On Covers of Point Sets in Finite Geometries

Siaw Lynn Ng

Thesis submitted to
The University of London
for the degree of
Doctor of Philosophy
1998.

Royal Holloway and Bedford New College,
University of London.

Abstract

This thesis discusses two substructures in finite geometry.

Firstly we investigate k-arcs in projective planes covering a line. In a finite projective plane, a k-arc $\mathcal{K}$ covers a line l_∞ disjoint from it if every point on l_∞ lies on a secant to $\mathcal{K}$. This concept arises from the problem of trying to ascertain the size of the smallest set of elements for which no linear (n, q, t)-perfect hash family exists. In particular, in $PG(2, q)$, the Desarguesian plane of order q, no linear (q^2, q, k)-perfect hash family exists if there is a k-arc covering a line. We are interested in finding k-arcs covering a given line l_∞ such that k is small with respect to q. We obtain a lower bound on the size of such k-arcs and prove that there are only 4 cases where this bound is met. These cases are characterised by the property that every point on l_∞ is covered by exactly one secant to the k-arc. We then consider the generalisation to n-regular k-arcs, where every point on l_∞ is covered by exactly n secants. We show that n is at most $\frac{k}{2}$ and characterise $\frac{k}{2}$-regular k-arcs as hyperovals in planes of even order. In planes of odd order, however, there are no $\frac{k}{2}$-regular k-arcs, but we show that $(\frac{k}{2}-1, \frac{k}{2})$-regular k-arcs, where half the points on l_∞ lie on $\frac{k}{2}-1$ secants and the other half on $\frac{k}{2}$ secants, are precisely the ovals in the plane. In addition, we present examples and constructions of families of small k-arcs covering a line in $PG(2, q)$.

We consider also the generalisation of k-arcs covering a line to (k, n)-arcs covering an arbitrary set of points in the plane and obtain lower bounds on k. Furthermore, we show that the concept of k-arcs covering a line can be extended to that of sets of points covering a hyperplane in higher dimensional projective spaces and show that, in fact, a k-arc covering a line in $PG(2, q)$ also covers a hyperplane in $PG(n, q)$ for all $n > 2$.

Secondly we investigate the properties of a certain type of family of planes in $PG(5, q)$ introduced by Yoshiara. This is a family of $q+3$ planes $\mathcal{E} = \{\pi_o, \ldots, \pi_{q+2}\}$ such that

(1) the set $\mathcal{O}_i = \{\pi_i \cap \pi_j \mid j \in \{0, \ldots, q+2\} \setminus \{i\}\}$ is a hyperoval in π_i for all $i = 0, \ldots, q+2$;

(2) any 3 planes in $\mathcal{E}$ span $PG(5, q)$.

This structure may be used to construct a family of Extended Generalised Quadrangles of order $(q+1, q-1)$. We are interested principally in the combinatorial and geometric properties of $\mathcal{E}$. We show that the dual of $\mathcal{E}$ also satisfies conditions (1) and (2), and that this leads to new examples. We also present a coordinatisation of $\mathcal{E}$ and prove a necessary and sufficient condition for a set of o-polynomials to determine $\mathcal{E}$.

Acknowledgements

I would like to thank my supervisor Professor Fred Piper and my advisor Professor Peter Wild for supervising my work and providing guidance and inspiration.

I am grateful to the staff and students of the maths department at Royal Holloway for making the past three years very enjoyable.

Thanks also to my family and my friends for their support. Special thanks are due to Dr Jon Chambers for his support and understanding.

Finally I would like to acknowledge the financial support of the Sarawak Tunku Abdul Rahman Scholarship Foundation.

Contents

List of Figures

Chapter 1

Introduction

The first four sections of this chapter gives some of the necessary background to this thesis. For a comprehensive treatment of projective geometry we refer the reader to the books by Hirschfeld [15] and Hughes and Piper [17], and more details on sharply focused sets can be found in Chapter 5 of Jackson's thesis [18]. The last section describes the motivation for this research and gives an outline of the thesis.

1.1 Projective and affine planes

A **projective plane** is a set of points and lines with an incidence relation between points and lines such that

1. Any two distinct points are incident with a unique line.
2. Any two distinct lines are incident with a unique point.
3. There are four points such that no three are collinear.

If $\mathcal{P}$ is a projective plane, let $\mathcal{P}'$ be a set of points and lines with an incidence relation such that the points and lines of $\mathcal{P}'$ are respectively the lines and points of $\mathcal{P}$, and two elements in $\mathcal{P}'$ are incident if and only if they are incident in $\mathcal{P}$. Then $\mathcal{P}'$ is also a projective plane and is called the **dual** of $\mathcal{P}$.

In a finite projective plane of order q, there are q^2+q+1 points and q^2+q+1 lines. Every line is incident with $q+1$ points and every point is incident with $q+1$ lines. We write Π_q for a projective plane of order q.

For every prime power q there is a projective plane $PG(2,q)$ defined over the Galois Field of order q, $GF(q)$. The points are given homogeneous coordinates

$$\{(x_0,x_1,x_2) \mid x_i \text{ not all zero, } x_i \in GF(q)\}$$

such that (x_0,x_1,x_2) and $\rho(x_0,x_1,x_2)$, $\rho \in GF(q)\setminus\{0\}$, represent the same point. From now on we write $GF(q)^*$ for $GF(q)\setminus\{0\}$. A line of $PG(2,q)$ is a set of points (x_0,x_1,x_2) satisfying a homogeneous linear equation

$$ax_0+bx_1+cx_2=0, \quad a,b,c \in GF(q) \text{ not all zero.}$$

We sometimes represent a line by the homogeneous coordinates $[a,b,c]$.

A ***k*-arc** in Π_q is a set of k points such that no three are collinear. It is well known that $k \leq q+1$ if q is odd and $k \leq q+2$ if q is even. A $(q+1)$-arc is called an **oval** and a $(q+2)$-arc is called a **hyperoval**. A k-arc $\mathcal{K}$ is **complete** if every point in the plane lies on a secant to $\mathcal{K}$. A **(k,n)-arc** is a set of k points such that every line in the plane meets it in at most n points and some line meets it in n points. A k-arc is therefore a $(k,2)$-arc. We say a line is a ***t*-secant** of $\mathcal{K}$ if it meets $\mathcal{K}$ in t points. A 1-secant is also called a tangent or a unisecant.

A **subplane** Π_o of a projective plane Π is a subset of elements of Π which forms a projective plane with the incidence relation inherited from Π. If Π_q is a projective plane of order q and Π_o is a proper subplane of Π_q of order q_o, then either $q=q_o^2$ or $q \geq q_o^2+q_o$. If $q=q_o^2$ then we call Π_o a **Baer subplane**. The lines of Π_q meets a Baer subplane Π_o in either 1 or q_o+1 points and are called tangents or secants respectively. We refer to a secant to a subplane Π_o as a line of Π_o or a **Baer subline** if Π_o is a Baer subplane.

An **affine plane** $\mathcal{A}$ is a set of points and lines with an incidence relation between points and lines such that

1. Any two distinct points are incident with a unique line.
2. Given any line l and any point P not on l there is a unique line m such that P is incident with m, and l and m have no point in common.

3. There are three non-collinear points.

Two lines l and m are **parallel** if $l = m$ or l and m do not intersect. Parallelism is an equivalence relationship and every point is on exactly one line from each parallel class.

An affine plane of order q, $\mathcal{A}_q$, has q^2 points and q^2+q lines. Every point is incident with $q+1$ lines and every line is incident with q points. An affine plane of order q, $\mathcal{A}_q$, can be constructed from a projective plane Π_q by removing a fixed line, say l_∞, and the points of Π_q on l_∞. We write $\mathcal{A}_q = \Pi_q^{l_\infty}$, and if $\Pi_q = PG(2,q)$, $\mathcal{A}_q$ is denoted $AG(2,q)$. For any affine plane $\mathcal{A}$, there is, up to isomorphism, a unique projective plane Π, such that $\mathcal{A} = \Pi^{l_\infty}$ for some line l_∞ of Π. We call l_∞ the line at infinity or the ideal line, the points of $\mathcal{A}$ affine points and the lines of $\mathcal{A}$ affine lines. The set of lines of Π through each point on l_∞ corresponds to a parallel class of $\mathcal{A}$. There are $q+1$ parallel classes in $\mathcal{A}_q$ and q lines in each class.

A **collineation** of a projective plane Π is a bijection from points to points and from lines to lines which preserve collinearity. A collineation of order 2 is an **involution**. If a collineation σ fixes a line l pointwise and a point V linewise then σ is a **(V,l)-perspectivity**. We call V the **centre** and l the **axis** of the perspectivity. A plane Π is **(V,l)-transitive** if for all points A, B of Π collinear with V, there is a (V,l)-perspectivity mapping A to B. If Π is (X,l_∞)-transitive for all points X on l_∞, then l_∞ is a **translation line** of Π. We say that Π a **translation plane with respect to l_∞** and we call $\mathcal{A} = \Pi^{l_\infty}$ a **translation plane**.

1.2 Sharply focused sets

Let $\mathcal{K}$ be a k-arc, $k > 2$, and let l be a line external to $\mathcal{K}$. The **intersection set** or **focus** of $\mathcal{K}$ on l is defined to be

$$\mathrm{Int}(\mathcal{K}, l) = \{AB \cap l \mid A, B \in \mathcal{K}, A \neq B\}.$$

By considering the secants through a fixed point on $\mathcal{K}$, we see that

$$|\mathrm{Int}(\mathcal{K}, l)| \geq k - 1.$$

If $|\mathrm{Int}(\mathcal{K}, l)| = k$ then $\mathcal{K}$ is said to be **sharply focused** on l. For instance, any 3-arc is sharply focused on any line missing it.

Wettl [21] showed that in $PG(2,q)$, if $\mathcal{K}$ is sharply focused on l then $\mathcal{K}$ is contained in a conic. Jackson [18] showed that given a conic $\mathcal{C}$ and a line l, for any $s|n$, $n = |\mathcal{C} \setminus l|$, there is a partition of the conic $\mathcal{C}$ into sharply focused sets of size s, and these are the only sharply focused sets in $PG(2,q)$.

The results of Jackson in [18] depend on conics and the groups acting on them, so before giving a summary of the results we give a brief description of conics in $PG(2,q)$.

In $PG(2,q)$, an **irreducible conic** $\mathcal{C}$ is a set of points (x,y,z) satisfying an irreducible homogenous quadratic equation over $GF(q)$:

$$Ax^2 + By^2 + Cz^2 + Fyz + Gxz + Hxy = 0.$$

From now on we shall use the term conic to mean an irreducible conic. A conic is a $(q+1)$-arc. A well-known result of Segre says that in $PG(2,q)$, q odd, every oval is a conic. If q is odd, a point of $PG(2,q)$ not on $\mathcal{C}$ is **external** or **internal** to $\mathcal{C}$ according to whether it lies on 2 or 0 tangent to $\mathcal{C}$. If q is even, the tangents to $\mathcal{C}$ are concurrent in a point N, called the **nucleus** and the set $\mathcal{C} \cup \{N\}$ forms a (regular) hyperoval.

The projective group $PGL(3,q)$ acts transitively on conics of $PG(2,q)$. The orthogonal group $PGO(3,q)$ is a subgroup of $PGL(3,q)$ fixing a conic $\mathcal{C}$ and acts 3-transitively on the points of $\mathcal{C}$. If q is odd, $PGO(3,q)$ acts transitively on the set of external points and the set of internal points of $\mathcal{C}$, and hence on the set of external lines and the set of secants of $\mathcal{C}$. If q is even, $PGO(3,q)$ fixes the nucleus N and is transitive on all points not on $\mathcal{C} \cup \{N\}$. Every point P not on $\mathcal{C}$, P not the nucleus of $\mathcal{C}$ if q is even, is the centre of a unique involution $[P]$ in $PGO(3,q)$. If A, B are two points of $\mathcal{C}$, then $[P]$ interchanges A and B if and only if P, A, B are collinear. If l_∞ is any line and $P \in l_\infty \setminus \mathcal{C}$, then $[P]$ fixes l_∞, so $[P] \in PGO(3,q)_{l_\infty}$. We call such involutions in $PGO(3,q)_{l_\infty}$ **proper involutions**. If l_∞ is a line secant or external to $\mathcal{C}$, then the group $PGO(3,q)_{l_\infty}$ fixing $\mathcal{C}$ and l_∞ is isomorphic to the dihedral group of order $2n$, $\mathcal{D}_{2n}$, where $n = q+1$ if l_∞ is external and $n = q-1$ if

l_∞ is a secant. We may write

$$PGO(3,q)_{l_\infty} = \langle \alpha,\ \gamma \mid \alpha^2 = \gamma^n = 1,\ \alpha\gamma\alpha = \gamma^{-1} \rangle,$$

where α, $\alpha\gamma$, ..., $\alpha\gamma^{n-1}$ are the proper involutions $[P]$, $P \in l_\infty \setminus \mathcal{C}$, and γ acts regularly on $\mathcal{C} \setminus l_\infty$.

An operation $\oplus$ can be defined on the points of $\mathcal{C}$ as follows:

Fix a point $P \in \mathcal{C}$, and for points Q, $R \in \mathcal{C}$,

$$Q \oplus R = ((QR \cap l_\infty)P \cap \mathcal{C}) \setminus \{P\},$$

where QR is the line joining the points Q and R, and QQ represents the tangent to $\mathcal{C}$ at Q. We let $QQ \cap \mathcal{C} = \{Q, Q\}$. It was shown in [18] that $(\mathcal{C}, \oplus)$ is a cyclic group of order $n = |\mathcal{C} \setminus l_\infty|$. The points on $\mathcal{C}$ and the points on l_∞ can be identified with the integers modulo n, $\boldsymbol{Z}_n$, in the following manner: the point P is labelled $(\!(0)\!)$ and the point P^{γ^i} labelled $(\!(i)\!)$. A point X on $l_\infty \setminus \mathcal{C}$ is labelled $\langle\!\langle i \rangle\!\rangle$ if X, $(\!(0)\!)$, $(\!(i)\!)$ are collinear. Then the point $\langle\!\langle k \rangle\!\rangle$ lies on the secant $(\!(i)\!)(\!(j)\!)$ if and only if $i + j \equiv k \bmod n$.

The following results and sketches of proofs are summarised from [18, Chapter 5].

Result 1.2.1 Let l_∞ be a line secant or external to $\mathcal{C}$. Let $H = PGO(3,q)_{l_\infty} = \langle \alpha,\ \gamma \mid \alpha^2 = \gamma^n = 1,\ \alpha\gamma\alpha = \gamma^{-1} \rangle$, where $n = |l_\infty \setminus \mathcal{C}|$. For any $s \mid n$, $s \geq 3$, let $\mathcal{K}(s) = \{K_1, \ldots, K_{\frac{n}{s}}\}$ be the orbits of $N = \langle \gamma^{\frac{n}{s}} \rangle$ on $\mathcal{C}$, each of size s. Then $K \in \mathcal{K}(s)$ is a sharply focused set.

Sketch of proof: Let A be a point of K and let $[P]$ be the (unique) proper involution fixing A. Let $J = \langle [P], N \rangle$. Then $J \cong \mathcal{D}_{2s}$, the dihedral group of order $2s$. It is shown that $J = H_K$, the subgroup of H fixing K:

Since N is a normal subgroup of H, the orbits of N form a system of blocks for H, so both $[P]$ and N fix K, hence J fixes K and so $J \leq H_K$. By the orbit-stabiliser theorem,

$$|H_A| = \frac{|H|}{|A^H|} = \frac{2n}{n} = 2.$$

Since $(H_K)_A \leq H_A$ and $(H_K)_A$ contains $[P]$ and the identity collineation, we must have $|(H_K)_A| = 2$. Since $N \leq H_K$, we have $|A^{H_K}| = s$. By the orbit-stabiliser

theorem again,

$$|H_K| = |(H_K)_A| \cdot |A^{H_K}| = 2 \cdot s = 2s = |J|.$$

Hence $J = H_K$.

Next it is shown that the set $I = \{P \mid [P] \text{ is a proper involution in } H_K\}$ is the focus of K on l_∞. Now, $|I| = s$. If s is odd, then the s proper involutions each fixes a point of K, so there are $(s-1)/2$ secants through each P. This accounts for all the secants of K meeting l_∞. If s is even, $[P]$ fixes two points or none at all in K. There are $s/2$ involutions $[P]$ fixing two points of K and there are $(s-2)/2$ secants through each P. The remaining $s/2$ proper involutions fix no points in K and so there are $s/2$ secants through each centre. This accounts for all the secants. Hence $I = \text{Int}(K, l_\infty)$ and so K is sharply focused on l_∞. □

Such sharply focused sets are called **subgroup induced**. Identifying the points of $\mathcal{C}$ with $\boldsymbol{Z}_n$, the sharply focused sets are precisely the cosets of the subgroups of $\boldsymbol{Z}_n$.

Result 1.2.2 Let K_i, $K_j \in \mathcal{K}(s)$ and

$$\text{Int}(K_i, K_j, l_\infty) = \{AB \cap l_\infty \mid A \in K_i, B \in K_j\}.$$

Then,

(a) For K_i, $K_j \in \mathcal{K}(s)$, $K_i \neq K_j$, $|\text{Int}(K_i, K_j, l_\infty)| = s$.

(b) For $K \in \mathcal{K}(s)$, $\text{Int}(K, l_\infty) \cap \text{Int}(K, K_i, l_\infty) = \emptyset$ for all $K_i \in \mathcal{K}(s) \setminus \{K\}$.

(c) For any $K \in \mathcal{K}(s)$, $\text{Int}(K, K_i, l_\infty) \cap \text{Int}(K, K_j, l_\infty) = \emptyset$ for all $K_i \neq K_j$, K_i, $K_j \in \mathcal{K}(s) \setminus \{K\}$.

(d) If $\text{Int}(l_\infty)$ is the set of distinct sets $\text{Int}(K, l_\infty)$, $\text{Int}(K, K_i, l_\infty)$, K, $K_i \in \mathcal{K}(s)$, then $\text{Int}(l_\infty)$ partitions $l_\infty \setminus \mathcal{C}$.

Sketch of proof:

(a) If $P \in \text{Int}(K_i, K_j, l_\infty)$, then $[P]$ interchanges K_i, K_j, so that through P there are $|K_i| = s$ secants. Since there are only s^2 secants joining points in K_i and K_j, $|\text{Int}(K_i, K_j, l_\infty)| = s$.

(b) Suppose $A \in \mathrm{Int}(K, l_\infty) \cap \mathrm{Int}(K, K_i, l_\infty)$, then $[A]$ fixes K, since K is sharply focused. But $A \in \mathrm{Int}(K, K_i, l_\infty)$ implies that $[A]$ maps K to K_i. This is a contradiction, so $\mathrm{Int}(K, l_\infty) \cap \mathrm{Int}(K, K_i, l_\infty) = \emptyset$.

(c) Suppose $A \in \mathrm{Int}(K, K_i, l_\infty) \cap \mathrm{Int}(K, K_j, l_\infty)$. Then $[A]$ maps K to K_i and also maps K to K_j. This is a contradiction, so $\mathrm{Int}(K, K_i, l_\infty) \cap \mathrm{Int}(K, K_j, l_\infty) = \emptyset$.

(d) By (a), $|\mathrm{Int}(K, l_\infty)| = |\mathrm{Int}(K, K_i, l_\infty)| = s$. By (b) and (c),

$$\begin{aligned} |\mathrm{Int}(l_\infty)| &= s + (|\mathcal{K}(s)| - 1)s \\ &= n, \end{aligned}$$

and the result follows. □

The next result describes the types of points on $\mathrm{Int}(K, l_\infty)$ with respect to $\mathcal{C}$ in $PG(2, q)$, q odd:

Result 1.2.3 Let $K \in \mathcal{K}(s)$ and let $h = n/s$, $s \geq 3$. Let $H = PGO(3, q)_{l_\infty}$.

(a) If s is odd or if both s and h are even, then $\mathrm{Int}(K, l_\infty)$ contains only external points and there is a unique $K' \in \mathcal{K}(s) \setminus \{K\}$ such that $H_{K'} = H_K$ and $\mathrm{Int}(K, l_\infty) = \mathrm{Int}(K', l_\infty)$.

(b) If s is even and h is odd, then half of the points in $\mathrm{Int}(K, l_\infty)$ are external points and the other half are internal, and K is the only element of $\mathcal{K}(s)$ fixed by H_K.

1.3 Derivation

Let Π be a projective plane of order q^2 and let $\mathcal{A} = \Pi^{l_\infty}$. Let $\mathcal{D}$ be a set of $q+1$ points on l_∞ such that for every pair A, B of points of $\mathcal{A}$ for which the line AB intersects l_∞ in a point of $\mathcal{D}$, there is a Baer subplane of Π containing A, B and $\mathcal{D}$. We call $\mathcal{D}$ a **derivation set** and any Baer subplane containing $\mathcal{D}$ is said to belong to $\mathcal{D}$.

We define a new structure $\mathcal{D}(\mathcal{A})$ as follows:

1. The points of $\mathcal{D}(\mathcal{A})$ are the points of $\mathcal{A}$.

2. The lines of $\mathcal{D}(\mathcal{A})$ are of two types: the Baer subplanes belonging to $\mathcal{D}$ and the lines of $\mathcal{A}$ which intersect l_∞ in $l_\infty \backslash \mathcal{D}$.

3. The incidence in $\mathcal{D}(\mathcal{A})$ is the natural one.

It can be shown that $\mathcal{D}(\mathcal{A})$ is an affine plane of order q^2, which can be completed to a projective plane Π' by adding the line l'_∞ so that $\mathcal{D}(\mathcal{A}) = \Pi'^{l'_\infty}$. The points of $l_\infty \backslash \mathcal{D}$ correspond to $q^2 - q$ points of l'_∞. The remaining $q+1$ points of l'_∞ is denoted by $\mathcal{D}'$.

If $\mathcal{A}$ is a translation plane, then so is $\mathcal{D}(\mathcal{A})$. If $\Pi = PG(2, q^2)$, then any Baer subline of l_∞ is a derivation set and Π' is the Hall plane of order q^2.

1.4 Projective and affine spaces

Let V be a vector space of $n+1$ dimension over $GF(q)$. The ***n*-dimensional projective space of order *q***, $PG(n, q)$, is defined as follows: a t-dimensional projective subspace is a $(t+1)$-dimensional vector subspace of V, $0 \leq t \leq n$. The incidence relation in $PG(n, q)$ is that of subspace containment. Projective subspaces of $PG(n, q)$ of dimension 0,1,2 and $n-1$ are called points, lines, planes and hyperplanes respectively. We usually abbreviate the term "t-dimensional subspace" to "t-space". The empty projective subspace has dimension -1.

For any space $\mathcal{S}$ there is a **dual** space $\mathcal{S}'$ whose points and hyperplanes are respectively the hyperplanes and points of $\mathcal{S}$. If $\mathcal{S}$ is $PG(n, q)$, then $\mathcal{S}'$ is also an n-dimensional projective space over $GF(q)$. A theorem in $\mathcal{S}$ stated in terms of points and hyperplanes gives a dual theorem in $\mathcal{S}'$ by substituting points for hyperplanes and hyperplanes for points. Hence the dual of an r-space in $\mathcal{S}$ is an $(n-r-1)$-space.

The points of $PG(n, q)$ are given homogeneous coordinates

$$\{(x_0, x_1, \ldots, x_n) \mid x_i \text{ not all zero}, x_i \in GF(q)\}$$

such that $(x_0, x_1, \ldots, x_n)$ and $\rho(x_0, x_1, \ldots, x_n)$, $\rho \in GF(q) \setminus \{0\}$, represent the same point. A hyperplane of $PG(n, q)$ is a set of points $(x_0, x_1, \ldots, x_n)$ satisfying

a homogeneous linear equation

$$a_0x_0 + a_1x_1 + \cdots + a_nx_n = 0,\ a_i \in GF(q) \text{ not all zero,}$$

and is represented by the homogeneous coordinates $[a_0, a_1, \ldots, a_n]$.

A **collineation** of $PG(n,q)$ is a bijection that preserves incidence. A **projectivity** $\mathcal{T}$ of $PG(n,q)$ is a collineation given by a non-singular matrix T such that a point $X = (x_0, x_1, \ldots, x_n)$ is mapped to the point $X^{\mathcal{T}} = Y = (y_0, y_1, \ldots, y_n)$ if and only if

$$(x_0, x_1, \ldots, x_n)T = \rho(y_0, y_1, \ldots, y_n) \text{ for some } \rho \in GF(q)^*.$$

An automorphism σ of $GF(q)$ can be extended to a collineation σ of $PG(n,q)$. A point $X = (x_0, x_1, \ldots, x_n)$ is mapped under σ to the point $X^\sigma = (x_0^\sigma, x_1^\sigma, \ldots, x_n^\sigma)$. The Fundamental Theorem of Projective Geometry says that every collineation $\mathcal{T}'$ of $PG(n,q)$ is given by $\mathcal{T}' = \sigma\mathcal{T}$, where σ is an automorphism of $GF(q)$ and $\mathcal{T}$ is a projectivity. If $\{P_0, \ldots, P_{n+1}\}$ and $\{P'_0, \ldots, P'_{n+1}\}$ are two sets of $n+2$ points in $PG(n,q)$ such that no $n+1$ points from the same set lie in a hyperplane, then there is a unique projective $\mathcal{T}$ such that $P'_i = P_i^{\mathcal{T}}$ for all $i = 0, \ldots, n+1$. A **correlation** $\mathcal{T}$ is a projectivity from $\mathcal{S} = \mathcal{PG}(\backslash, \amalg)$ to its dual $\mathcal{S}'$. If $\mathcal{T}$ is involutary then $\mathcal{T}$ is a **polarity**.

Every line of $PG(n,q)$ contains $q+1$ points and $PG(n,q)$ contains $q^n + \cdots + q + 1$ points. There are

$$\prod_{i=0}^{m} \frac{q^{n-i+1} - 1}{q^{i+1} - 1}$$

subspaces of dimension m, each of which contains $q^m + \cdots + q + 1$ points of $PG(n,q)$. The dimension of the intersection $X \cap Y$ and span $\langle X, Y \rangle$ of subspaces X, Y can be determined using Grassman's identity:

$$\dim X + \dim Y = \dim (X \cap Y) + \dim \langle X, Y \rangle.$$

Let W be an n-dimensional vector space over $GF(q)$. Then the set of all cosets of subspaces of W is called the ***n*-dimensional affine space of order *q***, denoted $AG(n,q)$. The cosets of i-dimensional subspaces of W are the i-dimensional flats of $AG(n,q)$. Incidence is subspace containment. The 0-, 1-, 2- and $(n-1)$-dimensional flats of $AG(n,q)$ are called points, lines, planes and hyperplanes respectively. Two

given i-dimensional flats are parallel if and only if they belong to the same subspace of W. In this thesis we are mainly concerned with parallel classes of hyperplanes.

An n-dimensional affine space $AG(n,q)$ of order q can be obtained by removing from $PG(n,q)$ a fixed hyperplane $\mathcal{H}_\infty$ together with all the subspaces contained in it. We call $\mathcal{H}_\infty$ the hyperplane at infinity. The hyperplanes of a parallel class of $AG(n,q)$ are the hyperplanes containing a given $(n-2)$-dimensional subspace of $\mathcal{H}_\infty$, so there is a correspondence between the parallel classes of $AG(n,q)$ and the hyperplanes of $\mathcal{H}_\infty$.

1.5 Motivation and outline

The motivation for the first part of this research arises from the problem of trying to ascertain the size of the smallest set of elements for which no linear (n,q,t)-perfect hash family exists. We give a brief description of perfect hash families taken from [5] and refer the interested reader to [5] and [3] for a detailed description and a more extensive bibliography.

Let V be a set of order n and let F be a set of order q. A set S of functions from V to F is an (n,q,t)-perfect hash family if for any t-subset P of V, there exists a function ϕ in S which is injective when restricted to P. An (n,q,t)-perfect hash family is linear if F may be identified with the field of order q, $GF(q)$, and V a vector space over F, such that S becomes a set of linear functionals. In this case, q is a prime power and $n = q^d$ for some $d \geq 2$.

Interpreted geometrically, the elements of V are the points of the affine space $AG(d,q)$, and for any linear functional ϕ, the set of point $v \in V$ with $\phi(v) = \gamma$, where γ is an element of $GF(q)$, forms a hyperplane of $AG(d,q)$, and ϕ corresponds to a parallel class of hyperplanes. Hence a set of parallel classes determines a linear (q^d,q,t)-perfect hash family if any t points of $AG(d,q)$ belong to distinct hyperplanes of some parallel class in the set. By embedding $AG(d,q)$ in $PG(d,q)$ such that $AG(d,q) = PG(d,q) \setminus \mathcal{H}_\infty$ for some hyperplane $\mathcal{H}_\infty$ of $PG(d,q)$, a parallel class of hyperplanes of $AG(d,q)$ corresponds to the hyperplanes of $PG(d,q)$ containing a given $(d-2)$-dimensional subspace in $\mathcal{H}_\infty$. Then a set of parallel

classes S is a linear (q^d, q, t)-perfect hash family if and only if for every set P of t points, there is a $(d-2)$-dimensional subspace in $\mathcal{H}_\infty$ corresponding to a parallel class in S such that the secants of P miss it. In particular, in $PG(2,q)$, no linear (q^2, q, k)-perfect hash family exists if there is a k-arc $\mathcal{K}$ covering a line l_∞, that is, every point on l_∞ lies on a secant of $\mathcal{K}$. The first part of this thesis investigates such k-arcs:

In Chapter 2, we give a definition of k-arcs covering a line, and obtain a lower bound on the size of such k-arcs, as well as present some examples and constructions of families of small k-arcs covering a line in $PG(2,q)$. We discuss also the notion of irreducibility in this context.

In Chapter 3 we discuss 1-regular k-arcs $\mathcal{K}$ covering a line l_∞. These are precisely the k-arcs meeting the lower bound in Chapter 2, and are characterised by the property that every point on l_∞ lies on exactly one secant of $\mathcal{K}$. We show that there are only four cases where such k-arcs exist if q is a prime power, and we discuss this in detail. We then consider the generalisation to n-regular k-arcs $\mathcal{K}$, where every point of l_∞ lies on exactly n secants of $\mathcal{K}$. It is shown that n is at most $k/2$ and the $k/2$-regular k-arcs are characterised as hyperovals in planes of even order. We consider also (n_1, n_2)-regular k-arcs $\mathcal{K}$, where half the points of l_∞ lie on n_1 secants to $\mathcal{K}$ and the other half on n_2 secants. The last section of Chapter 3 discusses some concepts and results in the literature related to those of Chapters 2 and 3.

Chapter 4 examines some generalisations of k-arcs covering a line. We consider (k, n)-arcs covering arbitrary sets of points in the plane, as well as the generalisation of the concept to sets of points covering a hyperplane in higher dimensional projective spaces. We show that in fact a k-arc covering a line in $PG(2,q)$ also covers a hyperplane in $PG(n,q)$ for all $n > 2$. This implies that if there is no linear (q^2, q, k)-perfect hash family then there is no (q^n, q, k)-perfect hash family for all $n > 2$. We discuss also some open questions that arise from this research.

The last chapter of this thesis chronicles the investigation into the combinatorial and geometric properties of a family of planes in $PG(5,q)$ constructed by Yoshiara. A detailed outline of this chapter is given at the end of Section 5.1.

Chapter 2

Arcs covering a line

This chapter introduces the concept of k-arcs covering a line in finite projective planes. In Section 2.1, we establish a lower bound on such k-arcs. Section 2.2 gives some examples of k-covers arising from existing structures in a projective plane and Section 2.3 gives two new constructions in the Desarguesian planes using sharply focused sets. We give examples of minimum k-covers in small planes, of order $q \leq 11$, in Section 2.4 and discuss irreducible k-covers in Section 2.5.

2.1 Definitions and lower bounds

Let Π_q be a projective plane of order q. Let $\mathcal{K}$ be a k-arc in Π_q and let l_∞ be a line disjoint from $\mathcal{K}$.

Definition 2.1.1 We say that a pair of distinct points Q_1, Q_2 **covers** a point P if P lies on the line Q_1Q_2. We say that $\mathcal{K}$ **covers** l_∞ if every point on l_∞ lies on at least one secant of $\mathcal{K}$, and we call $\mathcal{K}$ a ***k*-cover** for l_∞.

By simple counting we obtain the following lower bound on the size of a k-cover $\mathcal{K}$:

Theorem 2.1.2 If $\mathcal{K}$ is a k-cover for l_∞ in Π_q, then

$$k \geq \frac{1+\sqrt{8q+9}}{2},$$

with equality if and only if every point on l_∞ lies on exactly one secant of $\mathcal{K}$.

Proof: The number of distinct secants to $\mathcal{K}$ is $k(k-1)/2$ and each secant meets l_∞ exactly once. Hence, if $\mathcal{K}$ covers l_∞ then

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

Rearranging the above equation we have

$$k^2 - k - 2(q+1) \geq 0,$$

and since $k \geq 0$, we have

$$k \geq \frac{1+\sqrt{8q+9}}{2}.$$

Every point on l_∞ lies on exactly one secant of $\mathcal{K}$ if and only if the number of secants of $\mathcal{K}$ is exactly $q+1$, that is, $k(k-1)/2 = q+1$, and the result follows. □

Definition 2.1.3 We say that a k-cover $\mathcal{K}$ of l_∞ is **1-regular** if every point of l_∞ lies on exactly one secant to $\mathcal{K}$. In general, $\mathcal{K}$ is an ***n*-regular** k-cover if every point on l_∞ lies on exactly n secants of $\mathcal{K}$.

Using the same counting argument as in the proof of Theorem 2.1.2 above, if $\mathcal{K}$ is an n-regular k-cover then

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

so that

$$k^2 - k - 2n(q+1) = 0.$$

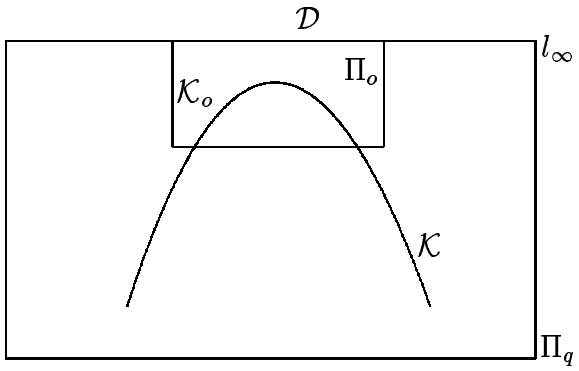
Taking the positive root, we have

$$k = \frac{1+\sqrt{1+8n(q+1)}}{2}.$$

We discuss 1-regular k-covers in Section 3.1 and n-regular k-covers in Section 3.2.

If Π_q is a plane of square order admitting a Baer subplane Π_o which in turn admits a k_o-cover $\mathcal{K}_o$ for a line $l_\infty \cap \Pi_o$ of Π_o, then $\mathcal{K}_o$ can be extended to a k-cover $\mathcal{K}$ of l_∞ containing $\mathcal{K}_o$ by adding some points in $\Pi_q \setminus \Pi_o$. The following result gives a lower bound for the number of points which must be added in such an extension:

Figure 2.1: Extension of $\mathcal{K}_o$ to $\mathcal{K}$.



Theorem 2.1.4 Let Π_q be a projective plane of order q, q a square, and let l_∞ be a line of Π_q. Let Π_o be a Baer subplane of Π_q such that l_∞ is a secant to Π_o. Let $\mathcal{K}_o \subseteq \Pi_o$ be a k_o-cover of $l_\infty \cap \Pi_o = \mathcal{D}$. (See Figure 2.1.) Suppose $\mathcal{K}$ is a k-cover of Π containing $\mathcal{K}_o$. Then

$$k \geq \frac{1 + \sqrt{1 + 4[k_o(k_o - 1) + 2(q - \sqrt{q})]}}{2} .$$

Equality is achieved if and only if the points of $\mathcal{K} \setminus \mathcal{K}_o$ lie on distinct lines of Π_o missing $\mathcal{K}_o$, no secant joining two points of $\mathcal{K} \setminus \mathcal{K}_o$ meets l_∞ in $\mathcal{D}$, and every point on $l_\infty \setminus \mathcal{D}$ is covered exactly once.

Proof: Through every point on $\Pi_q \setminus \Pi_o$ there pass q tangents and one secant to Π_o. Since l_∞ is a secant to Π_o, every affine line through a point on $l_\infty \setminus \mathcal{D}$ meets $\mathcal{K}_o$ in at most one point.

Let P be a point of $\mathcal{K} \setminus \mathcal{K}_o$. Then P lies on a unique line l_o of Π_o. If l_o is a tangent to $\mathcal{K}_o$, then $\mathcal{K}_o \cup \{P\}$ covers $k_o - 1$ points of $l_\infty \setminus \mathcal{D}$. If l_o misses $\mathcal{K}_o$, then $\mathcal{K}_o \cup \{P\}$ covers k_o points of $l_\infty \setminus \mathcal{D}$. Since there are $(k - k_o)$ points of $\mathcal{K} \setminus \mathcal{K}_o$, the secants of $\mathcal{K}$ of type $\{PQ \mid P \in \mathcal{K} \setminus \mathcal{K}_o,\ Q \in \mathcal{K}_o\}$ covers at most $(k - k_o)k_o$ points of $l_\infty \setminus \mathcal{D}$.

On the other hand, the secants of type $\{PQ \mid P,\ Q \in \mathcal{K} \setminus \mathcal{K}_o\}$ covers at most $\begin{pmatrix} k-k_o \\ 2 \end{pmatrix}$ points of $l_\infty \setminus \mathcal{D}$. So if $\mathcal{K}$ is a k-cover for l_∞, we must have

$$\begin{pmatrix} k-k_o \\ 2 \end{pmatrix} + k_o(k-k_o) \geq q - \sqrt{q}.$$

Collecting terms in k, we have

$$k^2 - k - [k_o(k_o-1) + 2(q-\sqrt{q})] \geq 0,$$

and since $k \geq 0$, we have

$$k \geq \frac{1 + \sqrt{1 + 4[k_o(k_o-1) + 2(q-\sqrt{q})]}}{2}.$$

Equality is achieved, that is, $\begin{pmatrix} k-k_o \\ 2 \end{pmatrix} + k_o(k-k_o) = q - \sqrt{q}$, if and only if

(a) the secants joining a point of $\mathcal{K} \setminus \mathcal{K}_o$ and a point of $\mathcal{K}_o$ cover exactly $k_o(k-k_o)$ points of $l_\infty \setminus \mathcal{D}$, that is, every point $P \in \mathcal{K} \setminus \mathcal{K}_o$ lies on a line of Π_o missing $\mathcal{K}_o$,

(b) the secants joining points of $\mathcal{K} \setminus \mathcal{K}_o$ cover exactly $\begin{pmatrix} k-k_o \\ 2 \end{pmatrix}$ points of $l_\infty \setminus \mathcal{D}$, that is, the points of $\mathcal{K} \setminus \mathcal{K}_o$ lie on distinct lines of Π_o and no secant PQ, $P, Q \in \mathcal{K} \setminus \mathcal{K}_o$, meets l_∞ in $\mathcal{D}$, and

(c) every point on $l_\infty \setminus \mathcal{D}$ is covered exactly once.

Hence equality is achieved if and only if the points of $\mathcal{K} \setminus \mathcal{K}_o$ lie on distinct lines of Π_o missing $\mathcal{K}_o$, no secant PQ, $P, Q \in \mathcal{K} \setminus \mathcal{K}_o$ meets l_∞ in $\mathcal{D}$, and every point on $l_\infty \setminus \mathcal{D}$ is covered exactly once. □

The question then arises as to whether, in general, one can extend an n-regular $\mathcal{K}_o$-cover $\mathcal{K}_o$ in Π_o to an n-regular k-cover $\mathcal{K}$ in Π_q. We discuss this in Section 3.2. In the next section we give some examples of k-covers.

