Bounds for complete arcs in finite projective planes

E. V. D. Pichanick

Submitted for the degree of Doctor of Philosophy

University of Sussex

January 2016

Declaration

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

Signature:

Author’s name:

UNIVERSITY OF SUSSEX

E. V. D. PICHANICK, SUBMITTED FOR DOCTOR OF PHILOSOPHY

Bounds for complete arcs in finite projective planes

Abstract

This thesis uses algebraic and combinatorial methods to study subsets of the Desarguesian plane $\Pi_q = \mathrm{PG}(2, q)$. Emphasis, in particular, is given to complete (k, n)-arcs and plane projective curves. Known Diophantine equations for subsets of $\mathrm{PG}(2, q)$, no more than n of which are collinear, have been applied to k-arcs of arbitrary degree. This yields a new lower bound for complete (k, n)-arcs in $\mathrm{PG}(2, q)$ and is a generalization of a classical result of Barlotti. The bound is one of few known results for complete arcs of arbitrary degree and establishes new restrictions upon the parameters of associated projective codes. New results governing the relationship between $(k, 3)$-arcs and blocking sets are also provided. Here, a sufficient condition ensuring that a blocking set is induced by a complete $(k, 3)$-arc in the dual plane Π_q^* is established and shown to complement existing knowledge of relationships between k-arcs and blocking sets. Combinatorial techniques analyzing $(k, 3)$-arcs in suitable planes are then introduced. Utilizing the numeric properties of non-singular cubic curves, plane $(k, 3)$-arcs satisfying prescribed incidence conditions are shown not to attain existing upper bounds. The relative sizes of $(k, 3)$-arcs and non-singular cubic curves are also considered. It is conjectured that $m_3(2, q)$, the size of the largest complete $(k, 3)$-arc in $\mathrm{PG}(2, q)$, exceeds the number of rational points on an elliptic curve. Here, a sufficient condition for its positive resolution is given using combinatorial analysis. Exploiting its structure as a $(k, 3)$-arc, the elliptic curve is then considered as a method of constructing cubic arcs and results governing completeness are established. Finally, classical theorems relating the order of the plane Π_q to the existence of an elliptic curve with a specified number of rational points are used to extend theoretical results providing upper bounds to $t_3(2, q)$, the size of the smallest possible complete $(k, 3)$-arc in $\mathrm{PG}(2, q)$.

Acknowledgements

I dedicate this work to my mother without whose unquestioning support and encouragment mathematics would have remained a distant dream. I hope to emulate your selfless example of care and concern for others even when this has proved to be at great cost to yourself. You have always been my most trusted guide and mentor. To my brother; we always tried to learn together and I hope to once more. We who wander are not always lost. To Rui and Chuck, you are and always will be our closest family. I thank Professor James Hirschfeld who has, throughout my studies, availed his help with a fatherly hand. He has shown patience and understanding of the difficulties with which my family has struggled. I also thank those at Sussex whose friendship has helped me to continue with this work. I thank Christof, Haidar, Ansgar, Nima and Christophe for their care, their concern and their support during these years as well as their valued friendship. I thank Christof and Haidar for their guidance and give thanks to Ansgar for his patience during this past year. I thank Martin for his support and friendship and count myself fortunate to have shared an office with him, an exemplar of dignity and grace. I also thank Giannis for his friendship, his humour and his wonderful candour during many an entertaining discussion.

Contents

List of Tables

Chapter 1

Introduction and background

1.1 Introduction to projective spaces

Definition 1.1 (Relation)**.** An n-ary *relation* on the sets $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n$ is a non-empty subset $\mathcal{R}$ of the n-fold Cartesian product $\mathcal{F} = \prod_{i=1}^{n} \mathcal{F}_i$. The ordered n-tuple $\alpha = (f_1, \ldots, f_n)$ satisfies the relation $\mathcal{R}$ if $\alpha \in \mathcal{R}$ and, if $n = 2$, $\mathcal{R}$ is a *binary* relation. Here, $a\mathcal{R}b$ is often written for the ordered pair $(a, b) \in \mathcal{R}$.

Definition 1.2 (Geometry, [11])**.** A *geometry* is a non-empty set $\mathcal{F}$ equipped with a binary relation $\mathcal{I}$ which is both reflexive and symmetric. That is, the relation $\mathcal{I}$ satisfies the following pair of axioms for all elements x and y in $\mathcal{F}$.

(1) $(x, x) \in \mathcal{I}$.

(2) If $(x, y) \in \mathcal{I}$ then $(y, x) \in \mathcal{I}$.

Here, $\mathcal{I}$ is an *incidence relation*. Typically, however, the notion of an *incidence structure* and, in particular, an *incidence geometry* has greater utility.

Definition 1.3 (Incidence structure, [11])**.** An incidence structure is a triple $\Pi = (\mathcal{P}, \mathcal{L}, \mathcal{I})$, where $\mathcal{P}$ is a set of *points*, $\mathcal{L}$ is a set of lines and $\mathcal{I}$ is an incidence relation between the points and lines of Π. An incident point-line pair in Π is a *flag*. An incidence structure Π is an *incidence geometry* if the following axioms are additionally satisfied.

(1) Every pair of distinct points is incident with a unique line of Π.

(2) Every line of Π is incident with at least two distinct points.

(3) There are at least three points in Π, not all of which are collinear.

Now, note that the following definition, Definition 1.4, has been adapted from [3, Chapter 1] to include an explicit reference to an incidence geometry.

Definition 1.4 (Projective space, [3])**.** A *projective space* is an incidence geometry Π satisfying the following pair of axioms.

(1) Every line of Π contains at least three points.

(2) Let $\mathcal{T}$ be a triangle with vertices $\mathcal{V} = \{v_1, v_2, v_3\}$ and sides $\mathcal{E} = \{t_1, t_2, t_3\}$. If a line ℓ meets t_1 and t_2 in the points P_1 and P_2 with $P_i \notin \mathcal{V}$ for $i = 1, 2$ then ℓ meets t_3 in some other point P of Π.

The axiomatic approach established here captures the differences between projective geometries and their *affine* counterparts. Definition 1.4 highlights the absence of *parallel lines* in projective geometries. It is often, however, more convenient to consider projective spaces as quotient structures since their close association with quotient sets is readily exploited as a method of construction. First, recall that if $\mathbb{K}$ is a field, of arbitrary characteristic, the vector space $\mathcal{V}$ of dimension $(n + 1)$ over $\mathbb{K}$ with additive identity $\mathbf{0} = (0, \ldots, 0)$ is denoted by $V(n + 1, \mathbb{K})$. If, however, $\mathcal{V}$ is defined over a finite field $\mathbf{F}_q$, the vector space is instead denoted by $V(n + 1, q)$.

Proposition 1.5. *Let $\mathcal{V} = V(n + 1, \mathbb{K})$ be a vector space over a field $\mathbb{K}$. Define a relation $\sim$ on the set $\mathcal{W} = \mathcal{V} \setminus \{\mathbf{0}\}$ by the identification $X \sim Y$ if and only if there exists $\lambda \in \mathbb{K} \setminus \{0\}$ such that $Y = \lambda X$. Then, $\sim$ is an equivalence relation on $\mathcal{W}$ with quotient set denoted by $\mathbb{P}(\mathcal{V})$.*

Definition 1.6 (Classical spaces, [8])**.** The *classical* n-dimensional projective space associated to the vector space $\mathcal{V} = V(n + 1, \mathbb{K})$ is the quotient set $\mathbb{P}(\mathcal{V})$. A projective space $\mathbb{P}(\mathcal{V})$ of dimension $n \geq 3$ is a *spatial geometry*.

Note 1.7. Here, for $n \geq 2$, verification of the axioms readily establishes that the quotient set $\mathbb{P}(\mathcal{V})$ is a projective space. Also, note the fact that a point of $\mathbb{P}(\mathcal{V})$ is a *set*; the equivalence class of a non-zero vector $X \in \mathcal{V}$ and is denoted by $\mathbf{P}(X)$.

When explicit reference to the dimension of the projective space is required, write $\mathrm{PG}(n, \mathbb{K})$ for the n-dimensional projective space $\mathbb{P}(\mathcal{V})$. This illustrates, in particular, that the $(n+1)$-dimensional vector space $V(n + 1, \mathbb{K})$ induces only an n-dimensional projective space. This apparent loss of dimension is explained by the following characterization of projective spaces.

Given the $\mathbb{K}$-vector space $\mathcal{V} = V(n + 1, \mathbb{K})$, the n-dimensional projective space $\mathrm{PG}(n, \mathbb{K})$ coincides exactly with the set of all 1-dimensional subspaces of $\mathcal{V}$. Formally,

$$\mathrm{PG}(n, \mathbb{K}) := \Big\{ \langle X \rangle \;\Big|\; X \in \mathcal{V} \setminus \{\mathbf{0}\} \Big\}.$$

Here, $\langle X \rangle$ is the 1-dimensional subspace spanned by the non-zero vector X in $\mathcal{V}$. This description is seen to be equivalent through the following isomorphism of sets:

$$\begin{aligned} \phi : \mathrm{PG}(n, \mathbb{K}) &\longrightarrow \mathbb{P}(\mathcal{V}), \\ \langle X \rangle &\longmapsto \mathbf{P}(X). \end{aligned}$$

Notation 1.8. Analogous to the notation used for vector spaces, the n-dimensional projective space over a *finite field* $\mathbf{F}_q$ is denoted by $\mathrm{PG}(n, q)$.

Before restricting attention to a particular class of projective space, additional properties of the general n-dimensional projective space must be considered.

1.1.1 Coordinates and projective subspaces

Coordinates are readily established in classical projective spaces, that is, projective spaces of the form $\mathrm{PG}(n, q)$ constructed over finite fields. Here, the known structure of the underlying vector space is exploited to facilitate computations in projective coordinate systems. First, recall that an element X in an $\mathbf{F}_q$-vector space $\mathcal{V}$ with basis $\mathbf{e} = \{e_0, e_1, \ldots, e_n\}$ admits a unique decomposition as an $\mathbf{F}_q$-linear combination of basis vectors. If $X \in \mathcal{V}$ is of the form $X = \alpha_0\mathbf{e}_0 + \alpha_1\mathbf{e}_1 + \cdots + \alpha_n\mathbf{e}_n$, then the column vector $[X]_\mathbf{e} = [\alpha_0, \alpha_1, \ldots, \alpha_n]^\top$ is its *coordinate vector* with respect to the basis $\mathbf{e}$. Now, if X is non-zero, then $\langle X \rangle \in \mathrm{PG}(n, q)$ and the elements of $[X]_\mathbf{e}$ are the *homogeneous coordinates* of the point $\langle X \rangle$. In $\mathrm{PG}(n, q)$, the ratio of homogeneous coordinates is denoted by $[\alpha_0 : \alpha_1 : \cdots : \alpha_n]$. Here, the term homogeneous illustrates that projective coordinates are invariant under scalar multiplication. Indeed, if $X \in \mathcal{V} \backslash \{\mathbf{0}\}$ and if $\lambda \in \mathbf{F}_q$ is non-zero, then $\mathbf{P}(X) = \mathbf{P}(\lambda X)$ as the subspaces spanned by these vectors coincide. Thus, the tuple $[\lambda\alpha_0 : \lambda\alpha_1 : \cdots : \lambda\alpha_n]$ is also a ratio of homogeneous coordinates for the non-zero vector $X \in \mathcal{V}$ with coordinate vector $[X]_\mathbf{e} = [\alpha_0, \ldots, \alpha_n]^\top$. The underlying structure of the vector space $\mathcal{V} = V(n+1, q)$ is also exploited to imbue classical projective spaces with concepts of linearity. The points $\mathbf{P}(X_1), \mathbf{P}(X_2), \ldots, \mathbf{P}(X_n)$ are *linearly independent* in $\mathrm{PG}(n, q)$ if their corresponding vectors $X_1, \ldots, X_n$ are linearly independent in $V(n+1, q)$. Here, for $1 \leq i \leq n$, the vector X_i is a representative for the equivalence class $\mathbf{P}(X_i)$.

Substructures of classical projective spaces are now considered. The projective subspaces of $\mathrm{PG}(n, q)$ are closely associated to the vector subspaces of $V(n+1, q)$. Note that it is often convenient to use the notation $\mathrm{PG}(n, q)$ and $\mathbb{P}(\mathcal{V})$ concurrently.

Definition 1.9 (Projective subspaces)**.** A subset S of the projective space $\mathrm{PG}(n, q)$ is a *projective subspace* if $S = \mathbb{P}(\mathcal{W})$ where $\mathcal{W}$ is a vector subspace of $V(n+1, q)$. Also, if $\dim(\mathcal{W}) = d$ then

S is a $(d-1)$-dimensional projective subspace of $\mathrm{PG}(n, q)$.

Here, note again an apparent loss of dimension when alternating between the vector subspaces of $V(n+1, q)$ and their induced projective subspaces. To illustrate this, observe that in $\Pi = \mathrm{PG}(n, q)$ a 0-dimensional projective subspace is a point $\mathbf{P}(X)$. It is, however, associated to a 1-dimensional vector subspace of $V(n+1, q)$. Similarly, a 1-dimensional projective subspace is a line of Π but is associated to a plane containing the origin in $V(n+1, q)$. A plane in $\mathrm{PG}(n, q)$ is a 2-dimensional projective structure but is associated to a 3-dimensional subspace of $V(n+1, q)$. Finally, a subspace of dimension $(n-1)$ in $\mathrm{PG}(n, q)$ is a *hyperplane*. Also, it is often useful to adopt terminology for complementary subspaces. A subspace S of dimension $n-r$ in Π is said to have *codimension* r.

1.2 Finite projective planes

A strengthening of the axioms characterizing projective spaces yields an important class of projective space, the projective plane. Here, in contrast to spatial geometries, only the axiomatic approach is desirable.

Definition 1.10 (Projective plane, [8])**.** A *projective plane* is an incidence structure $\Pi = (\mathcal{P}, \mathcal{L}, \mathcal{I})$, satisfying the following axioms.

(1) Every pair of distinct points is incident with a unique line.

(2) Every pair of distinct lines intersects in a unique point of Π.

(3) There exists a set of four distinct points in Π, no three of which are collinear.

The plane Π is said to be *finite* if the set of its points is finite.

It is readily shown that in a finite projective plane Π, see [9, Chapter 3], there is an integer n in $\mathbf{N}$, the *order* of Π, satisfying the properties presented below in Theorem 1.11. A plane Π of order n is often denoted by Π_n.

Theorem 1.11 (Order)**.** *Let* $\Pi = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ *be a finite projective plane. Then, there is an integer* n *in* $\mathbf{N}$ *satisfying the following properties with respect to the points and lines of* Π:

(1) *any line* ℓ *in* Π *contains* $n+1$ *points and any point* P *is incident with* $n+1$ *lines*;

(2) *the total number of points and lines in* Π *is* n^2+n+1.

Proof See [9, Chapter 3]. ■

An obvious question arises when considering the range of integers n in $\mathbf{N}$ which may occur as the order of a finite projective plane Π_n. If n is of the form p^h where p is prime and $h \geq 1$, the answer is established by the following Proposition.

Proposition 1.12. *The classical projective space* $\Pi_q = \mathrm{PG}(2, q)$ *is a projective plane of order q.*

Proof See [9, Chapter 3]. ■

Now, it is opportune to mention that homogeneous coordinates permit a simple interpretation of incidence between the points and lines of $\mathrm{PG}(2, q)$. Let $\mathcal{P}$ and $\mathcal{L}$ denote respectively the set of points and lines of the plane $\Pi_q = \mathrm{PG}(2, q)$. Then, if

$$\mathcal{P} = \left\{ \mathbf{P}(X) = [\lambda x, \lambda y, \lambda z] \,\middle|\, x, y, z \in \mathbf{F}_q; \lambda \in {\mathbf{F}_q}^* \right\},$$

and

$$\mathcal{L} = \left\{ \ell = aX + bY + cZ \,\middle|\, a, b, c \in \mathbf{F}_q \right\},$$

the point $\mathbf{P}(X) = [x, y, z]$ is incident with the line ℓ with equation $aX + bY + cZ$ in Π_q precisely when $ax + by + cz = 0$.

Now, returning to the question of order, in general, it is not known if there is a finite projective plane Π_n of order $n \in \mathbf{N}$ if $n \neq p^h$ for any prime p and $h \in \mathbf{N}$. Theorem 1.13 does, however, restrict the possibilities for a plane Π_n of order n if n has distinct prime divisors. Recall that an integer n is a sum of *integral squares* if there exists a pair of integers a and b such that $n = a^2 + b^2$.

Theorem 1.13 (Bruck-Ryser). *Let* $n \in \mathbf{N}$ *be such that* $n \in \{1, 2\}$ $(\mathit{mod}\ 4)$ *and suppose that* n *is not a sum of integral squares. Then, there is no projective plane* Π_n *of order* n.

Theorem 1.13 precludes the existence of an infinite number of projective planes. It demonstrates, in particular, that there is no projective plane of order n if $n \in \{6, 14, 21\}$. This, together with the work of Lam, see [29], has prompted the following conjecture; see [22, Chapter 2].

Conjecture 1.14. *If* Π_n *is a finite projective plane of order* n*, then* $n = p^h$ *for some prime* p *and some* $h \in \mathbf{N}$.

Before discussing further properties of finite projective planes, the following nomenclature is introduced.

Definition 1.15. A set of lines concurrent at a point P of a projective plane Π is a *pencil* of lines. A set of points incident with a fixed line ℓ in Π is a *range* of points.

Definition 1.16 (Perspective)**.** Let Π be a finite projective plane containing a pair of triangles $\mathcal{T}_1$ and $\mathcal{T}_2$ with vertex-sets $\{a_1, b_1, c_1\}$ and $\{a_2, b_2, c_2\}$ and edge-sets $\{e_1, f_1, g_1\}$ and $\{e_2, f_2, g_2\}$ respectively. Futhermore, let $E = e_1 \cap e_2$, $F = f_1 \cap f_2$ and $G = g_1 \cap g_2$ be the points of intersection of corresponding edges. Then, the following nomenclature is used.

(1) $\mathcal{T}_1$ and $\mathcal{T}_2$ are in *perspective* from a point Q if a_1a_2, b_1b_2 and c_1c_2 is a pencil of lines at Q.

(2) The triangles are in *perspective* from a line ℓ if the points E, F and G are incident with ℓ.

Crucially, Definition 1.16 yields the following distinction between projective planes.

Definition 1.17 (Desarguesian planes)**.** Let Π be a projective plane in which any pair of triangles T_1 and T_2, in perspective from a point Q, are necessarily in perspective from a line ℓ. The plane Π is then said to be *Desarguesian*.

Theorem 1.18. *The classical projective plane* $\Pi_q = \mathrm{PG}(2, q)$ *is Desarguesian.*

Proof See [11, Chapter 2]. ■

1.2.1 Projective completion and non-Desarguesian planes

Theorem 1.18 restricts attention to classical planes and suggests that the incidence properties of a projective plane may be dependent upon its method of construction. Projective *completion* is one such method. It yields a method of constructing non-Desarguesian planes, see [10, Chapter 5], for which the following definition is introduced.

Definition 1.19 (Affine plane, [33])**.** An affine plane $\mathcal{A} = (\mathcal{P}, \mathcal{L}, \mathcal{I})$, with $\mathcal{I}$ the set of its flags, is an incidence structure satisfying the following axioms.

(1) Every pair of points is incident with a unique line.

(2) For every pair $(p, \ell) \notin \mathcal{I}$ there is a unique line $\ell' \in \mathcal{L}$ such that $(p, \ell') \in \mathcal{I}$ and $\ell \cap \ell' = \emptyset$.

(3) There exists a set of four points in $\mathcal{A}$, no three of which are collinear.

Definition 1.20 (Projective completion, [33])**.** Let $\mathcal{A} = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ be an arbitrary affine plane. The projective completion of $\mathcal{A}$ is the incidence structure $\Pi = (\mathcal{P}', \mathcal{L}', \mathcal{I})$ constructed in accordance with the following algorithm applied to each class $\mathcal{C}$ of parallel lines in $\mathcal{A}$.

(1) Add to each class $\mathcal{C}$ an *ideal* point p^* with which all lines of $\mathcal{C}$ are incident.

(2) Add to $\mathcal{A}$ a unique line ℓ_∞ with which all ideal points are incident.

Here, ℓ_∞ is the *line at infinity* with respect to $\mathcal{A}$ and direct verification of the axioms demonstrates that Π is indeed a projective plane. Recall that the homogeneous coordinates of an arbitrary point $\mathbf{P}(X) \in \mathrm{PG}(2,q)$ satisfy the following equality for any $\alpha \in \mathbf{F}_q^*$:

$$[x,y,z] = [\alpha x, \alpha y, \alpha z].$$

Note that here, at least one of x,y,z is non-zero. Thus, without loss of generality, if $z \neq 0$, there exist elements $a,b \in \mathbf{F}_q$ such that the following equalities hold:

$$[x,y,z] = [\frac{x}{z}, \frac{y}{z}, 1] = [a,b,1].$$

The association of the point $(a,b) \in \mathbf{F}_q^2$ with the point $[a,b,1] \in \mathrm{PG}(2,q)$ yields an injection $\phi : \mathbf{F}_q^2 \hookrightarrow \mathrm{PG}(2,q)$. In this case, $\ell_\infty = \{[x,y,0] \mid x,y \in \mathbf{F}_q\}$ with at least one of $x,y \neq 0$ and the following relations hold:

$$\mathbf{F}_q^2 \subset \mathrm{PG}(2,q); \quad \mathrm{PG}(2,q) = \mathbf{F}_q^2 \cup \ell_\infty.$$

Note, however, that the known examples of finite non-Desarguesain planes have order equal to a non-trivial power of a prime p. That is, thus far, the only known planes of prime order are Desargusian. This has prompted the following conjecture; see [22, Chapter 2].

Conjecture 1.21. *Let Π_n be a finite projective plane of order n. If n is prime, then Π_n is Desarguesian.*

1.3 Mappings between projective spaces

A generalization of linear maps between vector spaces is now introduced. This generalization is then seen to be the basis upon which *projective transformations*, mappings between classical projective spaces, are built.

