order 8.

Example 1.19. The group that is denoted $\mathbf{H}_3$ in the classification is the semidirect product of $\mathbf{Z}_4 \times \mathbf{Z}_2$ by $\mathbf{Z}_2$ that realizes φ and is generated by

$$\left\langle ((m,n),h) \mid m^4 = n^2 = h^2 = 1,\, \varphi_h(m) = m,\, \varphi_h(n) = m^2 n,\, mn = nm \right\rangle,$$

where $(m,n) \in \mathbf{Z}_4 \times \mathbf{Z}_2$ and $h \in \mathbf{Z}_2$.

The group $\mathbf{H}_3$ has order 16. The element 1 has order 1, the elements m^2, n, m^2n, h, m^2h, mnh and m^3nh have order 2 and the elements m, m^3, mn, m^3n, mh, m^3h, nh and m^2nh have order 4. The square of all elements of order 4 is m^2 and the square of all other elements is 1.

Example 1.20. The group that is denoted $\mathbf{H}_4$ in the classification is the semidirect product of $\mathbf{Z}_4 \times \mathbf{Z}_2$ by $\mathbf{Z}_2$ that realizes φ and is generated by

$$\left\langle (n,h) \mid n^4 = h^4 = 1,\, \varphi_h(n) = n^3h^2,\, \varphi_h(n^3) = nh^2 \right\rangle,$$

where $\mathbf{Z}_4 \times \mathbf{Z}_2 = \{1, n, n^2, n^3, h^2, nh^2, n^2h^2, n^3h^2\}$ and $h \in \mathbf{Z}_2 = \{1, h\}$.

The group $\mathbf{H}_4$ has order 16. The element 1 has order 1, the elements n^2, nh, n^3h, h^2, n^2h^2, nh^3 and n^3h^3 have order 2 and the elements n, n^3, h, n^2h, nh^2, n^3h^2, h^3 and n^2, h^3 have order 4. The elements 1, n^2 and h^2 are the only squares of $\mathbf{H}_4$.

Example 1.21. The group that is denoted $\mathbf{H}_5$ in the classification is the semidirect product of $\mathbf{Z}_4$ by $\mathbf{Z}_4$ that realizes φ and is generated by

$$\left\langle (n,h) \mid n^4 = h^4 = 1,\, \varphi_h(n) = n^3 \right\rangle.$$

The group $\mathbf{H}_5$ has order 16. The element 1 has order 1, the elements m^2, h^2 and m^2h^2 have order 2 and all other elements have order 4. The elements 1, n^2 and h^2 are the only squares of $\mathbf{H}_5$.

Example 1.22. The semidirect product of $(\mathbf{Z}_3 \times \mathbf{Z}_3) \rtimes \mathbf{Z}_2$ realizes φ and is generated by

$$\left\langle ((m,n),h) \mid m^3 = n^3 = h^2 = 1,\, mn = nm,\, \varphi_h(m) = m^2,\, \varphi_h(n) = n^2 \right\rangle,$$

where $(m,n) \in \mathbf{Z}_3 \times \mathbf{Z}_3$ and $h \in \mathbf{Z}_2$.

The element 1 has order 1, the elements of the form (m^i, n^j) $((i,j) \neq (0,0))$ have order 3, and all other elements have order 2.

Example 1.23. The Frobenius group of order 20 is the semidirect product of $\mathbf{Z}_5$ by $\mathbf{Z}_4$ that realizes φ and is generated by

$$\left\langle (n,h) \mid n^5 = h^4 = 1,\, \varphi_h(n) = n^3 \right\rangle,$$

where $n \in \mathbf{Z}_5$ and $h \in \mathbf{Z}_4$.

The element 1 has order 1, the elements n^i $(i \neq 0)$ have order 5, the elements n^ih^2 have order 2 and all other elements have order 4.

Example 1.24. The Frobenius group of order 21 is the semidirect product of $\mathbf{Z}_7$ by $\mathbf{Z}_3$ that realizes φ and is generated by

$$\left\langle (n,h) \mid n^7 = h^3 = 1,\, \varphi_h(n) = n^4 \right\rangle,$$

where $n \in \mathbf{Z}_7$ and $h \in \mathbf{Z}_3$.

The element 1 has order 1, the elements n^i $(i \neq 0)$ have order 7 and all other elements have order 3.

Example 1.25. The semidirect product of $\mathbf{Z}_3$ by $\mathbf{Z}_8$ realizes φ and is generated by

$$\left\langle (n,h) \mid n^3 = h^8 = 1,\, \varphi_h(n) = hnh^{-1} \right\rangle,$$

where $n \in \mathbf{Z}_3$ and $h \in \mathbf{Z}_8$.

The group $\mathbf{Z}_3 \rtimes_\varphi \mathbf{Z}_8$ has order 24. The element 1 has order 1, the element h^4 has order 2, the elements n and n^2 have order 3, the elements h^2 and h^4 have order 4, the elements nh^4 and n^2h^4 have order 6, the elements nh^2, n^2h^2, nh^6 and n^2h^6 have order 12 and all other elements have order 8.

Example 1.26. The semidirect product of $\mathbf{Z}_3$ by $\mathbf{D}_4$ realizes φ and is generated by

$$\left\langle (n,(h_1,h_2)) \mid n^3 = h_1^4 = h_2^2 = 1,\, h_2h_1h_2 = h_1^3,\, \varphi_{h_1}(n) = n^2,\, \varphi_{h_2}(n) = n \right\rangle,$$

where $n \in \mathbf{Z}_3$ and $(h_1,h_2) \in \mathbf{D}_4$.

The group $\mathbf{Z}_3 \rtimes_\varphi \mathbf{D}_4$ has order 24. The element 1 has order 1, the elements n and n^2 have order 3, the elements h_1, nh_1, n^2h_1, h_1^3, nh_1^3 and $n^2h_1^3$ have order 4, the elements nh_1^2, $n^2h_1^2$, nh_2, n^2h_2, $nh_1^2h_2$ and $n^2h_1^2h_2$ have order 6 and all other elements have order 2.

Example 1.27. The only group of order greater than 24 used in the Chapter 3 classification is the semidirect of $\mathbf{Z}_{19}$ by $\mathbf{Z}_3$ that realize φ and is generated by

$$\left\langle (h,n) \mid h^{19} = n^3 = 1,\, \varphi_h(n) = n^7 \right\rangle,$$

where $n \in \mathbf{Z}_{19}$ and $h \in \mathbf{Z}_3$.

The group $\mathbf{Z}_{19} \rtimes_\varphi \mathbf{Z}_3$ has order 57. The element 1 has order 1, the elements n^i $(i \neq 0)$ have order 19 and all other elements have order 3.

1.2.6 Dihedral groups

Definition 1.28. The *dihedral* group $\mathbf{D}_n$ consists of the $2n$ elements

$$\begin{array}{cccc} 1 & \alpha & \dots & \alpha^{n-1} \\ \beta & \alpha\beta & \dots & \alpha^{n-1}\beta, \end{array}$$

where $\alpha^n = \beta^2 = 1$ and

$$\beta\alpha\beta^{-1} = \alpha^{-1} = \alpha^{n-1}. \tag{1.1}$$

Note 1.29. Equation (1.1) gives

$$\beta\alpha^i\beta^{-1} = \alpha^{-i}. \tag{1.2}$$

Equation (1.2) determines the products

$$\alpha^i\alpha^j \in \mathbf{D}_n,$$

$$\alpha^i\beta\alpha^j = \alpha^i\beta\alpha^j\beta^{-1}\beta = \alpha^{i-j}\beta \in \mathbf{D}_n,$$

$$\alpha^i\beta\alpha^j\beta = \alpha^{i-j}\beta^2 = \alpha^{i-j} \in \mathbf{D}_n.$$

These are sufficient to determine that $\mathbf{D}_n$ is closed.

The inverse of α^i is α^{n-i} and the inverse of $\alpha^i\beta$ is $\alpha^i\beta$; hence, all elements of the form $\alpha^i\beta$ have order 2.

The Dihedral group $\mathbf{D}_n$ is isomorphic to the semidirect product of $\mathbf{Z}_n$ by $\mathbf{Z}_2$ that realizes φ and is generated by

$$\left\langle (a,b) \mid a^n = b^2 = 1,\, \varphi_b(a) = a^{-1} \right\rangle,$$

where $a \in \mathbf{Z}_n$ and $b \in \mathbf{Z}_2$.

The dihedral groups $\mathbf{D}_4$, $\mathbf{D}_5$, $\mathbf{D}_6$, $\mathbf{D}_7$, $\mathbf{D}_8$, $\mathbf{D}_9$, $\mathbf{D}_{10}$, $\mathbf{D}_{11}$, $\mathbf{D}_{12}$ are used in the Chapter 3 classification.

Example 1.30. For the dihedral group $\mathbf{D}_{12}$, the identity element has order 1 and all twelve elements of the form $\alpha^i\beta$ have order 2. The element α^6 has order 2, the elements α^4 and α^8 have order 3, the elements α^3 and α^9 have order 4, the elements α^2 and α^{10} have order 6 and the elements α, α^5, α^7 and α^{11} have order 12.

1.2.7 Dicyclic groups

The *Dicyclic Group* of order $4n$, denoted $\mathbf{Q}_{2n}$ is the group generated by

$$\left\langle (a,b) \mid a^2 = b^n,\, b^{2n} = 1,\, bab = a \right\rangle.$$

In general, $\mathbf{Q}_{2n}$ consists of the elements

$$\mathbf{Q}_{2n} = \{1, a, b, ab, b^2, ab^2, \ldots, b^{2n-1}, ab^{2n-1}\}.$$

The subgroup

$$H = \{1, b, b^2, \ldots, b^{2n-1}\}$$

is isomorphic to $\mathbf{Z}_{2n}$. Since $ba = ab^{-1} \Rightarrow b^ia = ab^{-i}$, the product ab^iab^j becomes $a^2b^{j-i} = b^{n+j-i} \in H$; hence, no subgroup of order 2 exists that does not contain an element of H. The elements of H have their order determined by $\mathbf{Z}_{2n}$. The equation

$$(ab^i)^4 = (ab^iab^i)^2 = (b^nb^{-i}b^i)^2 = b^{2n} = 1$$

ensures that all other elements have order 4.

1.2.8 The Special Linear Group $SL(2,3)$

The special linear group $SL(2,3)$ is the group consisting of all 2×2 matrices over the Galois field of order 3 with determinant 1. The special linear group has order 24 and construction

$$\left\langle (a,b,c) \mid a^3 = b^3 = c^2 = abc \right\rangle.$$

1.2.9 Groups of large order

In the Chapter 3 classification, there is one complete $(19, 3)$-arc the automorphism group of which has order 57; this group is described in Example 1.27. In the Chapter 5 classification, there is one incomplete $(18, 3)$-arc the automorphism group of which has order 60. This group is the alternating group of degree 5, denoted $\mathbf{A}_5$.

1.3 Finite Fields

Definition 1.31. A *field* is a set of elements F such that

(i) the set F together with the operation of addition is an Abelian group with identity element 0,

(ii) the set $F \setminus \{0\}$ together with the operation of multiplication is an Abelian group with identity element 1,

(iii) the operations of addition and multiplication on the set F are distributive; that is, $f_1(f_2 + f_3) = f_1f_2 + f_1f_3$ and $(f_1 + f_2)f_3 = f_1f_3 + f_2f_3$, for all $f_1, f_2, f_3 \in F$,

(iv) the set F has no zero divisors; that is, if $f_1f_2 = 0$, then $f_1 = 0$, $f_2 = 0$ or both.

Such a field is denoted $\langle F, +, \times \rangle$ or for convenience F.

Definition 1.32. Let E be a non-empty subset of the field F. Then E is called a subfield of F if and only if E is a field under the operations of F. The prime subfield of F is the intersection of every subfield of F.

Definition 1.33. A *finite field* or *Galois field* is a field that contains a finite number of elements.

Theorem 1.34. *The set* $\mathbf{Z}_\mathrm{n}$ *of integers modulo* n*, is a field if and only if* n *is a prime.*

Proof See [13, Theorem 16.7]. □

Theorem 1.35. *The prime subfield* P *of a finite field* F *is isomorphic to the field* $\mathbf{Z}_\mathrm{p}$*, where* p *is a prime.*

Proof The prime subfield P necessarily contains the elements 0 and 1 and so contains the elements

$$\{1 + 1, 1 + 1 + 1, \ldots\}.$$

Since F is finite, there must exist a smallest positive integer p such that

$$\overbrace{1 + 1 + \cdots + 1}^{p \text{ times}} = 0.$$

Since a field does not contain zero divisors, p must be a prime. The listed elements of P are isomorphic to the field $\mathbf{Z}_p$; hence, P contains no additional elements. □

Definition 1.36. The *characteristic* of a finite field F is p if the prime subfield of F is isomorphic to the field $\mathbf{Z}_p$, where p is a prime.

Theorem 1.37. *A finite field F of characteristic p has order p^n, where n is a positive integer.*

Proof (Outline). Let $[F : P] = n$; that is, the dimension of F over P is n or every basis of F over P has exactly n elements. If $f_1, f_2, \ldots, f_n$ is a basis for F over P, then every element of F can be expressed uniquely in the form

$$\lambda_1 f_1 + \lambda_2 f_2 + \cdots + \lambda_n f_n,$$

where $\lambda_i \in P$. Hence, $|F| = p^n$. □

Theorem 1.38. *There exists up to isomorphism exactly one field with order $q = p^n$.*

Proof See [13, Theorem 20.3]. □

Note 1.39. Since $F\backslash\{0\}$ is an Abelian group of order $q-1$ under multiplication, the order of every cycle in $F\backslash\{0\}$ divides $q-1$; hence, $f^{q-1} = 1$ or equivalently $f^q = f$, for all $f \in F\backslash\{0\}$. In addition, [13, Theorem 20.8] states that the multiplicative group $F\backslash\{0\}$ is cyclic, therefore

$$GF(q) = \{0, 1, f, f^2, \ldots, f^{q-2} \mid f^{q-1} = 1\}.$$

Construction 1.40. The *Galois field* of order 2 denoted $GF(2)$ or $\mathbf{F}_2$, is constructed as the residue class of integers modulo 2 and this construction is unique up to isomorphism:

$$\mathbf{Z}_2 \cong \mathbf{F}_2 = \{0, 1 \mid 2 = 0\}.$$

The *Galois field* of order p denoted $GF(p)$ or $\mathbf{F}_p$, where p is an odd prime, is constructed as the residue class of integers modulo p and this construction is unique up to isomorphism:

$$\mathbf{Z}_p \cong \mathbf{F}_p = \{-(p-1)/2, \ldots, -1, 0, 1, \ldots, (p-1)/2 \mid p = 0\}.$$

The *Galois field* of order p^n denoted $GF(p^n)$ or $\mathbf{F}_{p^n}$, where p is a prime, is constructed as $\mathbf{F}_p[T]/(F(T))$, where $F(T)$ is a monic irreducible polynomial of degree n over $\mathbf{F}_p$ and this construction is unique up to isomorphism:

$$\mathbf{F}_{p^n} = \{a_0 + a_1 t + \cdots + a_{n-1} t^{n-1} \mid a_i \in \mathbf{F}_p, F(t) = 0\}.$$

Example 1.41. The first example is the field $\mathbf{F}_{11}$ which is used throughout this work; the second field has prime power order.

(1) $\mathbf{F}_{11} = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5 \mid 11 = 0\}$.

(2) $\mathbf{F}_8 = \{0, 1 = t^7, t, t^2, t^3 = t^2 + 1, t^4 = t^2 + t + 1, t^5 = t + 1, t^6 = t^2 + t \mid$
$F(t) = t^3 + t^2 + 1 = 2 = 0\}$.

1.3.1 Automorphisms and the Frobenius Automorphism

For a field F, consider the map $\phi : GF(p^h) \to GF(p^h)$, where $f\phi = f^p$, for $f \in F$, from which are derived the maps $\phi^i : GF(p^h) \to GF(p^h)$, where $f\phi^i = f^{p^i}$, for $f \in F$ and $i = 2, \ldots, h-1$.

Proposition 1.42. *The maps ϕ^i are automorphisms of $GF(p^h)$ and the Frobenius automorphism ϕ generates the automorphism group for the Galois field of order p^h; that is,*

$$\mathrm{aut}(GF(p^h)) = \{1, \phi, \phi^2, \ldots, \phi^{h-1}\}.$$

Hence, $\mathrm{aut}(GF(p^h))$ *is isomorphic to* $\mathbf{Z}_h$.

Proof The maps ϕ^i are homomorphic since

$$(f_1 f_2)\phi^i = (f_1 f_2)^{p^i} = f_1^{p^i} f_2^{p^i} = f_1\phi^i f_2\phi^i$$

and

$$(f_1 + f_2)\phi^i = (f_1 + f_2)^{p^i} = f_1^{p^i} + f_2^{p^i} = f_1\phi^i + f_2\phi^i.$$

(one to one) If $f^a\phi^i = f^b\phi^i$, then $f^{ap^i} = f^{bp^i}$; hence, $a = b$, as $GF(p^h)\backslash\{0\}$ is cyclic. **(onto)** Let $f^a \in GF(p^h))$. Then $f^{ap^{h-i}} = f^{ap^{h-i}p^i} = f^{ap^h} = f^a$. Hence, the maps ϕ^i are automorphisms.

Let $\sigma \in \mathrm{aut}(GF(p^h))$ and suppose $f\sigma \neq f^{p^i}$. Then as $GF(p^h)$ is cyclic, $f\sigma = f^m$, where $m \neq p^i$, for all $i \in \{0, \ldots, h-1\}$. The image of σ is $\{f^{am} \mid a = 0, \ldots, p^{h-1}\}$ and since no such value of am divides p^h, the image does not contain the element f. By contradiction, if $\sigma \in \mathrm{aut}(GF(p^h))$, then $\sigma = \phi^i$. □

1.4 Projective space

Let $V = V(k, q)$ be a k-dimensional vector space over the finite field $\mathbf{F}_q$, where $q = p^h$. Then any two vectors $X = (x_0, \ldots, x_{k-1})$ and $Y = (y_0, \ldots, y_{k-1})$ of $V \setminus \{0\}$ are called equivalent if $Y = tX$, for some $t \in \mathbf{F}_q \setminus \{0\}$. The equivalence class of a vector $X = (x_0, \ldots, x_{k-1})$ of $V \setminus \{0\}$ is the subset of $V \setminus \{0\}$ given by $\{tX = (tx_0, \ldots, tx_{k-1}) \mid t \in \mathbf{F}_q \setminus \{0\}\}$.

Definition 1.43. The $(k-1)$-*dimensional projective space over the finite field* $\mathbf{F}_q$, denoted $PG(k-1, q)$, is the set consisting of the equivalence classes of vectors of the k-dimensional vector space $V(k, q)$.

The elements of $PG(k-1, q)$ are called *points* and the point denoted $P(X)$ is the equivalence class of the vector X. Since $P(tX) = P(X)$, for all $t \in \mathbf{F}_q \setminus \{0\}$, if the first non-zero component of tX is a one, $tX = (0, \ldots, 0, 1, \ldots)$, then for consistency this vector is used to represent the point $P(X)$.

Definition 1.44. The subspaces of the projective space $PG(k-1, q)$ are defined as follows:

- the (-1)-dimensional subspace of $PG(k-1, q)$ is the empty set.
- the points or 0-dimensional subspaces of $PG(k-1, q)$ are the 1-dimensional subspaces of V.

- the *lines* or 1-dimensional subspaces of $PG(k-1,q)$ are the 2-dimensional subspaces of V.
- the *planes* or 2-dimensional subspaces of $PG(k-1,q)$ are the 3-dimensional subspaces of V.
- ...
- the *hyperplanes* or $(k-2)$-dimensional subspaces of $PG(k-1,q)$ are the $(k-1)$-dimensional subspaces of V.

An m-dimensional subspace or *m-space* of $PG(k-1,q)$ is denoted Π_m.

An m-dimensional subspace of $PG(k-1,q)$ is incident with an $(m+i)$-dimensional subspace of $PG(k-1,q)$ if the corresponding $(m+1)$-dimensional subspace of V is contained in the corresponding $(m+i+1)$-dimensional subspace of V.

The points $P(X_0),\ldots,P(X_r)$ are linearly independent if and only if the vectors $X_0,\ldots,X_r$ are linearly independent. Hence, the point $P(X_i)$ is incident with the line through the points $P(X_0)$ and $P(X_1)$ if and only if the vector X_i is a linear combination of the vectors X_0 and X_1.

Theorem 1.45. *Let S be a d-dimensional subspace of the finite projective space $PG(k-1,q)$, where $1 \le d \le k-1$. Then the following facts hold:*

(i) *the number of points of S is*

$$q^d + q^{d-1} + \cdots + q + 1 = \frac{q^{d+1}-1}{q-1};$$

(ii) *if s is a point of S, then in S there are*

$$q^{d-1} + \cdots + q + 1$$

lines through the point s;

(iii) *the number of lines in S is*

$$\frac{(q^d + q^{d-1} + \cdots + q + 1)(q^{d-1} + \cdots + q + 1)}{q+1}.$$

Proof (i) A $(d+1)$-dimensional subspace of the vector space V, given by

$$\{\alpha_0 X_0 + \alpha_1 X_1 + \cdots + \alpha_d X_d \mid \alpha_i \in \mathbf{F}_q\},$$

contains $q^{d+1}-1$ non-zero vectors; hence, there are

$$\frac{q^{d+1}-1}{q-1}$$

points of S.

(ii) Let s be a point that is incident with S, then there are $q^d + \cdots + q$ additional points that are incident with S. Since each line in S that is incident with P is incident with $q+1$ points of S, in S there are

$$\frac{q^d + \cdots + q}{q} = q^{d-1} + \cdots + q + 1$$

lines through the point s.

(iii) The subspace S consists of $q^d + \cdots + q + 1$ points and every point of S is incident with $q^{d-1} + \cdots + q + 1$ lines in S, but every line in S is incident with $q+1$ points of S. Hence, there are

$$\frac{(q^d + q^{d-1} + \cdots + q + 1)(q^{d-1} + \cdots + q + 1)}{q+1}$$

lines in S. □

The line through the points $P(X)$ and $P(Y)$ is denoted $L(X, Y)$.

Lemma 1.46. *The line through the points $P(X)$ and $P(Y)$ in $PG(k-1, q)$ is the set of points $\{P(X + \alpha Y) \cup P(Y) \mid \alpha \in \mathbf{F}_q\}$.*

Proof The 2-dimensional subspace of V containing the vectors X and Y is

$$\{aX + bY \mid a, b \in \mathbf{F}_\mathrm{q}\}$$

and

$$P(aX + bY) = \begin{cases} P(X + ba^{-1}Y) & \text{if } a \neq 0, \\ P(Y) & \text{if } a = 0. \end{cases}$$ □

Notation 1.47. The 2-dimensional projective space $PG(2, q)$ is called the projective plane.

The projective plane $PG(2, q)$ contains $q^2 + q + 1$ points and $q^2 + q + 1$ lines. Every point of $PG(2, q)$ is incident with $q+1$ lines and every line in $PG(2, q)$ is incident with $q+1$ points. The points of $PG(2, q)$ have the form $P(0, 0, 1)$, $P(0, 1, x_2)$ or $P(1, x_1, x_2)$, where $x_1, x_2 \in \mathbf{F}_q$.

1.5 Collineations of the projective space

Definition 1.48. If $\mathcal{P}_1$ and $\mathcal{P}_2$ are two projective spaces $PG(k-1, q)$, then a *collineation* of $PG(k-1, q)$ is a bijection $\mathfrak{T} : \mathcal{P}_1 \longrightarrow \mathcal{P}_2$ that preserves incidence structures.

Definition 1.49. A collineation $\mathfrak{T} : \mathcal{P}_1 \longrightarrow \mathcal{P}_2$ is called a *projectivity* of $PG(k-1, q)$ if it is induced by a linear map of $V(k, q)$. That is, $\mathfrak{T}$ maps $P(X)$, a point of $\mathcal{P}_1$, onto $P(Y)$, a point of $\mathcal{P}_2$, if and only if $tY = Xg$, where $t \in \mathbf{F}_q \setminus \{0\}$ and g is a non-singular matrix. Such a projectivity is denoted $(\mathfrak{T}, g)$ or g if the map $\mathfrak{T}$ is not stated; $(\mathfrak{T}, g) = (\mathfrak{T}, cg)$, for all $c \in \mathbf{F}_q \setminus \{0\}$.

Let $x = P(X)$ be a point of $PG(k-1,q)$. Then the result of the right action of a matrix g on x denoted x^g is the point $P(Xg)$.

For a projectivity $(\mathfrak{T}, g)$ of $PG(k-1,q)$, if $\Pi_{m_1} \subset \Pi_{m_2}$, then $\Pi_{m_1} g \subset \Pi_{m_2} g$, since incidence structures are preserved.

Example 1.50. Let $\mathfrak{T} : PG(2,q) \longrightarrow PG(2,q)$ be a projectivity. Then $\mathfrak{T}$ maps the line

$$L(X,Y) = \{P(Z) \mid Z \in \{X + \alpha Y \mid \alpha \in \mathbf{F}_q\} \cup Y\}$$

to the line

$$L(Xg, Yg) = \{P(Z) \mid Z \in \{Xg + \alpha Yg \mid \alpha \in \mathbf{F}_q\} \cup Yg\}.$$

Definition 1.51. A set of $k+1$ points of $PG(k-1,q)$ is called a *frame* if and only if the vectors representing k of these points form a basis of $V(k,q)$.

Subsequently, in $PG(k-1,q)$, no hyperplane is incident with more than $k-1$ points of a frame. In $PG(2,q)$, no line is incident with more than 2 points of a frame. Let the set of k vectors $X_0, \ldots, X_{k-1}$ form a basis of $V(k,q)$. Then the set of $k+1$ points $P(X_0) \ldots, P(X_{k-1})$, $P(X_0 + \cdots + X_{k-1})$ is a frame of $PG(k-1,q)$.

The *standard frame* is $e_0 = P(1,0,\ldots,0), \ldots, e_{k-1} = P(0,\ldots,0,1), e_k = P(1,\ldots,1)$.

Theorem 1.52. *For $(\mathfrak{T}, g)$ a projectivity and $\mathcal{P}$ a projective space $PG(k-1,q)$, if the projectivity $\mathfrak{T} : \mathcal{P} \to \mathcal{P}$ maps every point of a frame to itself, then $\mathfrak{T}$ is the identity mapping $\mathfrak{I}$ or $g = \mathrm{I}$. This projectivity is denoted $(\mathfrak{I}, \mathrm{I})$.*

Proof Let $P(X_i)$ be a point of $\mathcal{P}$. Then $X_i g = a_i X_i$, where $a_i \in \mathbf{F}_q \setminus \{0\}$, for all $i = 0, \ldots, k-1$; hence,

$$(X_0 + \cdots + X_{k-1})g = a_0 X_0 + \cdots + a_{k-1} X_{k-1}.$$

However, it is also true that

$$(X_0 + \cdots + X_{k-1})g = a(X_0 + \cdots + X_{k-1}) = aX_0 + \cdots + aX_{k-1}.$$

So, $g = a\mathrm{I}$. □

Corollary 1.53. *Let the $k+1$ points $P(X_0), \ldots, P(X_{k-1}), P(X_k = X_0 + \cdots + X_{k-1})$ be a frame of $PG(k-1,q)$. Then there is exactly one projectivity of $PG(k-1,q)$ such that $\mathfrak{T}(e_i) = P(X_i)$.*

Proof The linear map $\mathfrak{T}$ that is defined by $\mathfrak{T}(e_i) = P(X_i)$, for $i = 0, \ldots, k-1$, also maps e_k onto $P(X_k)$. If there are two such projectivities $\mathfrak{T}_1$ and $\mathfrak{T}_2$, then $\mathfrak{T}_1 \mathfrak{T}_2^{-1}$ is the identity, by Theorem 1.52; hence, $\mathfrak{T}_1 = \mathfrak{T}_2$. □

Definition 1.54. The *general linear group* $GL(k,q)$ is the group of bijective linear transformations of V with respect to the operation of composition of maps.

Definition 1.55. The *collineation group* $P\Gamma L(k,q)$ is the group of collineations of $PG(k-1,q)$ with respect to the operation of composition of maps.

Definition 1.56. The *projective general linear group* $PGL(k,q)$ is the group of projectivities of $PG(k-1,q)$ with respect to the operation of composition of maps.

Theorem 1.57. *The cardinality of the groups* $GL(k,q)$, $PGL(k,q)$ *and* $P\Gamma L(k,q)$ *are*

(i) $|GL(k,q)| = (q^k-1)(q^k-q)\dots(q^k-q^{k-1}) = q^{k(k-1)/2}\prod_{i=1}^{k}(q^i-1)$,

(ii) $|PGL(k,q)| = |GL(k,q)|/(q-1)$,

(iii) $|P\Gamma L(k,q)| = h\,|PGL(k,q)|$, *where* $q=p^h$ *and* p *is a prime.*

Proof (i) Let g be a $k\times k$ non-singular matrix with elements selected from $\mathbf{F}_q$. Then as no row can be zero or a linear combination of previous rows, the rows may be selected in q^k-1, $q^k-q,\dots,q^k-q^{k-1}$ ways.

(ii) Since $(\mathfrak{T},g)=(\mathfrak{T},tg)$, for all $t\in\mathbf{F}_q\setminus\{0\}$, every projectivity is given by $q-1$ matrices.

(iii) See The Fundamental Theorem of Projective Geometry, Section 1.5.1. □

Example 1.58. For $PG(2,11)$, the projective general linear group $PGL(3,11)$ has cardinality

$$(11^3-1)(11^3-11)(11^3-11^2)/(11-1) = 193,116,000.$$

1.5.1 Automorphisms

An automorphism acting on a field $GF(p^h)$ can be extended to an *automorphic collineation* on $PG(k-1,q)$; this is given by $P(X)\sigma = P(X\sigma)$, where $X\sigma=(x_0\sigma,x_1\sigma,\dots,x_{k-1}\sigma)$ and $P(X)\in PG(k-1,q)$.

Notation 1.59. For convenience $x\sigma$ and $X\sigma$ may be denoted x^σ and X^σ.

The Fundamental Theorem of Projective Geometry

(i) If $\mathfrak{T}' : S\to S$ is a collineation, then $\mathfrak{T}'=\sigma\mathfrak{T}$, where σ is an automorphic collineation on $PG(k-1,q)$ and $\mathfrak{T}$ is a projectivity.

If $q=p^h$, then

$$\mathrm{aut}(GF(p^h)) = \{1,\phi,\phi^2,\dots,\phi^{h-1}\};$$

hence, for every projectivity there exist h collineations. If $P(X')=P(X)\mathfrak{T}'$, then for every $m\in\mathbf{N}_h$, there exists $t\in GF(q)\setminus\{0\}$ and g a non-singular matrix such that

$$tX' = X^{p^m}g,$$

where $X^{p^m}=(x_0^{p^m},\dots,x_{k-1}^{p^m})$.

(ii) If $\{P_0,\dots,P_k\}$ and $\{P_0',\dots,P_k'\}$ are $(k+1)$-arcs of $PG(2,q)$, then there exists a unique projectivity $\mathfrak{T}$ such that $P_i'=P_i\mathfrak{T}$, for all $i\in\overline{\mathbf{N}}_k$.

1.6 Arcs

Definition 1.60. An (n, r)-*arc* S in the projective plane $PG(2, q)$ is a set of n points of $PG(2, q)$ such that no $r + 1$ points are collinear and some r points are collinear. If $r = 2$, then S is called an n-arc. The size of the largest (n, r)-arc in $PG(2, q)$ is denoted $m_r(2, q)$.

A line ℓ in $PG(2, q)$ is called an *i-secant* of an (n, r)-arc S if and only if ℓ is incident with i points of S. A 0-secant is called an *external line*, an i-secant is called an *internal line*, for $i \in [1, \ldots, q + 1]$.

Definition 1.61. An (n, r)-arc S in the projective plane $PG(2, q)$ is called *complete* if it is not contained within an $(n + 1, r)$-arc that is also in $PG(2, q)$ or equivalently if every point of $PG(2, q)$ is incident with at least one r-secant of S.

Two (n, r)-arcs S_1 and S_2 of $PG(2, q)$ are said to be projectively equivalent if there exists a projectivity $(\mathfrak{T}, g) \in PGL(3, q)$ that maps S_1 onto S_2; that is, $X_i g = tY_i$, for all points $P(X_i) \in S_1$ and $P(Y_i) \in S_2$, where $i = 0, \ldots, n - 1$.

Let τ_i denote the number of i-secants of an (n, r)-arc S in $PG(2, q)$, let $\rho_i = \rho_i(s)$ denote the number of i-secants through the point $s \in S$ and let $\sigma_i = \sigma_i(x)$ denote the number of i-secants through the point $x \in PG(2, q) \setminus S$. Then [5, Lemma 1.2.1] is presented in Lemma 1.62.

Lemma 1.62. *For an* (n, r)-arc S *the following equations hold:*

(i) (a)
$$\sum_{i=0}^{r} \tau_i = q^2 + q + 1, \tag{1.3}$$

(b)
$$\sum_{i=1}^{r} i\tau_i = n(q + 1), \tag{1.4}$$

(c)
$$\sum_{i=2}^{r} \frac{i(i-1)\tau_i}{2} = \frac{n(n-1)}{2}; \tag{1.5}$$

(ii) (a)
$$\sum_{i=1}^{r} \rho_i(s) = q + 1, \tag{1.6}$$

(b)
$$\sum_{i=2}^{r} (i-1)\rho_i(s) = n - 1; \tag{1.7}$$

(iii) (a)
$$\sum_{i=1}^{r} \sigma_i(x) = q + 1, \tag{1.8}$$

(b)
$$\sum_{i=2}^{r} i\sigma_i(x) = n; \tag{1.9}$$

(iv)
$$i\tau_i = \sum_{s\in S} \rho_i(s); \tag{1.10}$$

(v)
$$(q+1-i)\tau_i = \sum_{x\in PG(2,q)\setminus S} \sigma_i(x). \tag{1.11}$$

Proof These equations represent the number of elements in the following sets:

(i) (a) $\{s \mid s \in PG(2,q)\}$,
(b) $\{(s,\ell) \mid s \in \ell \cup S, \forall \text{ lines } \ell\}$,
(c) $\{(s,s',\ell) \mid s \neq s', s, s' \in S, \ell \ni s, s'\}$;

(ii) (a) $\{\ell \mid \ell \ni s\}$,
(b) $\{(s',\ell) \mid s' \in (\ell \cup S) \setminus \{s\}, \ell \ni s\}$;

(iii) (a) $\{\ell \mid \ell \ni x\}$,
(b) $\{(s,\ell) \mid s \in (\ell \cup S), \ell \ni x\}$;

(iv) $\{(s,\ell_i) \mid s \in (\ell_i \cup S), \ell_i \text{ a } i\text{-secant of } S\}$;

(v) $\{(x,\ell_i) \mid x \in (\ell_i \cup PG(2,q) \setminus \{S\}), \ell_i \text{ a } i\text{-secant of } S\}$.

□

Theorem 1.63. *If S is an (n,r)-arc of $PG(2,q)$ with an i-secant, then $m_r(2,q) \leq (r-1)q+i$.*

Proof Let x be a point of S that is incident with an i-secant of S, then the remaining q lines through x are each incident with at most $r-1$ points of S other than x. □

Theorem 1.64. *Let S be an (n,r)-arc of $PG(2,q)$, where $(r,q)=1$, that has an external line. Then $m_r(2,q) \leq (r-1)q+1$.*

Theorem 1.65. *Let S be an (n,r)-arc of $PG(2,q)$ that does not possess an external line. Then*
$$m_r(2,q) \leq (r-1)q + q - \sqrt{q^2+q-nq}.$$

Theorem 1.66. *Let S be an (n,r)-arc of $PG(2,p)$, where p is a prime.*

(i) *If $n > q/2+1$, then $m_r(2,q) \leq (r-1)q + r - (q+1)/2$.*

(ii) *If $n < q/2+1$, then $m_r(2,q) \leq (r-1)q+1$.*

Theorems 1.64, 1.65 and 1.66 can all be found with proofs in [5, Section 12.5]. The largest size of an (n, r)-arc S in $PG(2, q)$, denoted $m_r(2, q)$, has an upper bound derived from Theorems 1.63 to 1.66. Let the smallest known upper bound for $m_r(2, q)$ be m. Suppose $m_r(2, q) = m$; if an (m, r)-arc is discovered by some method, for example by a random search, then $m_r(2, q) = m$. If $m_r(2, q) < m$ and some $(m_r(2, q), r)$-arc is discovered, then this is not enough information to determine that no (n, r)-arc exists, for $n = m_r(2, q) + 1, \ldots, m$. If $m_r(2, q) < m$, then an exhaustive search for an $(m_r(2, q), r)$-arc is the only way to determine that no (n, r)-arc exists, for $n = m_r(2, q) + 1, \ldots, m$. Table 1.1 gives all the known values of $m_r(2, q)$ for $q \leq 11$, as they were prior to this work.

Table 1.1: $m_r(2, q)$ for $q \leq 11$

r \ q	2	3	4	5	7	8	9	11
2	4	4	6	6	8	10	10	12
3	7	9	9	11	15	15	17	21
4		13	16	16	22	28	28	$32-34$
5			21	25	29	33	37	$43-45$
6				31	36	42	48	56
7					49	49	55	67
8					57	64	65	78
9						73	81	$89-90$
10							91	$100-102$
11								121
12								133

1.7 The Stabilizer Group

If x is a point of $PG(2, q)$, then x^g denotes the image of x through the right action of the non-singular matrix g that induces the projectivity $\mathfrak{T}$; that is, $(\mathfrak{T}, g) \in PGL(3, q)$. Let S be a set of points of $PG(2, q)$, possibly an (n, r)-arc. Then $S^g = \{x^g \mid x \in S\}$.

Definition 1.67. For $G \leqslant PGL(3, q)$, if $(\mathfrak{T}, g) \in PGL(3, q)$, then the *orbit* of a point $x \in PG(2, q)$ through G is the set $x^G = \{x^g \mid g \in G\}$. The *orbit* of $S \subset PG(2, q)$ through G is the set $\{x^G \mid x \in S\}$.

Definition 1.68. A set $S \subseteq PG(2, q)$ is said to be *stabilized* by the projectivity $(\mathfrak{T}, g) \in PGL(3, q)$ if and only if $S^g = S$.

The automorphism or stabilizer group of a set $S \subseteq PG(2, q)$ is the largest subgroup of $PGL(3, q)$, the elements of which stabilize the set S; that is,

$$\mathrm{aut}(S) = \{(\mathfrak{T}, g) \in PGL(3, q) \mid S^g = S\}.$$

Note 1.69. The stabilizer groups are used to further classify the classes of projectively equivalent (n, r)-arcs in $PG(2, q)$.