2.2 Examples of k-covers

Example 2.2.1 Let $\mathcal{K}$ be a complete arc in a projective plane of order q, Π_q, that is, every point of Π_q lies on a secant of $\mathcal{K}$. In other words, $\mathcal{K}$ covers every point of Π_q and hence every line of Π_q disjoint from it. It follows that a complete k-arc is a k-cover for every line disjoint from it. In Π_q, a complete k-arc satisfies

$$\frac{3+\sqrt{8q+1}}{2} \leq k \leq \begin{cases} q+1 & \text{if } q \text{ is odd,} \\ q+2 & \text{if } q \text{ is even,} \end{cases}$$

so there is a k-cover for a line with k in that range. The upper bounds are well-known. The lower bound is obtained as follows (see [15]): Let $\mathcal{K}$ be a k-arc and l a tangent to $\mathcal{K}$ at a point P. If the $(k-1)(k-2)/2$ secants of $\mathcal{K}$ do not cover $l \setminus \{P\}$, then $\mathcal{K}$ is incomplete. This is certainly the case if $q > (k-1)(k-2)/2$. So a complete arc satisfies $(k-1)(k-2)/2 \geq q$, that is, $k \geq (3+\sqrt{8q+1})/2$.

In $PG(2,q)$, there is a complete k-arc and hence a k-cover with the following values:

$$k = \begin{cases} \dfrac{q+5}{2} & \text{if } q \equiv -1 \bmod 4, \\ \dfrac{q+4}{2} & \text{if } q \text{ is even.} \end{cases}$$

These examples can be found in [15]. We describe them briefly here:

In $PG(2,q)$, $q \equiv -1 \bmod 4$, a set of $(q+5)/2$ points can be chosen consisting of an external point Q of a conic $\mathcal{C}$, the 2 points of contact of the tangents to $\mathcal{C}$ through Q, and one point of $\mathcal{C}$ on each of the $(q-1)/2$ secants of $\mathcal{C}$ through Q, so that it forms a complete arc. For example, if α is a primitive root of $GF(q)$, the $(q+5)/2$ points

$$\left\{(1,\alpha^{2i},\alpha^{-2i}) \mid i \in \left\{1,\ldots,\frac{q-1}{2}\right\}\right\} \cup \{(1,0,0),(0,1,0),(0,0,1)\}$$

is a complete arc.

In $PG(2,q)$, q even, a set of $(q+4)/2$ points can be chosen consisting of a point Q not on a hyperoval $\mathcal{O}$, and one of the points of $\mathcal{O}$ on each of the $(q+2)/2$ secants to $\mathcal{O}$ through Q. Now, in $GF(2^h)$, let $D(t) = t + t^2 + t^4 + \cdots + t^{2^{h-1}}$. Then an element t of $GF(2^h)$ is said to belong to Category 0 or 1 according to whether the value of $D(t)$ is 0 or 1. It can be shown that the $(q+4)/2$ points

$$\left\{(t,t^2,1) \mid t \text{ belongs to Category } 1\right\} \cup \{(1,0,0),(1,s,0)\},$$

where s is of Category 1, is a complete arc. $\square$

The k-covers described above have sizes the order of $q/2$, which far exceeds the order of the lower bound of Theorem 2.1.2, which is $\sqrt{2q}$. In the next example we describe a family of k-covers which are not complete arcs in general. This family of k-covers has k the order of $4\sqrt{q}$.

Example 2.2.2 In [12], Giulietti and Ughi constructed a family of $4(\sqrt{q}-1)$-arcs $\mathcal{K}$ in $PG(2,q)$, where $q=p^2$ and $p \equiv -1 \bmod 4$ is a prime. These arcs are complete for $q \leq 961$ and for $961 < q \leq 16129$, there is a complete arc $\bar{\mathcal{K}}$ containing $\mathcal{K}$ with $|\bar{\mathcal{K}}| \leq 6\sqrt{q}$. In [11], Giulietti generalised this construction to $q=p^2$, where p is any odd prime power. He showed that this construction yields many small complete arcs in $PG(2,q)$ for $q \leq 1681$ and $q = 2401$. Giulietti's construction $\mathcal{K}$ is as follows:

Let $q=p^2$, p an odd prime power. Let θ be a quadratic non-residue in $GF(p)$ and let $i \in GF(q)$, $i^2=\theta$. Then $\mathcal{K} = \mathcal{K}_1 \cup \mathcal{K}_2 \cup \mathcal{K}_3 \cup \mathcal{K}_4$, with

$$\begin{aligned}
\mathcal{K}_1 &= \left\{ P(\alpha) = \left(\alpha, -\frac{\theta}{\alpha}, 1\right) \mid \alpha \in GF(p)^* \right\}, \\
\mathcal{K}_2 &= \left\{ Q(\beta) = \left(\beta, -\frac{i\theta}{\beta}, 1\right) \mid \beta \in GF(p)^* \right\}, \\
\mathcal{K}_3 &= \left\{ R(\gamma) = \left(i\gamma, -\frac{\theta}{\gamma}, 1\right) \mid \gamma \in GF(p)^* \right\}, \\
\mathcal{K}_4 &= \left\{ S(\delta) = \left(i\delta, -\frac{i}{\delta}, 1\right) \mid \delta \in GF(p)^* \right\}.
\end{aligned}$$

By using a computer, Giulietti showed that, while $\mathcal{K}$ is complete in many cases as mentioned above, for $q = 1681$, 1849, 2209, and $2401 < q \leq 6241$, $\mathcal{K}$ is *not* complete for all valid values of θ. We show that, nevertheless, $\mathcal{K}$ covers the line $z=0$ for all q.

Proof: Every element of $GF(q)$ can be written in the form $a+ib$, with a, $b \in GF(p)$. The points on $z=0$ can be written as

$$\{ (1, a+ib, 0) \mid a, b \in GF(p) \} \cup \{(0,1,0)\}.$$

We partition the points on $z=0$ into several parts,

$$L_0 = \{(0,1,0), (1,0,0)\},$$

$$
\begin{aligned}
L_1 &= \{(1,a,0) \mid a \in GF(p)^*\},\\
L_2 &= \{(1,ia,0) \mid a \in GF(p)^*\},\\
L_3 &= \{(1,a+ib,0) \mid a \neq -b, a, b \in GF(p)^*\},\\
L_4 &= \{(1,a-ia,0) \mid a \in GF(p)^*\},
\end{aligned}
$$

and prove that each part is covered by $\mathcal{K}$:

(a) The points $L_0 = \{(0,1,0),(1,0,0)\}$ are covered:

The points $(1,-\theta,1)$ on $\mathcal{K}_1$ and $(1,-i\theta,1)$ on $\mathcal{K}_2$ cover the point $(0,1,0)$, while the points $(1,-\theta,1)$ on $\mathcal{K}_1$ and $(i,-\theta,1)$ on $\mathcal{K}_3$ cover the point $(1,0,0)$.

(b) The points $L_1 = \{(1,a,0) \mid a \in GF(p)^*\}$ are covered by $\mathcal{K}_1$:

The points $(1,-\theta,1)$, $(\beta,-\theta/\beta,1)$ of $\mathcal{K}_1$, $\beta \neq 1$, cover the point $(1,x,0)$ if and only if

$$
\begin{vmatrix}
1 & x & 0\\
1 & -\theta & 1\\
\beta & -\frac{\theta}{\beta} & 1
\end{vmatrix} = 0,
$$

that is,

$$
x(1-\beta) = \theta\left(\frac{1-\beta}{\beta}\right),
$$

and so $x = \theta/\beta$.

As β ranges through $GF(p)^* \setminus \{1\}$, x ranges through $GF(p)^* \setminus \{\theta\}$. Also, the points $(\alpha,-\theta/\alpha,1)$, $(\alpha^{-1},-\theta/\alpha^{-1},1)$ of $\mathcal{K}_1$, $\alpha \neq 1$, cover $(1,\theta,0)$, since

$$
\begin{vmatrix}
1 & \theta & 0\\
\alpha & -\frac{\theta}{\alpha} & 1\\
\alpha^{-1} & -\frac{\theta}{\alpha^{-1}} & 1
\end{vmatrix} = \left(-\frac{\theta}{\alpha} + \frac{\theta}{\alpha^{-1}}\right) - \theta\left(\alpha - \alpha^{-1}\right) = 0.
$$

Hence all the points of L_1 are covered by $\mathcal{K}_1$.

(c) The points $L_2 = \{(1,ia,0) \mid a \in GF(p)^*\}$ are covered by $\mathcal{K}_2$:

The points $(1,-i\theta,1)$, $(\beta,-i\theta/\beta,1)$ of $\mathcal{K}_2$, $\beta \neq 1$, cover the point $(1,ix,0)$ if and only if

$$
\begin{vmatrix}
1 & ix & 0\\
1 & -i\theta & 1\\
\beta & -\frac{i\theta}{\beta} & 1
\end{vmatrix} = 0,
$$

that is,

$$ix(1-\beta) = i\theta\left(\frac{1-\beta}{\beta}\right),$$

and so $x = \theta/\beta$.

As above, x ranges through $GF(p)^* \setminus \{\theta\}$ as β ranges through $GF(p)^* \setminus \{1\}$, and the points $(\alpha, -i\theta/\alpha, 1)$, $(\alpha^{-1}, -i\theta/\alpha^{-1}, 1)$ of $\mathcal{K}_2$ cover $(1, i\theta, 0)$. Hence all the points of L_2 are covered by $\mathcal{K}_2$.

(d) The set $L_3 = \{(1, a+ib, 0) \mid a \neq -b, a, b \in GF(p)^*\}$ is covered:

The point $(1, x, 0)$ is covered by $(\alpha, -\theta/\alpha, 1)$ of $\mathcal{K}_1$, $(\beta, -i\theta/\beta, 1)$ of $\mathcal{K}_2$, $\alpha \neq \beta$, if and only if

$$\begin{vmatrix} 1 & x & 0 \\ \alpha & -\frac{\theta}{\alpha} & 1 \\ \beta & -\frac{i\theta}{\beta} & 1 \end{vmatrix} = 0,$$

that is,

$$x = -\frac{\theta}{\alpha(\alpha-\beta)} + i\frac{\theta}{\beta(\alpha-\beta)},$$

and $(1, x, 0)$ is covered by $(i\alpha, -\theta/\alpha, 1)$ of $\mathcal{K}_3$, $(i\beta, -i/\beta, 1)$ of $\mathcal{K}_4$, $\alpha \neq \beta$, if and only if

$$\begin{vmatrix} 1 & x & 0 \\ i\alpha & -\frac{\theta}{\alpha} & 1 \\ i\beta & -\frac{i}{\beta} & 1 \end{vmatrix} = 0,$$

that is,

$$x = \frac{1}{\beta(\alpha-\beta)} - i\frac{1}{\alpha(\alpha-\beta)}.$$

Let

$$F_1 = \left\{ \left(\frac{1}{\beta(\alpha-\beta)}, -\frac{1}{\alpha(\alpha-\beta)} \right) \mid \alpha, \beta \in GF(p)^*,\ \alpha \neq \beta \right\},$$
$$F_2 = \left\{ \left(-\frac{\theta}{\alpha(\alpha-\beta)}, \frac{\theta}{\beta(\alpha-\beta)} \right) \mid \alpha, \beta \in GF(p)^*,\ \alpha \neq \beta \right\}.$$

We show that $|F_1| = |F_2| = \frac{1}{2}(p-1)(p-2)$ and $F_1 \cap F_2 = \emptyset$. This means that as α, β range through $GF(p)^*$, $\alpha \neq \beta$,

$$\frac{1}{\beta(\alpha-\beta)} - i\frac{1}{\alpha(\alpha-\beta)} \quad \text{and} \quad -\frac{\theta}{\alpha(\alpha-\beta)} + i\frac{\theta}{\beta(\alpha-\beta)}$$

takes on every value of $a+ib$, $a \neq -b$, $a, b \in GF(p)^*$ and so the set L_3 is covered by $\mathcal{K}$.

Let $\beta \in GF(p)^*$ be fixed and let

$$(F_1)_\beta = \left\{ \left(\frac{1}{\beta(\alpha-\beta)}, \ -\frac{1}{\alpha(\alpha-\beta)} \right) \ | \ \alpha \in GF(p)^*, \ \alpha \neq \beta \right\}.$$

Then,

$$\frac{1}{\beta(\alpha_1-\beta)} = \frac{1}{\beta(\alpha_2-\beta)} \ \Leftrightarrow \ \alpha_1 = \alpha_2,$$

so as α ranges through $GF(p)^* \setminus \{\beta\}$, the ordered pairs in $(F_1)_\beta$ take on distinct values. Hence $|(F_1)_\beta| = p-2$.

For a fixed β,

$$\left(\frac{1}{(-\beta)[(-\alpha)-(-\beta)]}, \ -\frac{1}{(-\alpha)[(-\alpha)-(-\beta)]} \right) = \left(\frac{1}{\beta(\alpha-\beta)}, \ -\frac{1}{\alpha(\alpha-\beta)} \right)$$

so that $(F_1)_\beta = (F_1)_{-\beta}$.

Suppose $\beta \neq \pm\gamma$, and suppose that there is an ordered pair $(x,y) \in (F_1)_\beta \cap (F_1)_\gamma$, then there are $\alpha_1 \neq \beta, \alpha_2 \neq \gamma$ such that

$$\beta(\alpha_1-\beta) = \gamma(\alpha_2-\gamma) \ \text{ and } \ \alpha_1(\alpha_1-\beta) = \alpha_2(\alpha_2-\gamma).$$

Hence

$$\frac{\alpha_1}{\beta} = \frac{\alpha_2}{\gamma} = k, \ \text{ for some } k \in GF(p)^*, \ k \neq 1.$$

Substituting $\alpha_1 = k\beta$ and $\alpha_2 = k\gamma$, the above equations become

$$\beta^2(k-1) = \gamma^2(k-1) \ \text{ and } \ k\beta^2(k-1) = k\gamma^2(k-1),$$

which implies that $\beta^2 = \gamma^2$, since $k \neq 0, 1$, but this is a contradiction since $\beta \neq \pm\gamma$, so we conclude that $(F_1)_\beta \cap (F_1)_\gamma = \emptyset$. Hence we have that

$$|F_1| = \left| \bigcup_{\beta \in GF(p)^*} (F_1)_\beta \right| = \frac{1}{2}(p-1)(p-2).$$

A similar argument shows that $|F_2| = \frac{1}{2}(p-1)(p-2)$.

Now, suppose that there is an ordered pair $(x,y) \in F_1 \cap F_2$. Then there exist $\alpha_1, \alpha_2, \beta_1, \beta_2$ such that $\alpha_1 \neq \beta_1, \alpha_2 \neq \beta_2$ and

$$\left(-\frac{\theta}{\alpha_1(\alpha_1-\beta_1)}, \ \frac{\theta}{\beta_1(\alpha_1-\beta_1)} \right) = \left(\frac{1}{\beta_2(\alpha_2-\beta_2)}, \ -\frac{1}{\alpha_2(\alpha_2-\beta_2)} \right).$$

Hence,

$$-\frac{\theta}{\alpha_1(\alpha_1-\beta_1)} = \frac{1}{\beta_2(\alpha_2-\beta_2)} \quad \text{and} \quad \frac{\theta}{\beta_1(\alpha_1-\beta_1)} = -\frac{1}{\alpha_2(\alpha_2-\beta_2)},$$

which gives

$$-\alpha_1(\alpha_1-\beta_1) = \theta\beta_2(\alpha_2-\beta_2) \qquad (\dagger)$$

and

$$-\beta_1(\alpha_1-\beta_1) = \theta\alpha_2(\alpha_2-\beta_2).$$

Adding the two equations, we have

$$\beta_1^2 - \alpha_1^2 = \theta(\alpha_2^2-\beta_2^2) \qquad (\ddagger)$$

and taking ratio we have

$$\frac{\alpha_2}{\beta_2} = \frac{\beta_1}{\alpha_1} = k, \text{ for some } k \in GF(p)^*, \ k \neq 1.$$

If $k \neq -1$, then substituting $\alpha_1 = \beta_1/k$, $\alpha_2 = k\beta_2$, equation $(\ddagger)$ becomes

$$\beta_1^2 - \frac{\beta_1^2}{k^2} = \theta(k\beta_2)^2 - \theta\beta_2^2,$$

that is,

$$\left(\frac{\beta_1}{k\beta_2}\right)^2 = \theta.$$

If $k = -1$, then substituting $\beta_1 = -\alpha_1$, $\beta_2 = -\alpha_2$, equation $(\dagger)$ becomes

$$-\alpha_1(\alpha_1+\alpha_1) = \theta(-\alpha_2)(\alpha_2+\alpha_2),$$

that is,

$$\left(\frac{\alpha_1}{\alpha_2}\right)^2 = \theta.$$

However, there is a contradiction in both cases, since θ is not a quadratic residue modulo p, so we must have $F_1 \cap F_2 = \emptyset$. This proves that L_3 is covered by $\mathcal{K}$.

(e) Lastly, the points $L_4 = \{(1, a-ia, 0) \mid a \in GF(p)^*\}$ are covered:

We use the fact that a point P is covered by $\mathcal{K}$ if and only if P^τ is covered by $\mathcal{K}$, where τ is a collineation fixing $\mathcal{K}$. In [11], it was shown that the group

$H = \langle \phi_\rho, \psi, \eta \mid \rho \in GF(p)^* \rangle$ is a subgroup of $PGL(3, q^2)$ which fixes $\mathcal{K}$ and $z = 0$, where

$$\phi_\rho = \begin{pmatrix} \rho & 0 & 0 \\ 0 & \rho^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \psi = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \eta = \begin{pmatrix} \frac{i}{\theta} & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

If $P = (1, a - ia, 0)$ then

$$P^{\phi_\rho} = \left(1, \frac{a}{\rho^2}(1-i), 0\right), \quad P^{\phi_\rho \eta} = \left(1, \frac{\theta a}{\rho^2}(1-i), 0\right).$$

There is therefore a collineation τ that maps $(1, a - ia, 0)$ to $(1, b - ib)$, $b \neq a$, a, b non-zero, where

$$\tau = \begin{cases} \phi_\rho, \ \rho = \sqrt{a/b}, & \text{if } a/b \text{ is a quadratic residue modulo } p, \\ \phi_\rho \eta, \ \rho = \sqrt{\theta a/b}, & \text{if } a/b \text{ is not a quadratic residue modulo } p. \end{cases}$$

This shows that H is transitive on L_4 and therefore if one point of L_4 is covered, all points of L_4 are covered. Since

$$\begin{vmatrix} 1 & \frac{2\theta}{\theta-1}(1-i) & 0 \\ 1 & -\theta & 1 \\ -i & \theta & 1 \end{vmatrix} = (-\theta - \theta) - \frac{2\theta}{\theta - 1}(1-i)(1+i) = 0,$$

the point $(1, 2\theta(1-i)/(\theta-1), 0)$ is covered by the line joining the points $(1, -\theta, 1)$ of $\mathcal{K}_1$ and $(-i, \theta, 1)$ of $\mathcal{K}_3$, and so L_4 is covered. □

We note that in the above example, $\mathcal{K}_1$, $\mathcal{K}_2$, $\mathcal{K}_3$ and $\mathcal{K}_4$ are all sharply focused sets, each fixed by the subgroup $\{\phi_\rho \mid \rho \in GF(p)^*\}$ of the cyclic group G of order $q - 1$ fixing the conic $xy = -\theta z^2$ containing $\mathcal{K}_1$, $\mathcal{K}_4$, as well as the conic $xy = -i\theta z^2$ containing $\mathcal{K}_2$, $\mathcal{K}_3$. (See Section 1.2.) The group G is in fact $\langle \phi_{\rho_o} \rangle$, where ρ_o is a generator of the multiplicative group $GF(q)^*$. From the proof above we note also that all the points on $z = 0$ are covered more than once:

(a) In L_0, the point $(0, 1, 0)$ is covered by the pair of points $\{P(\alpha), Q(\alpha)\}$, while the point $(1, 0, 0)$ is covered by the pair of points $\{P(\alpha), R(\alpha)\}$, for all $\alpha \in GF(p)^*$. So each point in L_0 is covered at least $p - 1$ times.

(b) Every point in L_1 is covered at least $(p-3)/2$ times by $\mathcal{K}_1$ and $(p-3)/2$ times by $\mathcal{K}_4$, since $\mathcal{K}_1$ and $\mathcal{K}_4$ are both sharply focused on L_1.

(c) Similarly, every point in L_2 are covered at least $(p-3)/2$ times by $\mathcal{K}_2$ and $(p-3)/2$ times by $\mathcal{K}_3$, since both $\mathcal{K}_2$ and $\mathcal{K}_3$ are sharply focused on L_2.

(d) The points on L_3 are covered at least twice, since a point on L_3 covered by $P(\alpha)$ on $\mathcal{K}_1$, $Q(\beta)$ on $\mathcal{K}_2$ is also covered by the pair $\{P(-\alpha), Q(-\beta)\}$. Similarly, a point covered by the points $R(\alpha)$ on $\mathcal{K}_3$, $S(\beta)$ on $\mathcal{K}_4$ is also covered by the pair $\{R(-\alpha), S(-\beta)\}$.

(e) The points $P(\alpha)$ on $\mathcal{K}_1$, $R(-\alpha)$ on $\mathcal{K}_3$ cover the point $X(\alpha)$ on L_4, where

$$X(\alpha) = \left(1, -\frac{2\theta}{\alpha^2(1-\theta)}(1-i), 0\right),$$

since $P(\alpha)$, $R(-\alpha)$ cover $(1, x, 0)$ if and only if

$$\begin{vmatrix} 1 & x & 0 \\ \alpha & -\frac{\theta}{\alpha} & 1 \\ -i\alpha & \frac{\theta}{\alpha} & 1 \end{vmatrix} = 0,$$

that is, $x = -2\theta(1-i)/\alpha^2(1-\theta)$. It is staightforward to verify that $X(\alpha)$ is also covered by the pair of points $\{P(-\alpha), R(\alpha)\}$. These two pairs of points $\{P(\alpha), R(-\alpha)\}$, $\{P(-\alpha), R(\alpha)\}$, are in fact the images of $\{P(1), R(-1)\}$ and $\{P(-1), R(1)\}$ respectively under ϕ_α.

Similarly, the points $Q(\beta)$ on $\mathcal{K}_2$ and $S(-\beta/\theta)$ on $\mathcal{K}_4$ cover the point $Y(\beta)$ on L_4, where

$$Y(\beta) = \left(1, \frac{2\theta^2}{\beta^2(\theta-1)}(1-i), 0\right),$$

since $Q(\beta)$, $S(-\beta/\theta)$ cover $(1, x, 0)$ if and only if

$$\begin{vmatrix} 1 & x & 0 \\ \beta & -\frac{i\theta}{\beta} & 1 \\ -\frac{\beta}{i} & \frac{i\theta}{\beta} & 1 \end{vmatrix} = 0,$$

that is $x = 2\theta^2(1-i)/\beta^2(\theta-1)$. The point $Y(\beta)$ is also covered by another pair of points, $\{Q(-\beta), S(\beta/\theta)\}$. These two pairs of points $\{Q(\beta), S(-\beta/\theta)\}$, $\{Q(-\beta), S(\beta/\theta)\}$, are images of $\{R(1), P(-1)\}$ and $\{R(-1), P(1)\}$ respectively under $\phi_\beta\eta$.

From these observations, it would appear that some of the points on the $\mathcal{K}_i$'s can be removed without affecting the ability of the remaining points to cover $z = 0$. This is certainly true in the following case:

Let B be a subset of $GF(p)^*$ of size $(p-1)/2$ such that if b_1, b_2 are in B, then $b_1 \neq -b_2$. Let $\hat{\mathcal{K}_2}$ be the subset of $\mathcal{K}_2$ with

$$\hat{\mathcal{K}_2} = \{Q(\beta) \mid \beta \in B\},$$

and let $\mathcal{K}' = \mathcal{K} \setminus \{\hat{\mathcal{K}_2}\}$. Then the points in L_0, L_1 and L_2 would still be covered by $\mathcal{K}'$, while the points on L_3 formerly covered by a secant joining $Q(\beta)$ on $\hat{\mathcal{K}_2}$ to a point $P(\alpha)$ on $\mathcal{K}_1$ would still be covered by the pair $\{Q(-\beta), P(-\alpha)\}$. As for L_4, the points formerly covered by a secant joining $Q(\beta)$ on $\hat{\mathcal{K}_2}$ to the point $S(-\beta/\theta)$ on $\mathcal{K}_4$ would still be covered by the pair $\{Q(-\beta), S(\beta/\theta)\}$. Hence, by removing the points of $\hat{\mathcal{K}_2}$ from $\mathcal{K}$, we have a $7(\sqrt{q}-1)/2$-cover of $z = 0$. However, it is not clear exactly how many more points may be removed from $\mathcal{K}'$ before it ceases to cover $z = 0$.

In the next section we present two families of k-covers constructed using sharply focused sets. They give examples of k-covers about half the size of the k-covers in Example 2.2.2.

2.3 Two new constructions

We use sharply focused sets to construct two families of k-arcs covering a line in $PG(2,q)$. Before that, we deduce the following result from Results 1.2.1 and 1.2.2 and interpret it in terms of point sets covering a line:

Lemma 2.3.1 Let $\mathcal{C}$ be a conic in $PG(2,q)$ and l_∞ a line external or secant to $\mathcal{C}$. Let $\mathcal{K}(s)$ be the set of subgroup induced sharply focused sets of size s on $\mathcal{C}' = \mathcal{C} \setminus l_\infty$. For $K \in \mathcal{K}(s)$ and $P \in \mathcal{C}' \setminus K$, let

$$\mathrm{Int}(K, P, l_\infty) = \{AP \cap l_\infty \mid A \in K\}.$$

Then,

(a) $|\mathrm{Int}(K, P, l_\infty)| = s$ for $P \in \mathcal{C}' \setminus K$, that is, the lines joining P to K cover s points on l_∞.

(b) If $P \in \mathcal{C}' \setminus K$, then $\mathrm{Int}(K, l_\infty) \cap \mathrm{Int}(K, P, l_\infty) = \emptyset$, that is, $\mathrm{Int}(K, l_\infty)$ and $\mathrm{Int}(K, P, l_\infty)$ are disjoint subsets of points on l_∞ if P belongs to a sharply focused set in $\mathcal{K}(s)$ different from K. Hence the $(s+1)$-arc $K \cup \{P\}$ covers 2s points on l_∞.

(c) $\mathrm{Int}(K, P', l_\infty) \cap \mathrm{Int}(K, P'', l_\infty) = \emptyset$ if $P' \in K'$, $P'' \in K''$, K', $K'' \in \mathcal{K}(s) \setminus \{K\}$, $K' \neq K''$, that is, $\mathrm{Int}(K, P', l_\infty)$ and $\mathrm{Int}(K, P'', l_\infty)$ are disjoint subsets of points on l_∞ if P' and P'' belong to distinct sharply focused sets in $\mathcal{K}(s)$ different from K.

Proof: We recall from Section 1.2 that if K, K' are distinct sharply focused sets in $\mathcal{K}(s)$ then

$$\begin{aligned} \mathrm{Int}(K, l_\infty) &= \{AB \cap l_\infty \mid A, B \in K, A \neq B\}, \\ \mathrm{Int}(K, K', l_\infty) &= \{AB \cap l_\infty \mid A \in K, B \in K'\}. \end{aligned}$$

If we define, for a point $P \in \mathcal{C}' \setminus K$, the set of secants S_{KP} to be

$$S_{KP} = \{AP \mid A \in K\},$$

and for K, K',

$$S_{KK'} = \{AB \mid A \in K, B \in K'\},$$

then $\mathrm{Int}(K, P, l_\infty)$ and $\mathrm{Int}(K, K', l_\infty)$ are the sets of points on l_∞ covered by the sets of secants S_{KP} and $S_{KK'}$ respectively.

(a) This follows from the fact that $|K| = s$, and the lines PA, PB meet l_∞ in distinct points if A, B are distinct points of K.

(b) If $P \notin K$ then P belongs to a sharply focused set K' in $\mathcal{K}(s)$ distinct from K. The set of secants S_{KP} is then a subset of $S_{KK'}$. By Result 1.2.2(b), $\mathrm{Int}(K, l_\infty)$ and the set of points $\mathrm{Int}(K, K', l_\infty)$ covered by $S_{KK'}$ are disjoint, so it follows that the set $\mathrm{Int}(K, P, l_\infty)$ covered by S_{KP} must also be disjoint from $\mathrm{Int}(K, l_\infty)$.

The $(s+1)$-arc $K \cup \{P\}$ covers $2s$ points on l_∞ because K covers a set of s points and the secants PA, $A \in K$ cover a disjoint set of s points.

(c) As in (b) above, the set of secants $S_{KP'}$ is a subset of $S_{KK'}$, and the set $S_{KP''}$ is a subset of $S_{KK''}$. By Result 1.2.2(c), the two sets of points $\mathrm{Int}(K, K', l_\infty)$ and $\mathrm{Int}(K, K'', l_\infty)$ on l_∞ covered by the two sets of secants $S_{KK'}$ and $S_{KK''}$ are disjoint, so it follows that $\mathrm{Int}(K, P', l_\infty)$ and $\mathrm{Int}(K, P'', l_\infty)$ must also be disjoint. □

Corollary 2.3.2 Let $\mathcal{C}$ be a conic in $PG(2, q)$ and l_∞ a line external or secant to $\mathcal{C}$. Let $\mathcal{K}(s)$ be the set of subgroup induced sharply focused sets of size s on $\mathcal{C}' = \mathcal{C} \setminus l_\infty$ and let $n = |\mathcal{C}'|$. Let $K \in \mathcal{K}(s)$ and let $\mathcal{P}(K)$ be a system of distinct representatives of the sharply focused sets in $\mathcal{K}(s)$ different from K. Then the set $K \cup \{P \mid P \in \mathcal{P}(K)\}$ covers $l_\infty \setminus \mathcal{C}$.

Proof: Let $\mathrm{Int}'(l_\infty) = \{\mathrm{Int}(K, l_\infty)\} \cup \{\mathrm{Int}(K, P, l_\infty) \mid P \in \mathcal{P}(K)\}$. Then by Lemma 2.3.1 and Result 1.2.2(d), $\mathrm{Int}'(l_\infty)$ partitions $l_\infty \setminus \mathcal{C}$ and so $K \cup \{P \mid P \in \mathcal{P}(K)\}$ covers $l_\infty \setminus \mathcal{C}$. □

Construction 2.3.3 follows from Corollary 2.3.2:

Construction 2.3.3 In $PG(2, q)$, there is a k-arc $\mathcal{K}$ covering any given line l_∞ with $k = s + \frac{q+1}{s} - 1$ for any $s | q + 1$, $s \geq 3$. The construction is as follows:

Let $\mathcal{C}$ be a conic disjoint from l_∞. Let $\langle \gamma \rangle$ be the (unique) cyclic group of order $q + 1$ in $PGO(3, q)_{l_\infty}$ fixing $\mathcal{C}$ and l_∞. For any s dividing $q + 1$, the subgroup $N = \langle \gamma^{(q+1)/s} \rangle$ partitions the points of $\mathcal{C}$ into orbits of size s, each of which is sharply focused on l_∞ (Result 1.2.1). Let the orbits be denoted $\mathcal{K}(s) = \{K_1, \cdots, K_{\frac{q+1}{s}}\}$. Let K_i be one of the sharply focused sets in $\mathcal{K}(s)$ and let $\mathcal{P}(K_i)$ be a system of distinct representatives of the sharply focused sets in $\mathcal{K}(s)$ different from K_i,

$$\mathcal{P}(K_i) = \left\{ P_j \mid j = 1, \ldots, \frac{q+1}{s},\ j \neq i \right\},$$

where P_j is a representative of the sharply focused set K_j in $\mathcal{K}(s)$. Now, let $\mathcal{K} = \{K_i\} \cup \{P \mid P \in \mathcal{P}(K_i)\}$, that is, $\mathcal{K}$ consists of K_i together with one point from each of the other sharply focused set. Then $\mathcal{K}$ is a $(s + (q+1)/s - 1)$-arc and by Corollary 2.3.2, $\mathcal{K}$ covers l_∞.

For this construction we have $2\sqrt{q+1} - 1 \leq k \leq q + 1$. This construction yields k-covers with k close to the lower bound $2\sqrt{q+1} - 1$ only if there is a factor s of $q+1$

close to $\sqrt{q+1}$, for example, if $q+1=s^2$, $q+1=s(s+1)$ or $q+1=(s-1)(s+1)$. We give some examples below to show that this construction does give small k-covers in these special cases.

In the first case, if q is a prime power, then $q+1=s^2$ if and only if $(q,s)=(3,2)$ or $(8,3)$. For $(q,s)=(3,2)$, the construction does not apply since we need $s\geq 3$. For $q=8$, the lower bound $2\sqrt{q+1}-1=5$ is attained and coincides with that of Theorem 2.1.2, so this construction gives a best possible k-cover for $q=8$. For $q\neq 3,8$, $k>2\sqrt{q+1}-1$. In the instance where $q+1=s(s+1)$, we have $k=2s=\sqrt{4q+5}-1$, so the construction gives k-covers of the order of $2\sqrt{q}$ when q is of the form $s(s+1)-1$ for some positive integer s. The following table gives a numerical comparison of such k with that of the lower bound in Theorem 2.1.2.

s	q	$k=\sqrt{4q+5}-1$	$\lfloor\frac{1}{2}+\frac{\sqrt{8q+9}}{2}\rfloor$
2	5	4	4
3	11	6	6
4	19	8	7
5	29	10	9
6	41	12	10
8	71	16	13

In the case where $q+1=(s-1)(s+1)$, we have $k=2\sqrt{q+2}-1$, and the following table gives a comparison of such k with that of the lower bound in Theorem 2.1.2 for small q.

s	q	$k=2\sqrt{q+2}-1$	$\lfloor\frac{1}{2}+\frac{\sqrt{8q+9}}{2}\rfloor$
3	7	5	5
5	23	9	8
7	47	13	11
9	79	17	14

We see then that this construction gives smallest possible k-covers for some small q. If q is odd, we can always construct a k-cover with $k=(q+3)/2$ by taking $s=(q+1)/2$. This gives a smaller k-cover than that given by a complete arc in Example 2.2.1. □

Now, a conic covers every line disjoint from it. Using sharply focused sets and ideas from Theorem 2.1.4, we construct a family of k-covers in $PG(2,q)$, q a square, with k at most $2\sqrt{q}+1$. We extend a conic contained in a Baer subplane to a k-cover by adding points from sharply focused sets outside the Baer subplane.

Construction 2.3.4 Let $\Pi_q = PG(2,q)$, q a square, $\sqrt{q} > 5$, and let l_∞ be a line of Π_q. Let Π_o be a Baer subplane secant to l_∞. Let $\mathcal{C}_o$ be a conic in Π_o disjoint from $l_\infty \cap \Pi_o$ and $\mathcal{C}$ the conic containing $\mathcal{C}_o$ in Π_q. Since l_∞ misses $\mathcal{C}_o$, it must meet $\mathcal{C}$ in two distinct points. Let $\{P_1, P_2\} = \mathcal{C} \cap l_\infty$.

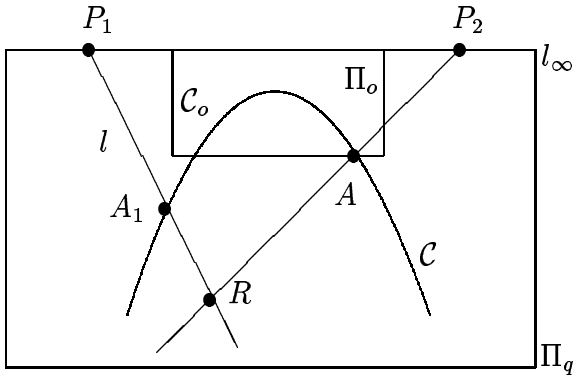
The subgroup of $PGO(3,\sqrt{q})$ fixing both $\mathcal{C}_o$ and $l_\infty \cap \Pi_o$ is isomorphic to the dihedral group of order $2(\sqrt{q}+1)$ (see Section 1.2). Let G be the cyclic subgroup of order $\sqrt{q}+1$ fixing both $\mathcal{C}_o$ and l_∞. Then G acts regularly on the points of $\mathcal{C}_o$ and, as a subgroup of $PGO(3,q)_{l_\infty}$ acting on Π_q, partitions $\mathcal{C} \setminus \{P_1, P_2\}$ into $\sqrt{q}-1$ orbits of $\sqrt{q}+1$ points and fixes $\{P_1, P_2\}$. Each orbit is sharply focused on l_∞ and, by Corollary 2.3.2, the set of points consisting of an orbit together with one point from each of the remaining orbits covers $l_\infty \setminus \mathcal{C} = l_\infty \setminus \{P_1, P_2\}$. We show that it is possible to choose at most one point from each of the $\sqrt{q}-2$ orbits on $\mathcal{C} \setminus \{P_1, P_2\}$ other than $\mathcal{C}_o$ and a point off the conic so that, together with $\mathcal{C}_o$, they form an arc which covers l_∞. Note that, by part (c) of Lemma 2.3.1, points from distinct orbits cover disjoint parts of $l_\infty \setminus \mathcal{C}$ when joined to the points of $\mathcal{C}_o$.

Let A_1 be any point on $\mathcal{C} \setminus \mathcal{C}_o$. Let l be the line P_1A_1. At most $\sqrt{q}(\sqrt{q}+1)/2$ points of $l \setminus \{P_1, A_1\}$ lie on a secant to $\mathcal{C}_o$, and one on the tangent to $\mathcal{C}$ at P_2. Let R be a point chosen from the remaining $(q-1) - (q+\sqrt{q})/2 - 1 > 0$ points on $l \setminus \{P_1, A_1\}$ not lying on a secant to $\mathcal{C}_o$ or the tangent to P_2. Let A be the point $\mathcal{C} \cap RP_2$. (See Figure 2.2.) Then P_1 is covered by RA_1 and P_2 is coverd by RA.

There are at most $\sqrt{q}+1$ secants through R joining a point of $\mathcal{C}_o$ and a point of $\mathcal{C} \setminus \mathcal{C}_o$. Let these points on $\mathcal{C} \setminus \mathcal{C}_o$ be called bad points and the remaining points on $\mathcal{C} \setminus \mathcal{C}_o$ good points. (See Figure 2.3.) So there are at most $\sqrt{q}+1$ bad points. We show that it is possible to choose only good points so that together with $\mathcal{C}_o$ and R, they form an arc covering l_∞.

There are two possible distributions of bad points among the orbits: either all the bad points lie in one single orbit, or they are distributed among n orbits,

Figure 2.2: Points A_1, A and R_1 in Construction 2.3.4.



$2 \leq n \leq \sqrt{q} - 2$. We consider the two cases separately.