Definition 1.22. Let $T : \mathcal{V} \longrightarrow \mathcal{W}$ be a map between the $\mathbf{F}_q$-vector spaces $\mathcal{V}$ and $\mathcal{W}$. Then T is *semilinear* if the following properties hold for any u, v in $\mathcal{V}$ and for any λ in $\mathbf{F}_q$.
(1) $T(u+v) = T(u) + T(v)$.
(2) $T(\lambda v) = \sigma(\lambda) T(v)$ for some $\sigma \in \mathrm{Aut}(\mathbf{F}_q)$.
Here, σ is the *companion automorphism* for T and, if σ is the identity automorphism on $\mathbf{F}_q$, T is linear.

The following proposition is established by direct verification of the group axioms.

Proposition 1.23. *The set $\Gamma L(\mathcal{V})$ of all invertible semilinear maps on an $\mathbf{F}_q$-vector space $\mathcal{V}$ is a group under composition. If $\mathcal{V} = V(n,q)$, the group is denoted by $\Gamma L(n,q)$.*

Definition 1.24 (Collineation)**.** Let $\Pi = \mathbb{P}(\mathcal{V})$ and $\Pi' = \mathbb{P}(\mathcal{W})$ be a pair of n-dimensional projective spaces, with $n \geq 2$, associated to the $\mathbf{F}_q$-vector spaces $\mathcal{V}$ and $\mathcal{W}$. A map $\mathfrak{T} : \Pi \longrightarrow \Pi'$ is an *isomorphism* or *collineation* if it is a bijection preserving incidence. Denote the set of all collineations on $\mathrm{PG}(n,q)$ by $\mathrm{P\Gamma L}(n+1,q)$.

Note that the map $\mathfrak{T} : \Pi \longrightarrow \Pi'$ *preserves incidence* if it preserves inclusion with respect to projective subspaces. More specifically, if S and S' are a pair of subspaces in Π, then $S \subset S'$ implies that $\mathfrak{T}(S) \subset \mathfrak{T}(S')$.

Proposition 1.25. *Let $T : \mathcal{V} \longrightarrow \mathcal{W}$ be a semilinear bijection between the $\mathbf{F}_q$-vector spaces $\mathcal{V}$ and $\mathcal{W}$ with $\sigma \in \mathrm{Aut}(\mathbf{F}_q)$ its companion automorphism and $\dim(\mathcal{V}) = \dim(\mathcal{W}) = 3$. Define a mapping $\mathfrak{T} : \mathbb{P}(\mathcal{V}) \longrightarrow \mathbb{P}(\mathcal{W})$ as follows:*

$$\mathfrak{T}(\mathbf{P}(X)) = \mathbf{P}(T(X)) \textit{ where } X \in \mathcal{V} \setminus \{\mathbf{0}\}. \tag{1.1}$$

Then $\mathfrak{T}$ is a collineation between the projective planes $\mathbb{P}(\mathcal{V})$ and $\mathbb{P}(\mathcal{W})$.

Proof Let $\mathbf{P}(X_1), \mathbf{P}(X_2)$ and $\mathbf{P}(X_3)$ be three collinear points in $\mathbb{P}(\mathcal{V})$. Thus, the corresponding vectors X_1, X_2 and X_3 are linearly dependent over $\mathbf{F}_q$ and there exist scalars λ_1, λ_2 and λ_3, not all zero, such that $\lambda_1 X_1 + \lambda_2 X_2 + \lambda_3 X_3 = \mathbf{0}$. It follows that $T(\lambda_1 X_1 + \lambda_2 X_2 + \lambda_3 X_3) = T(\mathbf{0}) = \mathbf{0}$. By assumption, T is semilinear with companion automorphism $\sigma \in \mathrm{Aut}(\mathbf{F}_q)$. This implies that

$$\sigma(\lambda_1)T(X_1) + \sigma(\lambda_2)T(X_2) + \sigma(\lambda_3)T(X_3) = \mathbf{0}. \tag{1.2}$$

Recall, if $\lambda \in {\mathbf{F}_q}^*$ then $\sigma(\lambda) \neq 0$ for any $\sigma \in \mathrm{Aut}(\mathbf{F}_q)$. Since $\lambda_i \neq 0$ for at least one $1 \leq i \leq 3$, it follows by Equation (1.2) that the vectors $T(X_1)$, $T(X_2)$ and $T(X_3)$ are linearly dependent whence $\mathbf{P}(T(X_1))$, $\mathbf{P}(T(X_2))$ and $\mathbf{P}(T(X_3))$ are collinear. Now, since T is a bijection, the result follows.

■

Proposition 1.26. *The set $\mathrm{P\Gamma L}(n+1,q)$ of all collineations on $\mathrm{PG}(n,q)$ is a group with respect to the operation of composition.*

Proof This follows by direct verification of the group axioms on the set $\mathrm{P\Gamma L}(n+1,q)$. ■

Definition 1.27. The group $\mathrm{P\Gamma L}(n+1,q)$ is said to be the *full group* of collineations on $\mathrm{PG}(n,q)$. It is the group of all *automorphisms* on $\mathrm{PG}(n,q)$.

Definition 1.28 (Isomorphic subsets)**.** A pair of non-empty sets $\mathcal{K}_1$ and $\mathcal{K}_2$ in $\mathrm{PG}(n,q)$ are *isomorphic* if there is a collineation $\mathfrak{T} \in \mathrm{P\Gamma L}(n+1,q)$ such that $\mathfrak{T}(\mathcal{K}_1) = \mathcal{K}_2$.

Note that Proposition 1.25 demonstrates that, for vector spaces $\mathcal{V}$ and $\mathcal{W}$ of dimension three, semilinear bijections induce collineations between the projective planes $\mathbb{P}(\mathcal{V})$ and $\mathbb{P}(\mathcal{W})$. Moreover, this result can be extended to spatial geometries. Of greater interest, however, is Theorem 1.29 which establishes the extent to which the converse holds. Although a number of different views of the Fundamental Theorem of Projective Geometry exist, here, owing to its clarity, the exposition developed in [8] is given.

Theorem 1.29 (The Fundamental Theorem of Projective Geometry)**.** *In $\Pi = \mathrm{PG}(n,q)$, with $n \geq 2$, every collineation is derived from a semilinear bijection on the associated vector space $V(n+1,q)$.*

It is natural to consider the subgroups of the group $\mathrm{P\Gamma L}(n+1,q)$ of automorphisms on $\mathrm{PG}(n,q)$. Here, the subgroup generated by collineations associated to linear maps is now discussed.

Definition 1.30 (Projectivity)**.** Let Π and Π' be a pair of projective spaces $\mathrm{PG}(n,q)$ of dimension $n \geq 2$ with $\mathfrak{T} : \Pi \longrightarrow \Pi'$ a collineation between them. Then, $\mathfrak{T}$ is a *projectivity* if it is induced by a linear map $T : \mathcal{V} \longrightarrow \mathcal{W}$ between the underlying vector spaces. Denote the set of all projectivities on $\mathrm{PG}(n,q)$ by $\mathrm{PGL}(n+1,q)$.

Proposition 1.31. *Let $T : \mathcal{V} \longrightarrow \mathcal{W}$ be a linear injection between the 3-dimensional $\mathbf{F}_q$-vector spaces $\mathcal{V}$ and $\mathcal{W}$. Define a map $\mathfrak{T} : \mathbb{P}(\mathcal{V}) \longrightarrow \mathbb{P}(\mathcal{W})$ by the following equality:*

$$\mathfrak{T}(\mathbf{P}(X)) = \mathbf{P}(T(X)) \text{ where } X \in \mathcal{V} \setminus \{\mathbf{0}\}. \tag{1.3}$$

Then, $\mathfrak{T}$ is a projectivity between the planes $\mathbb{P}(\mathcal{V})$ and $\mathbb{P}(\mathcal{W})$.

Proof That $\mathfrak{T}$ preserves incidence is clear; a linear map is necessarily semilinear and its method of construction is identical to that used in Example 1.25. Now, as a linear injection, between $\mathbf{F}_q$-vector spaces of the same dimension, the Rank-Nullity theorem implies that $T : \mathcal{V} \longrightarrow \mathcal{W}$ is a bijection. Thus, $\mathfrak{T}$ is a bijection preserving incidence making it a collineation. Since $\mathfrak{T}$ is induced by a linear map, the result follows.

■

Proposition 1.32. *The set $\mathrm{PGL}(n+1,q)$ of all projectivities on $\mathrm{PG}(n,q)$ is a group with respect to the operation of composition.*

Proof The result follows by direct verification of the group axioms on the set $\mathrm{PGL}(n+1,q)$.

■

Definition 1.33. The group $\mathrm{PGL}(n+1,q)$ is the *projective general linear group* of the projective space $\mathrm{PG}(n,q)$.

Definition 1.34 (Projective equivalence)**.** A pair of non-empty sets $\mathcal{K}_1$ and $\mathcal{K}_2$ in $\mathrm{PG}(n,q)$ are *projectively equivalent* if there is a projectivity $\mathfrak{T} \in \mathrm{PGL}(n+1,q)$ such that $\mathfrak{T}(\mathcal{K}_1) = \mathcal{K}_2$.

Comparison of Definitions 1.28 and 1.34 reveals that in $\mathrm{PG}(n,q)$, subsets which are projectively equivalent are necessarily isomorphic. The converse, however, need not hold; a distinction of some importance when considering the classification of plane algebraic curves.

1.3.1 Duality in projective planes

Recall that $\mathcal{V}^*$, the set of all linear functionals on a vector space $\mathcal{V}$ over a field $\mathbf{F}_q$, is itself an $\mathbf{F}_q$-vector space under the pointwise addition and scalar multiplication of functionals. $\mathcal{V}^*$ is the *dual* of the vector space $\mathcal{V}$ and, accordingly, admits a *dual projective space* $\mathbb{P}(\mathcal{V}^*)$. Much of the interplay between $\mathbb{P}(\mathcal{V})$ and $\mathbb{P}(\mathcal{V}^*)$ is determined by the following result from Linear Algebra.

Theorem 1.35. *Suppose that $\mathcal{V}$ is a finite-dimensional vector space over a field $\mathbf{F}_q$ with basis $\mathbf{e} = \{e_1, e_2, \dots, e_n\}$. Then, the set $\mathcal{F} = \{f_1, f_2, \dots, f_n\}$ is a basis for the dual vector space $\mathcal{V}^*$ where, for $1 \leq i \leq n$, the linear functional $f_i : \mathcal{V} \longrightarrow \mathbf{F}_q$ is given by the following equality:*

$$f_i(\sum_{j=1}^{n} \alpha_j e_j) = \alpha_i.$$

In particular, it follows that $\dim(\mathcal{V}) = \dim(\mathcal{V}^*) = n$*.*

Sets of the form $ann(S) = \{f \in \mathcal{V}^* \mid f(s) = 0 \ , \forall\ s \in S\}$, induced by subspaces $S \neq \emptyset$ of $\mathcal{V}$, provide a similar relationship between the projective subspaces of $\mathbb{P}(\mathcal{V})$ and those of the dual $\mathbb{P}(\mathcal{V}^*)$. Here, $ann(S)$ is the *annihilator* of the subspace S of $\mathcal{V}$ and is a subspace of the dual $\mathcal{V}^*$.

Now, recall that by extending a basis $\mathbf{s} = \{s_1, s_2, \dots, s_m\}$ for the subspace $S \leq \mathcal{V}$ to a basis $\mathbf{e} = \{s_1, \dots, s_m, s_{m+1}, \dots, s_n\}$ for $\mathcal{V}$, it can be readily shown that the set $\mathcal{F} = \{f_{m+1}, f_{m+2}, \dots, f_n\}$ is a basis for $ann(S) \leq \mathcal{V}^*$. Thus, Theorem 1.35 yields the following identity for the vector subspaces $S \leq \mathcal{V}$ and $ann(S) \leq \mathcal{V}^*$:

$$\dim(S) + \dim(ann(S)) = \dim(\mathcal{V}). \tag{1.4}$$

Now, since $\mathcal{V}^*$ is an $\mathbf{F}_q$-vector space, it too admits a dual $(\mathcal{V}^*)^*$. Thus, if $\dim(\mathcal{V}) = n$, application of Theorem 1.35 to $\mathcal{V}^*$ yields the following equalities:

$$n = \dim(\mathcal{V}) = \dim(\mathcal{V}^*) = \dim((\mathcal{V}^*)^*).$$

Here, however, the map $\phi : \mathcal{V} \longrightarrow (\mathcal{V}^*)^*$ given by $v \longmapsto f(v)\ \ \forall\, f \in \mathcal{V}^*$ and $\forall\, v \in \mathcal{V}$ defines a canonical isomorphism onto $(\mathcal{V}^*)^*$. These observations give the following result.

Theorem 1.36. *For an $\mathbf{F}_q$-vector space $\mathcal{V}$, there is a bijective correspondence between $\mathcal{H}$, the set of hyperplanes in $\mathbb{P}(\mathcal{V})$, and the dual space $\mathbb{P}(\mathcal{V}^*)$. In particular, $\mathbb{P}(\mathcal{V}) \cong \mathcal{H}^*$ where $\mathcal{H}^*$ is the set of hyperplanes in $\mathbb{P}(\mathcal{V}^*)$.*

Definition 1.37. Let $\Pi_1 = (\mathcal{P}_1, \mathcal{L}_1, \mathcal{I}_1)$ and $\Pi_2 = (\mathcal{P}_2, \mathcal{L}_2, \mathcal{I}_2)$ be a pair of projective spaces. A bijection $\sigma : \Pi_1 \longrightarrow \Pi_2$ is a *correlation* if it reverses incidence. More specifically, σ is a correlation if the following property holds for every point $P \in \mathcal{P}_1$ and every line $\ell \in \mathcal{L}_1$:

$$P \in \ell \Longleftrightarrow \sigma(\ell) \in \sigma(P).$$

Note in particular that a correlation between the projective plane $\Pi_q = \mathrm{PG}(2, q)$ and its dual Π_q^* is a bijection $\sigma : \Pi_q \longrightarrow \Pi_q^*$ interchanging points and lines. Thus, σ relates any property exhibited by the points of the plane $\Pi_q = \mathrm{PG}(2, q)$ to an equivalent statement about the lines of the dual plane Π_q^*. This is the principle of *projective duality*; see [22, Chapter 2].

1.4 Plane algebraic curves

A *monomial* of *degree* d is a product of the form $X_1^{r_1} X_2^{r_2} \cdots X_n^{r_n}$ where $d = r_1 + r_2 + \cdots + r_n$ and the symbols X_i are *indeterminates*. A polynomial is a finite linear combination of monomials with coefficients in a ring K. The ring of all such polynomials is denoted by $K[X_1, X_2, \ldots, X_n]$ and the degree $\deg(F)$ of a polynomial F is the largest degree of its monomials. Furthermore, F is *homogeneous* if its monomials have the same degree. Equivalently, F is homogeneous if there exists λ in K and $d \in \mathbf{N}$ such that $F(\lambda X_1, \ldots, \lambda X_n) = \lambda^d F(X_1, \ldots, X_n)$.

Definition 1.38. A *plane algebraic curve* $\mathcal{C}$ over a field $\mathbf{F}_q$ is a pair $(\mathbf{V}(F), (F))$ where (F) is the principal ideal generated by a homogeneous polynomial F in $\mathbf{F}_q[X, Y, Z]$ and $\mathbf{V}(F)$ is the set of $\mathbf{F}_q$-*rational points* on the curve $\mathcal{C}$, given explicitly by the following equality:

$$\mathbf{V}(F) = \Big\{(x : y : z) \in \mathrm{PG}(2, q) \Big|\ G((x, y, z)) = 0\ \ \forall\, G \in (F)\Big\}.$$

Here, the set $\mathbf{V}(F)$ is a *projective variety* and the *degree* of the curve $\mathcal{C}$, denoted $\deg(\mathcal{C})$, is the degree of the polynomial F.

Note that in $\mathrm{PG}(2, q)$ the set $\mathbf{V}(F)$ of a homogeneous polynomial $F \in \mathbf{F}_q[X, Y, Z]$ is well defined. To demonstrate this, suppose that F is a homogeneous polynomial of degree $d \geq 1$ and let

$\mathbf{P}(X) = (x : y : z) \in \mathbf{V}(F)$ with corresponding non-zero vector $X \in V(3, q)$. Then, for any non-zero vector $Y \in V(3, q)$, the equality $\mathbf{P}(X) = \mathbf{P}(Y)$ holds, in $\mathrm{PG}(2, q)$, if and only if $Y = \lambda X$ for some $\lambda \in \mathbf{F}_q{}^*$. Since F is homogeneous, this implies that $F(Y) = F(\lambda X) = \lambda^d F(X) = 0$. Thus, $F(Y) = 0$ which, by definition, implies that $\mathbf{P}(Y) \in \mathbf{V}(F)$; this establishes the claim.

As the incidence properties of a curve $\mathcal{C} = (\mathbf{V}(F), (F))$ are largely determined by the polynomial F, it is often suitable to forgo the algebraic formalism in Definition 1.38. Toward this end, the curve $\mathcal{C} = (\mathbf{V}(F), (F))$ is interpreted as the pair $(\mathbf{Z}(F), F)$ where $\mathbf{Z}(F)$ is the *zero set* of the polynomial $F \in (F)$. Here, F is the *defining polynomial* of the curve $\mathcal{C} = (\mathbf{V}(F), (F))$ and, accordingly, the curve is often also denoted by $\mathcal{C} : F(X, Y, Z) = 0$ or simply by $\mathcal{C}_F$. When reference to the defining polynomial is superfluous, $\mathcal{C}$ is written for an arbitrary curve.

A non-zero polynomial $F \in \mathbf{F}_q[X, Y, Z]$ of degree $d \geq 1$ is *irreducible* if it cannot be decomposed into a product of two non-constant polynomials of lower degree over the field $\mathbf{F}_q$. An algebraic curve $\mathcal{C} : F(X, Y, Z)$ is irreducible if its defining polynomial F is irreducible; otherwise the curve $\mathcal{C}$ is *reducible* or *degenerate*. A curve $\mathcal{C}$ is *absolutely irreducible* if its defining polynomial F is irreducible over $\overline{\mathbf{F}}_q$, the algebraic closure of the field $\mathbf{F}_q$.

Definition 1.39. Let $\mathcal{C}_F$ be a reducible projective curve with defining polynomial F. Suppose that $F = GH$ with G and H a pair of irreducible non-constant homogeneous polynomials in $\mathbf{F}_q[X, Y, Z]$. The curves $\mathcal{C}_G$ and $\mathcal{C}_H$ are the *irreducible components* of the curve $\mathcal{C}_F$.

Now, consider a projective curve $\mathcal{C} : F(X, Y, Z) = 0$ of degree $d \geq 1$ in $\Pi_q = \mathrm{PG}(2, q)$. Observe that the polynomial $f(X, Y) := F(X, Y, 1)$ defines an associated curve $\mathcal{A}_f$ in the affine plane $\mathbb{A}^2 = \Pi_q \setminus \ell_\infty$. The curve $\mathcal{A}_f$ is an *affine section* of the curve $\mathcal{C}_F$ and, with respect to the underlying vector space $V(3, q)$, $\mathcal{A}_f$ is the restriction of $\mathcal{C}_F$ to the plane $Z = 1$. Similarly, one can consider the affine sections $\mathcal{A}_g$ and $\mathcal{A}_h$ determined by the polynomials $g(X, Z) := F(X, 1, Z)$ and $h(Y, Z) := F(1, Y, Z)$ respectively. Conversely, the projective *closure* of an affine curve $\mathcal{C}_f$ of degree $d \geq 1$ is the curve $\overline{\mathcal{C}}$ with defining polynomial F satisfying an equation of the following form:

$$F(X, Y, Z) = Z^d f\left(\frac{X}{Z}, \frac{Y}{Z}\right).$$

The presence of affine sections in a given projective curve is readily exploited to simplify projective curves. This is demonstrated in §1.4.1 where the intersection of projective curves is considered.

1.4.1 Tangents to algebraic curves

Definition 1.40 (Non-singular curve)**.** Suppose that $P = (x_0 : y_0 : z_0)$ is a rational point on an algebraic curve $\mathcal{C} : F(X, Y, Z) = 0$ defined over $\mathbf{F}_q$. The curve $\mathcal{C}$ is *non-singular* at P if at least one of its partial derivatives, $\partial F/\partial X$, $\partial F/\partial Y$, $\partial F/\partial Z$, is non-vanishing at P. If every point on the curve $\mathcal{C}$ is non-singular, the curve is itself non-singular.

Equivalently, a rational point P on the curve $\mathcal{C}$ is non-singular if P is incident with a unique tangent line to the curve at P. In this case, the tangent line to C_F at P is the projective line with the following equation:

$$X\frac{\partial F}{\partial X}(P) + Y\frac{\partial F}{\partial Y}(P) + Z\frac{\partial F}{\partial Z}(P) = 0. \tag{1.5}$$

Affine sections yield a simple interpretation of non-singular curves in $\mathrm{PG}(2,q)$. The projective curve $\mathcal{C} : F(X,Y,Z) = 0$ is non-singular, precisely when each of its affine sections is non-singular.

Definition 1.41 (Intersection multiplicity)**.** The *intersection multiplicity* $\mu_p(\mathcal{C}_f, \mathcal{C}_g)$ of distinct algebraic curves $\mathcal{C}_f$ and $\mathcal{C}_g$ in $\mathrm{AG}(2,q)$ at a point $P \in \mathcal{C}_f \cap \mathcal{C}_g$ is the dimension $\dim(\mathcal{O}_p/(f,g))$ of the vector space $\mathcal{O}_p/(f,g)$. Here, $\mathcal{O}_p$ is a *local ring* at P, a ring with a unique maximal ideal, and (f,g) is the ideal generated by the polynomials f and g.

This extends to projective curves through an appropriate choice of coordinates. By construction, at least one of the coordinates of a point $\mathbf{P}(X) = (x_0, x_1, x_2) \in \Pi_q = \mathrm{PG}(2,q)$ is non-zero. The subsequent selection of an anti-flag $(\mathbf{P}(X), \ell_\infty)$, that is, a non-incident point line pair, yields an affine plane $\Pi_q \backslash \ell_\infty$ containing the point $p = (\frac{x_{i_1}}{x_j}, \frac{x_{i_2}}{x_j})$ where i_1, i_2 and $j \in \{0,1,2\}$. Then, the intersection multiplicity $\mu_p(\mathcal{C}_f, \mathcal{C}_g)$ of the point $\mathbf{P}(X)$ on distinct projective curves $\mathcal{C}_f$ and $\mathcal{C}_g$ is $\dim(\mathcal{O}_p/(f,g))$ in the sense of Definition 1.41.