Proposition 1.70. *For every 4-arc $\{x^{(0)}, x^{(1)}, x^{(2)}, x^{(3)}\}$ in $PG(2, q)$, there exists a projectivity $(\mathfrak{T}, g) \in PGL(3, q)$ such that $x^{(i)g} = e_i$, for $i = 0, \ldots, 3$.*

Proof Let

$$g^{-1} = \begin{pmatrix} \alpha x^{(0)} \\ \beta x^{(1)} \\ \gamma x^{(2)} \end{pmatrix},$$

where α, β and γ are uniquely determined by

$$(1,1,1)^{g^{-1}} = (\alpha x_0^{(0)} + \beta x_0^{(1)} + \gamma x_0^{(2)}, \alpha x_1^{(0)} + \beta x_1^{(1)} + \gamma x_1^{(2)}, \alpha x_2^{(0)} + \beta x_2^{(1)} + \gamma x_2^{(2)}) = x^{(3)}.$$

Then $x^{(i)g} = e_i$ as required. □

Proposition 1.71. *In $PG(2, q)$, if the projectivity $(\mathfrak{T}, g) \in PGL(2, q)$ maps each point of the 4-arc $\{x^{(0)}, x^{(1)}, x^{(2)}, x^{(3)}\}$ to itself, then $\langle g \rangle$ is isomorphic to $\mathbf{Z}_1$.*

Proof Suppose $x^{(i)h} = e_i$, for $i = 0, \ldots, 3$, then $h^{-1}gh$ maps each point of the standard frame to itself and $h^{-1}gh = \mathrm{I}$, by Theorem 1.52. Hence, $g = \mathrm{I}$. □

1.8 Duality

Definition 1.72. For any projective space $PG(r, q)$, there is a dual projective space $PG(r, q)^*$. The points and hyperplanes of $PG(r, q)^*$ are the hyperplanes and points of $PG(r, q)$.

If there is a theorem that is true in $PG(r, q)$, then there exists an equivalent theorem that is true in $PG(r, q)^*$. The theorem in $PG(r, q)^*$ is obtained by replacing points with hyperplanes and hyperplanes with points in $PG(r, q)$. This is not quite sufficient to obtain the new theorem, since any i linearly independent points define an $(i-1)$-dimensional projective space and i linearly independent hyperplanes intersect in a $(r - i)$-dimensional projective space. Hence, the language used to describe the incidence structures of the theorem in $PG(r, q)^*$ needs to be modified from that used to describe the incidence structures of the theorem in $PG(r, q)$. For example, in $PG(2, q)$ two points define a line and two lines intersect on a point.

1.9 Linear codes

A linear $[n, k, d]_q$-code $\mathfrak{C}$ over the finite field $\mathbf{F}_q$ is a k-dimensional subspace of the n-dimensional vector space $V(n, q)$ with non-zero vectors having weight at least d. That is, if $x = (x_0, \ldots, x_{n-1}) \in \mathfrak{C}$, then at least d of the x_i are non-zero.

Let $v_0, v_1, \ldots, v_{k-1}$, be a basis for $\mathfrak{C}$ and define the generator matrix M of the linear code $\mathfrak{C}$ to be the $k \times n$ matrix with j-th row v_{j-1}, for $j = 1, \ldots, k$. Let $u_0, u_1, \ldots u_{n-1} \in V(k, q)$ be the columns of the generator matrix M. Then $(u_i)_j = (v_j)_i$, for $i = 0, \ldots, n-1, j = 0, \ldots, k-1$.

For all $a = (a_0, \ldots, a_{k-1}) \in (\mathbf{F}_q)^k$, since the weight of the vector

$$\left(\sum_{j=0}^{k-1} a_j (v_j)_0, \ldots, \sum_{j=0}^{k-1} a_j (v_j)_{n-1} \right)$$

is at least d, it has at most $n - d$ zero coordinates. Hence, for $i = 0, \ldots, n-1$,

$$\sum_{j=0}^{k-1} a_j (v_j)_i = 0,$$

has $n - d$ solutions; equivalently,

$$\sum_{j=0}^{k-1} a_j (u_i)_j = 0,$$

has $n - d$ solutions.

This is equivalent to stating that of the n vectors u_i, for $i = 0, \ldots n-1$, at most $n - d$ are incident with the hyperplane

$$\sum_{j=0}^{k-1} a_j X_j = 0.$$

Therefore, an $(n, n-d)$-arc in $PG(k-1, q)$ is equivalent to a linear $[n, k, d]_q$-code $\mathfrak{C}$, where any two columns of the generator matrix of $\mathfrak{C}$ are linearly independent. This linear independence ensures that any two columns are projectively inequivalent.

Note 1.73. This description of the link between (n, r)-arcs and linear codes is taken from [2], in which more details can be found.

Example 1.74. The largest size of an $(n, 4)$-arc in $PG(2, 11)$ is $n = 32$ and this is equivalent to $n = 32$ is the largest value for which there exists a linear $[n, 3, n-4]_{11}$-code.

The spectrum of $(n, 3)$-arcs in $PG(2, 11)$ is $n = 3, \ldots, 21$ and this is equivalent to $n = 3, \ldots, 21$ is the range of n for which there exist linear $[n, 3, n-3]_{11}$-codes.

Chapter 2

The Non-Existence of Complete 12-arcs in $PG(2, 31)$

This work is a forerunner to that conducted on $(n, 3)$-arcs and $(n, 4)$-arcs in $PG(2, 11)$. Table 2.1 is taken from [7] and it shows the size of all complete arcs that were known prior to this work, where 12? and 13? indicate that the existence of a complete 12-arc and a complete 13-arc is unknown. The original aim of this work was to determine the existence of a complete 12-arc or a complete 13-arc in $PG(2, 31)$ and the size of the smallest complete n-arc.

Table 2.1: The size of all complete arcs for $q \leq 32$

q	n
2	4
3	4
4	6
5	6
7	6, 8
8	6, 10
9	6, 7, 8, 10
11	7, 8, 9, 10, 12
13	8, 9, 10, 12, 14
16	9, 10, 11, 12, 13, 17
17	10, 11, 12, 13, 14, 18
19	10, 11, 12, 13, 14, 20
23	10, 12, 13, 14, 15, 16, 17, 24
25	12, 13, 14, 15, 16, 17, 18, 21, 26
27	12, 13, 14, 15, 16, 17, 18, 19, 22, 28
29	13, 14, 15, 16, 17, 18, 19, 20, 21, 24, 30
31	12?, 13?, 14, 15, 16, 17, 18, 19, 20, 21, 22, 32
32	12?, 13?, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 34

An algorithm based on that used in [3] determined one representative from every class of projectively equivalent 8-arcs in $PG(2, 31)$, of which there are 3 768 298.

Note 2.1. For a description of this algorithm see Chapter 3.

A second algorithm is used to determine if it is possible to extend any of these projectively inequivalent 8-arcs to a complete 12-arc or a complete 13-arc. However, this version of the algorithm is too inefficient to determine the non-existence of complete 13-arcs; so, only the non-existence of complete 12-arcs is established.

2.1 A brief description of the second algorithm

The second algorithm takes as input an 8-arc containing the standard frame, represented as $S = \{e_0, e_1, e_2, e_3, s_0, s_1, s_2, s_3\}$ and tests every appropriate 12-arc extension of S, represented as $S \cup \{x_0, x_1, x_2, x_3\}$, for completeness. That is, the point x_0 is not on a bisecant of S, the point x_1 is not on a bisecant of $S \cup \{x_0\}$, the point x_2 is not on a bisecant of $S \cup \{x_0, x_1\}$ and the point x_3 is not on a bisecant of $S \cup \{x_0, x_1, x_2\}$. If it is possible to add additional points $y_0, \ldots, y_m$ to the 12-arc $S \cup \{x_0, x_1, x_2, x_3\}$, then this 12-arc cannot be complete. Let σ be a permutation on $\overline{\mathbf{N}}_3$. Then the 12-arcs $S \cup \{x_0\sigma, x_1\sigma, x_2\sigma, y_i\}$ are not complete, for $i = 0, \ldots, m$, as it is possible to add the point $x_3\sigma$ to each of these new 12-arcs.

2.2 A full description of the second algorithm

The projective plane $PG(2,31)$ contains $q^2+q+1 = 993$ points and 993 lines. Every point is represented by a unique number $x_i \in \overline{\mathbf{N}}_{992}$ and every line is represented by a unique number $\ell_i \in \overline{\mathbf{N}}_{992}$. The numbers representing the points of $PG(2,31)$ are ordered; if x represents the point $P(X_0, X_1, X_2)$ and y represents the point $P(Y_0, Y_1, Y_2)$, then

$$x < y \equiv \begin{cases} X_0 \leq Y_0 \\ \text{or } X_0 = Y_0 \text{ and } X_1 \leq Y_1 \\ \text{or } X_0 = Y_0,\ X_1 = Y_1 \text{ and } X_2 \leq Y_2. \end{cases}$$

Since each point is incident with $q+1 = 32$ lines and each line is incident with $q+1 = 32$ points, a point is also represented by the 1×32 array $\{\ell_0, \ell_1, \ldots, \ell_{31}\}$ and a line by the 1×32 array $\{x_0, x_1, \ldots, x_{31}\}$.

The second algorithm is based around a $(31-2) \times (31-2)$ array $incidence_{29\times29}$ with elements comprising unique numbers in the range $0, \ldots, 992$. The numbers in a row of $incidence_{29\times29}$ represent the points on a line through the point e_0 excluding e_0 itself. The numbers in a column of $incidence_{29\times29}$ represent the points on a line through the point e_1 excluding e_1 itself. The array $incidence_{29\times29}$ has dimension 29×29, because the lines incident with the pairs of points

$$(e_0, e_1), (e_0, e_2), (e_0, e_3), (e_1, e_2), (e_1, e_3), (e_2, e_3)$$

are not considered. This is because, $incidence_{29\times29}$ is used as a reference for adding new points to each extension of an 8-arc containing the standard frame. If the point represented by the number in the i-th row and j-th column of $incidence_{29\times29}$ is added to an n-arc, then

all the points represented by numbers in the i-th row and j-th column are on bisecants of the new $(n+1)$-arc.

In both algorithms, after the standard frame $\{e_0, e_1, e_2, e_3\}$ is created all subsequent points are added in the order of their row position in $incidence_{29\times 29}$. For example, given the 8-arc $S = \{e_0, e_1, e_2, e_3, s_0, s_1, s_2, s_3\}$, where s_i is incident with the r_i-th row of $incidence_{29\times 29}$, the inequality $r_0 < r_1 < r_2 < r_3$ holds. This adds a further restriction to the points that can be added to an extension of an 8-arc, since the point x_2 can not be selected from row 28 as this would leave no row from which to select the point x_3,..., the point s_0 can not be selected from rows $22, \ldots, 28$ as this would leave insufficient rows from which to select the points $s_1, \ldots, s_3, x_0, \ldots, x_3$.

Note 2.2. The ordering of points in the construction of a 12-arc does not affect the exhaustive nature of the search, because if x is a point in the r-th row of $incidence_{29\times 29}$ that is not on a bisecant of $S \cup \{x_0, \ldots, x_N\}$, where $r_{i+4} < r < r_{i+4+1}$, then the $(i+10)$-arc $S \cup \{x_0, \ldots, x_i, x\}$ is searched at a previous stage.

Notation 2.3. The element in the i-th row and j-th column of an array X is denoted $X[i][j]$.

A 29×29 array $remove8_{29\times 29}$ is associated with both the array $incidence_{29\times 29}$ and the 8-arc $S_8 = \{e_0, e_1, e_2, e_3, s_0, s_1, s_2, s_3\}$.

$$remove8_{29\times 29}[i][j] = \begin{cases} 0 & \text{if } incidence_{29\times 29}[i][j] \text{ is incident with a bisecant of } S_8, \\ 1 & \text{otherwise.} \end{cases}$$

A 29×29 array $remove9_{29\times 29}$ is associated with the arrays $incidence_{29\times 29}$ and $remove8_{29\times 29}$ and the 9-arc $S_9 = \{e_0, e_1, e_2, e_3, s_0, s_1, s_2, s_3\} \cup \{x_0\}$.

$$remove9_{29\times 29}[i][j] = \begin{cases} 0 & \text{if } remove8_{29\times 29}[i][j] = 0 \\ & \text{or } incidence_{29\times 29}[i][j] \text{ is incident with a bisecant of } S_9, \\ x_0 & \text{otherwise.} \end{cases}$$

A 29×29 array $remove10_{29\times 29}$ is associated with the arrays $incidence_{29\times 29}$, $remove8_{29\times 29}$ and $remove9_{29\times 29}$ and the 10-arc $S_{10} = \{e_0, e_1, e_2, e_3, s_0, s_1, s_2, s_3\} \cup \{x_0, x_1\}$.

$$remove10_{29\times 29}[i][j] = \begin{cases} 0 & \text{if } remove8_{29\times 29}[i][j] = 0 \\ & \text{or } remove9_{29\times 29}[i][j] = x_0 \\ & \text{or } incidence_{29\times 29}[i][j] \text{ is incident with a bisecant of } S_{10}, \\ x_1 & \text{otherwise.} \end{cases}$$

A 29×29 array $remove11_{29\times 29}$ is associated with the arrays $incidence_{29\times 29}$, $remove8_{29\times 29}$, $remove9_{29\times 29}$ and $remove10_{29\times 29}$ and the 11-arc $S_{11} = \{e_0, e_1, e_2, e_3, s_0, s_1, s_2, s_3\} \cup \{x_0, x_1, x_2\}$.

$$remove11_{29\times29}[i][j] = \begin{cases} 0 & \text{if } remove8_{29\times29}[i][j] = 0 \\ & \text{or } remove9_{29\times29}[i][j] = x_0 \\ & \text{or } remove10_{29\times29}[i][j] = x_1 \\ & \text{or } incidence_{29\times29}[i][j] \text{ is incident with a bisecant of } S_{11}, \\ x_2 & \text{otherwise.} \end{cases}$$

A 29×29 array $remove12_{29\times29}$ is associated with the arrays $incidence_{29\times29}$, $remove8_{29\times29}$, $remove9_{29\times29}$, $remove10_{29\times29}$ and $remove11_{29\times29}$ and the 12-arc

$$S_{12} = \{e_0, e_1, e_2, e_3, s_0, s_1, s_2, s_3\} \cup \{x_0, x_1, x_2, x_3\}.$$

$$remove12_{29\times29}[i][j] = \begin{cases} 0 & \text{if } remove8_{29\times29}[i][j] = 0 \\ & \text{or } remove9_{29\times29}[i][j] = x_0 \\ & \text{or } remove10_{29\times29}[i][j] = x_1 \\ & \text{or } remove11_{29\times29}[i][j] = x_2 \\ & \text{or } incidence_{29\times29}[i][j] \text{ is incident with a bisecant of } S_{12}, \\ x_3 & \text{otherwise.} \end{cases}$$

Consider the following 5×5 segment of $incidence_{29\times29}$;

$$\begin{pmatrix} x_{0,0} & x_{0,1} & x_{0,2} & x_{0,3} & x_{0,4} \\ x_{1,0} & x_{1,1} & x_{1,2} & x_{1,3} & x_{1,4} \\ x_{2,0} & x_{2,1} & x_{2,2} & x_{2,3} & x_{2,4} \\ x_{3,0} & x_{3,1} & x_{3,2} & x_{3,3} & x_{3,4} \\ x_{4,0} & x_{4,1} & x_{4,2} & x_{4,3} & x_{4,4} \end{pmatrix}.$$

Example 2.4. In this example the corresponding 5×5 segment of $remove8_{29\times29}$ is considered. For the 12-arc $S_{12} = \{e_0, e_1, e_2, e_3, s_0, s_1, s_2, s_3\} \cup \{x_0, x_1, x_2, x_3\}$, if $remove8_{29\times29}[i][j] = 1$ and $removeX_{29\times29}[i][j] = x_{X-9}$, for $X \in [9, \ldots, 12]$, then the element $remove8_{29\times29}[i][j]$ is replaced by x_{X-9}. This produces the following 5×5 segment of array.

$$A = \begin{pmatrix} x_0 & x_3 & 0 & x_2 & 0 \\ 0 & x_1 & x_2 & 0 & 0 \\ 0 & x_0 & x_0 & x_1 & 0 \\ x_0 & 0 & 1 & 0 & x_0 \\ x_1 & 0 & x_0 & 0 & 0 \end{pmatrix}$$

Since the point represented by $x_{3,2}$ corresponds to a 1 in the array A, this point is not on a bisecant of S_{12}; hence, S_{12} is not complete.

The arrays $remove8_{29\times29}$ and $remove9_{29\times29}$ are destroyed and recreated for every new 8-arc. For efficiency, if extensions of the 8-arc $S_8 = \{e_0, e_1, e_2, e_3, s_0, s_1, s_2, s_3\}$ are being

considered, then the array $remove9_{29\times 29}$ is not destroyed and recreated for every 9-arc extension of S_8. Instead, if $S_8 \cup \{x_0^{(i)}\}$ is the i-th 9-arc extension of S_8 to be considered, then all the values $x_0^{(1)}, \ldots, x_0^{(i-1)}$ are still present in $remove9_{29\times 29}$ and these combined with any 0 elements are grouped together as elements that are different from $x_0^{(i)}$. Similarly, the arrays $remove10_{29\times 29}$, $remove11_{29\times 29}$ and $remove12_{29\times 29}$ are destroyed and recreated for every 9-arc, 10-arc and 11-arc and not for every 10-arc, 11-arc and 12-arc.

2.3 Results

The second algorithm did not discover a complete 12-arc in $PG(2, 31)$, which combined with the exhaustive nature of the search implies that no complete 12-arc exists in $PG(2, 31)$. The second algorithm proved too slow for a similar search of all 13-arcs in $PG(2, 31)$ to be completed; hence, the size of the smallest complete n-arc in $PG(2, 31)$ could not be determined.

Therefore, while this method is not sufficient for its original purpose, that is, to discover the size of the smallest complete n-arc in $PG(2, 31)$, it did increase the lower bound for the value of n. This work has been superseded and the non-existence of both a complete 12-arc and a complete 13-arc, for $q = 31, 32$, is shown in [8].

Chapter 3

The Classification of Complete $(n, 3)$-arcs in $PG(2, 11)$

3.1 The algorithm

Every point of $PG(2, 11)$ is represented by a unique number from the set $\{0, \ldots, 132\}$.

$0 = e_3 = (0, 0, 1)$	$1 = (0, 1, -5)$	$\ldots$	$6 = e_2 = (0, 1, 0)$
$\ldots$	$11 = (0, 1, 5)$	$12 = (1, -5, -5)$	$\ldots$
$72 = e_1 = (1, 0, 0)$	$\ldots$	$84 = e_4 = (1, 1, 1)$	$\ldots$
$132 = (1, 5, 5)$			

This creates the following ordering of points in the projective plane of order eleven. If x represents the point $P(X_0, X_1, X_2)$ and y represents the point $P(Y_0, Y_1, Y_2)$, then

$$x < y \equiv \begin{cases} X_0 \leq Y_0 \\ \text{or } X_0 = Y_0 \text{ and } X_1 \leq Y_1 \\ \text{or } X_0 = Y_0,\ X_1 = Y_1 \text{ and } X_2 \leq Y_2. \end{cases}$$

Every line in $PG(2, 11)$ is represented by a unique number from the set $\{0, \ldots, 132\}$.

A point x of $PG(2, 11)$ is incident with $q + 1 = 12$ lines and is therefore associated with the set $\{\ell_0, \ldots, \ell_{11}\}$, where $\ell_i \in \{0, \ldots, 132\}$ represents a line through x. A line ℓ in $PG(2, 11)$ is incident with 12 points and is therefore associated with the set $\{x_0, \ldots, x_{11}\}$, where $x_i \in \{0, \ldots, 132\}$ represents a point on ℓ.

Similarly, an (n, r)-arc in $PG(2, 11)$ is represented as a set of n appropriate numbers from the set $\{0, \ldots, 132\}$.

Notation 3.1. The notation (n, r^-)-arc is used to denote an (n, γ)-arc, where γ is known to be less than or equal to r.

Proposition 3.2. *Let $\mathfrak{P}_5 = \{x_1, x_2, x_3, x_4, x_5\}$ be a set of 5 points that is contained in an $(n, 3)$-arc, where $n \geq 5$. Then, some subset of 4 points in $\mathfrak{P}_5$ is a 4-arc.*

Proof There are three possibilities either $\mathfrak{P}_5$ is a 5-arc, $\mathfrak{P}_5$ has one trisecant or $\mathfrak{P}_5$ has two trisecants. If $\mathfrak{P}_5$ has one trisecant, then it may be assumed without loss of generality that

the points $\{x_1, x_2, x_3\}$ are collinear. Hence, the set of points $\{x_i, x_j, x_4, x_5\}$ forms a 4-arc. If $\mathfrak{P}_5$ has two trisecants, then it may be assumed without loss of generality that the two trisecants intersect at the point x_1. Hence, the set $\{x_2, x_3, x_4, x_5\}$ forms a 4-arc. □

Since an $(n, 3)$-arc contains a 4-arc if $n \geq 5$, the standard frame $S_4 = \{e_1, e_2, e_3, e_4\}$ is used as the base on which all $(n \geq 5, 3)$-arcs are constructed. The standard frame S_4 is projectively equivalent to every 4-arc, by Corollary 1.53.

Define R_n to be the set containing one representative from every class of projectively equivalent $(n, 3^-)$-arc, for all $n \in \{5, \ldots, 21\}$. Algorithm 1 shows how the set R_{n+1} is constructed from the set R_n, for $n = 4, \ldots, 20$.

Algorithm 1 Algorithm for producing the set R_n, for $n = 5, \ldots, 21$

```
R_4 = {S_4}
for n = 4 → 20 do
  R_{n+1} = ∅
  for all S ∈ R_n do
    for all x ∈ PG(2,q)\S do
      if S ∪ {x} is an (n+1, 3^-)-arc then
        if {S ∪ {x}}^g ∈ R_{n+1}, for any g ∈ PGL(3,q) then
          Do nothing
        else
          Add S ∪ {x} to R_{n+1}
        end if
      end if
    end for
  end for
end for
```

The projective equivalence of two $(n, 3^-)$-arcs is determined by the equality of their canonical form.

3.1.1 Invariants and canonical forms for $(n, 3)$-arcs in $PG(2, q)$

Notation 3.3. Let S be an $(n, 3^-)$-arc in $PG(2, q)$ and let x be a point of $PG(2, q)$. Then denote the number of bisecants of S through x as $b_S(x)$ and the number of trisecants of S through x as $t_S(x)$.

Proposition 3.4. *The number of bisecants and trisecants through a point x of $PG(2, q)$ is invariant under the right action of g, for all $(\mathfrak{T}, g) \in PGL(3, q)$. That is, $b_{S^g}(x^g) = b_S(x)$ and $t_{S^g}(x^g) = t_S(x)$, for all $(\mathfrak{T}, g) \in PGL(3, q)$.*

Proof Let $P(\alpha X + Y), \alpha \neq 0$ be a third point on the line through the points $P(X)$ and $P(Y)$. Then $P((\alpha X + Y)g) = P(\alpha Xg + Yg), \alpha \neq 0$ is a third point on the line through the points $P(Xg)$ and $P(Yg)$. □

Definition 3.5 (Line invariant)**.** For every line ℓ in $PG(2, q)$ the line invariant is defined as

$$I_S(\ell) = \sum_{x \in \ell \setminus S} 2^{(q+2)t_S(x)+b_S(x)}.$$

The line invariant satisfies

$$I_{S^g}(\ell^g) = \sum_{x^g \in \ell^g \setminus S^g} 2^{(q+2)t_{S^g}(x^g)+b_{S^g}(x^g)} = \sum_{x \in \ell \setminus S} 2^{(q+2)t_S(x)+b_S(x)} = I_S(\ell),$$

for all $(\mathfrak{T}, g) \in PGL(3, q)$.

Note 3.6. Definition 3.5 differs from the definition of the line invariant given in [3], as it is adapted to work with $(n, 3)$-arcs and this definition is improved in Section 3.2.1.

Definition 3.7 (Point invariant)**.** For every point x of $PG(2, q)$, the point invariant is defined as

$$I_S(x) = \sum_{\ell, x \in \ell} h(I_S(\ell)),$$

where h is a simple hash function. The point invariant satisfies

$$I_{S^g}(x^g) = \sum_{\ell^g, x^g \in \ell^g} h(I_{S^g}(\ell^g)) = \sum_{\ell, x \in \ell} h(I_S(\ell)) = I_S(x),$$

for all $(\mathfrak{T}, g) \in PGL(3, q)$.

For $i = I_S(\ell) \pmod{127} + 126$, the *hash function* $h(I_S(\ell)) = (0, \ldots, 0, 1, 0, \ldots, 0)$ has a 1 in the i-th position, representing the value 13^i. Since $I_S(x)$ is the sum of hash functions, it is an array, the i-th element of which is denoted as $I_S(x)_i$. To ensure that $I_S(x)$ represents any value uniquely, the restriction $0 \leq I_S(x)_i \leq 12$ is imposed on the elements of $I_S(x)$. If $I_S(x)_i = a + 13b$, where $a \in \{0, \ldots, 12\}$ and $b > 0$, then $I_S(x)_i = a$ and $I_S(x)_{i+1}$ is incremented by b, for all $i \in \{126, \ldots, N\}$. Hence, $I_S(x)$ uniquely represents the value

$$\sum_{x \in S} 13^i I_S(x).$$

Note 3.8. It should be noted that, for $q = 11$, if $I_S(x)_i = a + 13b$, then $b = 0$, since only 12 hash functions are being summed.

Definition 3.9 (Set Invariant)**.** The set invariant is defined as

$$I(S) = \sum_{x \in S} I_S(x).$$

The set invariant satisfies,

$$I(S^g) = \sum_{x^g \in S^g} I_{S^g}(x^g) = \sum_{x \in S} I_S(x) = I(S),$$

for all $(\mathfrak{T}, g) \in PGL(3, q)$.

Definition 3.10 (Quasi-Orbits)**.** The point invariant I_S induces a partition $I_S\backslash\backslash S$ on S in the following way. Two points x and x' belong to the same part $U \in I_S\backslash\backslash S$ if and only if $I_S(x) = I_S(x')$; in which case the notation $I_S(U) = I_S(x)$ is used. The parts of this partition are called quasi-orbits of S. From the definition of the point invariant,

$$I_{S^g}(U^g) = I_{S^g}(x^g) = I_S(x) = I_S(U);$$

hence,

$$U^g \in I_{S^g}\backslash\backslash S^g \Leftrightarrow U \in I_S\backslash\backslash S,$$

for all $(\mathfrak{T}, g) \in PGL(3, q)$.

The parts of the partition $I_S\backslash\backslash S$ are ordered, first according to magnitude and then according to their point invariant value. That is, if $U, U' \in I_S\backslash\backslash S$, then $U < U'$ if and only if $|U| < |U'|$ or $\{|U| = |U'|$ and $I_S(U) < I_S(U')\}$. The ordered partition of S into quasi-orbits is denoted

$$I_S\backslash\backslash S = \{U_1, U_2, U_3, \ldots\}, \text{ where } U_1 < U_2 < U_3 < \cdots .$$

It follows directly from the definition of quasi-orbits that

$$I_{S^g}(U^g) = I_S(U)$$

and

$$|U^g| = |U|,$$

for all $(\mathfrak{T}, g) \in PGL(3, q)$. Hence,

$$I_{S^g}\backslash\backslash S^g = \{U_1^g, U_2^g, U_3^g, \ldots\}, \text{ where } U_1^g < U_2^g < U_3^g < \cdots .$$

Note 3.11. The construction of the canonical form differs from that given in [3] so as to work with $(n, 3)$-arcs.

Construction 3.12. Let $U_{\min 5}(S)$ be the first set containing exactly 5 points in the ordered partition $I_S\backslash\backslash S$. If no such set exists, then $U_{\min 5}(S)$ is the first set with the minimum number of points greater than or equal to 5 in the ordered sets

(1) $\{U_{i_1} \cup U_{i_2}\}$ $i_1 < i_2$, every ordered pair of parts,

(2) $\{U_{i_1} \cup U_{i_2} \cup U_{i_3}\}$ $i_1 < i_2 < i_3$, every ordered union of three parts,

(3) $\{U_{i_1} \cup U_{i_2} \cup U_{i_3} \cup U_{i_4}\}$ $i_1 < i_2 < i_3 < i_4$, every ordered union of four parts,

(4) $\{U_{i_1} \cup U_{i_2} \cup U_{i_3} \cup U_{i_4} \cup U_{i_5}\}$ $i_1 < i_2 < i_3 < i_4 < i_5$, every ordered union of five parts.

The set $U_{\min 5}(S)$ contains at least five points with the property 'at most three points on a line'. At least four of these five points must have the property 'at most two points on a line'; that is, they form a 4-arc. It follows directly from the definition of the ordering of quasi orbits that $U_{\min 5}(S^g) = U_{\min 5}(S)^g$, for all $(\mathfrak{T}, g) \in PGL(3, q)$.

Definition 3.13 (Canonical Form)**.** Let $\{x_1, x_2, x_3, x_4\}$ be an arrangement of a 4-arc from $U_{\min 5}(S)$, where S is an $(n,3^-)$-arc in $PG(2,q)$ and let $(\mathfrak{T}, g) \in PGL(3,q)$ be such that $x_1^g = e_1$, $x_2^g = e_2$, $x_3^g = e_3$, $x_4^g = e_4$. Then S^g is an $(n,3^-)$-arc that is projectively equivalent to S. The points of S^g are ordered in ascending numerical value. For all arrangements of all 4-arcs in $U_{\min 5}(S)$, define the *canonical form of* S $\mathrm{can}(S)$, to be the smallest of all such ordered S^g, with regard to the lexical ordering of their points.

Proposition 3.14. *Let S and T be $(n,3^-)$-arcs in $PG(2,q)$. Then $\mathrm{can}(S) = \mathrm{can}(T)$ if and only if S and T are projectively equivalent.*

Proof Let $T = S^h$, where $(\mathfrak{T}_h, h) \in PGL(3,q)$. Then $U_{\min 5}(T) = U_{\min 5}(S)^h$. Suppose the points $x_1, x_2, x_3, x_4 \in U_{\min 5}(S)$ form a 4-arc, then the points $x_1^h, x_2^h, x_3^h, x_4^h \in U_{\min 5}(T)$ also form a 4-arc.

If $(\mathfrak{T}_g, g) \in PGL(3,q)$ is such that $x_1^g = e_1$, $x_2^g = e_2$, $x_3^g = e_3$, $x_4^g = e_4$, then $(\mathfrak{T}_h^{-1}\mathfrak{T}_g, h^{-1}g) \in PGL(3,q)$ is such that $x_1^{hh^{-1}g} = e_1$, $x_2^{hh^{-1}g} = e_2$, $x_3^{hh^{-1}g} = e_3$, $x_4^{hh^{-1}g} = e_4$ and $T^{h^{-1}g} = S^g$. Hence, the points from $U_{\min 5}(S)$ produce the same set of ordered $(n,3)$-arcs as the points from $U_{\min 5}(T)$, making the minimum of this set both $\mathrm{can}(S)$ and $\mathrm{can}(T)$.

If $\mathrm{can}(S) = \mathrm{can}(T)$, $\mathrm{can}(S) = S^{g_1}$ and $\mathrm{can}(T) = T^{g_2}$, where $(\mathfrak{T}_{g_1}, g_1), (\mathfrak{T}_{g_2}, g_2) \in PGL(3,q)$, then $T = S^{g_1 g_2^{-1}}$; hence, S and T are projectively equivalent. □

The algorithm produces a list containing one representative from every class of projectively equivalent $(n,3^-)$-arcs and a corresponding list of canonical forms. Both these lists are stored. The list of $(n,3^-)$-arcs is used in the construction of $(n+1,3^-)$-arcs and the list of canonical forms is used to determine projective equivalence.

A number, $N \in \{0, \ldots, 4\ 826\ 808\}$, is generated for every canonical form and this number is based on the numbers that represent the points in this canonical form. The number N is not unique for each projectively inequivalent $(n,3^-)$-arc. However, two projectively equivalent $(n,3^-)$-arcs produce the same N. This allows the list of canonical forms to be partitioned so that, when a new $(n,3^-)$-arc is to be added, its canonical form only needs to be checked against a small proportion of the elements of the list.

An array of vectors of length 4 826 808 is used, the Nth element of which is the position in the two lists of all canonical forms that produce the number N and their corresponding $(n,3^-)$-arcs. This array is used for fast reference.

Remark 3.15. The advantage of this method is that it allows for the points forming an $(n,3^-)$-arc to be selected in an ordered fashion. This works well for $(n,3^-)$-arcs in $PG(2,11)$, but for $q \geq 13$ the array is to large. The disadvantage is the necessity to store such a large array in active memory, as this makes it impractical to have multiple programs searching through all $(n,3^-)$-arcs that arise from different $(n-1,3^-)$-arcs on one machine. It is possible to produce multiple lists of projectively inequivalent $(n+1,3^-)$-arcs from subsets of R_n, but this makes additional searches necessary to remove duplicate entries, since projective inequivalence is not preserved between lists generated from different subsets of R_n.

3.2 Improvements to the algorithm

There are at least three possible improvements to this algorithm, with regard to increasing its speed and decreasing its storage needs. The first improvement is to the construction of the

line invariant $I_S(\ell)$. The second improvement is to the calculation of the canonical form. The third improvement involves using a specific orbit of $I_S\backslash\backslash S$ to partition the $(n+1,3^-)$-arcs into sets that are closed under projective equivalence. This final improvement is the most significant as it removes the necessity to use the array of size 4 826 808 in active memory and the need to store the canonical form for every projectively inequivalent $(n,3^-)$-arc that arises.

3.2.1 Improvement to the invariant

For $r=3$, equations (1.6) and (1.7) are $\tau_0+\tau_1+\tau_2+\tau_3=q+1$ and $\tau_1+2\tau_2+3\tau_3=n$; so, for specific q, the values τ_0 and τ_1 can be determined if τ_2 and τ_3 are known. If there are M possible pairs (τ_2,τ_3), then define the map f to be

$$f(\tau_2,\tau_3)\to i\in(0,\ldots,M-1),$$

where

$$f(\tau_2^{(1)},\tau_3^{(1)})>f(\tau_2^{(2)},\tau_3^{(2)}) \text{ if } \tau_3^{(1)}>\tau_3^{(2)}$$

and

$$f(\tau_2^{(1)},\tau_3^{(1)})>f(\tau_2^{(2)},\tau_3^{(2)}) \text{ if } \tau_3^{(1)}=\tau_3^{(2)} \text{ and } \tau_2^{(1)}>\tau_2^{(2)}.$$

A point x that is incident with τ_2 bisecants and τ_3 trisecants is associated with a value $f(\tau_2,\tau_3)$.

An improvement to the invariant $I_S(l)$ is achieved by replacing $(q+2)t_S(x)+b_S(x)$ with $f(\tau_2,\tau_3)$. The value of $2^{f(\tau_2,\tau_3)}$ is faster to calculate than $2^{(q+2)t_S(x)+b_S(x)}$, since $(q+2)t_S(x)+b_S(x)\geq f(\tau_2,\tau_3)$ and $(q+2)t_S(x)+b_S(x)>f(\tau_2,\tau_3)$ if $t_S(x)>0$.

Example 3.16. For $q=11$ and $k=10$, the possibilities for $(\tau_0,\tau_1,\tau_2,\tau_3)$ with corresponding $f(\tau_2,\tau_3)$ are as follows.

$(\tau_0,\tau_1,\tau_2,\tau_3)$	$f(\tau_2,\tau_3)$
$(2,10,0,0)$	$f(0,0)=0$
$(3,8,1,0)$	$f(1,0)=1$
$(4,6,2,0)$	$f(2,0)=2$
$(5,4,3,0)$	$f(3,0)=3$
$(6,2,4,0)$	$f(4,0)=4$
$(7,0,5,0)$	$f(5,0)=5$
$(4,7,0,1)$	$f(0,1)=6$
$(5,5,1,1)$	$f(1,1)=7$
$(6,3,2,1)$	$f(2,1)=8$
$(7,1,3,1)$	$f(3,1)=9$
$(6,4,0,2)$	$f(0,2)=10$
$(7,2,1,2)$	$f(1,2)=11$
$(8,0,2,2)$	$f(2,2)=12$
$(8,1,0,3)$	$f(0,3)=13$

3.2.2 Improvement to the canonical form

Instead of considering every permutation of 4 points from the set U_{min5}, the sets of 4 points that are used to create the canonical form are selected as follows.

From the partition $I_S\backslash\backslash S$, select $U_1,\ldots,U_m$ such that $U_1\cup\cdots\cup U_{m-1}$ contains fewer than 5 points and $U_1\cup\cdots\cup U_m$ contains at least 5 points. The first $|U_1|$ points to be selected consist of all permutations of points from U_1, the next $|U_2|$ points consist of all permutations of points from U_2, ..., the next $|U_{m-1}|$ points consist of all permutations of points from U_{m-1}. The remaining $5-|U_1\cup\cdots\cup U_{m-1}|$ points consist of all permutations of $5-|U_1\cup\cdots\cup U_{m-1}|$ points from U_m. Hence, there are

$$\frac{|U_1|!|U_2|!\ldots|U_{m-1}|!|U_m|!}{||U_m|-(5-|U_1\cup\cdots\cup U_{m-1}|)|!}$$

sets of 5 ordered points. For each of these sets of 5 points, subsets of 4 points are selected so as to preserve the ordering of the points by their quasi-orbits. In the original method there are at least 5! ways of choosing 4 ordered points from U_{min5}, here there may be as few as 5.

Proposition 3.17. *Let S and T be $(n,3^-)$-arcs in $PG(2,q)$. Then $\mathrm{can}(S)=\mathrm{can}(T)$ if and only if S and T are projectively equivalent.*

Proof Let $T=S^h$, where $(\mathfrak{T}_h,h)\in PGL(3,q)$. Then the 5 ordered points $\{x_1,x_2,x_3,x_4,x_5\}$ are selected from $I_S\backslash\backslash S$ if and only if the 5 ordered points $\{x_1^h,x_2^h,x_3^h,x_4^h,x_5^h\}$ are selected from $I_T\backslash\backslash T$. The 4 points $\{x_{i_1},x_{i_2},x_{i_3},x_{i_4}\}$ of $\{x_1,x_2,x_3,x_4,x_5\}$ form a 4-arc if and only if the 4 points $\{x_{i_1}^h,x_{i_2}^h,x_{i_3}^h,x_{i_4}^h\}$ of $\{x_1^h,x_2^h,x_3^h,x_4^h,x_5^h\}$ form a 4-arc.

If $(\mathfrak{T}_g,g)\in PGL(3,q)$ is such that $x_{i_1}^g=e_1$, $x_{i_2}^g=e_2$, $x_{i_3}^g=e_3$, $x_{i_4}^g=e_4$, then $(\mathfrak{T}_h^{-1}\mathfrak{T}_g,h^{-1}g)\in PGL(3,q)$ is such that $x_{i_1}^{hh^{-1}g}=e_1$, $x_{i_2}^{hh^{-1}g}=e_2$, $x_{i_3}^{hh^{-1}g}=e_3$, $x_{i_4}^{hh^{-1}g}=e_4$ and $T^{h^{-1}g}=S^g$. Hence, the sets of 5 ordered points from $I_S\backslash\backslash S$ and $I_T\backslash\backslash T$ produce the same set of ordered $(n,3^-)$-arcs making the minimum of this set both $\mathrm{can}(S)$ and $\mathrm{can}(T)$.