Suppose there are $\sqrt{q}+1$ bad points all in one orbit ω. Then $A_1 \notin \omega$, $A \notin \omega$, and every line joining R to a point of $\mathcal{C}_o$ is a line joining a point of ω to a point of $\mathcal{C}_o$, so $\mathrm{Int}(\mathcal{C}_o, R, l_\infty) \subseteq \mathrm{Int}(\mathcal{C}_o, \omega, l_\infty)$. However, $|\mathrm{Int}(\mathcal{C}_o, \omega, l_\infty)| = \sqrt{q}+1$ by Result 1.2.2(a), and since R does not lie on a secant to $\mathcal{C}_o$, $|\mathrm{Int}(\mathcal{C}_o, R, l_\infty)| = \sqrt{q}+1$. So

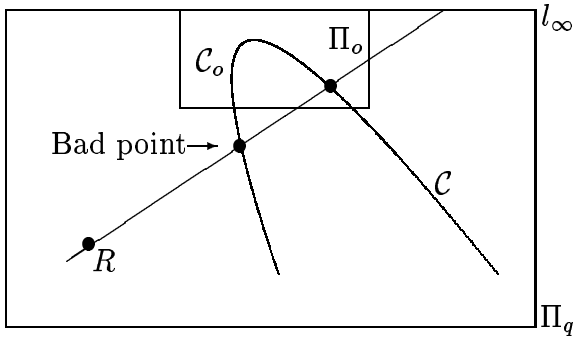
$$\mathrm{Int}(\mathcal{C}_o, \omega, l_\infty) = \mathrm{Int}(\mathcal{C}_o, R, l_\infty).$$

That is, the points on l_∞ covered by the secants joining points of ω to $\mathcal{C}_o$ are covered by the secants RP, $P \in \mathcal{C}_o$. This means that we do not need to choose a point of ω to cover $\mathrm{Int}(\mathcal{C}_o, \omega, l_\infty)$ on l_∞, since these points are covered by the secants joining R to points of $\mathcal{C}_o$. We then choose $\{A_2, \ldots, A_{\sqrt{q}-3}\}$ from the remaining orbits, which do not contain any bad points, as follows:

If A and A_1 belong to the same orbit or $A \in \mathcal{C}_o$ then choose A_{h+1}, $h = 1, \ldots, \sqrt{q}-4$, successively from each of the remaining $\sqrt{q}-4$ orbits on $\mathcal{C} \setminus \mathcal{C}_o$ which are not ω and do not contain A_1, such that A_{h+1} does not lie on RA_i for all $i \leq h$. This is possible since the number of such lines is at most $\sqrt{q}-4$, and each such line contains at most one point of the $(h+1)^{\text{th}}$ orbit. Let $\mathcal{K} = \mathcal{C}_o \cup \{R, A, A_1, A_2, \ldots, A_{\sqrt{q}-3}\}$. Then

$$|\mathcal{K}| = \begin{cases} (\sqrt{q}+1) + (\sqrt{q}-2) = 2\sqrt{q}-1 & \text{if } A \in \mathcal{C}_o, \\ (\sqrt{q}+1) + (\sqrt{q}-1) = 2\sqrt{q} & \text{if } A,\ A_1 \text{ lie in the same orbit.} \end{cases}$$

Figure 2.3: Bad points in Construction 2.3.4.



If A and A_1 belong to different orbits and $A \notin \mathcal{C}_o$, let $A_2 = A$ and choose $\{A_3, \ldots, A_{\sqrt{q}-3}\}$ as before. Then $\mathcal{K} = \mathcal{C}_o \cup \{R, A_1, A_2, \ldots, A_{\sqrt{q}-3}\}$ and

$$|\mathcal{K}| = (\sqrt{q}+1) + (\sqrt{q}-2) = 2\sqrt{q} - 1.$$

If there are $\sqrt{q}+1$ bad points distributed among n orbits $\omega_1, \ldots, \omega_n$, $2 \leq n \leq \sqrt{q}-2$, then every one of ω_i has between 1 and $\sqrt{q}+2-n$ bad points (and hence between $\sqrt{q}$ and $n-1$ good points). Since they cannot all have $\sqrt{q}+2-n$ bad points, at least one orbit, say ω_n must have at most $\sqrt{q}+1-n$ bad points and hence at least n good points, and $\omega_1, \ldots, \omega_{n-1}$ each has at least $n-1$ good points.

Now, if A and A_1 belong to the same orbit or $A \in \mathcal{C}_o$, let A_2 be any good point from ω_1, then pick A_{i+1} from the good points of ω_i, $i = 2, \ldots, n$, such that A_{h+1} does not lie on RA_j for all $j = 2, \ldots, h$, $2 \leq h \leq n$. This is possible since $\omega_1, \ldots, \omega_{n-1}$ have at least $n-1$ good points and ω_n has at least n good points. Choose $\{A_{n+2}, \ldots, A_{\sqrt{q}-2}\}$ from the remaining orbits such that A_{h+1} does not lie on RA_j for all $j \leq h$, $n+1 \leq h \leq \sqrt{q}-3$. This is possible since there are at most $\sqrt{q}-4$ such lines. Let $\mathcal{K} = \mathcal{C}_o \cup \{R, A, A_1, A_2, \ldots, A_{\sqrt{q}-2}\}$ and

$$|\mathcal{K}| = \begin{cases} (\sqrt{q}+1) + (\sqrt{q}-1) = 2\sqrt{q} & \text{if } A \in \mathcal{C}_o, \\ (\sqrt{q}+1) + \sqrt{q} = 2\sqrt{q}+1 & \text{if } A,\ A_1 \text{ lie in the same orbit.} \end{cases}$$

If A and A_1 belong to different orbits and $A \notin \mathcal{C}_o$, let $A_2 = A$ and choose the points $\{A_3, \ldots, A_{n+2}\}$ and $\{A_{n+3}, \ldots, A_{\sqrt{q}-2}\}$ as before. Then $\mathcal{K} = \mathcal{C}_o \cup$

$\{R, A_1, A_2, \ldots, A_{\sqrt{q}-2}\}$ and

$$|\mathcal{K}| = (\sqrt{q}+1) + (\sqrt{q}-1) = 2\sqrt{q}.$$

If there are strictly fewer than $\sqrt{q}+1$ bad points distributed among n orbits, $1 \leq n \leq \sqrt{q}-2$, then the above argument still works, giving

$$|\mathcal{K}| = \begin{cases} 2\sqrt{q} & \text{if } A, A_1 \text{ in the same orbit and } A \in \mathcal{C}_o, \\ 2\sqrt{q}+1 & \text{if } A, A_1 \text{ in the same orbit and } A \notin \mathcal{C}_o, \\ 2\sqrt{q} & \text{if } A, A_1 \text{ in different orbits.} \end{cases}$$

In all cases, the points of $\mathcal{C}_o$ together with the A_i's cover $l_\infty \setminus \mathcal{C}$ by Corollary 2.3.2 and the points $\{P_1, P_2\}$ are covered by RA_1 and RA. Furthermore, the points R and the A_i's have been chosen so that $\mathcal{K}$ is an arc. Hence $\mathcal{K}$ is a k-cover of l_∞ of order at most $2\sqrt{q}+1$. □

2.4 Minimum k-covers in small planes

Let $m(q)$ denote the smallest k for which a k-arc exists that covers a line l_∞ in a projective plane of order q. From Theorem 2.1.2 and the examples in Sections 2.2, 2.3, we have

$$\frac{1+\sqrt{8q+9}}{2} \leq m(q) \leq \begin{cases} \dfrac{q+3}{2} & \text{if } q \text{ is odd (Construction 2.3.3),} \\ \dfrac{q+4}{2} & \text{if } q \text{ is even (Example 2.2.1).} \end{cases}$$

For small q, $q \leq 11$, we have $m(q) = \left\lfloor \frac{1}{2} + \frac{\sqrt{8q+9}}{2} \right\rfloor$:

q	$m(q) = \lfloor \frac{1}{2} + \frac{\sqrt{8q+9}}{2} \rfloor$	Description
2	3	A triangle.
3	4	A quadrangle.
4	4	A quadrangle, see Example 2.4.1 below.
5	4	Construction 2.3.3 in $PG(2,5)$, $s = 3$.
7	5	Construction 2.3.3 in $PG(2,7)$, $s = 4$.
8	5	Construction 2.3.3 in $PG(2,8)$, $s = 3$.
9	5	A 5-arc in the Hall plane of order 9, see Theorem 3.1.5 in the next chapter.
11	6	Construction 2.3.3 in $PG(2,11)$, $s = 3$ or 4.

Example 2.4.1 In $PG(2,4)$, the line $z = 0$ is covered by the quadrangle $ABCD$, where A is the point with homogeneous coordinate $(1,1,1)$, B the point $(0,1,\alpha^2)$, C the point $(1,0,1)$, and D the point $(0,1,1)$, and α is the primitive root of x^2+x+1 over $GF(2)$. Note that in $PG(2,4)$, the diagonal points of a quadrangle are collinear, hence the points A, B, C, D must be chosen so that at most one diagonal point is on $z = 0$. □

Related to the concept of a minimum cover is that of an *irreducible* cover. We discuss this in the next section.

2.5 Irreducible k-covers

Definition 2.5.1 A k-cover $\mathcal{K}$ for a line l_∞ is **irreducible** if for all points P on $\mathcal{K}$, $\mathcal{K} \setminus \{P\}$ is not a cover for l_∞.

For example, 1-regular k-covers, as well as the k-arcs constructed using Construction 2.3.3 with $s = (q+1)/2$, q odd, are irreducible covers. In the first case, this is because a 1-regular k-cover $\mathcal{K}$ covers each point on l_∞ exactly once, so that the removal of any one point P results in the loss of $k-1$ secants, so there would be $k-1$ points on l_∞ not covered by $\mathcal{K} \setminus \{P\}$. In the second case, the $(q+3)/2$-cover $\mathcal{K}$ constructed using Construction 2.3.3 with $s = (q+1)/2$ lies on a conic which is partitioned into two sharply focused sets F_1, F_2, each of size $(q+1)/2$, and $\mathcal{K}$

consists of one of the sharply focused sets, say F_1, and a point Q from the other. Half of the points on l_∞ lie in the focus of F_1, that is, they lie on secants joining points of F_1. Each point on the other half of l_∞, however, lies on exactly one secant of $\mathcal{K}$ which joins Q to a point of F_1. So if a point of F_1 is removed then one of the points in that half would not be covered, while if Q is removed, then all the points in that half would not be covered. Hence $\mathcal{K}$ is irreducible. On the other hand, n-regular k-arcs, $n \geq 2$, are not irreducible covers, since every point on l_∞ lies on more than one secant and the removal of any single point of $\mathcal{K}$ would leave l_∞ still covered.

A minimum cover is necessarily irreducible, while the converse is not true. For example, in $PG(2, 11)$, a minimum k-cover has $k = 6$, so a 7-cover constructed using Construction 2.3.3 with $s = (q + 1)/2 = 6$ is irreducible but not minumum.

Call a secant of $\mathcal{K}$ **critical** if it covers a point on l_∞ not covered by any other secants. We have the following bounds on the number of critical secants of $\mathcal{K}$.

Lemma 2.5.2 Let $c(\mathcal{K})$ be the number of critical secants of $\mathcal{K}$. Then,

$$\frac{k}{2} \leq c(\mathcal{K}) \leq \frac{k(k-1)}{2}.$$

Proof: The upper bound follows from the fact that $\mathcal{K}$ has $k(k-1)/2$ secants. It is reached when all secants of $\mathcal{K}$ are critical, that is, when $\mathcal{K}$ is a 1-regular cover. The lower bound is derived from the fact that in an irreducible cover $\mathcal{K}$, every point P of $\mathcal{K}$ lies on at least one critical secant, for otherwise P could be removed and the points on l_∞ covered by a secant on P would still be covered by other secants, contradicting the irreducibility of $\mathcal{K}$. We count the set of flags

$$F = \{(P, l) \mid P \in \mathcal{K},\ l \text{ a critical secant of } \mathcal{K}\}.$$

There are k points on $\mathcal{K}$ and each point lies on at least one critical secant, so $|F| \geq k$. On the other hand, there are $c(\mathcal{K})$ critical secants, and each one lies on two points of $\mathcal{K}$, so $|F| = 2\,c(\mathcal{K})$. Hence we have $2\,c(\mathcal{K}) \geq k$ and the result follows. □

Using Lemma 2.5.2, we prove an upper bound of an irreducible cover:

Theorem 2.5.3 If $\mathcal{K}$ is an irreducible k-cover for a line l_∞ in a projective plane of order q, then

$$k \leq \frac{2(q+3)}{3}.$$

Proof: We count the flags

$$F = \{(P, l) \mid P \in l_\infty,\ l \text{ a secant of } \mathcal{K}\}.$$

Firstly, there are $k(k-1)/2$ secants of $\mathcal{K}$ and each one lie on exactly one point of l_∞, so $|F| = k(k-1)/2$. On the other hand, there are $c(\mathcal{K})$ points on l_∞, each lying on 1 critical secant, and $q+1-c(\mathcal{K})$ points on l_∞ each lying on at most $k/2$ secants of $\mathcal{K}$. So $|F| \leq (q+1-c(\mathcal{K}))(k/2) + c(\mathcal{K})$. Hence we have

$$\begin{aligned} \frac{k(k-1)}{2} &\leq (q+1-c(\mathcal{K}))\frac{k}{2} + c(\mathcal{K}) \\ &= \frac{k(q+1)}{2} - c(\mathcal{K})\left(\frac{k}{2} - 1\right) \\ &\leq \frac{k(q+1)}{2} - \frac{k}{2}\left(\frac{k}{2} - 1\right), \end{aligned}$$

since $c(\mathcal{K}) \geq k/2$ by Lemma 2.5.2. Simplifying the final inequality, we have

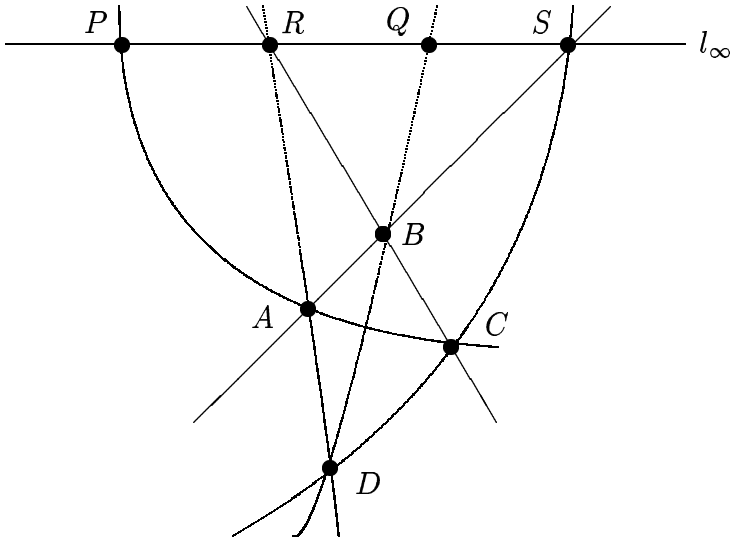
$$k \leq \frac{2(q+3)}{3}.$$

□

From the proofs of Lemma 2.5.2 and Theorem 2.5.3, we see that this upper bound is reached only if there are exactly $k/2$ critical secants and each of the $q+1-k/2$ points on l_∞ not on a critical secant lies on exactly $k/2$ secants of $\mathcal{K}$. This forces k to be even, and implies that critical secants partition the points of $\mathcal{K}$ into pairs, and the secants through each one of the $q+1-k/2$ points on l_∞ not on a critical secant also partition the points of $\mathcal{K}$ into pairs. The upper bound is certainly reached in the smallest case $q = 3$. In this case, $k = 4$, that is, $\mathcal{K}$ is a quadrangle in Π_3, a projective plane of order 3. We illustrate this in Figure 2.4. The four points of the quadrangle $\mathcal{K}$ are labelled A, B, C and D, while the points on l_∞ are labelled P, Q, R, and S. Then two of the points, P, Q, lie on critical secants AC and BD, while the remaining points R, S lie on two secants each. It is not clear, however, if the upper bound is reached at all for larger q.

In the next chapter we discuss n-regular k-covers, including 1-regular k-covers, which are precisely those for which k reaches the lower bound of Theorem 2.1.2.

Figure 2.4: An irreducible 4-cover in Π_3.



Chapter 3

Regular k-covers

This chapter discusses n-regular k-covers. Section 3.1 examines in detail the cases where the lower bound on k-covers is met. These are the 1-regular k-covers. In Section 3.2 we consider the generalisation of 1-regular k-covers to n-regular k-covers and characterise the k-covers when n is maximum. Section 3.3 introduces (n_1, n_2)-regular k-covers, and Section 3.4 discusses other related work.

3.1 1-regular k-covers

From Theorem 2.1.2, if $\mathcal{K}$ is a k-arc covering a line in Π_q, then $k \geq (1+\sqrt{8q+9})/2$. In this section we determine when this bound is met if q is a prime power.

Lemma 3.1.1 Let q be a prime power, that is, $q = p^h$, where p a prime and $h \geq 1$. If $8q + 9$ is a square then $q \in \{2, 5, 9, 27\}$.

Proof: Suppose $8q + 9$ is a square, that is, $8q + 9 = x^2$ for some positive integer x. Since $q = p^h$, we have

$$8p^h = x^2 - 9,$$

that is,

$$2^3 p^h = (x-3)(x+3).$$

Hence we have

$$x - 3 = 2^{n_1} p^{h_1} \tag{3.1}$$

$$x + 3 = 2^{n_2} p^{h_2} \tag{3.2}$$

with $n_1 + n_2 = 3$, $h_1 + h_2 = h$, where n_1, n_2, h_1, h_2 are non-negative integers. Subtracting equation (3.1) from equation (3.2) we have

$$2^{n_2} p^{h_2} - 2^{n_1} p^{h_1} = 2 \cdot 3. \tag{3.3}$$

The only possible values for n_1 and n_2 are $(n_1, n_2) \in \{(0,3), (1,2), (2,1), (3,0)\}$. We consider equation (3.3) for all four possible values of (n_1, n_2):

(a) $(n_1, n_2) = (0, 3)$: Equation (3.3) becomes $2^3 p^{h_2} - p^{h_1} = 2 \cdot 3$.

(i) If $h_1 \geq h_2$ then $p^{h_2}(8 - p^{h_1 - h_2}) = 2 \cdot 3$ and so $p^{h_2} = 1$, 2 or 3.

If $p^{h_2} = 1$ then we must have $h_2 = 0$ and $8 - p^{h_1} = 6$. Hence $p = 2$, $h_1 = 1$ and so $q = 2$.

If $p^{h_2} = 2$ then we have $p = 2$ and $h_2 = 1$. Hence $8 - 2^{h_1 - 1} = 3$, which has no solution for h_1.

If $p^{h_2} = 3$ then $p = 3$ and $h_2 = 1$. Hence $8 - 3^{h_1 - 1} = 2$, which also has no solution for h_1.

(ii) If $h_1 < h_2$ then $p^{h_1}(8p^{h_2 - h_1} - 1) = 2 \cdot 3$. Since $8p^{h_2 - h_1} - 1 > 2 \cdot 3$ if $h_2 > h_1$, there is no solution in this case.

Hence in this case the only possible value for q is $q = 2$.

(b) $(n_1, n_2) = (1, 2)$: Equation (3.3) becomes $2^2 p^{h_2} - 2p^{h_1} = 2 \cdot 3$, that is, $2p^{h_2} - p^{h_1} = 3$.

(i) If $h_1 \geq h_2$ then $p^{h_2}(2 - p^{h_1 - h_2}) = 3$, and so $p^{h_2} = 1$ or 3.

If $p^{h_2} = 1$ then $h_2 = 0$ and $2 - p^{h_1} = 3$. This means that $p^{h_1} = -1$, and so there is no solution for h_1 in this case.

If $p^{h_2} = 3$ then $p = 3$ and $h_2 = 1$. This means that we have $3^{h_1 - 1} = 1$ and so $h_1 = 1$. Hence $q = 3^2$.

(ii) If $h_1 < h_2$ then $p^{h_1}(2p^{h_2 - h_1} - 1) = 3$, and so $p^{h_1} = 1$ or 3.

If $p^{h_1} = 1$ then $h_1 = 0$ and $2p^{h_2} - 1 = 3$. Hence we must have $p^{h_2} = 2$ and so $q = 2$.

If $p^{h_1} = 3$ then $h_1 = 1$ and $p = 3$. Hence $2 \cdot 3^{h_2 - 1} = 2$, so $h_2 = 1$, and so $q = 3^2$.

Hence in this case the only possible values for q are $q = 2$ and 9.

(c) $(n_1, n_2) = (2, 1)$: Equation (3.3) becomes $2p^{h_2} - 2^2 p^{h_1} = 2 \cdot 3$, that is, $p^{h_2} - 2p^{h_1} = 3$.

(i) If $h_1 \geq h_2$ then $p^{h_2}(1 - 2p^{h_1 - h_2}) = 3$. Since $1 - 2p^{h_1 - h_2} < 0$ if $h_1 \geq h_2$, there is no solution in this case.

(ii) If $h_1 < h_2$ then $p^{h_1}(p^{h_2 - h_1} - 2) = 3$, and so $p^{h_1} = 1$ or 3.

If $p^{h_1} = 1$ then $h_1 = 0$ and $p^{h_2} - 2 = 3$. Hence $q = 5$.

If $p^{h_1} = 3$ then $h_1 = 1$ and $p = 3$. Hence $3^{h_2 - 1} = 3$ and so $q = 3^3$.

Hence the only possible values of q in this case are $q = 5$ and 27.

(d) $(n_1, n_2) = (3, 0)$: Equation (3.3) becomes $p^{h_2} - 2^3 p^{h_1} = 2 \cdot 3$.

(i) If $h_1 \geq h_2$ then $p^{h_2}(1 - 8p^{h_1 - h_2}) = 2 \cdot 3$. Since $1 - 8p^{h_1 - h_2} < 0$ if $h_1 \geq h_2$, there is no solution in this case.

(ii) If $h_1 < h_2$ then $p^{h_1}(p^{h_2 - h_1} - 8) = 2 \cdot 3$, so $p^{h_1} = 1$, 2 or 3.

If $p^{h_1} = 1$ then $p^{h_2} - 8 = 6$ so there is no solution in this case.

If $p^{h_1} = 2$ then $h_1 = 1$, $p = 2$ and $2^{h_2 - 1} - 8 = 3$, so there is no solution for h_2.

If $p^{h_1} = 3$ then $h_1 = 1$, $p = 3$ and $3^{h_2 - 1} - 8 = 2$, so there is also no solution for h_2 in this case.

Hence in this case there is no solution for q.

Thus we conclude that 2, 5, 9 and 27 are the only possible values of q for which q is a prime power and $8q + 9$ is a square. □

Since the 1-regular k-covers are precisely those with $k = (1 + \sqrt{8q + 9})/2$, we have the following corollary:

Corollary 3.1.2 If $\mathcal{K}$ is a 1-regular k-cover in a projective plane of prime power order q, then $\mathcal{K}$ must be one of the following:

(a) $q = 2$ and $\mathcal{K}$ is a 3-arc;

(b) $q = 5$ and $\mathcal{K}$ is a 4-arc;

(c) $q = 9$ and $\mathcal{K}$ is a 5-arc;

(d) $q = 27$ and $\mathcal{K}$ is an 8-arc.

In the rest of this section we investigate the existence of 1-regular k-covers in each of the four cases of Corollary 3.1.2. For the first two cases we have the following result:

Theorem 3.1.3 There exists a 1-regular 3-cover in $PG(2,2)$ and a 1-regular 4-cover in $PG(2,5)$.

Proof: Let l_∞ be any line in $PG(2,2)$. Then any triangle not on l_∞ is a 3-arc in $PG(2,2)$ which covers l_∞. Since a triangle has 3 secants and covers the 3 points on l_∞, it is 1-regular.

In $PG(2,5)$, Construction 2.3.3 gives a 4-cover $\mathcal{K}$ for any line l_∞ with $s = 3$, that is, $\mathcal{K}$ lies on a conic $\mathcal{C}$ disjoint from l_∞, where $\mathcal{C}$ is partitioned into two sharply focused sets of 3 points each, and $\mathcal{K}$ consists of the points of one of the sharply focused sets together with one point from the other. Since $\mathcal{K}$ has 6 secants and covers the 6 points on l_∞, it must be 1-regular. □

Theorem 3.1.4 There is no 1-regular 5-cover in $PG(2,9)$.

Proof: Let l_∞ be any line in $PG(2,9)$. Suppose $\mathcal{K}$ is a 1-regular 5-arc covering l_∞ in $PG(2,9)$. Then $\mathcal{K}$ lies on a conic $\mathcal{C}$ disjoint from l_∞, for every 5-arc lies on a conic in $PG(2,q)$, and if $\mathcal{C}$ is not disjoint from l_∞ then the points of $l_\infty \cap \mathcal{C}$ will not be covered by any secants of $\mathcal{C} \setminus l_\infty$. Now, the ten points on $\mathcal{C}$ can be partitioned into two sharply focused sets, both focusing on the external points of l_∞ (Result 1.2.3). Hence the only possible distribution of the points of $\mathcal{K}$ on $\mathcal{C}$ are

(1) $\mathcal{K}$ is one of the sharply focused sets;

(2) four points of $\mathcal{K}$ belong to one of the sharply focused set and one belongs to the other;

(3) three points of $\mathcal{K}$ belong to one of the sharply focused set and two belong to the other.

The first case cannot occur, since $\mathcal{K}$ would then cover only the five external points of l_∞. In the second case, there are six secants to the four points of $\mathcal{K}$ in one sharply focused set, and these six secants meet l_∞ in only the five external points. Hence at least one of the external points on l_∞ lie on more than one secant and so $\mathcal{K}$ cannot be 1-regular. In the last case, let P_1, P_2 P_3 denote the three points belonging to one of the sharply focused set and Q_1, Q_2 denote the two points belonging to the other. Then the secants P_1P_2, P_1P_3, P_2P_3 and Q_1Q_2 meet l_∞ in the external points. The remaining six secants are of the form P_iQ_j and they meet l_∞ in internal points (Result 1.2.2(b)), so at least one of the external points on l_∞ is not covered by $\mathcal{K}$. Hence if $\mathcal{K}$ is a 1-regular 5-cover of l_∞ then it does not lie on a conic. This contradicts the fact that every 5-arc lies on a conic. Hence we conclude that there is no 1-regular 5-cover in $PG(2,9)$. □

There are four non-isomorphic projective planes of order 9: the Desarguesian plane $PG(2,9)$, the Hall plane, its dual, and the Hughes plane. Even though there is no 1-regular 5-cover in $PG(2,9)$ by the above result, it is possible that such a 5-cover exists in one of the other planes. The next result is obtained using a computer search:

Theorem 3.1.5 There exists a 1-regular 5-arc covering the translation line in the Hall plane of order 9. There exists also 1-regular 5-arcs covering any affine line.

Proof: The Hall plane $\mathcal{H}$ of order 9 is obtained from $PG(2,9)$ by derivation (see Section 1.3). Let $PG(2,9)$ be coordinatised by the Galois field of order 9,

$$GF(9) = \left\{ 0, \alpha^n \mid n = 0, \ldots, 7,\ \alpha^2 - \alpha - 1 = 0 \right\},$$

where α is a primitive element of $GF(9)$. Let l_∞ be the line $z = 0$ and let the derivation set $\mathcal{D}$ be the Baer subline $\{(1, x, 0) \mid x \in GF(3)\} \cup \{(0, 1, 0)\}$. This is the standard derivation set. Then the points and lines of $\mathcal{H}$ may be represented as follows ([17, Chapter X]):

- The affine points of $\mathcal{H}$ are the points of $PG(2,9) \setminus l_\infty$, that is, points of the form $(x, y, 1)$, x,$y \in GF(9)$.

- The affine lines of $\mathcal{H}$ are of two types. The lines of $\mathcal{H}$ which are lines of $PG(2,9)$ meeting l_∞ in a point not in $\mathcal{D}$ are of the form $y = mx + c$, where $m \in GF(9) \setminus GF(3)$, $c \in GF(9)$. For each $m \in GF(9) \setminus GF(3)$, the set of lines $\{y = mx + c \mid c \in GF(9)\}$ forms a parallel class.

  The lines of $\mathcal{H}$ which are the Baer subplanes of $PG(2,9)$ belonging to $\mathcal{D}$ are the sets $\mathcal{R}(a,b,c) = \{(ua+b, va+c, 1) \mid u, v \in GF(3)\}$, where a, b, $c \in GF(9)$, $a \neq 0$. Now, $\mathcal{R}(a_1,b_1,c_1)$ and $\mathcal{R}(a_2,b_2,c_2)$ are disjoint or coincident if and only if $a_2/a_1 \in GF(3)$, and are coincident if and only if $a_2/a_1 \in GF(3)$, $(b_2-b_1)/a_1 \in GF(3)$ and $(c_2-c_1)/a_1 \in GF(3)$. So the 36 distinct affine lines of $\mathcal{H}$ of this form are $\mathcal{R}(a,b,c)$, $a \in \{1, \alpha, \alpha^2, \alpha^3\}$ and b, $c \in \{0, \alpha a, -\alpha a\}$. For each $a \in \{1, \alpha, \alpha^2, \alpha^3\}$, the set of lines $\{\mathcal{R}(a,b,c) \mid b, c \in \{0, \alpha a, -\alpha a\}\}$ forms a parallel class.

- The ideal points of $\mathcal{H}$ are $(1,m,0)$, $m \in GF(9) \setminus GF(3)$, and $\mathcal{R}(a)$, $a \in \{1, \alpha, \alpha^2, \alpha^3\}$. The ideal point $(1,m,0)$ corresponds to the parallel class of lines $\{y = mx + c \mid c \in GF(9)\}$, while the ideal point $\mathcal{R}(a)$ corresponds to the parallel class of lines $\{\mathcal{R}(a,b,c) \mid b, c \in \{0, \alpha a, -\alpha a\}\}$.

- The ideal line (translation line) of $\mathcal{H}$ is the set of ideal points.

Using the above representation, a computer search was performed and the following 1-regular 5-covers were found:

The translation line is covered by the 5-arc $\mathcal{K}_1$:

$$\mathcal{K}_1 = \left\{A(0,0,1), B(0,1,1), C(-1,-\alpha,1), D(-1,\alpha,1), E(\alpha^3,\alpha,1)\right\}.$$

It is straight forward to verify that the line AB meets the translation line in $\mathcal{R}(1)$, AC meets it in $(1,\alpha,0)$, AD in $(1,-\alpha,0)$, AE in $(1,-\alpha^2,0)$, BC in $(1,\alpha^2,0)$, BD in $(1,\alpha^3,0)$, BE in $\mathcal{R}(\alpha^3)$, CD in $\mathcal{R}(\alpha)$, CE in $(1,-\alpha^3,0)$ and DE in $\mathcal{R}(\alpha^2)$.

The affine line $y = \alpha x$ is covered by the 5-arc $\mathcal{K}_2$:

$$\mathcal{K}_2 = \left\{A(1,0,1), B(0,1,1), C(-1,\alpha,1), D(-1,-\alpha^2,1), E(1,\alpha^3,1)\right\}.$$

The line AB meets the line $y = \alpha x$ in $(0,0,1)$, AC meets it in $(1,\alpha,0)$, AD in $(-\alpha^3,1,1)$, AE in $(-\alpha^2,-\alpha^3,1)$, BC in $(\alpha^2,\alpha^3,1)$, BD in $(1,\alpha,1)$, BE in

$(\alpha^3, -1, 1)$, CD in $(-\alpha, -\alpha^2, 1)$, CE in $(\alpha, \alpha^2, 1)$ and DE in $(-1, -\alpha, 1)$. Since the automorphism group of $\mathcal{H}$ is transitive on the affine lines of $\mathcal{H}$, there is a 1-regular 5-cover for every affine line in $\mathcal{H}$. □

Corollary 3.1.6 Let Π_9 be a translation plane of order 9 and let l_∞ be a translation line of Π_9. Then there exists a 1-regular 5-arc covering l_∞ if and only if Π_9 is the Hall plane of order 9. □

Since there is no 1-regular 5-cover in $PG(2,9)$, a 1-regular 5-cover in $\mathcal{H}$ must either not derive to an arc in $PG(2,9)$, or derive to a 5-arc in $PG(2,9)$ which is not a 1-regular cover. The example of a 5-cover for the translation line in Theorem 3.1.5 is a 5-arc in $PG(2,9)$ contained in the conic $\alpha x^2 + y^2 - yz + \alpha^3 xz - xy = 0$ but is not a 5-cover in $PG(2,9)$. We consider 5-covers for the translation line in $\mathcal{H}$ which do not derive to arcs in $PG(2,9)$.

Theorem 3.1.7 Let $\mathcal{K}$ be a 1-regular 5-cover for the translation line l_∞ in $\mathcal{H}$ which does not derive to a 5-arc in $PG(2,9)$. Let $\mathcal{K} = \{A, B, C, D, E\}$ and let $\mathcal{D}$ be a derivation set. Then $\mathcal{K}$ must derive to one of the following configurations:

(i) The points A, B, C are collinear and both AB and DE meet l_∞ in $X \in \mathcal{D}$. See Figure 3.1(i).

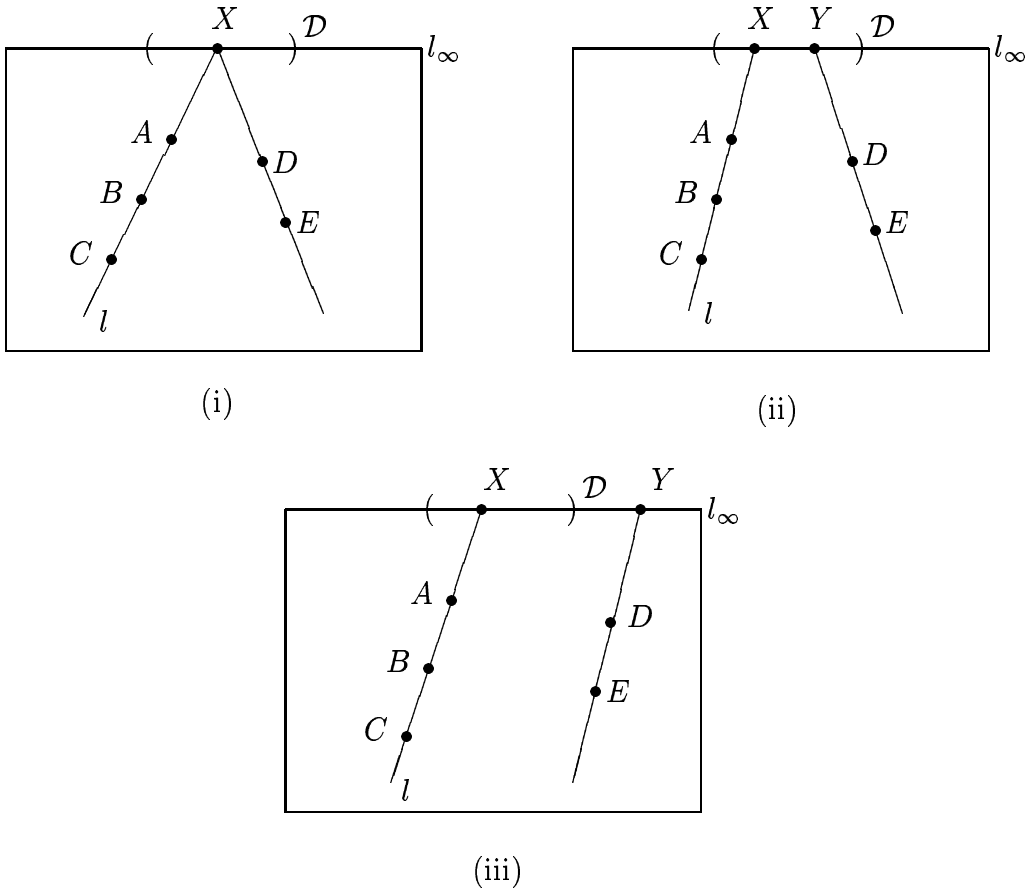
(ii) The points A, B, C are collinear and AB meets l_∞ in the point X which lies in $\mathcal{D}$. The line DE meets l_∞ in $Y \in \mathcal{D}$, $Y \neq X$. See Figure 3.1(ii).

(iii) The points A, B, C are collinear and AB meets l_∞ in $X \in \mathcal{D}$, and the line DE meets l_∞ in $Y \notin \mathcal{D}$. See Figure 3.1(iii).

In the first two configurations of $\mathcal{K}$, AB, AC, BC, DE cover the ideal points $\mathcal{R}(1)$, $\mathcal{R}(\alpha)$, $\mathcal{R}(\alpha^2)$, $\mathcal{R}(\alpha^3)$, and DA, DB, DC, EA, EB, EC cover the remaining ideal points in $l_\infty \setminus \mathcal{D}$. In the last case, AB, AC, BC cover three of the four ideal points $\mathcal{R}(a)$, $a \in \{1, \alpha, \alpha^2, \alpha^3\}$, and one of DA, DB, DC, EA, EB, EC covers the remaining one, while the remainder, with DE, covers $l_\infty \setminus \mathcal{D}$.

Proof: We identify the affine points of $\mathcal{H}$ with the points of $PG(2,9)$ and specify "line of $PG(2,9)$" or "line of $\mathcal{H}$" as the case arises.

Figure 3.1: Possible configurations deriving to 5-covers in $\mathcal{H}$.



Since $\mathcal{K}$ does not derive to a 5-arc in $PG(2,9)$, at least three points of $\mathcal{K}$ must be collinear in $PG(2,9)$. Let l be the line in $PG(2,9)$ containing at least 3 points of $\mathcal{K}$. Then l must meet l_∞ in $\mathcal{D}$, for otherwise l would be a line of $\mathcal{H}$ and $\mathcal{K}$ would not be an arc in $\mathcal{H}$. We show that there are exactly 3 points of $\mathcal{K}$ on l.

Suppose all 5 points of $\mathcal{K}$ lie on l, then all the secants of $\mathcal{K}$ are lines of $\mathcal{H}$ corresponding to Baer subplanes in $PG(2,9)$, and the points on $l_\infty \setminus \mathcal{D}$ are not covered at all. This contradicts the assumption that $\mathcal{K}$ is a 5-cover in $\mathcal{H}$. Suppose then that l contains 4 points, say A, B, C and D, of $\mathcal{K}$. Then there are at most 4 secants AE, BE, CE, DE covering points on $l_\infty \setminus \mathcal{D}$, but $l_\infty \setminus \mathcal{D}$ has 6 points, so $\mathcal{K}$ is not a 5-cover in $\mathcal{H}$. Hence l must have exactly 3 points, say A, B, C of $\mathcal{K}$.

Since l meets l_∞ in $\mathcal{D}$, the secants AB, AC, BC are lines of $\mathcal{H}$ corresponding to Baer subplanes in $PG(2,9)$, and since $\mathcal{K}$ is 1-regular, they must cover three of the four ideal points $\mathcal{R}(a)$, $a \in \{1, \alpha, \alpha^2, \alpha^3\}$. The line joining the remaining two points D, E meets l_∞ either in $l \cap l_\infty$, $\mathcal{D} \setminus \{l \cap l_\infty\}$ or $l_\infty \setminus \mathcal{D}$, corresponding to cases (i), (ii) or (iii) respectively. The properties of the secants follow from the assumption that $\mathcal{K}$ is a 1-regular 5-cover for l_∞ in $\mathcal{H}$. □

The next two results show that the first two configurations do not exist.

Theorem 3.1.8 There is no configuration in $PG(2,9)$ satisfying case (i) of Theorem 3.1.7.

Proof: Let l_∞ be the line $z = 0$ in $PG(2,9)$ and $\mathcal{D}$ the standard derivation set. The collineation group G of $PG(2,9)$ fixing $\mathcal{D}$ is 2-transitive on the points of $\mathcal{D}$, so we may pick X to be the point $(1,0,0)$. The subgroup of G fixing X is transitive on affine points, hence we may pick the point A to be $(0,0,1)$. This determines the line l to be the line $y = 0$. The subgroup of G fixing both X and A is transitive on $l \setminus \{A, X\}$, so we may pick B to be $(1,0,1)$. Let G' be the subgroup of G fixing X, A and B. Then the set of affine lines $y + tz = 0$ through X, $t \in \{\pm 1, \pm\alpha, \pm\alpha^2, \pm\alpha^3\}$, is partitioned into 4 orbits $\{y \pm tz = 0\}$, $t = 1, \alpha, \alpha^2, \alpha^3$, under G', so we need only to consider the points D, E on $y + tz = 0$ for $t = 1, \alpha, \alpha^2, \alpha^3$.

Let C be $(c,0,1)$. Then $c \notin GF(3)$, since C can't lie in the same Baer subplane as A and B. The points D, E lie on $y+tz = 0$ for some t. Let D be $(d,-t,1)$, E $(e,-t,1)$. We show that there is no c, d, e and t such that $\mathcal{K} = \{A, B, C, D, E\}$ satisfies case (i) of Theorem 3.1.7. Now, for any fixed $t \in \{1, \alpha, \alpha^2, \alpha^3\}$ and $c \in GF(9) \setminus GF(3)$, we have:

(a) The points A, B lie in $\mathcal{R}(1,0,0)$, so AB covers $\mathcal{R}(1)$ in $\mathcal{H}$. The points A, C lie in $\mathcal{R}(c,0,0)$, so AC covers $\mathcal{R}(c)$ in $\mathcal{H}$.