The impetus for Definition 1.41 is provided by a need to understand the interaction between plane algebraic curves. The preliminary result in this direction, see [39, Chapter 14], was proved by Gauss in (1799) over $\mathbb{C}$, the field of complex numbers, and is presented in Theorem 1.42.

Theorem 1.42 (The Fundamental Theorem of Algebra, [39])**.** *Let $F \in \mathbb{C}[X]$ be a non-trivial polynomial of degree $d \geq 1$. Then, F has exactly d complex roots when those roots are counted with multiplicity.*

Geometrically, Theorem 1.42 is a statement about the number of points in which the *affine* curve $\mathcal{C} : Y - F(X) = 0$ meets the line $Y = 0$ over $\mathbb{C}$. A generalization of Theorem 1.42 to more arbitrary curves and fields is given by Theorem 1.43.

Theorem 1.43 (Bézout)**.** *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be a pair of projective algebraic curves with no common components defined over a field $\mathbb{K}$. Then, counting with multiplicity over the algebraic closure $\overline{\mathbb{K}}$ of the field $\mathbb{K}$, the curves $\mathcal{C}_1$ and $\mathcal{C}_2$ meet in exactly $\deg(\mathcal{C}_1) \cdot \deg(\mathcal{C}_2)$ points.*

If at least one of the curves is linear, the following description of intersection multiplicity is sufficient. Given a rational point $P = (x_0, y_0) \in \mathrm{AG}(2, q)$ on a plane algebraic curve $\mathcal{C}$ with $\deg(\mathcal{C}) \geq 2$, suppose that ℓ is a line containing P with finite slope and that ℓ is not a component of $\mathcal{C}$. Then, $\mu_p(\mathcal{C}, \ell)$ is the largest integer m such that

$$g(x) = (x - x_0)^m r(x) \tag{1.6}$$

where $r \in \mathbf{F}_q[x]$ and $r(x_0) \neq 0$. Here, g is said to be the *intersection polynomial* of ℓ and $\mathcal{C}$ at P. If, however, ℓ has infinite slope, an analogous decomposition in y is instead obtained. Now, if $\mu_p(\mathcal{C}, \ell) = 1$ for a line ℓ containing P, then P is a non-singular point of $\mathcal{C}$. If, however, $\mu_p(\mathcal{C}, \ell) \geq 2$ for every line in the plane, P is singular. This suggests an intrinsic multiplicity of a point on a curve. Call m_0 the multiplicity of a point P on a curve $\mathcal{C}$ if $m_0 = \min\{\mu_p(\mathcal{C}, \ell) \mid P \in \ell \cap \mathcal{C}\}$. Thus, if $\mu_p(\mathcal{C}, \ell) \geq m_0 + 1$ for an arbitrary line ℓ in the plane, then ℓ is a tangent to $\mathcal{C}$ at P. A line ℓ is an *inflexional tangent* to $\mathcal{C}$ at a non-singular point $P \in \mathcal{C}$ if $\mu_p(\mathcal{C}, \ell) \geq 3$; P is a *point of inflexion*.

For curves of low degree, the following terminology is used. A non-singular curve of degree two is a *conic* and a curve of degree three is a *cubic curve*.

1.4.2 Normal forms of cubic curves

Note that any classification of curves of degree $d \geq 1$ in $\mathrm{PG}(2, q)$ is dependent upon adopted conventions of equivalence. Two prevalent perspectives emerge.

Definition 1.44. Let $\mathcal{C}$ and $\mathcal{D}$ be plane algebraic curves of degree $d \geq 1$ in $\mathrm{PG}(2, q)$ where $\mathcal{C} = (\mathbf{V}(F), (F))$ and $\mathcal{D} = (\mathbf{V}(G), (G))$. A *polynomial map* is a function $f : \mathcal{C} \longmapsto \mathcal{D}$ where $\mathbf{x} = (x_1, x_2, x_3) \in \mathbf{V}(F)$ implies that $f(\mathbf{x}) = (y_1, y_2, y_3) \in \mathbf{V}(G)$. Here, $y_i = f_i(\mathbf{x})$ and f_i is a rational function for $i \geq 1$. Call $\mathcal{C}$ and $\mathcal{D}$ *isomorphic* or *birationally equivalent* if there is a polynomial map $g : \mathcal{D} \longmapsto \mathcal{C}$ such that $g \circ f = id_{\mathcal{C}}$ and $f \circ g = id_{\mathcal{D}}$.

Definition 1.45. The algebraic curves $\mathcal{C}$ and $\mathcal{D}$ of degree $d \geq 1$ in $\Pi_q = \mathrm{PG}(2, q)$ are *projectively equivalent* if there is a projectivity $\phi : \Pi_q \longrightarrow \Pi_q$ such that $\phi(\mathcal{C}) = \mathcal{D}$. That is, the curves $\mathcal{C}$ and $\mathcal{D}$ are projectively equivalent if there is a linear change of variables between them.

Over the field $\mathbf{F}_q$, a general cubic equation has the following form:

$$F(X, Y, Z) = aX^3 + bX^2Y + cXY^2 + dY^3 + (eX^2 + fXY + gY^2)Z + (hX + iY)Z^2 + jZ^3.$$

Of greater interest, however, is the collection of cubic forms describing irreducible and, in particular, non-singular cubic curves. Over a field $\mathbf{F}_q$, of arbitrary characteristic, a non-singular cubic curve $\mathcal{C}$

in $\mathrm{PG}(2, q)$ is isomorphic to a cubic curve $\mathcal{C}'_F$ in *Weierstrass Normal Form* with defining polynomial F given by the following form; see [36, Chapter 1]:

$$F(X, Y, Z) = Y^2 Z + a_1 XYZ + a_3 YZ^2 - X^3 - a_2 X^2 Z - a_4 XZ^2 - a_6 Z^3. \tag{1.7}$$

If the field $\mathbf{F}_q$ has characteristic $p \neq 2, 3$, however, the polynomial F is further simplified. In this case, see [36, Chapter 1] or [43, Chapter 2], the curve $\mathcal{C}$ is isomorphic to a cubic curve $\mathcal{C}'_F$ in *Reduced Weierstrass Form*, where

$$F(X, Y, Z) = Y^2 Z - X^3 - aXZ^2 - bZ^3. \tag{1.8}$$

Thus, taking $Z = 1$ in Equation (1.8), over a field $\mathbf{F}_q$ of characteristic $p > 3$, the affine sections of a non-singular cubic curve C_F are of the form $Y^2 = f(X) \in \mathbf{F}_q[X]$ where

$$f(X) = X^3 + aX + b \ \text{ with } a, b \in \mathbf{F}_q. \tag{1.9}$$

Note that while a non-singular cubic curve C in $\mathrm{PG}(2, q)$ is isomorphic to a curve in Weierstrass Normal Form, Equation (1.7) is not a characterization of non-singular cubic curves. The curve $\mathcal{C}$ with equation $Y^2 - X^3 = 0$, having a singularity at the point $(0 : 0 : 1)$, is a suitable counterexample. Additional properties are therefore needed. These are now presented within the context of cubic curves over fields of characteristic $p > 3$. Let K be a splitting field for the polynomial f of degree n over a field L. That is, $f = a_n(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ where, for $1 \leq i \leq n$, the elements α_i are the roots of f in K. The *discriminant* of the polynomial f is $\Delta_f = a_n^{2n-2}\delta_f^2$ where

$$\delta_f := \prod_{i \neq j} (\alpha_i - \alpha_j).$$

Definition 1.46. Let $\mathcal{C}$ be an arbitrary cubic curve over a field $\mathbf{F}_q$ of characteristic $p > 3$ with affine equation $Y^2 = f(X)$ where $f(X) = X^3 + aX^2 + bX + c$ with $a, b, c \in \mathbf{F}_q$. Then, the *discriminant* $\Delta(\mathcal{C})$ of the curve $\mathcal{C}$ is just the discriminant $\Delta(f)$ of the polynomial f given explicitly by the following equality:

$$\Delta(\mathcal{C}) = -4a^3c + (ab)^2 + 18abc - 4b^3 - 27c^2. \tag{1.10}$$

In particular, over the field $\mathbf{F}_q$, a curve $\mathcal{C}$ with affine equation $Y^2 = X^3 + bX + c$ has discriminant

$$\Delta(\mathcal{C}) = -(4b^3 + 27c^2). \tag{1.11}$$

Much of the utility in the discriminant is provided by its characterization of non-singular cubic curves in $\mathrm{PG}(2, q)$. In particular, over a field of characteristic $p > 3$, a cubic curve $\mathcal{C}$ with affine equation $Y^2 - f(X) = 0$ where $f(X) = X^3 + aX^2 + bX + c$ and $a, b, c \in \mathbf{F}_q$ is non-singular if and only if $\Delta(\mathcal{C}) \neq 0$; see [36, Chapter 1]. Alternatively, the curve is non-singular precisely when the polynomial f has distinct roots.

Lemma 1.47. *Let $\mathcal{C}$ be a non-singular cubic curve in $\mathrm{PG}(2, q)$ where $\mathbf{F}_q$ is a finite field of arbitrary characteristic. Then, the curve $\mathcal{C}$ meets the line $Z = 0$ in a single point $\mathcal{O} = (0 : 1 : 0)$. Over $\overline{\mathbf{F}}_q$, the algebraic closure of the field $\mathbf{F}_q$, the point $\mathcal{O}$ is a point of inflexion of the curve $\mathcal{C}$.*

Proof The intersection of the curve $\mathcal{C}_F$ with the line $Z = 0$, the line at infinity ℓ_∞, is considered. Here, F is the defining polynomial of an arbitrary non-singular cubic curve $\mathcal{C}$ given by Equation (1.7). Observe that the intersection is non-empty since $\mathcal{O} = (0 : 1 : 0)$ is a point on both $\mathcal{C}_F$ and ℓ_∞. Thus, let $P = (x : y : z) \in \ell_\infty \cap \mathcal{C}$ be an arbitrary point of the intersection. Since $P \in \ell_\infty$, it follows that $z = 0$ and therefore, by Equation (1.7), the following holds:

$$0 = F(P) = F(x, y, 0) = -x^3.$$

This establishes that $x = 0$ and it follows, since $P \in \mathrm{PG}(2, q)$, that $y \neq 0$ and therefore $P = (0 : 1 : 0)$, dividing by y if necessary. Now, since P is a rational point of the non-singular curve $\mathcal{C}$, there is a unique tangent line t to the curve $\mathcal{C}$ at P. Algebraic manipulation demonstrates that the tangent t to the curve $\mathcal{C}$ at P is the line ℓ_∞ with equation $Z = 0$. Above, it was established that the line ℓ_∞ meets the curve $\mathcal{C}$ in a single point $\mathcal{O}$. Thus, since $\overline{\mathbf{F}}_q$ is algebraically closed, Bezout's theorem implies that $\mu_{\mathcal{O}}(\ell_\infty, \mathcal{C}) = 3$. Here, $\mu_{\mathcal{O}}(\ell_\infty, \mathcal{C})$ is the intersection multiplicity of the line ℓ_∞ with the curve $\mathcal{C}$ at $\mathcal{O}$. It follows, therefore, that $\mathcal{O}$ is indeed a point of inflexion.

■

Definition 1.48. An elliptic curve in $\mathrm{PG}(2, q)$ is a non-singular cubic curve E over the field $\mathbf{F}_q$ with a fixed rational point $\mathcal{O}$. Typically, $\mathcal{O} = (0 : 1 : 0)$, the point at infinity with respect to the curve E.

Definition 1.49. Let E be an elliptic curve over a field $\mathbf{F}_q$ of characteristic $p > 3$. Recall from Equation (1.9) that the affine sections of the curve E satisfy the equation $Y^2 = X^3 + aX + b$. Now, the *modular invariant* of the curve E is the quantity $j = j(E)$ given by the following equality:

$$j(E) := 1728 \frac{4a^3}{4a^3 + 27b^2}. \tag{1.12}$$

For convenience, call the modular invariant of a curve E its j-invariant.

1.4.3 The Hasse Weil Theorem

Questions on the enumeration of rational points emerge when studying algebraic curves. A pencil of lines through a point P on a conic $\mathcal{Q}$ readily yields a birational equivalence between $\mathcal{Q}$ and a line of the plane. Such an equivalence also exists for *singular* cubic curves in $\mathrm{PG}(2,q)$. The general problem is, however, non-trivial and, thus far, results have only established a range of values for the number of points on a curve.

Theorem 1.50 (Hasse–Weil)**.** *Let $\mathcal{C}$ be a non-singular curve of degree d in $\mathrm{PG}(2,q)$. Then, the number N_i of $\mathbf{F}_{q^i}$-rational points on the curve $\mathcal{C}$ satisfies the following bound:*

$$|N_i - (q^i+1)| \;\leq (d-1)(d-2)\sqrt{q^i}. \tag{1.13}$$

Here, an $\mathbf{F}_{q^i}$-rational point on a curve $\mathcal{C}$ in $\mathrm{PG}(2,q)$ is just a point $\mathbf{P}(X)$ in $\mathrm{PG}(2,q^i)$ satisfying the equation of the curve. Also, note that Equation (1.13) is customarily given in terms of the *genus* $g=(d-1)(d-2)/2$ of the curve $\mathcal{C}$. Now, application of Theorem 1.50 to the rational points on a non-singular cubic curve reveals that N_1 satisfies the following estimate:

$$|N_1 - (q+1)| \;\leq 2\sqrt{q}. \tag{1.14}$$

Equivalently, the Hasse-Weil Theorem establishes that N_1, the number of rational points on a non-singular cubic curve, lies within the following interval:

$$q+1-2\sqrt{q} \leq N_1 \leq q+1+2\sqrt{q}. \tag{1.15}$$

It is often convenient to denote the set of $\mathbf{F}_q$-rational points of an elliptic curve E by $E(\mathbf{F}_q)$. That is,

$$E(\mathbf{F}_q) = \{(x,y)\in E \;\mid\; x,y\in\mathbf{F}_q\}\cup\{\mathcal{O}\}\,.$$

Definition 1.51. The *class* of an algebraic curve $\mathcal{C}=(\mathbf{V}(F),(F))$ of degree $d\geq 1$ in the plane $\mathrm{PG}(2,q)$, is the largest number of distinct tangents through an external point $Q\in\mathrm{PG}(2,\overline{\mathbf{F}}_q)$ and is denoted by $\gamma(\mathcal{C})$.

Lemma 1.52. *Let $\mathcal{C}$ be an arbitrary cubic curve defined over the field $\mathbf{F}_q$. Then, $\gamma(\mathcal{C})$ satisfies the following pair of upper bounds:*

(1) $\gamma(\mathcal{C})\leq 6$ *if q is odd;*

(2) $\gamma(\mathcal{C})\leq 3$ *if q is even.*

Proof See, [22, Chapter 11]. ■

Chapter 2

Arcs and blocking sets in finite planes

2.1 Introduction to complete arcs in Desarguesian planes

Finite geometry is often concerned with properties inherited by a collection of points in a finite projective plane, subject to known incidence conditions. In the Desarguesian projective plane $\Pi_q = \mathrm{PG}(2, q)$, considerable interest is given to the existence of combinatorial characterizations of algebraic curves. Towards this end, the notion of an arc has been crucial, emanating from the work of Bose and Segre; see Theorems 2.8 and 2.9 respectively.

Definition 2.1 (Plane (k, n)-arcs)**.** In a finite projective plane $\Pi_q = \mathrm{PG}(2, q)$, a (k, n)-arc $\mathcal{K}$ is a collection of k points in Π_q where no $n + 1$, but some n of the points in $\mathcal{K}$, are collinear. Here, the integer n is the *degree* of the arc and $k > n$.

In analogy with plane algebraic curves, standard nomenclature is adopted for arcs of small degree. In particular, a $(k, 2)$-arc $\mathcal{K}$ is an *arc*. When explicit reference to its size is desirable, however, a $(k, 2)$-arc $\mathcal{K}$ is a k-arc. Also, a $(q + 1)$-arc is an *oval* and a $(q + 2)$-arc is a *hyperoval*. In addition to this standard nomenclature, in this thesis, a $(k, 3)$-arc $\mathcal{K}$ is a *cubic arc*.

Definition 2.2 (Complete (k, n)-arcs)**.** The (k, n)-arc $\mathcal{K}$ in $\mathrm{PG}(2, q)$ is *complete* if it admits no extension to a larger arc $\mathcal{K}'$ of the same degree. More precisely, the (k, n)-arc $\mathcal{K}$ is complete if it cannot be embedded in any (k', n)-arc $\mathcal{K}'$ with $k' > k$.

With respect to a (k, n)-arc $\mathcal{K}$, the lines of the plane may be classified according to their incidence with $\mathcal{K}$. A line ℓ is an *i-secant* to $\mathcal{K}$ if $|\mathcal{K} \cap \ell| = i$ where $0 \leq i \leq n$; denote by τ_i their total number in Π_q. In particular, a line which does not meet $\mathcal{K}$ in any point of the plane is an *external* line, a line meeting $\mathcal{K}$ in a singleton is a *unisecant* or *tangent* line while lines meeting $\mathcal{K}$ in two and three points are *bisecants* and *trisecants* respectively. The utility of this is clear when it is observed that a (k, n)-arc $\mathcal{K}$ is a set of size k in $\mathrm{PG}(2, q)$ satisfying the following incidence conditions:

(1) $\tau_i \geq 0$ for $i < n$;

(2) $\tau_n > 0$;

(3) $\tau_i = 0$ for $i > n$.

Note 2.3. Here, note that existence of a (k, n)-arc $\mathcal{K}$ necessarily implies the existence of at least one n-secant in the plane $\mathrm{PG}(2, q)$.

With respect to a (k, n)-arc $\mathcal{K}$, the points of $\Pi_q = \mathrm{PG}(2, q)$ may also be classified according to incidence; in this case, with respect to the lines of Π_q. For each *external* point $Q \in \Pi_q \backslash \mathcal{K}$, let $\sigma_i(Q)$ denote the total number of i-secants to $\mathcal{K}$ at Q where $0 \leq i \leq n$. Similarly, for each *internal* point $P \in \mathcal{K}$, let $\rho_i(P)$ denote the total number of i-secants to $\mathcal{K}$ at P. In the latter instance, note that $1 \leq i \leq n$. For a point $Q \in \Pi_q \backslash \mathcal{K}$, call $\sigma_n(Q)$ the *index* of Q with respect to $\mathcal{K}$. Similarly, the index of a point $P \in \mathcal{K}$, denoted by $\rho_n(P)$, is the number of n-secants with which P is incident. Within this context, a (k, n)-arc $\mathcal{K}$ in Π_q is complete if no point of $\Pi_q \backslash \mathcal{K}$ has index zero. This means that, with respect to a complete (k, n)-arc $\mathcal{K}$, every point $Q \in \Pi_q \backslash \mathcal{K}$ lies on at least one n-secant to $\mathcal{K}$. Altering our perspective, subsets of $\Pi_q = \mathrm{PG}(2, q)$ can also be characterized by their incidence with the lines of the plane. A set $\mathcal{K}$ of size k is a k-set of *type* (m, n) if every line of Π_q meets $\mathcal{K}$ in either m or n points. The following k-sets are of particular importance.

Definition 2.4 (Unital, [8])**.** A unital in $\Pi_q = \mathrm{PG}(2, q)$, is a $(q\sqrt{q} + 1)$-set $\mathcal{U}$ of type $(1, \sqrt{q} + 1)$. That is, $\mathcal{U}$ is a set of size $q\sqrt{q} + 1$ in which every line of Π_q meets $\mathcal{U}$ in either 1 or $\sqrt{q} + 1$ points.

Definition 2.5 (Baer subplane, [8])**.** A Baer subplane of $\Pi_q = \mathrm{PG}(2, q)$ is a $(q + \sqrt{q} + 1)$-set $\mathcal{B}$ of type $(1, \sqrt{q} + 1)$.

Note 2.6. Although the theory of unitals and projective subplanes is itself the scope of considerable research, in this thesis, it is discussed only in respect to blocking sets; see Theorems 2.12 and 2.13.

Now, in analogy with the problem of enumerating the rational points on an algebraic curve, see Theorem 1.50, establishment of theoretical bounds for the size of a k-arc $\mathcal{K}$ of degree $n \geq 2$ in $\mathrm{PG}(2, q)$ is a point of considerable interest. Research in this direction began with a result by Bose, a result presented in Theorem 2.8. Prior to this, however, the following lemma is considered.

Lemma 2.7. *Let $\mathcal{K}$ be a k-arc in $\Pi_q = \mathrm{PG}(2, q)$. Then, for an external point $Q \in \Pi_q \backslash \mathcal{K}$, the following equality holds:*

$$\sigma_1(Q) + 2\sigma_2(Q) = k.$$

Proof With respect to the k-arc $\mathcal{K}$ in Π_q, a line meeting $\mathcal{K}$ is either a unisecant or a bisecant. Thus, for a fixed point $Q \in \Pi_q \backslash \mathcal{K}$, the lines of the plane meet $\mathcal{K}$ in either a pair of points or in a unique point. Taking account of both, it follows that $\sigma_1(Q) + 2\sigma_2(Q) = k$ which gives the result. ■

Theorem 2.8 (Bose, [13]). *Let $\mathcal{K}$ be a k-arc in* $\mathrm{PG}(2,q)$. *Then,*

(1) *if q is odd, $k \le q+1$;*

(2) *if q is even, $k \le q+2$.*

Proof (1) Suppose there is a $(q+2)$-arc $\mathcal{K}$ in $\Pi_q = \mathrm{PG}(2,q)$ with q odd. Counting the bisecants to $\mathcal{K}$ yields $(q+2)(q+1)/2$ bisecants in total with exactly $q+1$ at every point P of $\mathcal{K}$. This implies that every line containing a point P of $\mathcal{K}$ is a bisecant. Thus, for arbitrary $Q \in \Pi_q \backslash \mathcal{K}$, $\sigma_1(Q) = 0$; applying Lemma 2.7 to the point Q shows that $2\sigma_2(Q) = k = q+2$. Since q is odd, the latter is a contradiction.