If $\mathrm{can}(S)=\mathrm{can}(T)$, $\mathrm{can}(S)=S^{g_1}$ and $\mathrm{can}(T)=T^{g_2}$, where $(\mathfrak{T}_{g_1},g_1),(\mathfrak{T}_{g_2},g_2)\in PGL(3,q)$, then $T=S^{g_1g_2^{-1}}$; hence, S and T are projectively equivalent. □

Example 3.18 (An example from $PG(2,11)$)**.** Let $S=\{0,1,6,12,13,38,72,84,102\}$, where $U_1=\{72\}$, $U_2=\{0,38\}$, $U_3=\{84,12\}$, $U_4=\{1,13\}$ and $U_5=\{6,102\}$. Then $U_{min5}=\{72,0,38,84,12\}$ and in the original method all 5! permutations of 4 points from these 5 points are considered. In the new method, for each of the ordered sets $S_1=\{72,0,38,84,12\}$, $S_2=\{72,0,38,12,84\}$, $S_3=\{72,38,0,84,12\}$ and $S_4=\{72,38,0,12,84\}$, every ordered subset of 4 points is considered. For S_1, the 4-arc $\{0,38,84,12\}$ is mapped under the right action of the matrix

$$\begin{pmatrix}-4&-4&3\\-4&4&1\\-3&0&0\end{pmatrix}$$

to $\{e_1,e_2,e_3,e_4\}$ and S to $\{0,6,9,24,58,72,84,85,90\}$. For S_1 and S_2, the 4-arc $\{72,0,38,12\}$ is mapped under the right action of the matrix

$$\begin{pmatrix}-2&0&0\\3&-5&-1\\0&4&0\end{pmatrix}$$

to $\{e_1, e_2, e_3, e_4\}$ and S to $\{0, 6, 57, 60, 72, 84, 90, 114, 117\}$. For S_1 and S_2, the 4-arc $\{72, 0, 38, 84\}$ is mapped under the right action of the matrix

$$\begin{pmatrix} 3 & 0 & 0 \\ 1 & -2 & 4 \\ 0 & -5 & 0 \end{pmatrix}$$

to $\{e_1, e_2, e_3, e_4\}$ and S to $\{0, 6, 27, 30, 54, 60, 72, 84, 87\}$. For S_2, the 4-arc $\{0, 38, 12, 84\}$ is mapped under the right action of the matrix

$$\begin{pmatrix} -5 & -5 & 1 \\ -2 & -1 & 4 \\ 1 & 0 & 0 \end{pmatrix}$$

to $\{e_1, e_2, e_3, e_4\}$ and S to $\{0, 6, 15, 40, 64, 72, 75, 84, 85\}$. For S_3, the 4-arc $\{38, 0, 84, 12\}$ is mapped under the right action of the matrix

$$\begin{pmatrix} 4 & 4 & -1 \\ 1 & 4 & -4 \\ 0 & -1 & 0 \end{pmatrix}$$

to $\{e_1, e_2, e_3, e_4\}$ and S to $\{0, 6, 15, 40, 64, 72, 75, 84, 85\}$. For S_3 and S_4, the 4-arc $\{72, 38, 0, 12\}$ is mapped under the right action of the matrix

$$\begin{pmatrix} 2 & 0 & 0 \\ -3 & 1 & 5 \\ 0 & 0 & -4 \end{pmatrix}$$

to $\{e_1, e_2, e_3, e_4\}$ and S to $\{0, 6, 27, 30, 54, 60, 72, 84, 87\}$. For S_3 and S_4, the 4-arc $\{72, 38, 0, 84\}$ is mapped under the right action of the matrix

$$\begin{pmatrix} -3 & 0 & 0 \\ -1 & -4 & 2 \\ 0 & 0 & 5 \end{pmatrix}$$

to $\{e_1, e_2, e_3, e_4\}$ and S to $\{0, 6, 57, 60, 72, 84, 90, 114, 117\}$. Hence the canonical form of S is the ordered set of points $\{0, 6, 9, 24, 58, 72, 84, 85, 90\}$. The number N is calculated as follows:

$(1(0)+10^3(6)+10^6(9)+10^9(24)+10^{12}(58)+1(72)+10^3(84)+10^6(85)+10^9(90))\text{mod}(4\ 826\ 809)$.

3.2.3 Removing the need to store and reference $\text{can}(S)$ for every $(n, 3)$-arc S

The most costly part of this algorithm in terms of speed and storage is calculating and storing the canonical form for every projectively inequivalent $(n, 3)$-arc that arises, as well as using the vector of length 4 826 808 for referencing these canonical forms.

Definition 3.19. If $U_i = \{x\} \in I_S \backslash\backslash S$, then the point $x \in S$ is called a *singleton* of S.

Let R_n be the set containing one representative from every class of projectively equivalent $(n,3^-)$-arcs. For $S \in R_n$, let $x_i \in PG(2,q)\backslash S$, where $t_S(x_i) = 0$, be the smallest singleton $U_1 = \{x_i\}$ of the partition $I_{S\cup\{x_i\}}\backslash\backslash S \cup \{x_i\}$ such that $S \cup \{x_i\}$ is an $(n,3^-)$-arc. Then the set of all $(n+1,3^-)$-arcs $S \cup U_1$ is denoted $R_{n+1}^{(S)} \subset R_{n+1}$.

Proposition 3.20. *The set* $\bigcup_{S\in R_n} R_{n+1}^{(S)}$ *contains at least one representative from every class of projectively equivalent* $(n+1,3^-)$-arcs *that possesses at least one singleton.*

Proof Let $T\cup\{x\}$ be any $(n+1,3^-)$-arc such that $U_1 = \{x\}$ in the partition $I_{T\cup\{x\}}\backslash\backslash T\cup\{x\}$. Then T is an $(n,3^-)$-arc. Since $T^g \in R_n$, for some $(\mathfrak{T},g) \in PGL(3,q)$, the set of points $T^g \cup \{x\}^g$ is an $(n+1,3^-)$-arc with $U_1 = \{x^g\}$ in the partition $I_{T^g\cup\{x\}^g}\backslash\backslash T^g \cup \{x\}^g$. That is, $T^g \cup \{x\}^g \in \bigcup_{S\in R_n} R_{n+1}^{(S)}$. □

Proposition 3.21. *Let* $S_1\cup\{x_1\}, S_2\cup\{x_2\} \in \bigcup_{S\in R_n} R_{n+1}^{(S)}$, *where* $U_1 = \{x_1\}$ *in the partition* $I_{S_1\cup\{x_1\}}\backslash\backslash S_1 \cup \{x_1\}$ *and* $U_1 = \{x_2\}$ *in the partition* $I_{S_2\cup\{x_2\}}\backslash\backslash S_2 \cup \{x_2\}$. *Then* $S_1^g \cup \{x_1\}^g = S_2 \cup \{x_2\}$ *only if* $S_1^g = S_2$.

Proof Suppose $S_1^g \cup \{x_1\}^g = S_2 \cup \{x_2\}$, then the equality of the singletons $x_1^g = x_2$ follows from the equality of the partitions $I_{S_1^g\cup\{x_1\}^g}\backslash\backslash S_1^g \cup \{x_1\}^g = I_{S_2\cup\{x_2\}}\backslash\backslash S_2 \cup \{x_2\}$. Hence, $S_1^g = S_2$. □

Proposition 3.21 implies that an $(n+1,3^-)$-arc $S\cup\{x_1\}$ in $\bigcup_{S\in R_n} R_{n+1}^{(S)}$ is only projectively equivalent to an $(n+1,3^-)$-arc in $\bigcup_{S\in R_n} R_{n+1}^{(S)}$.

That is, if R_n is split into a number of disjoint subsets, then each subset generates a set of $(n+1,3^-)$-arcs with singletons that are projectively inequivalent to all $(n+1,3^-)$-arcs with singletons that are generated by other subsets. Hence, multiple copies of the algorithm may operate on different subsets of R_n simultaneous, without any further work to remove projectively equivalent $(n+1,3^-)$-arcs with singletons.

All $(n+1,3^-)$-arcs that do not possess a singleton are handled separately, but these are sparse.

Remark 3.22. To make the classification of all classes of projectively equivalent $(n,3^-)$-arcs in $PG(2,q)$ practical for $q \geq 13$, this improvement to the algorithm is necessary as it will allow multiple copies of the algorithm to run on multiple machines.

Note 3.23. If the aim is to determine $m_3(2,q)$ the size of the largest $(n,3^-)$-arc in $PG(2,q)$ and not classification, one possible speed improvement is to construct $\bigcup_{S\in R_n} R_{n+1}^{(S)}$ as the set containing every $(n+1,3^-)$-arc $S\cup\{x\}$, with singleton $U_1 = \{x\}$ that is constructed from the $(n,3^-)$-arc S of R_n, for $n > N$. If every $(n+1,3^-)$-arc without a singleton is also passed into $\bigcup_{S\in R_n} R_{n+1}^{(S)}$, for $n > N$, then the need to determine the canonical form is completely removed. For sufficiently large N the increase in the magnitude of $\bigcup_{S\in R_n} R_{n+1}^{(S)}$ is small.

Table 3.1: Spectrum of complete $(n, 3)$-arcs

13	14	15	16	17	18	19	20	21

Table 3.2: Number of inequivalent $(n, 3)$-arcs

n	inequivalent complete $(n, 3)$-arcs
13	5
14	146
15	71 584
16	1 573 677
17	2 082 781
18	259 585
19	4 176
20	15
21	2

n	inequivalent incomplete $(n, 3)$-arcs
5	3
6	38
7	543
8	6 743
9	70 550
10	574 775
11	3 520 994
12	15 291 641
13	44 020 755

n	inequivalent incomplete $(n, 3)$-arcs
14	76 935 881
15	73 086 254
16	31 342 655
17	3 801 624
18	74 273
19	291
20	2

3.3 The classification

Table 3.1 gives the spectrum of sizes of complete $(n, 3)$-arcs in $PG(2, 11)$. Table 3.2 gives the number of classes of projectively equivalent $(n, 3)$-arcs in $PG(2, 11)$.

In Table 3.3, the classes of projectively equivalent complete $(n, 3)$-arcs in $PG(2, 11)$ are further classified according to their automorphism groups. An entry of the form $\mathbf{G} : \alpha$ indicates that there are α classes of projectively equivalent $(n, 3)$-arcs with automorphism group isomorphic to $\mathbf{G}$.

Note 3.24. In Chapter 5, the classes of projectively equivalent incomplete $(n, 3)$-arcs in $PG(2, 11)$ are further classified according to their automorphism groups. This is achieved using a different and much faster method as described fully in Chapter 5.

To determine the automorphism or stabilizer group of an $(n, 3)$-arc S, first calculate every projectivity $(\mathfrak{T}, g) \in PGL(3, q)$ that maps S to itself; that is $S^g = S$. This is achieved by finding every g that maps a 4-arc of S onto $\{e_1, e_2, e_3, e_4\}$ and then determining if $S^g = S$. The group of stabilizers of S consists of all such projectivities. If this group has order $i = 1, 2, 3, 5, 7, 11, 13, 15, 17, 19, 23$, then it is isomorphic to $\mathbf{Z}_i$. If the group has order $i = 4, 6, 8, 9, 10, 12, 14, 18, 20, 21, 22, 24$, then the group with which it is isomorphic is determined by the order of its elements. In Tables 3.4 to 3.16, an entry of the form 3,2 indicates that this group has 2 elements of order 3. If the ordering of elements in groups of order 16 is not unique, then these groups may be distinguished by identifying if the group is Abelian or non-Abelian or by the cardinality of the set $\{g^2 \mid g \in \mathbf{G}\}$.

There are two groups that are used in the classification of classes of projectively equivalent $(n, 3)$-arcs in $PG(2, 11)$ that are not in one of these tables, the first is $\mathbf{Z}_{19} \rtimes \mathbf{Z}_3$; this group

Table 3.3: Classification by automorphism group

$n = 13$	$\mathbf{Z}_2 : 1$	$\mathbf{Z}_6 : 1$	$\mathbf{S}_3 : 2$	$\mathbf{D}_5 : 1$
$n = 14$	$\mathbf{Z}_1 : 138$	$\mathbf{Z}_2 : 8$		
$n = 15$	$\mathbf{Z}_1 : 70\ 705$ $\mathbf{Z}_2 \times \mathbf{Z}_2 : 6$ $\mathbf{S}_4 : 2$	$\mathbf{Z}_2 : 794$ $\mathbf{Z}_6 : 2$	$\mathbf{Z}_3 : 56$ $\mathbf{S}_3 : 15$	$\mathbf{Z}_4 : 2$ $\mathbf{D}_5 : 2$
$n = 16$	$\mathbf{Z}_1 : 1\ 572\ 864$ $\mathbf{Z}_6 : 2$	$\mathbf{Z}_2 : 613$ $\mathbf{S}_3 : 1$	$\mathbf{Z}_3 : 196$	$\mathbf{Z}_2 \times \mathbf{Z}_2 : 1$
$n = 17$	$\mathbf{Z}_1 : 2\ 078\ 955$ $\mathbf{Z}_5 : 5$ $\mathbf{D}_5 : 3$	$\mathbf{Z}_2 : 3\ 782$ $\mathbf{Z}_8 : 1$	$\mathbf{Z}_4 : 9$ $\mathbf{D}_4 : 5$	$\mathbf{Z}_2 \times \mathbf{Z}_2 : 20$ $\mathbf{Q}_4 : 1$
$n = 18$	$\mathbf{Z}_1 : 259\ 174$ $\mathbf{Z}_2 \times \mathbf{Z}_2 : 1$ $\mathbf{S}_4 : 1$	$\mathbf{Z}_2 : 234$ $\mathbf{Z}_5 : 1$	$\mathbf{Z}_3 : 166$ $\mathbf{S}_3 : 3$	$\mathbf{Z}_4 : 4$ $\mathbf{A}_4 : 1$
$n = 19$	$\mathbf{Z}_1 : 4\ 055$ $\mathbf{Z}_2 \times \mathbf{Z}_2 : 5$	$\mathbf{Z}_2 : 76$ $\mathbf{S}_3 : 3$	$\mathbf{Z}_3 : 35$ $\mathbf{Z}_{19} \rtimes \mathbf{Z}_3 : 1$	$\mathbf{Z}_4 : 1$
$n = 20$	$\mathbf{Z}_1 : 13$	$\mathbf{Z}_2 : 2$		
$n = 21$	$\mathbf{Z}_7 \rtimes \mathbf{Z}_3 : 2$			

has one Abelian normal subgroup of order 19, nineteen Abelian non-normal subgroups of order 3 and one subgroup of order 1, the identity. The second is a group of order 60 that is described in Section 1.2.9.

Table 3.4: Groups of order 4

$\mathbf{Z}_4$ $\mathbf{Z}_2 \times \mathbf{Z}_2$	1,1 1,1	2,1 2,3	4,2

Table 3.5: Groups of order 6

$\mathbf{Z}_6$ $\mathbf{S}_3$	1,1 1,1	2,1 2,3	3,2 3,2	6,2

Table 3.6: Groups of order 8

$\mathbf{Z}_8$	1,1	2,1	3,2	8,4
$\mathbf{Z}_2 \times \mathbf{Z}_4$	1,1	2,3	4,4	
$(\mathbf{Z}_2)^3$	1,1	2,7		
$\mathbf{D}_4$	1,1	2,5	4,2	
$\mathbf{Q}_4$	1,1	2,1	4,6	

Table 3.7: Groups of order 9

$\mathbf{Z}_9$	1,1	3,2	9,6
$\mathbf{Z}_3 \times \mathbf{Z}_3$	1,1	3,8	

Table 3.8: Groups of order 10

$\mathbf{Z}_{10}$	1,1	2,1	5,4	10,4
$\mathbf{D}_5$	1,1	2,5	5,4	

Table 3.9: Groups of order 12

$\mathbf{Z}_{12}$	1,1	2,1	3,2	4,2	6,2	12,4
$\mathbf{Z}_6 \times \mathbf{Z}_2$	1,1	2,3	3,2	6,6		
$\mathbf{D}_6$	1,1	2,7	3,2	6,2		
$\mathbf{Q}_6$	1,1	2,1	3,2	4,6	6,2	
$\mathbf{A}_4$	1,1	2,3	3,8			

Table 3.10: Groups of order 14

$\mathbf{Z}_{14}$	1,1	2,1	7,6	14,6
$\mathbf{D}_7$	1,1	2,7	7,6	

Table 3.11: Groups of order 16

$\mathbf{Z}_{16}$	1,1	2,1	4,2	8,4	16,8		
$\mathbf{Z}_8 \times \mathbf{Z}_2$	1,1	2,3	4,4	8,8		Abelian	
$\mathbf{Z}_4 \times \mathbf{Z}_4$	1,1	2,3	4,12			Abelian	
$\mathbf{Z}_4 \times (\mathbf{Z}_2)^2$	1,1	2,7	4,8			Abelian	
$(\mathbf{Z}_2)^4$	1,1	2,15					
$\mathbf{D}_8$	1,1	2,9	4,2	8,4			
$\mathbf{Q}_8$	1,1	2,1	4,10	8,4			
$\mathbf{D}_4 \times \mathbf{Z}_2$	1,1	2,11	4,4				
$\mathbf{Q}_4 \times \mathbf{Z}_2$	1,1	2,3	4,12			non-Abelian	$\lvert\{g^2 \mid g \in \mathbf{G}\}\rvert = 2$
$\mathbf{Z}_8 \rtimes \mathbf{Z}_2$, $\mathbf{H}_1$	1,1	2,3	4,4	8,8		non-Abelian	
$\mathbf{Z}_8 \rtimes \mathbf{Z}_2$, $\mathbf{H}_2$	1,1	2,5	4,6	8,4			
$\mathbf{Z}_4 \rtimes \mathbf{Z}_2$	1,1	2,3	4,12			non-Abelian	$\lvert\{g^2 \mid g \in \mathbf{G}\}\rvert = 3$
$(\mathbf{Z}_4 \times \mathbf{Z}_2) \rtimes \mathbf{Z}_2$, $\mathbf{H}_3$	1,1	2,7	4,8			non-Abelian	$\lvert\{g^2 \mid g \in \mathbf{G}\}\rvert = 2$
$(\mathbf{Z}_4 \times \mathbf{Z}_2) \rtimes \mathbf{Z}_2$, $\mathbf{H}_4$	1,1	2,7	4,8			non-Abelian	$\lvert\{g^2 \mid g \in \mathbf{G}\}\rvert = 3$

Table 3.12: Groups of order 18

$\mathbf{Z}_{18}$	1,1	2,1	3,2	6,2	9,6	18,6
$\mathbf{Z}_6 \times \mathbf{Z}_3$	1,1	2,1	3,8	6,8		
$\mathbf{D}_9$	1,1	2,9	3,2	9,6		
$\mathbf{S}_3 \times \mathbf{Z}_3$	1,1	2,3	3,8	6,6		
$(\mathbf{Z}_3 \times \mathbf{Z}_3) \rtimes \mathbf{Z}_2$	1,1	2,9	3,8			

Table 3.13: Groups of order 20

$\mathbf{Z}_{20}$	1,1	2,1	4,2	5,4	10,5	20,7
$\mathbf{Z}_{10} \times \mathbf{Z}_2$	1,1	2,3	5,4	10,12		
$\mathbf{D}_{10}$	1,1	2,11	5,4	10,4		
$\mathbf{Q}_{10}$	1,1	2,1	4,10	5,4	10,4	
$\mathbf{Z}_5 \rtimes \mathbf{Z}_4$	1,1	2,5	4,10	5,4		

Table 3.14: Groups of order 21

$\mathbf{Z}_{21}$	1,1	3,2	7,6	21,12
$\mathbf{Z}_7 \rtimes \mathbf{Z}_3$	1,1	3,14	7,6	

Table 3.15: Groups of order 22

$\mathbf{Z}_{22}$	1,1	2,1	11,10	22,10
$\mathbf{D}_{11}$	1,1	2,11	11,10	

Table 3.16: Groups of order 24

$\mathbf{Z}_{24}$	1,1	2,1	3,2	4,2	6,2	8,4	12,4	24,8
$\mathbf{Z}_{12} \times \mathbf{Z}_2$	1,1	2,3	3,2	4,4	6,6	12,8		
$\mathbf{Z}_6 \times (\mathbf{Z}_2)^2$	1,1	2,7	3,2	6,14				
$\mathbf{S}_4$	1,1	2,9	3,8	4,6				
$\mathbf{D}_{12}$	1,1	2,13	3,2	4,2	6,2	12,4		
$\mathbf{Q}_{12}$	1,1	2,1	3,2	4,14	6,2	12,4		
$\mathbf{D}_6 \times \mathbf{Z}_2$	1,1	2,15	3,2	6,6				
$\mathbf{A}_4 \times \mathbf{Z}_2$	1,1	2,7	3,8	6,8				
$\mathbf{Q}_6 \times \mathbf{Z}_3$	1,1	2,3	4,12	6,6				
$\mathbf{D}_4 \times \mathbf{Z}_3$	1,1	2,5	3,2	4,2	6,10	12,4		
$\mathbf{Q}_4 \times \mathbf{Z}_3$	1,1	2,1	3,2	4,6	6,2	12,12		
$\mathbf{S}_3 \times \mathbf{Z}_4$	1,1	2,7	3,2	4,8	6,2	12,4		
$\mathbf{SL}(2,3)$	1,1	2,1	3,8	4,6	6,8			
$\mathbf{Z}_3 \rtimes \mathbf{Z}_8$	1,1	2,1	3,2	4,2	6,2	8,12	12,4	
$\mathbf{Z}_4 \rtimes \mathbf{D}_4$	1,1	2,9	3,2	4,6	6,6			

Chapter 4

The Largest Complete $(n, 4)$-arcs in $PG(2, 11)$

Given the classification of all $(n, 3)$-arcs up to projective equivalence in $PG(2, 11)$, it will be established that no $(n, 3)$-arc may be extended to a $(33, 4)$-arc. By the existence of complete $(32, 4)$-arcs, the size of the largest $(n, 4)$-arc in $PG(2, 11)$ is 32.

Let S_k denote the $(n + k, 4)$-arc $S \cup \{x_0\} \cup \cdots \cup \{x_{k-1}\}$, where S is an $(n, 3)$-arc and $x_0, \ldots, x_{k-1}$ are k suitably chosen points; that is, S_k is an extension of the $(n, 3)$-arc S.

Proposition 4.1. *The only points that need to be considered in the extension of S to S_k are those points that are on at least one trisecant of S.*

Proof If S is complete, then every point $x \notin S$ is on at least one trisecant of S. If S is not complete and $x \notin S$ is a point that is not on a trisecant of S, then $S \cup \{x\}$ is an $(n+1, 3)$-arc. However, all the extensions of $(n + 1, 3)$-arcs are considered separately. □

Proposition 4.2. *If it is possible to extend an $(n, 3)$-arc S to a $(33, 4)$-arc in $PG(2, 11)$, then $n \geq 12$.*

Proof If it is possible to extend S to the $(33, 4)$-arc $S_{33-n} = S \cup \{x_0\} \cup \cdots \cup \{x_{33-n-1}\}$, then the $33 - n$ points $x_i \in S_{33-n} \backslash S$ are selected from unique trisecants of S. Therefore S has at least $33 - n$ trisecants. Substituting $r = 3$ and $\tau_3 = 33 - n$ into Equation 1.5 gives,

$$2\tau_2 = n^2 + 5n - 198.$$

For $n \in \overline{\mathbf{N}}$, the value of τ_2 is non-negative if and only if $n \geq 12$. □

Let $q_{S_k}(x)$ denote the number of 4-secants of $S_k = S \cup \{x_0\} \cup \cdots \cup \{x_{k-1}\}$ through the point x. One limitation on the points $x_i \in S_k \backslash S$ is that a new point x_k may only be added to S_k if $q_{S_k}(x_k) = 0$.

4.1 The algorithm

For every class of projectively equivalent $(n, 3)$-arcs in $PG(2, 11)$, where $n \geq 12$, consider a representative S. The algorithm determines if S may be extended to a complete $(33, 4)$-arc by considering every possible extension $S \cup \{x_0\} \cup \cdots \cup \{x_{33-n-1}\}$, where the points $x_0, \ldots, x_{33-n-1}$ are on at least one trisecant of S. The point x_i is not on a 4-secant of $S \cup \{x_0\} \cup \cdots \cup \{x_{i-1}\}$ and the ordering of the points follows the appropriate structure.

Every extension of an $(n, 3)$-arc S that could possibly be extended to a $(33, 4)$-arc will be considered ensuring an exhaustive search. For speed improvements, an ordering is imposed on the points that are used to extend S; this does not alter the exhaustive nature of the search.

4.1.1 Ordering of points

For an $(n, 3)$-arc S, only points from $PG(2, 11)\backslash S$ that are on at least one trisecant of S are to be used in the extension of S. A table is constructed containing one entry for each point of $PG(2, 11)\backslash S$ that is on at least one trisecant of S.

Construction 4.3. Let S have t trisecants. Then a table is created with t rows, where every row consists of the nine points of a unique trisecant of S that are not in S.

For rows $0, \ldots, t-1$ in order, all but the first instances of every point are removed and if after this process a row is left empty, then the row is also removed. This removal of points leaves a table containing one entry for each point of $PG(2, q)\backslash S$ that is on at least one trisecant of S. At most one point from a row may be added to an $(n + k, 4)$-arc extended from S.

Removing points in this way ensures that the first rows $0, \ldots$ contain a much higher number of points than any of the last rows $\ldots, t-1$. Rows are rearranged as necessary so as to maximize this property.

The points represented on this table are ordered according to their row.

Construction 4.4. The points on this table are ordered according to their row in descending order. That is, for $S \cup \{x_0\} \cup \cdots \cup \{x_{33-n-1}\}$, if r_i denotes the row containing x_i the $(i+1)$-th point to be added to S in this sequence, then $x_0 < x_1 < \cdots < x_{33-n-2} < x_{33-n-1}$ if and only if $r_0 > r_1 > \cdots > r_{33-n-2} > r_{33-n-1}$. No ordering of points within the rows is needed, as no two points may be added to S from the same row.

As the points $x_0, \ldots, x_{33-n-1}$ are added to S so as to ensure that $x_0 < x_1 < \cdots < x_{33-n-1}$, with regard to this new ordering, the $(i+1)$-th point to be added to S may only be selected from a limited number of rows. The $(i + 1)$-th point may only be selected from the rows $0, \ldots, r_{i-1} - 1$, where r_{i-1} denotes the row from which the i-th point is selected. Further, the $(i + 1)$-th point is not selected from the rows $0, \ldots, ((33 - n) - 1) - (i + 1)$, since the points $x_{i+1}, \ldots, x_{(33-n)-1}$, of which there are $((33 - n) - 1) - (i + 1)$ must be selected from these rows.

Note 4.5. A further advantage of selecting points from rows in descending order is that points are being selected from rows containing very few points. The points from the rows containing the most points are the last to be added to S; hence, many of them are incident with 4-secants of $S \cup \{x_0\} \cup \cdots \cup \{x_i\}$ and as such they are removed from consideration.

Example 4.6. Consider $S = \{0, 1, 6, 12, 13, 23, 25, 35, 37, 47, 50, 62, 66, 72, 84, 110\}$, a complete $(16, 3)$-arc in $PG(2, 11)$. To extend S to a $(33, 4)$-arc, 17 points $x_0, \ldots, x_{16}$ need to be added to S. Table 4.1 is produced for S and it contains one entry for every point of $PG(2, 11)\backslash S$ that is on at least one trisecant of S. The points in a row of Table 4.1 are selected from a unique trisecant of S and only the first instances of every point are shown. Hence, only one point from a row may be added to S. The $(16, 3)$-arc S has 29 not 27 trisecants, but 2 of these trisecants consist of points that are incident with other trisecants and so would be blank; hence, they are removed. The ordering of the points in Table 4.1 is $103 < 73 < 114 < 128 < \{92, 129\} < \{115, 130\} < \ldots$.

The number (i) indicates the lowest value row from which the $(i+1)$-th point to be added to S, x_i, may be selected. For example, the 7-th point to be added to S, x_6, may only be selected from rows ≥ 10 and $\leq r_5$, the row containing the 6-th point to be added to S.

Table 4.1: Point selections

row 0	7	8	9	10	11	2	3	4	5	(16)
row 1	18	19	20	21	22	14	15	16	17	(15)
row 2	29	30	31	32	33	24	26	27	28	(14)
row 3	40	41	42	43	44	34	36	38	39	(13)
row 4	51	52	53	54	55	45	46	48	49	(12)
row 5	63	64	65	56	57	58	59	60	61	(11)
row 6	81	98	104	121	127	75				(10)
row 7	82	90	109	117	125	74				(9)
row 8	87	93	116	122	70					(8)
row 9	78	95	101	118	124					(7)
row 10	94	119	126	69						(6)
row 11	86	96	106	76						(5)
row 12	79	112	123	68						(4)
row 13	88	99	132	77						(3)
row 14	102	111	131							(2)
row 15	89	100	67							(1)
row 16	80	91	113							(0)
row 17	83	105								
row 18	108	120								
row 19	85	97								
row 20	107	71								
row 21	115	130								
row 22	92	129								
row 23	128									
row 24	114									
row 25	73									
row 26	103									

4.2 Results

The search showed the non-existence of $(33, 4)$-arcs in $PG(2, 11)$; hence, $m_4(2, 11) = 32$. A search for $(32, 4)$-arcs in $PG(2, 11)$ extended from complete $(n, 3)$-arcs produced four projectively inequivalent $(32, 4)$-arcs, with representatives from each equivalence class displayed in Table 4.2 and described below.

Table 4.2: Projectively inequivalent $(32, 4)$-arcs in $PG(2, 11)$

$0=(0,0,1)$	$0=(0,0,1)$	$0=(0,0,1)$	$0=(0,0,1)$
$1=(0,1,-5)$	$1=(0,1,-5)$	$1=(0,1,-5)$	$1=(0,1,-5)$
$2=(0,1,-4)$	$2=(0,1,-4)$	$2=(0,1,-4)$	$2=(0,1,-4)$
$6=(0,1,0)$	$6=(0,1,0)$	$6=(0,1,0)$	$6=(0,1,0)$
$12=(1,-5,-5)$	$12=(1,-5,-5)$	$12=(1,-5,-5)$	$17=(1,-5,0)$
$17=(1,-5,0)$	$13=(1,-5,-4)$	$19=(1,-5,2)$	$18=(1,-5,1)$
$19=(1,-5,2)$	$19=(1,-5,2)$	$22=(1,-5,5)$	$22=(1,-5,5)$
$32=(1,-4,4)$	$29=(1,-4,1)$	$24=(1,-4,-4)$	$24=(1,-4,-4)$
$44=(1,-3,5)$	$31=(1,-4,3)$	$39=(1,-3,0)$	$26=(1,-4,-2)$
$47=(1,-2,-3)$	$32=(1,-4,4)$	$41=(1,-3,2)$	$28=(1,-4,0)$
$49=(1,-2,-1)$	$39=(1,-3,0)$	$44=(1,-3,5)$	$36=(1,-3,-3)$
$53=(1,-2,3)$	$41=(1,-3,2)$	$50=(1,-2,0)$	$37=(1,-3,-2)$
$56=(1,-1,-5)$	$44=(1,-3,5)$	$51=(1,-2,1)$	$44=(1,-3,5)$
$62=(1,-1,1)$	$45=(1,-2,-5)$	$52=(1,-2,2)$	$45=(1,-2,-5)$
$64=(1,-1,3)$	$49=(1,-2,-1)$	$57=(1,-1,-4)$	$49=(1,-2,-1)$
$69=(1,0,-3)$	$51=(1,-2,1)$	$64=(1,-1,3)$	$54=(1,-2,4)$
$72=(1,0,0)$	$56=(1,-1,-5)$	$65=(1,-1,4)$	$59=(1,-1,-2)$
$77=(1,0,5)$	$60=(1,-1,-1)$	$69=(1,0,-3)$	$64=(1,-1,3)$
$84=(1,1,1)$	$65=(1,-1,4)$	$72=(1,0,0)$	$65=(1,-1,4)$
$85=(1,1,2)$	$72=(1,0,0)$	$73=(1,0,1)$	$67=(1,0,-5)$
$88=(1,1,5)$	$75=(1,0,3)$	$82=(1,1,-1)$	$69=(1,0,-3)$
$95=(1,2,1)$	$77=(1,0,5)$	$84=(1,1,1)$	$72=(1,0,0)$
$97=(1,2,3)$	$84=(1,1,1)$	$86=(1,1,3)$	$82=(1,1,-1)$
$98=(1,2,4)$	$85=(1,1,2)$	$100=(1,3,-5)$	$84=(1,1,1)$
$103=(1,3,-2)$	$87=(1,1,4)$	$101=(1,3,-4)$	$88=(1,1,5)$
$105=(1,3,0)$	$92=(1,2,-2)$	$109=(1,3,4)$	$89=(1,2,-5)$
$107=(1,3,2)$	$93=(1,2,-1)$	$111=(1,4,-5)$	$90=(1,2,-4)$
$114=(1,4,-2)$	$97=(1,2,3)$	$113=(1,4,-3)$	$97=(1,2,3)$
$120=(1,4,4)$	$101=(1,3,-4)$	$121=(1,4,5)$	$102=(1,3,-3)$
$122=(1,5,-5)$	$103=(1,3,-2)$	$124=(1,5,-3)$	$109=(1,3,4)$
$123=(1,5,-4)$	$123=(1,5,-4)$	$130=(1,5,3)$	$117=(1,4,1)$
$125=(1,5,-2)$	$125=(1,5,-2)$	$131=(1,5,4)$	$119=(1,4,3)$

As is stated in Definition 5.1, a $(32, 4)$-arc S will be said to have the form $(t_0, t_1, t_2, t_3, t_4)$ if it has exactly t_0 external lines, t_1 unisecants, t_2 bisecants, t_3 trisecants and t_4 4-secants. A point is said to have the form $(a_0, a_1, a_2, a_3, a_4)$ if it is incident with a_0 external lines, a_1 unisecants, a_2 bisecants, a_3 trisecants and a_4 4-secants.

S_1

The first complete $(32, 4)$-arc S_1 has the form $(20, 2, 16, 30, 65)$, with ten points of the form $(0, 0, 0, 5, 7)$, ten points of the form $(0, 0, 1, 3, 8)$, two points of the form $(0, 1, 1, 0, 10)$ and ten points of the form $(0, 0, 2, 1, 9)$. Its complement has twenty-five points of the form $(2, 0, 2, 4, 4)$, twenty points of the form $(2, 1, 1, 3, 5)$, ten points of the form $(3, 0, 1, 2, 6)$, twenty-five points of the form $(2, 0, 3, 2, 5)$, ten points of the form $(3, 0, 0, 4, 5)$, ten points of the form $(4, 0, 0, 0, 8)$ and one point of the form $(0, 2, 5, 0, 5)$.

S_2

The second complete $(32, 4)$-arc S_2 has the form $(10, 22, 16, 10, 75)$, with twelve points of the form $(0, 1, 1, 0, 10)$, ten points of the form $(0, 1, 0, 2, 9)$ and ten points of the form $(0, 0, 2, 1, 9)$. Its complement has ten points of the form $(0, 4, 2, 0, 6)$, ten points of the form $(2, 0, 3, 2, 5)$, twenty points of the form $(1, 3, 1, 1, 6)$, twenty-five points of the form $(2, 2, 1, 0, 7)$, ten points of the form $(1, 2, 3, 0, 6)$, five points of the form $(0, 2, 4, 2, 4)$, ten points of the form $(2, 2, 0, 2, 6)$, ten points of the form $(0, 4, 1, 2, 5)$ and one point of the form $(0, 2, 5, 0, 5)$.

S_3

The third complete $(32, 4)$-arc S_3 has the form $(10, 22, 16, 10, 75)$, with twelve points of the form $(0, 1, 1, 0, 10)$, ten points of the form $(0, 0, 2, 1, 9)$ and ten points of the form $(0, 1, 0, 2, 9)$. Its complement has fourty points of the form $(1, 3, 1, 1, 6)$, ten points of the form $(2, 2, 1, 0, 7)$, five points of the form $(2, 0, 4, 0, 6)$, five points of the form $(0, 4, 2, 0, 6)$, ten points of the form $(3, 1, 0, 1, 7)$, ten points of the form $(1, 2, 3, 0, 6)$, ten points of the form $(1, 1, 3, 3, 4)$ and one point of the form $(0, 2, 5, 0, 5)$.

S_4

The fourth complete $(32, 4)$-arc S_4 has the form $(10, 22, 16, 10, 75)$, with twelve points of the form $(0, 0, 1, 3, 8)$, eight points of the form $(0, 1, 1, 0, 10)$ and twelve points of the form $(0, 1, 0, 2, 9)$. Its complement has four points of the form $(3, 0, 1, 2, 6)$, twenty-four points of the form $(2, 2, 0, 2, 6)$, eight points of the form $(1, 2, 2, 2, 5)$, eight points of the form $(2, 1, 2, 1, 6)$, sixteen points of the form $(1, 3, 0, 3, 5)$, seven points of the form $(0, 4, 2, 0, 6)$, sixteen points of the form $(2, 2, 1, 0, 7)$, eight points of the form $(0, 4, 1, 2, 5)$, four points of the form $(2, 0, 2, 4, 4)$, four points of the form $(0, 2, 3, 4, 3)$ and two points of the form $(2, 0, 3, 2, 5)$.

Chapter 5

Symmetry

5.1 Introduction

In this chapter ideas of symmetry are constructed and defined for (n, r)-arcs in $PG(2, q)$. A notion of symmetry between points and lines with respect to some (n, r)-arc in $PG(2, q)$ is also defined.

The symmetry between points and lines with respect to each of the four $(32, 4)$-arcs in $PG(2, 11)$ is used to demonstrate that using this type of symmetry it is possible to discover the duals of these four $(32, 4)$-arcs.

Definition 5.1. An (n, r)-arc S in $PG(2, q)$ with t_0 external lines, t_1 unisecants, ..., t_r r-secants is said to have the *form* $(t_0, t_1, \ldots, t_r)$.

A point of $PG(2, q)\backslash S$ on a_0 external lines of S, a_1 unisecants of S, ..., a_r r-secants of S is said to have the *form* $(a_0, a_1, \ldots, a_r)$ *with respect to* S.

A point of S on s_1 unisecants of S, s_2 bisecants of S, ..., s_r r-secants of S is said to have the *form* $(0, s_1, s_2, \ldots, s_r)$ *with respect to* S.