(b) The points B, C lie in $\mathcal{R}(c-1, \alpha(c-1), 0)$ if $c \in \{\alpha, -\alpha, \alpha^2\}$ and $\mathcal{R}(c-1, -\alpha(c-1), 0)$ if $c \in \{-\alpha^2, \alpha^3, -\alpha^3\}$, so BC covers $\mathcal{R}(c-1)$ in $\mathcal{H}$. This can be verified as follows:

Let

$$L(c) = \{(u(c-1) + \alpha(c-1), 0, 1) \mid u \in GF(3)\}$$

and

$$L'(c) = \{(u(c-1) - \alpha(c-1), 0, 1) \mid u \in GF(3)\}.$$

Then $L(c)$ is a subset of $\mathcal{R}(c-1, \alpha(c-1), 0)$, while $L'(c)$ is a subset of $\mathcal{R}(c-1, -\alpha(c-1), 0)$.

For $c \in \{\alpha, -\alpha, \alpha^2\}$, if $c = \alpha$ then $L(c) = \{(1,0,1), (\alpha,0,1), (-\alpha^2,0,1)\}$, if $c = -\alpha$ then $L(c) = \{(-\alpha^3,0,1), (1,0,1), (-\alpha,0,1)\}$, and if $c = \alpha^2$ then $L(c) = \{(\alpha^2,0,1), (\alpha^3,0,1), (1,0,1)\}$, so in all three cases, B, C lie in $L(c)$. Hence, if $c \in \{\alpha, -\alpha, \alpha^2\}$, the points B, C lie in $\mathcal{R}(c-1, \alpha(c-1), 0)$.

For $c \in \{-\alpha^2, \alpha^3, -\alpha^3\}$, if $c = -\alpha^2$ then $L'(c) = \{(1,0,1), (-\alpha^2,0,1), (\alpha,0,1)\}$, if $c = \alpha^3$ then $L'(c) = \{(\alpha^2,0,1), (1,0,1), (\alpha^3,0,1)\}$, if $c = -\alpha^3$ then $L'(c) = \{(-\alpha^3,0,1), (-\alpha,0,1), (1,0,1)\}$, so in all three cases, B, $C \in L'(c)$. Hence for $c \in \{-\alpha^2, \alpha^3, -\alpha^3\}$, B, C lie in $\mathcal{R}(c-1, -\alpha(c-1), 0)$.

(c) The line AD meets l_∞ in $(-dt^{-1}, 1, 0)$ and AE meets l_∞ in $(-et^{-1}, 1, 0)$. Since both these points must lie in $l_\infty \setminus \mathcal{D}$, we have $d, e \neq 0, \pm t$.

Similarly, BD covers $((1-d)t^{-1}, 1, 0)$ and BE covers $((1-e)t^{-1}, 1, 0)$ and both the points must lie in $l_\infty \setminus \mathcal{D}$, so $d, e \neq 1, 1 \pm t$.

Furthermore, for any c, the line CD covers $((c-d)t^{-1}, 1, 0)$, while CE covers $((c-e)t^{-1}, 1, 0)$, so $d, e \neq c, c \pm t$.

Let N be the set $\{0, 1, c, \pm t, 1 \pm t, c \pm t\}$. Then, if $\mathcal{K}$ satisfies case (i) of Theorem 3.1.7, there must be $d, e \in GF(9) \setminus N$ for some $t \in \{1, \alpha, \alpha^2, \alpha^3\}$ and $c \in GF(9) \setminus GF(3)$.

By considering all possible values of t and c, we show that either $N = GF(9)$, which means that there is no d, e such that $\mathcal{K}$ forms the configuration of Theorem 3.1.7(i), or for all valid choices of d, e, the point D, E cover $\mathcal{R}(t)$.

For $t = 1$, if $c \in \{\alpha, -\alpha^2, \alpha^3\}$, the only possible values of d and e are $\{-\alpha, -\alpha^2, \alpha^3\}$ and for all these values, D and E lie in $\mathcal{R}(1, -\alpha, 0)$. If $c \in \{-\alpha, \alpha^2, -\alpha^3\}$, the only possible values of d and e are $\{\alpha, \alpha^2, -\alpha^3\}$ and for all these values, D and E lie in $\mathcal{R}(1, \alpha, 0)$. Hence in all cases, DE covers $\mathcal{R}(t)$.

For $t = \alpha$, if $c \in \{-\alpha^2, -\alpha^3\}$, then $N = GF(9)$, so there is no d, e such that $\mathcal{K}$ satisfies case (i) of Theorem 3.1.7. If $c \in \{\alpha, -\alpha, \alpha^2, \alpha^3\}$, then the only possible

values for d and e are $\{-1, -\alpha^2, -\alpha^3\}$ and for these values, both D and E lie in $\mathcal{R}(\alpha, -\alpha^2, 0)$. Hence DE covers $\mathcal{R}(t)$.

Similarly, for $t = \alpha^2$, if $c \in \{\alpha, \alpha^3\}$ then $N = GF(9)$, while for the remaining values of c, the only possible values for d and e are $\{-1, \alpha, \alpha^3\}$, and for these values, both D and E lie in $\mathcal{R}(\alpha^2, \alpha^3, 0)$. So DE covers $\mathcal{R}(t)$.

Lastly, for $t = \alpha^3$, if $c \in \{-\alpha, \alpha^2\}$ then $N = GF(9)$, while for the remaining values of c, the only possible values for d and e are $\{-1, -\alpha, \alpha^2\}$, and for these values, both D and E lie in $\mathcal{R}(\alpha^3, -1, 0)$. So DE covers $\mathcal{R}(t)$.

Consider the values of t and c where DE covers $\mathcal{R}(t)$. Since AB, AC, BC cover $\mathcal{R}(1)$, $\mathcal{R}(c)$, $\mathcal{R}(c-1)$ respectively, we must have $t = c + 1$. In this case, however,

$$N = \{0, \pm 1, \pm c, \pm(c+1), \pm(c-1)\} = GF(9).$$

So for all values of t and c, there is no d, e such that $\mathcal{K}$ satisfies case (i) of Theorem 3.1.7. □

Similarly, we show that

Theorem 3.1.9 There is no configuration in $PG(2, 9)$ satisfying case (ii) of Theorem 3.1.7.

Proof: By the same argument as the proof of the previous result, we choose $A(0, 0, 1)$, $B(1, 0, 1)$, $X(1, 0, 0)$ and $Y(0, 1, 0)$. Let C be $(c, 0, 1)$, then since C cannot lie in the same Baer subplane as A and B, $c \in \{\pm\alpha, \pm\alpha^2, \pm\alpha^3\}$. Let D, E be on the line $x + tz = 0$, $t \in GF(9)$, $D = (-t, d, 1)$, $E = (-t, e, 1)$, $d, e \neq 0$.

(a) As in the proof of the previous result, AB covers $\mathcal{R}(1)$, AC covers $\mathcal{R}(c)$ and BC covers $\mathcal{R}(c-1)$ in $\mathcal{H}$.

(b) If $t = 0$, -1 or $-c$, then AD, BD, or CD respectively meets l_∞ in Y. Since we require that AD, BD and CD cover points of $l_\infty \setminus \mathcal{D}$, we must have $t \notin \{0, -1, -c\}$, so $t \in \{1, c, \pm(c+1), \pm(c-1)\}$.

(c) The lines AD, AE, BD, BE, CD and CE cover $(-td^{-1}, 1, 0)$, $(-te^{-1}, 1, 0)$, $(-(1+t)d^{-1}, 1, 0)$, $(-(1+t)e^{-1}, 1, 0)$, $(-(c+t)d^{-1}, 1, 0)$ and $(-(c+t)e^{-1}, 1, 0)$

respectively, and since we require that all these points lie in $l_\infty \setminus \mathcal{D}$, we must have

$$d, e \notin \{0, \pm t, \pm(1+t), \pm(c+t)\} = N.$$

Hence we have, if $\mathcal{K}$ satisfies case (ii) of Theorem 3.1.7,

$$\begin{aligned}
t = 1 &\Rightarrow d, e \in \{c, -c, c-1, -c+1\}, \\
t = c &\Rightarrow d, e \in \{1, -1, c-1, -c+1\}, \\
t = c+1 &\Rightarrow d, e \in \{1, -1, c, -c\}, \\
t = c-1 &\Rightarrow d, e \in \{1, -1\}, \\
t = -c+1 &\Rightarrow d, e \in \{c, -c\}, \\
t = -c-1 &\Rightarrow d, e \in \{c-1, -c+1\}.
\end{aligned}$$

Let $e = -d$, that is, D is the point $(-t, d, 1)$ and E the point $(-t, -d, 1)$. We show that DE covers $\mathcal{R}(d)$. Now, there is a Baer subplane $\mathcal{R}(d, x, 0)$, $x \in \{0, \alpha d, -\alpha d\}$, containing both D and E if and only if there are elements u, v_1, v_2 of $GF(3)$ such that

$$\begin{aligned}
ud + x &= -t, \\
v_1 d &= d, \\
v_2 d &= -d.
\end{aligned}$$

Now, $v_1 = 1$, $v_2 = -1$ are certainly solutions for the last two equations. As for the first equation, the following addition table show that, for any $t \in GF(9)$, there is always a u in $GF(3)$ and an x in $\{0, \alpha d, -\alpha d\}$ such that $ud + x = -t$:

		x		
	$+$	0	αd	$-\alpha d$
	0	0	αd	$-\alpha d$
ud	d	d	$(\alpha+1)d$	$(-\alpha+1)d$
	$-d$	$-d$	$(\alpha-1)d$	$(-\alpha-1)d$

Since all the entries of the table are distinct for $d \neq 0$, we conclude that there is always a Baer subplane $\mathcal{R}(d, x, 0)$, $x \in \{0, \alpha d, -\alpha d\}$, containing D and E. Hence if $e = -d$ then DE covers $\mathcal{R}(d)$. So, in the last three cases, where $t = c-1$, $-c+1$,

$-c-1$, DE covers $\mathcal{R}(1)$, $\mathcal{R}(c)$ and $\mathcal{R}(c-1)$ respectively. However, $\mathcal{R}(1)$, $\mathcal{R}(c)$ and $\mathcal{R}(c-1)$ are already covered by AB,AC and BC, so the only valid choices for t are 1, c and $c+1$.

If $\mathcal{K}$ satisfies case (ii) of Theorem 3.1.7, then, from (a) and (c), we must have, for some c, d, e and t, DE covers $\mathcal{R}(c+1)$, and

$$\{-td^{-1}, -te^{-1}, -(1+t)d^{-1}, -(1+t)e^{-1}, -(c+t)d^{-1}, -(c+t)e^{-1}\} = GF(9)\backslash GF(3).$$

By trying all valid values of t, d and e for each choice of c, we conclude that there is no c, d,e and t such that $\mathcal{K}$ satisfies case (ii) of Theorem 3.1.7. □

By performing a computer search, we have the following result:

Theorem 3.1.10 There is a 1-regular 5-cover in the Hall plane of order 9 which derives to the configuration in Result 3.1.7 (iii).

Proof: Let A be the point $(0,0,1)$, B $(1,0,1)$, C $(\alpha,0,1)$, D $(0,\alpha^2,1)$ and E $(\alpha^2,\alpha^3,1)$. Then AB covers $\mathcal{R}(1)$, AC covers $\mathcal{R}(\alpha)$, AD covers $\mathcal{R}(\alpha^2)$, AE covers $(-\alpha^3,1,0)$, BC covers $\mathcal{R}(\alpha^3)$, BD covers $(\alpha^2,1,0)$, BE covers $(-\alpha^2,1,0)$, CD covers $(\alpha^3,1,0)$, CE covers $(-\alpha,1,0)$ and DE covers $(\alpha,1,0)$. □

By fixing A and B, an exhaustive computer search found 384 distinct 5-covers containing A, B, three quarters of which derive to 5-arcs in $PG(2,9)$ and the rest derive to the configuration in Theorem 3.1.7 (iii). Since there are $\begin{pmatrix} 9^2 \\ 2 \end{pmatrix} = 3240$ choices of A, B, and each 5-cover is counted $\begin{pmatrix} 5 \\ 2 \end{pmatrix} = 10$ times, there are altogether

$$\frac{3240 \times 384}{10} = 124416$$

1-regular 5-covers in the Hall plane of order 9.

For completeness, we investigate the existence of 1-regular 5-covers in the two other planes of order 9, the dual Hall plane and the Hughes plane.

Theorem 3.1.11 There exists a 1-regular 5-cover for each line in the dual Hall plane of order 9.

Proof: The dual of a 1-regular 5-arc covering a fixed line is a set of five lines no three concurrent such that the intersection of every pair of lines lies on distinct lines through a fix point. There is a 1-regular 5-cover in the dual Hall plane of order 9 if and only if the dual exists in the Hall plane of order 9.

Using the same representation as in Theorem 3.1.5, we perform a computer search and obtain the following result:

Let $P(0,0,1)$ be a fixed affine point in the Hall plane $\mathcal{H}$. Then P corresponds to a line not through the translation point in the dual Hall plane. The lines of $\mathcal{H}$ through P are $\mathcal{R}(1,0,0)$, $\mathcal{R}(\alpha,0,0)$, $\mathcal{R}(\alpha^2,0,0)$, $\mathcal{R}(\alpha^3,0,0)$, $y=\alpha x$, $y=-\alpha x$, $y=\alpha^2 x$, $y=-\alpha^2 x$, $y=\alpha^3 x$, $y=-\alpha^3 x$. Let $\mathcal{K}'$ be the set of 5 lines of $\mathcal{H}$ consisting of:

$$\begin{aligned} l_1 &: \text{ the translation line,} \\ l_2 &: y=\alpha x+1, \\ l_3 &: y=-\alpha x-1, \\ l_4 &: y=-\alpha^2 x-1, \\ l_5 &: y=-\alpha^3 x-\alpha \end{aligned}$$

Then we have the following incidence:

$$\begin{aligned} l_1\cap l_2 &= (1,\alpha,0)\in y=\alpha x, \\ l_1\cap l_3 &= (1,-\alpha,0)\in y=-\alpha x, \\ l_1\cap l_4 &= (1,-\alpha^2,0)\in y=-\alpha^2 x, \\ l_1\cap l_5 &= (1,-\alpha^3,0)\in y=-\alpha^3 x, \\ l_2\cap l_3 &= (\alpha^3,0,1)\in \mathcal{R}(\alpha^3,0,0), \\ l_2\cap l_4 &= (-\alpha,-\alpha,1)\in \mathcal{R}(\alpha,0,0), \\ l_2\cap l_5 &= (-\alpha^2,\alpha,1)\in y=\alpha^3 x, \\ l_3\cap l_4 &= (0,-1,1)\in \mathcal{R}(1,0,0), \\ l_3\cap l_5 &= (\alpha,\alpha^3,1)\in y=\alpha^2 x, \\ l_4\cap l_5 &= (\alpha^2,0,1)\in \mathcal{R}(\alpha^2,0,0). \end{aligned}$$

Hence $\{l_1,l_2,l_3,l_4,l_5\}$ forms a dual 1-regular 5-cover for the point $(1,0,0)$ in the Hall plane, so there exists a 1-regular 5-arc covering a line not through the translation

point in the dual Hall plane of order 9.

Similarly, the lines of $\mathcal{H}$ $\{l'_1, l'_2, l'_3, l'_4, l'_5\}$ with

$$\begin{aligned} l'_1 &: \mathcal{R}(1,0,0), \\ l'_2 &: \mathcal{R}(\alpha,0,0), \\ l'_3 &: y = -\alpha x - 1, \\ l'_4 &: y = -\alpha x + 1, \\ l'_5 &: \mathcal{R}(\alpha^3,1,0), \end{aligned}$$

form a dual 1-regular 5-cover for the point $(1, \alpha, 0)$ which corresponds to a line through the translation point in the dual plane. Hence there is a 1-regular 5-arc covering any line in the dual Hall plane of order 9. □

Theorem 3.1.12 There is a 1-regular 5-arc covering a complex line and a 1-regular 5-arc covering a real line in the Hughes plane of order 9.

Proof: We represent the Hughes plane of order 9 as in [17, Section IX.6] with $GF(9)$ represented as in the proof of Theorem 3.1.5:

- The points are the elements of $V \setminus \{(0,0,0)\}$, where $V = \{(x_0, x_1, x_2) \mid x_i \in N\}$, N is the regular nearfield of order 9 with elements and the addition operation of $GF(9)$ but with multiplication defined as

$$x \cdot y = \begin{cases} yx & \text{if } y \text{ is a square in } GF(9), \\ yx^3 & \text{otherwise,} \end{cases}$$

  and with the proviso that $k(x_0, x_1, x_2)$ refers to the same point as (x_0, x_1, x_2) if $k \in N \setminus \{0\}$.

- The lines are the point sets $L(t)A^m$, $0 \leq m \leq 12$, t ranges over $N \setminus \{0, -1\}$, where $L(t)$ is the set of points satisfying the equation

$$x_0 + x_1 t + x_2 = 0,$$

  and A is a 3×3 matrix in $PGL(3,3)$ of order 13. In this case, we use

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

- Incidence is containment.

The Hughes plane of order 9 contains $PG(2,3)$ as a Baer subplane, and we call a line secant to $PG(2,3)$ a real line and a line tangent to $PG(2,3)$ a complex line. The automorphism group of the plane is transitive on the set of real lines and on the set of complex lines. Using a computer search, we have the result that the complex line $L(\alpha)$ is covered by the 5-arc

$$\{(-1,-1,1),(-1,1,1),(0,-1,1),(0,-\alpha,1),(-\alpha,0,1)\},$$

and the real line $L(1)$ is covered by the 5-arc

$$\left\{(-1,-1,1),(-1,1,1),(0,-\alpha,1),(0,-\alpha^2,1),(\alpha,\alpha,1)\right\}.$$

□

As a corollary to Theorems 3.1.4, 3.1.5, 3.1.11 and 3.1.12, we have

Theorem 3.1.13 Let Π_9 be a projective plane of order 9. Then a 1-regular 5-cover exists if and only if Π_9 is not the Desarguesian plane of order 9.

For $q = 27$, we show that if a 1-regular 8-cover exists in $PG(2,27)$, then it does not lie on a conic.

Theorem 3.1.14 In $PG(2,27)$, a 1-regular 8-cover does not lie on a conic.

Proof: The proof of this result is similar to that of Theorem 3.1.4. Let $\mathcal{K}$ be a 1-regular 8-arc in $PG(2,27)$ covering a line l_∞. Suppose that $\mathcal{K}$ lies on a conic $\mathcal{C}$, which must be disjoint from l_∞, for otherwise the points $l_\infty \cap \mathcal{C}$ cannot be covered by $\mathcal{K}$. The 28 points on $\mathcal{C}$ can be partitioned into 2 sharply focused sets, both focusing on the external points on l_∞ (Result 1.2.3). The only possible distributions of the points of $\mathcal{K}$ on $\mathcal{C}$ are:

(1) All 8 points of $\mathcal{K}$ lie in one of the sharply focused sets.

(2) 7 points of $\mathcal{K}$ lie in one of the sharply focused sets and 1 lies in the other.

(3) 6 points of $\mathcal{K}$ lie in one of the sharply focused sets and 2 lie in the other.

(4) 5 points of $\mathcal{K}$ lie in one of the sharply focused sets and 3 lie in the other.

(5) 4 points of $\mathcal{K}$ lie in one of the sharply focused sets and 4 lie in the other.

We show that in all of the 5 cases, $\mathcal{K}$ cannot be a 1-regular cover of l_∞ and hence $\mathcal{K}$ does not lie on a conic.

In the first case, all the points of $\mathcal{K}$ lies on one of the sharply focused sets and so the secants of $\mathcal{K}$ meet l_∞ only in external points, so the internal points on l_∞ are not covered.

In the second case, the 21 secants of the 7 points of $\mathcal{K}$ lying in one of the sharply focused sets meet l_∞ in the 14 external points, so some external point lies on more than one secant, which contradicts the property that $\mathcal{K}$ is 1-regular. Similarly, in the third case, the 15 secants of the 6 points of $\mathcal{K}$ in one of the sharply focused set meet l_∞ in the 14 external points, so one external point of l_∞ lie on more than 1 secant.

In the fourth case, the 5 points on one sharply focused set cover at most 10 external points on l_∞, and the remaining 3 points cover another 3 external points on l_∞. The remaining 15 secants cover internal points on l_∞, So there is at least one external point on l_∞ not covered by $\mathcal{K}$. Similarly, in the last case, the 4 points on one sharply focused set cover at most 6 external points on l_∞ and the other 4 points on the other sharply focused set cover at most 6 external points. The remaining 16 secants cover internal points, so there are at least 2 external points on l_∞ not covered by $\mathcal{K}$.

Hence in every case, we showed that either l_∞ is not covered by $\mathcal{K}$, or some point on it lies on more than one secant to $\mathcal{K}$, which contradicts the property of $\mathcal{K}$ as a 1-regular cover. So $\mathcal{K}$ does not lie on a conic. □

By a computer search we have

Theorem 3.1.15 There exists a 1-regular 8-cover for the line $z = 0$ in $PG(2, 27)$.

Proof: Let l_∞ be the line $z = 0$ in $PG(2, 27)$. Let $GF(27)$ be represented by

$$GF(27) = \left\{0, 1, \alpha^n \mid n = 1, \ldots, 25,\ \alpha^3 - \alpha + 1 = 0\right\}.$$

Then the 8-arc

$$\begin{aligned}\mathcal{K} &= \big\{(0,0,1),(1,0,1),(0,1,1),(\alpha,\alpha,1),(\alpha^2,\alpha^5,1),\\ &\quad (\alpha^3,\alpha^{15},1),(\alpha^{14},\alpha^{21},1),(\alpha^{23},\alpha^{20},1)\big\}\end{aligned}$$

found by computer search is a 1-regular 8-arc covering l_∞. □

By Corollary 3.1.2, Theorem 3.1.3, Theorem 3.1.5 and Theorem 3.1.15, we have

Theorem 3.1.16 Let Π_q be a projective plane of order q, q a prime power. Then, a 1-regular k-cover exists if and only if $q \in \{2, 5, 9, 27\}$.

3.2 n-regular k-covers

We give a few characterisations of n-regular k-covers in Π_q. Recall that a k-arc $\mathcal{K}$ is an n-regular k-cover of a line l_∞ if every point on l_∞ lies on exactly n secants to $\mathcal{K}$.

Theorem 3.2.1 If $\mathcal{K}$ is an n-regular k-cover for l_∞ in a projective plane of order q, then

$$n \leq \frac{k}{2}$$

and $n = k/2$ if and only if q is even and $\mathcal{K}$ is a $(q+2)$-arc.

Proof: Every point on l_∞ can lie on at most $k/2$ secants to $\mathcal{K}$ if $\mathcal{K}$ is a k-arc, so the inequality follows. If $\mathcal{K}$ is a $(q+2)$-arc, q even, then $\mathcal{K}$ has no tangents, and every point on l_∞ lies on exactly $k/2$ secants to $\mathcal{K}$. If $\mathcal{K}$ is not a $(q+2)$-arc then there is at least one tangent to each point on $\mathcal{K}$ so that every point on l_∞ lies on at most $(k-1)/2$ secants. □

For the second largest n, we have the following characterisation:

Theorem 3.2.2 Let $\mathcal{K}$ be an n-regular k-cover for l_∞ in a projective plane of order q. Then $n = (k-1)/2$ if and only if q is even and $\mathcal{K}$ is a $(q+1)$-arc with the nucleus not on l_∞.

Proof: If q is even and $\mathcal{K}$ is a $(q+1)$-arc with the nucleus not on l_∞, then every point on l_∞ lies on exactly one tangent to $\mathcal{K}$ and hence on exactly $(k-1)/2$ secants. Conversely, if $\mathcal{K}$ is a $(k-1)/2$-regular cover, then k must be odd and every point of l_∞ lies on exactly one tangent and $(k-1)/2$ secants. Counting the number of secants of $\mathcal{K}$ we have

$$\frac{k(k-1)}{2} = (q+1)\left(\frac{k-1}{2}\right)$$

which implies that $k = q+1$ and hence q is even. Since every point of l_∞ lies on exactly one tangent to $\mathcal{K}$, the nucleus of $\mathcal{K}$ is not on l_∞. □

By Theorem 2.1.4, it is possible that, in a projective plane of square order admitting a Baer subplane Π_o, a k_o-cover in Π_o for a Baer subline of l_∞ can be extended to a k-arc covering the whole of l_∞. The following discusses the possibility of extending n-regular k_o-covers in planes of prime powers q, where q is a square.

From Section 2.1, an n-regular k-cover in Π_q has

$$k = \frac{1+\sqrt{8nq+(8n+1)}}{2} = f(n,q).$$

Hence if $\mathcal{K}_o$ is an n-regular k_o-cover in a Baer subplane Π_o and is contained in a k-cover for l_∞, then $k_o = f(n,\sqrt{q})$ and by Theorem 2.1.4,

$$k \geq \frac{1+\sqrt{8q+8\sqrt{q}(n-1)+(8n+1)}}{2} = g(n,q).$$

Now, let

$$\begin{aligned}\Delta_1 &= 8nq+(8n+1),\\ \Delta_2 &= 8q+8\sqrt{q}(n-1)+(8n+1).\end{aligned}$$

Then $\Delta_1 - \Delta_2 = 8(n-1)(q-\sqrt{q}) \geq 0$ with equality if and only if $n=1$. Hence $f(n,q) \geq g(n,q)$ with equality only if $n=1$. This implies that for all n, it may be possible to extend an n-regular k_o-cover to an n-regular k-cover.

For $n=1$, however, if q a prime power, 1-regular k-arcs exist only if $q = 2$, 5, 9 or 27. Only 9 is a square but there is no 1-regular cover in Π_3. Hence in planes of prime power orders, a 1-regular k-cover cannot be extended.

For $n>1$, if an n-regular cover $\mathcal{K}_o$ for a Baer subline of l_∞ can be extended to an n-regular k-cover $\mathcal{K}$ for the whole line, then $k = f(n,q)$, and every point of $\mathcal{K} \setminus \mathcal{K}_o$

must lie on distinct lines of Π_o missing $\mathcal{K}_o$, and for every pair of points P, Q of $\mathcal{K} \setminus \mathcal{K}_o$, PQ covers a point of $l_\infty \setminus \mathcal{D}$. It is not clear if such an extension is always possible, but for small n and q, $n \leq 4$, $q \leq 13^2$, the only n, q such that both $f(n,q)$ and $f(n,\sqrt{q})$ are integers is $n = 2$, $q = 4$. In this case, $k_o = 4$, $k = 5$ and $\mathcal{K}_o$ is the affine plane $PG(2,2) \setminus l_\infty$, and so every point in $\Pi_4 \setminus l_\infty$ lies on a line meeting $\mathcal{K}_o$ in 2 points. This means that no point of $\Pi_4 \setminus l_\infty$ can be added to $\mathcal{K}_o$ to extend it to a 2-regular cover of l_∞.

3.3 (n_1, n_2)-regular k-covers

For a regular cover, every point on l_∞ is of the same type, that is, every point on l_∞ lies on the same number of secants and tangents. A conic in $PG(2,q)$, q odd, however, is not a regular cover for any line l_∞ disjoint from it. There are two types of points on l_∞: $(q+1)/2$ points of l_∞ lie on $(q-1)/2$ secants, and the other $(q+1)/2$ points lie on $(q+1)/2$ secants to the conic.

Definition 3.3.1 In a projective plane Π_q of odd order q, we say a k-arc $\mathcal{K}$ is an **(n_1, n_2)-regular** k-cover for l_∞ if $\mathcal{K}$ is disjoint from l_∞, and exactly half of the points on l_∞ lie on n_1 secants and the other half on n_2 secants.

A conic in $PG(2,q)$, for example, is a $((q-1)/2, (q+1)/2)$-regular $(q+1)$-cover. The next results are on $((q-1)/2, (q+1)/2)$-regular covers in arbitrary projective planes of odd order:

Theorem 3.3.2 In a projective plane of odd order q, if $\mathcal{K}$ is a $((q-1)/2, (q+1)/2)$-regular cover, then $\mathcal{K}$ is a $(q+1)$-arc.

Proof: Let $\mathcal{K}$ be a $((q-1)/2, (q+1)/2)$-regular k-cover. Then,

$$\left(\frac{q+1}{2}\right)\left(\frac{q-1}{2}\right) + \left(\frac{q+1}{2}\right)\left(\frac{q+1}{2}\right) = \frac{k(k-1)}{2},$$

that is,

$$q(q+1) = k(k-1),$$

and so $k = q+1$. Hence $\mathcal{K}$ is a $(q+1)$-arc. □

Theorem 3.3.3 If $\mathcal{K}$ is a $(q+1)$-arc in a projective plane Π_q of odd order q, then $\mathcal{K}$ is a $((q-1)/2, (q+1)/2)$-regular cover.

Proof: Firstly, we prove that every point in Π_q lies on 0,1 or 2 tangents to $\mathcal{K}$. A point P lies on exactly one tangent if and only if P lies on $\mathcal{K}$. For, if P does not lie on $\mathcal{K}$ and P lies on at least one tangent l, then, since $q+1$ is even, P must lie on at least one more tangent. There are q tangents to $\mathcal{K}$ other than l and q points on l not on $\mathcal{K}$, each of which lies on at least one more tangent other than l. Hence P lies on exactly two tangents.

Now, every point on l_∞ lies on either two tangents or none at all, hence every point on l_∞ lies on either $(q-1)/2$ secants or $(q+1)/2$ secants. Suppose there are n_1 points on l_∞ lying on $(q-1)/2$ secants and n_2 points on $(q+1)/2$ secants. Then,

$$n_1\left(\frac{q-1}{2}\right) + n_2\left(\frac{q+1}{2}\right) = \frac{q(q+1)}{2} \quad \text{and} \quad n_1 + n_2 = q+1.$$

Substituting $n_2 = q+1-n_1$, we have

$$n_1(q-1) + (q+1-n_1)(q+1) = q(q+1),$$

and so

$$n_1 = \frac{q+1}{2}\ .$$

Hence $\mathcal{K}$ is a $((q-1)/2, (q+1)/2)$-regular cover. □

Theorem 3.3.4 Let $\mathcal{K}$ be a k-arc in Π_q, q odd. Then $\mathcal{K}$ is a $((k-2)/2, k/2)$-cover if and only if $\mathcal{K}$ is a $(q+1)$-arc.

Proof: Suppose $\mathcal{K}$ is a $((k-2)/2, k/2)$-cover, then

$$\left(\frac{q+1}{2}\right)\left(\frac{k-2}{2}\right) + \left(\frac{q+1}{2}\right)\left(\frac{k}{2}\right) = \frac{k(k-1)}{2},$$

which implies that $k = q+1$. The converse is Theorem 3.3.3. □

Next we consider $(n, n+1)$-regular covers. If $\mathcal{K}$ is an $(n, n+1)$-regular k-cover then

$$\frac{k(k-1)}{2} = \frac{q+1}{2}n + \frac{q+1}{2}(n+1).$$

Solving the quadratic in k and taking the positive root, we have

$$k = \frac{1 + \sqrt{1 + 4(q+1)(2n+1)}}{2} .$$

A $(q+1)$-arc, for example, is an $(n, n+1)$-regular cover with $n = (q-1)/2$. However, the converse is not true in general, that is, an $(n, n+1)$-regular cover is not necessarily a $(q+1)$-arc. For example, using Construction 2.3.3, the 6-arc in $PG(2,9)$ consisting of a sharply focused set F of 5 points on a conic $\mathcal{C}$ and a point of $\mathcal{C} \setminus F$ is an $(n, n+1)$-regular cover with $n = 1$. Another example, found by a computer search, is when $q = 17$, $k = 10$ and $n = 2$. If the points on a conic in $PG(2,17)$ disjoint from a line l_∞ are identified with the integers modulo 18 (see Section 1.2), the 10-arc $\{(\!(0)\!), (\!(1)\!), (\!(2)\!), (\!(4)\!), (\!(5)\!), (\!(6)\!), (\!(8)\!), (\!(10)\!), (\!(12)\!), (\!(15)\!)\}$ is a $(2,3)$-regular cover of l_∞.

The next section discusses some ideas and results related to those in the last chapter and the preceding sections of this chapter.

3.4 Related work and other results

In Chapter 2 we answered partially a question of G. Ebert mentioned in [7] regarding how large a set of points in $AG(2,q)$ must be if it determines all possible directions of the affine plane. This is equivalent to asking how large a set of points in $PG(2,q)$ must be to cover a given line. We obtained a lower bound and characterised the set of points satisfying the bound as 1-regular k-arcs. The lower bound is met only if q satisfies the condition that $8q+9$ is an integer square. It is not clear in general what the smallest set of points must be if $8q+9$ is not a square. For small q, there are examples for which the lower bound in Theorem 2.1.2 is best possible, as shown in Section 2.4. For large q, Construction 2.3.4 gives a family of k-covers in planes of square orders, where k is of order $2\sqrt{q}$, while the lower bound is of order $\sqrt{2q}$. For arbitrary q, the smallest examples we have are the complete arcs in Example 2.2.1, and those constructed in Construction 2.3.3, of order a fraction of q. It will be of interest to construct a family of k-covers with smaller order for arbitrary q.

In view of the fact that points on a conic in $PG(2,q)$ may be identified with $\boldsymbol{Z}_{q+1}$

(see Section 1.2), if there exists a subset A of $\boldsymbol{Z}_{q+1}$ such that every element g in $\boldsymbol{Z}_{q+1}$ can be written as a sum $g = u + v$, $u, v \in A$, $u \neq v$, then there is a $|A|$-arc lying on a conic in $PG(2, q)$ which will cover a line disjoint from it. Theorem 2.1.2 and the results of Section 3.1 can thus be reworded as follows:

If G is a cyclic group of order $n = q + 1$, q a prime power, and A is a subset of G, $|A| = a$, satisfying the condition that every element $g \in G$ can be written as $g = u + v$, where $u, v \in A$, $u \neq v$, then

$$n \leq \frac{a(a-1)}{2}.$$

Equality is achieved if and only if $n \in \{3, 6\}$. In the case of equality, every element in G is written exactly once as the sum of two distinct elements in A.

In [13], Graham and Sloane showed that if $n(k)$, $k > 2$, is the largest number n such that a k element subset A of $\boldsymbol{Z}_n$ exists with the property that every element of $\boldsymbol{Z}_n$ can be written as a sum of two distinct elements of A, then

$$\frac{5}{18}(k-1)^2 \leq n(k) \leq \frac{k(k-1)}{2}.$$

It was shown that equality holds in the upper bound if and only if $(k, n(k)) = (3, 3)$ or $(4, 6)$. This is the same as our result. The lower bound is not relevant to our work because it implies that $k < 324n^2/25 + 1$, which is trivially true since a k-arc satisfies $k \leq q + 2 < 324(q+1)^2/25 + 1$.

There are examples of A and $\boldsymbol{Z}_{q+1}$ for small q given in [13] which imply the existence of k-covers in $PG(2, q)$. For example, there is a 7-cover in $PG(2, 16)$, an 8-cover in $PG(2, 23)$, and a 9-cover in $PG(2, 31)$, all lying on conics and all giving best possible k-covers according to the lower bound of Theorem 2.1.2. However, this method will at best give us a proper subset of all possible k-arcs covering a line because such a k-arc does not necessarily lie on a conic, as exemplified in the case of a 1-regular 8-cover in $PG(2, 27)$.

In [7], Blokhuis, Wilbrink and Sali proved a similar but more general result:

If G is a finite abelian group of odd order n, and $A \subseteq G$, $|A| = a$, satisfies the condition that every element $g \in G$ can be written as $g = u + v$, where $u, v \in A$,

$u \neq v$, then

$$n \leq \begin{cases} \dfrac{(a-1)^2+1}{2} & \text{if } a \text{ is even,} \\ \dfrac{(a-1)^2+2}{2} & \text{if } a \text{ is odd.} \end{cases}$$

Equality is achieved if and only if $n \in \{3, 5, 9, 13, 25, 243\}$. In the case of equality, exactly one element of G can be written $a/2$ or $(a-1)/2$ times depending on whether a is even or odd, and the remaining elements can be written exactly once, as a sum of two distinct elements in A.

The two results overlapped only in $n = 3$. The two approaches are different: we fixed n and obtained a lower bound on a while Blokhuis, Wilbrink and Sali fixed a and obtained an upper bound on odd n. It is not clear if the method of proof for the result can be modified to give an indication to the size of the smallest set of points covering a line in $PG(2, q)$ and other planes. It is also not obvious if an analogous group structure can be imposed on arbitrary complete arcs.

In the next chapter we discuss some generalisations of the notion of k-arcs covering a line in projective planes.

Chapter 4

Some generalisations of k-covers

This chapter discusses some generalisations of k-arcs covering a line in a projective plane. In Section 4.1, we examine (k, n)-arcs covering a disjoint set of points T and obtain lower bounds on k in terms of n and the intersection properties between T and the lines of the plane. In Section 4.2, we show that the concept of k-arcs covering a line can be extended to that of sets of points covering a hyperplane in higher dimensional projective spaces and show that, in fact, a k-arc covering a line in $PG(2, q)$ also covers a hyperplane in $PG(n, q)$ for all $n > 2$. In the last section we discuss some open questions.

4.1 (k, n)-arcs covering arbitrary sets of points

Let Π_q be a projective plane of order q. A (k, n)-arc in Π_q is a set of k points such that every line of Π_q meets it in at most n points and some line meets it in n points. Let T be a non-empty set of t points and let $\mathcal{K}$ be a (k, n)-arc disjoint from T. We say that $\mathcal{K}$ covers T if every point of T lies on a t-secant of $\mathcal{K}$, $t \geq 2$.

Let $\mathcal{L}(T)$ be the set of lines of Π_q containing less than q points of T and let $\mu(T)$ be the minimum number of lines belonging to $\mathcal{L}(T)$ such that T lies in the union of these lines. These definitions are made because we are primarily concerned with obtaining a lower bound on k by counting the number of secants of $\mathcal{K}$ that would contain T, and a line containing q or more points of T cannot be a secant of $\mathcal{K}$ and

hence is disregarded.

Lemma 4.1.1 Let m be the maximum number of collinear points of T, that is, T is a (t, m)-arc. Then

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

Proof: If $m = 1$, T is a single point, that is, $t = 1$, and so $\mu(T) = 1 = t/m$ since exactly one line is required to cover T.

If $2 \leq m \leq q-1$, then let $\mathcal{M}(T)$ be a subset of $\mu(T)$ lines of $\mathcal{L}(T)$ such that T lies in the union of the lines in $\mathcal{M}(T)$. We count the flags

$$F = \{(P, l) \mid P \in T, l \in \mathcal{M}(T)\}.$$

Firstly, there are t points of T and each point lies on at least one line of $\mathcal{M}(T)$, so $|F| \geq t$. On the other hand, there are $\mu(T)$ lines in $\mathcal{M}(T)$, each line containing at most m points of T, so $|F| \leq \mu(T)\ m$. Hence $\mu(T) \geq t/m$.

If $m = q$ or $q+1$, let l' be an m-secant of T. Then the m points of T on l' must lie on m distinct lines of $\mathcal{L}(T)$, so $\mu(T) \geq m$. □

Lemma 4.1.2 Let $\mathcal{K}$ be a (k, n)-arc in Π_q. Then $\mathcal{K}$ has the maximum number of secants of all (k, n)-arcs when exactly one of the secants of $\mathcal{K}$ is an n-secant and the rest are 2-secants.

Proof: Let $s_{\mathcal{K}}$ be the number of secants of $\mathcal{K}$, and let s_n be the number of n-secants of $\mathcal{K}$. We count the number of flags $F = \{(P, l) \mid P \in \mathcal{K},\ l \text{ a secant of } \mathcal{K}\}$.