(2) Suppose now that q is even and $\mathcal{K}$ is an oval in $\mathrm{PG}(2,q)$. Counting the bisecants to $\mathcal{K}$ gives $q(q+1)/2$, in total, with q at every point $P \in \mathcal{K}$. Thus, every point $P \in \mathcal{K}$ lies on a unique tangent line giving $q+1$ tangents in all. Now, consider an arbitrary bisecant ℓ in Π_q meeting $\mathcal{K}$ in the points P_1 and P_2 and fix an external point Q on ℓ. The size of $\mathcal{K} \backslash \{P_1, P_2\}$ is odd, q being even, so Lemma 2.7 implies that $\sigma_1(Q) \ge 1$. This holds for all such Q on ℓ. Now, on the one hand, as $\sigma_1(P_1) = \sigma_1(P_2) = 1$ and $\sigma_1(Q) \ge 1$ for $Q \in \mathcal{K}^c \cap \ell$, at least $q+1$ tangent lines to $\mathcal{K}$ meet ℓ. On the other hand, this being the total number of tangents in Π_q, the points of ℓ lie on exactly one tangent line. Now, ℓ being arbitrary, it follows that any two tangents to $\mathcal{K}$ meet at a point $\mathcal{N} \in \Pi_q \backslash \mathcal{K}$ not on any bisecant to $\mathcal{K}$. Thus, $\mathcal{N}$ contains all $q+1$ tangent lines to $\mathcal{K}$ and $\mathcal{K} \cup \{\mathcal{N}\}$ is, therefore, a hyperoval.

■

Developing upon the work of Bose, knowledge of both the size and structure of k-arcs was augmented considerably by Segre. For arbitrary q, it is readily verified that a non-singular conic $\mathcal{Q}$ in $\Pi_q = \mathrm{PG}(2,q)$, is a set of $q+1$ points, and, by virtue of Bézout's Theorem, see Theorem 1.43, no three of the points in $\mathcal{Q}$ are collinear. It follows that $\mathcal{Q}$ is an oval. If, however, q is odd, Segre demonstrated that the converse holds additionally, thereby providing a classification of ovals in planes of odd characteristic.

Theorem 2.9 (Segre, [37]). *In* $\mathrm{PG}(2,q)$*, with q odd, an oval is a conic.*

Examination of Theorem 2.9 is pertinent. It gives a combinatorial characterization of an algebraic curve. More specifically, Segre's result shows, in $\mathrm{PG}(2,q)$ with q odd, if no three points of an arbitrary set $\mathcal{Q}$ of size $q+1$ are collinear, then there exists a quadratic form $F \in \mathbf{F}_q[X,Y,Z]$ such that $\mathcal{Q} = \mathbf{V}(F)$. Here, $\mathbf{V}(F)$ is the variety of the polynomial F; see Definition 1.38. In contrast, however, in a projective plane of even order, ovals can be constructed which do not occur as the variety of a quadratic form. These ovals, therefore, do not admit representation as a conic and the classification of their corresponding hyperovals, for $q \geq 64$, is a significant outstanding problem. In this thesis, however, combinatorial arguments are presented for complete (k, n)-arcs in $\mathrm{PG}(2, q)$ of arbitrary degree $n \geq 2$, with particular attention given to cubic arcs. Note that because of their relationships with algebraic curves in $\mathrm{PG}(2, q)$, highlighted by Segre's characterization of non-singular conics in $\mathrm{PG}(2, q)$ with q odd, our interest in (k, n)-arcs is, in this thesis, restricted to the Desarguesian plane.

2.1.1 Arcs in relation to linear codes

Besides the combinatorial relationships shared by (k, n)-arcs and algebraic curves, the existence and classification of (k, n)-arcs is motivated by their close association with the theory of linear codes. If $\mathcal{V}$ is an m-dimensional vector space defined over a finite field $\mathbf{F}_q$, the *weight* of a non-zero vector $v \in \mathcal{V}$ is the number of its non-zero coordinates. Over a field $\mathbf{F}_q$, a linear $[m, s, d]_q$-code $\mathcal{C}$ of *length* m, *dimension* s and *minimum distance* d, is an s-dimensional subspace of $\mathcal{V}$ with all non-zero vectors $v \in \mathcal{C}$ of weight $w = w(v) \geq d$. Here, the integers m, s and d are the *parameters* of the code $\mathcal{C}$ and its elements are *words* or *codewords*. A matrix G is a *generator* matrix for the linear code $\mathcal{C}$ if its rows are a basis for $\mathcal{C}$. Also, the *dual* code, $\mathcal{C}^{\perp}$, of an $\mathbf{F}_q$-linear code $\mathcal{C}$, is the linear code consisting of all $y \in \mathcal{V}$ *orthogonal* to every $x \in \mathcal{C}$. Here, $x = (x_1, x_2, \ldots, x_m)$ and $y = (y_1, y_2, \ldots, y_m)$ are said to be orthogonal in $\mathcal{V}$ if $x_1y_1 + x_2y_2 + \ldots + x_my_m = 0$. Now, it is known, see [38], that a linear $[m, s, d]_q$-code $\mathcal{C}$ satisfies the following bound due to Singleton:

$$d \leq m - s + 1. \tag{2.1}$$

If the code $\mathcal{C}$ achieves equality here, it is *maximum distance separable* and is called an MDS-code. The difference $\delta(\mathcal{C}) = m - s + 1 - d$, of a linear $[m, s, d]_q$-code $\mathcal{C}$ failing to achieve equality is its *defect*. Also, $\mathcal{C}$ is *near* MDS or NMDS, precisely when $\delta(\mathcal{C}) = \delta(\mathcal{C}^{\perp}) = 1$. Now, an $[m + 1, s, d + 1]_q$-code $\mathcal{E}$ *extends* an $[m, s, d]_q$-code $\mathcal{C}$, if $\mathcal{C}$ is obtained from $\mathcal{E}$ by deleting a fixed coordinate from each codeword in $\mathcal{E}$. Note that if such a code $\mathcal{E}$ exists, the code $\mathcal{C}$ is said to be *extendable*. Otherwise, $\mathcal{C}$ is non-extendable.

Within the context of complete arcs, it has been shown, see [21], that existence of a complete $(k, 3)$-arc $\mathcal{K}$ in $\mathrm{PG}(2, q)$ is equivalent to the existence of a non-extendable NMDS-code $\mathcal{C}$ with parameters $[k, 3, k - 3]_q$. Alternatively, a code $\mathcal{C}$ is *projective* if every pair of columns in G, its generator matrix, is linearly independent over $\mathbf{F}_q$. It therefore follows that existence of a complete $(k, 3)$-arc $\mathcal{K}$ is equivalent to the existence of a non-extendable projective $[k, 3, k - 3]_q$-code $\mathcal{C}$.

2.1.2 Arcs in relation to blocking sets

This section gives an account of the relevant details from the theory of blocking sets. Wherever possible, the theory is discussed within the context of its implications for complete arcs in Desarguesian planes. A thorough description, however, is given in [22, Chapter 13].

Definition 2.10. A subset $\mathcal{B}$, of size k in $\Pi_q = \mathrm{PG}(2,q)$, is a (k,t)-*blocking set* if every line meets $\mathcal{B}$ in at least t points, with some line meeting $\mathcal{B}$ in exactly t points. Here, $\mathcal{B}$ is also called a t-fold blocking set of size k and, when $t = 1$, $\mathcal{B}$ is just a blocking set.

Note that if $Q \in \mathrm{PG}(2,q) \backslash \mathcal{B}$, where $\mathcal{B}$ is a blocking set in $\mathrm{PG}(2,q)$, then each line at Q meets $\mathcal{B}$ in at least one point. It follows that $\mathcal{B}$ has size $k \geq q+1$. On the other hand, since no two lines of a projective plane are parallel, the set of points on a line of $\mathrm{PG}(2,q)$ is a trivial example of a blocking set meeting the lower bound. A blocking set $\mathcal{B}$ is *non-trivial* if it contains no line of $\mathrm{PG}(2,q)$ entirely. From this it is readily deduced that the complement of a non-trivial blocking set is itself a blocking set. Finally, a blocking set $\mathcal{B}$ in which no proper subset is also a blocking set is *irreducible* or *minimal*.

Lemma 2.11. *A blocking set $\mathcal{B}$ in the projective plane $\Pi_q = \mathrm{PG}(2,q)$ is irreducible if and only if every point of $\mathcal{B}$ is incident with at least one tangent line in Π_q.*

Proof Assume that the blocking set $\mathcal{B}$ is minimal and fix an arbitrary point $P \in \mathcal{B}$. By minimality of $\mathcal{B}$, no proper subset $\mathcal{B}'$ of $\mathcal{B}$ is a blocking set. In particular, the set $\mathcal{B}' := \mathcal{B} \backslash \{P\}$ is not a blocking set. It follows that there is a line ℓ in Π_q such that $|\mathcal{B}' \cap \ell| = 0$. The set $\mathcal{B}$ is, however, a blocking set so $|\mathcal{B} \cap \ell| \geq 1$ for any line ℓ in Π_q. Together, these statements imply that $|\mathcal{B} \cap \ell| = 1$ and ℓ is therefore a unisecant at $P \in \mathcal{B}$. Since P is arbitrary, necessity has been established. Conversely, suppose that every point of $\mathcal{B}$ is incident with at least one tangent line in Π_q and let $\mathcal{B}'$ be a proper subset of the blocking set $\mathcal{B}$. Since $\mathcal{B}'$ is proper, there is a point $P \in \mathcal{B} \setminus \mathcal{B}'$ and a line ℓ in Π_q such that $\mathcal{B} \cap \ell = \{P\}$. It therefore follows that $\mathcal{B}' \cap \ell = \emptyset$ and thus $\mathcal{B}'$ is not a blocking set. Since $\mathcal{B}'$ is arbitrary, this establishes the result. ■

Bounds for both arbitrary and irreducible blocking sets have been well explored. In particular, the following Theorem by Bruen was the first significant result in this direction.

Theorem 2.12 (Bruen, [14]). *Let $\mathcal{B}$ be a non-trivial blocking set of size k in $\mathrm{PG}(2,q)$. Then, the following bounds hold:*

$$q + \sqrt{q} + 1 \;\leq\; k \;\leq\; q^2 - \sqrt{q}. \tag{2.2}$$

Here, an irreducible blocking set $\mathcal{B}$ has size $k = q + \sqrt{q} + 1$ if and only if q is square and $\mathcal{B}$

is a Baer subplane of $\mathrm{PG}(2,q)$*. If, on the other hand,* $\mathcal{B}$ *has size* $k = q^2 - \sqrt{q}$*, then* $\mathcal{B}$ *is the complement of a Baer subplane in* $\mathrm{PG}(2,q)$*.*

Aditionally, in [17], Bruen and Thas were later able to establish an upper bound to the size of an irreducible blocking set $\mathcal{B}$ in $\mathrm{PG}(2,q)$.

Theorem 2.13 (Bruen-Thas, [17])**.** *If* $\mathcal{B}$ *is an irreducible blocking set of size* k *in* $\mathrm{PG}(2,q)$*, then* $\mathcal{B}$ *satisfies the following bound:*

$$k \;\leq\; q\sqrt{q}+1. \tag{2.3}$$

Here, equality occurs if and only if $\mathcal{B}$ *is a unital.*

The interplay between $(k,2)$-arcs in Π_q and blocking sets in the dual plane Π_q^* is well established. The main results in this direction are presented in Propositions 2.15 and 2.16. Before this, however, the following nomenclature is introduced.

Definition 2.14. Let $\mathcal{B}$ be a t-fold blocking set of size r in the dual plane Π_q^* where $\Pi_q = \mathrm{PG}(2,q)$. Then, $\mathcal{B}$ is *derived* from the (k,n)-arc $\mathcal{K}$ if it is the image of the n-secants to $\mathcal{K}$ under a correlation $\phi : \Pi_q \longrightarrow \Pi_q^*$. Here, $\mathcal{B}$ is said to be (k,n)-arc derived. If $n = 2$, $\mathcal{B}$ is k-arc derived.

Proposition 2.15 (Bruen-Fisher, [15])**.** *Let* $\mathcal{K}$ *be a* k*-arc in* $\Pi_q = \mathrm{PG}(2,q)$*. If* $\mathcal{K}$ *is complete and* $k < q+2$ *then the bisecants to* $\mathcal{K}$ *induce a non-trivial blocking set* $\mathcal{B}$ *in the dual plane* Π_q^**.*

Proof Let $\mathcal{K}$ be a complete k-arc in $\Pi_q = \mathrm{PG}(2,q)$ and suppose that $\mathcal{B}$ is a subset of the dual plane Π_q^* induced by the bisecants to $\mathcal{K}$. Observe that every point of Π_q, both internal and external, is incident with at least one bisecant to $\mathcal{K}$. This means that every line of the dual plane Π_q^* meets the set $\mathcal{B}$. Now, if $\mathcal{K}$ has size $k < q+2$, then, since $k-1$ is the largest number of bisecants at a point of Π_q and $k-1 < q+1$, it follows that no line of Π_q^* is wholly contained in $\mathcal{B}$. Thus, $\mathcal{B}$ is a non-trivial blocking set. ■

Proposition 2.16 (Bruen-Fisher, [15])**.** *A blocking set* $\mathcal{B}$ *of size* r *is* k*-arc derived if and only if the following hold:*

(1) $r \leq k(k-1)/2$*;*

(2) *the number of* $(k-1)$*-secants incident with* $\mathcal{B}$ *is at least* k*;*

(3) *no three of the* $(k-1)$*-secants are concurrent.*

In this chapter, we adapt Propositions 2.15 and 2.16 to examine complete $(k,3)$-arcs in the plane $\Pi_q = \mathrm{PG}(2,q)$. In Proposition 2.29, a relationship between the size of a complete $(k,3)$-arc $\mathcal{K}$ in Π_q and its induced blocking set $\mathcal{B}$, in the dual plane Π_q^*, is established.

2.2 Bounds and equations for arcs in Desarguesian planes

The Tallini Scafati bound

Owing to their inherent complexity, few general bounds have been established for the size of a complete (k, n)-arc $\mathcal{K}$ in $\mathrm{PG}(2, q)$. Additionally, most attention has been directed towards combinatorial arguments imposing only upper bounds on the size of (k, n)-arcs in $\mathrm{PG}(2, q)$. The following proposition, presented by Tallini Scafati, was a formative result in this direction.

Proposition 2.17 (Tallini Scafati, [41])**.** *Let $\mathcal{K}$ be a set of size k in $\mathrm{PG}(2, q)$. If $\mathcal{K}$ is a (k, n)-arc, with $n \geq 2$, having at least one m-secant where $1 \leq m \leq n$, then $k \leq q(n-1)+m$. In particular, an arbitrary (k, n)-arc $\mathcal{K}$ satisfies the following bound:*

$$k \leq q(n-1)+n. \tag{2.4}$$

Proof Consider the (k, n)-arc $\mathcal{K}$ in $\Pi_q = \mathrm{PG}(2, q)$. Suppose that the line ℓ in Π_q meets $\mathcal{K}$ in exactly m points where $1 \leq m \leq n$. Pick a point $P \in \mathcal{K}$ incident with the line ℓ and count the points of $\mathcal{K}$ on the pencil of lines at P. Since Π_q has order q, Theorem 1.11 implies that

$$\rho_n(P) \leq q+1.$$

Thus, no more than q lines at P are incident with the $n-1$ points of $\mathcal{K} \setminus \{P\}$. This, together with those points of $\mathcal{K}$ incident with ℓ, yields $k \leq q(n-1)+m$. Finally, from the observations given in Note 2.3, an arbitrary k-arc of degree n is incident with at least one n-secant. Thus, taking $m = n$ in the first part of this proof gives $k \leq q(n-1)+n$ and thereby establishes the result. ■

Definition 2.18 (Large complete arcs)**.** Let $\mathcal{K}$ be a complete (k, n)-arc in $\mathrm{PG}(2, q)$. Then, the following nomenclature is used.

(1) If $k = q(n-1)+n$, then $\mathcal{K}$ is said to be *maximal*.

(2) If $\mathcal{K}$ is not maximal but is, however, the largest complete k-arc of degree n in $\mathrm{PG}(2, q)$, it is *extremal*.

Notation 2.19. (1) Let $m_n(2, q)$ denote the size of the largest complete (k, n)-arc in the plane $\mathrm{PG}(2, q)$.

(2) Similarly, let $t_n(2, q)$ denote the size of the smallest complete (k, n)-arc in $\mathrm{PG}(2, q)$.

The incidence equations

Now, Lemma 2.20 introduces an important collection of incidence equations for a set of points in $\Pi_q = \mathrm{PG}(2,q)$. These equations relate, in the most general possible sense, the size, the degree and the incidence properties of a (k,n)-arc $\mathcal{K}$ in $\mathrm{PG}(2,q)$ to the order of the plane Π_q in which $\mathcal{K}$ is embedded. Note in particular that the equations, having only integral solutions, are often called the Diophantine equations for a set of points in $\mathrm{PG}(2,q)$.

Lemma 2.20 (Incidence equations)**.** *Let $\mathcal{K}$ be a (k,n)-arc in $\mathrm{PG}(2,q)$. Then, the following equations hold:*

(i) $\sum\limits_{i=0}^{n} \tau_i = q^2+q+1,$

(ii) $\sum\limits_{i=1}^{n} i\tau_i = k(q+1),$

(iii) $\sum\limits_{i=1}^{n} i(i-1)\tau_i = k(k-1),$

(iv) $\sum\limits_{i=1}^{n} \rho_i(P) = q+1,$

(v) $\sum\limits_{i=2}^{n} (i-1)\rho_i(P) = k-1,$

(vi) $\sum\limits_{i=0}^{n} \sigma_i(Q) = q+1,$

(vii) $\sum\limits_{i=1}^{n} i\sigma_i(Q) = k,$

(viii) $\sum\limits_{P\in\mathcal{K}} \rho_i(P) = i\tau_i$ *with* $1 \leq i \leq n,$

(ix) $\sum\limits_{Q\in\pi\backslash\mathcal{K}} \sigma_i(Q) = (q+1-i)\tau_i$ *with* $0 \leq i \leq n,$

Proof In each case, a double counting argument is applied to an appropriate set $\mathcal{S}$. The complete combinatorial argument is given for the first three equalities. Proof of the remaining cases is only outlined.

(i) Fix $i \in [0,n]$ and let S_i be the set of all i-secants in Π_q, with $\mathcal{L}$ the set of all lines in Π_q. Thus, $\mathcal{L} = \bigcup\limits_{i=0}^{n} S_i$. Since the union is disjoint, the following equalities are obtained:

$$q^2+q+1 = \Big|\mathcal{L}\Big| = \Big|\bigcup_{i=0}^{n} S_i\Big| = \bigcup_{i=0}^{n}\Big|S_i\Big| = \sum_{i=0}^{n}\tau_i.$$

(ii) Count the flags in the set $S := \{(P,\ell) \mid P \in \mathcal{K} \text{ and } P \in \ell\}$. On the one hand, a fixed point $P \in \mathcal{K}$ is incident with $q+1$ lines in Π_q and a point $P \in \mathcal{K}$ may be selected in k ways. On the other hand, from a fixed i-secant in Π_q, a point $P \in \mathcal{K}$ can be chosen in i ways; τ_i is the total number of i-secants in Π_q. A sum over all m-secants for $1 \leq m \leq n$ yields the equality.

(iii) Count the triples in the set $S := \{(P, P', \ell) \mid P, P' \in \mathcal{K} \cap \ell,\ P \neq P'\}$. A pair of distinct points (P, P') is incident with a unique line in Π_q. Also, from $\mathcal{K}$, an *ordered* pair (P, P') can be selected in $k(k-1)$ ways. Conversely, fix an arbitrary i-secant ℓ in Π_q. An ordered pair (P, P') with $P \neq P'$ can be selected from ℓ in exactly $i(i-1)$ ways and the total number of i-secants in Π_q is just τ_i. Since (P, P') must be chosen from a line meeting $\mathcal{K}$ in at least two points, taking a sum over all m-secants with $2 \leq m \leq n$ yields the equality.

(iv) Count the total number of lines through a point P of $\mathcal{K}$.

(v) Count the elements of the set $S := \{(P', \ell) \mid P, P' \in \ell \cap \mathcal{K},\ P' \neq P\}$.

(vi) Count the number of lines through a point $Q \in \Pi_q \backslash \mathcal{K}$.

(vii) Count the elements of the set $S := \{(P, Q, \ell) \mid P \in \mathcal{K}, \ell = PQ\}$.

(viii) For a fixed $i \in [1, n]$, count the i-secants to $\mathcal{K}$ by counting the number of i-secants $\rho_i(P)$ at each point P of $\mathcal{K}$.

(ix) For a fixed $i \in [0, n]$, count the number of i-secants by counting the number of i-secants $\sigma_i(Q)$ at each point Q in $\Pi_q \backslash \mathcal{K}$.

■

2.2.1 Lower bounds for complete arcs in Desarguesian planes

In this subsection, a combinatorial technique establishing a lower bound for the general complete k-arc $\mathcal{K}$, see Theorem 2.21, is analyzed in depth. A central part of the research in this thesis has been to adapt this technique, presented by Barlotti in [3], to study complete arcs of arbitrary degree in $\mathrm{PG}(2, q)$. In Theorem 2.22, this allows us to establish a new lower bound for the size of the general complete (k, n)-arc $\mathcal{K}$ in $\mathrm{PG}(2, q)$. Crucially, the new result provides one of only two such bounds presently known.