Proposition 5.2. *No form is common to both points of S and points of $PG(2, q)\backslash S$.*

Proof Let a be a point of $PG(2, q)\backslash S$ with the form $(a_0, a_1, \ldots, a_r)$ and s be a point of S with the form $(0, s_1, s_2, \ldots, s_r)$. If

$$(a_0, a_1, \ldots, a_r) = (0, s_1, s_2, \ldots, s_r),$$

then Equation 1.9 becomes

$$\sum_{i=2}^{r} i s_i = n$$

and subtracting Equation 1.7 gives

$$\sum_{i=1}^{r} s_i = 1;$$

a contradiction to Equation 1.6. □

5.1.1 Construction

For an (n,r)-arc S in $PG(2,q)$, let there be N_a different forms of point in $PG(2,q)\backslash S$ and let there be N_s different forms of point in S. In $PG(2,q)\backslash S$ the forms of the points are $(a_0^{(i)}, a_1^{(i)}, \ldots, a_r^{(i)})$, for $i = 0, \ldots, N_a - 1$ and in S the forms of the points are $(0, s_1^{(i)}, \ldots, s_r^{(i)})$, for $i = 0, \ldots, N_s - 1$.

Let $L_1^{(j)}$ be the set consisting of every line that is incident with $n(a^{(i)}, j)$ points from the set $a^{(i)}$, for $i = 0, \ldots, N_a - 1$ and $n(s^{(i)}, j)$ points from the set $s^{(i)}$, for $i = 0, \ldots, N_s - 1$ and suppose that there are M_1 unique sets of lines. That is,

$$L_1^{(j)} = \{\ell \mid \ell = (\overbrace{a^{(0)}, \ldots, a^{(0)}}^{n(a^{(0)},j)}, \ldots, \overbrace{a^{(N_a-1)}, \ldots, a^{(N_a-1)}}^{n(a^{(N_a-1)},j)}, \overbrace{s^{(0)}, \ldots, s^{(0)}}^{n(s^{(0)},j)}, \ldots, \overbrace{s^{(N_s-1)}, \ldots, s^{(N_s-1)}}^{n(s^{(N_s-1)},j)})\},$$

for $j = 0, \ldots, M_1 - 1$.

Let $P_1^{(i)}$ be the set consisting of every point that is incident with $m(L_1^{(j)}, i)$ lines from the set $L_1^{(j)}$ and suppose that there are N_1 unique sets of points. That is,

$$P_1^{(i)} = \{x \mid x = \cup(\overbrace{L_1^{(0)}, \ldots, L_1^{(0)}}^{m(L_1^{(0)},i)}, \overbrace{L_1^{(1)}, \ldots, L_1^{(1)}}^{m(L_1^{(1)},i)}, \ldots, \overbrace{L_1^{(M_1-1)}, \ldots, L_1^{(M_1-1)}}^{m(L_1^{(M_1-1)},i)}\}),$$

for $i = 0, \ldots, N_1 - 1$.

If $M_1 \neq N_1$, then the sets $L_2^{(j)}$ and $P_2^{(i)}$, for $j = 0, \ldots, M_2 - 1$ and $i = 0, \ldots, N_2 - 1$, are constructed from the sets $L_1^{(j)}$ and $P_1^{(i)}$, for $j = 0, \ldots, M_1 - 1$ and $i = 0, \ldots, N_1 - 1$.

Let $L_2^{(j)}$ be the set consisting of every line that is incident with $n(P_1^{(i)}, j)$ points from the set $P_1^{(i)}$ and suppose that there are M_2 unique sets of lines. That is,

$$L_2^{(j)} = \{\ell \mid \ell = (\overbrace{P_1^{(0)}, \ldots, P_1^{(0)}}^{n(P_1^{(0)},j)}, \overbrace{P_1^{(1)}, \ldots, P_1^{(1)}}^{n(P_1^{(1)},j)}, \ldots, \overbrace{P_1^{(N_1-1)}, \ldots, P_1^{(N_1-1)}}^{n(P_1^{(N_1-1)},j)})\},$$

for $j = 0, \ldots, M_2 - 1$.

Let $P_2^{(i)}$ be the set consisting of every point that is incident with $m(L_2^{(j)}, i)$ lines from the set $L_2^{(j)}$ and suppose that there are N_2 unique sets of points. That is,

$$P_2^{(i)} = \{x \mid x = \cup(\overbrace{L_2^{(0)}, \ldots, L_2^{(0)}}^{m(L_2^{(0)},i)}, \overbrace{L_2^{(1)}, \ldots, L_2^{(1)}}^{m(L_2^{(1)},i)}, \ldots, \overbrace{L_2^{(M_2-1)}, \ldots, L_2^{(M_2-1)}}^{m(L_2^{(M_2-1)},i)})\},$$

for $i = 0, \ldots, N_2 - 1$.

If $M_2 \neq N_2$, then the sets $L_3^{(j)}$ and $P_3^{(i)}$, for $j = 0, \ldots, M_3 - 1$ and $i = 0, \ldots, N_3 - 1$, are constructed from the sets $L_2^{(j)}$ and $P_2^{(i)}$, for $j = 0, \ldots, M_2 - 1$ and $i = 0, \ldots, N_2 - 1$, in the same way that these sets are constructed from the sets $L_1^{(j)}$ and $P_1^{(i)}$, for $j = 0, \ldots, M_1 - 1$ and $i = 0, \ldots, N_1 - 1$. This process continues until $M_\Gamma = N_\Gamma$.

Note 5.3. If a set of points $P_\Gamma^{(i)}$ contains a point of S, then as $P_\Gamma^{(i)}$ is a more detailed description of the form of a set of points, $P_\Gamma^{(i)} \subset S$ by Proposition 5.2. Similarly, if a set of points $P_\Gamma^{(i)}$ contains a point of $PG(2,q)\backslash S$, then $P_\Gamma^{(i)} \subset PG(2,q)\backslash S$ by Proposition 5.2.

5.1.2 Definitions

Definition 5.4. Let S be an (n,r)-arc in $PG(2,q)$ and suppose that Γ is the smallest positive integer such that $M_\Gamma = N_\Gamma$, then S is called *weakly symmetrical of level* Γ *and size* M_Γ.

Notation 5.5. The order of the set $P_\Gamma^{(i)}$ is denoted $o(P_\Gamma^{(i)})$ and the order of the set $L_\Gamma^{(j)}$ is denoted $o(L_\Gamma^{(j)})$.

For an (n,r)-arc S in $PG(2,q)$, every point belongs to exactly one set of points and every line belongs to exactly one set of lines; hence,

$$\sum_{i=0}^{M_\Gamma-1} o(P_\Gamma^{(i)}) = \sum_{j=0}^{N_\Gamma-1} o(L_\Gamma^{(j)}) = q^2+q+1,$$

for every possible Γ, M_Γ and N_Γ.

Definition 5.6. Let S be a weakly symmetrical (n,r)-arc in $PG(2,q)$ of level Γ, let $L_\Gamma^{(j)}$ be the set of lines

$$L_\Gamma^{(j)} = \{\ell \mid \ell = (\overbrace{P_\Gamma^{(0)},\ldots,P_\Gamma^{(0)}}^{\lambda_0},\overbrace{P_\Gamma^{(1)},\ldots,P_\Gamma^{(1)}}^{\lambda_1},\ldots,\overbrace{P_\Gamma^{(\delta)},\ldots,P_\Gamma^{(\delta)}}^{\lambda_\delta})\}$$

and let $P_\Gamma^{(i)}$ be the set of points

$$P_\Gamma^{(i)} = \{x \mid x = \cup(\overbrace{L_\Gamma^{(0\sigma)},\ldots,L_\Gamma^{(0\sigma)}}^{\lambda_{0\sigma}},\overbrace{L_\Gamma^{(1\sigma)},\ldots,L_\Gamma^{(1\sigma)}}^{\lambda_{1\sigma}},\ldots,\overbrace{L_\Gamma^{(\delta\sigma)},\ldots,L_\Gamma^{(\delta\sigma)}}^{\lambda_{\delta\sigma}})\}$$

where σ is a permutation on $\overline{\mathbf{N}}_\delta$. If in addition $o(L_\Gamma^{(j)}) = o(P_\Gamma^{(i)})$, then the set of lines $L_\Gamma^{(j)}$ and the set of points $P_\Gamma^{(i)}$ are called *symmetrical of level* Γ *and order* $o(L_\Gamma^{(j)})$ *with respect to* S, this is denoted as $L_\Gamma^{(j)} \overset{S}{\leftrightarrow} P_\Gamma^{(i)}$.

Note 5.7. The symmetry between the points and lines with respect to an (n,r)-arc S in $PG(2,q)$ is used in this work to find the duals of the four $(32,4)$-arcs in $PG(2,11)$ and the duals of the q-arcs and $(q+1)$-arcs in $PG(2,q)$, for $q = 11,13,17,19$.

Definition 5.8. A weakly symmetrical (n,r)-arc S in $PG(2,q)$ of level Γ and size M_Γ is called *strongly symmetrical* if and only if there exists a permutation σ on $\overline{\mathbf{N}}_{M_\Gamma-1}$ such that

$$o(P_\Gamma^{(i)}) = o(L_\Gamma^{(i\sigma)}).$$

Hence, there exists an equal number of sets of points P_Γ of order Ω and sets of lines L_Γ of order Ω.

Notation 5.9. For a strongly symmetrical (n,r)-arc S in $PG(2,q)$ of level Γ, where Γ is the smallest positive integer for which S is strongly symmetrical, the spectrum

$$W(S,\Gamma) = \{o(P_\Gamma^{(0)}),\ldots,o(P_\Gamma^{(M_\Gamma-1)})\},$$

together with the sizes

$$\left|\{P_\Gamma^{(i)} \mid o(P_\Gamma^{(i)}) = y\}\right|,$$

for all $y \in W(S,\Gamma)$, are called the strong symmetrical properties of S.

Definition 5.10. A strongly symmetrical (n, r)-arc S in $PG(2, q)$ of level Γ and size M_Γ is called *completely symmetrical* if and only if there exists a permutation σ on $\overline{\mathbf{N}}_{M_\Gamma - 1}$ such that

$$o(P_\Gamma^{(i)}) = o(L_\Gamma^{(i\sigma)})$$

and

$$P_\Gamma^{(i)} \overset{S}{\leftrightarrow} L_\Gamma^{(i\sigma)},$$

for all $i \in \overline{\mathbf{N}}_{M_\Gamma - 1}$.

Notation 5.11. For a completely symmetrical (n, r)-arc S in $PG(2, q)$ the strong symmetrical properties combined with the symmetrical properties of sets of points and lines are called the complete symmetrical properties.

Note 5.12. It is possible for an (n, r)-arc S in $PG(2, q)$ to be strongly symmetrical of level Γ and size M_Γ and completely symmetrical, but not completely symmetrical of level Γ and size M_Γ. For example, in $PG(2, 11)$ the incomplete 11-arc is strongly symmetrical of level 1 but it is not completely symmetrical of level 1, it is however both strongly and completely symmetrical of level 2 with $M_1 = M_2$.

Conjecture 5.13. *Every* (n, r)-arc *in* $PG(2, q)$ *is weakly symmetrical. Every weakly symmetrical* (n, r)-arc *of level* Γ_1 *and size* M_{Γ_1} *in* $PG(2, q)$ *is strongly symmetrical of level* Γ_1 *and size* M_{Γ_1}. *Every strongly symmetrical* (n, r)-arc *of level* Γ_1 *and size* M_{Γ_1} *in* $PG(2, q)$ *is completely symmetrical of level* Γ_2 *and size* M_{Γ_2}, *where* $\Gamma_2 > \Gamma_1$ *and* $M_{\Gamma_2} \geq M_{\Gamma_1}$.

Note 5.14. All n-arcs in $PG(2, q)$, for $q = 11, 13, 17, 19$ are completely symmetrical of levels $1, 2$ or 3 and are of various sizes. All $(n, 3)$-arcs in $PG(2, 11)$ are at least strongly symmetrical of levels $1, 2$ or 3 and are of various sizes.

Note 5.15. The strong symmetrical properties of (n, r)-arcs in $PG(2, q)$ are used to classify the classes of projectively equivalent incomplete $(n, 3)$-arcs in $PG(2, 11)$. The classification of incomplete $(n, 3)$-arcs is no more complicated than the classification of complete $(n, 3)$-arcs, but there are more than 248 million classes of projectively equivalent incomplete $(n, 3)$-arcs and less than 4 million classes of projectively equivalent complete $(n, 3)$-arcs; making the classification method used for complete $(n, 3)$-arcs impractical for the incomplete $(n, 3)$-arcs. The new method of classification is described in detail in Chapter 6.

5.2 Dual

In this section S is assumed to be completely symmetrical.

Let S^* denote the dual of an (n, r)-arc S in $PG(2, q)$; that is, S^* is a set consisting of n lines in $PG(2, q)$ at most r of which are incident with any point of $PG(2, q)$.

Definition 5.16. A point of $PG(2, q)$ is called an i-point if and only if it is on exactly i lines of S^*.

A dual of an (n, r)-arc S^* with s_0 0-points, s_1 unipoints, s_2 bipoints, ..., s_r r-points is said to have the *form* $(s_0, s_1, \ldots, s_r)$.

A line through b_0 0-points, b_1 unipoints, b_2 bipoints, ..., b_r r-points is said to have the *form* $(b_0, b_1, \ldots, b_r)$ *with respect to* S^*.

Note 5.17. An (n, r)-arc S has the form $(t_0, t_1, \ldots, t_r)$ if and only if its dual has the form $(t_0, t_1, \ldots, t_r)$. There exists a point of $PG(2, q)$ that has the form $(a_0, a_1, \ldots, a_r)$ with respect to S if and only if there exists a line in $PG(2, q)$ that has the form $(a_0, a_1, \ldots, a_r)$ with respect to S^*.

Since S is completely symmetrical, it is possible to map the n points of S given by $\{P_\Gamma^{(i)} \mid P_\Gamma^{(i)} \subset S\}$ to a set of n lines $\{L_\Gamma^{(j)} \mid L_\Gamma^{(j)} \overset{S}{\leftrightarrow} P_\Gamma^{(i)} \subset S\}$.

As it may be possible to map S to more than one such set of lines, select n lines $\overline{S}$ to satisfy the conditions: 'the set of lines $\overline{S}$ consists of n lines at most 4 of which intersect at any point' and 'some point is on exactly 4 lines of $\overline{S}$'. If S is complete, then every line of $\overline{S}$ is incident with at least one 4-point. The dual of S is $\overline{S}$.

The 4 complete $(32, 4)$-arcs in $PG(2, 11)$ S_1, S_2, S_3 and S_4 are symmetrical and linked to their duals through this symmetry.

Example 5.18. For the first of the 4 complete $(32, 4)$-arcs S_1, the points of S_1 are labeled $s^{(0)}, \ldots, s^{(3)}$ to distinguish their form and the points of $PG(2, 11) \backslash S_1$ are labeled $a^{(0)}, \ldots, a^{(6)}$ to distinguish their form. The lines in $PG(2, 11)$ have the following incidence structure and quantities.

$$
\begin{aligned}
\left|\ell^{(0)} = \{\ell_k^{(0)} = (a^{(0)}, a^{(0)}, a^{(0)}, a^{(0)}, a^{(1)}, a^{(1)}, a^{(2)}, a^{(2)}, a^{(3)}, s^{(0)}, s^{(0)}, s^{(1)})\}\right| &= 10\\
\left|\ell^{(1)} = \{\ell_k^{(1)} = (a^{(0)}, a^{(0)}, a^{(1)}, a^{(2)}, a^{(3)}, a^{(3)}, a^{(4)}, a^{(5)}, s^{(0)}, s^{(1)}, s^{(2)}, s^{(3)})\}\right| &= 20\\
\left|\ell^{(2)} = \{\ell_k^{(2)} = (a^{(1)}, a^{(1)}, a^{(3)}, a^{(3)}, a^{(3)}, a^{(3)}, a^{(5)}, a^{(5)}, s^{(0)}, s^{(0)}, s^{(1)}, s^{(1)})\}\right| &= 10\\
\left|\ell^{(3)} = \{\ell_k^{(3)} = (a^{(0)}, a^{(0)}, a^{(0)}, a^{(1)}, a^{(1)}, a^{(3)}, a^{(3)}, a^{(4)}, a^{(4)}, s^{(0)}, s^{(0)}, s^{(3)})\}\right| &= 10\\
\left|\ell^{(4)} = \{\ell_k^{(4)} = (a^{(0)}, a^{(1)}, a^{(1)}, a^{(2)}, a^{(2)}, a^{(3)}, a^{(3)}, a^{(5)}, s^{(0)}, s^{(0)}, s^{(3)}, s^{(3)})\}\right| &= 10\\
\left|\ell^{(5)} = \{\ell_k^{(5)} = (a^{(0)}, a^{(0)}, a^{(0)}, a^{(1)}, a^{(1)}, a^{(3)}, a^{(3)}, a^{(4)}, a^{(4)}, s^{(0)}, s^{(1)}, s^{(1)})\}\right| &= 10\\
\left|\ell^{(6)} = \{\ell_k^{(6)} = (a^{(0)}, a^{(0)}, a^{(3)}, a^{(4)}, a^{(4)}, a^{(5)}, a^{(5)}, a^{(6)}, s^{(0)}, s^{(0)}, s^{(3)}, s^{(3)})\}\right| &= 5\\
\left|\ell^{(7)} = \{\ell_k^{(7)} = (a^{(1)}, a^{(1)}, a^{(2)}, a^{(2)}, a^{(3)}, a^{(3)}, a^{(4)}, a^{(4)}, s^{(1)}, s^{(1)}, s^{(3)}, s^{(3)})\}\right| &= 10\\
\left|\ell^{(8)} = \{\ell_k^{(8)} = (a^{(0)}, a^{(0)}, a^{(0)}, a^{(0)}, a^{(1)}, a^{(1)}, a^{(5)}, a^{(5)}, s^{(1)}, s^{(1)}, s^{(3)}, s^{(3)})\}\right| &= 10\\
\left|\ell^{(9)} = \{\ell_k^{(9)} = (a^{(0)}, a^{(0)}, a^{(0)}, a^{(2)}, a^{(2)}, a^{(3)}, a^{(3)}, a^{(3)}, a^{(3)}, a^{(6)}, s^{(1)}, s^{(1)})\}\right| &= 5\\
\left|\ell^{(10)} = \{\ell_k^{(10)} = (a^{(0)}, a^{(0)}, a^{(0)}, a^{(1)}, a^{(1)}, a^{(3)}, a^{(3)}, a^{(3)}, a^{(3)}, a^{(3)}, s^{(3)}, s^{(3)})\}\right| &= 10\\
\left|\ell^{(11)} = \{\ell_k^{(11)} = (a^{(0)}, a^{(0)}, a^{(0)}, a^{(1)}, a^{(1)}, a^{(2)}, a^{(2)}, a^{(3)}, a^{(3)}, a^{(4)}, a^{(5)}, a^{(5)})\}\right| &= 10\\
\left|\ell^{(12)} = \{\ell_k^{(12)} = (a^{(1)}, a^{(1)}, a^{(1)}, a^{(1)}, a^{(1)}, a^{(1)}, a^{(1)}, a^{(1)}, a^{(1)}, a^{(1)}, a^{(6)}, s^{(2)})\}\right| &= 2\\
\left|\ell^{(13)} = \{\ell_k^{(13)} = (a^{(0)}, a^{(0)}, a^{(1)}, a^{(1)}, a^{(2)}, a^{(3)}, a^{(3)}, a^{(3)}, a^{(4)}, a^{(4)}, a^{(5)}, a^{(5)})\}\right| &= 10\\
\left|\ell^{(14)} = \{\ell_k^{(14)} = (a^{(0)}, a^{(0)}, a^{(0)}, a^{(0)}, a^{(0)}, a^{(3)}, a^{(3)}, a^{(3)}, a^{(3)}, a^{(3)}, s^{(2)}, s^{(2)})\}\right| &= 1
\end{aligned}
$$

The sets of points of $PG(2,11)$ can now be expressed in terms of the sets of lines $\ell^{(j)}$ with which they are incident. Here, a $*$ indicates that $P^{*(i)} = P^{(i)} \subset S_1$, in particular $s^{(0)} = P^{(0)}$, $s^{(1)} = P^{(1)}$, $s^{(2)} = P^{(7)}$ and $s^{(3)} = P^{(10)}$.

$$
\begin{aligned}
\left|P^{*(0)} = \{P_k^{*(0)} = (\ell^{(0)}, \ell^{(0)}, \ell^{(1)}, \ell^{(1)}, \ell^{(2)}, \ell^{(2)}, \ell^{(3)}, \ell^{(3)}, \ell^{(4)}, \ell^{(4)}, \ell^{(5)}, \ell^{(6)})\}\right| &= 10 \\
\left|P^{*(1)} = \{P_k^{*(1)} = (\ell^{(0)}, \ell^{(1)}, \ell^{(1)}, \ell^{(2)}, \ell^{(2)}, \ell^{(5)}, \ell^{(5)}, \ell^{(7)}, \ell^{(7)}, \ell^{(8)}, \ell^{(8)}, \ell^{(9)})\}\right| &= 10 \\
\left|P^{(2)} = \{P_k^{(2)} = (\ell^{(0)}, \ell^{(0)}, \ell^{(1)}, \ell^{(1)}, \ell^{(5)}, \ell^{(5)}, \ell^{(6)}, \ell^{(8)}, \ell^{(10)}, \ell^{(10)}, \ell^{(11)}, \ell^{(11)})\}\right| &= 10 \\
\left|P^{(3)} = \{P_k^{(3)} = (\ell^{(0)}, \ell^{(1)}, \ell^{(2)}, \ell^{(3)}, \ell^{(4)}, \ell^{(5)}, \ell^{(7)}, \ell^{(8)}, \ell^{(10)}, \ell^{(11)}, \ell^{(12)}, \ell^{(13)})\}\right| &= 20 \\
\left|P^{(4)} = \{P_k^{(4)} = (\ell^{(0)}, \ell^{(0)}, \ell^{(1)}, \ell^{(1)}, \ell^{(4)}, \ell^{(4)}, \ell^{(7)}, \ell^{(7)}, \ell^{(9)}, \ell^{(11)}, \ell^{(11)}, \ell^{(13)})\}\right| &= 10 \\
\left|P^{(5)} = \{P_k^{(5)} = (\ell^{(0)}, \ell^{(0)}, \ell^{(1)}, \ell^{(1)}, \ell^{(3)}, \ell^{(3)}, \ell^{(8)}, \ell^{(8)}, \ell^{(9)}, \ell^{(10)}, \ell^{(13)}, \ell^{(13)})\}\right| &= 10 \\
\left|P^{(6)} = \{P_k^{(6)} = (\ell^{(0)}, \ell^{(0)}, \ell^{(2)}, \ell^{(2)}, \ell^{(6)}, \ell^{(7)}, \ell^{(7)}, \ell^{(10)}, \ell^{(10)}, \ell^{(13)}, \ell^{(13)}, \ell^{(14)})\}\right| &= 5 \\
\left|P^{*(7)} = \{P_k^{*(7)} = (\ell^{(1)}, \ell^{(1)}, \ell^{(1)}, \ell^{(1)}, \ell^{(1)}, \ell^{(1)}, \ell^{(1)}, \ell^{(1)}, \ell^{(1)}, \ell^{(1)}, \ell^{(12)}, \ell^{(14)})\}\right| &= 2 \\
\left|P^{(8)} = \{P_k^{(8)} = (\ell^{(1)}, \ell^{(1)}, \ell^{(2)}, \ell^{(2)}, \ell^{(3)}, \ell^{(3)}, \ell^{(7)}, \ell^{(9)}, \ell^{(10)}, \ell^{(10)}, \ell^{(11)}, \ell^{(11)})\}\right| &= 10 \\
\left|P^{(9)} = \{P_k^{(9)} = (\ell^{(1)}, \ell^{(1)}, \ell^{(2)}, \ell^{(4)}, \ell^{(4)}, \ell^{(5)}, \ell^{(5)}, \ell^{(9)}, \ell^{(10)}, \ell^{(10)}, \ell^{(13)}, \ell^{(13)})\}\right| &= 10 \\
\left|P^{*(10)} = \{P_k^{*(10)} = (\ell^{(1)}, \ell^{(1)}, \ell^{(3)}, \ell^{(4)}, \ell^{(4)}, \ell^{(6)}, \ell^{(7)}, \ell^{(7)}, \ell^{(8)}, \ell^{(8)}, \ell^{(10)}, \ell^{(10)})\}\right| &= 10 \\
\left|P^{(11)} = \{P_k^{(11)} = (\ell^{(1)}, \ell^{(1)}, \ell^{(3)}, \ell^{(3)}, \ell^{(5)}, \ell^{(5)}, \ell^{(6)}, \ell^{(7)}, \ell^{(7)}, \ell^{(11)}, \ell^{(13)}, \ell^{(13)})\}\right| &= 10 \\
\left|P^{(12)} = \{P_k^{(12)} = (\ell^{(1)}, \ell^{(1)}, \ell^{(2)}, \ell^{(2)}, \ell^{(4)}, \ell^{(6)}, \ell^{(8)}, \ell^{(8)}, \ell^{(11)}, \ell^{(11)}, \ell^{(13)}, \ell^{(13)})\}\right| &= 10 \\
\left|P^{(13)} = \{P_k^{(13)} = (\ell^{(3)}, \ell^{(3)}, \ell^{(4)}, \ell^{(4)}, \ell^{(5)}, \ell^{(5)}, \ell^{(8)}, \ell^{(8)}, \ell^{(9)}, \ell^{(11)}, \ell^{(11)}, \ell^{(14)})\}\right| &= 5 \\
\left|P^{(14)} = \{P_k^{(14)} = (\ell^{(6)}, \ell^{(6)}, \ell^{(6)}, \ell^{(6)}, \ell^{(6)}, \ell^{(9)}, \ell^{(9)}, \ell^{(9)}, \ell^{(9)}, \ell^{(9)}, \ell^{(12)}, \ell^{(12)})\}\right| &= 1
\end{aligned}
$$

The sets of lines of $PG(2,11)$ can now be expressed in terms of the sets of points $P^{(i)}$ with which they are incident. Here, a $*$ indicates that the line $L^{*(j)} \in \overline{S}_1$, the dual of S_1 and $\left|L^{(j)}\right| = \left|\ell^{(j)}\right|$.

$$
\begin{aligned}
L^{*(0)} &= \{L_k^{*(0)} = (P^{*(0)}, P^{*(0)}, P^{*(1)}, P^{(2)}, P^{(2)}, P^{(3)}, P^{(3)}, P^{(4)}, P^{(4)}, P^{(5)}, P^{(5)}, P^{(6)})\} \\
L^{(1)} &= \{L_k^{(1)} = (P^{*(0)}, P^{*(1)}, P^{(2)}, P^{(3)}, P^{(4)}, P^{(5)}, P^{*(7)}, P^{(8)}, P^{(9)}, P^{*(10)}, P^{(11)}, P^{(12)})\} \\
L^{(2)} &= \{L_k^{(2)} = (P^{*(0)}, P^{*(0)}, P^{*(1)}, P^{*(1)}, P^{(3)}, P^{(3)}, P^{(6)}, P^{(8)}, P^{(8)}, P^{(9)}, P^{(12)}, P^{(12)})\} \\
L^{*(3)} &= \{L_k^{*(3)} = (P^{*(0)}, P^{*(0)}, P^{(3)}, P^{(3)}, P^{(5)}, P^{(5)}, P^{(8)}, P^{(8)}, P^{*(10)}, P^{(11)}, P^{(11)}, P^{(13)})\} \\
L^{(4)} &= \{L_k^{(4)} = (P^{*(0)}, P^{*(0)}, P^{(3)}, P^{(3)}, P^{(4)}, P^{(4)}, P^{(9)}, P^{(9)}, P^{*(10)}, P^{*(10)}, P^{(12)}, P^{(13)})\} \\
L^{(5)} &= \{L_k^{(5)} = (P^{*(0)}, P^{*(1)}, P^{(1)}, P^{(2)}, P^{(2)}, P^{(3)}, P^{(3)}, P^{(9)}, P^{(9)}, P^{(11)}, P^{(11)}, P^{(13)})\} \\
L^{(6)} &= \{L_k^{(6)} = (P^{*(0)}, P^{*(0)}, P^{(2)}, P^{(2)}, P^{(6)}, P^{*(10)}, P^{*(10)}, P^{(11)}, P^{(11)}, P^{(12)}, P^{(12)}, P^{(14)})\} \\
L^{*(7)} &= \{L_k^{*(7)} = (P^{*(1)}, P^{*(1)}, P^{(3)}, P^{(3)}, P^{(4)}, P^{(4)}, P^{(6)}, P^{(8)}, P^{*(10)}, P^{*(10)}, P^{(11)}, P^{(11)})\}
\end{aligned}
$$

$$
\begin{aligned}
L^{(8)} &= \{L_k^{(8)} = (P^{*(1)}, P^{*(1)}, P^{(2)}, P^{(3)}, P^{(3)}, P^{(5)}, P^{(5)}, P^{*(10)}, P^{*(10)}, P^{(12)}, P^{(12)}, P^{(13)})\} \\
L^{(9)} &= \{L_k^{(9)} = (P^{*(1)}, P^{*(1)}, P^{(4)}, P^{(4)}, P^{(5)}, P^{(5)}, P^{(8)}, P^{(8)}, P^{(9)}, P^{(9)}, P^{(13)}, P^{(14)})\} \\
L^{(10)} &= \{L_k^{(10)} = (P^{(2)}, P^{(2)}, P^{(3)}, P^{(3)}, P^{(5)}, P^{(6)}, P^{(8)}, P^{(8)}, P^{(9)}, P^{(9)}, P^{*(10)}, P^{*(10)})\} \\
L^{(11)} &= \{L_k^{(11)} = (P^{(2)}, P^{(2)}, P^{(3)}, P^{(3)}, P^{(4)}, P^{(4)}, P^{(8)}, P^{(8)}, P^{(11)}, P^{(12)}, P^{(12)}, P^{(13)})\} \\
L^{*(12)} &= \{L_k^{*(12)} = (P^{(3)}, P^{(3)}, P^{(3)}, P^{(3)}, P^{(3)}, P^{(3)}, P^{(3)}, P^{(3)}, P^{(3)}, P^{(3)}, P^{*(7)}, P^{(14)})\} \\
L^{(13)} &= \{L_k^{(13)} = (P^{(3)}, P^{(3)}, P^{(4)}, P^{(5)}, P^{(5)}, P^{(6)}, P^{(9)}, P^{(9)}, P^{(11)}, P^{(11)}, P^{(12)}, P^{(12)})\} \\
L^{(14)} &= \{L_k^{(14)} = (P^{(6)}, P^{(6)}, P^{(6)}, P^{(6)}, P^{(6)}, P^{*(7)}, P^{*(7)}, P^{(13)}, P^{(13)}, P^{(13)}, P^{(13)}, P^{(13)})\}
\end{aligned}
$$

The complete symmetrical properties of S_1 in $PG(2,11)$ can be described as follows. For the points of S_1,

$$\left|P^{(0)} \overset{S}{\leftrightarrow} L^{(7)}\right| = \left|P^{(1)} \overset{S}{\leftrightarrow} L^{(3)}\right| = 10,$$

$$\left|P^{(7)} \overset{S}{\leftrightarrow} L^{(12)}\right| = 2, \ \left|P^{(10)} \overset{S}{\leftrightarrow} L^{(0)}\right| = 10.$$

For the points of $PG(2,11)\backslash S_1$,

$$\left|P^{(3)} \overset{S}{\leftrightarrow} L^{(1)}\right| = 20,$$

$$\left|P^{(2)} \overset{S}{\leftrightarrow} L^{(10)}\right| = \left|P^{(4)} \overset{S}{\leftrightarrow} L^{(8)}\right| = 10,$$

$$\left|P^{(5)} \overset{S}{\leftrightarrow} L^{(4)}\right| = \left|P^{(8)} \overset{S}{\leftrightarrow} L^{(5)}\right| = 10,$$

$$\left|P^{(6)} \overset{S}{\leftrightarrow} L^{(6)}\right| = \left|P^{(13)} \overset{S}{\leftrightarrow} L^{(9)}\right| = 5,$$

$$\left|P^{(9)} \overset{S}{\leftrightarrow} L^{(11)}\right| = \left|P^{(11)} \overset{S}{\leftrightarrow} L^{(2)}\right| = \left|P^{(12)} \overset{S}{\leftrightarrow} L^{(13)}\right| = 10,$$

$$\left|P^{(14)} \overset{S}{\leftrightarrow} L^{(14)}\right| = 1.$$

5.2.1 The duals of the complete $(32,4)$-arcs in $PG(2,11)$

Here, the forms of the duals of the complete $(32,4)$-arcs S_1, S_2, S_3 and S_4 in $PG(2,11)$ are described.

The dual of S_1

The complete $(32,4)$-arc S_1 is completely symmetrical. Link the set of points $P^{(0)}$ with the set of lines $L^{(7)}$, the set of points $P^{(1)}$ with the set of lines $L^{(3)}$, the set of points $P^{(7)}$ with the set of lines $L^{(12)}$ and the set of points $P^{(10)}$ with the set of lines $L^{(0)}$. Then $\overline{S}_1 = L^{(0)} \cup L^{(3)} \cup L^{(7)} \cup L^{(12)}$ is the dual of S_1 and it contains the lines:

$$
\begin{aligned}
\{(0,0,1) + \alpha(0,1,1) : \alpha \in F_{11}\} \cup (0,1,1) &\in L^{(0)} \\
\{(0,0,1) + \alpha(1,3,1) : \alpha \in F_{11}\} \cup (1,3,1) &\in L^{(3)} \\
\{(0,0,1) + \alpha(1,-1,1) : \alpha \in F_{11}\} \cup (1,-1,1) &\in L^{(3)} \\
\{(0,0,1) + \alpha(1,2,1) : \alpha \in F_{11}\} \cup (1,2,1) &\in L^{(0)}
\end{aligned}
$$

$$\begin{aligned}
\{(0,1,-5)+\alpha(1,1,-1):\alpha\in F_{11}\}\cup(1,1,-1) &\in L^{(7)}\\
\{(0,1,-5)+\alpha(1,1,0):\alpha\in F_{11}\}\cup(1,1,0) &\in L^{(7)}\\
\{(0,1,-4)+\alpha(1,1,-3):\alpha\in F_{11}\}\cup(1,1,-3) &\in L^{(0)}\\
\{(0,1,-3)+\alpha(1,1,-1):\alpha\in F_{11}\}\cup(1,1,-1) &\in L^{(12)}\\
\{(0,1,-3)+\alpha(1,1,0):\alpha\in F_{11}\}\cup(1,1,0) &\in L^{(7)}\\
\{(0,1,-3)+\alpha(1,1,1):\alpha\in F_{11}\}\cup(1,1,1) &\in L^{(3)}\\
\{(0,1,-2)+\alpha(1,1,-2):\alpha\in F_{11}\}\cup(1,1,-2) &\in L^{(7)}\\
\{(0,1,-2)+\alpha(1,1,-1):\alpha\in F_{11}\}\cup(1,1,-1) &\in L^{(0)}\\
\{(0,1,-2)+\alpha(1,1,1):\alpha\in F_{11}\}\cup(1,1,1) &\in L^{(7)}\\
\{(0,1,-1)+\alpha(1,1,4):\alpha\in F_{11}\}\cup(1,1,4) &\in L^{(12)}\\
\{(0,1,-1)+\alpha(1,1,-5):\alpha\in F_{11}\}\cup(1,1,-5) &\in L^{(7)}\\
\{(0,1,-1)+\alpha(1,1,-3):\alpha\in F_{11}\}\cup(1,1,-3) &\in L^{(3)}\\
\{(0,1,0)+\alpha(1,1,0):\alpha\in F_{11}\}\cup(1,1,0) &\in L^{(0)}\\
\{(0,1,0)+\alpha(1,1,3):\alpha\in F_{11}\}\cup(1,1,3) &\in L^{(3)}\\
\{(0,1,0)+\alpha(1,1,4):\alpha\in F_{11}\}\cup(1,1,4) &\in L^{(3)}\\
\{(0,1,1)+\alpha(1,1,3):\alpha\in F_{11}\}\cup(1,1,3) &\in L^{(3)}\\
\{(0,1,1)+\alpha(1,1,-3):\alpha\in F_{11}\}\cup(1,1,-3) &\in L^{(0)}\\
\{(0,1,1)+\alpha(1,1,-1):\alpha\in F_{11}\}\cup(1,1,-1) &\in L^{(3)}\\
\{(0,1,2)+\alpha(1,1,4):\alpha\in F_{11}\}\cup(1,1,4) &\in L^{(0)}\\
\{(0,1,3)+\alpha(1,1,-5):\alpha\in F_{11}\}\cup(1,1,-5) &\in L^{(3)}\\
\{(0,1,3)+\alpha(1,1,-3):\alpha\in F_{11}\}\cup(1,1,-3) &\in L^{(3)}\\
\{(0,1,3)+\alpha(1,1,-2):\alpha\in F_{11}\}\cup(1,1,-2) &\in L^{(0)}\\
\{(0,1,4)+\alpha(1,1,-2):\alpha\in F_{11}\}\cup(1,1,-2) &\in L^{(0)}\\
\{(0,1,4)+\alpha(1,1,4):\alpha\in F_{11}\}\cup(1,1,4) &\in L^{(7)}\\
\{(0,1,4)+\alpha(1,1,-5):\alpha\in F_{11}\}\cup(1,1,-5) &\in L^{(7)}\\
\{(0,1,5)+\alpha(1,1,-2):\alpha\in F_{11}\}\cup(1,1,-2) &\in L^{(7)}\\
\{(0,1,5)+\alpha(1,1,0):\alpha\in F_{11}\}\cup(1,1,0) &\in L^{(0)}\\
\{(0,1,5)+\alpha(1,1,1):\alpha\in F_{11}\}\cup(1,1,1) &\in L^{(7)}
\end{aligned}$$

The dual of the complete $(32,4)$-arc S_1 has twenty 0-points, two unipoints, sixteen bipoints, thirty tripoints and sixty-five 4-points.

The dual of the complete $(32,4)$-arc S_1 consists of ten lines of the form $(0,0,0,5,7)$ that are denoted as $L^{(7)}$, ten lines of the form $(0,0,1,3,8)$ that are denoted as $L^{(3)}$, two lines of the form $(0,1,1,0,10)$ that are denoted as $L^{(12)}$ and ten lines of the form $(0,0,2,1,9)$ that are denoted as $L^{(0)}$.

Its complement has twenty-five lines of the form $(2,0,2,4,4)$, twenty lines of the form $(2,1,1,3,5)$, ten lines of the form $(3,0,1,2,6)$, twenty-five lines of the form $(2,0,3,2,5)$, ten lines of the form $(3,0,0,4,5)$, ten lines of the form $(4,0,0,0,8)$ and one line of the form $(0,2,5,0,5)$.