Since $|\mathcal{K}| = k$ and through every point of $\mathcal{K}$ there are at most $k-1$ secants, we have

$$|F| \leq k(k-1).$$

On the other hand, on s_n of the secants, there are n points of $\mathcal{K}$ and on $s_{\mathcal{K}} - s_n$ of the secants, there are at least 2 points of $\mathcal{K}$. Hence

$$|F| \geq n s_n + 2(s_{\mathcal{K}} - s_n).$$

Combining the inequalities, we have

$$k(k-1) \geq ns_n + 2(s_{\mathcal{K}} - s_n),$$

and so

$$s_{\mathcal{K}} \leq \frac{k(k-1)}{2} - \frac{s_n(n-2)}{2}.$$

Hence $s_{\mathcal{K}}$ is maximum when $s_n = 1$, that is, $\mathcal{K}$ has exactly one n-secant, and all other secants of $\mathcal{K}$ are 2-secants. □

Theorem 4.1.3 Let T be a (t,m)-arc and $\mathcal{K}$ a (k,n)-arc covering T. Then

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

where

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

Proof: We count the flags

$$F = \{(P,l) \mid P \in \mathcal{K},\ l \text{ a secant of } \mathcal{K}\}.$$

Firstly , there are k points in $\mathcal{K}$, each of which lies on at most $k-1$ secants, and at least n of which lie on at most $k-n+1$ secants, so

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

On the other hand, since $\mathcal{K}$ covers T, the number of secants of $\mathcal{K}$ must be at least $\mu(T)$, and there are at least 2 points of $\mathcal{K}$ on each secant, and n points on at least one of the secants. So we have

$$|F| \geq n + 2(\mu(T) - 1).$$

Combining the two inequalities, we have

$$k^2 - k - n^2 + 2n \geq n + 2(\mu(T) - 1),$$

that is,

$$k^2 - k - (n^2 - n + 2(\mu(T) - 1)) \ \geq \ 0,$$

and so, since $k \geq 0$, we have

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

The lower bound on $\mu(T)$ is proved in Lemma 4.1.1. □

From the proof of Theorem 4.1.3, if equality is achieved then exactly one secant of $\mathcal{K}$ is an n-secant, the remaining $n(k-n)+\begin{pmatrix} k-n \\ 2 \end{pmatrix}$ secants being 2-secants, and T is contained in the union of exactly $\mu(T)$ lines which are all the secants of $\mathcal{K}$. We show, in the following examples, that the lower bound of Theorem 4.1.3 is met in some cases.

Example 4.1.4 If T is a single point and $\mathcal{K}$ is a (k,n)-arc covering T, then $\mu(T) = 1$, and by Theorem 4.1.3,

$$k \geq \frac{1+\sqrt{4(n^2-n+2\cdot 1)-7}}{2} = \frac{1+\sqrt{(2n-1)^2}}{2} = n.$$

The lower bound is achieved when $\mathcal{K}$ is just n points collinear with T. □

Example 4.1.5 If T is a $(t,2)$-arc and $\mathcal{K}$ is a $(k,2)$-arc, then $\mu(T) = t/2$ and the lower bound of Theorem 4.1.3 becomes

$$k \geq \frac{1+\sqrt{4(2^2-2+2\cdot\frac{t}{2})-7}}{2} = \frac{1+\sqrt{4t+1}}{2}.$$

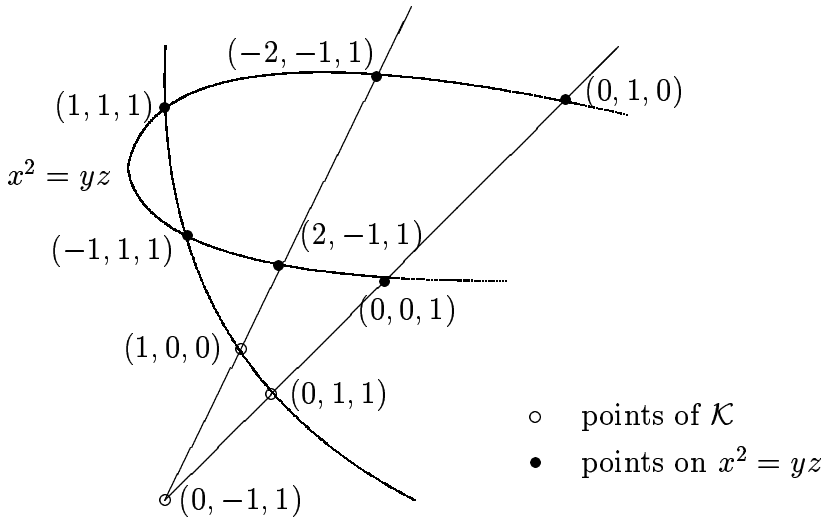
There are examples meeting this lower bound. For instance in $PG(2,5)$, the 3-arc $\{(1,0,0),(0,-1,1),(0,1,1)\}$ covers the conic $x^2 = yz$ (See Figure 4.1), and in $PG(2,11)$, the 4-arc $\{(0,1,1),(0,-4,1),(3,0,1),(4,-3,1)\}$ found by computer search covers the conic $x^2 = yz$. □

Example 4.1.6 If T is a (t,q)-arc and $\mathcal{K}$ is a (k,n)-arc covering T, then $\mu(T) \geq q$, and

$$k \geq \frac{1+\sqrt{4(n^2-n+2q)-7}}{2} = \frac{1+\sqrt{8(q-1)+(2n-1)^2}}{2}.$$

There are examples meeting this bound when T is a $(q+1,q)$-arc and $\mathcal{K}$ is a (k,n)-arc. For example, by using a computer, we found the 3-arc $\mathcal{K}$ in $PG(2,3)$ covering

Figure 4.1: A 3-arc covering $x^2 = yz$ in $PG(2,5)$.



the $(4,3)$-arc T, where

$$\begin{aligned} \mathcal{K} &= \{(1,0,1),(-1,0,1),(0,-1,1)\}, \\ T &= \{(1,0,0),(1,1,0),(1,-1,0),(0,0,1)\}, \end{aligned}$$

and the $(4,3)$-arc $\mathcal{K}'$ in $PG(2,4)$ covering the $(5,4)$-arc T', where, with $\alpha^2+\alpha+1 = 0$,

$$\begin{aligned} \mathcal{K}' &= \{(0,1,1),(1,\alpha,1),(\alpha^2,\alpha,1),(0,\alpha,1)\}, \\ T' &= \{(0,0,1),(0,1,0),(1,0,0),(1,1,0),(1,\alpha^2,0).\end{aligned}$$

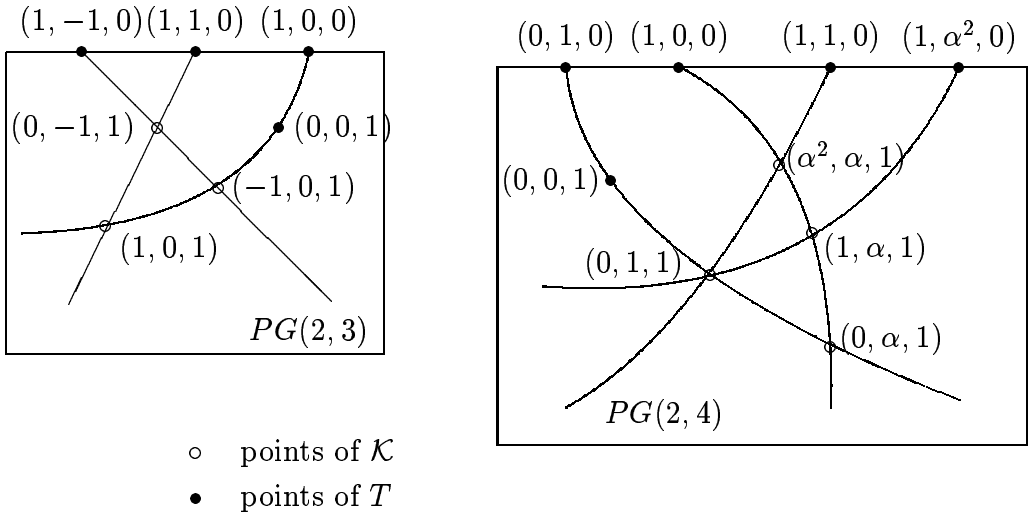
(See Figure 4.2.) □

Example 4.1.7 If T is a line or contains lines and $\mathcal{K}$ is a (k,n)-arc covering it, then $\mu(T) \geq q+1$, and

$$k \geq \frac{1+\sqrt{4(n^2-n+2(q+1))-7}}{2} = \frac{1+\sqrt{8q+(2n-1)^2}}{2}.$$

There are examples where the lower bound is achieved. For instance, if T is a line and $\mathcal{K}$ is a k-arc, then 1-regular k-covers meet the lower bound. If $n = 3$,

Figure 4.2: Arcs covering $(q+1, q)$-arcs.



the $(5, 3)$-arc $\{(0, 1, 1), (0, 0, 1), (0, -1, 1), (1, 0, 1), (-1, 3, 1)\}$ found by a computer search covers the line $z = 0$ in $PG(2, 7)$. Note that in this and Example 4.1.6, the lower bounds do not take into account the size of T. In fact, if $\mathcal{K}$ covers a line (or q points of a line) then every set consisting of that line and points on the secants of $\mathcal{K}$ is also covered by $\mathcal{K}$. □

Now, a set of points S covers a set of points T if every point on T lies on a t-secant of S, $t \geq 2$. It is clear then that a set S of more than one point always covers itself, since every point of S lies on a secant of S. In view of this, we consider a set S covering a set T containing it. We obtain the following result:

Theorem 4.1.8 Let T be a set of t points in a projective plane Π_q of order q and let S be a set of s points contained in T. Suppose that T is a (t, m)-arc, $3 \leq m \leq q+1$, and S is an (s, n)-arc. If S covers T, then

$$s \geq s(n; t, m)$$

where

$$s(n; t, m) = \frac{(m-4) + \sqrt{(m-4)^2 - 4(m-2)[2m - (m-2)n^2 + (m-4)n - 2t]}}{2(m-2)}.$$

Proof: We count the flags $F = \{(Q, l) \mid Q \in T \setminus S,\ l \text{ a secant of } S\}$:

The number of points in $T \setminus S$ is $t - s$ and there is at least one secant of S on each of these points, so $|F| \geq t - s$.

On the other hand, S has at most

$$n(s-n) + \begin{pmatrix} s-n \\ 2 \end{pmatrix} + 1$$

secants, each one of which has at most $m - 2$ points of $T \setminus S$ and one of which has at most $m - n$ points of $T \setminus S$, so

$$|F| \leq \left(n(s-n) + \begin{pmatrix} s-n \\ 2 \end{pmatrix} \right) (m-2) + (m-n).$$

Combining the two inequalities we have

$$t - s \leq \left(n(s-n) + \begin{pmatrix} s-n \\ 2 \end{pmatrix} \right) (m-2) + (m-n),$$

and the inequality $s \geq s(n; t, m)$ follows. □

If equality is achieved, then exactly one of the secants of S is an n-secant and all the others are 2-secants, every secant of S has m points of T and every point of T lies on exactly one secant of S.

For the case when $m = 2$, that is, T is a t-arc, if S is contained in T and covers T then S must be the whole of T. For if S is a proper subset of T, then every line through a point P in $T \setminus S$ would meet S in at most one point since T is an arc, so that S would not cover P. In fact, a set T that is not covered by any proper subset of itself is necessarily an arc. This is because if T is not covered by any proper subset of itself, then for any point P in T, every line through P must meet $T \setminus \{P\}$ in at most one point. Thus every line of the plane meet T in at most two points, so T is an arc. Hence we have the following result:

Theorem 4.1.9 A set T of t points in a projective plane of order q is not covered by any proper subset of itself if and only if T is a t-arc. □

Example 4.1.10 If T is a line of a projective plane Π_q of order q, that is, T is a $(q+1, q+1)$-arc, and if S is an (s, n)-arc in T that covers T, then

$$s \geq s(n; q+1, q+1) = n.$$

This bound is met since S would just be n points on T.

If T is the whole of Π_q and S is an s-arc covering T, then S is a complete arc, and

$$s \geq s(2; q^2+q+1, q+1) = \frac{q-3}{2(q-1)} + \frac{\sqrt{[4(q-1)-(q-3)]^2 + 8q^2(q-1)}}{2(q-1)},$$

and this bound is met only if every point of T lies on exactly one secant of S. This bound is not as good as the existing bounds (for example, the one obtained from blocking sets by Ball in [1], which has $s \geq \lfloor \sqrt{2q} + 2 \rfloor$). We give a numerical comparison of $s(2; q^2+q+1, q+1)$ with the lower bound on the size of complete arcs given in Example 2.2.1 ($s \geq (3+\sqrt{8q+1})/2$) and that given by Ball [1] ($s \geq \lfloor \sqrt{2q} + 2 \rfloor$) for a few values of q:

q	$\lfloor \frac{3+\sqrt{8q+1}}{2} \rfloor$	$\lfloor \sqrt{2q} + 2 \rfloor$	$\lfloor s(2; q^2+q+1, q+1) \rfloor$
2	4	4	4
5	5	6	5
41	11	12	10
49	12	12	11
101	16	17	15
1009	47	47	46

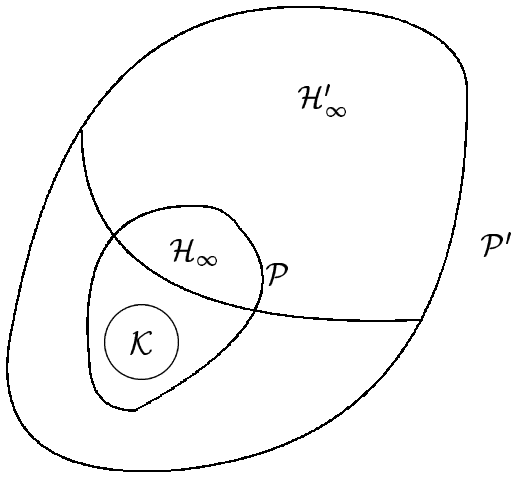
□

4.2 *k*-covers in projective spaces

Let $\mathcal{P} = PG(n, q)$ be the projective space of dimension n over the field of order q. Let $\mathcal{H}_\infty$ be a fixed hyperplane of $\mathcal{P}$ designated as the hyperplane at infinity. Then $\mathcal{P} \setminus \mathcal{H}_\infty$ is the affine space $AG(n, q)$. A parallel class of hyperplanes of $AG(n, q)$ corresponds to the hyperplanes of $\mathcal{P}$, excluding $\mathcal{H}_\infty$, containing a given $(n-2)$-dimensional subspace in $\mathcal{H}_\infty$. Each parallel class contains q hyperplanes and these hyperplanes partition the affine points of $\mathcal{P}$. There are $(q^n - 1)/(q-1)$ parallel classes.

We say that a set of affine points $\mathcal{K}$ in $\mathcal{P}$ covers a parallel class of $AG(n, q)$ (or the corresponding $(n-2)$-dimensional subspace in $\mathcal{H}_\infty$) if there is a hyperplane

Figure 4.3: Embedding $\mathcal{P}$ in $\mathcal{P}'$.



belonging to that parallel class containing at least two points of $\mathcal{K}$, and we say that $\mathcal{K}$ covers $\mathcal{H}_\infty$ in $\mathcal{P}$ if $\mathcal{K}$ covers every parallel class. This is equivalent to saying that the secants to $\mathcal{K}$ meet every $(n-2)$-dimensional subspace in $\mathcal{H}_\infty$.

Theorem 4.2.1 Let $\mathcal{P} = PG(n,q)$ and let $\mathcal{H}_\infty$ be the hyperplane at infinity. Let $\mathcal{K}$ be a set of k points in $\mathcal{P}$ covering $\mathcal{H}_\infty$. Then there is a set of k points covering the hyperplane at infinity $\mathcal{H}'_\infty$ of $\mathcal{P}' = PG(n+1,q)$.

Proof: Since $\mathcal{K}$ covers $\mathcal{H}_\infty$, for every $(n-2)$-dimensional subspace in $\mathcal{H}_\infty$, there is a hyperplane of $\mathcal{P}$ through it containing two points of $\mathcal{K}$. Now, let $\mathcal{P}$ be embedded in $\mathcal{P}'$ as a hyperplane meeting $\mathcal{H}'_\infty$ in the $(n-1)$-dimensional subspace $\mathcal{H}_\infty$ (see Figure 4.3). We show that $\mathcal{K}$ covers $\mathcal{H}'_\infty$, that is, for each $(n-1)$-dimensional subspace in $\mathcal{H}'_\infty$, there is a hyperplane of $\mathcal{P}'$ through it containing at least two points of $\mathcal{K}$.

The parallel class of hyperplanes of $\mathcal{P}'$ through $\mathcal{H}_\infty$ is covered, since it contains $\mathcal{P}$ and hence $\mathcal{K}$. Let β be an $(n-1)$-dimensional subspace of $\mathcal{H}'_\infty$, $\beta \neq \mathcal{H}_\infty$, and let Σ_β be the parallel class of hyperplanes of $\mathcal{P}'$ through β. Let $X = \mathcal{H}_\infty \cap \beta$. Then X is an $(n-2)$-dimensional subspace contained in $\mathcal{H}_\infty$. The q hyperplanes in the

parallel class Σ_β meet $\mathcal{P}$ in q distinct $(n-1)$-dimensional subspaces containing X, that is, the intersections of the q hyperplanes of the parallel class Σ_β with $\mathcal{P}$ form the parallel class of hyperplanes of $\mathcal{P}$ through X. Since $\mathcal{K}$ covers $\mathcal{H}_\infty$, one of these intersections contains at least two points of $\mathcal{K}$. Hence one of the hyperplanes in Σ_β contains at least two points of $\mathcal{K}$, so Σ_β is covered. This is true for all parallel classes of $\mathcal{P}'$. Hence $\mathcal{K}$ covers $\mathcal{H}'_\infty$ in $\mathcal{P}'$. □

As a corollary to the above theorem, we have

Corollary 4.2.2 If there is a k-arc covering a line in $PG(2,q)$, then there is a k-cap covering a hyperplane in $PG(n,q)$ for all $n > 2$.

Proof: Let $\mathcal{K}$ be a k-arc covering a line l_∞ in $\Pi = PG(2,q)$ and let $\mathcal{H}_\infty$ be a hyperplane in $PG(n,q)$, $n > 2$. Let Π be embedded in $PG(n,q)$ in such a way that Π meets $\mathcal{H}_\infty$ in the line l_∞. Then $\mathcal{K}$ is a k-cap in $PG(n,q)$ and, by applying Theorem 4.2.1 inductively, $\mathcal{K}$ covers $\mathcal{H}_\infty$. □

There are $(q^n-1)/(q-1)$ parallel classes of hyperplanes in $PG(n,q)$, so it would seem that for a set of k points to cover a hyperplane $\mathcal{H}_\infty$ in $PG(n,q)$, we would need

$$\frac{k(k-1)}{2} \geq \frac{q^n-1}{q-1}.$$

However, by Corollary 4.2.2, all that is necessary is a k-cap $\mathcal{K}$ contained in a plane Π of $PG(n,q)$ which meets $\mathcal{H}_\infty$ in a line l_∞ such that $\mathcal{K}$ covers l_∞ in Π. Hence, since there are $q+1$ points on l_∞, the lower bound on k is

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

that is, $k \geq (1+\sqrt{8q+9})/2$.

The case when $n = 3$ gives an interesting example relating to blocking sets in planes:

Example 4.2.3 Let $\Sigma = PG(3,q)$ and let π_∞ be the plane at infinity of Σ. Let $\mathcal{K}$ be a k-cap in $\Sigma \setminus \pi_\infty$ covering π_∞. Let $\mathcal{B}$ be the points of intersections of the secants of $\mathcal{K}$ with π_∞. Then, since $\mathcal{K}$ covers π_∞, the secants of $\mathcal{K}$ meet every line of π_∞, that is, $\mathcal{B}$ forms a blocking set of π_∞, in the sense that every line of π_∞ contains a point of $\mathcal{B}$.

If $\mathcal{B}$ is a line then

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

which gives the lower bound of Corollary 4.2.2.

If $\mathcal{B}$ is a non-trivial blocking set (that is, $\mathcal{B}$ does not contain a line), then it is well-known (see, for example, [8]) that

$$|\mathcal{B}| \geq q+\sqrt{q}+1.$$

In this case, $\mathcal{K}$ does not lie in a plane. We have

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

and hence

$$k \geq \frac{1+\sqrt{8q+9+8\sqrt{q}}}{2}.$$

If $\mathcal{K}$ lies in a plane then $\mathcal{B}$ is certainly a line. However, it is not clear if the converse is true.

In general, let $\Sigma = PG(n,q)$ and let $\mathcal{H}_\infty$ be the hyperplane at infinity of Σ. Let $\mathcal{K}$ be a k-cap in $\Sigma \setminus \mathcal{H}_\infty$ covering $\mathcal{H}_\infty$ and let $\mathcal{B}$ be the points of intersections of the secants of $\mathcal{K}$ with $\mathcal{H}_\infty$. If $\mathcal{K}$ is contained in a hyperplane $\mathcal{H}$ of Σ, then $\mathcal{B}$ lies wholly in a hyperplane $\mathcal{H} \cap \mathcal{H}_\infty$ of $\mathcal{H}_\infty$. This is certainly the case when $\mathcal{K}$ is inherited by embedding, as in Theorem 4.2.1. Again, it is not clear if the converse is true, that is, whether $\mathcal{B}$ lying in a hyperplane of $\mathcal{H}_\infty$ necessarily implies that $\mathcal{K}$ is contained in a hyperplane of Σ.

If $\mathcal{B}$ does not lie in a hyperplane of $\mathcal{H}_\infty$ then $\mathcal{B}$ must be a 1-blocking set in $\mathcal{H}_\infty$, that is, every hyperplane of $\mathcal{H}_\infty$ contains a point of $\mathcal{B}$, and as shown by Beutelspacher in [2, Theorem 1],

$$|\mathcal{B}| \geq q+\sqrt{q}+1.$$

Hence in this case,

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

and so

$$k \geq \frac{1+\sqrt{8q+9+8\sqrt{q}}}{2}.$$

□

4.3 Some open questions

In this section we discuss some open questions arising from the generalisation of k-covers.

The set of all complete arcs forms a subset of the set of all k-arcs covering a line. Consider a $(q+1)$-arc $\mathcal{K}$ in a projective plane Π_q of order q, q even. Every point P on Π_q, P not the nucleus of $\mathcal{K}$, lies on $q/2$ secants and 1 tangent of $\mathcal{K}$, while the nucleus lies on $q+1$ tangents and no secant. Hence $\mathcal{K}$ covers all lines missing $\mathcal{K}$, but is not a complete arc. One of the questions that arises is as follows: If $\mathcal{K}$ is a k-arc covering a line in Π_q, how many other lines does $\mathcal{K}$ cover if $\mathcal{K}$ is not a complete arc? Furthermore, is there an $\epsilon_{q,k}$ such that if $\mathcal{K}$ covers n lines, $n > \epsilon_{q,k}$, then $\mathcal{K}$ covers all lines, that is, $\mathcal{K}$ is a complete arc?

In Example 4.1.7, we see that if a k-arc $\mathcal{K}$ covers a set of points T containing a line, then $\mathcal{K}$ covers all the points on the secants of $\mathcal{K}$ as well, and the lower bound on k does not depend on $|T|$. We ask whether there is a lower bound on k in terms of the number of lines T contains: if T is the union of α lines, is there a lower bound $\kappa(\alpha)$ such that if $\mathcal{K}$ covers T then $k \geq \kappa(\alpha)$?

In Theorem 4.1.8, the lower bound is achieved only if T lies in the secants generated by S. One may ask then, if T is a union of α lines, what is the minimal number of points in a set $S \subseteq T$ that could "generate" T (that is, T lies wholly in the secants of S)? By "minimal" we mean that for every point P of S, the set of points $S \backslash \{P\}$ does not generate T.

We conjecture that if T is a set of α lines and S is a minimal set of s points contained in T such that S generates T, then

$$\frac{1+\sqrt{8\alpha+1}}{2} \leq s \leq \alpha+1,$$

where the lower bound is met when T is the set of secants of an s-arc, and the upper bound is met when T is a set of α concurrent lines. The lower bound is easily proved, since a set of s points has at most $s(s-1)/2$ secants. The upper bound is yet to be proved. At present we have only proof that $s \leq 2\alpha$, by observing the fact that if S is minimal then through every point of S there must be a line of T which contains exactly one other point of S. There is hence a "skeleton" graph G

in T whose vertices V are the points of S and whose edges E are the lines of T containing exactly two points of S. The degree of each vertex of G is at least 1, so that by counting the set $\{(P, l) \mid P \in V,\ l \in E,\ P \in l\}$, we have $s \leq 2\alpha$.

Chapter 5

Some properties of a family of planes by Yoshiara

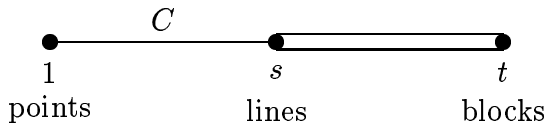
In this chapter we investigate the properties of a family of planes in $PG(5,q)$ constructed by Yoshiara [22] which is used to construct a family of extended generalised quadrangles of order $(q+1, q-1)$. We are interested mainly in the combinatorial and geometric properties of the family of planes in $PG(5,q)$ and will not discuss in any detail the properties of the resulting extended generalised quadrangles. The interested reader is refered to [22], [20] and [23].

5.1 Introducton

Let $\mathcal{E} = \{\pi_o, \ldots, \pi_{q+2}\}$ be a set of $q+3$ planes in $PG(5,q)$, q even, such that

$$\left.\begin{array}{ll} \text{(a)} & \text{the intersection of two planes } \pi_i,\ \pi_j \text{ in } \mathcal{E} \text{ is a point for all} \\ & i,\ j = 0, \ldots, q+2,\ i \neq j; \\ \text{(b)} & \text{the set } \mathcal{O}_i = \{\pi_i \cap \pi_j \mid j \in \{0, \ldots, q+2\} \setminus \{i\}\} \text{ is a hyperoval} \\ & \text{in } \pi_i \text{ for all } i = 0, \ldots, q+2; \\ \text{(c)} & \text{the planes in } \mathcal{E} \text{ span } PG(5,q). \end{array}\right\} (\dagger)$$

An extended generalised quadrangle (EGQ) of order (s,t) is a connected geometry with three types of elements, points, lines and blocks, belonging to the following diagram:



such that the point-residues are generalised quadrangles of order (s,t), the block-residues are isomorphic to the complete graph on $s+2$ vertices, and the line-residues are generalised digons. (See [19] for details on diagram geometries.) We describe briefly how an EGQ of order $(q+1,q-1)$ (denoted EGQ$(q+1,q-1)$) is constructed from $\mathcal{E}$:

Let Σ denote the 5-space containing the $q+3$ planes $\mathcal{E}=\{\pi_0,\ldots,\pi_{q+2}\}$ and let Σ be embedded as a hyperplane in a 6-dimensional projective space $PG(6,q)$. Let

$$\begin{aligned}
\mathcal{G}_2 &= \text{the set of projective points in } PG(6,q)\setminus\Sigma,\\
\mathcal{G}_1 &= \text{the set of projective lines of the form } \langle \pi_i\cap\pi_j, P\rangle,\\
&\quad \pi_i,\pi_j\in\mathcal{E},\ \pi_i\neq\pi_j \text{ and } P\in\mathcal{G}_2,\\
\mathcal{G}_0 &= \text{the set of projective 3-spaces of the form } \langle \pi_i, P\rangle,\\
&\quad \text{where } \pi_i\in\mathcal{E} \text{ and } P\in\mathcal{G}_2.
\end{aligned}$$

Then $\mathcal{G}_0$, $\mathcal{G}_1$ and $\mathcal{G}_2$ are respectively the points, lines and blocks of an EGQ$(q+1,q-1)$ Γ with $q^3(q+3)$ points, $q^5(q+3)(q+2)/2$ lines, q^6 blocks, and incidence given by symmetrised inclusion. The residue of a point $\langle\pi_i,P\rangle$ is isomorphic to the dual of the Tits quadrangle $T_2^*(\mathcal{O}_i)$ for $i=0,\ldots,q+2$.

(Briefly, the Tits quadrangle is constructed as follows: Let $\mathcal{O}$ be a hyperoval in the plane $\Pi=PG(2,q)$, $q=2^h$, and let Π be embedded as a hyperplane in $PG(3,q)$. The Tits quadrangle $T_2^*(\mathcal{O})$ is then a generalised quadrangle of order $(q-1,q+1)$, with points defined as the points of $PG(3,q)\setminus\Pi$, and lines defined as the set of lines of the form $\{PQ \mid P\in PG(3,q)\setminus\Pi,\ Q\in\mathcal{O}\}$.)

In [20] it was shown that if there is a point P_o in $PG(5,q)$ which is not contained in any of the hyperplanes $\langle\pi_i,\pi_j\rangle$, $i\neq j$, then, by projecting π_i from P_o onto a hyperplane $\mathcal{H}$ not containing P_o, the set of planes $\{\alpha_0,\ldots,\alpha_{q+2}\}$, where α_i is the projection of π_i, satisfies only conditions (a) and (b) of (†) in $PG(4,q)$. By embedding $PG(4,q)$ as a hyperplane in a 5-space $PG(5,q)$, an EGQ$(q+1,q-1)$ with $q^2(q+3)$ points, $q^4(q+3)(q+2)/2$ lines and q^5 blocks can be constructed:

Let Σ' denote the 4-space containing $\{\alpha_0, \ldots, \alpha_{q+2}\}$ and let Σ' be embedded as a hyperplane in a 5-space $PG(5,q)$. Then the points, lines and blocks of the EGQ$(q+1, q-1)$ Γ' are respectively $\mathcal{G}_0'$, $\mathcal{G}_1'$ and $\mathcal{G}_2'$, where

$$\begin{aligned}
\mathcal{G}_2' &= \text{the set of projective points in } PG(5,q) \setminus \Sigma', \\
\mathcal{G}_1' &= \text{the set of projective lines of the form } \langle \alpha_i \cap \alpha_j, P \rangle, \alpha_i \neq \alpha_j, P \in \mathcal{G}_2, \\
\mathcal{G}_0' &= \text{the set of 3-spaces of the form } \langle \alpha_i, P \rangle, P \in \mathcal{G}_2.
\end{aligned}$$

Suppose now that Σ is a 5-space containing a set of $q+3$ planes $\mathcal{E}$ satisfying conditions (†), and suppose that there is a point of projection P_o in Σ not contained in any hyperplane spanned by pairs of planes of $\mathcal{E}$. If Γ is the EGQ constructed by embedding Σ in $PG(6,q)$, then, by choosing another hyperplane $\bar{\Sigma}$ of $PG(6,q)$ not containing P_o, Γ can be projected from P_o onto $\bar{\Sigma}$, and this projection is the EGQ Γ'. Hence Γ is a q-fold covering of Γ' and conversely, Γ' is a q-fold quotient of Γ . We refer the reader to [20] for details.

There are two known constructions for a set $\mathcal{E}$ of $q+3$ planes in $PG(5,q)$, q even, satisfying conditions (†). They are described in Examples 5.1.1 and 5.1.2.

Example 5.1.1 In [22], Yoshiara constructed as follows a set of $q+3$ planes in $PG(5,q)$, q even, satisfying conditions (†). Let $\mathcal{O}^*$ be a dual hyperoval of $PG(2,q)$, q even, that is, a set of $q+2$ lines no three of which are concurrent. Let ϕ be a bijection from the points of $PG(2,q)$ onto the Veronese surface $\mathcal{V}_2^4$ in $PG(5,q)$:

$$\begin{array}{rcccl}
\phi & : & PG(2,q) & \to & PG(5,q) \\
 & & (x_0, x_1, x_2) & \mapsto & (x_0^2, x_1^2, x_2^2, x_0x_1, x_0x_2, x_1x_2).
\end{array}$$

The $q+2$ lines of $\mathcal{O}^*$ are mapped by ϕ onto $q+2$ conics $\mathcal{C}_0, \ldots, \mathcal{C}_{q+1}$ of $\mathcal{V}_2^4$ and if N_i is the nucleus of the conic $\mathcal{C}_i$ then the set $\{N_0, N_1, \ldots, N_{q+1}\}$ is a hyperoval in the nucleus of $\mathcal{V}_2^4$. (See [16] for a detailed description of the Veronese surface.) Let π_i be the conic plane containing the hyperoval $\mathcal{O}_i = \mathcal{C}_i \cup \{N_i\}$, $i = 0, \ldots, q+1$, and let π_{q+2} be the nucleus of $\mathcal{V}_2^4$ containing $\mathcal{O}_{q+2} = \{N_0, N_1, \ldots, N_{q+1}\}$. Then the set of planes $\{\pi_0, \ldots, \pi_{q+2}\}$ satisfies conditions (†). The hyperovals $\mathcal{O}_i$, $i = 0, \ldots, q+1$, are regular, while the hyperoval $\mathcal{O}_{q+2}$ is projectively equivalent to the dual of $\mathcal{O}^*$. We shall use $\mathcal{E}(\mathcal{O}^*)$ to denote this family of $q+3$ planes and refer to it as the Yoshiara construction using the Veronese map.

The point-residue of a point $\langle \pi_i, P \rangle$ of the extended generalised quadrangle resulting from this construction is isomorphic to the dual of the Tits quadrangle $T_2^*(\mathcal{O}_i)$, $i \in \{0, \ldots, q+2\}$. In particular, if $\mathcal{O}^*$ is a dual regular hyperoval, then the resulting EGQ is the extension of the dual of $T_2^*(\mathcal{O})$, where $\mathcal{O}$ is a regular hyperoval.

In [20], Thas showed that if P is one of the $(q^2 - q)/2$ points of $\mathcal{V}_2^4$ not contained in a plane of $\mathcal{E}(\mathcal{O}^*)$, then P is not contained in any hyperplane spanned by pairs of planes of $\mathcal{E}(\mathcal{O}^*)$. Hence $\mathcal{E}(\mathcal{O}^*)$ admits a points of projection and the resulting EGQ admits a q-fold quotient. □

Example 5.1.2 In [20], Thas constructed another set of $q + 3$ planes satisfying conditions (†) using the Klein correspondence. The Klein correspondence θ maps each line l of $PG(3, q)$ to a point of $PG(5, q)$. If l is the line joining the points (x_0, x_1, x_2, x_3), (y_0, y_1, y_2, y_3), then

$$l^\theta = (l_{01}, l_{02}, l_{03}, l_{12}, l_{31}, l_{23})$$

where $l_{ij} = x_i y_j - x_j y_i$. The image of θ is the set of points on the Klein quadric $x_0 x_5 + x_1 x_4 + x_2 x_3 = 0$. (See [14] for more details.)

Let $\mathcal{K}$ be a $(q + 1)$-arc of $PG(3, q)$, q even and $q > 2$, that is, $\mathcal{K}$ is a set of $q + 1$ points in $PG(3, q)$ no four of which are in a plane. Then $\mathcal{K}$ can be written in the form

$$\{(1, t, t^{2^m}, t^{2^m+1}) \mid t \in GF(q)\} \cup \{(0, 0, 0, 1)\}$$

with $q = 2^h$, $(m, h) = 1$, $1 \leq m \leq h - 1$. Let $\mathcal{K} = \{P_0, \ldots, P_q\}$. Through each point P_i of $\mathcal{K}$ there pass exactly two special unisecants l_i, m_i of $\mathcal{K}$ at P_i such that for each $j \neq i$, the planes $\langle P_j, l_i \rangle$, $\langle P_j, m_i \rangle$ meet $\mathcal{K}$ in only P_i and P_j. The special unisecants can be labelled in such a way that $\{l_0, \ldots, l_q\}$ and $\{m_0, \ldots, m_q\}$ are the systems of generators of a hyperbolic quadric. For each $i \in \{0, \ldots, q\}$, the $q + 2$ points in $PG(5, q)$

$$\begin{aligned} (P_i P_j)^\theta &= P_{ij}, \quad j \in \{0, \ldots, q\} \setminus \{i\}, \\ l_i^\theta &= L_i, \\ m_i^\theta &= M_i \end{aligned}$$

form a hyperoval $\mathcal{O}_i$ of a plane π_i of the Klein quadric. Further, $\{L_0, \ldots, L_q\}$ is a conic $\mathcal{C}_{q+1}$ of some plane π_{q+1} and $\{M_0, \ldots, M_q\}$ is a conic $\mathcal{C}_{q+2}$ of some plane π_{q+2}, and $N = \pi_{q+1} \cap \pi_{q+2}$ is the common nucleus of $\mathcal{C}_{q+1}$ and $\mathcal{C}_{q+2}$. The set of planes $\{\pi_0, \ldots \pi_{q+2}\}$ satisfies conditions (†). The hyperovals $\mathcal{O}_i$, $i = 0, \ldots, q$, are projectively equivalent to

$$\tilde{\mathcal{O}} = \{(1, t, t^{2^m}) \mid t \in GF(q)\} \cup \{(0,0,1), (0,1,0)\},$$

while the hyperovals $\mathcal{C}_{q+1} \cup \{N\}$, $\mathcal{C}_{q+2} \cup \{N\}$ are regular. We shall refer to this as the Thas construction using the Klein map.

The point-residue of a point $\langle \pi_i, P \rangle$, $i \in \{0, \ldots, q\}$, of the EGQ resulting from this construction is isomorphic to the dual of $T_2^*(\tilde{\mathcal{O}})$ while the point-residue of a point $\langle \pi_i, P \rangle$, $i = q+1$ or $q+2$, is isomorphic to $T_2^*(\mathcal{O})$, where $\mathcal{O}$ is a regular hyperoval. This EGQ is isomorphic to that constructed from $\mathcal{E}(\mathcal{O}^*)$ if and only if $\mathcal{O}^*$ is regular and $\mathcal{K}$ is the twisted cubic. It was shown in [20] that the image under θ of an imaginary chord of $\mathcal{K}$ is a point of projection and hence this EGQ also admits a q-fold quotient. □

In the subsequent sections of this chapter we investigate the structure of families of planes satisfying conditions (†). We shall use $\mathcal{E}$ to denote such a family of planes and we shall say that a point or a line belongs to $\mathcal{E}$ if it lies on a plane of $\mathcal{E}$.

In Section 5.2 we give some combinatorial properties of $\mathcal{E}$ and obtain an upper and lower bound on the number of hyperplanes generated by pairs of planes of $\mathcal{E}$ containing a given point.

Section 5.3 describes the intersections of $\mathcal{E}$ with subspaces of $PG(5, q)$ as well as the relation between the subspaces spanned by elements of $\mathcal{E}$ and other subspaces of $PG(5, q)$. We show also that the dual of $\mathcal{E}$ satisfies conditions (†).

Section 5.4 describes a coordinatisation of $\mathcal{E}$. It gives explicit equations of the planes of $\mathcal{E}$ and the hyperplanes spanned by pairs of planes. Using this, we are able to prove necessary and sufficient conditions for a set of o-polynomials to determine $\mathcal{E}$.

In Section 5.5, we examine the Yoshiara construction in detail using the coordinate system described in Section 5.4 and present a new family of $q+3$ planes satisfying

conditions (†) which is the dual of the Yoshiara construction.

In Section 5.6, we examine the Thas construction and show that it is self-dual, and finally, in Section 5.7, we discuss some of the open problems.

5.2 Combinatorial results

We state first some properties of $\mathcal{E}$ which follow immediately from the definition.

By (a), every pair of planes in $\mathcal{E}$ meet in a point and so span a hyperplane. By (b) every three planes in $\mathcal{E}$ meet in the empty set and by (c), span $PG(5,q)$. Thus of the q^2+q+1 hyperplanes through a fixed plane in $\mathcal{E}$, exactly $q+2$ of them contain another plane in $\mathcal{E}$. The remaining q^2-1 hyperplanes must meet each of the other planes in $\mathcal{E}$ in a line. Hence a hyperplane in $PG(5,q)$ meets $\mathcal{E}$ in either 2 planes and $q+1$ lines of $\mathcal{E}$, 1 plane and $q+2$ lines of $\mathcal{E}$ or $q+3$ lines of $\mathcal{E}$. There are $\begin{pmatrix} q+3 \\ 2 \end{pmatrix}$ hyperplanes containing 2 planes of $\mathcal{E}$ and $(q^2-1)(q+3)$ hyperplanes containing 1 plane of $\mathcal{E}$.