Theorem 2.21 (Barlotti, [3]). *Let $\mathcal{K}$ be a k-arc in $\Pi_q = \mathrm{PG}(2, q)$ where $k < q + 1$. Then, if $\mathcal{K}$ is complete, the following bound holds*:

$$q \leq \frac{(k-1)(k-2)}{2}.$$

Proof If $\mathcal{K}$ is a k-arc in $\mathrm{PG}(2,q)$, the total number of its bisecants is $k(k-1)/2$ with exactly $k-1$ at each point $P \in \mathcal{K}$. Thus, each point $P \in \mathcal{K}$ is incident with $(q+1)-(k-1) = q+2-k$ unisecants. Since $k < q+1$, it follows that $\rho_1(P) > 0$ for any $P \in \mathcal{K}$. Thus, let ℓ be a tangent at some such point P in $\mathcal{K}$. Then, the number of bisecants to $\mathcal{K}$ not incident with P is

$$\frac{k(k-1)}{2} - (k-1) \;=\; \frac{(k-1)(k-2)}{2}.$$

By completeness, however, $\sigma_2(Q) \geq 1$ for every point Q on ℓ other than P itself. Since the unisecant ℓ contains exactly q such points Q, it follows that $q \leq (k-1)(k-2)/2$. ■

Observe that Barlotti's lower bound for the complete k-arc $\mathcal{K}$ is established by comparing the order q of the plane $\mathrm{PG}(2,q)$ with the number of bisecants meeting a tangent line to $\mathcal{K}$. From this perspective, it is reasonable to infer that efforts to extend Barlotti's result, to produce a lower bound for the general (k,n)-arc $\mathcal{K}$ of arbitrary degree, are contingent upon similar comparisons with the number of n-secants to $\mathcal{K}$ in $\mathrm{PG}(2,q)$. However, the secant distribution for the general (k,n)-arc, with $n \geq 3$, is far less amenable to combinatorial arguments. In this thesis, the incidence equations for the general (k,n)-arc $\mathcal{K}$ are successfully introduced as a means to establish the desired comparison. This method is now presented in Theorem 2.22.

Theorem 2.22 (Hirschfeld-Pichanick, [24]). *Let $\mathcal{K}$ be a complete (k,n)-arc in $\mathrm{PG}(2,q)$, where $n \geq 2$ and $q \geq n$. Then*

$$k \geq \sqrt{n(n-1)(q+1)}.$$

Proof The following standard equations for a (k,n)-arc $\mathcal{K}$ in $\mathrm{PG}(2,q)$, see Equations (iii) and (ix) of Lemma 2.20, are used:

$$\begin{aligned} \sum_{i=2}^{n} i(i-1)\tau_i &= k(k-1); && (2.5)\\ (q+1-i)\tau_i &= \sum_{Q\in\pi\backslash\mathcal{K}} \sigma_i(Q). && (2.6)\end{aligned}$$

Now, if $\mathcal{K}$ is complete, then $\sigma_n(Q) \geq 1$ for any $Q \in \Pi_q\backslash\mathcal{K}$; so equation (2.6) implies that

$$(q+1-n)\tau_n \geq (q^2+q+1)-k. \tag{2.7}$$

From equation (2.5), the following holds:

$$2\tau_2 + 6\tau_3 + \cdots + n(n-1)\tau_n = k(k-1).$$

Thus,

$$(n-1)(n-2)\tau_{n-1} + n(n-1)\tau_n \leq k(k-1)$$

and

$$(n-2)\tau_{n-1} + n\tau_n \leq \frac{k(k-1)}{(n-1)}.$$

Now, since $\tau_i \geq 0$ for any $i = 0, 1, \ldots, n$,

$$\begin{aligned} \tau_n \leq \tau_n + \frac{(n-2)}{n}\tau_{n-1} &= \frac{1}{n}\{n\tau_n + (n-2)\tau_{n-1}\} \\ &\leq \frac{1}{n}\left(\frac{k(k-1)}{n-1}\right). \end{aligned}$$

It has therefore been shown that the n-secants to a (k,n)-arc $\mathcal{K}$ satisfy the following bound:

$$\tau_n \leq \frac{k(k-1)}{n(n-1)}. \tag{2.8}$$

Substituting this expression into the left hand side of (2.7), the following bound is obtained:

$$(q+1-n)\tau_n \leq (q+1-n)\frac{k(k-1)}{n(n-1)}.$$

This implies that

$$q^2 + q + 1 - k \leq (q+1-n)\frac{k(k-1)}{n(n-1)},$$

and subsequent algebraic manipulation yields the following inequality:

$$\begin{aligned} q^2 + q + 1 &\leq (q+1-n)\frac{k(k-1)}{n(n-1)} + k, \\ &= \frac{k(q+1-n)(k-1) + k(n-1)n}{n(n-1)}. \end{aligned}$$

Thus, it follows that

$$q^2 + q + 1 \leq \frac{k}{n(n-1)}(kq + k - kn - q - 1 + n^2). \tag{2.9}$$

Now, observe that

$$kq + k - kn - q - 1 + n^2 \;=\; kq - k(n-1) - q - 1 + n^2.$$

Since $k \geq n$ and $n \geq 2$, the following inequality holds:

$$-k(n-1) \;\leq\; -n(n-1) = n - n^2.$$

Thus, using this inequality gives the following:

$$\begin{aligned} kq - k(n-1) - q - 1 + n^2 &\leq kq + n - n^2 - (q+1) + n^2 \\ &= kq + n - (q+1). \end{aligned}$$

Now, $q+1 > n$ and so $n - (q+1) < 0$; therefore $kq + n - (q+1) < kq$. Using this last inequality in (2.9) yields the following bound:

$$q(q+1) < q^2 + q + 1 \leq \frac{k^2 q}{n(n-1)};$$

thus

$$n(n-1)(q+1) \leq k^2.$$

Finally, taking square roots,

$$k \geq \sqrt{n(n-1)(q+1)}. \tag{2.10}$$

This establishes the result. ■

Observe that the proof of Theorem 2.22 is dependent upon establishing that, for a (k,n)-arc $\mathcal{K}$, the number of its n-secants τ_n satisfies the following estimate:

$$\tau_n \leq \frac{k(k-1)}{n(n-1)}.$$

This suggests that the n-secants to a (k,n)-arc play a pivotal role in the imposition of bounds and is a concept explored throughout this thesis. Also, observe that considerable utility in Theorem 2.22 is gained by its validity for k-arcs of arbitrary degree $n \geq 2$. This is in contrast to much of the existing work in this direction, see [30], [31] and [7] for example, where bounds are established using restrictions upon n and q. Indeed, only in [34] has another lower bound for general arcs of arbitrary degree been established. There, a lower bound for k, the size of a (k,n)-arc $\mathcal{K}$ covering a (t,m)-arc $\mathcal{T}$ disjoint from $\mathcal{K}$, is obtained by counting the minimum number of lines $\mu(\mathcal{T})$ in a *covering* of $\mathcal{T}$. A covering of $\mathcal{T}$ by $\mathcal{K}$ is a collection of i-secants to $\mathcal{K}$, where $i \geq 2$, such that $\mathcal{T}$ lies in their union. For completeness, the result is presented in the following theorem.

Theorem 2.23 (Siaw-Lynn Ng, [34]). *Let $\mathcal{T}$ be a (t,m)-arc covered by a (k,n)-arc $\mathcal{K}$ in* $\mathrm{PG}(2,q)$*. Then*

$$k \geq \frac{1 + \sqrt{4(n^2 - n + 2\mu(\mathcal{T})) - 7}}{2},$$

where

$$\mu(\mathcal{T}) \geq \begin{cases} t/m & \text{if } m \leq q-1, \\ m & \text{if } m > q-1. \end{cases}$$

Proof See [34, Chapter 4]. ■

Further comparisons between the Barlotti bound for $(k, 2)$-arcs, see Theorem 2.21, and the bound presented in Theorem 2.22 are pertinent. Theorem 2.21 gives a necessary condition for the existence of a complete k-arc in $\mathrm{PG}(2, q)$. It indicates that, in the case of a $(k, 2)$-arc $\mathcal{K}$, for the arc to be complete, it is necessary that $k \geq \sqrt{2q + \frac{1}{4}} + \frac{3}{2}$. Owing to its validity for k-arcs of arbitrary degree, the lower bound presented in Theorem 2.22 gives a necessary condition for the existence of a general complete (k, n)-arc $\mathcal{K}$. However, specializing Theorem 2.22 to arcs of degree two yields the following corollary.

Corollary 2.24. *In* $\mathrm{PG}(2, q)$, *if* $\mathcal{K}$ *is a complete* k*-arc then*

$$k \geq \sqrt{2q + 2}\,.$$

Better estimates for bounds on small complete k-arcs have been discovered since the original work of Barlotti. In [2, Chapter 3], Ball showed that for arbitrary q, a complete arc in $\mathrm{PG}(2, q)$ has size $k \geq \lfloor \sqrt{2q} + 2 \rfloor$. There it was also shown that if $q = p^h$, with p prime and $1 \leq h \leq 2$, then the lower bound for a complete k-arc $\mathcal{K}$ can be improved to $k \geq \sqrt{3q} + \frac{1}{2}$. This culminated in a result by Polverino, see [35], who extended Ball's result to include the case $q = p^3$. Crucially, in [2, Chapter 3], Ball uses blocking sets induced, in the dual plane Π_q^*, by a k-arc $\mathcal{K}$ in the plane $\Pi_q = \mathrm{PG}(2, q)$. Ball's result inspires some of the methodology underpinning later work on cubic arcs in this thesis; for this reason, it is pertinent to examine its proof in some detail. Accordingly, the result is presented in the following theorem.

Theorem 2.25 (Ball, [2])**.** *Let* $\mathcal{K}$ *be a* k*-arc in the plane* $\Pi_q = \mathrm{PG}(2, q)$, *with* q *arbitrary. Then, if* $\mathcal{K}$ *is complete, it follows that*

$$k \geq \lfloor \sqrt{2q} + 2 \rfloor.$$

Proof By Proposition 2.15, it is known that the bisecants to a complete $(k, 2)$-arc $\mathcal{K}$ in the plane $\Pi_q = \mathrm{PG}(2, q)$ induce a blocking set $\mathcal{B}$ in the dual plane Π_q^*. Thus, application of Bruen's lower bound to the set $\mathcal{B}$, see Theorem 2.12, implies that $|\mathcal{B}| \geq q + 1 + \sqrt{q}$. Now, the total number of bisecants to the k-arc $\mathcal{K}$ is $k(k-1)/2$ so it follows that

$$\frac{k(k-1)}{2} \geq q + 1 + \sqrt{q}.$$

Basic algebraic manipulation then shows that $k \geq \lfloor \sqrt{2q} + 2 \rfloor$ which establishes the result. ■

It is instructive to compare, in planes of small order, some of the numerical values attained by the above theoretical bounds. Towards this end, the following notation for these bounds is introduced.

Notation 2.26.

Let $b_n(2,q) = \left\lceil \sqrt{n(n-1)(q+1)} \ \right\rceil$, where $\lceil r \rceil$ is the smallest integer of size at least r;

let $B(q) = \left\lceil \frac{3}{2} + \sqrt{2q + \frac{1}{4}} \ \right\rceil$;

let $S(q) = \left\lceil \sqrt{2q} + 2 \ \right\rceil$.

Table 2.1: Comparison of lower bounds for complete k-arcs in $\mathrm{PG}(2,q)$ for $2 \leq q \leq 11$.

q	2	3	4	5	7	8	9	11
$b_2(2,q)$	3	3	4	4	4	5	5	5
$B(q)$	4	4	5	5	6	6	6	7
$S(q)$	4	5	5	6	6	6	7	7

Table 2.1 makes it clear that in planes of small order, the lower bounds given by both Barlotti and Ball are better than the lower bound given by $b_n(2,q)$ in Theorem 2.22, when the latter is specialized to arcs of degree two. This is not unexpected, however, given the applicability of the bound $b_n(2,q)$ to k-arcs of arbitrary degree $n \geq 2$.

Proceeding with an empirical analysis of the bound $b_n(2,q)$, our focus is briefly restricted to $(k,3)$-arcs in $\mathrm{PG}(2,q)$. Table 2.2 compares the exact numerical values attained by cubic arcs of both largest and smallest size to the corresponding theoretical bound given by $b_n(2,q)$ when $n = 3$. Note that in Table 2.2, for $q = 4$, the complete reference is [22, Chapter 12].

Table 2.2: Bounds for complete $(k,3)$-arcs for $4 \leq q \leq 16$.

q	4	5	7	8	9	11	13	16
$b_3(2,q)$	6	6	7	8	8	9	10	11
$t_3(2,q)$	7	9	9	11	12	13	15	15
$m_3(2,q)$	9	11	15	15	17	21	23	28
References	[22]	[18]	[18]	[18]	[18]	[18]	[18]	[7]

Continuing with this restriction of attention to plane $(k, 3)$-arcs, Theorem 2.22 yields the following result for projective codes.

Theorem 2.27. *Let $\mathcal{C}$ be a projective $[k, 3, k-3]_q$ code over a field $\mathbf{F}_q$ where $k < \sqrt{6q+6}$. Then, the code $\mathcal{C}$ is extendable.*

Proof Observe that by §2.1.1 p.21, existence of a complete $(k, 3)$-arc $\mathcal{K}$ is equivalent to the existence of a projective code $\mathcal{C}$ with parameters $[k, 3, k-3]_q$. Thus, taking $n = 3$ in Theorem 2.22 the result immediately follows by contraposition.

■

This section concludes with Corollary 2.28. Note, in particular, that Corollary 2.28 indicates that if the degree of a complete (k, n)-arc $\mathcal{K}$ is large enough, then $\mathcal{K}$ necessarily contains at least as many points as there are within a line of the plane.

Corollary 2.28. *Let $\mathcal{K}$ be a complete (k, n)-arc in $\mathrm{PG}(2, q)$ where $n \geq \sqrt{q} + 1$. Then it follows that $k > q$.*

Proof By virtue of Theorem 2.22, the following holds:

$$k \geq \sqrt{n(n-1)(q+1)} \ > \sqrt{(n-1)^2(q+1)} = (n-1)\sqrt{q+1}.$$

Now, if $n \geq \sqrt{q} + 1$, then the following inequalities hold:

$$(n-1)\sqrt{q+1} \geq \sqrt{q}\,\sqrt{q+1} > q.$$

It therefore follows that $k > q$, which establishes the result.

■

2.3 New results for complete cubic arcs using blocking sets

Aspects of the structure of $(k, 3)$-arcs in $\mathrm{PG}(2, q)$ are now investigated. In particular, in Proposition 2.29, a new sufficient condition establishing the existence of at least one trisecant at the internal points of a $(k, 3)$-arc $\mathcal{K}$ in $\mathrm{PG}(2, q)$ is given. Also, in Theorems 2.37 and 2.38, the combinatorial technique originally invoked by Ball in Theorem 2.25, to study complete $(k, 2)$-arcs in $\mathrm{PG}(2, q)$, is adapted to give a classification of complete cubic arcs in terms of their trisecants. Note that Proposition 2.29 adapts the technique developed by Bruen and Fisher in Proposition 2.15 to the more complicated incidence structure of the $(k, 3)$-arc in $\mathrm{PG}(2.q)$.

Proposition 2.29. *Let $\mathcal{K}$ be a $(k,3)$-arc in $\Pi_q = \mathrm{PG}(2,q)$. If $k > q+2$, then the following statements hold.*

(1) *Every point of $\mathcal{K}$ is incident with at least one trisecant.*

(2) *If $\mathcal{K}$ is complete, its trisecants induce a blocking set $\mathcal{B}$ in the dual plane Π_q^*.*

Proof The following two equations for an arbitrary point P in a (k,n)-arc $\mathcal{K}$ in $\mathrm{PG}(2,q)$ are used; see Equations (iv) and (v) of Lemma 2.20:

$$\begin{aligned}\sum_{i=2}^{n}(i-1)\rho_i(P) &= (k-1),\\ \sum_{i=1}^{n}\rho_i(P) &= (q+1).\end{aligned}$$

Thus, taking $n=3$ in both of these equations gives the following:

$$\rho_2(P)+2\rho_3(P) = k-1, \tag{2.11}$$

$$\rho_1(P)+\rho_2(P)+\rho_3(P) = q+1. \tag{2.12}$$

Taking the difference (2.11) $-$ (2.12), the following equality is obtained:

$$\rho_3(P)-\rho_1(P) = (k-1)-(q+1).$$

It therefore follows that

$$\begin{aligned}\rho_3(P) &= \rho_1(P)+(k-q-2)\\ &\geq k-q-2.\end{aligned}$$

Thus, taking $k > q+2$ ensures that P is incident with at least one trisecant to $\mathcal{K}$. Since P is arbitrary, if $k > q+2$, it necessarily implies that $\rho_3(P) > 0$ for any $P \in \mathcal{K}$.

Finally, if $\mathcal{K}$ is assumed to be complete, it follows that every point of Π_q is incident with at least one trisecant to $\mathcal{K}$ and so, in the dual plane Π_q^*, each line meets some point induced by a trisecant to $\mathcal{K}$; so the trisecants induce a blocking set.

■

Witness the central differences between Propositions 2.29 and 2.15. Examining the structure of a complete cubic arc $\mathcal{K}$ in $\mathrm{PG}(2,q)$, à priori, it is not even clear that all the points of $\mathcal{K}$ are incident with a trisecant. This is in stark contrast to the properties of a $(k,2)$-arc in $\mathrm{PG}(2,q)$. Thus, in $\Pi_q = \mathrm{PG}(2,q)$, in contrast to a k-arc derived blocking set, the parameters of a $(k,3)$-arc derived blocking set $\mathcal{B}$ are less easily determined. Here, $\mathcal{B}$ is an (r,t)-blocking set where $r = \tau_3$, the number of trisecants to $\mathcal{K}$, and t, defined as the smallest number of points in $\mathcal{B}$ with which a line of Π_q^* is incident, is equal to the smallest number of trisecants at any point P of the plane $\Pi_q = \mathrm{PG}(2,q)$. Again, à priori, it is not even known if the point P is an element of $\mathcal{K}$. An important logical inference can, however, be made. Since the $(k,3)$-arc $\mathcal{K}$ is assumed to be complete in Proposition 2.29, and since $k > q+2$, it follows that $t \geq 1$.

In [2, Chapter 2], Ball was able to extend Bruen's result governing the minimal size of a blocking set in $\mathrm{PG}(2,q)$, see Theorem 2.12, to include the general t-fold blocking set with $t \geq 1$. This is presented in the following theorem.

Theorem 2.30 (Ball, [2]). *Let $\mathcal{B}$ be a t-fold blocking set of size k in $\Pi_q = \mathrm{PG}(2,q)$, with $t \geq 1$. If $\mathcal{B}$ contains no line of Π_q entirely, then it follows that $k \;\geq\; qt + \sqrt{qt} + 1$.*

Application of Theorem 2.30 to a $(k,3)$-arc derived blocking set $\mathcal{B}$ is, therefore, contingent upon prior demonstration that the set $\mathcal{B}$ does not contain a line. To address this, a hitherto unseen result of Barlotti and Thas is now briefly introduced. For convenience in subsequent proofs in Chapter 2, the theorem is numbered both here and in Chapter 3. Its context and relevance, however, is only fully discussed in Chapter 3 of this thesis; see material before and after Theorem 3.9.

Theorem 2.31 (Barlotti-Thas; see [4] and [42]). *Let $\mathcal{K}$ be a complete $(k,3)$-arc in $\mathrm{PG}(2,q)$. If $q \geq 4$, then $k \leq 2q+1$.*

The Barlotti-Thas upper bound, presented in Theorem 2.31, is now used to obtain a suitable contradiction in the proof of Proposition 2.32.

Proposition 2.32. *If $\mathcal{B}$ is a $(k,3)$-arc derived blocking set in $\Pi_q = \mathrm{PG}(2,q)$ then $\mathcal{B}$ does not contain a line of Π_q and is, consequently, non-trivial.*

Proof Suppose that the blocking set $\mathcal{B}$ in Π_q is derived from the trisecants to a complete $(k,3)$-arc $\mathcal{K}$ in the dual plane Π_q^*. Now, assume for the purpose of contradiction that the set $\mathcal{B}$ contains a line $\ell \subset \Pi_q$. Thus, there is a set of $q+1$ collinear points in $\mathcal{B}$ and, since the points of $\mathcal{B}$ are induced by the trisecants of $\mathcal{K}$, we may conclude by duality that there is a pencil of $q+1$ trisecants at some point P in Π_q^*. We may therefore distinguish the following two cases. If $P \in \mathcal{K}$ then, counting the points of $\mathcal{K}$ on the pencil of lines at P, it follows that $k = 2q+3$. This, however, contradicts the Barlotti-Thas upper bound for cubic arcs. If $P \in \Pi_q^* \backslash \mathcal{K}$, on the other hand, then $\sigma_3(P) = q+1$ and, by Lemma 2.20(vii), it follows that $k = \sigma_1(P) + 2\sigma_2(P) + 3\sigma_3(P) \;\geq\; 3(q+1)$. This is a contradiction of the Tallini Scafati bound, Proposition 2.17, applied to cubic arcs.

■

Thus, Proposition 2.32 permits application of Theorem 2.30 to establish a lower bound to the number of trisecants τ_3 with which a complete cubic arc $\mathcal{K}$ in $\mathrm{PG}(2,q)$ is incident. This yields the following lower bound:

$$\tau_3 \geq qt + \sqrt{qt} + 1 \quad \text{where } t \geq 1. \tag{2.13}$$

This bound is now investigated for possible restrictions upon cubic arcs. In particular, owing to their secant distributions being more amenable to combinatorial arguments, the discussion is specialized to regular cubic arcs.

Definition 2.33 (Regular Arc)**.** Let $\mathcal{K}$ be a (k,n)-arc in $\mathrm{PG}(2,q)$. The arc is *regular* if, for any point $P \in \mathcal{K}$, the index $\rho_3(P) = e$ for some constant $e \geq 1$. The constant e is the *density* of the arc.

Note 2.34. Since $\mathcal{K}$ is a $(k,3)$-arc there exists at least one point $P \in \mathcal{K}$ incident with a trisecant. Thus, by regularity, all points of $\mathcal{K}$ are incident with at least one trisecant; so $e \geq 1$. Therefore, if a regular cubic arc in Π_q is complete, it induces a blocking set in Π_q^*.

Consider Equation (viii) of Lemma 2.20 for a (k,n)-arc $\mathcal{K}$ in $\mathrm{PG}(2,q)$:

$$\sum_{P \in \mathcal{K}} \rho_i(P) = i\tau_i.$$

Putting $i = 3$ gives the following:

$$3\tau_3 = \sum_{P \in \mathcal{K}} \rho_3(P) = \rho_3(P_1) + \rho_3(P_2) + \cdots + \rho_3(P_k).$$

Now, by the regularity of $\mathcal{K}$, for any $i = 2, \ldots, k$ it follows that $\rho_3(P_1) = \rho_3(P_i) = e$ for some constant $e \in \mathbf{N}$; hence

$$3\tau_3 = ke \ \text{ and } \ \tau_3 = ke/3. \tag{2.14}$$

Thus, combining Equation (2.14) with the inequality given in (2.13), the following estimate for the number of trisecants is obtained for a cubic arc which is both regular and complete:

$$\frac{ke}{3} \geq tq + \sqrt{tq} + 1.$$

Thus,

$$k \geq \frac{3}{e}(tq + \sqrt{tq} + 1). \tag{2.15}$$

This is investigated for specific values of e and t.