The dual of S_2

The complete $(32,4)$-arc S_2 is completely symmetrical. Its dual $\overline{S}_2$ consists of ten lines of the form $(0,1,1,0,10)$ that are denoted as $L^{(0)}$, ten lines of the form $(0,1,0,2,9)$ that are denoted as $L^{(1)}$, ten lines of the form $(0,0,2,1,9)$ that are denoted as $L^{(2)}$ and two lines of the form $(0,1,1,0,10)$ that are denoted as $L^{(3)}$ and these are separate from the lines of $L^{(0)}$.

$$
\begin{aligned}
\{(0,0,1)+\alpha(0,1,1):\alpha\in F_{11}\}\cup(0,1,1) &\in L^{(0)}\\
\{(0,0,1)+\alpha(1,-5,1):\alpha\in F_{11}\}\cup(1,-5,1) &\in L^{(1)}\\
\{(0,0,1)+\alpha(1,-3,1):\alpha\in F_{11}\}\cup(1,-3,1) &\in L^{(1)}\\
\{(0,0,1)+\alpha(1,-2,1):\alpha\in F_{11}\}\cup(1,-2,1) &\in L^{(0)}\\
\{(0,1,-5)+\alpha(1,1,-2):\alpha\in F_{11}\}\cup(1,1,-2) &\in L^{(0)}\\
\{(0,1,-5)+\alpha(1,1,2):\alpha\in F_{11}\}\cup(1,1,2) &\in L^{(1)}\\
\{(0,1,-5)+\alpha(1,1,-4):\alpha\in F_{11}\}\cup(1,1,-4) &\in L^{(1)}\\
\{(0,1,-4)+\alpha(1,1,4):\alpha\in F_{11}\}\cup(1,1,4) &\in L^{(0)}\\
\{(0,1,-4)+\alpha(1,1,-1):\alpha\in F_{11}\}\cup(1,1,-1) &\in L^{(2)}\\
\{(0,1,-4)+\alpha(1,1,0):\alpha\in F_{11}\}\cup(1,1,0) &\in L^{(2)}\\
\{(0,1,-3)+\alpha(1,1,1):\alpha\in F_{11}\}\cup(1,1,1) &\in L^{(2)}\\
\{(0,1,-3)+\alpha(1,1,-3):\alpha\in F_{11}\}\cup(1,1,-3) &\in L^{(0)}\\
\{(0,1,-3)+\alpha(1,1,-2):\alpha\in F_{11}\}\cup(1,1,-2) &\in L^{(2)}\\
\{(0,1,-2)+\alpha(1,1,-5):\alpha\in F_{11}\}\cup(1,1,-5) &\in L^{(0)}\\
\{(0,1,-2)+\alpha(1,1,-4):\alpha\in F_{11}\}\cup(1,1,-4) &\in L^{(1)}\\
\{(0,1,-2)+\alpha(1,1,-1):\alpha\in F_{11}\}\cup(1,1,-1) &\in L^{(1)}\\
\{(0,1,-1)+\alpha(1,1,4):\alpha\in F_{11}\}\cup(1,1,4) &\in L^{(2)}\\
\{(0,1,-1)+\alpha(1,1,-5):\alpha\in F_{11}\}\cup(1,1,-5) &\in L^{(3)}\\
\{(0,1,-1)+\alpha(1,1,-1):\alpha\in F_{11}\}\cup(1,1,-1) &\in L^{(1)}\\
\{(0,1,0)+\alpha(1,1,-5):\alpha\in F_{11}\}\cup(1,1,-5) &\in L^{(1)}\\
\{(0,1,0)+\alpha(1,1,-4):\alpha\in F_{11}\}\cup(1,1,-4) &\in L^{(0)}\\
\{(0,1,0)+\alpha(1,1,-2):\alpha\in F_{11}\}\cup(1,1,-2) &\in L^{(1)}\\
\{(0,1,1)+\alpha(1,1,4):\alpha\in F_{11}\}\cup(1,1,4) &\in L^{(2)}\\
\{(0,1,1)+\alpha(1,1,-5):\alpha\in F_{11}\}\cup(1,1,-5) &\in L^{(2)}\\
\{(0,1,1)+\alpha(1,1,-4):\alpha\in F_{11}\}\cup(1,1,-4) &\in L^{(0)}\\
\{(0,1,2)+\alpha(1,1,5):\alpha\in F_{11}\}\cup(1,1,5) &\in L^{(0)}\\
\{(0,1,3)+\alpha(1,1,3):\alpha\in F_{11}\}\cup(1,1,3) &\in L^{(1)}\\
\{(0,1,3)+\alpha(1,1,-2):\alpha\in F_{11}\}\cup(1,1,-2) &\in L^{(3)}\\
\{(0,1,3)+\alpha(1,1,1):\alpha\in F_{11}\}\cup(1,1,1) &\in L^{(2)}\\
\{(0,1,4)+\alpha(1,1,-1):\alpha\in F_{11}\}\cup(1,1,-1) &\in L^{(2)}\\
\{(0,1,4)+\alpha(1,1,0):\alpha\in F_{11}\}\cup(1,1,0) &\in L^{(2)}\\
\{(0,1,4)+\alpha(1,1,4):\alpha\in F_{11}\}\cup(1,1,4) &\in L^{(0)}
\end{aligned}
$$

The dual of the complete $(32,4)$-arc S_2 has ten 0-points, twenty-two unipoints, sixteen bipoints, ten tripoints and seventy-five 4-points.

The dual of the complete $(32,4)$-arc S_2 consists of twelve lines of the form $(0,1,1,0,10)$, ten lines of the form $(0,1,0,2,9)$ and ten lines of the form $(0,0,2,1,9)$.

Its complement has ten lines of the form $(0,4,2,0,6)$, ten lines of the form $(2,0,3,2,5)$, twenty lines of the form $(1,3,1,1,6)$, twenty-five lines of the form $(2,2,1,0,7)$, ten lines of the form $(1,2,3,0,6)$, five lines of the form $(0,2,4,2,4)$, ten lines of the form $(2,2,0,2,6)$, ten lines of the form $(0,4,1,2,5)$ and one line of the form $(0,2,5,0,5)$.

The dual of S_3

The complete $(32,4)$-arc S_3 is completely symmetrical. Its dual $\overline{S}_3$ consists of ten lines of the form $(0,0,2,1,9)$ that are denoted as $L^{(0)}$, ten lines of the form $(0,1,0,2,9)$ that are denoted as $L^{(1)}$, ten lines of the form $(0,1,1,0,10)$ that are denoted as $L^{(2)}$ and two lines of the form $(0,1,1,0,10)$ that are separate from the lines of $L^{(2)}$ and are denoted as $L^{(3)}$.

$$
\begin{aligned}
\{(0,0,1)+\alpha(0,1,1):\alpha\in F_{11}\}\cup(0,1,1) &\in L^{(0)}\\
\{(0,0,1)+\alpha(1,-3,1):\alpha\in F_{11}\}\cup(1,-3,1) &\in L^{(1)}\\
\{(0,0,1)+\alpha(1,-2,1):\alpha\in F_{11}\}\cup(1,-2,1) &\in L^{(2)}\\
\{(0,0,1)+\alpha(1,1,1):\alpha\in F_{11}\}\cup(1,1,1) &\in L^{(0)}\\
\{(0,1,-5)+\alpha(1,1,-1):\alpha\in F_{11}\}\cup(1,1,-1) &\in L^{(2)}\\
\{(0,1,-5)+\alpha(1,1,1):\alpha\in F_{11}\}\cup(1,1,1) &\in L^{(1)}\\
\{(0,1,-5)+\alpha(1,1,3):\alpha\in F_{11}\}\cup(1,1,3) &\in L^{(2)}\\
\{(0,1,-4)+\alpha(1,1,5):\alpha\in F_{11}\}\cup(1,1,5) &\in L^{(0)}\\
\{(0,1,-4)+\alpha(1,1,-1):\alpha\in F_{11}\}\cup(1,1,-1) &\in L^{(2)}\\
\{(0,1,-4)+\alpha(1,1,3):\alpha\in F_{11}\}\cup(1,1,3) &\in L^{(0)}\\
\{(0,1,-3)+\alpha(1,1,2):\alpha\in F_{11}\}\cup(1,1,2) &\in L^{(2)}\\
\{(0,1,-3)+\alpha(1,1,4):\alpha\in F_{11}\}\cup(1,1,4) &\in L^{(0)}\\
\{(0,1,-3)+\alpha(1,1,-3):\alpha\in F_{11}\}\cup(1,1,-3) &\in L^{(0)}\\
\{(0,1,-2)+\alpha(1,1,-5):\alpha\in F_{11}\}\cup(1,1,-5) &\in L^{(0)}\\
\{(0,1,-2)+\alpha(1,1,3):\alpha\in F_{11}\}\cup(1,1,3) &\in L^{(0)}\\
\{(0,1,-2)+\alpha(1,1,4):\alpha\in F_{11}\}\cup(1,1,4) &\in L^{(2)}\\
\{(0,1,-1)+\alpha(1,1,0):\alpha\in F_{11}\}\cup(1,1,0) &\in L^{(1)}\\
\{(0,1,-1)+\alpha(1,1,1):\alpha\in F_{11}\}\cup(1,1,1) &\in L^{(1)}\\
\{(0,1,0)+\alpha(1,1,-5):\alpha\in F_{11}\}\cup(1,1,-5) &\in L^{(0)}\\
\{(0,1,0)+\alpha(1,1,-2):\alpha\in F_{11}\}\cup(1,1,-2) &\in L^{(2)}\\
\{(0,1,0)+\alpha(1,1,0):\alpha\in F_{11}\}\cup(1,1,0) &\in L^{(1)}\\
\{(0,1,1)+\alpha(1,1,-4):\alpha\in F_{11}\}\cup(1,1,-4) &\in L^{(3)}\\
\{(0,1,1)+\alpha(1,1,-3):\alpha\in F_{11}\}\cup(1,1,-3) &\in L^{(2)}\\
\{(0,1,1)+\alpha(1,1,-1):\alpha\in F_{11}\}\cup(1,1,-1) &\in L^{(1)}\\
\{(0,1,2)+\alpha(1,1,-4):\alpha\in F_{11}\}\cup(1,1,-4) &\in L^{(1)}
\end{aligned}
$$

$$\begin{aligned}
\{(0,1,2)+\alpha(1,1,2):\alpha\in F_{11}\}\cup(1,1,2) &\in L^{(1)}\\
\{(0,1,2)+\alpha(1,1,4):\alpha\in F_{11}\}\cup(1,1,4) &\in L^{(1)}\\
\{(0,1,3)+\alpha(1,1,-3):\alpha\in F_{11}\}\cup(1,1,-3) &\in L^{(0)}\\
\{(0,1,4)+\alpha(1,1,0):\alpha\in F_{11}\}\cup(1,1,0) &\in L^{(1)}\\
\{(0,1,4)+\alpha(1,1,2):\alpha\in F_{11}\}\cup(1,1,2) &\in L^{(3)}\\
\{(0,1,4)+\alpha(1,1,-5):\alpha\in F_{11}\}\cup(1,1,-5) &\in L^{(2)}\\
\{(0,1,5)+\alpha(1,1,-4):\alpha\in F_{11}\}\cup(1,1,-4) &\in L^{(2)}
\end{aligned}$$

The dual of the complete $(32,4)$-arc S_3 has ten 0-points, twenty-two unipoints, sixteen bipoints, ten tripoints and seventy-five 4-points.

The dual of the complete $(32,4)$-arc S_3 consists of twelve lines of the form $(0,1,1,0,10)$, ten lines of the form $(0,0,2,1,9)$ and ten lines of the form $(0,1,0,2,9)$.

Its complement has forty lines of the form $(1,3,1,1,6)$, ten lines of the form $(2,2,1,0,7)$, five lines of the form $(2,0,4,0,6)$, five lines of the form $(0,4,2,0,6)$, ten lines of the form $(3,1,0,1,7)$, ten lines of the form $(1,2,3,0,6)$, ten lines of the form $(1,1,3,3,4)$ and one line of the form $(0,2,5,0,5)$.

The dual of S_4

The complete $(32,4)$-arc S_4 is completely symmetrical. Its dual $\overline{S}_4$ consists of eight lines of the form $(0,1,1,0,10)$ that are denoted as $L^{(0)}$, eight lines of the form $(0,0,1,3,8)$ that are denoted as $L^{(1)}$, four lines of the form $(0,1,0,2,9)$ that are denoted as $L^{(2)}$, four lines of the form $(0,1,0,2,9)$ that are separate from the lines of $L^{(2)}$ and are denoted as $L^{(3)}$, four lines of the form $(0,0,1,3,8)$ that are denoted as $L^{(4)}$ and four lines of the form $(0,1,0,2,9)$ that are separate from the lines of $L^{(2)}$ and $L^{(3)}$ and are denoted as $L^{(5)}$.

$$\begin{aligned}
\{(0,0,1)+\alpha(0,1,1):\alpha\in F_{11}\}\cup(0,1,1) &\in L^{(0)}\\
\{(0,0,1)+\alpha(1,-5,1):\alpha\in F_{11}\}\cup(1,-5,1) &\in L^{(1)}\\
\{(0,0,1)+\alpha(1,-4,1):\alpha\in F_{11}\}\cup(1,-4,1) &\in L^{(2)}\\
\{(0,0,1)+\alpha(1,5,1):\alpha\in F_{11}\}\cup(1,5,1) &\in L^{(3)}\\
\{(0,1,-5)+\alpha(1,1,0):\alpha\in F_{11}\}\cup(1,1,0) &\in L^{(0)}\\
\{(0,1,-5)+\alpha(1,1,-5):\alpha\in F_{11}\}\cup(1,1,-5) &\in L^{(4)}\\
\{(0,1,-5)+\alpha(1,1,-3):\alpha\in F_{11}\}\cup(1,1,-3) &\in L^{(4)}\\
\{(0,1,-4)+\alpha(1,1,4):\alpha\in F_{11}\}\cup(1,1,4) &\in L^{(0)}\\
\{(0,1,-4)+\alpha(1,1,5):\alpha\in F_{11}\}\cup(1,1,5) &\in L^{(3)}\\
\{(0,1,-4)+\alpha(1,1,-4):\alpha\in F_{11}\}\cup(1,1,-4) &\in L^{(3)}\\
\{(0,1,-3)+\alpha(1,1,-1):\alpha\in F_{11}\}\cup(1,1,-1) &\in L^{(1)}\\
\{(0,1,-3)+\alpha(1,1,4):\alpha\in F_{11}\}\cup(1,1,4) &\in L^{(1)}\\
\{(0,1,-3)+\alpha(1,1,-5):\alpha\in F_{11}\}\cup(1,1,-5) &\in L^{(0)}\\
\{(0,1,-2)+\alpha(1,1,-4):\alpha\in F_{11}\}\cup(1,1,-4) &\in L^{(1)}\\
\{(0,1,-2)+\alpha(1,1,-2):\alpha\in F_{11}\}\cup(1,1,-2) &\in L^{(1)}\\
\{(0,1,-2)+\alpha(1,1,1):\alpha\in F_{11}\}\cup(1,1,1) &\in L^{(5)}
\end{aligned}$$

$$\begin{aligned}
\{(0,1,0)+\alpha(1,1,-4):\alpha\in F_{11}\}\cup(1,1,-4) &\in L^{(4)}\\
\{(0,1,0)+\alpha(1,1,4):\alpha\in F_{11}\}\cup(1,1,4) &\in L^{(1)}\\
\{(0,1,0)+\alpha(1,1,5):\alpha\in F_{11}\}\cup(1,1,5) &\in L^{(3)}\\
\{(0,1,1)+\alpha(1,1,4):\alpha\in F_{11}\}\cup(1,1,4) &\in L^{(5)}\\
\{(0,1,1)+\alpha(1,1,5):\alpha\in F_{11}\}\cup(1,1,5) &\in L^{(0)}\\
\{(0,1,1)+\alpha(1,1,-1):\alpha\in F_{11}\}\cup(1,1,-1) &\in L^{(2)}\\
\{(0,1,2)+\alpha(1,1,-3):\alpha\in F_{11}\}\cup(1,1,-3) &\in L^{(0)}\\
\{(0,1,3)+\alpha(1,1,-5):\alpha\in F_{11}\}\cup(1,1,-5) &\in L^{(5)}\\
\{(0,1,3)+\alpha(1,1,-3):\alpha\in F_{11}\}\cup(1,1,-3) &\in L^{(4)}\\
\{(0,1,3)+\alpha(1,1,-1):\alpha\in F_{11}\}\cup(1,1,-1) &\in L^{(2)}\\
\{(0,1,4)+\alpha(1,1,-3):\alpha\in F_{11}\}\cup(1,1,-3) &\in L^{(0)}\\
\{(0,1,4)+\alpha(1,1,-5):\alpha\in F_{11}\}\cup(1,1,-5) &\in L^{(2)}\\
\{(0,1,4)+\alpha(1,1,-4):\alpha\in F_{11}\}\cup(1,1,-4) &\in L^{(5)}\\
\{(0,1,5)+\alpha(1,1,5):\alpha\in F_{11}\}\cup(1,1,5) &\in L^{(0)}\\
\{(0,1,5)+\alpha(1,1,-2):\alpha\in F_{11}\}\cup(1,1,-2) &\in L^{(1)}\\
\{(0,1,5)+\alpha(1,1,-1):\alpha\in F_{11}\}\cup(1,1,-1) &\in L^{(1)}
\end{aligned}$$

The dual of the complete $(32,4)$-arc S_4 has ten 0-points, twenty-two unipoints, sixteen bipoints, ten tripoints and seventy-five 4-points.

The dual of the complete $(32,4)$-arc S_4 consists of twelve lines of the form $(0,0,1,3,8)$, eight lines of the form $(0,1,1,0,10)$ and twelve lines of the form $(0,1,0,2,9)$.

Its complement has four lines of the form $(3,0,1,2,6)$, twenty-four lines of the form $(2,2,0,2,6)$, eight lines of the form $(1,2,2,2,5)$, eight lines of the form $(2,1,2,1,6)$, sixteen lines of the form $(1,3,0,3,5)$, seven lines of the form $(0,4,2,0,6)$, sixteen lines of the form $(2,2,1,0,7)$, eight lines of the form $(0,4,1,2,5)$, four lines of the form $(2,0,2,4,4)$, four lines of the form $(0,2,3,4,3)$ and two lines of the form $(2,0,3,2,5)$.

Chapter 6

Investigation of Symmetrical Properties

In this chapter the strong symmetrical properties of a given (n, r)-arc in $PG(2, q)$ as described in Definition 5.8 and the connection between these properties and the stabilizer group of the given (n, r)-arc are explored.

Tables 6.1, 6.2, 6.3, 6.4, 6.7, 6.9 and 6.11 classify either n-arcs or $(n, 3)$-arcs in $PG(2, q)$ up to projective equivalence for some specific value of q. All entries in these tables have the form

$$\mathbf{G}(M_\Gamma : \{\Gamma_0, \ldots, \Gamma_k\}) : y,$$

indicating that there are exactly y, classes of projectively equivalent (n, r)-arcs with stabilizer group isomorphic to $\mathbf{G}$ that are strongly symmetrical of levels $\Gamma_0, \ldots, \Gamma_k$ and size M_Γ.

Note 6.1. In this classification the level of strong symmetry Γ is taken as the the smallest positive integer for which such symmetry exists. Hence, the level of complete symmetry may be greater than Γ.

Tables 6.1, 6.7, 6.9 and 6.11 contain both complete and incomplete (n, r)-arcs, so in these tables y is written as y_1, $y_1 - y_2^c$ or y_2^c, where y_1 indicates the number of incomplete (n, r)-arcs and y_2 indicates the number of complete (n, r)-arcs. Tables 6.5, 6.6, 6.8, 6.10, 6.12 and 6.13 show the connection between the stabilizer group of strongly symmetrical (n, r)-arcs in $PG(2, q)$ and their strong symmetrical properties. For example, the entry

$\mathbf{D}_8$	order	1	2	4	8	16
	number	1	1	2	17	10

in Table 6.10 indicates that some n-arc S in $PG(2, 17)$ has stabilizer group isomorphic to $\mathbf{D}_8$ and that S is strongly symmetrical with

$$\left|\{P_\Gamma^{(i)} \mid o(P_\Gamma^{(i)}) = 1\}\right| = 1,$$

$$\left|\{P_\Gamma^{(i)} \mid o(P_\Gamma^{(i)}) = 2\}\right| = 1,$$

$$\left|\{P_\Gamma^{(i)} \mid o(P_\Gamma^{(i)}) = 4\}\right| = 2,$$

$$\left|\{P_\Gamma^{(i)} \mid o(P_\Gamma^{(i)}) = 8\}\right| = 17,$$
$$\left|\{P_\Gamma^{(i)} \mid o(P_\Gamma^{(i)}) = 16\}\right| = 10.$$

Note 6.2. There exists a unique correspondence between the stabilizer group of strongly symmetrical n-arcs in $PG(2,q)$ and their strong symmetrical properties, for $q = 11, 13, 17, 19$. In $PG(2,11)$, there exist two strongly symmetrical $(10,3)$-arcs with stabilizer group isomorphic to $\mathbf{Z}_{10}$, that have different strong symmetrical properties. There also exists a $(10,3)$-arc with stabilizer group isomorphic to $\mathbf{D}_{10}$; this has the same strong symmetrical properties as the first of the $(10,3)$-arcs with stabilizer group isomorphic to $\mathbf{Z}_{10}$, but they are distinguished by level.

Question 6.3. Is there a distinguishing relationship between the stabilizer group of an (n,r)-arc in $PG(2,q)$ and its strong symmetrical properties, for all r and q?

Lemma 6.4. *Let $(\mathfrak{T}, g) \in PGL(2,q)$ be an element other than the identity. Then there exists a line ℓ in $PG(2,q)$ such that ℓ^g does not coincide with ℓ.*

Proof Since g is not the identity element there exists a point p of $PG(2,q)$ such that p^g does not coincide with p. For ℓ_1 and ℓ_2, two lines through the point p, if p^g is not on ℓ_1, then ℓ_1 does not coincide with ℓ_1^g and if p^g is on ℓ_1, then p^g is not on ℓ_2; that is, ℓ_2 does not coincide with ℓ_2^g. □

Lemma 6.5. *If S is an (n,r)-arc in $PG(2,q)$ that is stabilized by the automorphism group $\mathbf{G}$ and ℓ is a line in $PG(2,q)$, then the symmetrical properties of the line ℓ^g, where $g \in \mathbf{G}$, are the symmetrical properties of the line ℓ.*

Proof The symmetrical properties of the line ℓ^g with respect to S^g are the symmetrical properties of the line ℓ with respect to S, since g is a projectivity. Since $S^g = S$, the symmetrical properties of the line ℓ^g with respect to S are the symmetrical properties of the line ℓ with respect to S. □

Proposition 6.6. *Let S be an (n,r)-arc in $PG(2,q)$. Then the stabilizer group of S is isomorphic to $\mathbf{Z}_1$ if $M_\Gamma = N_\Gamma = q^2 + q + 1$.*

Proof If $g \in stab(S) \neq \{\mathrm{I}\}$ and $A \neq \mathrm{I}$, then there exists a line ℓ in $PG(2,q)$ such that ℓ and ℓ^g do not coincide by Lemma 6.4. The lines ℓ and ℓ^g have the same symmetrical properties with respect to S by Lemma 6.5.

Hence, $M_\Gamma = q^2 + q + 1 \Rightarrow stab(S) = \{\mathrm{I}\}$. □

The follow conjectures are extensions of the information already collected and presented in Tables 6.1 to 6.13.

Conjecture 6.7. *Let S be an (n,r)-arc in $PG(2,q)$. The stabilizer group of S is isomorphic to $\mathbf{Z}_1$ if and only if $M_\Gamma = N_\Gamma = q^2 + q + 1$. The strong symmetrical structure of such an (n,r)-arc consists of $q^2 + q + 1$ points and lines.*

Conjecture 6.8. *Let S be an (n,r)-*arc *in $PG(2,q)$. The stabilizer group of S is isomorphic to $\mathbf{Z}_2$ if and only if $M_\Gamma = N_\Gamma = \frac{q^2-1}{2} + q + 2$. The strong symmetrical structure of such an (n,r)-*arc *consists of $q+2$ points and lines and $\frac{q^2-1}{2}$ sets of points and lines of order 2.*

Conjecture 6.9. *Let S be an (n,r)-*arc *in $PG(2,q)$. The stabilizer group of S is isomorphic to $\mathbf{Z}_\mathrm{p}$, where p is a prime, if and only if the strong symmetrical properties of such an (n,r)-*arc *consist of a_q points and lines and b_q sets of points and lines of order p, with $pb_q+a_q = q^2+q+1$. Here, a_q and b_q are constant for each value of q.*

Note 6.10. One possible line of investigation, with regard to proving these conjectures, is the effect that matrices of prime order have on the projective plane $PG(2,q)$. In particular, subsets of $PG(2,q)$ of the form

$$\{x^{g^i} \mid i \in \overline{\mathbf{N}}_{p-1}\},$$

where $(\mathfrak{T}, g) \in PGL(3,q)$ is isomorphic to $\mathbf{Z}_p$, are described in detail in Chapter 8.

6.1 The use of symmetrical properties in the classification of incomplete $(n,3)$-arcs in $PG(2,11)$

In this section the strong symmetrical properties as described in Definition 5.8 are used to classify the classes of projectively equivalent incomplete $(n,3)$-arcs in $PG(2,11)$. This is done by linking the stabilizer group of a given $(n,3)$-arc with its strong symmetrical properties. It is sufficient to consider only a small fraction of all incomplete $(n,3)$-arcs in the classification, since Proposition 6.6 states that if $M_\Gamma = N_\Gamma = 133$, then the stabilizer group is isomorphic to $\mathbf{Z}_1$ and $M_\Gamma = N_\Gamma = 133$ is the most common result. The n-arcs in $PG(2,11)$ are listed here, as both n-arcs and incomplete $(n,3)$-arcs are used to construct the complete $(n,3)$-arcs.

Table 6.1: Stabilizer group and symmetrical properties of all n-arcs in $PG(2,11)$

$n=5$	$\mathbf{Z}_2(73:2):1$	$\mathbf{D}_5(21:2):1$	
$n=6$	$\mathbf{Z}_1(133:2):1$ $\mathbf{Z}_4(37:2):2$ $\mathbf{D}_6(19:2):1$	$\mathbf{Z}_2(73:2):2$ $\mathbf{Z}_2 \times \mathbf{Z}_2(43:2):1$ $\mathbf{A}_4(15:2):1$	$\mathbf{Z}_3(45:2):2$ $\mathbf{S}_3(29:2):4$ $\mathbf{G}_{60}(7:1):1$
$n=7$	$\mathbf{Z}_1(133:2):7$ $\mathbf{Z}_5(29:2):1$ $\mathbf{Z}_7 \rtimes \mathbf{Z}_3(7:2):1^c$	$\mathbf{Z}_2(73:2):8$ $\mathbf{S}_3(29:2):1$	$\mathbf{Z}_3(45:2):2$ $\mathbf{D}_5(21:2):1$
$n=8$	$\mathbf{Z}_1(133:2):3$ $\mathbf{D}_4(25:2):1-1^c$	$\mathbf{Z}_2(73:2):6-5^c$ $\mathbf{D}_5(29:2):1^c$	$\mathbf{Z}_2 \times \mathbf{Z}_2(43:2):1^c$ $\mathbf{Z}_8 \rtimes \mathbf{Z}_2(38:2):1^c$
$n=9$	$\mathbf{Z}_2(73:2):1^c$	$\mathbf{Z}_3(45:2):1^c$	$\mathbf{S}_3(29:2):2-1^c$
$n=10$	$\mathbf{G}_{60}(5:1):1^c$		
$n=11$	$\mathbf{G}_{110}(5:1):1$		
$n=12$	$\mathbf{G}_{1320}(3:1):1^c$		

Table 6.2: Classification and symmetrical properties of complete $(n, 3)$-arcs

$n = 13$	$\mathbf{Z}_2(73 : 2) : 1$ $\mathbf{D}_5(21 : 1) : 1$	$\mathbf{Z}_6(25 : 2) : 1$	$\mathbf{S}_3(29 : \{1, 2\}) : 2$
$n = 14$	$\mathbf{Z}_1(133 : 2) : 138$	$\mathbf{Z}_2(73 : 1) : 8$	
$n = 15$	$\mathbf{Z}_1(133 : \{1, 2\}) : 70\ 705$ $\mathbf{Z}_4(37 : \{1, 2\}) : 2$ $\mathbf{S}_4(11 : \{1, 2\}) : 2$	$\mathbf{Z}_2(73 : \{1, 2\}) : 794$ $\mathbf{Z}_2 \times \mathbf{Z}_2(43 : \{1, 2\}) : 6$ $\mathbf{S}_3(29 : \{1, 2\}) : 15$	$\mathbf{Z}_3(45 : \{1, 2\}) : 56$ $\mathbf{Z}_6(25 : \{1, 2\}) : 2$ $\mathbf{D}_5(21 : \{1, 2\}) : 2$
$n = 16$	$\mathbf{Z}_1(133 : \{1, 2\}) : 1\ 572\ 864$ $\mathbf{Z}_2 \times \mathbf{Z}_2(4 : 2) : 1$	$\mathbf{Z}_2(73 : \{1, 2\}) : 613$ $\mathbf{Z}_6(25 : \{1, 2\}) : 2$	$\mathbf{Z}_3(45 : \{1, 2\}) : 196$ $\mathbf{S}_3(29 : 2) : 1$
$n = 17$	$\mathbf{Z}_1(133 : \{1, 2\}) : 2\ 078\ 955$ $\mathbf{Z}_2 \times \mathbf{Z}_2(43 : \{1, 2\}) : 20$ $\mathbf{D}_4(25 : 1) : 5$	$\mathbf{Z}_2(73 : \{1, 2\}) : 3\ 782$ $\mathbf{Z}_5(29 : \{1, 2\}) : 5$ $\mathbf{Q}_4(19, 1) : 1$	$\mathbf{Z}_4(37 : \{1, 2\}) : 9$ $\mathbf{Z}_8(19 : 2) : 1$ $\mathbf{D}_5(21 : \{1, 2\}) : 3$
$n = 18$	$\mathbf{Z}_1(133 : \{1, 2\}) : 259\ 174$ $\mathbf{Z}_4(37 : \{1, 2\}) : 4$ $\mathbf{S}_3(29 : \{1, 2\}) : 3$	$\mathbf{Z}_2(73 : \{1, 2\}) : 234$ $\mathbf{Z}_2 \times \mathbf{Z}_2(43 : 2) : 1$ $\mathbf{A}_4(15 : 1) : 1$	$\mathbf{Z}_3(45 : \{1, 2\}) : 166$ $\mathbf{Z}_5(29 : 2) : 1$ $\mathbf{S}_4(11 : 1) : 1$
$n = 19$	$\mathbf{Z}_1(133, \{1, 2\} : 4\ 055$ $\mathbf{Z}_4(37 : 2) : 1$ $\mathbf{Z}_{19} \rtimes \mathbf{Z}_3(3 : 1) : 1$	$\mathbf{Z}_2(73 : \{1, 2\}) : 76$ $\mathbf{Z}_2 \times \mathbf{Z}_2(43 : \{1, 2\}) : 5$	$\mathbf{Z}_3(45 : \{1, 2\} : 35$ $\mathbf{S}_3(29\{1, 2\} : 3$
$n = 20$	$\mathbf{Z}_1(133 : 2) : 13$	$\mathbf{Z}_2(73 : 2) : 2$	
$n = 21$	$\mathbf{Z}_7 \rtimes \mathbf{Z}_3(7 : 1) : 2$		

Table 6.3: Classification and symmetrical properties of incomplete $(n, 3)$-arcs, $n = 5, \ldots, 14$

$n = 5$	$\mathbf{Z}_2(73 : \{2, 3\}) : 1$	$\mathbf{Z}_2 \times \mathbf{Z}_2(43 : 2) : 1$	$\mathbf{D}_4(25 : 3) : 1$
$n = 6$	$\mathbf{Z}_1(133 : \{1, 2\}) : 18$ $\mathbf{Z}_5(29 : 2) : 1$ $\mathbf{S}_4(11 : 3) : 1$	$\mathbf{Z}_2(73 : 2) : 11$ $\mathbf{S}_3(29 : 2) : 1$	$\mathbf{Z}_3(45 : 2) : 5$ $\mathbf{D}_4(25 : 2) : 1$
$n = 7$	$\mathbf{Z}_1(133 : \{1, 2\}) : 432$ $\mathbf{Z}_4(37 : 2) : 2$ $\mathbf{D}_6(19 : 2) : 1$	$\mathbf{Z}_2(73 : 2) : 89$ $\mathbf{Z}_2 \times \mathbf{Z}_2(43 : 2) : 8$ $\mathbf{S}_4(11 : 2) : 1$	$\mathbf{Z}_3(45 :, 2) : 5$ $\mathbf{S}_3(29 : 2) : 6$
$n = 8$	$\mathbf{Z}_1(133 : \{1, 2\}) : 6\,498$ $\mathbf{Z}_2 \times \mathbf{Z}_2(43 : 2) : 13$	$\mathbf{Z}_2(73 : 2) : 329$ $\mathbf{D}_4(25 : 2) : 1$	$\mathbf{Z}_4(37 : 2) : 4$
$n = 9$	$\mathbf{Z}_1(133 : \{1, 2\}) : 68\,958$ $\mathbf{Z}_4(37 : 2) : 4$ $\mathbf{S}_3(29 : 2) : 29$ $\mathbf{Z}_8 \rtimes \mathbf{Z}_2(H_2)(13 : 1) : 1$	$\mathbf{Z}_2(73 : 2) : 1\,400$ $\mathbf{Z}_2 \times \mathbf{Z}_2(43 : 2) : 30$ $\mathbf{D}_4(25 : 2) : 3$	$\mathbf{Z}_3(45 : \{1, 2\}) : 122$ $\mathbf{Z}_6(25 : 2) : 1$ $\mathbf{D}_6(19, 1) : 2$
$n = 10$	$\mathbf{Z}_1(133 : \{1, 2\}) : 571\,469$ $\mathbf{Z}_4(37 : \{1, 2\}) : 30$ $\mathbf{Z}_6(25 : 2) : 1$ $\mathbf{Z}_{10}(15 : 1) : 1$ $\mathbf{A}_4(15 : 1) : 1$	$\mathbf{Z}_2(73 : \{1, 2\}) : 3\,089$ $\mathbf{Z}_2 \times \mathbf{Z}_2(43 : 2) : 37$ $\mathbf{S}_3(29 : \{1, 2\}) : 14$ $\mathbf{D}_5(21 : 1) : 2$ $\mathbf{D}_{10}(15 : 2) : 1$	$\mathbf{Z}_3(45 : \{1, 2\}) : 122$ $\mathbf{Z}_5(29 : 2) : 2$ $\mathbf{D}_4(25\{1, 2\}) : 5$ $\mathbf{D}_6(19 : 1) : 1$ $\mathbf{S}_4(11 : 1) : 1$
$n = 11$	$\mathbf{Z}_1(133 : \{1, 2\}) : 3\,510\,576$ $\mathbf{Z}_2 \times \mathbf{Z}_2(43 : \{1, 2\}) : 83$ $\mathbf{Z}_{10}(15 : 1) : 1$ $\mathbf{D}_{10}(15 : 2) : 1$	$\mathbf{Z}_2(73 : \{1, 2\}) : 10\,297$ $\mathbf{Z}_5(29 : \{1, 2\}) : 9$ $\mathbf{Z}_{10}(17 : 1) : 2$	$\mathbf{Z}_4(37 : \{1, 2\}) : 20$ $\mathbf{D}_4(25 : 2) : 2$ $\mathbf{D}_5(21 : \{1, 2\}) : 3$
$n = 12$	$\mathbf{Z}_1(133 : \{1, 2\}) : 15\,277\,048$ $\mathbf{Z}_4(37 : \{1, 2\}) : 22$ $\mathbf{Z}_6(25 : 1) : 2$ $\mathbf{Z}_{10}(15 : \{1, 2\}) : 1$ $\mathbf{D}_6(19 : 2) : 1$	$\mathbf{Z}_2(73 : \{1, 2\}) : 13\,670$ $\mathbf{Z}_2 \times \mathbf{Z}_2(43 : \{1, 2\}) : 77$ $\mathbf{S}_3(29 : \{1, 2\}) : 52$ $\mathbf{Z}_{10}(17 : \{1, 2\}) : 3$ $\mathbf{Q}_6(13 : 1) : 1$	$\mathbf{Z}_3(45 : \{1, 2\}) : 753$ $\mathbf{Z}_5(29 : \{1, 2\}) : 9$ $\mathbf{D}_4(25 : \{1, 2\}) : 2$ $\mathbf{D}_5(21 : \{1, 2\}) : 3$ $\mathbf{S}_4(11 : 1) : 3$
$n = 13$	$\mathbf{Z}_1(133 : \{1, 2\}) : 43\,986\,360$ $\mathbf{Z}_4(37 : \{1, 2\}) : 22$ $\mathbf{Z}_6(25 : 1) : 1$ $\mathbf{Z}_{10}(15 : 1) : 1$ $\mathbf{Q}_6(13 : 1) : 1$	$\mathbf{Z}_2(73 : \{1, 2\}) : 33\,602$ $\mathbf{Z}_2 \times \mathbf{Z}_2(43 : \{1, 2\}) : 132$ $\mathbf{S}_3(29 : \{1, 2\}) : 45$ $\mathbf{D}_5(21 : \{1, 2\}) : 2$ $\mathbf{D}_{10}(15 : 2) : 1$	$\mathbf{Z}_3(45 : \{1, 2\}) : 579$ $\mathbf{Z}_5(29 : 2) : 2$ $\mathbf{D}_4(25 : \{1, 2\}) : 5$ $\mathbf{D}_6(19 : 1) : 1$ $\mathbf{D}_{12}(13 : 2) : 1$
$n = 14$	$\mathbf{Z}_1(133 : \{1, 2\}) : 76\,912\,853$ $\mathbf{Z}_2 \times \mathbf{Z}_2(43 : \{1, 2\}) : 97$	$\mathbf{Z}_2(73 : \{1, 2\}) : 22\,843$ $\mathbf{Z}_7(19 : 1) : 2$	$\mathbf{Z}_4(37 : \{1, 2\}) : 77$ $\mathbf{D}_4(25 : \{1, 2\}) : 9$

Table 6.4: Classification and symmetrical properties of incomplete $(n, 3)$-arcs, $n = 15, \ldots, 20$

$n = 15$	$\mathbf{Z}_1(133 : \{1,2\}) : 73\ 050\ 084$ $\mathbf{Z}_4(37 : \{1,2\}) : 29$ $\mathbf{Z}_6(25 : 1) : 3$ $\mathbf{D}_5(21 : \{1,2\}) : 4$	$\mathbf{Z}_2(73 : \{1,2\}) : 34\ 769$ $\mathbf{Z}_2 \times \mathbf{Z}_2(43 : \{1,2\}) : 128$ $\mathbf{S}_3(29 : \{1,2\}) : 62$ $\mathbf{D}_6(19 : \{1,2\}) : 3$	$\mathbf{Z}_3(45 : \{1,2\}) : 1\ 161$ $\mathbf{Z}_5(29 : \{1,2\}) : 7$ $\mathbf{D}_4(25 : \{1,2\}) : 2$ $\mathbf{S}_4(11 : 1) : 2$
$n = 16$	$\mathbf{Z}_1(133 : \{1,2\}) : 31\ 333\ 540$ $\mathbf{Z}_4(37 : \{1,2\}) : 11$ $\mathbf{Z}_6(25 : 2) : 1$ $\mathbf{D}_4(25 : \{1,2\}) : 5$ $\mathbf{D}_6(19 : 1) : 1$	$\mathbf{Z}_2(73 : \{1,2\}) : 8\ 640$ $\mathbf{Z}_2 \times \mathbf{Z}_2(43 : \{1,2\}) : 30$ $\mathbf{S}_3(29 : \{1,2\}) : 9$ $\mathbf{Q}_4(19 : 1) : 1$	$\mathbf{Z}_3(45 : \{1,2\}) : 396$ $\mathbf{Z}_5(29 : 2) : 19$ $\mathbf{Z}_8(19 : 2) : 1$ $\mathbf{D}_5(21 : 2) : 1$
$n = 17$	$\mathbf{Z}_1(133 : \{1,2\}) : 3\ 797\ 839$ $\mathbf{Z}_2 \times \mathbf{Z}_2(43 : \{1,2\}) : 18$	$\mathbf{Z}_2(73 : \{1,2\}) : 3\ 159$ $\mathbf{Z}_5(29 : \{1,2\}) : 5$	$\mathbf{Z}_4(37 : 2) : 2$ $\mathbf{D}_5(21 : 2) : 1$
$n = 18$	$\mathbf{Z}_1(133 : \{1,2\}) : 73\ 995$ $\mathbf{Z}_4(37 : \{1,2\}) : 7$ $\mathbf{D}_4(25 : 1) : 1$	$\mathbf{Z}_2(73 : \{1,2\}) : 207$ $\mathbf{Z}_2 \times \mathbf{Z}_2(43 : 2) : 3$ $\mathbf{A}_4(15 : 2) : 2$	$\mathbf{Z}_3(45 : \{1,2\}) : 54$ $\mathbf{S}_3(29 : 2) : 2$ $\mathbf{G}_{60}(5 : 1) : 1$
n = 19	$\mathbf{Z}_1(133 : \{1,2\}) : 285$	$\mathbf{Z}_2(73 : 2) : 6$	
n = 20	$\mathbf{Z}_1(133 : 2) : 2$		

For a strongly symmetrical (n, r)-arc in $PG(2, q)$, every point is contained in exactly one set of points

$$\{P_\Gamma^{(i)} \mid i \in \overline{\mathbf{N}}_{M_\Gamma - 1}\},$$

so it follows immediately that

$$\sum_{i=0}^{M_\Gamma - 1} P_\Gamma^{(i)} = q^2 + q + 1$$

and likewise

$$\sum_{j=0}^{N_\Gamma - 1} L_\Gamma^{(j)} = q^2 + q + 1.$$

The set

$$\{P_\Gamma^{(i)} \mid i \in \overline{\mathbf{N}}_{M_\Gamma - 1}\}$$

can only represent the strong symmetrical properties of an (n, r)-arc in $PG(2, q)$ if there exists a set

$$\cup\{P_\Gamma^{(i)} \mid i \in J\} \subset \cup\{P_\Gamma^{(i)} \mid i \in \overline{\mathbf{N}}_{M_\Gamma - 1}\}$$

such that

$$\sum_{i \in J} o(P_\Gamma^{(i)}) = n,$$

by the extension of Proposition 5.2.