Let $\mathcal{H}_\mathcal{E}$ be the set of $\begin{pmatrix} q+3 \\ 2 \end{pmatrix}$ hyperplanes spanned by pairs of planes in $\mathcal{E}$. We classify the points of $PG(5,q)$ according to whether they lie on 0, 1 or 2 planes of $\mathcal{E}$.

There are $\begin{pmatrix} q+3 \\ 2 \end{pmatrix}$ points of $PG(5,q)$ lying on 2 planes of $\mathcal{E}$. These are the points on $\mathcal{O}_i$, $i=0,1,\ldots,q+2$. Every such point lies in $2q+3$ hyperplanes of $\mathcal{H}_\mathcal{E}$ and every hyperplane of $\mathcal{H}_\mathcal{E}$ contains $2q+3$ such points.

There are $(q+3)(q^2-1)$ points of $PG(5,q)$ lying on exactly one plane of $\mathcal{E}$. These are the points of $\pi_i \setminus \mathcal{O}_i$, $i=0,1,\ldots,q+2$. Every such point lies on $3(q+2)/2$ hyperplanes of $\mathcal{H}_\mathcal{E}$ since if P lies on $\pi_i \setminus \mathcal{O}_i$ then P lies in the $q+2$ hyperplanes of $\mathcal{H}_\mathcal{E}$ containing π_i, as well as on the $(q+2)/2$ hyperplanes $\langle \pi_j, \pi_k \rangle$ of $\mathcal{H}_\mathcal{E}$ where the line joining $\pi_j \cap \mathcal{O}_i$ and $\pi_k \cap \mathcal{O}_i$ is a secant of $\mathcal{O}_i$ through P. Every hyperplane $\langle \pi_i, \pi_j \rangle$ of $\mathcal{H}_\mathcal{E}$ contains at most $3(q^2-1)$ such points, with equality only if the $q+1$ lines $\pi_k \cap \langle \pi_i, \pi_j \rangle$, $k \in \{0,1,\ldots,q+2\} \setminus \{i,j\}$, are skew, since

$$|(\pi_i \cup \pi_j) \setminus (\mathcal{O}_i \cup \mathcal{O}_j)| = 2q^2 - 2$$

and each of the $q+1$ lines $\pi_k \cap \langle \pi_i, \pi_j \rangle$ contributes at most $q-1$ points lying on only one plane. By counting the set of flags

$$F = \{(H, P) \mid H \in \mathcal{H}_{\mathcal{E}},\ P \text{ lies on exactly one plane of } \mathcal{E}\}$$

we have

$$(q+3)(q^2-1)\frac{3(q+2)}{2} = |F| \leq \begin{pmatrix} q+3 \\ 2 \end{pmatrix} 3(q^2-1).$$

Since the two sides are equal we conclude that the $q+1$ lines $\pi_k \cap \langle \pi_i, \pi_j \rangle$ are indeed skew and hence every hyperplane of $\mathcal{H}_{\mathcal{E}}$ contains exactly $3(q^2-1)$ points lying on exactly one plane of $\mathcal{E}$.

There are

$$\frac{q^6-1}{q-1} - \begin{pmatrix} q+3 \\ 2 \end{pmatrix} - (q+3)(q^2-1) = q^5 + q^4 - \frac{5}{2}q^2 - \frac{q}{2} + 1$$

points of $PG(5,q)$ not lying on any plane of $\mathcal{E}$ and every hyperplane in $\mathcal{H}_{\mathcal{E}}$ contains

$$\frac{q^5-1}{q-1} - (2q+3) - 3(q^2-1) = (q^2-1)(q^2+q-1)$$

such points. The next result gives an upper and lower bound on the number of hyperplanes in $\mathcal{H}_{\mathcal{E}}$ containing such a point if it lies in a hyperplane of $\mathcal{H}_{\mathcal{E}}$.

Theorem 5.2.1 Let P be a point of $PG(5,q)$ not lying on any plane of $\mathcal{E}$ and let κ_P be the number of hyperplanes of $\mathcal{H}_{\mathcal{E}}$ containing P. If P lies in a hyperplane of $\mathcal{H}_{\mathcal{E}}$ then

$$3 \leq \kappa_P \leq q+3.$$

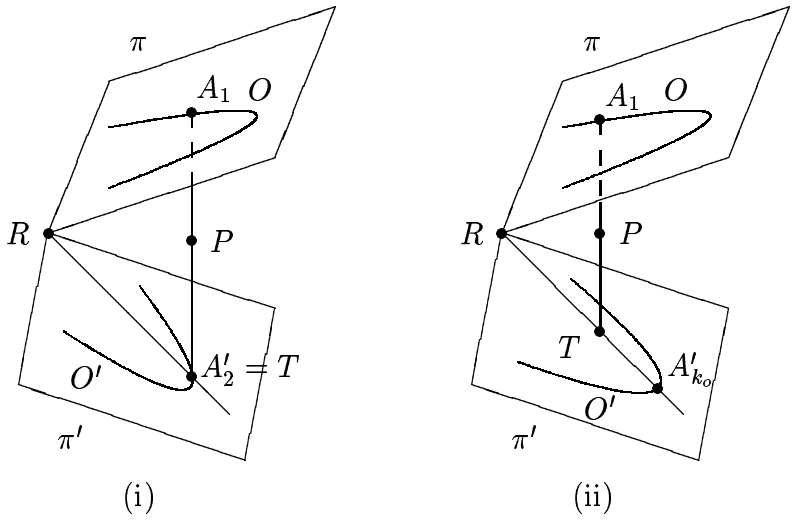
Proof: Firstly we prove that if P lies in the hyperplane $\langle \pi, \pi' \rangle \in \mathcal{H}_{\mathcal{E}}$, then P lies in exactly two hyperplanes of $\mathcal{H}_{\mathcal{E}}$ containing π, one of which is $\langle \pi, \pi' \rangle$.

Let $H = \langle \pi, \pi' \rangle$, $\pi, \pi' \in \mathcal{E}$, be a hyperplane in $\mathcal{H}_{\mathcal{E}}$ containing P, and for $\pi_i \in \mathcal{E} \setminus \{\pi, \pi'\}$, $i = 1, \ldots, q+1$, let $l_i = \pi_i \cap \langle \pi, \pi' \rangle$, $l_i \cap \pi = A_i$ and $l_i \cap \pi' = A_i'$. Let $\mathcal{O} = \{A_1, \ldots, A_{q+1}\}$ and $\mathcal{O}' = \{A_1', \ldots, A_{q+1}'\}$. Every point P in H not on any plane in $\mathcal{E}$ lies on a line joining a point of $\mathcal{O}$ to a point on π'. This is because $\langle \pi', P \rangle$ is a 3-space meeting π in a line l through $\pi \cap \pi'$. Since $\mathcal{O} \cup \{\pi \cap \pi'\}$ is a hyperoval, l must meet $\mathcal{O}$ in another point, say A_i. Since A_i is not on π', $\langle \pi', A_i \rangle$

is a 3-space and so equals $\langle \pi', P \rangle$. Now the points of $\langle \pi', A_i \rangle$ are just the points lying on lines joining A_i to points of π', so P must lie on a line joining A_i to π'. Let $\pi \cap \pi' = R$ and let P lie on a line, say, A_1T, $T \in \pi'$.

There are two possible cases: either T lies on $\mathcal{O}'$, say, $T = A'_2$, $A'_2 \neq A'_1$ (See Figure 5.1(i)), or T does not lie on $\mathcal{O}'$ (See Figure 5.1(ii)).

Figure 5.1: A point P not on any plane of $\mathcal{E}$.



If T lies on $\mathcal{O}'$, then P lies in $\langle \pi, \pi_2 \rangle$ and $\langle \pi', \pi_1 \rangle$ in addition to $\langle \pi, \pi' \rangle$. The remaining hyperplanes $\langle \pi, \pi_k \rangle$, $k \neq 2$, containing π do not contain P, since they contain A_1 but not T.

If T does not lie on $\mathcal{O}'$, then the line RT meets $\mathcal{O}'$ in a point A'_{k_o}. In this case, P lies in $\langle \pi, \pi_{k_o} \rangle$ and $\langle \pi', \pi_1 \rangle$ other than $\langle \pi, \pi' \rangle$. The remaining hyperplanes $\langle \pi, \pi_k \rangle$, $k \neq k_o$, containing π do not contain P since they contain A_1 but not T.

Hence we have shown that P lies in at least three hyperplanes of $\mathcal{H}_\mathcal{E}$, and if P lies in $\langle \pi, \pi' \rangle$, P lies in exactly one more hyperplane in $\mathcal{H}_\mathcal{E}$ containing π other than $\langle \pi, \pi' \rangle$.

Now, for each point P not lying on any plane of $\mathcal{E}$, let G_P be a graph on $q+3$ vertices, one for each plane in $\mathcal{E}$, such that (π_i, π_j) is an edge if and only if $\langle \pi_i, \pi_j \rangle$ contains P. Then, from above, if (π_i, π_j) is an edge then there is exactly one

$\pi_k \neq \pi_j$ such that (π_i, π_k) is an edge. Hence every vertex of G_P has valency either 0 or 2, and G_P has the maximum number $q+3$ of edges when G_P is a disjoint union of cycles with no isolated vertices. This means that P lies in at most $q+3$ hyperplanes of $\mathcal{H}_\mathcal{E}$. □

Let H be a fixed hyperplane in $\mathcal{H}_\mathcal{E}$ and let $\mathcal{P}_H$ be the set of $(q^2-1)(q^2+q-1)$ points in H that do not lie on any plane of $\mathcal{E}$. As before, let κ_P denote the number of hyperplanes in $\mathcal{H}_\mathcal{E}$ containing the point P.

Theorem 5.2.2 (a) $\displaystyle\sum_{P\in\mathcal{P}_H} \kappa_P = \frac{(q+1)(q-1)(q^3+8q^2+8q-6)}{2}.$

(b) $\displaystyle\sum_{P\in\mathcal{P}_H} (\kappa_P-1)(\kappa_P-2) = \frac{(q+1)(q-1)(q^4+11q^3+16q^2-4q-8)}{2}.$

Proof:

(a) We count the set of flags

$$F_1 = \{(P, H') \mid P \in \mathcal{P}_H,\ H' \in \mathcal{H}_\mathcal{E},\ H' \neq H,\ P \in H' \cap H\}.$$

Firstly, for each point P in $\mathcal{P}_H$ there are $\kappa_P - 1$ hyperplanes H' such that P lies in $H' \cap H$, so

$$\begin{aligned} |F_1| &= \sum_{P\in\mathcal{P}_H} (\kappa_P - 1) \\ &= \sum_{P\in\mathcal{P}_H} \kappa_P - |\mathcal{P}_H| \\ &= \sum_{P\in\mathcal{P}_H} \kappa_P - (q^2-1)(q^2+q-1). \end{aligned}$$

On the other hand, there are exactly

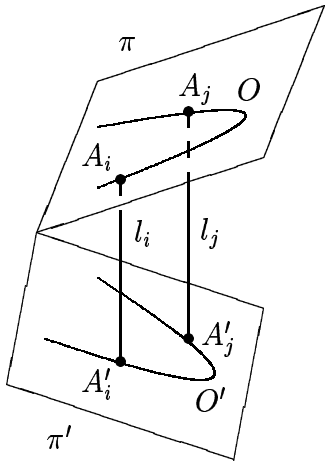
$$|\mathcal{H}_\mathcal{E}| - 1 = \left(\begin{pmatrix} q+3 \\ 2 \end{pmatrix} - 1\right)$$

hyperplanes H' in $\mathcal{H}_\mathcal{E}$ meeting H. If $H = \langle \pi, \pi' \rangle$, then, using the notations from the proof of Theorem 5.2.1,

$$H' \cap H = \langle \pi_i, \pi_j \rangle \cap H = \langle l_i, l_j \rangle$$

for some π_i, $\pi_j \in \mathcal{E} \setminus \{\pi, \pi'\}$. So $H' \cap H$ contains l_i, l_j on $\mathcal{E}$, meets π, π' each in a line, and meets all other l_k in a point. (See Figure 5.2.) Altogether there

Figure 5.2: $H' = \langle l_i, l_j \rangle$.



are $2(q+1) + 2(q-1) + (q-1) = 5q-1$ points in $H' \cap H$ lying on planes of $\mathcal{E}$ and so $H' \cap H$ contains

$$(q^3 + q^2 + q + 1) - (5q - 1) = (q-1)(q^2 + 2q - 2)$$

points of $\mathcal{P}_H$. Hence

$$|F_1| = \left(\begin{bmatrix} q+3 \\ 2 \end{bmatrix} - 1 \right) (q-1)(q^2 + 2q - 2).$$

Combining the two equalities, we have

$$\begin{aligned} \sum_{P \in \mathcal{P}_H} \kappa_P &= \left(\begin{bmatrix} q+3 \\ 2 \end{bmatrix} - 1 \right) (q-1)(q^2 + 2q - 2) + (q^2 - 1)(q^2 + q - 1) \\ &= \frac{(q+1)(q-1)(q^3 + 8q^2 + 8q - 6)}{2}. \end{aligned}$$

(b) We count the set of flags

$$F_2 = \{(P, H_1, H_2) \mid P \in H \cap H_1 \cap H_2,\ H_1,\ H_2 \in \mathcal{H}_\mathcal{E} \setminus \{H\} \text{ and } H_1 \neq H_2\}.$$

Firstly, there are $\left(\begin{bmatrix} q+3 \\ 2 \end{bmatrix} - 1 \right)$ choices for H_1 and $\left(\begin{bmatrix} q+3 \\ 2 \end{bmatrix} - 2 \right)$ choices for H_2. Since $H \cap H_1 \cap H_2$ is a plane,

$$|F_2| = \left(\begin{bmatrix} q+3 \\ 2 \end{bmatrix} - 1 \right) \left(\begin{bmatrix} q+3 \\ 2 \end{bmatrix} - 2 \right) (q^2 + q + 1).$$

On the other hand, there are $(q^5-1)/(q-1)$ points in H, $2q+3$ of which lie on exactly two planes of $\mathcal{E}$, $3(q^2-1)$ of which lie on exactly one plane of $\mathcal{E}$ and the remaining lie on no plane of $\mathcal{E}$. A point lying on two planes of $\mathcal{E}$ is contained in $2q+3$ hyperplanes of $\mathcal{H}_\mathcal{E}$ and a point lying on exactly one plane of $\mathcal{E}$ is contained in $3(q+2)/2$ hyperplanes of $\mathcal{H}_\mathcal{E}$, while a point P not lying on any plane of $\mathcal{E}$ is contained in κ_P hyperplanes of $\mathcal{H}_\mathcal{E}$. Hence

$$\begin{aligned} |F_2| &= (2q+3)(2q+2)(2q+1) + \\ &\quad 3(q^2-1)\left(\frac{3(q+2)}{2}-1\right)\left(\frac{3(q+2)}{2}-2\right) + \sum_{P\in\mathcal{P}_H}(\kappa_P-1)(\kappa_P-2). \end{aligned}$$

Combining the two equalities we have

$$\begin{aligned} \sum_{P\in\mathcal{P}_H}(\kappa_P-1)(\kappa_P-2) &= \left(\begin{pmatrix} q+3 \\ 2 \end{pmatrix}-1\right)\left(\begin{pmatrix} q+3 \\ 2 \end{pmatrix}-2\right)(q^2+q+1) \\ &\quad -(2q+3)(2q+2)(2q+1) \\ &\quad -3(q^2-1)\left(\frac{3(q+2)}{2}-1\right)\left(\frac{3(q+2)}{2}-2\right) \\ &= \frac{(q+1)(q-1)(q^4+11q^3+16q^2-4q-8)}{2}. \end{aligned}$$

□

Since there are $(q^2-1)(q^2+q-1)$ points in H, a point P in H not lying on a plane of $\mathcal{E}$ lies on an average of $\bar{\kappa}_P$ hyperplanes, where

$$\begin{aligned} \bar{\kappa}_P &= \frac{1}{|\mathcal{P}_H|}\sum_{P\in\mathcal{P}_H}\kappa_P \\ &= \frac{q^3+8q^2+8q-6}{2(q^2+q-1)}, \end{aligned}$$

with a variance of σ, where

$$\begin{aligned} \sigma &= \frac{1}{|\mathcal{P}_H|}\sum_{P\in\mathcal{P}_H}(\kappa_P-\bar{\kappa}_P)^2 \\ &= \frac{1}{(q^2-1)(q^2+q-1)}\sum_{P\in\mathcal{P}_H}\left((\kappa_P^2-3\kappa_P+2)+(3-2\bar{\kappa}_P)\kappa_P+(\bar{\kappa}_P^2-2)\right) \\ &= \frac{(q^6+14q^5+18q^4-40q^3-52q^2+20q+8)}{4(q^2+q-1)^2}. \end{aligned}$$

Hence if P is a point not on any plane of $\mathcal{E}$ and P is contained in a hyperplane of $\mathcal{H}_\mathcal{E}$, then P lies in about $q/2$ hyperplanes of $\mathcal{H}_\mathcal{E}$, with a variance of about $q^2/4$ and

hence a standard deviation of about $q/2$. This indicates that it is possible that κ_P does reach the upper bound of Theorem 5.2.1.

Now, consider the sum of κ_P over all the points of $PG(5,q)$ not on a plane of $\mathcal{E}$. Then, for each such point P, either $\kappa_P = 0$ or $3 \leq \kappa_P \leq q+3$ by Theorem 5.2.1. Counting the flags

$$\begin{aligned} F_1' &= \{(P,H) \mid P \in PG(5,q) \setminus \mathcal{E},\ H \in \mathcal{H}_{\mathcal{E}},\ P \in H\}, \\ F_2' &= \{(P,H_1,H_2) \mid P \in PG(5,q) \setminus \mathcal{E},\ H_1, H_2 \in \mathcal{H}_{\mathcal{E}},\ P \in H_1 \cap H_2\}, \end{aligned}$$

we have

$$\begin{aligned} \sum_{P \in PG(5,q)\setminus\mathcal{E}} \kappa_P &= \begin{pmatrix} q+3 \\ 2 \end{pmatrix} (q^2-1)(q^2+q-1), \\ \sum_{P \in PG(5,q)\setminus\mathcal{E}} \kappa_P(\kappa_P - 1) &= \begin{pmatrix} q+3 \\ 2 \end{pmatrix} \left(\begin{pmatrix} q+3 \\ 2 \end{pmatrix} - 1 \right) (q-1)(q^2+2q-2). \end{aligned}$$

Using these two equations, the average $\bar{\kappa}_P$ and variance σ in this case are

$$\begin{aligned} \bar{\kappa}_P &= \frac{1}{q^5+q^4-\frac{5}{2}q^2-\frac{1}{2}q+1} \begin{pmatrix} q+3 \\ 2 \end{pmatrix} (q^2-1)(q^2+q-1) \\ &= \frac{(q^2+q-1)(q+3)(q+2)(q+1)}{2q^4+4q^3+4q^2-q-2}, \\ \sigma &= \frac{1}{q^5+q^4-\frac{5}{2}q^2-\frac{1}{2}q+1} \sum_{P \in PG(5,q)\setminus\mathcal{E}} (\kappa_P - \bar{\kappa_P})^2 \\ &= \frac{1}{q^5+q^4-\frac{5}{2}q^2-\frac{1}{2}q+1} \sum_{P \in PG(5,q)\setminus\mathcal{E}} \kappa_P(\kappa_P-1) + (1-2\bar{\kappa}_P)\kappa_P + \bar{\kappa}_P^2 \\ &= \frac{(q+3)(q+2)(q+1)(4q^6+8q^5+3q^4+2q^3-20q^2-4q+8)}{4(2q^4+4q^3+4q^2-q-2)^2}. \end{aligned}$$

Hence, if every point of $PG(5,q)$ not lying on a plane of $\mathcal{E}$ is contained in a hyperplane of $\mathcal{H}_{\mathcal{E}}$, then it lies on an average of about $q/2$ hyperplanes with a variance of about $q/2$.

We had hoped that if we could show that every point not lying on any plane of $\mathcal{E}$ lies on at least $aq+b$ hyperplanes of $\mathcal{H}_{\mathcal{E}}$ with $a > 1/2$, then we could show by contradiction that a point of projection exists by counting the flags

$$F = \{(P,H) \mid P \in PG(5,q) \setminus \mathcal{E},\ H \in \mathcal{H}_{\mathcal{E}},\ P \in H\}$$

and obtaining

$$|F| = \begin{pmatrix} q+3 \\ 2 \end{pmatrix} (q^2-1)(q^2+q-1) \geq (q^5+q^4-\frac{5}{2}q^2-\frac{q}{2}+1)(aq+b).$$

This inequality would show a contradiction if $a > 1/2$. However, as the above result shows, the average number of hyperplanes of $\mathcal{H}_{\mathcal{E}}$ containing a point is about $q/2$, so that this counting argument does not give us an indication as to the existance of a point of projection.

In the next section we consider the intersections of $\mathcal{E}$ with subspaces of $PG(5,q)$.

5.3 Intersections of $\mathcal{E}$ with subspaces of $PG(5,q)$

We show first an elementary property about the set of intersection points of pairs of planes in $\mathcal{E}$:

Theorem 5.3.1 Let $\mathcal{O} = \bigcup_{i=0}^{q+2} \mathcal{O}_i$. Then $\mathcal{O}$ is a $\frac{(q+2)(q+3)}{2}$-cap in $PG(5,q)$.

Proof: Since every pair of planes in $\mathcal{E}$ meet in a unique point, and there are $\begin{pmatrix} q+3 \\ 2 \end{pmatrix}$ pair of planes, we have

$$|\mathcal{O}| = \begin{pmatrix} q+3 \\ 2 \end{pmatrix} = \frac{(q+2)(q+3)}{2}.$$

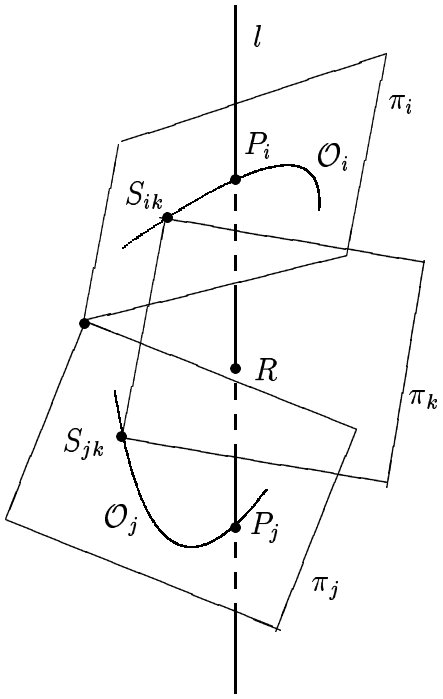
Let l be any line of $PG(5,q)$. If l lies on some plane π_i of $\mathcal{E}$, then l meets $\mathcal{O}$ in either exactly 2 points of $\mathcal{O}_i$ or none at all.

Suppose then that l does not lie on any plane of $\mathcal{E}$ and suppose that l meets $\mathcal{O}$ in 2 points lying on 2 distinct planes, say $P_i \in \mathcal{O}_i$ on π_i, and $P_j \in \mathcal{O}_j$ on π_j, $i \neq j$. We show that l does not contain a third point of $\mathcal{O}$.

Suppose on the contrary that l meets $\mathcal{O}$ in a third point, say $R \in \mathcal{O}_k$ on π_k. Let $\pi_k \cap \pi_i = S_{ik}$ and $\pi_k \cap \pi_j = S_{jk}$ (See Figure 5.3).

Since l does not lie on any plane of $\mathcal{E}$, $P_i \neq S_{ik}$ and $P_j \neq S_{jk}$, for otherwise l would lie on π_k.

Figure 5.3: l does not lie on any plane of $\mathcal{E}$.



If $P_i \neq S_{ik}$ and $P_j \neq S_{jk}$, then π_k meets $\langle \pi_i, \pi_j \rangle$ in the line $\langle S_{ik}, S_{jk} \rangle$ and the point R not on $\langle S_{ik}, S_{jk} \rangle$. Hence $\pi_k \subseteq \langle \pi_i, \pi_j \rangle$ which is again a contradiction. Hence every line of $PG(5, q)$ meets $\mathcal{O}$ in at most two points. □

We show next that any dual of $\mathcal{E}$ satisfies conditions (†):

Let $\mathcal{E}'$ be a dual of $\mathcal{E}$, that is, $\mathcal{E}'$ is a set of $q+3$ planes $\{\pi'_0, \ldots, \pi'_{q+2}\}$ such that

(a′) Every pair of planes π'_i, π'_j in $\mathcal{E}'$ span a hyperplane;

(b′) For each $i \in \{0, \ldots, q+2\}$, the set $\mathcal{O}'_i = \{\langle \pi'_i, \pi'_j \rangle \mid j \in \{0, \ldots, q+2\} \setminus \{i\}\}$ is a dual hyperoval containing π_i, that is, a set of $q+2$ hyperplanes containing π_i such that no three have a 3-space in common;

(c′) the intersection of the planes in $\mathcal{E}'$ is the empty space.

Theorem 5.3.2 The dual $\mathcal{E}'$ of $\mathcal{E}$ satisfies conditions (†).

Proof: Firstly, condition (a) of (†) follows from condition (a′) since

$$\dim\,(\pi_i' \cap \pi_j') = \dim\,\pi_i' + \dim\,\pi_j' - \dim\,(\langle \pi_i', \pi_j' \rangle) = 2 + 2 - 4 = 0,$$

so $\pi_i' \cap \pi_j'$ is a point.

To prove condition (c) of (†), we show that every 3 planes in $\mathcal{E}'$ span $PG(5,q)$. Suppose that there are 3 planes π_i', π_j', π_k' in $\mathcal{E}'$ spanning a hyperplane. Then $\langle \pi_i', \pi_j' \rangle = \langle \pi_i', \pi_k' \rangle$, but by (b′), they are supposed to be distinct. Hence the planes of $\mathcal{E}'$ span $PG(5,q)$.

To prove condition (b) of (†), we first show that for any fixed i, $\pi_i' \cap \pi_j'$, $j \in \{0, \ldots, q+2\} \setminus \{i\}$, are distinct points.

Suppose that $\pi_i' \cap \pi_j' = \pi_i' \cap \pi_k' = P$ for some point P on π_i' and $j \neq k$. Let $\pi_h' \in \mathcal{E}' \setminus \{\pi_i', \pi_j', \pi_k'\}$. Then by (a), π_h' meets π_i', π_j' and π_k' each in exactly one point, so we have either π_h' meets π_i', π_j' and π_k' in three distinct points or in the same point P. In the first case, we have

$$\begin{aligned} \langle \pi_h', \pi_i' \rangle \cap \langle \pi_h', \pi_j' \rangle &= \langle \pi_h', \pi_i' \cap \pi_j' \rangle = \langle \pi_h', P \rangle, \\ \langle \pi_h', \pi_i' \rangle \cap \langle \pi_h', \pi_k' \rangle &= \langle \pi_h', \pi_i' \cap \pi_k' \rangle = \langle \pi_h', P \rangle, \end{aligned}$$

so the three hyperplanes $\langle \pi_h', \pi_i' \rangle$, $\langle \pi_h', \pi_j' \rangle$ and $\langle \pi_h', \pi_k' \rangle$ all contain the 3-space $\langle \pi_h', P \rangle$, which contradicts (b′). So we must have the second case. However, since π_h' is arbitrary, every plane in $\mathcal{E}'$ meets in the point P, which contradicts (c′). This proves that pairs of planes meet in distinct points.

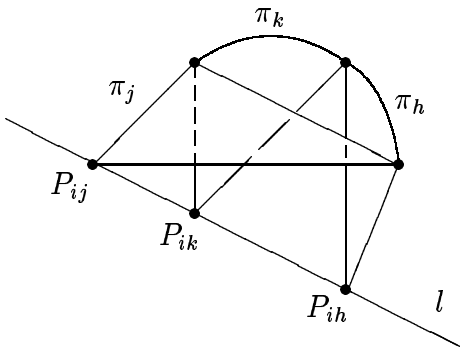
Let $\pi_i' \cap \pi_j' = P_{ij}$, $\pi_i' \cap \pi_k' = P_{ik}$, $\pi_i' \cap \pi_h' = P_{ih}$. We show that P_{ij}, P_{ik}, P_{ih} are not collinear. Suppose on the contrary that P_{ij}, P_{ik} and P_{ih} lie on a line l on π_i' (See Figure 5.4). From above, P_{ij}, P_{ik} and P_{ih} are distinct, and π_h' meets π_j' and π_k' each in a distinct point. Then,

$$\begin{aligned} \langle \pi_j', \pi_i' \rangle \cap \langle \pi_j', \pi_k' \rangle &= \langle \pi_j', P_{ik} \rangle = \langle \pi_j', l \rangle, \\ \langle \pi_j', \pi_i' \rangle \cap \langle \pi_j', \pi_h' \rangle &= \langle \pi_j', P_{ih} \rangle = \langle \pi_j', l \rangle. \end{aligned}$$

This means that $\langle \pi_j', \pi_i' \rangle$, $\langle \pi_j', \pi_k' \rangle$ and $\langle \pi_j', \pi_h' \rangle$ contain a 3-space $\langle \pi_j', l \rangle$, which contradicts condition (b′). This proves condition (b) of (†). □

Corollary 5.3.3 The set of $q+3$ plane $\mathcal{E}$ satisfies conditions (a′), (b′) and (c′). □

Figure 5.4: P_{ij}, P_{ik} and P_{ih} collinear.



As a corollary of Theorems 5.3.1 and 5.3.2, we have

Corollary 5.3.4 The hyperplanes $\langle \pi_i, \pi_j \rangle$, $\pi_i, \pi_j \in \mathcal{E}$, form a dual cap in $PG(5, q)$. □

The following result describes how the $q + 2$ hyperplanes generated by π_0 and π_i, $\pi_i \in \mathcal{E} \setminus \{\pi_0\}$, intersect a plane π disjoint from π_0:

Theorem 5.3.5 Let π_0 be a fixed plane in $\mathcal{E}$. Let π be a plane in $PG(5, q)$ skew to π_0, and let $\mathcal{H}_i = \langle \pi_i, \pi_o \rangle$, $i = 1, \ldots, q + 2$. Let $\mathcal{L} = \{\mathcal{H}_i \cap \pi = l_i \mid i = 1, \ldots, q + 2\}$. Then,

(a) At most 3 lines of $\mathcal{L}$ lie on a plane of $\mathcal{E}$.

(b) If exactly 3 lines of $\mathcal{L}$ lie on planes of $\mathcal{E}$ then no other plane in $\mathcal{E}$ meets π.

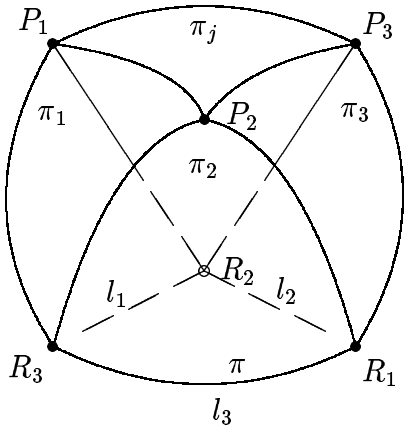
(c) The set $\mathcal{L}$ contains $q + 2$ distinct lines.

(d) The set of lines of $\mathcal{L}$ forms a dual hyperoval in π.

Proof:

(a) Suppose not. Without loss of genarality, let l_1, l_2, l_3, l_4 be 4 lines of $\mathcal{L}$ lying on π_1, π_2, π_3 and π_4 respectively. Then l_1, l_2, l_3, l_4 are lines of the plane π

Figure 5.5: $\langle P_1R_3, P_2R_2, P_3R_1\rangle = PG(5,q)$.



and must therefore pairwise intersect. Since l_i belongs to π_i, l_i meets another line l_j only in the point where π_i meets π_j. Consider l_1:

$$l_1 \cap l_j = \pi_1 \cap \pi_j \in \mathcal{O}_1 \text{ for } j = 2,3,4,$$

which contradicts the fact that $\mathcal{O}_1$ is a hyperoval. Hence there are at most 3 lines of $\mathcal{L}$ that lie on a plane of $\mathcal{E}$.

(b) Let π_1, π_2 and π_3 be the three planes such that $\pi_i \cap \pi = l_i$, $i = 1,2,3$. Let π_j be a plane of $\mathcal{E}$, $j \neq 1,2,3$. We show that $\langle \pi, \pi_j\rangle$ is $PG(5,q)$ and hence $\pi_j \cap \pi = \emptyset$.

Let $P_i = \pi_j \cap \pi_i$, $i = 1,2,3$, and let

$$\begin{aligned} \pi_1 \cap \pi_2 &= R_3, \\ \pi_1 \cap \pi_3 &= R_2, \\ \pi_2 \cap \pi_3 &= R_1. \end{aligned}$$

(See Figure 5.5.) We show that $\langle P_1R_3, P_2R_2, P_3R_1\rangle$ is $PG(5,q)$ and since it is contained in $\langle \pi, \pi_j\rangle$, this shows that $\langle \pi, \pi_j\rangle = PG(5,q)$.

The space spanned by the two lines P_1R_3 and P_2R_2 is a 3-space $\langle \pi_1, P_2\rangle$. Consider then $P_3R_1 \cap \langle \pi_1, P_2\rangle$:

If P_3R_1 lies in $\langle \pi_1, P_2 \rangle$ then the 3-space $\langle \pi_1, P_2 \rangle$ contains π_3 and π_1, which contradicts the property that every pair of planes in $\mathcal{E}$ spans a hyperplane.

If P_3R_1 meets $\langle \pi_1, P_2 \rangle$ in some point X on π_3 then $\langle \pi_1, P_2 \rangle$ contains the points X, R_2 of π_3. This means that π_3 meets $\langle \pi_1, P_2 \rangle$ in a line and so $\langle \pi_3, \pi_1, P_2 \rangle$ is a hyperplane. But then $\langle \pi_3, \pi_1, P_2 \rangle$ contains the three non-collinear points P_2, R_1 and R_3 of π_2 and hence contains π_2, which contradicts the property that every 3 planes span $PG(5, q)$.

Hence we conclude that $P_3R_1 \cap \langle \pi_1, P_2 \rangle = \emptyset$ and $\langle \pi_j, \pi \rangle = PG(5, q)$.

(c) Suppose without loss of generality that l_1, l_2 are not distinct, that is,

$$\langle \pi_0, \pi_1 \rangle \cap \pi = \langle \pi_0, \pi_2 \rangle \cap \pi = l.$$

Then

$$\langle \pi_0, \pi_1 \rangle = \langle \pi_0, \pi_2 \rangle = \langle \pi_0, l \rangle$$

and $\langle \pi_0, l \rangle$ is a hyperplane containing π_0, π_1 and π_2, which contradicts the property that every 3 planes span $PG(5, q)$.

(d) For convenience, we call a line in $\mathcal{L}$ "real" if it lies on some $\pi_i \in \mathcal{E}$ and "imaginary" otherwise. In (c) we showed that $\mathcal{L}$ is a set of $q + 2$ distinct lines of π. In (a) we showed that three "real" lines cannot be concurrent. We shall show in the following that no three lines, "real" or otherwise, can be concurrent.

- An "imaginary" line is not concurrent with two "real" lines:
  Let $l_1 = \langle \pi_1, \pi_0 \rangle \cap \pi$ be an "imaginary" line and let $l_2 = \pi_2 \cap \pi$ and $l_3 = \pi_3 \cap \pi$ be two "real" lines. Suppose that l_1, l_2 and l_3 are concurrent in a point R. Then the hyperplane $\langle \pi_0, \pi_1 \rangle$ contains

  1. l_1 and hence the point $\pi_2 \cap \pi_3 = R$ of π_3,
  2. the point $\pi_0 \cap \pi_3$ of π_3, and
  3. the point $\pi_1 \cap \pi_3$ of π_3.

  Since the three points are not collinear, $\langle \pi_0, \pi_1 \rangle$ contains π_3 which contradicts the property that every 3 planes span $PG(5, q)$.

- A "real" line is not concurrent with two "imaginary" lines:
  Let $l_1 = \langle \pi_1, \pi_0 \rangle \cap \pi$, $l_2 = \pi_2 \cap \pi$ and $l_3 = \langle \pi_3, \pi_0 \rangle \cap \pi$, with l_1 and l_3 "imaginary". Suppose that l_1, l_2 and l_3 are concurrent in a point R. Let $P_i = \pi_0 \cap \pi_i$ and let $\pi_1 \cap \pi_2 = R_3$, $\pi_1 \cap \pi_3 = R_2$, and $\pi_2 \cap \pi_3 = R_1$. Then the hyperplane $\langle \pi_0, \pi_1 \rangle$ contains the points R, P_2 and R_3 of π_2, so R, P_2 and R_3 must be collinear. On the other hand, the hyperplane $\langle \pi_0, \pi_3 \rangle$ contains the points R, P_2 and R_1 of π_2, so R, P_2 and R_1 must be collinear. This implies that P_2, R_3 and R_1 are collinear, which is impossible since they lie on a hyperoval on π_2.

- No three "imaginary" lines are concurrent:
  Let $l_i = \langle \pi_0, \pi_i \rangle \cap \pi$, $i = 1, 2, 3$, be "imaginary" lines and suppose that l_1, l_2 and l_3 are concurrent at a point R. Let $P_i = \pi_0 \cap \pi_i$ and let $\pi_1 \cap \pi_2 = R_3$, $\pi_1 \cap \pi_3 = R_2$, and $\pi_2 \cap \pi_3 = R_1$. Then,

  $$\langle \pi_0, \pi_3 \rangle \cap \langle \pi_0, \pi_2 \rangle = \langle \pi_0, l_3 \rangle \cap \langle \pi_0, l_2 \rangle = \langle \pi_0, R \rangle, \text{ and contains } R_1,$$

  and

  $$\langle \pi_0, \pi_1 \rangle \cap \langle \pi_0, \pi_2 \rangle = \langle \pi_0, l_1 \rangle \cap \langle \pi_0, l_2 \rangle = \langle \pi_0, R \rangle, \text{ and contains } R_3.$$

  Hence $\langle \pi_0, R \rangle$ is a 3-space which contains the three non-collinear points R_1, R_3 and P_2 of π_2, that is, $\langle \pi_0, R \rangle$ contains π_2. This contradicts the property that every pair of planes spans a hyperplane. □

The next two results describe the intersections of $\mathcal{E}$ with hyperplanes of $PG(5, q)$. Theorem 5.3.6 gives another proof that the lines $\pi_k \cap \langle \pi_i, \pi_j \rangle$, $k \in \{0, 1, \ldots, q+2\} \setminus \{i, j\}$, are mutually skew.

Theorem 5.3.6 Let $\mathcal{H}$ be a hyperplane intersecting $\mathcal{E}$ in 2 planes, say, π_0 and π_1. Let $\mathcal{L} = \{\pi_i \cap \mathcal{H} = l_i \mid i = 2, \ldots, q+2\}$. Then $\mathcal{L}$ is a set of $q+1$ mutually skew lines.

Proof: Any two lines l_j, l_k in $\mathcal{L}$ can meet only in the point $\pi_j \cap \pi_k$. Since l_j already contains two points of $\mathcal{O}_j$ on π_j (the points $\pi_j \cap \pi_0$ and $\pi_j \cap \pi_1$), it does not meet l_k. □

Theorem 5.3.7 Let $\mathcal{H}$ be a hyperplane intersecting $\mathcal{E}$ in exactly one plane, say π_{q+2}. Then $\mathcal{H}$ meets $\{\pi_0, \ldots, \pi_{q+1}\}$ in $q+2$ lines, every one of these lines meeting exactly one other line in a point, this point being $\mathcal{O}_i \cap \mathcal{O}_j$ for some i, j.