Lemma 2.35. *Let $\mathcal{K}$ be a regular cubic arc with density e in $\Pi_q = \mathrm{PG}(2,q)$. Assume further that $\mathcal{K}$ induces an (r,t)-blocking set $\mathcal{B}$ in the dual plane Π_q^*. Then, it follows that $e > t$.*

Proof Assume that $e \leq t$. Then $1 \leq t/e$ and so (2.15) becomes the following:

$$k \geq \frac{3}{e}(tq + \sqrt{tq} + 1) \geq 3q + \frac{3}{e}(\sqrt{tq} + 1) > 2q + 1.$$

This contradicts the Barlotti-Thas upper bound, see Theorem 2.31, for the largest possible size of a complete cubic arc in $\mathrm{PG}(2,q)$. Conclude, therefore, that $e > t$. ■

Lemma (2.35) implies that if $\mathcal{K}$ is a complete regular cubic arc, then there exists a point $Q \in \Pi_q \backslash \mathcal{K}$ such that $\sigma_3(Q) < e$. This follows since, if $\mathcal{B} \subset \Pi_q^*$ is the induced (r,t) blocking set, then, by definition, there is some line of Π_q^* meeting $\mathcal{B}$ in exactly t points, where t is some constant with $t \geq 1$. By Lemma (2.35), this line must correspond to a point $Q \in \Pi_q \backslash \mathcal{K}$. This observation is used in the proof of the following result.

Proposition 2.36. *Let $\mathcal{K}$ be a regular $(k,3)$-arc in $\mathrm{PG}(2,q)$. If $\mathcal{K}$ is complete, then $k \leq \tau_3$.*

Proof If $\mathcal{K}$ is regular, all its points are incident with either an odd or even number of trisecants.

First, assume that all points of $\mathcal{K}$ are incident with an odd number of trisecants and write $\rho_3(P_i) = 2m_i + 1 = e$ where $i = 1, 2, \ldots, k$ and e is the density of the arc. Now, observe that Lemma 2.35 implies that $m_i > 0$ for any i. So, enumerating the points of the arc gives the following equality:

$$3\tau_3 = \sum_{P \in \mathcal{K}} \rho_3(P) = \rho_3(P_1) + \rho_3(P_2) + \cdots + \rho_3(P_k).$$

Thus

$$3\tau_3 = (2m_1 + 1) + (2m_2 + 1) + \cdots + (2m_k + 1) = 2(m_1 + \cdots + m_k) + k.$$

Now, let m_s be defined as follows:

$$m_s = \min_{1 \leq i \leq k} (m_i) = m_1 = \cdots = m_k.$$

Then, it is clear that

$$3\tau_3 = 2m_s k + k = k(2m_s + 1),$$

and

$$k = \frac{3\tau_3}{2m_s + 1}.$$

Now, $m_s \geq 1$ implies that $2m_s + 1 \geq 3$; so

$$\frac{3}{2m_s+1} \leq 1$$

and it follows that

$$\frac{3\tau_3}{2m_s+1} \leq \tau_3.$$

Therefore,

$$|\mathcal{K}| = k \leq \tau_3.$$

Now, suppose that the points of $\mathcal{K}$ are incident with an even number of trisecants and write $\rho_3(P_i) = 2m_i = e$ for any $i = 1, 2, \ldots, k$, where $m_i > 0$ for every i. Enumerating the points of the arc as before, the following holds:

$$3\tau_3 = \sum_{P \in \mathcal{K}} \rho_3(P) = \rho_3(P_1) + \cdots + \rho_3(P_k).$$

By assumption, therefore, it follows that

$$3\tau_3 = 2m_1 + \cdots + 2m_k = 2(m_1 + \cdots + m_k).$$

From the definition of m_s,

$$2(m_1 + \cdots + m_k) = 2km_s \text{ and } 3\tau_3 = 2km_s.$$

Now, $m_i \neq 0$ for any $i = 1, 2 \ldots, k$ and since, by assumption, $\rho_3(P_i)$ is even for every $P_i \in \mathcal{K}$,

$$m_s \geq 2, \qquad 2m_s \geq 4, \qquad 1 \geq \frac{4}{2m_s};$$

therefore $1 \geq 3/(2m_s)$. Since

$$3\tau_3 \ = \ 2km_s$$

it follows that

$$\tau_3 \ \geq \ \frac{3}{2m_s}\tau_3 \ = \ k.$$

This proves that $\tau_3 \geq k$ in both of the above cases and therefore establishes the result. ■

The relation between the size of a cubic arc which is both regular and complete and the number of its trisecants, is now extended to a general complete $(k, 3)$-arc $\mathcal{K}$ in $\mathrm{PG}(2, q)$.

Theorem 2.37. *Consider the $(k,3)$-arc $\mathcal{K}$ in $\mathrm{PG}(2,q)$. If $\tau_3 \leq k$, then the following statements hold:*

(1) $k \leq q+5$;

(2) *if $\mathcal{K}$ is complete, then $q+2 \leq k \leq q+5$.*

Proof (1) Assume that $\mathcal{K}$ is a $(k,3)$-arc in $\Pi_q = \mathrm{PG}(2,q)$ where $\tau_3 \leq k$. Now, taking $n=3$ in Equations (ii) and (iii) of Lemma 2.20, the following equalities are obtained:

$$\tau_1 + 2\tau_2 + 3\tau_3 = k(q+1) \tag{2.16}$$

$$2\tau_2 + 6\tau_3 = k(k-1). \tag{2.17}$$

Taking their difference yields the following equality:

$$3\tau_3 - \tau_1 = k(k-q-2). \tag{2.18}$$

Thus,

$$3\tau_3 = \tau_1 + k(k-q-2). \tag{2.19}$$

Now, $\tau_3 \leq k$ so $3\tau_3 \leq 3k$ and it follows that $3k \geq \tau_1 + k(k-q-2)$. Since $k > 0$, division by k yields the following:

$$3 \geq \frac{\tau_1}{k} + k - q - 2.$$

Thus, it follows that

$$q + 5 - k \geq \frac{\tau_1}{k}.$$

Observe also that τ_1/k is certainly non-negative and hence $q+5-k \geq 0$ from which it follows that

$$q + 5 \geq k.$$

This establishes the first part of the proof.

(2) In order to prove (2), suppose now that the $(k,3)$-arc $\mathcal{K}$ is additionally complete. Then, by virtue of Equation (ix) in Lemma 2.20, it follows that

$$(q-2)\tau_3 \geq q^2 + q + 1 - k.$$

By assumption, however, $k \geq \tau_3$ which implies that

$$(q-2)k \ \geq \ q^2 + q + 1 - k.$$

Thus, after basic algebraic manipulation, the following inequality is obtained:

$$k(q-1) \geq q^2 + q + 1.$$

This, in turn, yields $k \geq (q^2+q+1)/(q-1)$ from which it follows that $k > (q^2+q+1)/q$. We may therefore conclude that $k > q+1$ which establishes the result.

■

Observe that Theorem 2.37 imposes a narrow range of values in which a complete cubic arc $\mathcal{K}$, satisfying the above conditions, can exist. This section concludes with an improvement to Theorem 2.37. Using Proposition 2.29, the following result further excludes the values of k which may be achieved by a complete $(k,3)$-arc $\mathcal{K}$ satisfying prescribed incidence conditions.

Theorem 2.38. *Let $\mathcal{K}$ be a complete $(k,3)$-arc in the projective plane $\Pi_q = \mathrm{PG}(2,q)$ with $q \geq 17$. Then, if $k \geq \tau_3$, it follows that $k = q+2$.*

Proof Assume that there exists a complete $(k,3)$-arc $\mathcal{K}$ in Π_q where $\tau_3 \leq k$ and suppose that $k \in \{q+3, q+4, q+5\}$. Now, Proposition 2.29 implies that the trisecants to the $(k,3)$-arc $\mathcal{K}$ constitute a blocking set in the dual plane Π_q^*. Thus, by virtue of Theorem 2.37, the following inequalities are obtained:

$$q+5 \geq k \geq \tau_3 \geq q+1+\sqrt{q}. \tag{2.20}$$

Since $q \geq 17$, however, the following holds:

$$q+1+\sqrt{q} \ > \ q+5.$$

Thus, owing to the inequalities presented in (2.20), it readily follows that

$$q+5 \ \geq \ k \geq q+1+\sqrt{q} > q+5.$$

This is a contradiction and therefore establishes the result.

■

Chapter 3

Elliptic curves and extremal cubic arcs

3.1 Cubic arcs of the largest size

In $\mathrm{PG}(2,q)$, cubic curves yield a simple method of constructing $(k,3)$-arcs and their associated codes. Indeed, Bézout's Theorem shows that the point-set of a cubic curve with at least one trisecant is a $(k,3)$-arc. The converse, however, need not hold. Because no line of $\mathrm{PG}(2,q)$ meets a cubic arc in more than three points, the general $(k,3)$-arc $\mathcal{K}$ necessarily satisfies Bézout's Theorem, but it need not satisfy the Hasse-Weil Theorem. Indeed, the Hasse-Weil theorem shows that $|\mathcal{C}| \leq 18$ for any cubic curve $\mathcal{C}$ in $\mathrm{PG}(2,11)$, and yet, in [30], a $(21,3)$-arc is presented in that plane. Thus, the set of cubic curves is contained in the set of cubic arcs of $\mathrm{PG}(2,11)$. In this chapter, the extent to which these sets coincide more widely is of central interest. Begin by finding the values attained by non-singular cubic curves in the Hasse-Weil interval.

Theorem 3.1 (Waterhouse, [44])**.** *Let $\mathbf{F}_q$ be a finite field of order $q = p^k$. Then, there is an elliptic curve E over $\mathbf{F}_q$ such that $|E(\mathbf{F}_q)| = q + 1 - t$ if and only if one of the following conditions is satisfied:*

(1) $t \not\equiv 0 \pmod{p}$ *and* $t^2 \leq 4q$;

(2) *k is odd and one of the following holds additionally:*

  (a) $t = 0$,

  (b) $p = 2$ *and* $t^2 = 2q$,

  (c) $p = 3$ *and* $t^2 = 3q$;

(3) *k is even and one of the following holds additionally:*

  (a) $t^2 = 4q$,

  (b) $p \not\equiv 1 \pmod{3}$ *and* $t^2 = q$,

  (c) $p \not\equiv 1 \pmod{4}$ *and* $t = 0$.

Proof For a concise proof, the reader is advised to consult [36, Chapter 3]. ■

Corollary 3.2 (Waterhouse, [44]). *There exists an elliptic curve E over $\mathbf{F}_q$ such that $|E(\mathbf{F}_q)| = N_1$ for every integer N_1 in the Hasse-Weil interval if and only if one of the following conditions holds:*

(1) *q is prime;*

(2) *q is the square of a prime p and one of the following holds additionally:*

  (a) $p = 2$ *or* $p = 3$,

  (b) $p \equiv 11 \pmod{12}$.

Let $N_q(1)$ and $L_q(1)$ denote respectively the largest and smallest number of rational points on an arbitrary non-singular cubic curve in $\mathrm{PG}(2, q)$. Also, for an odd integer $h \geq 3$, the prime power $q = p^h$ is *exceptional* if p divides $2\sqrt{q}$. Otherwise, q is *non-exceptional*. Then, Theorem 3.1 yields the following corollary, see [16].

Corollary 3.3 (Waterhouse, [44]). *In the plane $\Pi_q = \mathrm{PG}(2, q)$, the integers $N_q(1)$ and $L_q(1)$ satisfy the following equalities:*

$$N_q(1) = \begin{cases} q + 1 + 2\sqrt{q}, & \textit{if } q \textit{ is non-exceptional} \\ q + 2\sqrt{q}, & \textit{if } q \textit{ is exceptional}; \end{cases}$$

$$L_q(1) = \begin{cases} q + 1 - 2\sqrt{q}, & \textit{if } q \textit{ is non-exceptional} \\ q + 2 - 2\sqrt{q}, & \textit{if } q \textit{ is exceptional}. \end{cases}$$

When considering relationships between complete $(k, 3)$-arcs and non-singular cubic curves in $\mathrm{PG}(2, q)$, comparison of $m_3(2, q)$ and $N_q(1)$ is a good first point of inquiry. From Corollary 3.3, it is readily deduced that $m_3(2, q)$ satisfies the following bounds:

$$m_3(2, q) \geq \begin{cases} q + 2\sqrt{q} & \text{if } q \text{ is exceptional,} \\ q + 1 + 2\sqrt{q} & \text{if } q \text{ is non-exceptional.} \end{cases} \tag{3.1}$$

From Table 3.1, which gathers all known values of $m_3(2, q)$, it is evident that in all but one instance, however, $m_3(2, q)$ exceeds $N_q(1)$. This empirical analysis has prompted the following conjecture.

Conjecture 3.4 (Hirschfeld, [23]). *If $q \neq 4$ then $m_3(2, q) > N_q(1)$.*

Note 3.5. In Table 3.1, the reference for $m_3(2, 2)$ has been omitted owing to its immediacy. Indeed, observe that a subset $\mathcal{K}$ of $\Pi = \mathrm{PG}(2, 2)$ cannot contain four collinear points since each line of Π is incident with exactly three points. Also, for $q = 4$, the complete reference is [22, Chapter 12].

Table 3.1: Comparison of $N_q(1)$ and $m_3(2,q)$ for $q \leq 16$.

q	2	3	4	5	7	8	9	11	13	16
$N_q(1)$	5	7	9	10	13	14	16	18	21	25
$m_3(2,q)$	7	9	9	11	15	15	17	21	23	28
References		[26]	[22]	[18]	[18]	[18]	[18]	[18]	[18]	[7]

The comparison of $m_3(2,q)$ with existing theoretical upper bounds for complete $(k,3)$-arcs in $\mathrm{PG}(2,q)$ is another point of inquiry. For example, when the discussion is narrowed to complete cubic arcs, the Tallini Scafati bound given in Proposition 2.17 demonstrates that $m_3(2,q) \leq 2q+3$ for any $q \geq 2$. Now, theoretical bounds for the general extremal cubic arc can, to some extent, be improved by a classification of all $(k,3)$-arcs in a plane $\Pi_q = \mathrm{PG}(2,q)$ of specific order. Such a classification, predominantly given up to projective equivalence, is dependent upon exhaustive computational searches which, by their nature, are restricted to planes of low order. An example of research in this direction is given by the work of Coolsaet and Sticker, see [18], which gives a classification of complete $(k,3)$-arcs in planes of order $q \leq 13$; their work is later discussed within the context of minimal cubic arcs in §3.3, p.53.

However, broader efforts to understand the size and structure of $(k,3)$-arcs in the general Desarguesian plane $\mathrm{PG}(2,q)$, were greatly aided by the following result of Cossu concerning the existence of maximal arcs of arbitrary degree.

Theorem 3.6 (Cossu, [19])**.** *Suppose that $\mathcal{K}$ is a maximal (k,n)-arc in the plane $\Pi_q = \mathrm{PG}(2,q)$ where $2 \leq n < q$. Then, the following statements hold:*

(1) *the external lines to $\mathcal{K}$ form a maximal $((q+1-n)q/n, q/n)$-arc $\mathcal{K}'$ in the dual plane Π_q^*;*

(2) *in particular, $n \mid q$.*

Note that when Theorem 3.6 is applied to cubic arcs in $\mathrm{PG}(2,q)$, it precludes the existence of $(2q+3,3)$-arcs in Desarguesian planes of order $q \neq 3^h$. Additionally, Cossu established the non-existence of a $(21,3)$-arc in the plane $\mathrm{PG}(2,9)$. This augmented upon the work of Barlotti who had earlier established the following results.

Theorem 3.7 (Barlotti, [4])**.** *Suppose that $\mathcal{K}$ is a (k,n)-arc of size $k = q(n-1)+(n-1)$ in the plane $\Pi_q = \mathrm{PG}(2,q)$. Then $\mathcal{K}$ is incomplete.*

Theorem 3.8 (Barlotti, [4])**.** *If $\mathcal{K}$ is a (k,n)-arc in the plane $\Pi_q = \mathrm{PG}(2,q)$ where $q \not\equiv 0 \pmod{n}$ and $2 < n < q$, then $k \leq q(n-1)+n-2$.*

Application of Theorem 3.8 to $(k,3)$-arcs demonstrates, in particular, that $m_3(2,q) \leq 2q+1$ if $\gcd(3,q)=1$. Later, in [42], Thas extended Barlotti's result to arbitrary planes of order $q \geq 4$. Accordingly, the work of Barlotti and Thas yields the following seminal result.

Theorem 3.9 (Barlotti-Thas, [4] and [42]). *Let $\mathcal{K}$ be a complete $(k,3)$-arc in $\mathrm{PG}(2,q)$. If $q \geq 4$ then $k \leq 2q+1$.*

No further improvements have been made to this bound, however, since Thas's publication in 1975, the majority of known numerical values for $m_3(2,q)$ being obtained by exhaustive computational searches in planes of small order. Current consensus however, see [2, Chapter 1], is that the Barlotti-Thas upper bound is, in general, too high. A brief analysis of Table 3.2 bears testament to this. Crucially, Table 3.2 shows that in planes of order q, with $7 < q \leq 16$, the Barlotti-Thas upper bound is never attained.

Table 3.2: Comparison of $m_3(2,q)$ with the Barlotti-Thas upper bound for $4 \leq q \leq 16$.

q	4	5	7	8	9	11	13	16
$2q+1$	9	11	15	17	19	23	27	33
$m_3(2,q)$	9	11	15	15	17	21	23	28
References	[22]	[18]	[18]	[18]	[18]	[18]	[18]	[7]

3.2 New combinatorial methods for large cubic arcs

In this section, a new combinatorial analysis of large $(k,3)$-arcs satisfying specific incidence conditions in $\mathrm{PG}(2,q)$ is given. This analysis begins by considering the differences between $m_3(2,q)$ and the constant $2q+1$, enshrined by the Barlotti-Thas upper bound. Here, we first prove that for a specific class of cubic arcs, the Barlotti-Thas upper bound is never attained. This later enables a new comparison of $m_3(2,q)$ and $N_q(1)$ in planes of a suitable order.

Theorem 3.10 (Hirschfeld-Pichanick, [24]). *Let $\mathcal{K}$ be a complete $(k,3)$-arc of largest possible size in $\Pi_q = \mathrm{PG}(2,q)$, where each trisecant to $\mathcal{K}$ contains at least one point $Q \in \Pi_q \backslash \mathcal{K}$ of index one. If $q \geq 17$, then it follows that $k < \frac{3}{2}\left(q+\sqrt{q}+2\right)$.*

Proof Let $k = m_3(2,q)$ and define $m = \min\{\rho_3(P) \mid P \in \mathcal{K}\}$. Then, without loss of generality, assume that $\rho_3(P_1) = m$, relabelling if necessary. Counting the points of $\mathcal{K}$ on a pencil of lines through P_1, the following equality is obtained:

$$k = 2(m-1) + 3 + (q+1-m-\rho_1(P_1)).$$

It follows that

$$k = m + 2 + q - \rho_1(P_1).$$

If q is exceptional, then the inequalities presented in (3.1) yield the following:

$$k = m + 2 + q - \rho_1(P_1) \geq q + 2\sqrt{q}.$$

Therefore, the following bounds hold:

$$\begin{aligned} m &\geq 2\sqrt{q} + \rho_1(P_1) - 2, \\ &\geq 2\sqrt{q} - 2. \end{aligned}$$

Thus, for q exceptional, an arbitrary point P of a cubic arc with the largest possible size is incident with no fewer than $2\sqrt{q} - 2$ trisecants. Thus, the following holds:

$$\begin{aligned} \tau_3 &\geq \frac{k}{3}(2\sqrt{q} - 2) \\ &= \frac{2k}{3}(\sqrt{q} - 1). \end{aligned}$$

On the other hand, if q is non-exceptional, further application of the inequalities presented in (3.1) yields the following:

$$k = m + 2 + q - \rho_1(P_1) \geq q + 1 + 2\sqrt{q}.$$

In this instance, therefore, the following bounds are obtained:

$$\begin{aligned} m &\geq 2\sqrt{q} + \rho_1(P_1) - 1, \\ &\geq 2\sqrt{q} - 1. \end{aligned}$$

Hence, for q non-exceptional, an arbitrary point P of a cubic arc with the largest possible size is incident with no fewer than $2\sqrt{q} - 1$ trisecants. It follows that

$$\begin{aligned} \tau_3 &\geq \frac{k}{3}(2\sqrt{q} - 1) \\ &\geq \frac{k}{3}(2\sqrt{q} - 2) \\ &= \frac{2k}{3}(\sqrt{q} - 1). \end{aligned}$$

This establishes the following bound, valid for q both exceptional and non-exceptional:

$$k \leq \frac{3\tau_3}{2(\sqrt{q}-1)}.$$

Now, since $\mathcal{K}$ has the largest possible size, it follows that $k > q+2$. Thus, Proposition 2.29 implies that the trisecants to $\mathcal{K}$ induce a blocking set $\mathcal{B}$ in Π_q^*. Because each trisecant is, by assumption, incident with a point $Q \in \Pi_q \backslash \mathcal{K}$ of index one, the induced blocking set is irreducible. Applying the Bruen-Thas upper bound for an irreducible blocking set, see Theorem 2.13, it follows that $\tau_3 \leq q\sqrt{q}+1$, and the following bound is obtained:

$$k \leq \frac{3}{2}\left(\frac{q\sqrt{q}+1}{\sqrt{q}-1}\right).$$

Now, observe that

$$\frac{q\sqrt{q}+1}{\sqrt{q}-1} = \frac{q\sqrt{q}-1+2}{\sqrt{q}-1} = \frac{q\sqrt{q}-1}{\sqrt{q}-1} + \frac{2}{\sqrt{q}-1},$$

where

$$q\sqrt{q}-1 = (\sqrt{q})^3 - 1 = (\sqrt{q}-1)(q+\sqrt{q}+1).$$

Thus, the following holds:

$$k \leq \frac{3}{2}\left(q+\sqrt{q}+1+\frac{2}{\sqrt{q}-1}\right). \tag{3.2}$$

Since $q \geq 17$, it follows that

$$\sqrt{q}-1 > \sqrt{16}-1 = 3.$$

This yields the following estimate:

$$\frac{2}{\sqrt{q}-1} < \frac{2}{3}.$$

Application of this upper bound to the inequality presented in (3.2), yields the following estimates:

$$k \leq \frac{3}{2}\left(q+\sqrt{q}+1+\frac{2}{3}\right) < \frac{3}{2}\left(q+\sqrt{q}+2\right).$$

This establishes the result. ■

Analysis of this result is pertinent. Under only a single additional assumption on the geometry of the plane, Theorem 3.10 gives a significant improvement to the Barlotti-Thas upper bound. Although it is not known if there is a cubic arc satisfying the conditions of Theorem 3.10, it demonstrates that $\rho_3(P) \geq 2\sqrt{q}-2$ for an arbitrary point P in a complete cubic arc $\mathcal{K}$ of largest possible size. The existence, therefore, of such an arc is dependent upon the smallest number of trisecants with which a point $Q \in \Pi_q \backslash \mathcal{K}$ is incident. Note also that the proof of Theorem

3.10 yields an explicit relationship between the size of $\mathcal{K}$ and the number of its trisecants. This relationship is presented in Corollary 3.11.