Table 6.5: Stabilizer group and the orders of sets of points and lines

$\mathbf{Z}_1$	order	1				
	number	133				
$\mathbf{Z}_2$	order	1	2			
	number	13	60			
$\mathbf{Z}_3$	order	1	3			
	number	1	44			
$\mathbf{Z}_4$	order	1	2	4		
	number	1	6	30		
$\mathbf{Z}_2 \times \mathbf{Z}_2$	order	1	2	4		
	number	3	15	25		
$\mathbf{Z}_6$	order	1	3	6		
	number	1	4	20		
$\mathbf{S}_3$	order	1	3	6		
	number	1	12	16		
$\mathbf{Z}_7$	order	7				
	number	19				
$\mathbf{Z}_8$	order	1	4	8		
	number	1	3	15		
$\mathbf{D}_4$	order	1	2	4	8	
	number	1	2	12	10	
$\mathbf{Q}_4$	order	1	4	8		
	number	1	3	15		
$\mathbf{Z}_{10}$	order	1	2	5	10	20
	number	1	1	2	10	1
$\mathbf{Z}_{10}$	order	1	5	10		
	number	3	2	12		
$\mathbf{D}_5$	order	1	2	5	10	
	number	1	1	12	7	
$\mathbf{D}_6$	order	1	3	6	12	
	number	1	2	11	5	
$\mathbf{Q}_6$	order	1	6	12		
	number	1	2	10		
$\mathbf{A}_4$	order	3	4	6	12	
	number	1	1	5	8	
$\mathbf{H}_2$	order	1	4	8	16	
	number	1	1	6	5	
$\mathbf{D}_{10}$	order	1	2	5	10	20
	number	1	1	2	10	1
$\mathbf{Z}_7 \rtimes \mathbf{Z}_3$	order	7	21			
	number	1	6			
$\mathbf{S}_4$	order	3	4	6	12	24
	number	1	1	1	6	2

Table 6.6: Stabilizer group and the orders of sets of points and lines

$\mathbf{D}_{12}$	order	1	6	12		
	number	1	2	10		
$\mathbf{Z}_{19} \rtimes \mathbf{Z}_3$	order	19	57			
	number	1	2			
$\mathbf{G}_{60}$	order	6	10	12	15	30
	number	1	1	1	1	3
$\mathbf{G}_{60}$	order	10	18	30	45	
	number	1	1	2	1	
$\mathbf{G}_{110}$	order	1	11	55		
	number	1	2	2		
$\mathbf{G}_{1320}$	order	12	55	66		
	number	1	1	1		

6.2 Symmetrical properties of the complete $(21, 3)$-arcs in $PG(2, 11)$

6.2.1 The first $(21, 3)$-arc

The stabilizer group of the first $(21, 3)$-arc S_1 in $PG(2, 11)$ is isomorphic to the group $\mathbf{Z}_7 \rtimes \mathbf{Z}_3$ of order 21.

The $(21, 3)$-arc S_1 is strongly symmetric of level 1 and size 7 and completely symmetrical of level 1 and size 7, where the sets of points and lines $P^{(0)}, \ldots, P^{(6)}, L^{(0)}, \ldots, L^{(6)}$ have the complete symmetrical properties:

$$S_1 = P^{(0)} = \{L^{(0)}, L^{(0)}, L^{(0)}, L^{(1)}, L^{(1)}, L^{(1)}, L^{(2)}, L^{(3)}, L^{(3)}, L^{(3)}, L^{(4)}, L^{(4)}\},$$

$$P^{(1)} = \{L^{(0)}, L^{(1)}, L^{(2)}, L^{(2)}, L^{(3)}, L^{(3)}, L^{(3)}, L^{(4)}, L^{(4)}, L^{(5)}, L^{(5)}, L^{(6)}\},$$
$$P^{(2)} = \{L^{(0)}, L^{(0)}, L^{(0)}, L^{(2)}, L^{(2)}, L^{(2)}, L^{(2)}, L^{(2)}, L^{(2)}, L^{(4)}, L^{(4)}, L^{(4)}\},$$
$$P^{(3)} = \{L^{(0)}, L^{(0)}, L^{(0)}, L^{(0)}, L^{(1)}, L^{(2)}, L^{(3)}, L^{(4)}, L^{(5)}, L^{(6)}, L^{(6)}, L^{(6)}\},$$
$$P^{(4)} = \{L^{(0)}, L^{(1)}, L^{(1)}, L^{(2)}, L^{(2)}, L^{(2)}, L^{(3)}, L^{(3)}, L^{(3)}, L^{(6)}, L^{(6)}, L^{(6)}\},$$
$$P^{(5)} = \{L^{(0)}, L^{(1)}, L^{(2)}, L^{(3)}, L^{(3)}, L^{(4)}, L^{(4)}, L^{(4)}, L^{(4)}, L^{(6)}, L^{(6)}, L^{(6)}\},$$
$$P^{(6)} = \{L^{(0)}, L^{(1)}, L^{(1)}, L^{(1)}, L^{(1)}, L^{(2)}, L^{(2)}, L^{(4)}, L^{(4)}, L^{(5)}, L^{(6)}, L^{(6)}\},$$

where $o(S_1 = P^{(0)}) = o(P^{(1)}) = o(P^{(3)}) = o(P^{(4)}) = o(P^{(5)}) = o(P^{(6)}) = 21$ and $o(P^{(2)}) = 7$.

$$L^{(0)} = \{P^{(0)}, P^{(0)}, P^{(0)}, P^{(1)}, P^{(2)}, P^{(3)}, P^{(3)}, P^{(3)}, P^{(3)}, P^{(4)}, P^{(5)}, P^{(6)}\},$$

$$L^{(1)} = \{P^{(0)}, P^{(0)}, P^{(0)}, P^{(1)}, P^{(3)}, P^{(4)}, P^{(4)}, P^{(5)}, P^{(6)}, P^{(6)}, P^{(6)}, P^{(6)}\},$$
$$L^{(2)} = \{P^{(0)}, P^{(1)}, P^{(1)}, P^{(2)}, P^{(2)}, P^{(3)}, P^{(4)}, P^{(4)}, P^{(4)}, P^{(5)}, P^{(6)}, P^{(6)}\},$$
$$L^{(3)} = \{P^{(0)}, P^{(0)}, P^{(0)}, P^{(1)}, P^{(1)}, P^{(1)}, P^{(3)}, P^{(4)}, P^{(4)}, P^{(4)}, P^{(5)}, P^{(5)}\},$$

$$L^{(4)} = \{P^{(0)}, P^{(0)}, P^{(1)}, P^{(1)}, P^{(2)}, P^{(3)}, P^{(5)}, P^{(5)}, P^{(5)}, P^{(5)}, P^{(6)}, P^{(6)}\},$$
$$L^{(5)} = \{P^{(1)}, P^{(1)}, P^{(1)}, P^{(1)}, P^{(1)}, P^{(1)}, P^{(3)}, P^{(3)}, P^{(3)}, P^{(6)}, P^{(6)}, P^{(6)}\},$$
$$S^* = L^{(6)} = \{P^{(1)}, P^{(3)}, P^{(3)}, P^{(3)}, P^{(4)}, P^{(4)}, P^{(4)}, P^{(5)}, P^{(5)}, P^{(5)}, P^{(6)}, P^{(6)}\},$$

where $o(L^{(0)}) = o(L^{(1)}) = o(L^{(2)}) = o(L^{(3)}) = o(L^{(4)}) = o(S_1^* = L^{(6)}) = 21$ and $o(L^{(5)}) = 7$. Here,

$$S_1 = P^{(0)} \overset{S}{\leftrightarrow} L^{(6)} = S_1^*,$$
$$P^{(1)} \overset{S}{\leftrightarrow} L^{(2)},$$
$$P^{(2)} \overset{S}{\leftrightarrow} L^{(5)},$$
$$P^{(3)} \overset{S}{\leftrightarrow} L^{(0)},$$
$$P^{(4)} \overset{S}{\leftrightarrow} L^{(3)},$$
$$P^{(5)} \overset{S}{\leftrightarrow} L^{(1)},$$
$$P^{(6)} \overset{S}{\leftrightarrow} L^{(4)}.$$

That is, the set $P^{(0)}$ coincides with the 21 points in S_1 and $P^{(0)}$ is symmetrical with the set of external lines $L^{(6)}$, where $L^{(6)}$ is the dual of S_1 in $PG(2, 11)$. Further, the set of points $P^{(1)}$ is symmetrical with the set of unisecants $L^{(2)}$, the set of points $P^{(2)}$ is symmetrical with the set of external lines $L^{(5)}$, the set of points $P^{(3)}$ is symmetrical with the set of trisecants $L^{(0)}$, the set of points $P^{(4)}$ is symmetrical with the set of trisecants $L^{(3)}$, the set of points $P^{(5)}$ is symmetrical with the set of trisecants $L^{(1)}$ and the set of points $P^{(6)}$ is symmetrical with the set of bisecants $L^{(4)}$.

6.2.2 The second $(21, 3)$-arc

The stabilizer group of the second $(21, 3)$-arc S_2 in $PG(2, 11)$ is isomorphic to the group $\mathbf{Z}_7 \rtimes \mathbf{Z}_3$ of order 21.

The $(21, 3)$-arc S_2 is strongly symmetric of level 1 and size 7 and completely symmetrical of level 1 and size 7, where the sets of points and lines $P^{(0)}, \ldots, P^{(6)}, L^{(0)}, \ldots, L^{(6)}$ have the complete symmetrical properties:

$$S_2 = P^{(0)} = \{L^{(0)}, L^{(0)}, L^{(0)}, L^{(1)}, L^{(1)}, L^{(1)}, L^{(2)}, L^{(2)}, L^{(2)}, L^{(3)}, L^{(3)}, L^{(4)}\},$$
$$P^{(1)} = \{L^{(0)}, L^{(0)}, L^{(0)}, L^{(1)}, L^{(2)}, L^{(2)}, L^{(3)}, L^{(4)}, L^{(5)}, L^{(5)}, L^{(6)}, L^{(6)}\},$$
$$P^{(2)} = \{L^{(0)}, L^{(0)}, L^{(1)}, L^{(1)}, L^{(1)}, L^{(2)}, L^{(3)}, L^{(4)}, L^{(6)}, L^{(6)}, L^{(6)}, L^{(6)}\},$$
$$P^{(3)} = \{L^{(0)}, L^{(0)}, L^{(0)}, L^{(2)}, L^{(3)}, L^{(3)}, L^{(3)}, L^{(4)}, L^{(4)}, L^{(4)}, L^{(6)}, L^{(6)}\},$$
$$P^{(4)} = \{L^{(0)}, L^{(1)}, L^{(1)}, L^{(1)}, L^{(2)}, L^{(3)}, L^{(4)}, L^{(4)}, L^{(4)}, L^{(4)}, L^{(5)}, L^{(6)}\},$$
$$P^{(5)} = \{L^{(1)}, L^{(1)}, L^{(2)}, L^{(2)}, L^{(3)}, L^{(3)}, L^{(3)}, L^{(3)}, L^{(4)}, L^{(5)}, L^{(6)}, L^{(6)}\},$$
$$P^{(6)} = \{L^{(2)}, L^{(2)}, L^{(2)}, L^{(2)}, L^{(2)}, L^{(2)}, L^{(4)}, L^{(4)}, L^{(4)}, L^{(6)}, L^{(6)}, L^{(6)}\},$$

where $o(S_2 = P^{(0)}) = o(P^{(1)}) = o(P^{(2)}) = o(P^{(3)}) = o(P^{(4)}) = o(P^{(5)}) = 21$ and $o(P^{(6)}) = 7$.

$$L^{(0)} = \{P^{(0)}, P^{(0)}, P^{(0)}, P^{(1)}, P^{(1)}, P^{(1)}, P^{(2)}, P^{(2)}, P^{(3)}, P^{(3)}, P^{(3)}, P^{(4)}\},$$

$$L^{(1)} = \{P^{(0)}, P^{(0)}, P^{(0)}, P^{(1)}, P^{(2)}, P^{(2)}, P^{(2)}, P^{(4)}, P^{(4)}, P^{(4)}, P^{(5)}, P^{(5)}\},$$

$$L^{(2)} = \{P^{(0)}, P^{(0)}, P^{(0)}, P^{(1)}, P^{(1)}, P^{(2)}, P^{(3)}, P^{(4)}, P^{(5)}, P^{(5)}, P^{(6)}, P^{(6)}\},$$

$$L^{(3)} = \{P^{(0)}, P^{(0)}, P^{(1)}, P^{(2)}, P^{(3)}, P^{(3)}, P^{(3)}, P^{(4)}, P^{(5)}, P^{(5)}, P^{(5)}, P^{(5)}\},$$

$$L^{(4)} = \{P^{(0)}, P^{(1)}, P^{(2)}, P^{(3)}, P^{(3)}, P^{(3)}, P^{(4)}, P^{(4)}, P^{(4)}, P^{(4)}, P^{(5)}, P^{(6)}\},$$

$$L^{(5)} = \{P^{(1)}, P^{(1)}, P^{(1)}, P^{(1)}, P^{(1)}, P^{(1)}, P^{(4)}, P^{(4)}, P^{(4)}, P^{(5)}, P^{(5)}, P^{(5)}\},$$

$$S^* = L^{(6)} = \{P^{(1)}, P^{(1)}, P^{(2)}, P^{(2)}, P^{(2)}, P^{(2)}, P^{(3)}, P^{(3)}, P^{(4)}, P^{(5)}, P^{(5)}, P^{(6)}\},$$

where $o(S_2^* = L^{(0)}) = o(L^{(1)}) = o(L^{(2)}) = o(L^{(3)}) = o(L^{(4)}) = o(L^{(6)}) = 21$ and $o(L^{(5)}) = 7$. Here,

$$S_2 = P^{(0)} \overset{S}{\leftrightarrow} L^{(0)} = S_2^*,$$

$$P^{(1)} \overset{S}{\leftrightarrow} L^{(2)},$$

$$P^{(2)} \overset{S}{\leftrightarrow} L^{(3)},$$

$$P^{(3)} \overset{S}{\leftrightarrow} L^{(1)},$$

$$P^{(4)} \overset{S}{\leftrightarrow} L^{(4)},$$

$$P^{(5)} \overset{S}{\leftrightarrow} L^{(6)},$$

$$P^{(6)} \overset{S}{\leftrightarrow} L^{(5)}.$$

That is, the set $P^{(0)}$ coincides with the 21 points in S_2 and $P^{(0)}$ is symmetrical with the set of trisecants $L^{(0)}$, where $L^{(0)}$ is the dual of S_2 in $PG(2, 11)$. Further, the set of points $P^{(1)}$ is symmetrical with the set of trisecants $L^{(2)}$, the set of points $P^{(2)}$ is symmetrical with the set of bisecants $L^{(3)}$, the set of points $P^{(3)}$ is symmetrical with the set of trisecants $L^{(1)}$, the set of points $P^{(4)}$ is symmetrical with the set of unisecants $L^{(4)}$, the set of points $P^{(5)}$ is symmetrical with the set of external lines $L^{(6)}$ and the set of points $P^{(6)}$ is symmetrical with the set of external lines $L^{(5)}$.

6.3 Symmetrical properties for $q = 11, 13, 17, 19$

In this section the stabilizer group and strong symmetrical properties of n-arcs in $PG(2, q)$ are compared, for $q = 11, 13, 17, 19$.

The complete $(q+1)$-arc S in $PG(2, q)$, for $q = 11, 13, 17, 19$, has stabilizer group of order $(q-1)q(q+1)$ and is completely symmetrical with complete symmetrical properties that consist of three symmetrical sets of points and lines, denoted $P_\Gamma^{(0)}, P_\Gamma^{(1)}, P_\Gamma^{(2)}, L_\Gamma^{(0)}, L_\Gamma^{(1)}$ and $L_\Gamma^{(2)}$, with the following symmetrical structure:

$$S = P_\Gamma^{(0)} = \{\overbrace{L_\Gamma^{(0)}, \ldots, L_\Gamma^{(0)}}^{q}, L_\Gamma^{(1)}\},$$

$$P_\Gamma^{(1)} = \{\overbrace{L_\Gamma^{(0)}, \ldots, L_\Gamma^{(0)}}^{\frac{q+1}{2}}, \overbrace{L_\Gamma^{(2)}, \ldots, L_\Gamma^{(2)}}^{\frac{q+1}{2}}\},$$

$$P_\Gamma^{(2)} = \{\overbrace{L_\Gamma^{(0)}, \ldots, L_\Gamma^{(0)}}^{\frac{q-1}{2}}, L_\Gamma^{(1)}, L_\Gamma^{(1)} \overbrace{L_\Gamma^{(2)}, \ldots, L_\Gamma^{(2)}}^{\frac{q-1}{2}}\},$$

where $o(\{S = P_\Gamma^{(0)}\}) = q+1, o(P_\Gamma^{(1)}) = \frac{(q-1)q}{2}$ and $o(P_\Gamma^{(2)}) = \frac{q(q+1)}{2}$;

$$L_\Gamma^{(0)} = \{P_\Gamma^{(0)}, P_\Gamma^{(0)} \overbrace{P_\Gamma^{(1)}, \ldots, P_\Gamma^{(1)}}^{\frac{q-1}{2}}, \overbrace{P_\Gamma^{(2)}, \ldots, P_\Gamma^{(2)}}^{\frac{q-1}{2}}\},$$

$$L_\Gamma^{(1)} = \{P_\Gamma^{(0)} \overbrace{P_\Gamma^{(2)}, \ldots, P_\Gamma^{(2)}}^{q}\},$$

$$L_\Gamma^{(2)} = \{\overbrace{P_\Gamma^{(1)}, \ldots, P_\Gamma^{(1)}}^{\frac{q+1}{2}}, \overbrace{P_\Gamma^{(2)}, \ldots, P_\Gamma^{(2)}}^{\frac{q+1}{2}}\},$$

where $L_\Gamma^{(0)}$ is the set of bisecants, $L_\Gamma^{(1)}$ is the set of unisecants and $L_\Gamma^{(2)}$ is the set of external lines, with $o(L_\Gamma^{(0)}) = \frac{q(q+1)}{2}, o(L_\Gamma^{(1)}) = q+1$ and $o(L_\Gamma^{(2)}) = \frac{(q-1)q}{2}$. Here,

$$S = P_\Gamma^{(0)} \overset{S}{\leftrightarrow} L_\Gamma^{(1)} = S^*,$$

$$P_\Gamma^{(1)} \overset{S}{\leftrightarrow} L_\Gamma^{(2)},$$

$$P_\Gamma^{(2)} \overset{S}{\leftrightarrow} L_\Gamma^{(0)}.$$

That is, the set $P_\Gamma^{(0)}$ coincides with the $q+1$ points of S and $P_\Gamma^{(0)}$ is symmetrical with the set of unisecants $L_\Gamma^{(1)}$, where $L_\Gamma^{(1)}$ is the dual of S in $PG(2,q)$. Further, the set of points $P_\Gamma^{(1)}$ is symmetrical with the set of external lines $L_\Gamma^{(2)}$ and the set of points $P^{(2)}$ is symmetrical with the set of bisecants $L_\Gamma^{(0)}$.

The incomplete q-arc S in $PG(2,q)$, for $q = 11, 13, 17, 19$, has stabilizer group of order $(q-1)q$ and is completely symmetrical with complete symmetrical properties that consist of five symmetrical sets of points and lines, denoted $P_\Gamma^{(0)}, P_\Gamma^{(1)}, P_\Gamma^{(2)}, P_\Gamma^{(3)}, P_\Gamma^{(4)}, L_\Gamma^{(0)}, L_\Gamma^{(1)}, L_\Gamma^{(2)}, L_\Gamma^{(3)}$ and $L_\Gamma^{(4)}$, with the following symmetrical structure:

$$S = P_\Gamma^{(0)} = \{\overbrace{L_\Gamma^{(0)}, \ldots, L_\Gamma^{(0)}}^{q-2}, L_\Gamma^{(1)}, L_\Gamma^{(2)}\},$$

$$P_\Gamma^{(1)} = \{\overbrace{L_\Gamma^{(0)}, \ldots, L_\Gamma^{(0)}}^{\frac{q-1}{2}}, L_\Gamma^{(1)}, \overbrace{L_\Gamma^{(3)}, \ldots, L_\Gamma^{(3)}}^{\frac{q+1}{2}}\},$$

$$P_\Gamma^{(2)} = \{\overbrace{L_\Gamma^{(0)}, \ldots, L_\Gamma^{(0)}}^{\frac{q-1}{2}}, L_\Gamma^{(2)}, \overbrace{L_\Gamma^{(3)}, \ldots, L_\Gamma^{(3)}}^{\frac{q-1}{2}}, L_\Gamma^{(4)}\},$$

$$P_\Gamma^{(3)} = \{\overbrace{L_\Gamma^{(0)}, \ldots, L_\Gamma^{(0)}}^{\frac{q-3}{2}}, L_\Gamma^{(1)}, L_\Gamma^{(2)}, L_\Gamma^{(2)}, \overbrace{L_\Gamma^{(3)}, \ldots, L_\Gamma^{(3)}}^{\frac{q-1}{2}}\},$$

$$P_\Gamma^{(4)} = \{\overbrace{L_\Gamma^{(1)}, \ldots, L_\Gamma^{(1)}}^{q}, L_\Gamma^{(4)}\},$$

where $o(P_\Gamma^{(4)}) = 1, o(S = P_\Gamma^{(0)}) = o(P_\Gamma^{(2)}) = q$ and $o(P_\Gamma^{(1)}) = o(P_\Gamma^{(3)}) = \frac{(q-1)q}{2}$;

$$L_\Gamma^{(0)} = \{P_\Gamma^{(0)}, P_\Gamma^{(0)}, \overbrace{P_\Gamma^{(1)}, \ldots, P_\Gamma^{(1)}}^{\frac{q-1}{2}}, P_\Gamma^{(2)} \overbrace{P_\Gamma^{(3)}, \ldots, P_\Gamma^{(3)}}^{\frac{q-3}{2}}\},$$

$$L_\Gamma^{(1)} = \{P_\Gamma^{(0)}, \overbrace{P_\Gamma^{(1)}, \ldots, P_\Gamma^{(1)}}^{\frac{q-1}{2}}, \overbrace{P_\Gamma^{(3)}, \ldots, P_\Gamma^{(3)}}^{\frac{q-1}{2}}, P_\Gamma^{(4)}\},$$

$$L_\Gamma^{(2)} = \{P_\Gamma^{(0)}, P_\Gamma^{(2)}, \overbrace{P_\Gamma^{(3)}, \ldots, P_\Gamma^{(3)}}^{q-2}\},$$

$$L_\Gamma^{(3)} = \{\overbrace{P_\Gamma^{(1)}, \ldots, P_\Gamma^{(1)}}^{\frac{q+1}{2}}\}, P_\Gamma^{(2)}, \overbrace{P_\Gamma^{(3)}, \ldots, P_\Gamma^{(3)}}^{\frac{q-1}{2}}\},$$

$$L_\Gamma^{(4)} = \{\overbrace{P_\Gamma^{(2)}, \ldots, P_\Gamma^{(2)}}^{q}, P_\Gamma^{(4)}\},$$

where $L_\Gamma^{(0)}$ is the set of bisecants, $L_\Gamma^{(1)}$ and $L_\Gamma^{(2)}$ comprise the set of unisecants and $L_\Gamma^{(3)}$ and $L_\Gamma^{(4)}$ comprise the set of external lines, with $o(L_\Gamma^{(4)}) = 1, o(P_\Gamma^{(1)}) = o(P_\Gamma^{(2)}) = q$ and $o(P_\Gamma^{(0)}) = o(P_\Gamma^{(3)}) = \frac{(q-1)q}{2}$. Here,

$$S = P_\Gamma^{(0)} \overset{S}{\leftrightarrow} L_\Gamma^{(2)} = S^*,$$

$$P_\Gamma^{(1)} \overset{S}{\leftrightarrow} L_\Gamma^{(3)},$$

$$P_\Gamma^{(2)} \overset{S}{\leftrightarrow} L_\Gamma^{(1)},$$

$$P_\Gamma^{(3)} \overset{S}{\leftrightarrow} L_\Gamma^{(0)}$$

$$P_\Gamma^{(4)} \overset{S}{\leftrightarrow} L_\Gamma^{(4)}.$$

That is, the set $P_\Gamma^{(0)}$ coincides with the $q+1$ points in S and $P_\Gamma^{(0)}$ is symmetrical with the set of unisecants $L_\Gamma^{(2)}$, where $L_\Gamma^{(2)}$ is the dual of S in $PG(2,q)$. Further, the set of points $P_\Gamma^{(1)}$ is symmetrical with the set of external lines $L_\Gamma^{(3)}$, the set of points $P_\Gamma^{(2)}$ is symmetrical with the set of unisecants $L_\Gamma^{(1)}$, the set of points $P_\Gamma^{(3)}$ is symmetrical with the set of bisecants $L_\Gamma^{(0)}$ and the set of points $P_\Gamma^{(4)}$ is symmetrical with the set of external lines $L_\Gamma^{(4)}$.

The incomplete $(q-1)$-arc S, for $q = 17, 19$, has stabilizer group of order $2(q-1)$ and is completely symmetrical with complete symmetrical properties that consist of $5 + (q-1)$ symmetrical sets of points and lines such that

$$\left|\{P_\Gamma^{(i)} \mid o(P_\Gamma^{(i)}) = 1\}\right| = \left|\{L_\Gamma^{(j)} \mid o(L_\Gamma^{(j)}) = 1\}\right| = 1,$$

$$\left|\{P_\Gamma^{(i)} \mid o(P_\Gamma^{(i)}) = 2\}\right| = \left|\{L_\Gamma^{(j)} \mid o(L_\Gamma^{(j)}) = 2\}\right| = 1,$$

$$\left|\{P_\Gamma^{(i)} \mid o(P_\Gamma^{(i)}) = \frac{q-1}{2}\}\right| = \left|\{L_\Gamma^{(j)} \mid o(L_\Gamma^{(j)}) = \frac{q-1}{2}\}\right| = 2,$$
$$\left|\{P_\Gamma^{(i)} \mid o(P_\Gamma^{(i)}) = q-1\}\right| = \left|\{L_\Gamma^{(j)} \mid o(L_\Gamma^{(j)}) = q-1\}\right| = q-1,$$
$$\left|\{P_\Gamma^{(i)} \mid o(P_\Gamma^{(i)}) = 2(q-1)\}\right| = \left|\{L_\Gamma^{(j)} \mid o(L_\Gamma^{(j)}) = 2(q-1)\}\right| = 1.$$

The only $P_\Gamma^{(i)}$ of order 2 contains the only two points of $PG(2,q)$ that are not incident with a bisecant of S.

Conjecture 6.11. *The descriptions of the complete symmetrical structure of the complete* $(q+1)$-arc, *incomplete* q-arc *and incomplete* $(q-1)$-arc *are also true, for all prime* $q \geq 23$.

Question 6.12. Without finding a $(q+1)$-arc, q-arc or $(q-1)$-arc how easy is it to construct a group of order $(q-1)q(q+1)$, $(q-1)q$ or $2q$ such that every element of that group maps a line from a given set to a line in this same set in such a way that the structure of these sets is the same as the desired structure of the symmetrical properties?

A brief overview of the links between the stabilizer groups and the strong symmetrical properties of n-arcs in $PG(2,q)$ is presented in the following tables, for $q = 13, 17, 19$.

Table 6.7: Stabilizer group and symmetrical properties of n-arcs in $PG(2,13)$

n = 5	$\mathbf{Z}_2(99:2):1$	$\mathbf{Z}_4(51:2):1$	$\mathbf{S}_3(39:2):1$
$n=6$	$\mathbf{Z}_1(183:2):5$ $\mathbf{Z}_4(51:2):1$ $\mathbf{D}_6(25:2):1$ $\mathbf{G}_{36}(xx:x):1$	$\mathbf{Z}_2(99:2):7$ $\mathbf{Z}_2 \times \mathbf{Z}_2(57:2):1$ $\mathbf{A}_4(19:2):2$	$\mathbf{Z}_3(61:2):4$ $\mathbf{S}_3(39:2):3$ $\mathbf{S}_4(15:2):1$
$n=7$	$\mathbf{Z}_1(183:2):52$ $\mathbf{Z}_6(35:2):1$	$\mathbf{Z}_2(99:2):21$ $\mathbf{S}_3(39:2):1$	$\mathbf{Z}_3(61:2):4$ $\mathbf{D}_7(21:2):1$
$n=8$	$\mathbf{Z}_1(183:2):110$ $\mathbf{Z}_4(51:2):2$ $\mathbf{D}_4(33:2):2$ $\mathbf{S}_4(15:2):1$	$\mathbf{Z}_2(99:2):54$ $\mathbf{Z}_2 \times \mathbf{Z}_2(57:2):6$ $\mathbf{D}_6(25:2):1$	$\mathbf{Z}_3(61:2):1$ $\mathbf{S}_3(39:2):2-1^c$ $\mathbf{D}_7(21:2):1^c$
$n=9$	$\mathbf{Z}_1(183:2):41-17^c$ $\mathbf{Z}_4(51:2):2-1^c$ $\mathbf{G}_{36}(11:2):1$	$\mathbf{Z}_2(99:2):20-4^c$ $\mathbf{S}_3(39:2):6$	$\mathbf{Z}_3(61:2):1-5^c$ $\mathbf{Z}_3 \times \mathbf{Z}_3(21:2):2^c$
$n=10$	$\mathbf{Z}_1(183:2):1^c$ $\mathbf{Z}_2 \times \mathbf{Z}_2(57:2):2-4^c$ $\mathbf{A}_4(19:2):1$	$\mathbf{Z}_2(99:2):1-11^c$ $\mathbf{S}_3(39:2):1-2^c$ $\mathbf{S}_4(15:2):1^c$	$\mathbf{Z}_4(51:2):2^c$ $\mathbf{D}_4(33:2):1$
n = 11	$\mathbf{S}_3(39:2):2$		
n = 12	$\mathbf{D}_{12}(17:3):1$	$\mathbf{G}_{72}(9:2):1$	
n = 13	$\mathbf{G}_{156}(5:2):1$		
n = 14	$\mathbf{G}_{2184}(3:2):1^c$		

Table 6.8: Stabilizer group and the orders of sets of points and lines in $PG(2, 13)$

$\mathbf{Z}_1$	order	1					
	number	183					
$\mathbf{Z}_2$	order	1	2				
	number	15	84				
$\mathbf{Z}_3$	order	3					
	number	61					
$\mathbf{Z}_4$	order	1	2	4			
	number	3	6	42			
$\mathbf{Z}_2 \times \mathbf{Z}_2$	order	1	2	4			
	number	3	18	36			
$\mathbf{Z}_6$	order	1	3	6			
	number	3	4	28			
$\mathbf{S}_3$	order	1	2	3	6		
	number	1	1	14	23		
$\mathbf{D}_4$	order	1	2	4	8		
	number	1	3	14	15		
$\mathbf{Z}_3 \times \mathbf{Z}_3$	order	3	9				
	number	9	20				
$\mathbf{D}_6$	order	1	2	3	6	12	
	number	1	1	2	13	8	
$\mathbf{A}_4$	order	3	4	6			
	number	1	3	6			
$\mathbf{A}_4$	order	3	6	12			
	number	1	6	12			
$\mathbf{D}_7$	order	1	7	14			
	number	1	14	6			
$\mathbf{S}_4$	order	3	4	6	8	12	24
	number	1	1	2	1	7	3
$\mathbf{D}_{12}$	order	1	2	6	12	24	
	number	1	1	2	12	1	
$\mathbf{G}_{36}$	order	6	9	18	36		
	number	2	3	4	2		
$\mathbf{G}_{72}$	order	3	12	18	36		
	number	1	3	2	3		
$\mathbf{G}_{156}$	order	1	13	78			
	number	1	2	2			
$\mathbf{G}_{2184}$	order	14	78	91			
	number	1	1	1			

Table 6.9: Stabilizer group and symmetrical properties of n-arcs in $PG(2, 17)$

n = 5	$\mathbf{Z}_2(163:2):3$	$\mathbf{Z}_4(83:2):3$	
$n=6$	$\mathbf{Z}_1(307:2):32$ $\mathbf{Z}_4(83:2):3$ $\mathbf{D}_6(37:2):1$	$\mathbf{Z}_2(163:2):16$ $\mathbf{Z}_2\times\mathbf{Z}_2(91:2):2$ $\mathbf{A}_4(31:2):3$	$\mathbf{Z}_3(103:2):9$ $\mathbf{S}_3(61:2):7$ $\mathbf{S}_4(21:2):1$
$n=7$	$\mathbf{Z}_1(307:2):644$ $\mathbf{S}_3(61:2):2$	$\mathbf{Z}_2(163:2):75$	$\mathbf{Z}_3(103:2):12$
$n=8$	$\mathbf{Z}_1(307:2):5\ 025$ $\mathbf{Z}_2\times\mathbf{Z}_2(91:2):2$ $\mathbf{H}_2(27:2):1$	$\mathbf{Z}_2(163:2):389$ $\mathbf{D}_4(51:2):3$	$\mathbf{Z}_4(83:2):5$ $\mathbf{D}_8(31:2):1$
$n=9$	$\mathbf{Z}_1(307:2):17\ 086$ $\mathbf{Z}_4(83:2):9$ $\mathbf{D}_9(27:2):1$	$\mathbf{Z}_2(163:2):428$ $\mathbf{S}_3(61:2):19$	$\mathbf{Z}_3(103:2):88$ $\mathbf{Z}_8(43:2):2$
$n=10$	$\mathbf{Z}_1(307:2):19\ 571-341^c$ $\mathbf{Z}_4(83:2):7-7^c$ $\mathbf{D}_4(51:2):1$ $\mathbf{D}_8(31:2):1$ $\mathbf{S}_4(21:2):1^c$	$\mathbf{Z}_2(163:2):862-179^c$ $\mathbf{Z}_2\times\mathbf{Z}_2(91:2):33-8^c$ $\mathbf{Q}_4(43:2):1^c$ $\mathbf{H}_2(27:2):1^c$	$\mathbf{Z}_3(103:2):24-10^c$ $\mathbf{S}_3(61:2):4-9^c$ $\mathbf{A}_4(31:2):1-2^c$ $\mathbf{D}_9(27:2):1^c$
n = 11	$\mathbf{Z}_1(307:2):3\ 910-2\ 569^c$	$\mathbf{Z}_2(163:2):260-75^c$	
$n=12$	$\mathbf{Z}_1(307:2):53-336^c$ $\mathbf{Z}_4(83:2):1-1^c$ $\mathbf{D}_4(51:2):2^c$ $\mathbf{S}_4(21:2):2-3^c$	$\mathbf{Z}_2(163:2):13-152^c$ $\mathbf{Z}_2\times\mathbf{Z}_2(91:2):3-18^c$ $\mathbf{D}_6(37:2):1-2^c$	$\mathbf{Z}_3(103:2):1-18^c$ $\mathbf{S}_3(61:2):2-20^c$ $\mathbf{A}_4(31:2):1^c$
$n=13$	$\mathbf{Z}_1(307:2):1-1^c$ $\mathbf{Z}_4(83:2):2-1^c$	$\mathbf{Z}_2(163:2):4-4^c$ $\mathbf{S}_3(61:2):1^c$	$\mathbf{Z}_3(103:2):1^c$
n = 14	$\mathbf{Z}_2\times\mathbf{Z}_2(91:2):2$	$\mathbf{D}_4(51:2):1-1^c$	
n = 15	$\mathbf{S}_3(61:2):1$		
n = 16	$\mathbf{G}_{32}(21:2):1$		
n = 17	$\mathbf{G}_{272}(5:2):1$		
n = 18	$\mathbf{G}_{4896}(3:2):1^c$		

Table 6.10: Stabilizer group and the orders of sets of points and lines in $PG(2, 17)$