Proof: Every plane in $\mathcal{E}$ not in $\mathcal{H}$ meets $\mathcal{H}$ in a line. If $l_i = \pi_i \cap \mathcal{H}$, $i \neq q+2$, then l_i lies on π_i and meets $\mathcal{O}_i$ in the point $\pi_i \cap \pi_{q+2}$. Since $\mathcal{O}_i$ is a hyperoval, l_i must meet $\mathcal{O}_i$ in another point, which is the intersection of π_i with another plane π_j of $\mathcal{E}$ and so belongs to another of the $q+2$ lines. □

5.4 Coordinatisation of $\mathcal{E}$

It was shown in [15] that every hyperoval in $PG(2,q)$ can be written in the form

$$\{(F(x), x, 1) \mid x \in GF(q)\} \cup \{(1,0,0), (0,1,0)\}$$

with $F(0) = 0$, $F(1) = 1$ and such that F and F_s are permutations, where

$$F_s(x) = \frac{F(x+s) + F(s)}{x}, \quad s \in GF(q).$$

We call such a permutation F an o-polynomial. We show below that $\mathcal{E}$ can be coordinatised using o-polynomials:

Let π_1, π_2, π_3 be three arbitary planes of $\mathcal{E}$. Since we may choose any seven independent points in $PG(5,q)$ as fundamental points, we choose

$$\begin{aligned} \pi_1 \cap \pi_3 &= (1,0,0,0,0,0), \\ \pi_1 \cap \pi_2 &= (0,1,0,0,0,0), \\ \pi_2 \cap \pi_3 &= (0,0,1,0,0,0). \end{aligned}$$

We show that the remaining fundamental points may be chosen so that the hyperovals $\mathcal{O}_1$, $\mathcal{O}_2$, $\mathcal{O}_3$ on π_1, π_2, π_3 respectively may be written as

$$\begin{aligned} \mathcal{O}_1 &= \{A_x = (f(x), x, 0, 1, 0, 0)\} \cup \{(1,0,0,0,0,0), (0,1,0,0,0,0)\}, \\ \mathcal{O}_2 &= \{B_x = (0, g(\alpha(x)), \alpha(x), 0, 1, 0)\} \cup \{(0,1,0,0,0,0), (0,0,1,0,0,0)\}, \\ \mathcal{O}_3 &= \{C_x = (\beta(x), 0, h(\beta(x)), 0, 0, 1)\} \cup \{(1,0,0,0,0,0), (0,0,1,0,0,0)\}, \end{aligned}$$

where f, g, h are o-polynomials and α, β are permutations of $GF(q)$ such that for each $x \in GF(q)$,

$$\pi(x) = \langle A_x, B_x, C_x \rangle \in \mathcal{E}.$$

So $\mathcal{E} = \{\pi_1, \pi_2, \pi_3, \pi(x) \mid x \in GF(q)\}$.

(Note that by saying that f, g, h are o-polynomials, we are claiming that $f(0) = g(0) = h(0) = 0$ and $f(1) = g(1) = h(1) = 1$. We shall see in the following that the remaining fundamental points can be chosen so that this is indeed the case.)

We may choose

$$\begin{aligned} \pi_1 \cap \pi(0) &= (0,0,0,1,0,0), \\ \pi_2 \cap \pi(0) &= (0,0,0,0,1,0), \\ \pi_3 \cap \pi(0) &= (0,0,0,0,0,1) \end{aligned}$$

and so we may let $f(0) = g(0) = h(0) = \alpha(0) = \beta(0) = 0$.

Finally we may choose the seventh point $(1,1,1,1,1,1)$ to be a point on the line

$$\begin{aligned} l \;:\; & \langle \pi_2 \cap \pi(1), (1,0,0,0,0,0), (0,0,0,1,0,0), (0,0,0,0,0,1) \rangle \cap \\ & \langle \pi_3 \cap \pi(1), (0,1,0,0,0,0), (0,0,0,1,0,0), (0,0,0,0,1,0) \rangle. \end{aligned}$$

A point on $l \setminus \{(0,0,0,1,0,0)\}$ has the form

$$(\beta(1), \frac{h(\beta(1))g(\alpha(1))}{\alpha(1)}, h(\beta(1)), 0, \frac{h(\beta(1))}{\alpha(1)}, 1) + \lambda(0,0,0,1,0,0), \ \lambda \in GF(q),$$

so we may take $\beta(1) = h(1) = \alpha(1) = g(1) = 1$.

The o-polynomials f, g, h and the permutations α, β are related by the following equation:

Theorem 5.4.1 If $\mathcal{E}$ is coordinatised as above with o-polynomials f, g, h and permutations α, β, then for all $x, y \in GF(q)$, $x \neq y$,

$$\frac{(\, f(x) + f(y)\,)(\, g(\alpha(x)) + g(\alpha(y))\,)(\, h(\beta(x)) + h(\beta(y))\,)}{(\, x + y\,)(\, \alpha(x) + \alpha(y)\,)(\, \beta(x) + \beta(y)\,)} = 1.$$

Proof: Since every pair of planes $\pi(x)$, $\pi(y)$, spans a hyperplane, we have

$$\begin{vmatrix} f(x) & x & 0 & 1 & 0 & 0 \\ 0 & g(\alpha(x)) & \alpha(x) & 0 & 1 & 0 \\ \beta(x) & 0 & h(\beta(x)) & 0 & 0 & 1 \\ f(y) & y & 0 & 1 & 0 & 0 \\ 0 & g(\alpha(y)) & \alpha(y) & 0 & 1 & 0 \\ \beta(y) & 0 & h(\beta(y)) & 0 & 0 & 1 \end{vmatrix} = 0.$$

Adding row 1 to row 4, row 2 to row 5 and row 3 to row 6, we have

$$\begin{vmatrix} f(x) & x & 0 & 1 & 0 & 0 \\ 0 & g(\alpha(x)) & \alpha(x) & 0 & 1 & 0 \\ \beta(x) & 0 & h(\beta(x)) & 0 & 0 & 1 \\ f(x)+f(y) & x+y & 0 & 0 & 0 & 0 \\ 0 & g(\alpha(x))+g(\alpha(y)) & \alpha(x)+\alpha(y) & 0 & 0 & 0 \\ \beta(x)+\beta(y) & 0 & h(\beta(x))+h(\beta(y)) & 0 & 0 & 0 \end{vmatrix} = 0,$$

and expanding along the last column we have

$$\begin{vmatrix} f(x)+f(y) & x+y & 0 \\ 0 & g(\alpha(x))+g(\alpha(y)) & \alpha(x)+\alpha(y) \\ \beta(x)+\beta(y) & 0 & h(\beta(x))+h(\beta(y)) \end{vmatrix} = 0,$$

which gives the required equation. □

Using the equation of Theorem 5.4.1, putting $x = 1$, $y = 0$, we see that indeed $f(1) = 1$.

The equations of the planes in $\mathcal{E}$ are

$$\begin{aligned} \pi_1 &: x_2 = x_4 = x_5 = 0; \\ \pi_2 &: x_0 = x_3 = x_5 = 0; \\ \pi_3 &: x_1 = x_3 = x_4 = 0; \\ \pi(x) &: x_0 + f(x)x_3 + \beta(x)x_5 = 0, \\ &\quad x_1 + xx_3 + g(\alpha(x))x_4 = 0, \\ &\quad x_2 + \alpha(x)x_4 + h(\beta(x))x_5 = 0. \end{aligned}$$

Let $x,\ y \in GF(q),\ x \neq y$. The equations for $\pi_i \cap \pi(x),\ i = 1,2,3$, and $\pi(x) \cap \pi(y)$ are as follows:

$$\begin{aligned}
\pi_1 \cap \pi(x) &= (f(x), x, 0, 1, 0, 0) = A_x, \\
\pi_2 \cap \pi(x) &= (0, g(\alpha(x)), \alpha(x), 0, 1, 0) = B_x, \\
\pi_3 \cap \pi(x) &= (\beta(x), 0, h(\beta(x)), 0, 0, 1) = C_x, \\
\pi(x) \cap \pi(y) &= \\
&\left(f(x)\frac{g(\alpha(x)) + g(\alpha(y))}{x+y} + \beta(x)\frac{(\,f(x)+f(y)\,)(\,g(\alpha(x))+g(\alpha(y))\,)}{(\,x+y\,)(\,\beta(x)+\beta(y)\,)}, \right. \\
&\quad x\,\frac{g(\alpha(x)) + g(\alpha(y))}{x+y} + g(\alpha(x)), \\
&\quad \alpha(x) + h(\beta(x))\frac{(\,f(x)+f(y)\,)(\,g(\alpha(x))+g(\alpha(y))\,)}{(\,x+y\,)(\,\beta(x)+\beta(y)\,)}, \\
&\quad \left. \frac{g(\alpha(x)) + g(\alpha(y))}{x+y},\ 1,\ \frac{(\,f(x)+f(y)\,)(\,g(\alpha(x))+g(\alpha(y))\,)}{(\,x+y\,)(\,\beta(x)+\beta(y)\,)} \right).
\end{aligned}$$

Hence we have, in terms of $A_x,\ B_x,\ C_x$,

$$\pi(x) \cap \pi(y) = \frac{g(\alpha(x)) + g(\alpha(y))}{x+y}A_x + B_x + \frac{(\,f(x)+f(y)\,)(\,g(\alpha(x))+g(\alpha(y))\,)}{(\,\beta(x)+\beta(y)\,)(\,x+y\,)}C_x.$$

For any $\pi(x) \in \mathcal{E}$, the points $\pi(x) \cap \pi(y),\ y \in GF(q) \setminus \{x\}$, together with $\pi(x) \cap \pi_i$, $i = 1,2,3$, form a hyperoval on $\pi(x)$. Hence, if σ_x is the permutation of $GF(q)$ with

$$\sigma_x\ :\ \frac{g(\alpha(x)) + g(\alpha(y))}{x+y}\ \mapsto\ \frac{(\,f(x)+f(y)\,)(\,g(\alpha(x))+g(\alpha(y))\,)}{(\,\beta(x)+\beta(y)\,)(\,x+y\,)}$$

and $\sigma_x(0) = 0$, then σ_x defines a hyperoval on $\pi(x)$. We normalise σ_x as follows to obtain an o-polynomial σ_x^*: Let y_x be the element of $GF(q) \setminus \{x\}$ such that

$$\frac{g(\alpha(x)) + g(\alpha(y_x))}{x+y_x} = 1.$$

We define σ_x^* as the permutation of $GF(q)$ obtained from σ_x by dividing σ_x with the constant $(f(x)+f(y_x))/(\beta(x)+\beta(y_x))$:

$$\sigma_x^*\ :\ \frac{g(\alpha(x)) + g(\alpha(y))}{x+y}\ \mapsto\ \frac{(\,f(x)+f(y)\,)(\,g(\alpha(x))+g(\alpha(y))\,)}{(\,\beta(x)+\beta(y)\,)(\,x+y\,)} \cdot \frac{\beta(x)+\beta(y_x)}{f(x)+f(y_x)}.$$

Then σ^* defines a hyperoval, with $\sigma_x^*(0) = 0$, $\sigma_x^*(1) = 1$, so σ_x^* is an o-polynomial.

Dually, the equations for $\langle \pi_i, \pi(x) \rangle$, $i = 1, 2, 3$, and $\langle \pi(x), \pi(y) \rangle$, $x, y \in GF(q)$, $x \neq y$, are

$$\begin{aligned}
\langle \pi_2, \pi(x) \rangle &= [1, 0, 0, f(x), 0, \beta(x)], \\
\langle \pi_3, \pi(x) \rangle &= [0, 1, 0, x, g(\alpha(x)), 0], \\
\langle \pi_1, \pi(x) \rangle &= [0, 0, 1, 0, \alpha(x), h(\beta(x))], \\
\langle \pi(x), \pi(y) \rangle &= \Bigg[\frac{(\, g(\alpha(x)) + g(\alpha(y))\,)(\, h(\beta(x)) + h(\beta(y))\,)}{(\, \alpha(x) + \alpha(y)\,)(\, \beta(x) + \beta(y)\,)}, \\
&\quad 1, \frac{(\, g(\alpha(x)) + g(\alpha(y))\,)}{(\, \alpha(x) + \alpha(y)\,)}, \\
&\quad f(x)\frac{(\, g(\alpha(x)) + g(\alpha(y))\,)(\, h(\beta(x)) + h(\beta(y))\,)}{(\, \alpha(x) + \alpha(y)\,)(\, \beta(x) + \beta(y)\,)} + x, \\
&\quad \alpha(x)\frac{(\, g(\alpha(x)) + g(\alpha(y))\,)}{(\, \alpha(x) + \alpha(y)\,)} + g(\alpha(x)), \\
&\quad \beta(x)\frac{(\, g(\alpha(x)) + g(\alpha(y))\,)(\, h(\beta(x)) + h(\beta(y))\,)}{(\, \alpha(x) + \alpha(y)\,)(\, \beta(x) + \beta(y)\,)} + \\
&\quad h(\beta(x))\frac{(\, g(\alpha(x)) + g(\alpha(y))\,)}{(\, \alpha(x) + \alpha(y)\,)} \Bigg].
\end{aligned}$$

Let $L_x = \langle \pi_2, \pi(x) \rangle$, $M_x = \langle \pi_3, \pi(x) \rangle$ and $N_x = \langle \pi_1, \pi(x) \rangle$. Then, in terms of L_x, M_x and N_x,

$$\begin{aligned}
\langle \pi(x), \pi(y) \rangle &= \frac{(\, g(\alpha(x)) + g(\alpha(y))\,)(\, h(\beta(x)) + h(\beta(y))\,)}{(\, \alpha(x) + \alpha(y)\,)(\, \beta(x) + \beta(y)\,)} L_x + \\
&\quad M_x + \frac{(\, g(\alpha(x)) + g(\alpha(y))\,)}{(\, \alpha(x) + \alpha(y)\,)} N_x.
\end{aligned}$$

The hyperplanes $\langle \pi(x), \pi(y) \rangle$, $y \in GF(q) \setminus \{x\}$, together with $\langle \pi(x), \pi_i \rangle$, $i = 1, 2, 3$, form a dual hyperoval through $\pi(x)$, so if τ_x is the permutation of $GF(q)$ with

$$\tau_x \; : \; \frac{(\, g(\alpha(x)) + g(\alpha(y))\,)}{(\, \alpha(x) + \alpha(y)\,)} \; \mapsto \; \frac{(\, h(\beta(x)) + h(\beta(y))\,)(\, g(\alpha(x)) + g(\alpha(y))\,)}{(\, \beta(x) + \beta(y)\,)(\, \alpha(x) + \alpha(y)\,)}$$

and $\tau_x(0) = 0$, then τ_x defines a dual hyperoval through $\pi(x)$. As in the dual case, we normalise τ_x by dividing it through with the constant

$$\frac{h(\beta(x)) + h(\beta(z_x))}{\beta(x) + \beta(z_x)},$$

where z_x is the element of $GF(q) \setminus \{x\}$ such that

$$\frac{g(\alpha(x)) + g(\alpha(z_x))}{\alpha(x) + \alpha(z_x)} = 1.$$

Then τ_x^*, with

$$\tau_x^* \;:\; \frac{(\,g(\alpha(x))+g(\alpha(y))\,)}{(\,\alpha(x)+\alpha(y)\,)} \mapsto \frac{(\,h(\beta(x))+h(\beta(y))\,)(\,g(\alpha(x))+g(\alpha(y))\,)}{(\,\beta(x)+\beta(y)\,)(\,\alpha(x)+\alpha(y)\,)} \cdot \frac{\beta(x)+\beta(z_x)}{h(\beta(x))+h(\beta(z_x))}$$

is an o-polynomial.

If we let

$$\begin{aligned} f' &= f \circ \beta^{-1}, \\ g' &= g \circ \alpha, \\ h' &= h \circ \beta \circ \alpha^{-1}, \end{aligned}$$

then, writing x' for $\beta(x)$ and x'' for $\alpha(x)$,

$$\begin{aligned} L_x &= [1,0,0,f'(x'),0,x'], \\ M_x &= [0,1,0,x,g'(x),0], \\ N_x &= [0,0,1,0,x'',h'(x'')]. \end{aligned}$$

Since for each π_i, $i=1,2,3$, the hyperplanes $\langle \pi_i, \pi(x)\rangle$, $x \in GF(q)$, form a dual hyperoval, f', g' and h' are o-polynomials.

As a corollary to all the above observations, we have

Theorem 5.4.2 Let f, g, f', g' be o-polynomials and let $\alpha = g^{-1} \circ g'$ and $\beta = f'^{-1} \circ f$. Then there is a set of $q+3$ planes in $PG(5,q)$ satisfying conditions (†) if and only if there exist o-polynomials h, σ_x^*, τ_x^* such that

(a) For all $x \in GF(q)$,

$$h(\beta(x)) = \frac{x\,\alpha(x)\,\beta(x)}{f(x)\,g(\alpha(x))}$$

and for all $x, y \in GF(q)$, $x \neq y$,

$$h(\beta(x))+h(\beta(y)) = \frac{(\,x+y\,)(\,\alpha(x)+\alpha(y)\,)(\,\beta(x)+\beta(y)\,)}{(\,f(x)+f(y)\,)(\,g(\alpha(x))+g(\alpha(y))\,)};$$

(b) The funtion $h' = h \circ \beta \circ \alpha^{-1}$ is an o-polynomial; and

(c) For each $x \in GF(q)$,

$$\sigma_x^* \ : \ \frac{g(\alpha(x)) + g(\alpha(y))}{x+y} \ \mapsto \ \frac{(\, f(x)+f(y)\,)(\, g(\alpha(x))+g(\alpha(y))\,)}{(\,\beta(x)+\beta(y)\,)(\,x+y\,)} \cdot \frac{\beta(x)+\beta(y_x)}{f(x)+f(y_x)},$$

$$\tau_x^* \ : \ \frac{(\, g(\alpha(x))+g(\alpha(y))\,)}{(\,\alpha(x)+\alpha(y)\,)} \ \mapsto \ \frac{(\, h(\beta(x))+h(\beta(y))\,)(\, g(\alpha(x))+g(\alpha(y))\,)}{(\,\beta(x)+\beta(y)\,)(\,\alpha(x)+\alpha(y)\,)} \cdot \frac{\beta(x)+\beta(z_x)}{h(\beta(x))+h(\beta(z_x))}$$

for all $y \in GF(q) \setminus \{x\}$, where y_x, z_x are elements of $GF(q) \setminus \{x\}$ such that

$$\frac{g(\alpha(x)) + g(\alpha(y_x))}{x+y_x} = 1, \quad \frac{g(\alpha(x)) + g(\alpha(z_x))}{\alpha(x)+\alpha(z_x)} = 1.$$

□

There is a natural correspondence ψ between the points lying on two planes in $\mathcal{E}$ and the hyperplanes spanned by pairs of planes of $\mathcal{E}$:

$$\text{point } P = \pi_x \cap \pi_y \stackrel{\psi}{\longleftrightarrow} \text{hyperplane } \langle \pi_x, \pi_y \rangle.$$

It is natural to ask if this correspondence extends to a correlation Ψ of the whole space. Suppose that it does. Then Ψ is represented by a 6×6 matrix S over $GF(q)$, such that if P is a point $(p_0, p_1, p_2, p_3, p_4, p_5)$ then the corresponding hyperplane P^Ψ is given by

$$(p_0, p_1, p_2, p_3, p_4, p_5)S.$$

Since we have the following correspondence,

$$\begin{aligned}
\pi_1 \cap \pi_3 = (1,0,0,0,0,0) &\stackrel{\psi}{\longleftrightarrow} \langle \pi_1, \pi_3 \rangle = [0,0,0,0,1,0], \\
\pi_1 \cap \pi_2 = (0,1,0,0,0,0) &\stackrel{\psi}{\longleftrightarrow} \langle \pi_1, \pi_2 \rangle = [0,0,0,0,0,1], \\
\pi_2 \cap \pi_3 = (0,0,1,0,0,0) &\stackrel{\psi}{\longleftrightarrow} \langle \pi_2, \pi_3 \rangle = [0,0,0,1,0,0], \\
\pi_1 \cap \pi(0) = (0,0,0,1,0,0) &\stackrel{\psi}{\longleftrightarrow} \langle \pi_1, \pi(0) \rangle = [0,0,1,0,0,0], \\
\pi_2 \cap \pi(0) = (0,0,0,0,1,0) &\stackrel{\psi}{\longleftrightarrow} \langle \pi_1, \pi(0) \rangle = [1,0,0,0,0,0], \\
\pi_3 \cap \pi(0) = (0,0,0,0,0,1) &\stackrel{\psi}{\longleftrightarrow} \langle \pi_1, \pi(0) \rangle = [0,1,0,0,0,0],
\end{aligned}$$

the matrix S must be

$$S = \begin{pmatrix} 0 & 0 & 0 & 0 & \rho_0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \rho_1 \\ 0 & 0 & 0 & \rho_2 & 0 & 0 \\ 0 & 0 & \rho_2 & 0 & 0 & 0 \\ \rho_0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \rho_1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

for some $\rho_0, \rho_1, \rho_2 \in GF(q)^*$. By considering

$$\begin{aligned} \pi_1 \cap \pi(x) = (f(x), x, 0, 1, 0, 0) &\overset{\psi}{\longleftrightarrow} \langle \pi_1, \pi(x) \rangle = [0, 0, 1, 0, \alpha(x), h(\beta(x))], \\ \pi_2 \cap \pi(x) = (0, g(\alpha(x)), \alpha(x), 0, 1, 0) &\overset{\psi}{\longleftrightarrow} \langle \pi_2, \pi(x) \rangle = [1, 0, 0, f(x), 0, \beta(x)], \\ \pi_3 \cap \pi(x) = (\beta(x), 0, h(\beta(x)), 0, 0, 1) &\overset{\psi}{\longleftrightarrow} \langle \pi_3, \pi(x) \rangle = [0, 1, 0, x, g(\alpha(x)), 0], \end{aligned}$$

$x \neq 0$, we have

$$\begin{aligned} (f(x), x, 0, 1, 0, 0)S &= [0, 0, \rho_2, 0, \rho_0 f(x), \rho_1 x], \\ (0, g(\alpha(x)), \alpha(x), 0, 1, 0)S &= [\rho_0, 0, 0, \rho_2 \alpha(x), 0, \rho_1 g(\alpha(x))], \\ (\beta(x), 0, h(\beta(x)), 0, 0, 1)S &= [0, \rho_1, 0, \rho_2 h(\beta(x)), \rho_0 \beta(x), 0], \end{aligned}$$

and hence for all $x \in GF(q)^*$,

$$\frac{f(x)}{\alpha(x)} = \frac{\rho_2}{\rho_0}, \quad \frac{h(\beta(x))}{x} = \frac{\rho_1}{\rho_2}, \quad \frac{g(\alpha(x))}{\beta(x)} = \frac{\rho_0}{\rho_1}.$$

Putting $x = 1$, we get

$$\begin{aligned} \frac{f(1)}{\alpha(1)} = \frac{\rho_2}{\rho_0} = 1, \\ \frac{h(\beta(1))}{1} = \frac{\rho_1}{\rho_2} = 1, \\ \frac{g(\alpha(1))}{\beta(1)} = \frac{\rho_0}{\rho_1} = 1. \end{aligned}$$

We may take $\rho_0 = 1$. Then,

$$S = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and for all $x \in GF(q)$,

$$f(x) = \alpha(x),$$
$$g(\alpha(x)) = \beta(x),$$
$$h(\beta(x)) = x.$$

It is easily verified that for all $x, y \in GF(q)$,

$$\pi(x) \cap \pi(y) \overset{\Psi}{\longleftrightarrow} \langle \pi(x), \pi(y) \rangle,$$

since

$$\begin{aligned}
(\pi(x) \cap \pi(y))^{\Psi} &= \left[1,\ \frac{\alpha(x)+\alpha(y)}{x+y},\ \frac{\beta(x)+\beta(y)}{x+y},\ \alpha(x) + x\,\frac{\alpha(x)+\alpha(y)}{x+y},\right. \\
&\quad \left. \alpha(x)\,\frac{\beta(x)+\beta(y)}{x+y} + \beta(x)\,\frac{\alpha(x)+\alpha(y)}{x+y}, x\,\frac{\beta(x)+\beta(y)}{x+y} + \beta(x) \right] \\
&= \left[\frac{x+y}{\alpha(x)+\alpha(y)},\ 1,\ \frac{\beta(x)+\beta(y)}{\alpha(x)+\alpha(y)},\ \alpha(x)\frac{x+y}{\alpha(x)+\alpha(y)} + x,\right. \\
&\quad \left. \alpha(x)\frac{\beta(x)+\beta(y)}{\alpha(x)+\alpha(y)} + \beta(x),\ x\,\frac{\beta(x)+\beta(y)}{\alpha(x)+\alpha(y)} + \beta(x)\,\frac{x+y}{\alpha(x)+\alpha(y)} \right] \\
&= \langle \pi(x), \pi(y) \rangle.
\end{aligned}$$

Similarly, $(\langle \pi(x), \pi(y) \rangle)^{\Psi} = \pi(x) \cap \pi(y)$.

Hence we have

Theorem 5.4.3 If the correspondence ψ,

$$\text{point } \pi_x \cap \pi_y \overset{\psi}{\longleftrightarrow} \text{hyperplane } \langle \pi_x, \pi_y \rangle,$$

extends to a correlation Ψ of $PG(5, q)$, then Ψ is a polarity,

$$f(x) = \alpha(x),$$
$$g(\alpha(x)) = \beta(x),$$
$$h(\beta(x)) = x,$$

and for any point $P(p_0, p_1, p_2, p_3, p_4, p_5)$,

$$P^{\Psi} = [p_4, p_5, p_3, p_2, p_0, p_1].$$

□

In the next two examples, we deduce some properties of $\mathcal{E}$ from the properties of the o-polynomials used in the coordinatisation of $\mathcal{E}$.

Example 5.4.4 We show that if $f(x) = g(x) = f'(x) = g'(x) = F(x)$ in Theorem 5.4.2 for some o-polynomial $F(x)$, then all the hyperovals $\mathcal{O}_i$ as well as the dual hyperovals through each plane of $\mathcal{E}$ are regular.

Proof: If $f(x) = g(x) = f'(x) = g'(x) = F(x)$ then $\alpha(x) = g^{-1}g'(x) = x$ and $\beta(x) = f'^{-1}f(x) = x$. By Theorem 5.4.1, putting $y = 0$, we have

$$h(\beta(x)) = h(x) = \frac{x\alpha(x)\beta(x)}{f(x)g(\alpha(x))} = \frac{x^3}{F(x)^2}\,.$$

By Theorem 5.4.1 again, we must have

$$h(\beta(x)) + h(\beta(y)) = \frac{(\,x+y\,)(\,\alpha(x)+\alpha(y)\,)(\,\beta(x)+\beta(y)\,)}{(\,f(x)+f(y)\,)(\,g(\alpha(x))+g(\alpha(y))\,)}\,,$$

that is,

$$\frac{x^3}{F(x)^2} + \frac{y^3}{F(y)^2} = \frac{(x+y)^3}{(F(x)+F(y))^2} \quad \text{for all } x, y \neq 0,\ x \neq y.$$

This is trivially true for $q = 2$, so suppose that $q = 2^h$, $h > 1$. Then the above equation becomes

$$\left(x^3F(y)^2 + y^3F(x)^2\right)(F(x)+F(y))^2 = (x+y)^3F(x)^2F(y)^2,$$

Expanding this equation we have

$$x^3F(y)^4 + y^3F(x)^4 + x^2yF(x)^2F(y)^2 + xy^2F(x)^2F(y)^2 = 0,$$

that is,

$$x^2F(y)^2\left(xF(y)^2 + yF(x)^2\right) + y^2F(x)^2\left(yF(x)^2 + xF(y)^2\right) = 0.$$

Factoring, we have

$$\left(xF(y)^2 + yF(x)^2\right)(xF(y) + yF(x))^2 = 0,$$

that is, for all $x,\ y \in GF(q)^*$, $x \neq y$, either $x/y = F(x)^2/F(y)^2$ or $x/y = F(x)/F(y)$.

Let $y = 1$. Then, for all $x \in GF(q)^*$, $x \neq 1$, either $F(x) = \sqrt{x}$ or $F(x) = x$. Now, since F is an o-polynomial, we have $F(0) = 0$, $F(1) = 1$. If there is another

element, say x_o, in $GF(q)^*$, $x_o \neq 1$, such that $F(x_o) = x_o$, then the three points on π_1, $(F(0), 0, 0, 1, 0, 0)$, $(F(1), 1, 0, 1, 0, 0)$ and $(F(x_o), x_o, 0, 1, 0, 0)$ would lie on the line $x_2 = x_4 = x_5 = x_0 + x_1 = 0$, which contradicts the assumption that F is an o-polynomial. Hence for all $x \neq 1$, we must have $F(x) = \sqrt{x}$, that is, $F(x) = x^{2^{h-1}}$. In this case,

$$h(x) = h'(x) = \frac{x^3}{x^{2^{h-1}} x^{2^{h-1}}} = x^2$$

and

$$\sigma_x : \frac{\sqrt{x} + \sqrt{y}}{x + y} \mapsto \left(\frac{\sqrt{x} + \sqrt{y}}{x + y} \right)^2,$$

that is, $\sigma_x(y) = y^2$,

$$\tau_x : \frac{\sqrt{x} + \sqrt{y}}{x + y} \mapsto \frac{x^2 + y^2}{x + y} \frac{\sqrt{x} + \sqrt{y}}{x + y} = \sqrt{x} + \sqrt{y},$$

that is, $\tau_x(y) = \frac{1}{y}$, so that all the hyperovals $\mathcal{O}_i$ and dual hyperovals are regular. □

Example 5.4.5 It can also be shown, in a similar way, that if $f(x) = f'(x) = F(x)$ for some o-polynomial $F(x)$, and $g(x) = g'(x) = x^2$, that is, the hyperoval on π_2 and the dual hyperoval through π_3 are regular, then all the hyperovals $\mathcal{O}_i$ and the dual hyperovals through each plane of $\mathcal{E}$ are regular:

Since $f = f'$, $g = g'$, we have

$$\alpha(x) = \beta(x) = x, \ h(x) = \frac{x}{F(x)},$$

and by Theorem 5.4.1,

$$\frac{x}{F(x)} + \frac{y}{F(y)} = \frac{(x + y)^3}{(F(x) + F(y))(x^2 + y^2)} = \frac{x + y}{F(x) + F(y)},$$

that is,

$$\frac{xF(y) + yF(x)}{F(x)F(y)} = \frac{x + y}{F(x) + F(y)}.$$

Cross multiplying, we have

$$xF(y)^2 = yF(x)^2,$$

that is, for all $x, y \in GF(q)$, $x \neq y$,

$$\frac{x}{y} = \frac{F(x)^2}{F(y)^2}.$$

Hence, as before, $F(x) = h(x) = h'(x) = x^{2^{h-1}}$ if $q = 2^h$, and

$$\begin{aligned} \sigma_x &: \frac{x^2+y^2}{x+y} \mapsto \sqrt{x+y} \quad \text{so } \sigma_x(y) = y^{2^{h-1}}, \\ \tau_x &: x+y \mapsto \sqrt{x+y} \quad \text{so } \tau_x(y) = y^{2^{h-1}}. \end{aligned}$$

Hence all the hyperovals $\mathcal{O}_i$ and the dual hyperovals are regular. □

In the next section we show how the Yoshiara construction using the Veronese map can be described using the coordinatisation presented in this section. Using this coordinatisation we are able to show that the dual of the Yoshiara construction yields a new family of planes satisfying conditions (†).

5.5 A new family of $\mathcal{E}$

In this section we present a new family of $q+3$ planes satisfying conditions (†) which is the dual of the Yoshiara construction in Example 5.1.1. Firstly, we describe the Yoshiara construction $\mathcal{E}(\mathcal{O}^*)$ using the coordinatisation presented in the previous section.

Let $\mathcal{O}^*$ be the dual hyperoval

$$\{[1, t, \delta(t)] \mid t \in GF(q)\} \cup \{[0,0,1], [0,1,0]\}.$$

The Veronese map ϕ is defined as

$$\phi : (x_0, x_1, x_2) \rightarrow (x_0^2, x_1^2, x_2^2, x_0x_1, x_1x_2, x_0x_2).$$

The points on the lines of $\mathcal{O}^*$ are mapped to points in $PG(5,q)$ as follows:

(a) The points on the line $[0,0,1]$ are mapped under ϕ to points on the conic $\mathcal{C}_1$ on π_1:

$$\begin{aligned} (0,1,0) &\mapsto (0,1,0,0,0,0), \\ (1,0,0) &\mapsto (1,0,0,0,0,0), \\ (1,x,0) &\mapsto (1,x^2,0,x,0,0) = \left(\frac{1}{x}, x, 0, 1, 0, 0\right), \ x \neq 0. \end{aligned}$$

The nucleus N_1 of $\mathcal{C}_1$ is $(0,0,0,1,0,0)$. The o-polynomial f for $\mathcal{O}_1 = \mathcal{C}_1 \cup \{N_1\}$ is hence $f(x) = \frac{1}{x}$.

(b) The points on the line $[1,0,0]$ are mapped under ϕ to points on the conic $\mathcal{C}_2$ on π_2:

$$\begin{aligned}(0,0,1) &\mapsto (0,0,1,0,0,0),\\ (0,1,0) &\mapsto (0,1,0,0,0,0),\\ (0,1,x) &\mapsto (0,1,x^2,0,x,0) = \left(0,\frac{1}{x},x,0,1,0\right),\ x\neq 0.\end{aligned}$$

The nucleus N_2 of $\mathcal{C}_2$ is $(0,0,0,0,1,0)$. The o-polynomial g for $\mathcal{O}_2 = \mathcal{C}_2 \cup \{N_2\}$ is hence $g(x) = \frac{1}{x}$.

(c) Similarly, the points on the line $[0,1,0]$ are mapped under ϕ to points on the conic $\mathcal{C}_3$ on π_3:

$$\begin{aligned}(0,0,1) &\mapsto (0,0,1,0,0,0),\\ (1,0,0) &\mapsto (1,0,0,0,0,0),\\ (x,0,1) &\mapsto (x^2,0,1,0,0,x) = \left(x,0,\frac{1}{x},0,0,1\right),\ x\neq 0.\end{aligned}$$

The nucleus N_3 of $\mathcal{C}_3$ is $(0,0,0,0,0,1)$. The o-polynomial h for $\mathcal{O}_3 = \mathcal{C}_3 \cup \{N_3\}$ is hence $h(x) = \frac{1}{x}$.

For $t \in GF(q)^*$, the points on the line $[1,t,\delta(t)]$ that are mapped under ϕ to points of π_1, π_2, π_3 are as follows:

$$\begin{aligned}(t,1,0) &\mapsto \left(t,\frac{1}{t},0,1,0,0\right) = A_t,\\ \left(0,\frac{\delta(t)}{t},1\right) &\mapsto \left(0,\frac{\delta(t)}{t},\frac{t}{\delta(t)},0,1,0\right) = B_t,\\ (\delta(t),0,1) &\mapsto \left(\delta(t),0,\frac{1}{\delta(t)},0,0,1\right) = C_t.\end{aligned}$$

Recall that we defined $\pi(x) = \langle A_x, B_x, C_x\rangle$, where

$$\begin{aligned}A_x &= (f(x),x,0,1,0,0),\\ B_x &= (0,g(\alpha(x)),\alpha(x),0,1,0),\\ C_x &= (\beta(x),0,h(\beta(x)),0,0,1).\end{aligned}$$

It follows that the line $[1,t,\delta(t)]$, $t \in GF(q)^*$, is mapped under ϕ to the plane $\pi(\frac{1}{t})$, and the permutations α, β are

$$\begin{aligned}\alpha(x) &= \frac{1}{x\delta(\frac{1}{x})},\ x\in GF(q)^*,\ \ \alpha(0)=0,\\ \beta(x) &= \delta\left(\frac{1}{x}\right),\ x\in GF(q)^*,\ \ \beta(0)=0.\end{aligned}$$

Hence the set of $q+3$ planes in $\mathcal{E}(\mathcal{O}^*)$ is $\{\pi_1, \pi_2, \pi_3, \pi(x) \mid x \in GF(q)\}$.

Recall also that the o-polynomial σ_x for the (regular) hyperoval $\mathcal{O}(x)$ on $\pi(x)$, $x \neq 0$, is given by

$$\sigma_x \ : \ \frac{g(\alpha(x)) + g(\alpha(y))}{x+y} \ \mapsto \ \frac{(\, f(x)+f(y)\,)(\, g(\alpha(x))+g(\alpha(y))\,)}{(\,\beta(x)+\beta(y)\,)(\,x+y\,)},$$

that is,

$$\sigma_x \ : \ \frac{x\delta(\frac{1}{x}) + y\delta(\frac{1}{y})}{x+y} \ \mapsto \ \frac{\left(\frac{1}{x}+\frac{1}{y}\right)\left(x\delta(\frac{1}{x})+y\delta(\frac{1}{y})\right)}{\left(\delta(\frac{1}{x})+\delta(\frac{1}{y})\right)(x+y)}.$$

Lastly, $\pi(0)$ is the nucleus of the Veronese surface with the hyperoval $\mathcal{O}(0)$ given by the o-polynomial σ_0,

$$\sigma_0 \ : \ \frac{x\,\delta(\frac{1}{x})}{x} \ \mapsto \ \frac{\frac{1}{x}\,x\,\delta(\frac{1}{x})}{\delta(\frac{1}{x})x},$$

that is, $\sigma_0(x) = \delta^{-1}(x)$. Hence $\mathcal{O}(0)$ is projectively equivalent to $\mathcal{O}^*$, as already noted in Example 5.1.1.

Now, for the smallest case $q = 2$ the correspondence ψ between the points lying on two planes in $\mathcal{E}(\mathcal{O}^*)$ and the hyperplanes spanned by pairs of planes of $\mathcal{E}(\mathcal{O}^*)$ described in Theorem 5.4.3 extends to a null polarity of $PG(5,2)$, represented by the matrix

$$S = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

However, for $q > 2$, since $f \neq \alpha$, by Theorem 5.4.3, the correspondence ψ does not extend to a correlation of $PG(5,q)$. In fact, as mentioned before, we shall show below that the Yoshiara construction $\mathcal{E}(\mathcal{O}^*)$ is not self-dual in general.

Before that we quote a few results on hyperovals in $PG(2,q)$, q even, from [15].

As mentioned in Section 5.4, every hyperoval in $PG(2,q)$, q even, can be written in the form

$$\{(F(x), x, 1) \mid x \in GF(q)\} \cup \{(1,0,0), (0,1,0)\},$$

where F is an o-polynomial. We adopt the notation in [15] and denote such a hyperoval $\mathcal{D}(F)$. In particular, if $F(x) = x^r$ for some integer r, we write $\mathcal{D}(F) = \mathcal{D}(r)$, and if $\mathcal{D}(r)$ and $\mathcal{D}(m)$ are projectively equivalent we write $\mathcal{D}(r) \sim \mathcal{D}(m)$. Similarly, we write $\mathcal{D}'(F)$ and $\mathcal{D}'(r)$ for dual hyperovals.