Corollary 3.11. *Let $\mathcal{K}$ be a complete $(k, 3)$-arc in $\mathrm{PG}(2, q)$ of the largest possible size. Then, for $q \geq 17$, the following bound holds*:

$$k \leq \frac{3\tau_3}{2\sqrt{q} - 2}.$$

Proof Let $\mathcal{K}$ be a complete $(k, 3)$-arc of the largest possible size in $\mathrm{PG}(2, q)$. In the proof of Theorem 3.10, it is shown that for q both exceptional and non-exceptional, if $q \geq 17$, k satisfies the following bound:

$$k \leq \frac{3\tau_3}{2\sqrt{q} - 2}. \tag{3.3}$$

This establishes the result. ■

Now, an intuitive estimate for complete $(k, 3)$-arcs of the largest possible size is provided. Observe that, for $q \geq 17$, the following holds:

$$\sqrt{q} - 1 > \sqrt{q} - \frac{1}{4}\sqrt{q} = \frac{3}{4}\sqrt{q}.$$

By Corollary 3.11, therefore, it follows that

$$k < \frac{3/2}{(3\sqrt{q}/4)}\tau_3 \;=\; \frac{2}{\sqrt{q}}\tau_3.$$

Now, observe that, for $q \geq 17$,

$$\frac{2}{\sqrt{q}} < \frac{1}{2}.$$

Thus, if $\mathcal{K}$ is a complete $(k, 3)$-arc of largest possible size in $\mathrm{PG}(2, q)$ then it follows that

$$k < \frac{2}{\sqrt{q}}\tau_3 \;<\; \frac{\tau_3}{2}. \tag{3.4}$$

Recall that in Theorem 2.38 it was shown that, for an arbitrary complete $(k, 3)$-arc $\mathcal{K}$ in $\mathrm{PG}(2, q)$ with $q \geq 17$, if $k \geq \tau_3$ then $k = q + 2$. By contraposition, this means that a complete cubic arc of size $k \neq q + 2$, in a plane of order $q \geq 17$, satisfies the estimate $k < \tau_3$. In Corollary 3.11 and its subsequent discussion, we have shown that if $\mathcal{K}$ is, in addition, assumed to be of largest possible size, then this estimate can be improved to $k < \tau_3/2$.

Theorem 3.10 and Corollary 3.11 suggest that examination of the known secant distributions for extremal cubic arcs is instructive. A combinatorial approach to Conjecture 3.4, predicated upon the secant distributions listed in Table 3.3, is now presented.

Note 3.12. In Table 3.3, the distribution with the smallest number of trisecants is given whenever projectively distinct cubic arcs are known to exist.

Table 3.3: Secant distributions for extremal cubic arcs where $7 \leq q \leq 16$.

q	7	8	9	11	13	16
τ_0	12	18	17	28	44	63
τ_1	0	0	18	21	26	56
τ_2	15	30	16	21	43	42
τ_3	30	25	40	63	70	112
References	[18]	[18]	[5]	[30]	[31]	[7]

Here, Table 3.3 illustrates that, for $q \neq 8$, $\tau_3 \geq \max(\tau_0, \tau_1, \tau_2)$. Because of the counterexample in $\mathrm{PG}(2,8)$, extremal cubic arcs are now explored by imposing a weaker combinatorial assumption on the lines of the plane.

Lemma 3.13. *Let $\mathcal{K}$ be a $(k,3)$-arc in the plane $\Pi_q = \mathrm{PG}(2,q)$ satisfying the following pair of conditions:*

(1) $\tau_2 + \tau_3 \geq \max(\tau_0, \tau_1)$;

(2) $\tau_2 + \tau_3 \leq 6q\sqrt{q}$.

Then, it follows that $k < 24\sqrt{q}$.

Proof Assume first that $\tau_2 + \tau_3 \geq \max(\tau_0, \tau_1)$ and similarly that $\tau_2 + \tau_3 \leq 6q\sqrt{q}$. By Lemma 2.20 (ii), an arbitrary (k,n)-arc $\mathcal{K}$ in the plane Π_q satisfies the following standard equation:

$$\sum_{i=1}^{n} i\tau_i = k(q+1). \tag{3.5}$$

Taking $n = 3$ in (3.5) yields the following equality:

$$\tau_1 + 2\tau_2 + 3\tau_3 = k(q+1). \tag{3.6}$$

However, by assumption, $\tau_2 + \tau_3 \geq \max(\tau_0, \tau_1)$. Application of this to Equation (3.6) therefore yields the following bound:

$$4(\tau_2 + \tau_3) \geq k(q+1).$$

Now, since $\tau_2 + \tau_3 \leq 6q\sqrt{q}$, it follows that

$$k \leq \frac{4(\tau_2 + \tau_3)}{q+1} \leq 24\left(\frac{q\sqrt{q}}{q+1}\right).$$

Therefore, since $q+1>q$, the following bound for the size of the $(k,3)$-arc $\mathcal{K}$ is obtained:

$$k < \frac{24q\sqrt{q}}{q} = 24\sqrt{q}.$$

This establishes the result. ■

Theorem 3.14. *Suppose $\mathcal{K}$ is a complete $(k,3)$-arc of largest possible size in $\mathrm{PG}(2,q)$ where $q \geq 483$. If $\tau_2+\tau_3 \geq \max(\tau_0,\tau_1)$ and $\tau_2 < 2q\sqrt{q}$, then the following estimate holds:*

$$k > q+1+3\sqrt{q}.$$

Proof Since $\mathcal{K}$ is, by assumption, a cubic arc of largest possible size, the inequalities given in (3.1) indicate that $k \geq q+2\sqrt{q}$, for both exceptional and non-exceptional values of q. Furthermore, since $q \geq 483$, the following inequalities hold:

$$k \geq q+2\sqrt{q} > 483+2\sqrt{483} > 24\sqrt{q}.$$

By contraposition, in Lemma 3.13, either $\tau_2+\tau_3 < \max(\tau_0,\tau_1)$ or $\tau_2+\tau_3 > 6q\sqrt{q}$. Assumption, however, precludes the former and it follows that

$$\tau_2+\tau_3 > 6q\sqrt{q}. \tag{3.7}$$

Now, by Corollary 3.11 and its subsequent observations, it is clear that for $\mathcal{K}$, a complete $(k,3)$-arc in $\mathrm{PG}(2,q)$ of largest possible size, for $q \geq 17$ the following bound holds:

$$k \leq \frac{3\tau_3}{2\sqrt{q}-2}. \tag{3.8}$$

Application of this inequality to Equation (3.6) yields the following estimate:

$$\tau_1+2\tau_2+3\tau_3 < kq + \frac{3\tau_3}{2\sqrt{q}-2}.$$

Therefore,

$$\tau_1+2\tau_2+2\tau_3+\left(1-\frac{3}{2\sqrt{q}-2}\right)\tau_3 < kq$$

and it follows that

$$(\tau_2+\tau_3)+(\tau_1+\tau_2+\tau_3)+\left(1-\frac{3}{2\sqrt{q}-2}\right)\tau_3 < kq. \tag{3.9}$$

Now, since $\tau_2 + \tau_3 > \max(\tau_0, \tau_1)$, the following inequality is obtained:

$$(\tau_2 + \tau_3) + (\tau_1 + \tau_2 + \tau_3) > \tau_0 + \tau_1 + \tau_2 + \tau_3 = q^2 + q + 1.$$

Here, the latter equality is again obtained from the standard equations, see Equation (i) of Lemma 2.20, for a (k, n)-arc $\mathcal{K}$ in $\mathrm{PG}(2, q)$. This argument has thus established that

$$q^2 + q + 1 + \left(1 - \frac{3/2}{\sqrt{q} - 1}\right) \tau_3 < kq. \tag{3.10}$$

Now, by assumption, $\tau_2 < 2q\sqrt{q}$. Thus, since $\tau_2 + \tau_3 > 6q\sqrt{q}$, it follows that

$$\tau_3 = (\tau_2 + \tau_3) - \tau_2 \ > \ 6q\sqrt{q} - \tau_2 \ > \ 6q\sqrt{q} - 2q\sqrt{q} \ = \ 4q\sqrt{q}.$$

This yields the following estimate:

$$q^2 + q + 1 + \left(1 - \frac{3/2}{\sqrt{q} - 1}\right) 4q\sqrt{q} < kq. \tag{3.11}$$

Here,

$$\begin{aligned} \left(1 - \frac{3/2}{\sqrt{q} - 1}\right) 4q\sqrt{q} &= 4q(\sqrt{q} - 5/2)\frac{\sqrt{q}}{\sqrt{q} - 1}, \\ &> 4q(\sqrt{q} - 5/2). \end{aligned}$$

Also, observe that $4q(\sqrt{q} - 5/2) = 3q\sqrt{q} + (q\sqrt{q} - 10q) \geq 3q\sqrt{q}$ for $q \geq 100$. Here, since $q \geq 483$ by assumption, it follows that

$$kq > q^2 + q + 1 + 3q\sqrt{q}.$$

Finally, division by q yields the following bound:

$$k > q + 1 + 3\sqrt{q}.$$

This establishes the result. ■

Regarding elliptic curves, Theorem 3.14 immediately yields the following corollary.

Corollary 3.15. *Let $\mathcal{K}$ be a complete $(k, 3)$-arc of largest possible size in $\mathrm{PG}(2, q)$ where $q \geq 483$. If $\tau_2 + \tau_3 \geq \max(\tau_0, \tau_1)$ and $\tau_2 < 2q\sqrt{q}$, then $k > N_q(1)$, the largest number of rational points on an elliptic curve.*

The answers given by Corollary 3.15 to Conjecture 3.4 are evidently restricted by the presence of any incidence conditions. The corollary does, however, yield a sufficient condition for the positive resolution of the Hirschfeld conjecture, and, although a general proof of the conjecture has not been achieved in this thesis, Corollary 3.15 narrows the combinatorial properties of any possible counterexample.

3.3 Combinatorics of small cubic arcs

Conditions ensuring the completeness of plane $(k, 3)$-arcs is our final point of inquiry. This is particularly relevant when constructing projective codes admitting no proper extensions. Proposition 2.29, see Chapter 2, gives a condition which ensures that $\rho_3(P) \geq 1$ for any internal point P of a suitable cubic arc $\mathcal{K}$. In contrast, it yields no information regarding the external points of $\mathcal{K}$. Resolution of this problem for arbitrary $(k, 3)$-arcs, having no additional structure, is presently intractable. In this section, owing to their structure as algebraic curves, cubic arcs obtained from elliptic curves are examined for completeness. Theorem 3.16 is a significant result in this direction.

Theorem 3.16 (Hirschfeld-Voloch, [27]). *If $q \geq 79$ is not a power of 2 or 3, then an elliptic curve $\mathcal{C}$ with n rational points is a complete cubic arc unless the j-invariant $j(\mathcal{C}) = 0$, in which case the completion of $\mathcal{C}$ has at most $n + 3$ points.*

Attempts have been made to extend Theorem 3.16 to elliptic curves with arbitrary j-invariant. In particular, in [20], Giulietti obtains the following extension of the Hirschfeld-Voloch theorem.

Theorem 3.17. *Let $\mathbf{F}_q$ be a finite field of characteristic $p > 3$ where $q = p^h > 9887$ and either h is even or $p \equiv 1 \pmod 3$. Then, an elliptic curve E with $j(E) = 0$ and having an even number of $\mathbf{F}_q$-rational points is a complete cubic arc.*

Since Theorems 3.16 and 3.17 only hold in $\mathrm{PG}(2, q)$ if $q \geq 79$ and $q > 9887$ respectively, efforts have since been directed towards extensions to planes of lower order. In [1], Alderson and Bruen obtain the following result which gives a sufficient condition for the completeness of a curve based only on its size.

Theorem 3.18 (Alderson-Bruen, [1]). *Suppose $\mathcal{C}$ is a non-singular cubic curve of size N_1 in $\Pi_q = \mathrm{PG}(2, q)$ where $N_1 > q + 7$. Then, each point $Q \in \Pi_q \backslash \mathcal{C}$ is incident with at least one trisecant to $\mathcal{C}$ and, in particular, $\mathcal{C}$ is a complete cubic arc.*

Proof Let $\mathcal{C}$ be an incomplete non-singular cubic curve of size $N_1 > q + 7$. Then, there exists a point $Q \in \Pi_q \backslash \mathcal{C}$ where $\sigma_3(Q) = 0$. By Lemma 1.52, $\gamma(\mathcal{C}) \leq 6$ where $\gamma(\mathcal{C})$ is the class of the cubic curve $\mathcal{C}$, that is, the largest number of tangent lines to $\mathcal{C}$ incident with a point $Q \in \Pi_q \backslash \mathcal{C}$;

see Definition 1.51, p.17. Thus, Q is incident with at most 6 tangent lines to $\mathcal{C}$. Now, because no tangent line meets an arbitrary cubic curve, say Γ, in more than two distinct points, as $\mathcal{C}$ is a cubic curve, it follows that $\sigma_2(Q) \leq 6$. Counting the points of $\mathcal{C}$ on a pencil of lines at Q, the following equality is obtained:

$$\sigma_1(Q) + 2\sigma_2(Q) + 3\sigma_3(Q) = N_1.$$

Also, in a plane of order q, it is clear that $\sigma_1(Q) + \sigma_2(Q) + \sigma_3(Q) \leq q + 1$. Thus, writing $N_1 = \sigma_1(Q) + \sigma_2(Q) + \sigma_3(Q) + \sigma_2(Q) + 2\sigma_3(Q)$, it follows that

$$N_1 \leq q + 1 + \sigma_2(Q) + 2\sigma_3(Q) \leq q + 1 + 6 + 2\sigma_3(Q).$$

This implies that

$$N_1 \leq q + 7 + 2\sigma_3(Q) = q + 7 < N_1,$$

which is a contradiction. ■

The following result extends the combinatorial approach used by Alderson and Bruen to arbitrary $(k, 3)$-arcs. Proposition 3.19 establishes a sufficient condition for the completeness of a general cubic arc $\mathcal{K}$ in $\mathrm{PG}(2, q)$.

Proposition 3.19. *Let $\mathcal{K}$ be a $(k, 3)$-arc in $\Pi_q = \mathrm{PG}(2, q)$ where $\sigma_1(Q) \not\equiv k \pmod 2$ for any point $Q \in \Pi_q \backslash \mathcal{K}$. Then $\mathcal{K}$ is complete.*

Proof Assume, for the purpose of contradiction, that the $(k, 3)$-arc $\mathcal{K}$ is incomplete. Then, there exists a point $Q_0 \in \Pi_q \backslash \mathcal{K}$ such that $\sigma_3(Q_0) = 0$. Application of Lemma 2.20(vii) to the point Q_0 yields the following equality:

$$\sigma_1(Q_0) + 2\sigma_2(Q_0) + 3\sigma_3(Q_0) = k.$$

Here, however, $\sigma_3(Q_0) = 0$. Thus, $\sigma_1(Q_0) + 2\sigma_2(Q_0) = k$ and it follows that $k - \sigma_1(Q_0)$ is even. The latter implies that $k \equiv \sigma_1(Q_0) \pmod 2$ which is a contradiction. ■

Algebraic arguments are now used to count the rational points on an elliptic curve with zero j-invariant; this being the sole case in which an elliptic curve is incomplete as a plane $(k, 3)$-arc. By Equation (1.9), the affine equation for an elliptic curve E over a field $\mathbf{F}_q$ of characteristic $p > 3$ is $Y^2 = X^3 + aX + b$. Thus, Definition 1.49 implies that the curve E has zero j-invariant over $\mathbf{F}_q$ precisely when $a = 0$. This observation is used in Theorem 3.21 which extends the Alderson-Bruen result in planes of suitable order to a broader range of elliptic curves.

Notation 3.20. Recall that N_1 denotes the number of $\mathbf{F}_q$-rational points on a non-singular cubic curve.

Theorem 3.21. *Let E be an elliptic curve of size N_1 over a field $\mathbf{F}_q$ of characteristic $p > 3$. Then, if $\gcd(3, q-1) = 1$ and $N_1 \neq q+1$, the following statements hold:*
(1) *the curve E has non-zero j-invariant;*
(2) *if $q \geq 79$, then the curve E is complete as a plane cubic arc.*

Proof (1). Here, the proof is given by contradiction. Let E be an arbitrary elliptic curve over the field $\mathbf{F}_q$, of characteristic $p > 3$, and suppose that $j(E) = 0$. The above observations imply that the affine equation for the curve E is of the form $Y^2 = X^3 + b = f(X)$ for some $b \in \mathbf{F}_q^*$. Consider the map ϕ given by the following identity:

$$\phi : \mathbf{F}_q \longrightarrow \mathbf{F}_q,$$
$$\phi(x) = x^3 \text{ for any } x \in \mathbf{F}_q.$$

Restriction of ϕ to the set $\mathbf{F}_q^*$ induces a group homomorphism $\tilde{\phi}$ on the group $\mathbf{F}_q^*$ with multiplicative identity $1_{\mathbf{F}_q^*}$. Here, $\tilde{\phi}(x) = x^3 \; \forall \; x \in \; \mathbf{F}_q^*$ and it is now demonstrated that $\tilde{\phi}$ is a bijection.

Suppose $\tilde{\phi}(x_1) = \tilde{\phi}(x_2)$ for arbitrary elements x_1, x_2 in $\mathbf{F}_q^*$. Then, since $x_2 \in \mathbf{F}_q^*$ has a multiplicative inverse, it follows that $(x_1^3)(x_2^{-1})^3 = 1_{\mathbf{F}_q^*}$ and, by commutativity, the following equality is obtained:

$$(x_1 x_2^{-1})^3 = 1_{\mathbf{F}_q^*}. \tag{3.12}$$

Equation (3.12) implies that the order n of the group element $g = x_1 x_2^{-1}$ divides 3 which yields only two possibilities; namely, $n = 3$ or $n = 1$. Existence, however, of an element g of order 3 in the group $\mathbf{F}_q^*$, of order $q-1$, is a contradiction since $\gcd(q-1, 3) = 1$. Thus, g has order 1 and it follows that $x_1 x_2^{-1} = 1_{\mathbf{F}_q^*}$, from which we may deduce that $x_1 = x_2$. Thus, $\tilde{\phi}$ is an injection on $\mathbf{F}_q^*$ and consequently the map ϕ is an injection on $\mathbf{F}_q$. Now, as a translate of ϕ, the map $X^3 + b$ is an injection on $\mathbf{F}_q$ for every $b \in \mathbf{F}_q^*$ and, by virtue of the pigeon-hole principle, is therefore also a bijection. This establishes a correspondence between the affine points of E and the quadratic residues attained by f in $\mathbf{F}_q$. Observe, in particular, that a non-zero residue yields two distinct points on the curve E. Now, accounting for the points $(0:0:1)$ and $\mathcal{O} = (0:1:0)$, the latter being the unique ideal point on E, the number of rational points is given by the following equalities:

$$N_1 = 1 + 1 + 2\left\{\frac{q-1}{2}\right\} = q + 1.$$

This is a contradiction and thereby establishes (1). Now, consider the finite field $\mathbf{F}_q$ of characteristic

$p > 3$ where $\gcd(3, q-1) = 1$ and suppose that E is an elliptic curve in $\mathrm{PG}(2,q)$ of size $N_1 \neq q+1$. By the preceding result, the curve E has non-zero j-invariant and, since the field $\mathbf{F}_q$ has order $q \geq 79$ and characteristic $p > 3$, the Hirschfeld-Voloch theorem implies that E is complete. This establishes (2) and the result follows.

■

Now, recall from Notation 2.19, the size of the smallest possible complete cubic arc in a plane of order q is denoted by $t_3(2,q)$. Also, in Table 2.2, in addition to the known numeric values attained by complete cubic arcs of largest size, those attained by all the known complete $(k,3)$-arcs of smallest possible size were also given; see p.31.

Although (k,n)-arcs of minimal size in $\mathrm{PG}(2,q)$ have, in general, received less attention than their opposites, interest in minimal arcs remains prevalent, not least because of interest in the packing problem for (k,n)-arcs in $\mathrm{PG}(2,q)$; see [25] for further details regarding the packing problem. The classification of complete $(k,3)$-arcs in $\mathrm{PG}(2,q)$, with q fixed, is the principal method by which the packing problem is resolved. Accordingly, efforts to make computation more tractable by improvements to underlying search algorithms is an object of interest. Basic algorithms use a recursive method which generates a $(k,3)$-arc $\mathcal{K}$ from either a $(k',2)$-arc or $(k',3)$-arc $\mathcal{K}'$, with $\mathcal{K}' \subset \mathcal{K}$, through selection of an appropriate point $Q \in \Pi_q \backslash \mathcal{K}'$. The $(k,3)$-arc $\mathcal{K} = \mathcal{K}' \cup \{Q\}$ is then tested for completeness and the process repeated until all cubic arcs are found. Finally, a selection of representatives for the projectively distinct cubic arcs of a fixed size k_0 is made. Here, $(k,3)$-arcs of both largest and smallest size emerge as a mere by-product of the process, and, as the order of the plane increases, the algorithms need improvement.