$\mathbf{Z}_1$	order	1				
	number	307				
$\mathbf{Z}_2$	order	1	2			
	number	19	144			
$\mathbf{Z}_3$	order	1	3			
	number	1	102			
$\mathbf{Z}_4$	order	1	2	4		
	number	1	8	72		
$\mathbf{Z}_2 \times \mathbf{Z}_2$	order	1	2	4		
	number	3	24	64		
$\mathbf{S}_3$	order	1	3	6		
	number	1	18	42		
$\mathbf{Z}_8$	order	1	4	8		
	number	3	4	6		
$\mathbf{D}_4$	order	1	2	4	8	
	number	1	3	19	28	
$\mathbf{Q}_4$	order	1	2	4	8	
	number	1	3	3	36	
$\mathbf{D}_6$	order	1	3	6	12	
	number	1	2	18	16	
$\mathbf{A}_4$	order	3	4	6	12	
	number	1	1	8	21	
$\mathbf{D}_8$	order	1	2	4	8	16
	number	1	1	2	17	10
$\mathbf{H}_2$	order	1	2	4	8	16
	number	1	1	2	9	14
$\mathbf{D}_9$	order	1	9	18		
	number	1	18	8		
$\mathbf{S}_4$	order	3	4	6	12	24
	number	1	1	2	10	7
$\mathbf{G}_{32}$	order	1	2	8	16	32
	number	1	1	2	16	1
$\mathbf{G}_{272}$	order	1	17	136		
	number	1	2	2		
$\mathbf{G}_{4896}$	order	18	136	153		
	number	1	1	1		

Table 6.11: Stabilizer group and symmetrical properties of n-arcs in $PG(2, 19)$

$n = 5$	$\mathbf{Z}_1(381:2):1$ $\mathbf{D}_5(49:3):1$	$\mathbf{Z}_2(201:2):2$	$\mathbf{S}_3(75:3):1$
$n = 6$	$\mathbf{Z}_1(381:2):60$ $\mathbf{Z}_3(129:2):2$ $\mathbf{S}_3(75:2):7$ $\mathbf{G}_{36}(17:2):1$	$\mathbf{Z}_2(201:2):24$ $\mathbf{Z}_4(101:2):3$ $\mathbf{D}_6(45:2):1$ $\mathbf{G}_{60}(13:2):1$	$\mathbf{Z}_3(127:2):12$ $\mathbf{Z}_2 \times \mathbf{Z}_2(111:2):3$ $\mathbf{A}_4(37:2):3$
$n = 7$	$\mathbf{Z}_1(381:2):1\ 632$ $\mathbf{Z}_6(69:2):1$	$\mathbf{Z}_2(201:2):119$ $\mathbf{S}_3(75:2):2$	$\mathbf{Z}_3(127:2):14$
$n = 8$	$\mathbf{Z}_1(381:2):19\ 547$ $\mathbf{Z}_4(101:2):9$ $\mathbf{D}_4(61:2):4$ $\mathbf{S}_4(25:2):1$	$\mathbf{Z}_2(201:2):760$ $\mathbf{Z}_2 \times \mathbf{Z}_2(111:2):23$ $\mathbf{D}_6(45:2):1$	$\mathbf{Z}_3(127:2):8$ $\mathbf{S}_3(75:2):7$ $\mathbf{H}_2(31:2):1$
$n = 9$	$\mathbf{Z}_1(381:2):114\ 146$ $\mathbf{Z}_3(129:2):42$ $\mathbf{D}_9(33:2):1$	$\mathbf{Z}_2(201:2):1\ 134$ $\mathbf{S}_3(75:2):21$ $(\mathbf{Z}_3 \times \mathbf{Z}_3) \rtimes \mathbf{Z}_2(33:2):1$	$\mathbf{Z}_3(127:2):140$ $\mathbf{Z}_3 \times \mathbf{Z}_3(43:2):7$
$n = 10$	$\mathbf{Z}_1(381:2):276\ 049 - 1^c$ $\mathbf{Z}_4(101:2):36 - 1^c$ $\mathbf{Z}_9(45:2):1$ $\mathbf{D}_9(33:2):1$	$\mathbf{Z}_2(201:2):3\ 833 - 18^c$ $\mathbf{Z}_2 \times \mathbf{Z}_2(111:2):77 - 2^c$ $\mathbf{D}_5(49:3):3 - 2^c$ $\mathbf{D}_{10}(31:2):1$	$\mathbf{Z}_3(129:2):60 - 1^c$ $\mathbf{S}_3(75:2):14 - 2^c$ $\mathbf{A}_4(37:2):1^c$ $\mathbf{G}_{60}(13:2):1^c$
$n = 11$	$\mathbf{Z}_1(381:2):223\ 804 - 9\ 501^c$ $\mathbf{S}_3(75:2):12$ $\mathbf{D}_9(33:2):1$	$\mathbf{Z}_2(201:2):1\ 941 - 36^c$ $\mathbf{Z}_9(45:2):1$	$\mathbf{Z}_3(129:2):19 - 4^c$ $\mathbf{D}_5(49:3):1$
$n = 12$	$\mathbf{Z}_1(381:2):24\ 902 - 28\ 301^c$ $\mathbf{Z}_3(129:2):3 - 9^c$ $\mathbf{S}_3(75:2):8 - 37^c$ $\mathbf{D}_6(45:2):2 - 1^c$ $(\mathbf{Z}_3 \times \mathbf{Z}_3) \rtimes \mathbf{Z}_2(33:2):2^c$	$\mathbf{Z}_2(201:2):610 - 1\ 640^c$ $\mathbf{Z}_2 \times \mathbf{Z}_2(111:2):22 - 47^c$ $\mathbf{D}_4(61:2):5 - 4^c$ $\mathbf{A}_4(37:2):1 - 3^c$ $\mathbf{S}_4(25:\{1,2\}):1 - 3^c$	$\mathbf{Z}_3(127:2):14 - 73^c$ $\mathbf{Z}_4(101:2):5 - 11^c$ $\mathbf{Z}_3 \times \mathbf{Z}_3(43:2):2^c$ $\mathbf{D}_9(33:2):1^c$ $\mathbf{G}_{72}(13:2):1^c$
$n = 13$	$\mathbf{Z}_1(381:2):395 - 2\ 090^c$ $\mathbf{Z}_6(69:2):2$	$\mathbf{Z}_2(201:2):98 - 137^c$ $\mathbf{S}_3(75:2):2^c$	$\mathbf{Z}_3(127:2):6 - 3^c$
$n = 14$	$\mathbf{Z}_1(381:2):2 - 8^c$ $\mathbf{Z}_2 \times \mathbf{Z}_2(111:2):3 - 14^c$	$\mathbf{Z}_2(201:2):5 - 35^c$ $\mathbf{S}_3(75:2):2 - 4^c$	$\mathbf{Z}_4(101:2):8^c$ $\mathbf{D}_6(45:2):1 - 1^c$
$n = 15$	$\mathbf{Z}_1(381:2):1$ $\mathbf{D}_5(49:3):1$	$\mathbf{Z}_2(201:2):2$	$\mathbf{S}_3(75:2):1$
n = 16	$\mathbf{Z}_2 \times \mathbf{Z}_2(111:2):2$	$\mathbf{D}_4(61:2):1$	$\mathbf{A}_4(37:2):1$
n = 17	$\mathbf{S}_3(75:2):1$		
n = 18	$\mathbf{G}_{36}(23:3):1$		
n = 19	$\mathbf{G}_{342}(5:1):1$		
n = 20	$\mathbf{G}_{6840}(3:1):1^c$		

Table 6.12: Stabilizer group of order less than 24 in $PG(2, 19)$

$\mathbf{Z}_1$	order	1				
	number	381				
$\mathbf{Z}_2$	order	1	2			
	number	21	180			
$\mathbf{Z}_3$	order	3				
	number	127				
$\mathbf{Z}_3$	order	1	3			
	number	3	126			
$\mathbf{Z}_4$	order	1	2	4		
	number	1	10	90		
$\mathbf{Z}_2 \times \mathbf{Z}_2$	order	1	2	4		
	number	3	27	81		
$\mathbf{Z}_6$	order	1	3	6		
	number	3	6	60		
$\mathbf{S}_3$	order	1	2	3	6	
	number	1	1	20	53	
$\mathbf{D}_4$	order	1	2	4	8	
	number	1	2	22	36	
$\mathbf{Z}_9$	order	1	9			
	number	3	42			
$\mathbf{Z}_3 \times \mathbf{Z}_3$	order	3	9			
	number	1	42			
$\mathbf{D}_5$	order	1	5	10		
	number	1	20	28		
$\mathbf{D}_6$	order	1	2	3	6	12
	number	1	1	2	20	21
$\mathbf{A}_4$	order	3	6	12		
	number	1	9	27		
$\mathbf{H}_2$	order	1	4	8	16	
	number	1	1	11	18	
$\mathbf{D}_9$	order	1	2	9	18	
	number	1	1	20	11	
$(\mathbf{Z}_3 \times \mathbf{Z}_3) \rtimes \mathbf{Z}_2$	order	3	9	18		
	number	4	17	12		
$\mathbf{D}_{10}$	order	1	5	10	20	
	number	1	2	19	9	
$\mathbf{S}_4$	order	3	4	6	8	12	24
	number	1	1	1	1	12	9

Table 6.13: Stabilizer group of order greater than 24 in $PG(2, 19)$

$\mathbf{G}_{36}$	order	1	2	9	18	36	
	number	1	1	2	18	1	
$\mathbf{G}_{36}$	order	6	9	18	36		
	number	2	1	8	6		
$\mathbf{G}_{60}$	order	6	10	15	20	30	60
	number	1	1	1	1	7	2
$\mathbf{G}_{72}$	order	3	12	18	36	72	
	number	1	3	1	7	1	
$\mathbf{G}_{342}$	order	1	19	171			
	number	1	2	2			
$\mathbf{G}_{6840}$	order	20	171	190			
	number	1	1	1			

Chapter 7

Arcs Stabilized by Groups of Prime Order

7.1 Introduction

This chapter looks at automorphism groups of prime order that are generated by a single projectivity; that is, automorphism groups of the form $\langle g \rangle \cong \mathbf{Z}_p$, where $(\mathfrak{T}_g, g) \in PGL(3, q)$ and p is a prime. Such a projectivity can be used to partition $PG(2, q)$ into closed orbits of the form

$$x^{\langle g \rangle} = \{x^{g^i} \mid i \in \overline{\mathbf{N}}_{p-1}\},$$

where x is a point of $PG(2, q)$.

Let G be a group and suppose that p is a prime that satisfies $|G| = ap$. Then the group G possesses a subgroup of order p by [9, Theorem 7.1.1]. Hence, every group of order greater than 1 possesses a subgroup of prime order.

The main application of this chapter is classifying (n, r)-arcs in $PG(2, q)$ that are stabilized by a group that is isomorphic to $\mathbf{Z}_p$, without classifying the (n, r)-arcs that are stabilized by a group that is isomorphic to $\mathbf{Z}_1$.

Notation 7.1. The notation (n, r^-)-arc is used to denote an (n, γ)-arc, where γ is known to be less than or equal to r.

Proposition 7.2. *Let the projectivity $(\mathfrak{T}, g) \in PGL(3, q)$ possess the property '$\langle g \rangle$ is isomorphic to $\mathbf{Z}_p$', where p is a prime and suppose that S is the orbit of x through $\langle g \rangle$ given by*

$$S = \{x^{g^i} \mid i \in \overline{\mathbf{N}}_{p-1}\}.$$

Then the orbit S is a point if $x^{g^{i_1}} = x^{g^{i_2}}$, for any distinct $i_1, i_2 \in \overline{\mathbf{N}}_{p-1}$ and has order p otherwise.

Proof If $x^{g^N} = x$, for some point x and $N \in \mathbf{N}_{p-1}$, then

$$x^{g^{kN}} = x^{g^N g^{(k-1)N}} = x^{g^{(k-1)N}} = \cdots = x^{g^{2N}} = x^{g^N g^N} = x^{g^N} = x,$$

for all $k \in \overline{\mathbf{N}}_{p-1}$. The property '$k_1 \equiv k_2 \pmod{p}$ if and only if $k_1 N \equiv k_2 N \pmod{p}$, for all $k_1, k_2 \in \overline{\mathbf{N}}_{p-1}$' implies

$$\{x^{g^k} \mid k \in \overline{\mathbf{N}}_{p-1}\} = \{x^{g^{kN}} \mid k \in \overline{\mathbf{N}}_{p-1}\}.$$

Hence, $x^{g^{i_1}} = x^{g^{i_2}}$ or equivalently $x^{g^{i_1 - i_2}} = x$ if and only if

$$x = x^g = x^{g^2} = \cdots = x^{g^{p-1}};$$

otherwise,

$$x, x^g, x^{g^2}, \ldots, x^{g^{p-1}}$$

are all distinct points. □

Proposition 7.3. *In $PG(2,q)$, an (n,r)-*arc *S_n contains a 4-arc if and only if $n \geq r+2$.*

Proof If $r = 2$, then the proof is immediate, so assume that $r > 2$. Let ℓ be a line through r points of S_n.

A 4-arc contains at most two points on the line ℓ; hence, S_n contains a 4-arc only if $n \geq r+2$.

If $n \geq r+2$, then S_n must possess two points s_0 and s_1 that are not on the line ℓ. Every set comprising the points s_0, s_1 and two additional points on the line ℓ and not on the line through the points s_0 and s_1 is a 4-arc; hence, S_n contains a 4-arc if $n \geq r+2$. □

Proposition 7.4. *For an $(n, r \leq n-2)$-*arc *S_n in $PG(2,q)$, the group $\langle g \rangle \subseteq \mathrm{aut}(S_n)$ is isomorphic to $\mathbf{Z}_p$ if and only if the group $\langle h^{-1}gh \rangle \subseteq \mathrm{aut}(S_n^h)$ is isomorphic to $\mathbf{Z}_p$, where $(\mathfrak{T}_g, g), (\mathfrak{T}_h, h) \in PGL(3,q)$ and p is a prime. Further,*

$$\left|s^{\langle g \rangle}\right| = \left|(s^h)^{\langle h^{-1}gh \rangle}\right|.$$

Proof The map $\sigma : \langle g \rangle \mapsto \langle h^{-1}gh \rangle$ given by $(g)\sigma = h^{-1}gh$ is an isomorphism from $\langle g \rangle$ to $\langle h^{-1}gh \rangle$ and $\langle g \rangle$ is isomorphic to $\mathbf{Z}_p$; hence, $\langle h^{-1}gh \rangle$ is isomorphic to $\mathbf{Z}_p$.

If $s = s^g$, for some point $s \in S_n$, then $(s^h)^{h^{-1}gh} = s^{gh} = s^h$, for the point $s^h \in S_n^h$. If

$$\left|s^{\langle g \rangle}\right| = p,$$

then $(s^h)^{(h^{-1}gh)^i} = (s^h)^{h^{-1}g^i h} = (s^{g^i})^h \in S_n^h$. The elements of the set

$$\{(s^h)^{(h^{-1}gh)^i} = (s^{g^i})^h \mid i \in \overline{\mathbf{N}}_{p-1}\} \subset S_n^h$$

are distinct, by the bijectivity of h; that is,

$$\left|(s^h)^{\langle h^{-1}gh \rangle} = \{(s^h)^{(h^{-1}gh)^i} \mid i \in \overline{\mathbf{N}}_{p-1}\}\right| = p.$$

Hence, the group $\langle h^{-1}gh \rangle \subseteq \mathrm{aut}(S_n^h)$ is isomorphic to $\mathbf{Z}_p$.

If the group $\langle h^{-1}gh \rangle \subseteq \mathrm{aut}(S_n^h)$ is isomorphic to $\mathbf{Z}_p$, then a similar argument states that the group $\langle hh^{-1}ghh^{-1} \rangle = \langle g \rangle \subseteq \mathrm{aut}((S_n^h)^{h^{-1}}) = \mathrm{aut}(S_n)$ is isomorphic to $\mathbf{Z}_p$. □

The consequence of these propositions is that a representative from every class of projectively equivalent (n,r)-arcs, $n \geq r+2$, can be constructed by adding points to the standard frame $\{e_1, e_2, e_3, e_4\}$.

7.2 $p \geq r + 2$

Proposition 7.5. *Let S_p be a (p, r)-*arc *containing the standard frame in $PG(2, q)$, where $p > 3$ is a prime. Then the group $\langle g \rangle \subseteq \mathrm{aut}(S_p)$ is isomorphic to $\mathbf{Z}_p$ only if*

$$\left|s^{\langle g \rangle}\right| = p,$$

for all $s \in S_p$.

Proof If

$$\left|s^{\langle g \rangle}\right| \neq p,$$

then $s^g = s$, for all $s \in S_n$, by Proposition 7.2. As the group g maps each point of the standard frame to itself, $\langle g \rangle \cong \mathbf{Z}_1$, by Proposition 1.71; a contradiction. □

Proposition 7.6. *Let S_p be a $(p, r \leq p - 2)$-*arc *in $PG(2, q)$, where $p > 3$ is a prime. Then the group $\langle g \rangle \subseteq \mathrm{aut}(S_p)$ is isomorphic to $\mathbf{Z}_p$ only if*

$$\left|s^{\langle g \rangle}\right| = p,$$

for all $s \in S_p$.

Proof Every 4-arc can be mapped to the standard frame by Proposition 1.70 and S_p must contain a 4-arc by Proposition 7.3; hence, for some $(\mathfrak{T}_h, h) \in PGL(3, q)$, the (p, r)-arc S_p^h contains the standard frame.

By Proposition 7.4, the group $\langle f = h^{-1}gh \rangle \subseteq \mathrm{aut}(S_p^h)$ is isomorphic to $\mathbf{Z}_p$. By Proposition 7.5,

$$\left|(s^h)^{\langle f \rangle}\right| = p,$$

for all $s \in S_p$.

By Proposition 7.4, the group $\langle hfh^{-1} \rangle \subseteq \mathrm{aut}(S_p)$ is isomorphic to $\mathbf{Z}_p$ and

$$\left|s^{\langle g \rangle}\right| = p;$$

hence, the proposition holds with $g = hfh^{-1}$. □

Corollary 7.7. *Let S_n be an $(n > p, r \leq p - 2)$-*arc *in $PG(2, q)$, where $p > 3$ is a prime. Then the group $\langle g \rangle \subseteq \mathrm{aut}(S_n)$ is isomorphic to $\mathbf{Z}_p$ only if S_n contains a (p, r^-)-*arc *S_p, that is stabilized by $\langle g \rangle$.*

Proof If the group $\langle g \rangle \subseteq \mathrm{aut}(S_n)$ is isomorphic to $\mathbf{Z}_p$, then, by Proposition 7.2, either $s^g = s$, for all $s \in S_n$ or S_n contains an orbit satisfying

$$\left|s^{\langle g \rangle}\right| = p,$$

for some $s \in S_n$. If $s^g = s$, for all $s \in S_n$, then an application of Proposition 7.6 to any (p, r^-)-arc contained in S_n produces a contradiction; hence, S_n contains the set $S_p = s^{\langle g \rangle}$ and this set is necessarily a (p, r^-)-arc. □

Using Propositions 7.3, Proposition 7.6 can be rewritten by replacing the condition '$p \geq r+2$' with the less strict condition 'some subset of S_p is a 4-arc'; this gives Proposition 7.8.

Proposition 7.8. *Let S_p be a (p,r)-*arc *containing a* 4-arc *in $PG(2,q)$, where $p>3$ is a prime. Then the group $\langle g\rangle \subseteq \mathrm{aut}(S_p)$ is isomorphic to $\mathbf{Z}_p$ only if*

$$\left|s^{\langle g\rangle}\right| = p,$$

for all $s \in S_p$.

Theorem 7.9. *Let S_n be an $(n=\alpha p+m, r\leq p-2)$-*arc *in $PG(2,q)$, where $p>3$ is a prime and $m=0,\ldots,p-1$. Then the group $\langle g\rangle \subseteq \mathrm{aut}(S_n)$ is isomorphic to $\mathbf{Z}_p$ only if the group $\langle g\rangle$ stabilizes an $((\alpha-1)p+m, r^-)$-*arc *contained in S_n. Further, the set S_n is the union of m points that are closed under the right action of g and α distinct orbits of points through $\langle g\rangle$ of order p.*

Proof By Corollary 7.7, the set S_n contains an orbit $s^{\langle g\rangle}$, that satisfies

$$\left|s^{\langle g\rangle}\right| = p,$$

for some $s \in S_n$. As $s^{\langle g\rangle}$ is stabilized by the group $\langle g\rangle$, the $((\alpha-1)p+m, r^-)$-arc $S_n \backslash s^{\langle g\rangle}$ is stabilized by the group $\langle g\rangle$.

By repeated application of Corollary 7.7, the set S_n is the union of α distinct orbits of points through $\langle g\rangle$ of order p; the remaining m points are closed under the right action of g by Proposition 7.2. □

Example 7.10. Since there are no $(7,3^-)$-arcs in $PG(2,17)$ that are stabilized by a group that is isomorphic to $\mathbf{Z}_7$, Corollary 7.7 determines the non-existence of $(n>7,3^-)$-arcs in $PG(2,17)$ that are stabilized by a group that is isomorphic to $\mathbf{Z}_7$.

Construction 7.11. The primary significance of Theorem 7.9 is to the construction of an $(n=\alpha p+m, r\leq p-2)$-arc S_n in $PG(2,q)$ that is stabilized by a group $\langle g\rangle \cong \mathbf{Z}_p$, where $p>3$ is a prime and $m=0,\ldots,p-1$. As S_n is the union of a $(p+m,r^-)$-arc S_{p+m} that is stabilized by $\langle g\rangle$ and the $\alpha-1$ orbits

$$S_p^{(a)} = \{s_a^{g^i} \mid i \in \overline{\mathbf{N}}_{p-1}\},$$

where $\left|S_p^{(a)}\right| = p$, $s_a \in S_n \backslash S_{p+m}$, $a \in \mathbf{N}_\alpha$ and $s_{a_1} \neq s_{a_2}^{g^i}$, for all distinct $a_1, a_2 \in \mathbf{N}_\alpha$. Then S_n is constructed by adding the $\alpha-1$ orbits $S_p^{(a)}$ to the $(p+m,r^-)$-arc S_{p+m}.

If the construction starts with S_{p+m}^h and the group $\langle h^{-1}gh\rangle \subseteq \mathrm{aut}(S_{p+m}^h)$ is isomorphic to $\mathbf{Z}_p$, for some $(\mathfrak{T}_h, h) \in PGL(3,q)$, then adding the orbits

$$\{(s_a^h)^{(h^{-1}gh)^i} = s_a^{g^i h} \mid i \in \overline{\mathbf{N}}_{p-1}\},$$

to S_{p+m}^h produces the (n,r)-arc S_n^h.

7.3 $p < r + 2$ including $p = 2$ and $p = 3$

The method used in section 2 is not valid when $p = 2$ or $p = 3$, since in Proposition 7.5 it is not possible to have a bijective map from either 2 or 3 points to the standard frame; this also invalidates Propositions 7.6 and 7.8.

Proposition 7.12. *Let $S_{\alpha p+m}$ be an $(\alpha p+m, r)$-*arc *containing the stanard frame in $PG(2, q)$, where p is a prime and $m = 0, \ldots, p-1$. Then the group $\langle g\rangle \subseteq \mathrm{aut}(S_{\alpha p+m})$ is isomorphic to $\mathbf{Z}_p$ only if*

$$\left|s^{\langle g\rangle}\right| = p,$$

for some $s \in S_{\alpha p+m}$.

Proof If there does not exist a point $s \in S_{\alpha p+m}$ such that

$$\left|s^{\langle g\rangle}\right| = p,$$

then $s^g = s$, for all $s \in S_{\alpha p+m}$ by Proposition 7.2. As the group g maps each point of the standard frame to itself, $\langle g\rangle \subseteq \mathbf{Z}_1$ by Proposition 1.71; a contradiction. □

Proposition 7.13. *Let $S_{\alpha p+m}$ be an $(\alpha p + m, r)$-*arc *in $PG(2, q)$, where p is a prime, $m = 0, \ldots, p-1$ and $(\alpha - 1)p + m \leq r + 2 \leq \alpha p + m$. Then the group $\langle g\rangle \subseteq \mathrm{aut}(S_{\alpha p+m})$ is isomorphic to $\mathbf{Z}_p$ only if*

$$\left|s^{\langle g\rangle}\right| = p,$$

for some $s \in S_{\alpha p+m}$.

Proof Every 4-arc can be mapped to the standard frame by Proposition 1.70 and $S_{\alpha p+m}$ must contain a 4-arc by Proposition 7.3; hence, for some $(\mathfrak{T}_h, h) \in PGL(3, q)$, the (p, r)-arc $S^h_{\alpha p+m}$ contains the standard frame.

By Proposition 7.4, the group $\langle f = h^{-1}gh\rangle \subseteq \mathrm{aut}(S^h_{\alpha p+m})$ is isomorphic to $\mathbf{Z}_p$. By Proposition 7.12,

$$\left|(s^h)^{\langle f\rangle}\right| = p,$$

for some $s \in S_{\alpha p+m}$.

By Proposition 7.4, the group $\langle hfh^{-1}\rangle \subseteq \mathrm{aut}(S_{\alpha p+m})$ is isomorphic to $\mathbf{Z}_p$ and

$$\left|s^{\langle hfh^{-1}\rangle}\right| = p;$$

hence, the proposition holds with $g = hfh^{-1}$. □

Using Proposition 7.3, Proposition 7.13 can be rewritten by replacing the condition '$p \geq r+2$' with the less strict condition 'some subset of S_p is a 4-arc'; this gives Proposition 7.14.

Proposition 7.14. *Let $S_{\alpha p+m}$ be an $(\alpha p + m, r)$-*arc *containing a* 4-arc *in $PG(2, q)$, where p is a prime and $m = 0, \ldots, p-1$. Then the group $\langle g\rangle \subseteq \mathrm{aut}(S_{\alpha p+m})$ is isomorphic to $\mathbf{Z}_p$ only if*

$$\left|s^{\langle g\rangle}\right| = p,$$

for some $s \in S_{\alpha p+m}$.

Theorem 7.15. *Let S_n be an $(n = (\alpha+\beta)p+m, r)$*-arc *in $PG(2,q)$, where p is a prime, $m = 0, \ldots, p-1$ and $(\alpha-1)p+m \leq r+2 \leq \alpha p+m$. Then the group $\langle g\rangle \subseteq \mathrm{aut}(S_n)$ is isomorphic to $\mathbf{Z}_p$ only if the group $\langle g\rangle$ stabilizes an $((\alpha+\beta-1)p+m, r^-)$*-arc *contained in S_n. Further, S_n is the union of a set of order $(\alpha-1)p+m$ that is closed under the right action of g and $\beta+1$ distinct orbits of points through $\langle g\rangle$ of order p.*

Proof The set S_n contains at least m points with the property '$s_i^g = s_i$' by Proposition 7.2. If there exists an additional point in S_n with this property, then there exist an additional p points in S_n with this property. Removing either a subset

$$\{s_0, \ldots, s_{p-1}\},$$

where $s_i^g = s_i$ or an orbit $s^{\langle g\rangle}$, where $\left|s^{\langle g\rangle}\right| = p$, leaves an $((\alpha+\beta-1)p+m, r^-)$-arc that is stabilized by the group $\langle g\rangle$.

Every set of $\alpha p+m$ points in S_n contains at most $(\alpha-1)p+m$ points with the property '$s_i^g = s_i$' by Proposition 7.13; hence, S_n contains at most $(\alpha-1)p+m$ such points. Otherwise, S_n would contain a subset of $\alpha p+m$ such points, a contradiction to Proposition 7.13.

Let $S_{(\alpha-1)p+m}$ be a subset of S_n that contains every point with the property '$s_i^g = s_i$'. Then $S_n \backslash S_{(\alpha-1)p+m}$ consists of $\beta+1$ distinct orbits of points through $\langle g\rangle$ of order p. □

Construction 7.16. The primary significance of Theorem 7.15 is to the construction of an $(n = (\alpha+\beta)p+m, r)$-arc S_n in $PG(2,q)$ that is stabilized by a group $\langle g\rangle$, where $p > 3$ is a prime, $m = 0, \ldots, p-1$ and $(\alpha-1)p+m \leq r+2 \leq \alpha p+m$. As S_n is the union of an $(\alpha p+m, r^-)$-arc $S_{\alpha p+m}$ that is stabilized by $\langle g\rangle$ and the β orbits

$$S_p^{(a)} = \{s_a^{g^i} \mid i \in \overline{\mathbf{N}}_{p-1}\},$$

where $\left|S_p^{(a)}\right| = p$, $s_a \in S_n \backslash S_{\alpha p+m}$, $a \in \mathbf{N}_\beta$ and $s_{a_1} \neq s_{a_2}^{g^i}$, for all distinct $a_1, a_2 \in \mathbf{N}_\beta$. Then S_n is constructed by adding the β orbits $S_p^{(a)}$ to the $(\alpha p+m, r^-)$-arc $S_{\alpha p+m}$.

If the construction starts with $S_{\alpha p+m}^h$ and the group $\langle h^{-1}gh\rangle \subseteq \mathrm{aut}(S_{\alpha p+m}^h)$ is isomorphic to $\mathbf{Z}_p$, for some $(\mathfrak{T}_h, h) \in PGL(3,q)$, then adding the orbits

$$\{(s_a^h)^{(h^{-1}gh)^i} = s_a^{g^i h} \mid i \in \overline{\mathbf{N}}_{p-1}\},$$

to $S_{\alpha p+m}^h$ produces the (n,r)-arc S_n^h.

Example 7.17. Consider $(n,3)$-arcs in $PG(2,q)$. If $p = 2$, then $m = 0$ or 1 and $2\alpha - 2 + m \leq 5 \leq 2\alpha + m$. If $m = 0$, then $\alpha = 3$ and $2\alpha + m = 6$. If $m = 1$, then $\alpha = 2$ and $2\alpha + m = 5$.

Let S_{2n} be a $(2n, r)$-arc that is stabilized by the group $\langle g_1\rangle \cong \mathbf{Z}_2$. Then S_{2n} is the union of a $(6, r^-)$-arc S_6 that is stabilized by $\langle g_1\rangle$ and the $n-3$ sets

$$\{s_a, s_a^{g_1}\},$$

where $s_a \in S_{2n} \backslash S_6$, $a \in \mathbf{N}_{n-3}$ and $s_{a_1} \neq s_{a_2}^{g_1^i}$, for all distinct $a_1, a_2 \in \mathbf{N}_{n-3}$.

Let S_{2n+1} be a $(2n+1, r)$-arc that is stabilized by the group $\langle g_2\rangle \cong \mathbf{Z}_2$. Then S_{2n+1} is the union of a $(5, r^-)$-arc S_5 that is stabilized by $\langle g_2\rangle$ and the $n-2$ sets

$$\{s_a, s_a^{g_2}\},$$

where $s_a \in S_{2n+1} \backslash S_5$, $a \in \mathbf{N}_{n-2}$ and $s_{a_1} \neq s_{a_2}^{g_2^i}$, for all distinct $a_1, a_2 \in \mathbf{N}_{n-2}$.

Example 7.18. Consider $(n,3)$-arcs in $PG(2,q)$. If $p=3$, then $m=0,1$ or 2 and $3\alpha-3+m \leq 5 \leq 3\alpha+m$. If $m=0$, then $\alpha=2$ and $3\alpha+m=6$. If $m=1$, then $\alpha=2$ and $3\alpha+m=7$. If $m=2$, then $\alpha=1$ and $3\alpha+m=5$.

Let S_{3n} be a $(3n,r)$-arc that is stabilized by the group $\langle g_1\rangle \cong \mathbf{Z}_3$. Then S_{3n} is the union of a $(6,r^-)$-arc S_6 that is stabilized by $\langle g_1\rangle$ and the $n-2$ sets

$$\{s_a, s_a^{g_1}, s_a^{g_1^2}\},$$

where $s_a \in S_{3n}\backslash S_6$, $a \in \mathbf{N}_{n-2}$ and $s_{a_1} \neq s_{a_2}^{g_1^i}$, for all distinct $a_1, a_2 \in \mathbf{N}_{n-2}$.

Let S_{3n+1} be a $(3n+1,r)$-arc that is stabilized by the group $\langle g_2\rangle \cong \mathbf{Z}_3$. Then S_{3n+1} is the union of a $(7,r^-)$-arc S_7 that is stabilized by $\langle g_2\rangle \cong \mathbf{Z}_3$ and the $n-2$ sets

$$\{s_a, s_a^{g_2}, s_a^{g_2^2}\},$$

where $s_a \in S_{3n+1}\backslash S_7$, $a \in \mathbf{N}_{n-2}$ and $s_{a_1} \neq s_{a_2}^{g_2^i}$, for all distinct $a_1, a_2 \in \mathbf{N}_{n-2}$.

Let S_{3n+2} be a $(3n+2,r)$-arc that is stabilized by the group $\langle g_3\rangle \cong \mathbf{Z}_3$. Then S_{3n+2} is the union of a $(5,r^-)$-arc S_5 that is stabilized by $\langle g_3\rangle \cong \mathbf{Z}_3$ and the $n-1$ sets

$$\{s_a, s_a^{g_3}, s_a^{g_3^2}\},$$

where $s_a \in S_{3n+2}\backslash S_5$, $a \in \mathbf{N}_{n-1}$ and $s_{a_1} \neq s_{a_2}^{g_3^i}$, for all distinct $a_1, a_2 \in \mathbf{N}_{n-1}$.

7.4 Results

7.4.1 n-arcs

Expanding those 5-arcs and 6-arcs that are stabilized by groups that are isomorphic to $\mathbf{Z}_2$ in $PG(2,23)$ and $PG(2,29)$ produced q-arcs and $(q+1)$-arcs the automorphism groups of which matched those predicted in Conjecture 6.7.

7.4.2 $(n,3)$-arcs

Expanding $(5,3^-)$-arcs that are stabilized by groups that are isomorphic to $\mathbf{Z}_2$ in $PG(2,13)$ produces two $(23,3)$-arcs; the first has an automorphism group that is isomorphic to $\mathbf{Z}_2$ and in terms of symmetry it possesses fifteen points and lines and eighty-four sets of points and lines of order 2; the second has a automorphism group that is isomorphic to $\mathbf{Z}_4$ and in terms of symmetry it possesses one set of points and lines of order 3, two sets of points and lines of order 6 and four sets of points and lines of order 42.

Chapter 8

Subsets of $PG(2, q)$

8.1 Introduction

This chapter investigates the orbit of points of $PG(2, q)$ through the right action of elements of a group $\langle g \rangle \cong \mathbf{Z}_p$, where $(\mathfrak{T}_g, g) \in PGL(3, q)$ and p is a prime; that is, orbits of the form

$$x^{\langle g \rangle} = \{x^{g^i} \mid i \in \overline{\mathbf{N}}_{p-1}\}.$$

By Proposition 7.2, the orbit of a point $x \in PG(2, q)$ through $\langle g \rangle$ is a point if $x^g = x$ or a set of p points that is closed under the right action of g otherwise. By Proposition 8.1, a subset of lines in $PG(2, q)$ that is given by

$$\{\ell^{g^i} \mid i \in \overline{\mathbf{N}}_{p-1}\}$$

is a line if $\ell^g = \ell$ or a set of p lines that is closed under the right action of g otherwise. Hence, the focus of this investigation is the structure of those points and lines that are closed under the right action of g. All other points and lines are in sets of order p.

As every projectivity maps $PG(2, q)$ to itself bijectively, the existence of a projectivity $(\mathfrak{T}_g, g) \in PGL(3, q)$ with the property '$\langle g \rangle \cong \mathbf{Z}_p$' is dependent on the consistency of the structure of points and lines that are closed under the right action of g. In Sections 8.2, 8.3, 8.4, 8.5, 8.6 and 8.7 the structure of points that are closed under the right action of g are considered for specific instances of p.

This leads to restrictions on the prime p, for which there exists a matrix g satisfying $g^p = \alpha \mathrm{I}$ over $GF(q)$, that match those given by Sylow's Theorems.

For an (n, r)-arc S in $PG(2, q)$ that is closed under the right action of such a g, there are restrictions on n, that are determined by the number and the structure of all points that are closed under the right action of g and the fact that all other points in S generate subsets of order p that are closed under the right action of g.

8.1.1 Order of subsets of $PG(2, q)$

In this chapter the subsets of lines in $PG(2, q)$ are as important as the subsets of points; so, Proposition 7.2 is adapted for lines as follows.

Proposition 8.1. *Let the projectivity $(\mathfrak{T}_g, g) \in PGL(3,q)$ possess the property '$\langle g\rangle$ is isomorphic to $\mathbf{Z}_p$', where p is a prime and suppose that L is the subset of lines in $PG(2,q)$ given by*

$$L = \{\ell^{g^i} \mid i \in \overline{\mathbf{N}}_{p-1}\}.$$

Then the set L is a line if $\ell^g = \ell$ or a set of p lines that is closed under the right action of g otherwise.

Proof The proof follows the same argument as Proposition 7.2, with points x replaced by lines ℓ. □

Lemma 8.2 is included for completeness. Whereas, Theorem 8.3 and Lemmas 8.5 to 8.8 are used throughout this section.

Lemma 8.2. *For $(\mathfrak{T}_g, g) \in PGL(3,q)$, if every distinct orbit that is not a point has prime order p, then $\langle g\rangle \cong \mathbf{Z}_p$. Further, if every distinct subset of lines in $PG(2,q)$ of the form*

$$\{\ell^{g^i} \mid i \in \overline{\mathbf{N}}_{p-1}\}$$

that is not a line has prime order p, then $\langle g\rangle \cong \mathbf{Z}_p$.

Proof If

$$\left|x^{\langle g\rangle}\right| = p,$$

then p is the smallest positive natural number that satisfies $x^{g^p} = x$. If

$$\left|s^{\langle g\rangle}\right| = 1,$$

then $x^g = x$ and by extension $x^{g^p} = x$. Hence, g^p maps every point of $PG(2,q)$ to itself, making $g^p \equiv \mathrm{I}$ in $PGL(3,q)$.

A similar argument for ℓ shows that g maps every line in $PG(2,q)$ to itself; hence, g maps every point of $PG(2,q)$ to itself, making $g^p \equiv \mathrm{I}$ in $PGL(3,q)$. □

8.1.2 Construction

For $(\mathfrak{T}_g, g) \in PGL(3,q)$, where $\langle g\rangle \cong \mathbf{Z}_p$ and p is a prime, Theorem 8.3 and Lemma 8.4 to Lemma 8.8 give a brief overview of the general structure of points and lines in $PG(2,q)$ that are closed under the right action of g. The ideas they present are used in Sections 8.2, 8.3, 8.4, 8.5, 8.6 and 8.7 to help describe the structure of points and lines that are closed under the right action of g for specific instance of p.

Theorem 8.3. *For $(\mathfrak{T}_g, g) \in PGL(3,q)$, where $\langle g\rangle \cong \mathbf{Z}_p$ and p is a prime, Proposition 7.2 and Propositon 8.1 produce the following structure.*

(1) *If $|PG(2,q)| = pM + h$, then there are $pM_1 + h$ points that are closed under the right action of g and M_2 sets of points of order p that are closed under the right action of g, where $M = M_1 + M_2$.*

(2) *If* $|PG(2,q)| = pM + h$, *then there are* $pM_1 + h$ *lines that are closed under the right action of* g *and* M_2 *sets of lines of order* p *that are closed under the right action of* g, *where* $M = M_1 + M_2$.