Result 5.5.1 In $PG(2,q)$, q even, $q > 2$, $\mathcal{D}(r)$ is a hyperoval if and only if

(a) $(r, q-1) = 1$,

(b) $(r-1, q-1) = 1$,

(c) $[(x+1)^r + 1]/x$ is a permutation of $GF(q)$. □

From Table 8.3 of [15], there are five known infinite classes of hyperovals in $PG(2,q)$, $q = 2^h$, of the form $\mathcal{D}(k)$:

(a) $\mathcal{D}(2)$,

(b) $\mathcal{D}(2^n)$, $(n,h) = 1$,

(c) $\mathcal{D}(6)$, h odd,

(d) $\mathcal{D}(3\sigma + 4)$, $\sigma = 2^{(h+1)/2}$, h odd,

(e) $\mathcal{D}(\sigma + \lambda)$, $\sigma = 2^{(h+1)/2}$, h odd, and

$$\lambda = \begin{cases} 2^m & \text{if } h = 4m-1, \\ 2^{3m+1} & \text{if } h = 4m+1. \end{cases}$$

Result 5.5.2 If $\mathcal{D}(r)$ is a hyperoval in $PG(2,q)$, q even, then

$$\mathcal{D}(r) \sim \mathcal{D}(r_1) \sim \mathcal{D}(r_2) \sim \mathcal{D}(r_3),$$

where

(a) $rr_1 \equiv 1 \pmod{q-1}$ and $1 < r_1 < q-1$;

(b) $(r-1)(r_2-1) \equiv 1 \pmod{q-1}$ and $1 < r_1 < q-1$;

(c) $r + r_3 = q$. □

Now let $\mathcal{O}^* = \mathcal{D}'(k)$ be a dual hyperoval in $PG(2,q)$, q even. We consider the Yoshiara construction $\mathcal{E}(\mathcal{O}^*) = \mathcal{E}(k)$ using the Veronese map and the dual hyperoval $\mathcal{D}'(k)$

$$\{[0,1,0],[0,0,1]\} \cup \left\{[1,t,t^k] \mid t \in GF(q)\right\}.$$

From above,

$$\mathcal{E}(k) = \{\pi_1, \pi_2, \pi_3, \pi(x) \mid x \in GF(q)\},$$

where the o-polynomials f, g, h for the hyperovals

$$\mathcal{O}_i = \{\pi_i \cap \pi_j \mid j \neq i\} \cup \{\pi_i \cap \pi(x) \mid x \in GF(q)\},$$

$i = 1, 2, 3$ respectively, are

$$f(x) = g(x) = h(x) = x^{q-2},$$

and the o-polynomials σ_x for the hyperovals

$$\mathcal{O}(x) = \{\pi(x) \cap \pi \mid \pi \in \mathcal{E}(k) \setminus \{\pi(x)\}\}$$

are given by

$$\sigma_x \ : \ \frac{\frac{1}{x^{k-1}} + \frac{1}{y^{k-1}}}{x+y} \ \mapsto \ \frac{\left(\frac{1}{x} + \frac{1}{y}\right)\left(\frac{1}{x^{k-1}} + \frac{1}{y^{k-1}}\right)}{\left(\frac{1}{x^k} + \frac{1}{y^k}\right)(x+y)}.$$

In particular, the hyperoval $\mathcal{O}(0)$ is given by

$$\sigma_0 \ : \ \frac{1}{x^k} \mapsto \frac{1}{x},$$

that is, $\sigma_0(x) = x^{\frac{1}{k}}$. When there is no danger of ambiguity we shall call these hyperovals the hyperovals associated with $\mathcal{E}(k)$.

Recall from above that the permutations α and β are

$$\alpha(x) = \frac{1}{x \cdot \frac{1}{x^k}} = x^{k-1},$$
$$\beta(x) = \frac{1}{x^k} = x^{k(q-2)},$$

and their inverses are given by

$$\alpha^{-1}(x) = x^{\frac{1}{k-1}},$$
$$\beta^{-1}(x) = \frac{1}{x^{\frac{1}{k}}} = x^{\frac{q-2}{k}}.$$

As for the o-polynomials for the dual hyperovals associated with $\mathcal{E}(k)$, we have

(a) On π_2, the dual hyperoval

$$\mathcal{O}_2' = \{\langle \pi_2, \pi_1 \rangle, \langle \pi_2, \pi_3 \rangle, \langle \pi_2, \pi(x) \rangle \mid x \in GF(q)\}$$

has o-polynomial

$$f'(x) = f\beta^{-1}(x) = f(x^{\frac{q-2}{k}}) = x^{\frac{1}{k}}.$$

(b) On π_3, the dual hyperoval

$$\mathcal{O}_3' = \{\langle \pi_3, \pi_1 \rangle, \langle \pi_3, \pi_2 \rangle, \langle \pi_3, \pi(x) \rangle \mid x \in GF(q)\}$$

has o-polynomial

$$g'(x) = g\alpha(x) = g(x^{k-1}) = x^{(q-2)(k-1)}.$$

(c) On π_1, the dual hyperoval

$$\mathcal{O}_1' = \{\langle \pi_1, \pi_2 \rangle, \langle \pi_1, \pi_3 \rangle, \langle \pi_1, \pi(x) \rangle \mid x \in GF(q)\}$$

has o-polynomial

$$h'(x) = h\beta\alpha^{-1}(x) = h\beta\left(x^{\frac{1}{k-1}}\right) = h\left(x^{\frac{k(q-2)}{k-1}}\right) = x^{\frac{k}{k-1}}.$$

(d) On $\pi(x)$, the o-polynomial for the dual hyperoval

$$\mathcal{O}'(x) = \{\langle \pi(x), \pi \rangle \mid \pi \in \mathcal{E}(k) \setminus \{\pi(x)\}\}$$

is given by

$$\tau_x \ : \ \frac{\frac{1}{x^{k-1}} + \frac{1}{y^{k-1}}}{x^{k-1} + y^{k-1}} \mapsto \frac{\left(x^k + y^k\right)\left(\frac{1}{x^{k-1}} + \frac{1}{y^{k-1}}\right)}{\left(\frac{1}{x^k} + \frac{1}{y^k}\right)\left(x^{k-1} + y^{k-1}\right)},$$

that is,

$$\tau_x \ : \ \frac{1}{(xy)^{k-1}} \mapsto xy,$$

and so $\tau_x(y) = y^{\frac{q-2}{k-1}}$.

Note that the multiplicative inverses of k and $k-1$ exist in $GF(q)^*$ because by Result 5.5.1, $(k, q-1) = 1$ and $(k-1, q-1) = 1$.

Let $k_1 = 1/k$. Then, by Result 5.5.2(a), the dual hyperoval $\mathcal{D}'(k_1)$ is projectively equivalent to $\mathcal{D}'(k)$, so that the dual hyperoval $\mathcal{O}'_2 = \mathcal{D}'(k_1)$ defined by f' is equivalent to $\mathcal{D}'(k)$.

Now, for all $x \neq 0$,

$$\begin{aligned} g'(x) &= x^{(q-2)(k-1)} \\ &= x^{q(k-1)-2(k-1)} \\ &= x^{(k-1)-2(k-1)} \quad \text{since } x^q = q \\ &= x^{-(k-1)} \cdot x^{q-1} \quad \text{since } x^{q-1} = 1 \\ &= x^{q-k}, \end{aligned}$$

so the hyperoval $\mathcal{O}'_3 = \mathcal{D}'(q-k)$ defined by g' is projectively equivalent to $\mathcal{D}'(k)$ by Result 5.5.2(c).

Let $k_2 = k/(k-1)$. Then, since

$$(k-1)(k_2-1) = (k-1)\left(\frac{k}{k-1} - 1\right) \equiv 1 (\text{mod } q-1),$$

by Result 5.5.2(b), the hyperoval $\mathcal{O}'_1 = \mathcal{D}'(k_2)$ defined by h' is projectively equivalent to $\mathcal{D}'(k)$.

Lastly, let $k_3 = (q-2)/(k-1)$. Then, since

$$k_3\,(q-2)(k-1) = \frac{q-2}{k-1}(q-2)(k-1) \equiv 1 (\text{mod } q-1),$$

by Result 5.5.2(a), the hyperoval $\mathcal{O}'(x) = \mathcal{D}'(k_3)$ defined by τ_x is projectively equivalent to $\mathcal{O}'_3$ and hence equivalent to $\mathcal{D}'(k)$.

Let $\mathcal{E}'(k)$ denote the dual of $\mathcal{E}(k)$, so that the hyperovals associated with $\mathcal{E}'(k)$ are given by f', g', h' and τ_x, while the dual hyperovals associated with $\mathcal{E}'(k)$ are given by f, g, h and σ_x. By Theorem 5.3.2 and the above observations, we have

Theorem 5.5.3 The set of $q+3$ planes $\mathcal{E}'(k)$ satisfies conditions (†) and all the $q+3$ hyperovals associated with it are projectively equivalent to $\mathcal{D}(k)$. □

Hence we have

Corollary 5.5.4 In $PG(2,q)$, $q > 8$, if $\mathcal{D}(k)$ is not a regular hyperoval, then $\mathcal{E}'(k)$ is a set of $q+3$ planes satisfying conditions (†) which is not constructed from either the Veronese map or the Klein map.

Proof: From Example 5.1.1, if $\mathcal{E}'(k)$ is constructed from the Veronese map, then at least $q+2$ of the hyperovals associated with $\mathcal{E}'(k)$ must be regular. From Example 5.1.2, if $\mathcal{E}'(k)$ is constructed from the Klein map, then at least two of the hyperovals associated with $\mathcal{E}'(k)$ must be regular. However, since $\mathcal{D}(k)$ is not regular, none of the hyperovals associated with $\mathcal{E}'(k)$ is regular. Hence $\mathcal{E}'(k)$ is not constructed from the Veronese map or the Klein map. □

Therefore we have shown that if $\mathcal{D}(k)$ is not a regular hyperoval, the dual $\mathcal{E}'(k)$ of the Yoshiara construction $\mathcal{E}(k)$ is a new family of $q+3$ planes satisfying conditions (†). As a corollary of Theorem 5.5.3, we have also

Corollary 5.5.5 The EGQ resulting from $\mathcal{E}'(k)$ is an extension of the dual of the Tits quadrangle $T_2^*(\mathcal{O})$, where $\mathcal{O} = \mathcal{D}(k)$. □

Corollary 5.5.6 The set of $q+3$ planes $\mathcal{E}(\mathcal{O}^*)$ constructed by Yoshiara using the Veronese map is not self-dual in general. □

Both the Yoshiara and the Thas constructions (Examples 5.1.1 and 5.1.2) admit a point of projection P_o. We show here that the new family of $q+3$ planes $\mathcal{E}'(k)$ also admits such a point by showing that there is a hyperplane not containing any of the points of the hyperovals associated with $\mathcal{E}(k)$. Hence in the dual, there is a point not contained in any of the hyperplanes spanned by pairs of planes of $\mathcal{E}'(k)$.

We require a few more results from [15] and [16] on quadrics and the Veronese surface $\mathcal{V}_2^4$.

Result 5.5.7 A quadric $\mathcal{Q}(F)$ of $PG(2,q)$ is a set of points (x_0, x_1, x_2) satisfying the homogeneous quadratic F over $GF(q)$, where

$$F(x_0, x_1, x_2) = a_{00}x_0^2 + a_{11}x_1^2 + a_{22}x_2^2 + a_{01}x_0x_1 + a_{12}x_1x_2 + a_{02}x_0x_2.$$

The quadrics of $PG(2,q)$ belong to 4 orbits under the projective group $PGL(3,q)$. They are

(a) a repeated line, with canonical form $F = x_0^2$;

(b) a pair of distinct lines, with canonical form $F = x_0x_1$;

(c) a single point, with canonical form $F = x_0^2 + ax_ox_1 + bx_1^2$ irreducible;

(d) a conic with $q+1$ points, with canonical form $F = x_0^2 + x_1x_2$. □

Result 5.5.8 The quadrics of $PG(2,q)$ are mapped under ϕ onto all hyperplane sections of the Veronese surface $\mathcal{V}_2^4$ in $PG(5,q)$. Specifically, the quadric $\mathcal{Q}(F)$ is mapped to the intersection of the hyperplane

$$a_{00}x_0 + a_{11}x_1 + a_{22}x_2 + a_{01}x_3 + a_{12}x_4 + a_{02}x_5 = 0$$

with $\mathcal{V}_2^4$. □

Using these results, we show that a singular quadric with only one rational point P on $PG(2,q)$ is mapped under ϕ to a hyperplane section of $\mathcal{V}_2^4$ which contains a point of the hyperovals associated with $\mathcal{E}(k)$ only if P lies on $\mathcal{D}'(k)$ in $PG(2,q)$.

Lemma 5.5.9 Let $\mathcal{Q}(F)$ be a singular quadric with only one rational point $P = (p_0, p_1, p_2)$ on $PG(2,q)$. If P does not lie on $\mathcal{D}'(k)$ then $\mathcal{Q}(F)$ is mapped to a hyperplane section of $\mathcal{V}_2^4$ which does not contain any point of $\hat{\mathcal{O}}$, where

$$\hat{\mathcal{O}} = \left(\bigcup_{x \in GF(q)^*} \mathcal{O}(x) \bigcup_{i=1}^{3} \mathcal{O}_i \right) \setminus \{\mathcal{O}(0)\},$$

that is, $\hat{\mathcal{O}}$ consists of all the points of the hyperovals associated with $\mathcal{E}(k)$ not lying on $\pi(0)$.

Proof: Let $F(x_0, x_1, x_2) = a_{00}x_0^2 + a_{11}x_1^2 + a_{22}x_2^2 + a_{01}x_0x_1 + a_{12}x_1x_2 + a_{02}x_0x_2$. Suppose that the image of $\mathcal{Q}(F)$ under ϕ contains a point

$$R = (r_0, r_1, r_2, r_3, r_4, r_5)$$

in $\hat{\mathcal{O}}$. Then,

$$a_{00}r_0 + a_{11}r_1 + a_{22}r_2 + a_{01}r_3 + a_{12}r_4 + a_{02}r_5 = 0.$$

Since R is a point of a hyperoval on $\mathcal{E}(k) \setminus \{\pi(0)\}$, R belongs to $\mathcal{V}_2^4$ and has a preimage $\phi^{-1}(R) = (R_0, R_1, R_2)$ lying on $\mathcal{D}'(k)$ in $PG(2,q)$. So

$$(R_0^2, R_1^2, R_2^2, R_0R_1, R_1R_2, R_0R_2) = (r_0, r_1, r_2, r_3, r_4, r_5)$$

and $F(R_0, R_1, R_2) = 0$. However, $\mathcal{Q}(F)$ has only one rational point P in $PG(2,q)$, so $P = \phi^{-1}(R)$, which contradicts the assumption that P does not lie on $\mathcal{D}(k)$. So the intersection of the image of $\mathcal{Q}(F)$ with $\mathcal{V}_2^4$ does not contain a point of $\hat{\mathcal{O}}$. $\square$

We show next that such a hyperplane section does not contain a point of the hyperoval $\mathcal{O}(0)$ on $\pi(0)$.

Let $(r, s, 1)$ be a point of $PG(2,q)$ not on any of the lines of $\mathcal{D}'(k)$. Then we have

$$r \neq 0,\ s \neq 0,\ r + sx + x^k \neq 0 \text{ for all } x \in GF(q). \qquad (*)$$

In order to establish the equation of a singular quadric on $(r, s, 1)$ having only that one rational point, we perform the following transformations:

Let $x^2 + \lambda x + \mu$ be an irreducible quadratic over $GF(q)$. Then the quadric $\mathcal{Q}(F)$, with

$$F(x_0, x_1, x_2) = x_0^2 + \lambda x_0 x_1 + \mu x_1^2$$

has only one rational point $(0, 0, 1)$ on $PG(2,q)$ which lie on a line of $\mathcal{D}'(k)$. The matrix

$$A_F = \begin{pmatrix} 1 & \lambda & 0 \\ 0 & \mu & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

is associated with $\mathcal{Q}(F)$ in that

$$(x_0, x_1, x_2) A_F \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = F(x_0, x_1, x_2).$$

Now, to find the equation of a singular quadric of the same type on $(r, s, 1)$ we use the involution S,

$$S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ r & s & 1 \end{pmatrix}$$

where $(0, 0, 1)S = (r, s, 1)$. Suppose the quadric $\mathcal{Q}(G)$ is a singular quadric with only one rational point $(r, s, 1)$, then $\mathcal{Q}(G)$ has a matrix A_G associated with it such

that

$$(x_0, x_1, x_2) A_G \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = G(x_0, x_1, x_2).$$

So

$$(r, s, 1) A_G \begin{pmatrix} r \\ s \\ 1 \end{pmatrix} = G(r, s, 1) = 0,$$

that is,

$$(0, 0, 1) S A_G S^T \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = 0.$$

Hence we have

$$\begin{aligned} A_G &= S A_F S^T \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ r & s & 1 \end{pmatrix} \begin{pmatrix} 1 & \lambda & 0 \\ 0 & \mu & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & r \\ 0 & 1 & s \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & \lambda & 0 \\ 0 & \mu & 0 \\ r & \lambda r + \mu s & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & r \\ 0 & 1 & s \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & \lambda & r + \lambda s \\ 0 & \mu & \mu s \\ r & \lambda r + \mu s & r^2 + \lambda r s + \mu s^2 \end{pmatrix}, \end{aligned}$$

and $G(x_0, x_1, x_2) = x_0^2 + \mu x_1^2 + (r^2 + \lambda r s + \mu s^2) x_2^2 + \lambda x_0 x_1 + \lambda r x_1 x_2 + \lambda s x_0 x_2$. It is straightforward to verify that $\mathcal{Q}(G)$ is indeed a singular quadric having only one rational point $(r, s, 1)$. Under ϕ, $\mathcal{Q}(G)$ is mapped to the intersection of $\mathcal{V}_2^4$ with the hyperplane $\mathcal{H}$:

$$x_0 + \mu x_1 + \left(r^2 + \lambda r s + \mu s^2\right) x_2 + \lambda x_3 + \lambda r x_4 + \lambda s x_5 = 0.$$

Since (r, s, t) does not lie on any line of $\mathcal{D}'(k)$, by Lemma 5.5.9 $\mathcal{H}$ does not contain any of the image of the points on $\mathcal{D}'(k)$. It remains to be shown that $\mathcal{H}$ does not contain any point of the hyperoval $\mathcal{O}(0)$ on $\pi(0)$:

$$\mathcal{O}(0) = \{(0, 0, 0, 1, 0, 0), (0, 0, 0, 0, 0, 1)\} \cup \left\{(0, 0, 0, x, 1, x^{\frac{1}{k}}) \mid x \in GF(q)\right\}.$$

Now, $\mathcal{H}$ meets $\pi(0)$ in the line $x_3 + rx_4 + sx_5 = 0$. Since by $(*)$, $r \neq 0$, $s \neq 0$, $\mathcal{H}$ does not contain the points $(0,0,0,1,0,0)$, $(0,0,0,0,1,0)$ and $(0,0,0,0,0,1)$. As for the remaining points, $\mathcal{H}$ contains $(0,0,0,x,1,x^{\frac{1}{k}})$ if and only if $x + r + sx^{\frac{1}{k}} = 0$. Suppose that $\mathcal{H}$ does contain a point $(0,0,0,t_o,1,t_o^{\frac{1}{k}})$ of $\mathcal{O}(0)$ for some $t_o \in GF(q)$, then

$$t_o + r + st_o^{\frac{1}{k}} = 0.$$

Let $t = t_o^{\frac{1}{k}}$. Then $t_o = t^k$ and

$$t^k + r + st = 0,$$

which contradicts $(*)$. Hence $\mathcal{H}$ does not contain any point of the hyperplane on $\pi(0)$.

This proves that there is a hyperplane in $PG(5,q)$ which does not contain any point of the hyperovals associated with $\mathcal{E}(k)$. We therefore conclude that a point of projection exists for $\mathcal{E}'(k)$.

Corollary 5.5.10 The EGQ constructed from $\mathcal{E}'(k)$ admits a q-fold quotient. □

In the next section we consider the Thas construction using the Klein map in terms of the coordinatisation described in Section 5.4, and show that, in contrast to the Yoshiara construction, the Thas construction is isomorphic to its dual.

5.6 Self-duality of the Thas construction

We examine the Thas construction (Example 5.1.2) and its dual in this section. To begin with, we present the description of the construction given by Yoshiara in [23]:

Let $\mathcal{K}$ be a $(q+1)$-arc in $PG(3,q)$, q even, $q > 2$. Then $\mathcal{K}$ can be written in the form

$$\{(1,t,t^{2^m},t^{2^m+1}) \mid t \in GF(q)\} \cup \{(0,0,0,1)\}$$

with $q = 2^h$, $(m,h) = 1$, $1 \leq m \leq h-1$. We use P_t to denote the point $(1,t,t^{2^m},t^{2^m+1})$ and P_∞ the point $(0,0,0,1)$. Let l_t, m_t denote the special uni-

secants through P_t such that the sets of lines

$$\begin{aligned}\mathcal{L} &= \{l_t \mid t \in GF(q) \cup \{\infty\}\},\\ \mathcal{M} &= \{m_t \mid t \in GF(q) \cup \{\infty\}\}\end{aligned}$$

are the systems of generators of a hyperbolic quadric. Then, according to [23], the lines l_t, m_t, $t \in GF(q) \cup \{\infty\}$, are of the forms

$$\begin{aligned}l_t &= \left\{(x, y, xt^{2^m}, yt^{2^m}) \mid x, y \in GF(q)\right\},\\ m_t &= \{(x, xt, y, yt \mid x, y \in GF(q)\},\\ l_\infty &= \{(0, 0, x, y) \mid x, y \in GF(q)\},\\ m_\infty &= \{(0, x, 0, y) \mid x, y \in GF(q)\}.\end{aligned}$$

The Klein map θ is given by

$$l^\theta = (l_{01}, l_{02}, l_{03}, l_{12}, l_{31}, l_{23})$$

where $l_{ij} = x_i y_j - x_j y_i$, and (x_0, x_1, x_2, x_3), (y_0, y_1, y_2, y_3) are two distinct points on l. The Thas construction is as follows:

For each $i \in GF(q) \cup \{\infty\}$, the $q+2$ lines corresponding to P_i,

$$\{P_i P_j \mid j \in GF(q) \cup \{\infty\}, j \neq i\} \cup \{l_i, m_i\},$$

are mapped under θ to a hyperoval on a plane Π_i in $PG(5, q)$. The two sets of $q+1$ lines $\mathcal{L}$ and $\mathcal{M}$ are mapped to points on hyperovals on the planes $\Pi(\mathcal{L})$ and $\Pi(\mathcal{M})$ respectively. The details are as follows:

(a) Some of the points on Π_t corresponding to P_t, $t \in GF(q)$, are:

$$\begin{aligned}(P_t P_\infty)^\theta &= (0, 0, 1, 0, t, t^{2^m}),\\ l_t^\theta &= (1, 0, t^{2^m}, t^{2^m}, 0, t^{2^{m+1}}),\\ m_t^\theta &= (0, 1, t, t, t^2, 0).\end{aligned}$$

(b) Some of the points on Π_∞ corresponding to P_∞ are:

$$\begin{aligned}(P_\infty P_t)^\theta &= (0, 0, 1, 0, t, t^{2^m}),\\ l_\infty^\theta &= (0, 0, 0, 0, 0, 1),\\ m_\infty^\theta &= (0, 0, 0, 0, 1, 0).\end{aligned}$$

(c) Some of the points on $\Pi(\mathcal{L})$ corresponding to $\mathcal{L}$ are:

$$\begin{aligned} l_\infty^\theta &= (0,0,0,0,0,1), \\ l_t^\theta &= (1,0,t^{2^m},t^{2^m},0,t^{2^{m+1}}). \end{aligned}$$

(d) Some of the points on $\Pi(\mathcal{M})$ corresponding to $\mathcal{M}$ are:

$$\begin{aligned} m_\infty^\theta &= (0,0,0,0,1,0), \\ m_t^\theta &= (0,1,t,t,t^2,0). \end{aligned}$$

Now, in order to describe

$$\{\Pi_t \mid t \in GF(q) \cup \{\infty\}\} \cup \{\Pi(\mathcal{L}), \Pi(\mathcal{M})\}$$

in terms of our coordinate system and the o-polynomials of Theorem 5.4.2, we apply a simple transformation, a projectivity μ given by the matrix M,

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

so that $(x_0,x_1,x_2,x_3,x_4,x_5)^\mu = (x_5,x_4,x_3,x_2+x_3,x_1,x_0)$. This maps the planes Π_∞, $\Pi(\mathcal{M})$ and $\Pi(\mathcal{L})$ to π_1, π_2, π_3 of our system:

(a) On $\Pi_\infty^\mu = \pi_1$:

$$\begin{aligned} (P_\infty P_t)^\theta = (0,0,1,0,t,t^{2^m}) &\overset{\mu}{\longmapsto} (t^{2^m},t,0,1,0,0), \\ l_\infty^\theta = (0,0,0,0,0,1) &\overset{\mu}{\longmapsto} (1,0,0,0,0,0), \\ m_\infty^\theta = (0,0,0,0,1,0) &\overset{\mu}{\longmapsto} (0,1,0,0,0,0), \end{aligned}$$

so $f(x) = x^{2^m}$.

(b) On $\Pi(\mathcal{M})^\mu = \pi_2$:

$$\begin{aligned} m_t^\theta = (0,1,t,t,t^2,0) &\overset{\mu}{\longmapsto} (0,t^2,t,0,1,0), \\ m_\infty^\theta = (0,0,0,0,1,0) &\overset{\mu}{\longmapsto} (0,1,0,0,0,0), \end{aligned}$$

so $g(x) = x^2$.

(c) On $\Pi(\mathcal{L})^\mu = \pi_3$:

$$\begin{aligned} l_t^\theta = (1,0,t^{2^m},t^{2^m},0,t^{2^{m+1}}) &\overset{\mu}{\longmapsto} (t^{2^{m+1}},0,t^{2^m},0,0,1), \\ l_\infty^\theta = (0,0,0,0,0,1) &\overset{\mu}{\longmapsto} (1,0,0,0,0,0), \end{aligned}$$

so $h(x) = x^{2^{h-1}}$.

The points on Π_t that are mapped under μ to points on π_1, π_2, π_3 are

$$\begin{aligned} (P_tP_\infty)^\theta = (0,0,1,0,t,t^{2^m}) &\overset{\mu}{\longmapsto} (t^{2^m},t,0,1,0,0) = A_t, \\ m_t^\theta = (0,1,t,t,t^2,0) &\overset{\mu}{\longmapsto} (0,t^2,t,0,1,0) = B_t, \\ l_t^\theta = (1,0,t^{2^m},t^{2^m},0,t^{2^{m+1}}) &\overset{\mu}{\longmapsto} (t^{2^{m+1}},0,t^{2^m},0,0,1) = C_t. \end{aligned}$$

Since we defined $\pi(x) = \langle A_x, B_x, C_x \rangle$, we have $\Pi_t^\mu = \pi(t)$, with the permutations α, β as

$$\begin{aligned} \alpha(x) &= x, \\ \beta(x) &= x^{2^{m+1}}. \end{aligned}$$

The hyperoval $\mathcal{O}(x)$ on $\pi(x)$, $x \in GF(q)$, is given by

$$\sigma_x : \frac{x^2+y^2}{x+y} \mapsto \frac{\left(x^{2^m}+y^{2^m}\right)(x^2+y^2)}{(x^{2^{m+1}}+y^{2^{m+1}})(x+y)},$$

that is,

$$\sigma_x : x+y \mapsto \frac{1}{(x+y)^{2^m-1}} = (x+y)^{(2^m-1)(2^h-2)}.$$

Thus, for $y \neq 0$,

$$\begin{aligned} \sigma_x(y) &= y^{(2^m-1)(2^h-2)} \\ &= y^{2^h(2^m-1)-2(2^m-1)} \\ &= y^{-(2^m-1)} \quad \text{since } y^{2^h} = y \\ &= y^{-2^m+1} \cdot y^{2^h-1} \quad \text{since } y^{2^h-1} = 1 \\ &= y^{2^h-2^m}. \end{aligned}$$

Hence, by Result 5.5.2(c), $\mathcal{O}(x)$ is projectively equivalent to $\mathcal{D}(2^m)$.

In accordance with Example 5.1.2, we see that the hyperovals on π_2, π_3 corresponding to $\mathcal{L}$ and $\mathcal{M}$ are indeed regular, while the remaining hyperovals on π_1 and $\pi(x)$, $x \in GF(q)$, given by f and σ_x are isomorphic to $\mathcal{D}(2^m)$.

The null polarity ρ defined by the Klein quadric $\mathcal{Q}$ is given by the matrix

$$R = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

We show that this polarity exchanges π_2, π_3 while fixing every one of π_1, $\pi(t)$, $t \in GF(q)$. The equations for π_1, π_2, π_3 and $\pi(t)$ are:

$$\begin{aligned} \pi_1 &: x_2 = x_4 = x_5 = 0; \\ \pi_2 &: x_0 = x_3 = x_5 = 0; \\ \pi_3 &: x_1 = x_3 = x_4 = 0; \\ \pi(t) &: x_0 + t^{2^m} x_3 + t^{2^{m+1}} x_5 = 0, \\ &\quad\; x_1 + t x_3 + t^2 x_4 = 0, \\ &\quad\; x_2 + t x_4 + t^{2^m} x_5 = 0. \end{aligned}$$

Now,

$$\begin{aligned} \pi_2 &= \langle (0,1,0,0,0,0), (0,0,1,0,0,0), (0,0,0,0,1,0) \rangle, \\ \pi_2^\rho &= [0,0,0,0,1,0] \cap [0,0,0,1,0,0] \cap [0,1,0,0,0,0] = \pi_3, \\ \pi_3 &= \langle (1,0,0,0,0,0), (0,0,1,0,0,0), (0,0,0,0,0,1) \rangle, \\ \pi_3^\rho &= [0,0,0,0,0,1] \cap [0,0,0,1,0,0] \cap [1,0,0,0,0,0] = \pi_2. \end{aligned}$$

Hence ρ exchanges π_2 and π_3.

As for π_1 and $\pi(t)$, $t \in GF(q)$,

$$\pi_1 = \langle (1,0,0,0,0,0), (0,1,0,0,0,0), (0,0,0,1,0,0) \rangle,$$

$$\begin{aligned}
\pi_1^\rho &= [0,0,0,0,0,1] \cap [0,0,0,0,1,0] \cap [0,0,1,0,0,0] = \pi_1, \\
\pi(t) &= \langle (t^{2^m}, t, 0, 1, 0, 0), (0, t^2, t, 0, 1, 0), (t^{2^{m+1}}, 0, t^{2^m}, 0, 0, 1) \rangle, \\
\pi(t)^\rho &= [0,0,1,0,t,t^{2^m}] \cap [0,1,0,t,t^2,0] \cap [1,0,0,t^{2^m},0,t^{2^{m+1}}] = \pi(t).
\end{aligned}$$

Hence ρ fixes π_1 and $\pi(t)$. It is straightforward to verify that indeed, for all π_i, π_j in the set $\{\pi_1, \pi_2, \pi_3, \pi(t) \mid t \in GF(q)\}$, $\pi_i \neq \pi_j$,

$$(\pi_i \cap \pi_j)^\rho = \langle \pi_i^\rho, \pi_j^\rho \rangle.$$

Hence we conclude that

Theorem 5.6.1 The set of $(q+3)$ planes constructed by Thas using the Klein map is self-dual. □

5.7 Some open problems

In [20] it was shown that if there is a point P in $PG(5,q)$ which is not contained in any of the hyperplanes $\langle \pi_i, \pi_j \rangle$, $i \neq j$, then, by projecting π_i from P onto a hyperplane $\mathcal{H}$ not containing P, the set of planes $\{\alpha_0, \ldots, \alpha_{q+2}\}$, where α_i is the projection of π_i, satisfies only conditions (a) and (b) of (†) in $PG(4,q)$. It was shown that for both of the known constructions (Examples 5.1.1 and 5.1.2), as well as for the new family presented in Section 5.5, such a point of projection P exists, but it is not known if this is true in general. In this section we discuss the possiblities of improving some of our results as well as using them to determine the existence of such a point.

In Theorem 5.2.1, we showed that if a point of $PG(5,q)$ not lying on any plane of $\mathcal{E}$ is contained in a hyperplane spanned by two planes of $\mathcal{E}$, then it lies in at least three and at most $q+3$ such hyperplanes. The mean and variance of κ_P over a fixed hyperplane given in the paragraphs after Theorem 5.2.2 indicate that these bounds may be best possible. In examining the proof of Theorem 5.2.1, we see also the difficulty in determining whether hyperplanes not containing either π or π' contains P or not. For example, in the first case of the proof of Theorem 5.2.1, a hyperplane $\langle \pi_j, \pi_k \rangle$, $j, k \neq 1, 2$, contains P if and only if the line joining the points $A_jA_k \cap RA_1$ and P meets π' in the point $A'_jA'_k \cap RT$. This is certainly possible but

we do not have a proof. The mean and variance of κ_P calculated over all points of $PG(5,q)$ not on a plane of $\mathcal{E}$ also do not give an indication as to the existence of a point of projection. It would seem that the counting methods used in Section 5.2 at best show us that it is not impossible that such a point always exists.

Theorem 5.3.5 shows that if π is a plane disjoint from $\pi_0 \in \mathcal{E}$, then the lines $\langle \pi_i, \pi_0 \rangle \cap \pi$ form a dual hyperoval on π. Now, it was shown in [6] that in $PG(2,q)$, q even, the number of lines meeting a set of $q+2$ points is at least $\begin{pmatrix} q+2 \\ 2 \end{pmatrix} + \frac{q}{2}$ if the points do not form a hyperoval. Dually, the number of points lying on a set of $q+2$ lines is $\begin{pmatrix} q+2 \\ 2 \end{pmatrix}$ if the lines form a dual hyperoval and at least $\begin{pmatrix} q+2 \\ 2 \end{pmatrix} + \frac{q}{2}$ if not. Hence the set of hyperplanes $\langle \pi_0, \pi_i \rangle$, $i = 1, \ldots, q+2$, covers the least number of points possible on a plane disjoint to π_0. This seems to indicate that the hyperplanes spanned by pairs of planes in $\mathcal{E}$ cover the smallest possible number of points in $PG(5,q)$. It would be interesting if this could be used to decide whether, in general, there is a point not contained in any of these hyperplanes.

Using the property that the dual of $\mathcal{E}$ also satisfies conditions (†), the question of whether there exists a point not contained in any hyperplane spanned by two planes of $\mathcal{E}$ is equivalent to asking if there exists a hyperplane not incident with a point of $\mathcal{O}$. Hence if $\mathcal{O}$ is a 1-blocking set of $PG(5,q)$ (that is, any hyperplane of $PG(5,q)$ contains a point of $\mathcal{O}$ and any line of $PG(5,q)$ contains a point not in $\mathcal{O}$) then such a point does not exists. The lower bound for a 1-blocking set in $PG(5,q)$ is $q+1+\sqrt{q}$ ([2]) and $|\mathcal{O}|$ is certainly greater then this bound, but it is not clear if it is a 1-blocking set.

The general problem of constructing more families of planes $\mathcal{E}$ in $PG(5,q)$ is still open. It may be possible to try the known o-polynomials exhaustively using Theorem 5.4.2. However, one of the difficulties in this lies in the determination of the algebraic forms of the permutations α, β, and the o-polynomial h, h', σ_x and τ_x, given f, f', g and g'. For example, it is not clear what the algebraic form of the inverse of the o-polynomial, say, $g(x) = x^{1/6} + x^{3/6} + x^{5/6}$ is. This is required in order to determine α. Besides, the o-polynomials must be treated individually and not as a projective equivalance class, as shown in Section 5.5, where the hyperoval

$\mathcal{D}(k)$ appeared in different forms. It is also not obvious that one can always obtain an explicit formula for σ_x and τ_x. For example, even in the case of the Yoshiara construction using the Veronese map, it is not at all obvious what the form of the hyperoval given by

$$\sigma_x \ : \ \frac{x\delta(\frac{1}{x}) + y\delta(\frac{1}{y})}{x+y} \ \rightarrow \ \frac{\frac{1}{x\delta(\frac{1}{x})} + \frac{1}{y\delta(\frac{1}{y})}}{\frac{1}{\delta(\frac{1}{x})} + \frac{1}{\delta(\frac{1}{y})}}$$

is, even though we know that it is regular for $x \neq 0$. Furthermore, it is not clear how one can decide whether a set of planes determined by a set of o-polynomials is isomorphic to a set of planes determined by another set of o-polynomials.

The question of whether the duals of the Yoshiara construction $\mathcal{E}(\mathcal{O}^*)$ yield more new families of planes satisfying conditions (†) for other dual hyperovals $\mathcal{O}^*$ whose o-polynomials are not monomials also remains open. Again, one of the difficulties lies in the manipulation of the permutations and the o-polynomials. For example, using the o-polynomial $\delta(x) = x^{1/6} + x^{3/6} + x^{5/6}$ again, we have $\alpha(x) = 1/x\delta(1/x)$ and it is not clear what the algebraic form of α^{-1} is, which we need in order to establish h'.

This said, it is of course possible to run exhaustive searches using a computer for small cases of q, and while it may not be possible to determine whether two construction are isomorphic or not, it certainly is possible to determine the existence of a point of projection in these cases.

Bibliography

[1] S. Ball. On small complete arcs in a finite plane. *Discrete Maths*, 174:29–34, 1997.

[2] A. Beutelspacher. Blocking sets and partial spreads in finite projective spaces. *Geometriae Dedicata*, 9:425–449, 1980.

[3] S. R. Blackburn. Combinatorics and threshold cryptography. *To appear in* Combinatorial Designs and Their Applications, Pitman Research Notes in Mathematics.

[4] S. R. Blackburn, M. Burmester, Y. Desmedt, and P. R. Wild. *Efficient multiplicative sharing schemes*, volume 1070 of *Lecture Notes in Computer Science*, pages 107–118. Springer Verlag, Berlin, 1996.

[5] S. R. Blackburn and P. R. Wild. Optimal linear perfect hash families. *Journal of Combinatorial Theory Series A*, 83(2):233–250, 1998.

[6] A. Blokhuis and A. A. Bruen. The minimal number of lines intersected by a set of $q+2$ points, blocking sets and intersecting circles. *Journal of Combinatorial Theory Series A*, 50:308–315, 1989.

[7] A. Blokhuis, H. A. Wilbrink, and A. Sali. Perfect sumsets in finite abelian groups. *Linear Algebra and its Applications*, 226–228:47–56, 1995.

[8] A. A. Bruen. Blocking sets in finite projective planes. *SIAM Journal of Applied Mathematics*, 21:380–392, 1971.

[9] A. A. Bruen. Nuclei of sets of $q+1$ points in $PG(2,q)$ and blocking sets of Redei type. *Journal of Combinatorial Theory Series A*, 55:130–132, 1990.

[10] J. C. Fisher, J. W. P. Hirschfeld, and J. A. Thas. Complete arcs in planes of square order. *Annals of Discrete Maths*, 30:243–250, 1986.

[11] M. Giulietti. Some small complete arcs in $PG(2, q)$, q odd square. *Submitted to* the Journal of Geometry.

[12] M. Giulietti and E. Ughi. A small complete arc in $PG(2, q)$, $q = p^2$, $p \equiv 3$ mod 4. *Submitted to* Discrete Maths, Proceedings of Combinatorics '96.

[13] R. L. Graham and N. J. A. Sloane. On additive bases and harmonious graphs. *SIAM Journal of Algebraic and Discrete Methods*, 1:382–404, 1980.

[14] J.W.P. Hirschfeld. *Finite Projective Spaces of Three Dimensions.* Oxford University Press, Oxford, 1985.

[15] J.W.P. Hirschfeld. *Projective Geometries over Finite Fields.* Oxford University Press, Oxford, second edition, 1998.

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

[17] D. R. Hughes and F. C. Piper. *Projective Planes.* Springer-Verlag, New York, 1973.

[18] W. A. Jackson. *On designs which admits certain automorphisms.* PhD thesis, University of London, 1989.

[19] A. Pasini. *Diagram Geometries.* Oxford University Press, Oxford, 1994.

[20] J. A. Thas. Some new classes of extended generalized quadrangles of order $(q + 1, q - 1)$. *Bulletin of the Belgian Mathematical Society - Simon Stevin*, 5(2–3):461–467, 1998.

[21] F. Wettl. On the nuclei of a pointset of a finite projective plane. *Journal of Geometry*, 30:157–163, 1987.

[22] S. Yoshiara. A construction of extended generalized quadrangles using the Veronesean. *European Journal of Combinatorics*, 18(7):835–848, 1997.

[23] S. Yoshiara. The universal covers of a family of extended generalized quadrangles. *European Journal of Combinatorics*, 19:753–765, 1998.