Notation 3.22. Let 2^{Π} denote the set of all subsets of the set Π.

Now, on the one hand, improvements to these algorithms emerge through elimination of redundancies. For example, in [18], Coolsaet and Sticker adapt the method of *isomorph free* generation, developed by McKay in [32], to the classification of complete $(k,2)$ and $(k,3)$-arcs in $\mathrm{PG}(2,q)$. Narrowing our description of their algorithm to k-arcs, Coolsaet and Sticker improve the recursive algorithm, generating a k-arc $\mathcal{K}$ from a $(k-1)$-arc $\mathcal{K}'$ with $\mathcal{K}' \subset \mathcal{K}$, by introducing a function $F : 2^{\Pi} \longrightarrow 2^{\Pi}$ which selects a point $Q \in \Pi_q = \mathrm{PG}(2,q)$ from a subset $\mathcal{O} \subset \Pi_q$. The point Q is then incorporated to form the k-arc $\mathcal{K} = \mathcal{K}' \cup \{Q\}$. Here, F is chosen to identify subsets $\mathcal{O}$ of Π_q which minimize redundancy. Further improvements to the algorithm are earned through better selections of the function F; see [18] and [32]. On the other hand, speed in classification is also aided by improvements to the theoretical bounds $m_3(2,q)$ and $t_3(2,q)$; improvement in these bounds offers potential to reduce the size of the relevant search space. In this respect, Theorem 3.21 is now used to establish new theoretical bounds for complete $(k,3)$-arcs of minimal size.

Theorem 3.23. *Consider the projective plane* $\Pi_q = \mathrm{PG}(2, q)$ *over a field* $\mathbf{F}_q$ *of characteristic* $p > 3$ *where* $q \geq 79$*. Then, the following statements hold:*

(1) *if* q *is either a prime or a square then* $t_3(2, q) < q - 12$;

(2) *if* q *is prime or a square and, additionally,* $\gcd(3, q - 1) = 1$, *then* $t_3(2, q) < q - 15$.

Proof (1). Let $\Pi_q = \mathrm{PG}(2, q)$ be a plane of order $q \geq 79$ over a field $\mathbf{F}_q$ of characteristic $p > 3$. On the one hand, if $q = p$ for some prime p, then Corollary 3.2 (1) shows that for every integer N within the Hasse-Weil bound, there is at least one elliptic curve Γ over $\mathbf{F}_q$ of order N. In particular, there is at least one curve E in Π_q of order $N_1 = q + 1 - 2\sqrt{q}$. Furthermore, since the plane Π_q has order $q \geq 79$, the Hirschfeld-Voloch theorem implies that the curve E is either complete or, if not, its completion $\mathcal{K}$ admits no more than three points $Q \in \Pi_q \backslash E$. Also, $q \geq 79$ implies that

$$2\sqrt{q} > 2\sqrt{64} = 16. \tag{3.13}$$

This, in turn, gives the following bound:

$$q + 1 - 2\sqrt{q} + 3 < q + 4 - 16 = q - 12.$$

Here, note that the complete $(k, 3)$-arc $\mathcal{K}$ is arbitrary. Accordingly, $\mathcal{K}$ is not necessarily minimal and it follows that

$$t_3(2, q) < q - 12.$$

If, on the other hand $q = p^h$ with h even, Theorem 3.1 (3) similarly reveals that there is a curve E over $\mathbf{F}_q$ of order $q + 1 - 2\sqrt{q}$. Proceeding as in the first instance, the bound $t_3(2, q) < q - 12$ is again obtained. Having accounted for both cases, this completes the proof of (1).

To prove (2), assume additionally that $\gcd(3, q - 1) = 1$ where q is either prime or square. Applying Theorem 3.21, the curve E has non-zero j-invariant since $|E(\mathbf{F}_q)| = q + 1 - 2\sqrt{q}$. Note also that existence of the curve E is again implied by Corollary 3.2 (1) or Theorem 3.1 (3), according as $q = p$ or $q = p^h$ with h even. Now, Theorem 3.21 shows that the curve E is itself a complete cubic arc. Thus, proceeding as in the proof of (1), the inequality presented in (3.13) yields the following upper bound:

$$t_3(2, q) < q - 15.$$

This completes the proof. ■

Analysis of Theorem 3.23 is pertinent. The theorem only provides upper estimates for the lower bound $t_3(2, q)$. Thus, within the context of improvements to computational algorithms through a reduction in the size of the relevant search space, its use is only indirect. More illuminating is an analysis of this bound for $t_3(2,q)$ in association with Theorem 2.22. Specializing the latter to cubic arcs, a $(k,3)$-arc $\mathcal{K}$ is incomplete if $k < \sqrt{6q+6}$. Thus, if the plane $\mathrm{PG}(2,q)$ has characteristic $p > 3$ and is of order $q \geq 79$, with q either prime or a square, Theorems 2.22 and 3.23 together establish the following range of values for $t_3(2,q)$:

$$\sqrt{6q+6} \ \leq t_3(2,q) \ < q - 12.$$

If, in addition, $\gcd(3, q-1) = 1$, the range of values is slightly improved to the following estimate:

$$\sqrt{6q+6} \ \leq t_3(2,q) \ < q - 15.$$

This chapter concludes with a comparison of Theorem 3.23 to a recent result in this direction. In [6], a collection of complete $(k,3)$-arcs has been established through the selection of an appropriate subset of the plane quartic curve $\mathcal{Q}$ with equation $Y = X^4$. These cubic arcs, in planes of suitable order, yield new theoretical bounds for $t_3(2,q)$. More specifically, it was shown that for $q = \sigma^h \geq 3600\sigma^6$, with $\sigma = p^e$ non-square and $p \equiv 2 \pmod 3$ an odd prime, the following bound holds in $\mathrm{PG}(2,q)$:

$$k \leq \frac{\tau(\sigma)}{\sigma} q + 6. \tag{3.14}$$

Here, $\tau(\sigma)$ is given by the following identity:

$$\tau(\sigma) = \begin{cases} (p+5)/4 & \text{if } \sigma = p \geq 29; \\ 2\sqrt{\sigma p} + p - 4 & \text{if } \sigma \geq p^3. \end{cases}$$

In [6], in contrast to the bound presented in Theorem 3.23, it is observed that (3.14) is asymptotically smaller than q, thereby improving upon the estimates of $t_3(2,q)$ presented in Theorem 3.23. Consequently, Theorem 3.23 is thought to be of greatest utility when considering finite planes and, in particular, planes of relatively small order.

Chapter 4

Concluding remarks and continuing research

4.1 Summary of results

The principal contribution of this thesis lies within its use and adaptation of combinatorial techniques to improve upon existing bounds for complete (k, n)-arcs in $\mathrm{PG}(2, q)$. The results presented in this thesis also improve upon existing knowledge of the wider incidence structures associated to (k, n)-arcs in $\mathrm{PG}(2, q)$, a contribution most readily exemplified by our additions to the theory of blocking sets and projective codes. Inspired by Barlotti in his analysis of complete $(k, 2)$-arcs, we have used the incidence equations for a subset of $\mathrm{PG}(2, q)$ with at most n points on a line to prove that a complete k-arc $\mathcal{K}$, of degree $n \geq 2$, has size $k \geq \sqrt{n(n-1)(q+1)}$. The new lower bound gives a necessary condition for the completeness of the general (k, n)-arc and is the only such bound in existence for an arc of arbitrary degree. In spite of its generality, however, the bound has been shown to compare favourably with the existing bounds of both Barlotti and Ball when specializing the discussion to $(k, 2)$-arcs. A crucial point emerging from the proof of Theorem 2.22, is its comparison of τ_n, the number of n-secants with which a complete (k, n)-arc $\mathcal{K}$ is incident, to the constant

$$\frac{k(k-1)}{n(n-1)}.$$

Here, the constant is dependent only on the size and degree of $\mathcal{K}$. An analogous comparison was shown to lie at the heart of Barlotti's proof that a k-arc $\mathcal{K}$ in $\mathrm{PG}(2, q)$ is incomplete if $k < \sqrt{2q + \frac{1}{4}} + \frac{3}{2}$. The comparison proved pivotal in our generalization of the Barlotti result and suggested an approach which was then adapted to the study of complete $(k, 3)$-arcs in $\mathrm{PG}(2, q)$. Extending the work of Bruen and Fisher on k-arc derived blocking sets to $(k, 3)$-arc derived blocking sets, new bounds restricting the size of complete cubic arcs in $\mathrm{PG}(2, q)$ were established. This necessitated a widening of Ball's work on the relationship between k-arcs and blocking sets in $\mathrm{PG}(2, q)$ to the far more complicated incidence structure of the $(k, 3)$-arc, the secant distribution of the general $(k, 3)$-arc $\mathcal{K}$ being impervious to basic counting arguments. In Chapter 2, this work culminated in a classification of cubic arcs in terms of their trisecants. It was shown that for $\mathcal{K}$, a complete $(k, 3)$-arc in a plane of order $q \geq 17$, if $k \neq q + 2$ then $k < \tau_3$ where τ_3 is the total number of trisecants to $\mathcal{K}$.

In Chapter 3, cubic arcs were further explored through their close association with elliptic curves, initially by restricting attention to curves and arcs of largest size. Exploiting their connection with elliptic curves in the plane, a new upper bound for the complete $(k, 3)$-arc $\mathcal{K}$ of largest size, subject only to a restriction upon its trisecants, was established. When used in conjunction with the newly established results on blocking sets in Chapter 2, the known bounds for elliptic curves gave, in Theorem 3.10, a notable improvement to the Barlotti-Thas upper bound for $(k, 3)$-arcs satisfying a prescribed incidence condition. From the perspective of historical progression on bounds for $(k, 3)$-arcs, it was noted that Theorem 3.10 represents the only significant improvement to the Barlotti-Thas upper bound since its proof for arbitrary $q \geq 4$ in 1975. By imposing numerical restraints on their trisecants, a new technique for the analysis of the complete cubic arc $\mathcal{K}$ of largest size was then introduced. Here, a numerical assumption upon the relative numbers of i-secants to a complete $(k, 3)$-arc $\mathcal{K}$ resulted in a sufficient condition guaranteeing a positive resolution to the Hirschfeld conjecture. This analysis of $(k, 3)$-arcs from the perspective of their i-secants, with $0 \leq i \leq 3$, was developed in response to an empirical analysis of Table 3.3, which lists the known secant distributions for $(k, 3)$-arcs in $\mathrm{PG}(2, q)$.

Then, as the sole method of constructing general $(k, 3)$-arcs in $\mathrm{PG}(2, q)$, the completeness of elliptic curves as plane cubic arcs was a question addressed in this thesis. This was done within the context of the Hirschfeld-Voloch Theorem, see Theorem 3.16, as well as Theorem 3.18 by Alderson and Bruen. Using aspects of the algebra of finite fields as well as the properties of polynomials defining elliptic curves, a new and more readily applied interpretation of the Hirschfeld-Voloch Theorem was given in Theorem 3.21. Here, a condition for the completeness of a curve $\mathcal{C}$ was provided, in planes of suitable order, using only the size of that curve and the order of the plane $\mathrm{PG}(2, q)$. This, in contrast to existing computational methods of classification of $(k, 3)$-arcs, culminated in a theoretical result establishing new bounds for $t_3(2, q)$, the size of the smallest complete cubic arc. Finally, the newly established bounds were compared to the best known bounds for cubic arcs of minimal size provided by a recent result of Bartoli *et al.* (2015).

4.2 Future research

The loosening of incidence conditions in the theorems and combinatorial techniques presented in this thesis is the principal focus of our current research. In particular, a generalization of Theorem 3.10 to a cubic arc $\mathcal{K}$ with only some of its trisecants incident with points $Q \in \Pi_q \backslash \mathcal{K}$ of index one is a natural first object of inquiry. Extending Theorem 3.10 in this manner would improve consensus that the Barlotti-Thas upper bound for complete cubic arcs is not attained in $\mathrm{PG}(2, q)$ if $q > 7$. Towards this end, the properties of a *strong representative system* are being studied for their potential to aid us in the improvement of bounds for complete $(k, 3)$-arcs. A strong representative system is a set of flags in $\mathrm{PG}(2, q)$ of the form $\mathcal{S} = \{(P_1, \ell_i), \ldots, (P_n, \ell_n)\}$, where a point P_i is incident with the line ℓ_j if an only if $i = j$. The system $\mathcal{S}$ is *maximal* if it is not a proper subset of another strong representative system $\mathcal{S}'$. Owing to the existence of bounds governing their size, the properties of a strong representative system may prove useful. Indeed, in [28], it was shown that $|\mathcal{S}| \leq q\sqrt{q} + 1$ for a strong representative system $\mathcal{S}$ in $\mathrm{PG}(2, q)$. Also, in [12], it was shown that there is no maximal strong representative system $\mathcal{S}$, in $\mathrm{PG}(2, q)$, if $q + 1 < |\mathcal{S}| < q + \frac{1}{2}\sqrt{q}$. The development of bounds for $(k, 3)$-arcs in $\mathrm{PG}(2, q)$, might therefore be aided by a partition of the points of the plane into representative systems $\mathcal{S}$, each of size $s \leq q\sqrt{q} + 1$, upon which combinatorial arguments are more readily formulated. In general, owing to the simplicity in the incidence of the points and lines of a strong representative system $\mathcal{S}$, each point belonging to a unique flag of $\mathcal{S}$, combinatorial problems in $\mathrm{PG}(2, q)$ should reveal themselves to be more tractable when considered from this perspective.

Additionally, efforts to extend Theorem 3.14 are presently being considered through an application of the following result by Stinson.

Theorem 4.1 (Stinson, [40])**.** *The number of lines disjoint from a subset Y of size s in a projective plane Π_q of order q is at most*

$$\frac{q^3 + q^2 + q - qs}{q + s}.$$

This result is presently being adapted to the problem of complete (k, n)-arcs in $\mathrm{PG}(2, q)$ with great attention given to complete $(k, 3)$-arcs in particular. Such an adaptation, to an analogous statement about the number of i-secants to a $(k, 3)$-arc $\mathcal{K}$, might prove useful as a means to remove any need to assume that $\tau_2 + \tau_3 \geq \max(\tau_0, \tau_1)$ in Theorem 3.14. Indeed, for an arbitrary $(k, 3)$-arc $\mathcal{K}$ in $\mathrm{PG}(2, q)$, Stinson's result suggests that the following bound holds for τ_0, the number of external lines to $\mathcal{K}$:

$$\tau_0 \leq \frac{q^3 + q^2 + q - qk}{q + k}.$$

Also, the incorporation of additional Diophantine equations into the proof of Theorem 2.22 is presently being considered as a means to improve estimates of $t_n(2, q)$, the size of the smallest complete (k, n)-arc in $\mathrm{PG}(2, q)$. Here, the restriction of combinatorial arguments to k-arcs of fixed degree $n \geq 2$ in a plane Π_q of specific order q will aid in the establishing of finer counting arguments. Perhaps of greatest interest, however, is an extension of Theorem 2.22 to complete $(k; r, s; n, q)$-sets in spatial geometries. A $(k; r, s; n, q)$-set $\mathcal{K}$ is a set of k points in the spatial geometry $\mathrm{PG}(n, q)$, not contained in any proper subspace of $\mathrm{PG}(n, q)$, with at most r points of $\mathcal{K}$ incident with any subspace of dimension s in $\mathrm{PG}(n, q)$; see [26]. Here, still fewer theoretical bounds are known with much of the existing work in this direction restricted to $(k; 2, 1; n, q)$-sets, that is, sets of size k in $\Pi_q = \mathrm{PG}(n, q)$ no three of which are incident with a line of Π_q. Finally, in accordance with much of the research in finite geometry, incorporation of the combinatorial methods and results developed in this thesis to produce and improve computational methods for the classification of (k, n)-arcs is of great interest. Here, methods for parallel task scheduling using knowledge of elliptic curves is presently being explored.

Bibliography

[1] T. L. Alderson and A. A. Bruen, Codes from cubic curves and their extensions, Electron. J. Combin. **15** (2008), $\#42$.

[2] S. Ball, On sets of points in finite planes, DPhil. thesis, University of Sussex, (1994).

[3] A. Barlotti, Some topics in finite geometrical structures, Institute of Statistics Mimeo Ser. No. **439** (1965), University of North Carolina.

[4] A. Barlotti, Sui (k, n)-archi di un piano lineare finito, Boll. Un. Mat. Ital. **11** (1956), 553–556.

[5] M. Barnabei, D. Searby, C. Zucchini, On small (k, q)-arcs in planes of order q^2, J. Combin. Theory Ser. A **24** (1978), 241–246.

[6] D. Bartoli, M. Giulietti, G. Zini, Complete $(k, 3)$-arcs from quartic curves, Des. Codes Cryptogr. (2015), to appear.

[7] D. Bartoli, S. Marcugini and F. Pambianco, The non-existence of some NMDS codes and the extremal sizes of complete $(n, 3)$-arcs in $\mathrm{PG}(2, 16)$, Des. Codes Cryptogr. **72** (2014), 129–134.

[8] S. Barwick and G. Ebert, Unitals in projective planes, Springer Monographs in Mathematics, Springer-Verlag New York, (2008).

[9] L. M. Batten, Combinatorics of finite geometries, second ed., Cambridge University Press, (1997).

[10] M. K. Bennett, Affine and projective geometry, John Wiley & Sons, (1995).

[11] A. Beutelspacher and U. Rosenbaum, Projective geometry: from foundations to applications, Cambridge University Press, (1998).

[12] A. Blokhuis and K. Metsch, Large minimal blocking sets, strong representative systems, and partial unitals, Cambridge University Press, London Math. Soc. Lecture Note Series **191** (1993), 37–52.

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

[14] A. A. Bruen, Baer subplanes and blocking sets, Bull. Amer. Math. Soc. **76** (1970), 342–344.

[15] A. A. Bruen and J. C. Fisher, Blocking sets and complete k-arcs, Pacific J. Math., **53** (1974), 73–84.

[16] A. A. Bruen, J. W. P. Hirschfeld and D. L. Wehlau, Cubic curves, finite geometry and cryptography, Acta Appl. Math. **115** (2011), 265–278.

[17] A. A. Bruen and J. A. Thas, Blocking sets, Geom. Dedicata **6** (1977), 193–203.

[18] K. Coolsaet and H. Sticker, The complete $(k, 3)$-arcs of $\mathrm{PG}(2, q),\ q \leq 13$, J. Combin. Designs **20** (2012), 89–111.

[19] A. Cossu, Su alcune proprietà dei (k, n)-archi di un piano proiettivo sopra un corpo finito, Rend. Mat. e Appl. **20** (1961), 271–277.

[20] M. Giulietti, On the extendibility of near–MDS elliptic codes, Appl. Algebra Engrg. Comm. Comput. **15** (2004), 1–11.

[21] R. Hill, Optimal linear codes, cryptography and coding II, Oxford University Press, Oxford, (1992), pp. 75–104.

[22] J. W. P. Hirschfeld, Projective geometries over finite fields, second ed., Oxford University Press, Oxford, (1998), xiv+555 pp.

[23] J. W. P. Hirschfeld, Curves of genus 3, Rendiconti di Matematica, Serie VII **30** (2010), 77–88.

[24] J. W. P. Hirschfeld and E. V. D. Pichanick, Bounds for arcs of arbitrary degree in finite Desarguesian planes, J. Combin. Designs (2015), to appear.

[25] J.W.P. Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces, J. Statist. Planning Infer. **72** (1998), 355–380.

[26] J. W. P. Hirschfeld and J. A. Thas, Open problems in finite projective spaces, Finite Fields Appl. **32** (2015), 44–81.

[27] J. W. P. Hirschfeld and J. F. Voloch, The characterization of elliptic curves over finite fields, J. Austral. Math. Soc. Ser. A **45** (1988), 275–286.

[28] T. Illés, T. Szőnyi, and F. Wettl, Blocking sets and maximal strong representative systems in finite projective planes, Mitt. Math. Sem. Giessen **201** (1991), 97–107.

[29] C. W. H. Lam, The search for a finite projective plane of order ten, Amer. Math. Monthly **98** (1991), 305–318.

[30] S. Marcugini, A. Milani, F. Pambianco, Maximal $(n, 3)$-arcs in $\mathrm{PG}(2, 11)$, Discrete Math. **208/209** (1999), 421–426.

[31] S. Marcugini, A. Milani, F. Pambianco, Maximal $(n, 3)$-arcs in $\mathrm{PG}(2, 13)$, Discrete Math. **294** (2005), 139–145.

[32] B. D. McKay, Isomorph-free exhaustive generation, J. Algorithms, **26** (1998), 306–324.

[33] G. E. Moorhouse, Incidence geometry, Math. **5700** (2007), University of Wyoming.

[34] S. L. Ng, On covers of point sets in finite geometries, PhD. thesis, University of London, (1998).

[35] O. Polverino, Small minimal blocking sets and complete k-arcs, Discrete Math., **208/209** (1999), 469–476.

[36] S. Schmitt and H. G. Zimmer, Elliptic curves: a computational approach, Walter de Gruyter, (2003).

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

[38] R. C. Singleton, Maximum distance q-nary codes, IEEE Trans. Inform. Theory **10** (1964), 116–118.

[39] J. Stillwell, Mathematics and its history, third ed., Springer-Verlag New York, (2010).

[40] D. R. Stinson, Nonincident points and blocks in designs, Discrete Math. **313** (2013), 447–452.

[41] M. Tallini Scafati, Sui (k, n)-archi di un piano grafico finito, Atti Accad. Naz. Linceri Rend., **40** (1966), 373–378.

[42] J. Thas, Some results concerning $((q + 1)(n - 1), n)$-arcs, J. Combin. Theory Ser. A **19** (1975), 228–232.

[43] L. C. Washington, Elliptic curves, number theory and cryptography second ed., Chapman & Hall, (2008).

[44] W. C. Waterhouse, Abelian varieties over finite fields, Ann. Sci. Ecole Norm. Sup. **2** (1969), 521–560.