(3) *If a line* ℓ *in* $PG(2,q)$ *is closed under the right action of* g *and the point* x *is incident with* ℓ, *then every point in the orbit* $x^{\langle g\rangle}$ *is incident with* ℓ. *Hence, if* $q+1 = pN + k$, *then there are* $pN_1 + k$ *points on* ℓ *that are closed under the right action of* g *and* N_2 *sets of points of order* p *that are incident with* ℓ *and closed under the right action of* g, *where* $N = N_1 + N_2$.

(4) *If a point* x *of* $PG(2,q)$ *is closed under the right action of* g *and the line* ℓ *is incident with* x, *then every line in the set*

$$\{\ell^{g^i} \mid i \in \overline{\boldsymbol{N}}_{p-1}\}$$

is incident with x. *Hence, if* $q+1 = pN+k$, *then there are* $pN_1 + k$ *lines through* x *that are closed under the right action of* g *and* N_2 *sets of lines of order* p *that are incident with* x *and closed under the right action of* g, *where* $N = N_1 + N_2$.

Lemma 8.4. *If a line* ℓ *is incident with two points that are closed under the right action of* $(\mathfrak{T}_g, g) \in PGL(3,q)$, *then the line* ℓ *is closed under the right action of* g. *Similarly, if a point* x *is on two lines that are closed under the right action of* $(\mathfrak{T}_g, g) \in PGL(3,q)$, *then the point* x *is closed under the right action of* g.

Proof The proof follows immediately from the incidence structure of points and lines in the projective plane. See [6, Lemma 4.2]. □

Lemma 8.5. *For* $(\mathfrak{T}_g, g) \in PGL(3,q)$, *where* $\langle g\rangle \cong \mathbf{Z}_p$ *and* p *is a prime, if three collinear points* $x_0 = P(X_0), x_1 = P(X_1), x_0 + ax_1 = P(X_0 + aX_1)$ *of* $PG(2,q)$ *are closed under the right action of* g, *then every point on the line that is incident with the points* x_0, x_1 *and* $x_0 + ax_1$ *is closed under the right action of* g.

Proof If $X_0^g = \alpha X_0$, $X_1^g = \beta X_1$ and $(X_0 + aX_1)^g = \gamma(X_0 + aX_1)$, then $(X_0 + aX_1)^g = \alpha X_0 + \beta a X_1$; that is, $\gamma = \alpha = \beta$. Hence, $(X_0 + bX_1)^g = X_0^g + bX_1^g = \alpha X_0 + \alpha b X_1$. □

Note 8.6. In $PG(2,q)$, if the line

$$L(X_0, X_1) = \{P(Z) \mid Z \in \{X_0 + \alpha X_1 \mid \alpha \in GF(q)\} \cup X_1\}$$

through the points $x_0 = P(X_0)$ and $x_1 = P(X_1)$ is not incident with the point $x = P(X)$, then the $q+1$ lines through x are

$$L(X, Z), \forall P(Z) \in L(X_0, X_1).$$

Lemma 8.7. *For* $(\mathfrak{T}_g, g) \in PGL(3,q)$, *where* $\langle g\rangle \cong \mathbf{Z}_p$ *and* p *is a prime, if the three lines* $\ell = L(X, X_1), \ell_0 = L(X, X_0), \ell_a = L(X, X_0 + aX_1)$ *that pass through the point* $x = P(X)$ *are closed under the right action of* g, *then every line through* x *is closed under the right action of* g.

Proof If $\ell^g = \ell$, then $X_1^g = \delta(X + \beta X_1)$. If $\ell_0^g = \ell_0$, then $X_0^g = \delta_0(X + \beta_0 X_0)$. If $\ell_a^g = \ell_a$, then $(X_0 + aX_1)^g = \delta_1(X + \beta_1(X_0 + aX_1)) = (\delta_0 + a\delta)X + \delta_0\beta_0 X_0 + a\delta\beta X_1$. As X, X_0, X_1 are linearly independent, $\delta_1\beta_1 = \delta_0\beta_0 = \delta\beta$.

Let $\ell_b = L(X, X_0 + bX_1)$ be an additional line through the point x. Then

$$(X_0 + bX_1)^g = \delta_0(X + \beta_0 X_0) + a\delta(X + \beta X_1) = (\delta_0 + b\delta)X + \delta_1\beta_1(X_0 + bX_1);$$

that is, $\ell_b^g = \ell_b$. □

Lemma 8.8. *For $(\mathfrak{T}_g, g) \in PGL(3,q)$, where $\langle g\rangle \cong \mathbf{Z}_p$ and p is a prime, if n points of $PG(2,q)$ are closed under the right action of g, then at least $n-1$ of these points are collinear. As there are $q+1$ points on a line, there are at most $q+2$ points that are closed under the right action of g.*

Proof By Proposition 1.71, if g maps each point of a 4-arc to itself, then $g \equiv \mathrm{I}$. If these n points form an (n,r)-arc, where $r < n-1$, then $n \geq r+2$ and the set of n points contains a 4-arc by Proposition 7.3; hence, $g \equiv \mathrm{I}$, a contradiction to $\langle g\rangle \cong \mathbf{Z}_p$. □

8.2 $p = 2$

Note 8.9. It is stated in [6, Theorem 4.3] that for a collineation $\mathfrak{T}$ of order 2 in the projective plane, every point that is fixed by $\mathfrak{T}$ is incident with a line that is fixed by $\mathfrak{T}$ and every line that is fixed by $\mathfrak{T}$ is incident with a point that is fixed by $\mathfrak{T}$.

This section goes further and describes the structure of points and lines that are closed under the right action of a projectivity of order 2 in $PG(2,q)$ for the cases 'q is an odd prime' and 'q is an odd prime power'. The case of $q = 2^i$ is described in Sections 8.4 and 8.5.

Lemma 8.10. *Let ℓ ba a line in $PG(2, q > 2)$ that is closed under the right action of g, where $(\mathfrak{T}_g, g) \in PGL(3,q)$, $\langle g\rangle \cong \mathbf{Z}_2$ and $(\delta g)^2 = \mathrm{I}$ in $GL(3,q)$, for some $\delta \in GF(q)$. Then ℓ is incident with two points that are closed under the right action of g.*

Proof If the line ℓ is incident with more than two points that are closed under the right action of g, then the proof is complete. Otherwise, ℓ is incident with two points $x = P(X)$ and $y = P(Y)$ that satisfy $X^{\delta g} = \alpha Y$ and $Y^{\delta g} = \beta X$ and

$$X^{(\delta g)^2} = \alpha Y^{\delta g} = \alpha\beta X = X,$$

since $(\delta g)^2 = \mathrm{I}$ in $GF(q)$. Hence, $\beta = \frac{1}{\alpha}$ and the two points $x + \alpha y$ and $x - \alpha y$ are closed under right of g. □

Theorem 8.11. *The projective plane $PG(2,q)$, where q is an odd prime, has $\frac{q^2-1}{2}$ distinct sets of points and lines of order 2 and $q+2$ distinct points and lines, all of which are closed under the right action of g, where $(\mathfrak{T}_g, g) \in PGL(3,q)$ and $\langle g\rangle \cong \mathbf{Z}_2$. Further, the $q+2$ points that are closed under the right action of g comprise $q+1$ collinear points and one other point that is the intersection of $q+1$ lines, each of which is closed under the right action of g.*

Proof For $\langle g \rangle \cong \mathbf{Z}_2$, every point $x_0 = P(X_0)$ of $PG(2,q)$ satisfies $X_0^g = \alpha X_0$ or $X_0^g = \alpha X_1$, where $P(X_1) \neq P(X_0)$ and $X_1^g = \beta X_0$.

As q is an odd prime, q^2+q+1 is odd and $q+1$ is even. As q^2+q+1 is odd, $PG(2,q)$ contains at least one point $x_0 = P(X_0)$ and one line ℓ_0 that are closed under the right action of g by Theorem 8.3. As $q+1$ is even, every point that is closed under the right action of g is incident with an even number of lines that are closed under the right action of g by Theorem 8.3. As $q+1$ is even, every line that is closed under the right action of g is incident with an even number of points that are closed under the right action of g by Theorem 8.3.

Let $X_0^g = \alpha X_0$. Then $X_0^{g^2} = \alpha^2 X_0$ and as $g^2 = \gamma \mathrm{I}$ in $GF(q)$, it follows that $\gamma = \alpha^2$. Hence, Lemma 8.10 applies, with $\delta = \frac{1}{\alpha}$.

If x_0 and ℓ_0 are incident, then, as $q+1$ is even the line ℓ_0 is incident with a second point x_1 that is closed under the right action of g and the point x_0 is incident with a second line ℓ_1 that is closed under the right action of g. As $q+1$ is even, the point x_1 is incident with a second line ℓ_2 that is closed under the right action g. The point intersecting the lines ℓ_1 and ℓ_2 is closed under the right action of g and is distinct from the points x_0 and x_1.

If x_0 and ℓ_0 are not incident, then the line ℓ_0 is incident with two points x_1 and x_2 that are closed under the right action of g by Lemma 8.10. The line through the points x_0 and x_1 and the line through the points x_0 and x_2 are closed under the right action of g.

Hence, $PG(2,q)$ possesses three non-collinear points $x_0 = P(X_0), x_1 = P(X_1), x_2 = P(X_2)$ that satisfy $X_0^g = \alpha X_0$, $X_1^g = \beta X_1$ and $X_2 = \epsilon X_2$, where $\alpha^2 = \beta^2 = \epsilon^2 = \frac{1}{\delta^2}$. The equation $t^2 = 1$ has two solutions in $GF(q)$, so at least two of the values α, β, ϵ are not unique. Assume without loss of generality that $\alpha = \beta$, then

$$(X_0 + aX_1)^g = X_0^g + aX_1^g = \alpha(X_0 + aX_1),$$

for all $a \in \{1, \ldots, p-1\}$; that is, every point on the line through the points x_0 and x_1 is closed under the right action of g. A line through the point x_2 is incident with exactly two points that are closed under the right action of g and as such is itself closed under the right action of g.

No additional points are closed under the right action of g by Lemma 8.8. □

Corollary 8.12. *The projective plane $PG(2,q)$, where q is an odd prime power, either has the structure specified in Theorem 8.11 or there are exactly three points and three lines that are closed under the right action of g, where $(\mathfrak{T}_g, g) \in PGL(3,q)$ and $\langle g \rangle \cong \mathbf{Z}_2$. Further, these three points are not collinear and the three lines are their bisecants.*

Proof The existence of three such points and lines is demonstrated in the proof of Theorem 8.11 and as q is not a prime it is not possible to discard this case as it is in that proof. □

Note 8.13. For the special case of $q = 2^i$, see Sections 8.4 and 8.5.

8.3 $p = 3$

8.3.1 $q = 3N + 2$

Theorem 8.14. *In $PG(2,q)$, where $q = 3N+2$ and $N > 0$, there is exactly one point x and one line ℓ that are closed under the right action of g, where $(\mathfrak{T}_g, g) \in PGL(3,q)$ and*

$\langle g\rangle \cong \mathbf{Z}_3$. Further, x and ℓ are not incident and all other points and lines are in subsets of order 3 that are closed under the right action of g.

Proof If $q = 3N+2$ and $q+1 = 3N$, then $q^2+q+1 = 3M+1$. As $|PG(2,q)| = 3M+1$, there is at least one point and one line that are closed under the right action of g and there are $3h_1+1$ points and $3h_2+1$ lines that are closed under the right action of g by Theorem 8.3.

As $q+1 = 3N$, if a point is closed under the right action of g, then it is incident with $3N_1$ lines that are closed under the right action of g by Theorem 8.3. As $q+1 = 3N$, if a line is closed under the right action of g, then it is incident with $3N_2$ points that are closed under the right action of g by Theorem 8.3.

If $h_1 > 0$, then, by Lemma 8.8, there are at least three points on a line ℓ that are closed under the right action of g. By Lemma 8.5, all points on the line ℓ are closed under the right action of g; this gives $h_1 = N$. As $|PG(2,q)| = 3M+1$, there is one additional point x that is closed under the right action of g by Theorem 8.3; this gives the maximum number of $q+2$ points that are closed under the right action of g. A line through the point x is incident with exactly two points that are closed under the right action of g, a contradiction to $q+1 = 3N$; hence, $h_1 = 0$.

If $h_2 > 0$, then there are at least three lines through x that are closed under the right action of g by Theorem 8.3. As $q+1 = 3N$, each of these three lines is incident with at least three points that are closed under the right action of g, a contradiction to $h_1 = 0$. Similarly, if x is on ℓ, then at least three points on ℓ are closed under the right action of g, a contradiction to $h_1 = 0$; hence, $h_2 = 0$. □

8.3.2 $q = 3N+1$

Theorem 8.15. *In $PG(2,q)$, where $q = 3N+1$ and $N > 0$, there are $3h$ points and $3h$ lines all of which are closed under the right action of g, where $(\mathfrak{T}_g, g) \in PGL(3,q)$ and $\langle g\rangle \cong \mathbf{Z}_3$. The possible values of h are $h = 0$, $h = 1$ or $h = N+1$. All other points and lines are in subsets of order 3 that are closed under the right action of g.*

Proof If $q = 3N+1$ and $q+1 = 3N+2$, then $q^2+q+1 = 3M$. As $|PG(2,q)| = 3M$, there are $3h_1$ points and $3h_2$ lines that are closed under the right action of g by Construction 8.3.

As $q+1 = 3N+2$, if a point is closed under the right action of g, then it is incident with $3N_1+2$ lines that are closed under the right action of g by Theorem 8.3. As $q+1 = 3N+2$, if a line is closed under the right action of g, then it is incident with $3N_2+2$ points that are closed under the right action of g by Theorem 8.3.

If $h_1 = 0$ or $h_2 = 0$, then there are no points or lines that are closed under the right action of g.

If $h_1 = 1$ or $h_2 = 1$, then there are three non-collinear points that are closed under the right action of g and the three bisecants of this trio are closed under the right action of g.

If $h_1 > 1$ or $h_2 > 1$, then, by Lemma 8.8, there are at least three points on a line ℓ that are closed under the right action of g. Hence, all points on the line ℓ are closed under the right action of g by Lemma 8.5; this gives $h_1 = N+1$. As $q+1 = 3N+2$, there is one additional point x that is closed under the right action of g. If a line is incident with

the point x, then it is incident with two points that are closed under the right action of g and as such is itself closed under the right action of g; hence, $h_2 = N + 1$. This structure is consistent with $q + 1 = 3N + 2$. □

Note 8.16. For the special case of $q = 3^i$, see Section 8.4.

8.4 $p > 3$

If $q = pN+k$ and $q+1 = pN+k+1$, where $1 \leq k < p-1$, then $q^2+q+1 = pM+k^2+k+1$.

Note 8.17. Lemma 8.8 suggests that there are at most six possibilities for the number of points that are closed under the right action of g, where $(\mathfrak{T}_g, g) \in PGL(3, q)$, $\langle g \rangle \cong \mathbf{Z}_p$, p is a prime and $q > p > 3$. These are as follows.

(i) No points are closed under the right action of g.

(ii) Exactly one point is closed under the right action of g.

(iii) Exactly two points are closed under the right action of g.

(iv) Exactly three non-collinear points are closed under the right action of g.

(v) All the points on some line are closed under the right action of g.

(vi) All the points on some line and some additional point are closed under the right action of g.

It is known from [6, Theorem 4.9] that if every point on some line is closed under the right action of g, then every line through some point is closed under the right action of g, where $(\mathfrak{T}_g, g) \in PGL(3, q)$. Dually, if every line through some point is closed under the right action of g, then every point on some line is closed under the right action of g. By Lemma 8.18, the point closed linewise and the line closed pointwise under the right action of g are not incident.

Lemma 8.18. *In $PG(2, q)$, if every point on some line is closed under the right action of g, then there is an additional point that is closed under the right action of g, where $(\mathfrak{T}_g, g) \in PGL(3, q)$, $\langle g \rangle \cong \mathbf{Z}_p$, p is a prime and $q > p > 3$. Further, every line through this additional point is closed under the right action of g.*

Proof As $k + 1 > 1$, if x is a point that is closed under the right action of g and x is on a line that is closed under the right action of g, then the point x is on at least two lines that are closed under the right action of g by Theorem 8.3.

Hence, if there is a line ℓ such that every point on ℓ is closed under the right action of g, then the point $x_0 \in \ell$ is on a line $\ell_0 \neq \ell$ that is closed under the right action of g and the point $x_1 \in \ell$ is on a line $\ell_1 \neq \ell$ that is closed under the right action of g.

The point intersecting the lines ℓ_0 and ℓ_1 is not on the line ℓ and it is closed under the right action of g. □

8.4.1 p divides k^2+k+1

Theorem 8.19. *In $PG(2,q)$, if p divides k^2+k+1, then no point or line is closed under the right action of g, where $(\mathfrak{T}_g, g) \in PGL(3,q)$, $\langle g\rangle \cong \mathbf{Z}_p$, $p>3$ is a prime and $q=pn+k$ with $n>0$. All points and lines are therefore in subsets of order p that are closed under the right action of g.*

Proof If p divides k^2+k+1, then ph points are closed under the right action of g.

Suppose $h>0$.

As $p>3$, there is a line ℓ through at least $p-1>2$ points that are closed under the right action of g by Lemma 8.8. All $pn+k+1$ points on the line ℓ are closed under the right action of g by Lemma 8.5.

As $k>1$, if a point is both closed under the right action of g and on a line that is closed under the right action of g, then it is on at least three lines that are closed under the right action of g by Theorem 8.3. Hence, a point $x_0 \in \ell$ is on at least two lines $\ell_0 \neq \ell$ and $\ell_1 \neq \ell$ that are closed under the right action of g and a point $x_1 \in \ell$ is on a line $\ell_2 \neq \ell$ that is closed under the right action of g.

The point intersecting the lines ℓ_0 and ℓ_2 and the point intersecting the lines ℓ_1 and ℓ_2 are distinct, not on ℓ and closed under the right action of g, a contradiction to Lemma 8.8; hence, $h=0$.

If a line ℓ is closed under the right action of g, then p lines are closed under the right action of g. The intersection of two of these lines is closed under the right action of g and $h>0$, a contradiction. □

Note 8.20. It is immediate that, if no point or line is closed under the right action of g, where $(\mathfrak{T}_g, g) \in PGL(3,q)$ and $\langle g\rangle \cong \mathbf{Z}_p$, then p divides k^2+k+1.

8.4.2 $q=pN+1$, $q+1=pN+2$ or $k=1$

Lemma 8.21. *In $PG(2,q)$, if $k=1$, then there are either exactly three non-collinear points that are closed under the right action of g or every point on some line is closed under the right action of g, where $(\mathfrak{T}_g, g) \in PGL(3,q)$, $\langle g\rangle \cong \mathbf{Z}_p$, p is a prime and $q>p>3$.*

Proof If $k=1$, then $k^2+k+1=3$ and as $p>3$, there must exists at least three points and three lines that are closed under the right action of g. Either, these three points are non-collinear or every point on some line is closed under the right action of g by Lemma 8.5 in which case there is an additional point that is closed under the right action of g by Lemma 8.18. □

Lemma 8.22. *In $PG(2,q)$, if there are exactly three points and three lines that are closed under the right action of g, then $k=1$, where $(\mathfrak{T}_g, g) \in PGL(3,q)$, $\langle g\rangle \cong \mathbf{Z}_p$, p is a prime and $q>p>3$. Further, the three lines are the bisecants of the three points.*

Proof If there are exactly three points and three lines that are closed under the right action of g, then these three points must be non-collinear by Lemma 8.5. A line through any two of these points must consist of exactly $pN+2$ points by Theorem 8.3; hence, $k=1$. □

Lemma 8.23. *In $PG(2,q)$, if every point on a line ℓ is closed under the right action of g, then $k=1$, where $(\mathfrak{T}_g, g) \in PGL(3,q)$, $\langle g\rangle \cong \mathbf{Z}_p$, p is a prime and $q > p > 3$.*

Proof By Lemma 8.18, there is at least one additional point that is closed under the right action of g.

Suppose $k+1 > 2$. If a point is closed under the right action of g and on a line that is closed under the right action of g, then it is on at least three lines that are closed under the right action of g by Theorem 8.3.

Hence, if there is a line ℓ such that every point on that line is closed under the right action of g, then the point $x_0 \in \ell$ is on at least two lines $\ell_0 \neq \ell$ and $\ell_1 \neq \ell$ that are closed under the right action of g and the point $x_1 \in \ell$ is on a line $\ell_2 \neq \ell$ that is closed under the right action of g.

The point intersecting the lines ℓ_0 and ℓ_2 and the point intersecting the lines ℓ_1 and ℓ_2 are distinct, not on ℓ and closed under the right action g, a contradiction to Lemma 8.8. Hence, $k=1$. □

8.4.3 $k^2+k+1 = ph+1$ or $k = p-1$

Lemma 8.24. *In $PG(2,q)$, there is exactly one point x and one line ℓ that are closed under the right action of g if and only if $k = p-1$, where $(\mathfrak{T}_g, g) \in PGL(3,q)$, $\langle g\rangle \cong \mathbf{Z}_p$, p is a prime and $q > p > 3$. This point and line are not incident.*

Proof There is exactly one point and one line that are closed under the right action of g only if $k^2+k+1 = ph+1$.

There is exactly one point and one line that are closed under the right action of g if $k^2+k+1 = ph+1$; because if $k^2+k+1 = ph+1$ and there are at least $p+1 > 4$ points that are closed under the right action of g, then at least three of these points are collinear by Lemma 8.8 and all points on this line are closed under the right action of g by Lemma 8.5. Hence, $k=1$ by Lemma 8.23, a contradiction to $k = p-1$.

If $k^2+k+1 = ph+1$, then $k(k+1) = ph$. Hence, p must divide k or $k+1$; as $k < p$, it follows that $k = p-1$. If $k = p-1$, then $k^2+k+1 = p^2-p+1$.

If the point x and line ℓ are incident, then as $q+1 = pN+p$, the line ℓ is incident with $p > 3$ points that are closed under the right action of g; hence, every point on ℓ is closed under the right action of g by Lemma 8.5 and $k=1$ by Lemma 8.23, a contradiction to $k = p-1$. □

8.4.4 Two points

Lemma 8.25. *In $PG(2,q)$, it is not possible for exactly two points to be closed under the right action of g, where $(\mathfrak{T}_g, g) \in PGL(3,q)$, $\langle g\rangle \cong \mathbf{Z}_p$, p is a prime, and $q > p > 3$*

Proof If exactly two points are closed under the right action of g, then the line joining them contains exactly two points that are closed under the right action of g and as such is itself closed under the right action of g; that is, $k+1 = 2$ or $k = 1$. Hence, $k^2+k+1 = 3$; and as $p > 3$, there are at least three points that are closed under the right action of g; a contradiction. □

8.5 $q = p^i$, $i > 0$

Lemma 8.26. *In $PG(2,p^i)$, if ℓ is a line through two points x_1 and x_2 that are closed under the right action of g, then every point on the line ℓ is closed under the right action of g, where $(\mathfrak{T}_g, g) \in PGL(3,p^i)$, $\langle g\rangle \cong \mathbf{Z}_p$ and p is a prime.*

Proof If the points x_1 and x_2 are closed under the right action of g, then ℓ is closed under the right action of g. As $q+1 = p^i+1$, the line ℓ is incident with $ph+1$ points that are closed under the right action of g by Theorem 8.3. As $p \geq 2$, the line ℓ is incident with at least 3 points that are closed under the right action of g; hence, every point on the line ℓ is closed under the right action of g by Lemma 8.5. □

Lemma 8.27. *In $PG(2,p^i)$, if x is a point on two lines ℓ_1 and ℓ_2 that are closed under the right action of g, then every line through the point x is closed under the right action of g, where $(\mathfrak{T}_g, g) \in PGL(3,p^i)$, $\langle g\rangle \cong \mathbf{Z}_p$ and p is a prime.*

Proof If the lines ℓ_1 and ℓ_2 are closed under the right action of g, then x is closed under the right action of g. As $q+1 = p^i+1$, the point x is incident with $ph+1$ lines that are closed under the right action of g by Theorem 8.3. As $p \geq 2$, the point x is incident with at least 3 lines that are closed under the right action of g; hence, every line through the point x is closed under the right action of g by Lemma 8.7. □

Theorem 8.28. *In $PG(2,p^i)$, either all points on some line are closed under the right action of g or exactly one point x is closed under the right action of g, where $(\mathfrak{T}_g, g) \in PGL(3,q)$, $\langle g\rangle \cong \mathbf{Z}_p$ and p is a prime. Similarly, either all lines through some point are closed under the right action of g or exactly one line ℓ is closed under the right action of g. Further x and ℓ are incident.*

Proof As $q^2+q+1 = p^{2i}+p^i+1$, there is at least one point x and one line ℓ that are closed under the right action of g by Theorem 8.3.

If an additional point x_0 is closed under the right action of g and ℓ_0 is the line through the points x and x_0, then every point on the line ℓ_0 is closed under the right action of g by Lemma 8.26.

If a second additional point x_1 is closed under the right action of g, then every line through x_1 is incident with two points that are closed under the right action of g. Hence, every point of $PG(2,q)$ is closed under the right action of g by Lemma 8.26; that is, $g \equiv \mathrm{I}$, a contradiction to $\langle g\rangle \cong \mathbf{Z}_p$.

If an additional line ℓ_0 is closed under the right action of g, then every line through the intersection of the lines ℓ and ℓ_0 is closed under the right action of g by Lemma 8.27.

If a second additional line ℓ_1 is closed under the right action of g, then every point on ℓ_1 is incident with two lines that are closed under the right action of g. Hence, every line in $PG(2,q)$ is closed under the right action of g, by Lemma 8.27, as such every point of $PG(2,q)$ is closed under the right of g; that is, $g \equiv \mathrm{I}$, a contradiction to $\langle g\rangle \cong \mathbf{Z}_p$. □

8.6 $p = q + 1$

This work is concerned with prime values of p. Hence, if p is prime, then q is a 2 power.

Lemma 8.29. *In $PG(2, 2^i)$, if a point is closed under the right action of g, then either it is incident with $q + 1$ lines that are closed under the right action of g or it is not incident with any line that is closed under the right action of g, where $(\mathfrak{T}_g, g) \in PGL(3, 2^i)$, $\langle g \rangle \cong \mathbf{Z}_p$ and p is a prime. Similarly, if a line is closed under the right action of g, then either it is incident with $q + 1$ points that are closed under the right action of g or it is not incident with any point that is closed under the right action of g.*

Proof By Theorem 8.3, if a point that is closed under the right action of g is incident with a line that is closed under the right action of g, then it is incident with $p = q + 1$ lines that are closed under the right action of g. Similarly, if a line that is closed under the right action of g is incident with a point that is closed under the right action of g, then it is incident with $p = q + 1$ points that are closed under the right action of g. □

Theorem 8.30. *In $PG(2, 2^i)$, one point x and one line ℓ are closed under the right action of g, where $(\mathfrak{T}_g, g) \in PGL(3, 2^i)$, $\langle g \rangle \cong \mathbf{Z}_p$ and p is a prime. Further, x and ℓ are not incident.*

Proof As $(2^i)^2 + 2^i + 1 = p^2 - p + 1$, there is at least one point x and one line ℓ that are closed under the right action of g.

If x and ℓ are incident, then every point on ℓ and every line through x is closed under the right action of g by Lemma 8.29. Every point on every line through x is also closed under the right action of g by Lemma 8.29; that is, every point of $PG(2, 2^i)$ is closed under the right action of g. This is a contradiction to Lemma 8.8. Hence, x and ℓ are not incident.

If x_0 is a point that is not on ℓ and closed under the right action of g, then all points on the line ℓ_0 through x and x_0 are closed under the right action of g by Lemma 8.29. The point intersecting the lines ℓ and ℓ_0 is closed under the right action g; hence, every point on ℓ is closed under the right action of g by Lemma 8.29. This is a contradiction to Lemma 8.8.

If x_0 is a point on ℓ that is closed under the right action of g, then every point on ℓ is closed under the right action of g by Lemma 8.29. Every point on every line through x is closed under the right action of g by Lemma 8.29; that is, every point of $PG(2, 2^i)$ is closed under the right action of g. This is a contradiction to Lemma 8.8.

If ℓ_0 is a line that is closed under the right action of g, then the point intersecting the lines ℓ and ℓ_0 is closed under the right action of g. Hence, every point on ℓ and every point on ℓ_0 is closed under the right action of g by Lemma 8.29. This is a contradiction to Lemma 8.8. □

8.7 $p = q + k,\ k > 1$

Theorem 8.31. *In $PG(2, q)$, no points and no lines are closed under the right action of g, where $(\mathfrak{T}_g, g) \in PGL(3, q)$, $\langle g \rangle \cong \mathbf{Z}_p$, p is a prime and $p = q + k$.*

Proof If x is a point that is closed under the right action of g, then, by Theorem 8.3, every line through x is closed under the right action of g; otherwise, there are $q+k > q+1$ distinct lines through x. Likewise, every point on every line through x is closed under the right action of g by Theorem 8.3; that is, every point of $PG(2,q)$ is closed under the right action of g. This is a contradiction to Lemma 8.8.

If ℓ is a line that is closed under the right action of g, then, by Theorem 8.3, every point on ℓ is closed under the right action of g; otherwise, there are $q+k > q+1$ distinct points on ℓ. Likewise, every line through a point on ℓ is closed under the right action of g by Theorem 8.3; that is, every line in $PG(2,q)$ is closed under the right action of g and this is equivalent to every point of $PG(2,q)$ being closed under the right action of g. This is a contradiction to Lemma 8.8. □

Corollary 8.32. *For $p = q + k$, where p is a prime and $k > 1$, there exists a projectivity $(\mathfrak{T}_g, g) \in PGL(3,q)$, where $\langle g\rangle \cong \mathbf{Z}_p$ only if $k^2 - k + 1 = ph$.*

Proof As, $q^2+q+1 = pM+k^2-k+1$, if no points and no lines are closed under the right action of g, then $k^2 - k + 1 = ph$; so, the projectivity g exists only if $k^2 - k + 1$ by Theorem 8.31 □

8.8 Results

The results of Sections 8.4 to 8.7 give Theorem 8.33 and Corollary 8.34.

Theorem 8.33. *There are four possibilities for the number of points that are closed under the right action of g, where $(\mathfrak{T}_g, g) \in PGL(3,q)$, $\langle g\rangle \cong \mathbf{Z}_p$, p is a prime, $q > p > 3$ and $q^2 + q + 1 = pM + k^2 + k + 1$.*

(i) *No points are closed under the right action of g if and only if p divides $k^2 + k + 1$.*

(ii) *Exactly one point is closed under the right action of g if and only if $k = p - 1$.*

(iii) *Exactly three non-collinear points are closed under the right action of g only if $k = 1$.*

(iv) *All the points on some line and some additional point are closed under the right action of g only if $k = 1$.*

The condition $k = 1$ is satisfied only if exactly three non-collinear points are closed under the right action or all the points on some line and some additional point are closed under the right action of g.

Further, all other points are in subsets of order p that are closed under the right action of g and generated by repeated applications of g to a single point.

Corollary 8.34. *For $q > p > 3$, where p is a prime, there exists a projectivity $(\mathfrak{T}_g, g) \in PGL(3,q)$, where $\langle g\rangle \cong \mathbf{Z}_p$ only if $q^2 + q + 1 = pM$, $q = pN + 1$ or $q = pN + p - 1$.*

Proof By Theorem 8.33, there exists such a projectivity only if $k^2 + k + 1 = ph$, $k = 1$ or $k = p - 1$. □

Note 8.35. Corollary 8.32, Corollary 8.34, $q = p^i$ and $p = q + 1$ give all possible primes p for which there exists a projectivity $g \in PGL(3,q)$, where $\langle g\rangle \cong \mathbf{Z}_p$, for a given prime power q.

8.8.1 Connection to $GL(3,q)$

Note 8.36. For p a prime, if $g \in GL(3,q)$ is such that $g^p = \alpha\mathrm{I}$, then $g^{-1} = \frac{1}{\alpha}g^{p-1}$; hence $g \in PGL(3,q)$ and $g^p \equiv \mathrm{I}$ in $PGL(3,q)$. It follows immediately that the existence of such a $g \in GL(3,q)$ is dependent on the consistency of the structure of sets of points and lines in $PG(2,q)$ that are generated under the right action of the matrix g.

Theorem 8.37. *For $q > p > 3$, where p is a prime, there exists a matrix g over $GF(q)$ that satisfies $g^p = \alpha\mathrm{I}$, $\alpha \neq 0$, only if $q^2+q+1 = pM$, $q = pN+1$ or $q = pN+p-1$.*

Proof If $g^p = \alpha\mathrm{I}$, then $g^{-1} = \frac{1}{\alpha}g^{p-1}$; hence, $(\mathfrak{T}_{\beta g}, \beta g) \in PGL(3,q)$. As $(\beta g)^p = \beta^p g^p = \beta\alpha\mathrm{I} \equiv \mathrm{I}$ in $PGL(3,q)$, it follows that $\langle \beta g\rangle \cong \mathbf{Z}_p$. By Corollary 8.34, $q^2+q+1 = pM$, $q = pN+1$ or $q = pN+p-1$. □

Theorem 8.38. *For $p = q+k$, where p is a prime and $k > 1$, there exists a matrix g over $GF(q)$ that satisfies $g^p = \alpha\mathrm{I}$, $\alpha \neq 0$ only if $q^2+q+1 = pM'$.*

Proof If $g^p = \alpha\mathrm{I}$, then $g^{-1} = \frac{1}{\alpha}g^{p-1}$; hence, $(\mathfrak{T}_{\beta g}, \beta g) \in PGL(3,q)$. As $(\beta g)^p = \beta^p g^p = \beta\alpha\mathrm{I} \equiv \mathrm{I}$ in $PGL(3,q)$, it follows that $\langle \beta g\rangle \cong \mathbf{Z}_p$. By Corollary 8.32, $k^2-k+1 = ph$; hence, $q^2+q+1 = pM+ph$. □

The matrices

$$\mathrm{I} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \mathrm{J} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \mathrm{K} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

are elements of $GL(3,q)$, for all prime powers q. The element J has order 2 and the element K has order 3.

As

$$\begin{aligned} |GL(3,q)| &= (q^3-q^2)(q^3-q)(q^3-1) \\ &= (q-1)^3q^3(q+1)(q^2+q+1), \end{aligned}$$

if a prime p divides $|GL(3,q)|$, then one of the following holds:

$$p \mid q^2+q+1, \tag{8.1}$$
$$p \mid q-1, \tag{8.2}$$
$$p \mid q, \tag{8.3}$$
$$p \mid q+1, \tag{8.4}$$

by Sylow's Theorems. Property (8.1) is equivalent to $q^2+q+1 = pM$ in Theorem 8.37 and Theorem 8.38. Property (8.2) is equivalent to $q = pN+1$ and property (8.4) is equivalent to $q = pN+p-1$ in Theorem 8.37. The fact that the primes 2 and 3 must always divide $|GL(3,q)|$ is shown in (8.2), (8.3) and (8.4).

Note 8.39. The prime p used in Theorem 8.37 and Theorem 8.38 is bounded above by q^2+q+1.

8.9 Application to (n,r)-arcs

Let S be an (n,r)-arc in $PG(2,q)$ that is stabilized by a projectivity that is induced by a matrix g with the property '$g^p \equiv$ I', where p is a prime.

8.9.1 Restrictions on the form of n

As the previous sections give a complete description of the points that are closed under the right action of g, for all possible configurations of p and q and as all points in S are either closed under the right action of g or generate subsets of order p that are closed under the right action of g, the following restrictions can be placed on n.

$p = 3$

If $q = 3N + 2$, then $n = \alpha p$ or $n = 3\alpha + 1$. If $q = 3N + 1$ and $h = 0$ in Theorem 8.15, then $n = 3\alpha$. If $q = 3N + 1$ and $h \neq 0$ in Theorem 8.15, then $n = 3\alpha + i$, where $i \in \{0, 1, 2\}$.

$q > p > 3$

If $p \mid q^2 + q + 1$, then $n = \alpha p$. If $p \mid q + 1$, then $n = \alpha p + i$, where $i \in \{0, 1\}$. If $p \mid q - 1$, then in case (iii) of Theorem 8.33, $n = \alpha p + i$, where $i \in \{0, 1, 2, 3\}$. If $p \mid q - 1$, then in case (iv) of Theorem 8.33, $n = \alpha p + i$, where $i \in \{0, 1, \ldots, min(r + 1, p - 1)\}$.

$q = p^i$

If $q = p^i$ and exactly one point is closed under the right action of g, then $n = \alpha p + i$, where $i = \{0, 1\}$; otherwise if every point on some line is closed under the right action of g, then $n = \alpha p + i$, where $i = \{0, 1, \ldots, min(r, p - 1)\}$.

$p = q + 1$

If $p = q + 1$, then $n = \alpha p + i$, where $i = \{0, 1\}$.

$p = q + k$

If $p = q + k$, then $n = \alpha p$.

Bibliography

[1] R.B.J.T. Allenby, *Rings, Fields and Groups An Introduction to Abstract Algebra (Second Edition)*, Butterworth Heinemann, 1991.

[2] S. Ball and J.W.P. Hirschfeld, *Bounds on* (n, r)*-arcs and their application to linear codes*, Finite Fields Appl. **11** (2005), 326–336.

[3] K. Coolsaet and H. Sticker, *A full classification of the complete* k*-arcs of* $PG(2, 23)$ *and* $PG(2, 25)$, J. Combin. Des. **17** (2009), 459–477.

[4] K. Coolsaet and H. Sticker, *The complete* k*-arcs of* $PG(2, 27)$ *and* $PG(2, 29)$, J. Combin. Des. **19** (2011), 111–130.

[5] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields (Second Edition)*, Clarendon Press, Oxford, 1998.

[6] D.R. Hughes and F.C. Piper, *Projective Planes*, Springer, 1973.

[7] G. Kéri, *Types of superregular matrices and the number of* n*-arcs and complete* n*-arcs in* $\mathrm{PG}(2, q)$, J. Combin. Des. **14** (2006), 363–390.

[8] G. Kéri, *Correction to: "Types of superregular matrices and the number of* n*-arcs and complete* n*-arcs in* $\mathrm{PG}(r, q)$*"*, J. Combin. Des. **16** (2008), 262.

[9] W. Ledermann and A.J. Weir, *Introduction to Group Theory (Second Edition)*, Addison Wesley Longman Limited, 1996.

[10] S. Marcugini, A. Milani and F. Pambianco, *Maximal* $(n, 3)$*-arcs in* $PG(2, 11)$, Discrete Mathematics. **208/209** (1999), 421–426.

[11] S. Marcugini, A. Milani and F. Pambianco, *Classification of the* $(n, 3)$*-arcs in* $PG(2, 7)$, J. Geom. **80** (2004), 179–184.

[12] J.J. Rotman, *An Introduction to the Theory of Groups*, Allyn and Bacon, Inc, 1984.

[13] I. Stewart, *Galois Theory (Third Edition)*, Chapman & Hall/CRC Mathematics, 2004.

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