Characterisation and generalisation of k-arcs covering a line in projective planes.

Siaw-Lynn Ng
Maths Department, Royal Holloway
Egham, Surrey TW20 0EX, UK

Abstract

In a projective plane of order q, a k-arc $\mathcal{K}$ covers a line l_∞ disjoint from it if every point on l_∞ lies on a secant to $\mathcal{K}$. In [9], it was shown that a k-arc covers a line satisfies the lower bound $k \geq (1+\sqrt{8q+9})/2$ and attains this bound if and only if $q \in \{2,5,9,27\}$. These cases are characterised by the property that every point on l_∞ lies on exactly one secant to the k-arc. In this paper we consider the generalisation to n-regular k-arcs covering a line and characterise special cases of such k-arcs. 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. We discuss also some open questions that arise from this research.

1 Introduction

In a projective plane of order q, a k-arc $\mathcal{K}$ covers a line l_∞ disjoint from it if every point on l_∞ lies on a secant to $\mathcal{K}$. The concept of k-arcs covering a line 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 ([2]). In particular, no linear (q^2,q,k)-perfect hash family exists if there is a k-arc covering a line in $PG(2,q)$. In [9], it was shown that such a k-arc $\mathcal{K}$ satisfies the lower bound $k \geq (1+\sqrt{8q+9})/2$ and attains this bound if and only if $q \in \{2,5,9,27\}$. These cases are characterised by the property that every point on l_∞ lies on exactly one secant to $\mathcal{K}$. Here we generalise this property: a k-arc $\mathcal{K}$ covering a line l_∞ is n-regular if every point on l_∞ lies on exactly n secants to $\mathcal{K}$. 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.

We consider also the generalisation of k-arcs covering a line to k-arcs covering an arbitrary set of points in the plane. 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 $n > 2$.

This paper is organised as follows. In Section 2 we discuss the generalisation to n-regular k-arcs. In Section 3, we consider the generalisation to k-arcs covering arbitrary point sets and in Section 4 we examine the concept of k-covers in projective spaces. We conclude with a discussion of some ideas and results related to that of a k-arc covering a line.

2 Regular k-arcs covering a line

Let Π_q be a projective plane of order q. We recall firstly the definition of k-arcs covering a line given in [9]:

Definition 2.1 In a projective plane, 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** a line l_∞ disjoint from it if every point on l_∞ lies on at least one secant of $\mathcal{K}$, and we call $\mathcal{K}$ a ***k*-cover** for l_∞.

The following lower bound was obtained in [9]:

Theorem 2.2 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 $\mathcal{K}$.

In view of the characterisation of k-covers attaining the lower bound we have the following definition:

Definition 2.3 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 $\boldsymbol{n}$**-regular** k-cover for l_∞ if every point on l_∞ lies on exactly n secants to $\mathcal{K}$.

Hence we have the result from [9] that in a projective plane of order q where q is a prime power, a 1-regular k-cover exists if and only if $q \in \{2, 5, 9, 27\}$. In the remainder of this section we characterise n-regular k-covers for special cases of n. Firstly we prove an upper bound on n and characterise the case when the upper bound is reached:

Theorem 2.4 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. $\square$

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

Theorem 2.5 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_∞. $\square$

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:

Theorem 2.6 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 $l_\infty \cap \Pi_o = \mathcal{D}$.
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 $\binom{k - k_o}{2}$ points of $l_\infty \setminus \mathcal{D}$. So if $\mathcal{K}$ is a k-cover for l_∞, we must have

$$\binom{k - k_o}{2} + k_o(k - k_o) \geq q - \sqrt{q}.$$

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, $\binom{k-k_o}{2} + k_o(k-k_o) = q-\sqrt{q}$, 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 $\binom{k-k_o}{2}$ 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.

Now, by simple counting, 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 2.6,

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

Now, $f(n,q) \geq g(n,q)$ 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_∞.

Now, 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 2.7 In a projective plane Π_q of odd order q, we say a k-arc $\mathcal{K}$ is an $\boldsymbol{(n_1,n_2)}$**-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 result characterises $((k-2)/2,k/2)$-regular k-covers:

Theorem 2.8 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 $k = q + 1$.

To prove the converse we first 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. □

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 from Theorem 4.5 in [9], 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 5), the 10-arc $\{((0)), ((1)), ((2)), ((4)), ((5)), ((6)), ((8)), ((10)), ((12)), ((15))\}$ is a $(2,3)$-regular cover of l_∞.

3 Arcs covering arbitrary point sets

Recall that a point P is covered by two points Q_1, Q_2 if P lies on the line Q_1Q_2. We generalised the concept of k-arcs covering a line to that of a k-arc covering an arbitrary disjoint set of points.

Definition 3.1 Let $\mathcal{K}$ be a k-arc in a projective plane Π_q of order q, and let $\mathcal{L}$ be a set of points in Π_q disjoint from $\mathcal{K}$. We say that $\mathcal{K}$ covers $\mathcal{L}$ if every point of $\mathcal{L}$ lies on a secant to $\mathcal{K}$.

We consider a few special cases of $\mathcal{L}$.

Theorem 3.2 Let $\mathcal{L}$ be the complement of $\mathcal{K}$, that is, $\mathcal{L}$ consists of the points of $\Pi_q \setminus \mathcal{K}$. Then $\mathcal{K}$ is a complete arc.

Another interesting example is in the case of a $(q+1)$-arc $\mathcal{K}$ in an even order projective plane. In this case $\mathcal{K}$ covers all lines of Π_q that miss $\mathcal{K}$. In fact we have the following characterisation of such k-arcs:

Theorem 3.3 Let $\mathcal{K}$ be a k-arc in Π_q and let $\mathcal{L}$ be the set of points lying on lines missing $\mathcal{K}$. Then $\mathcal{K}$ covers $\mathcal{L}$ if and only if either $\mathcal{K}$ is a $(q+1)$-arc and q is even, or $\mathcal{K}$ is a complete arc.

Proof: Let $\mathcal{K}$ be a k-arc covering $\mathcal{L}$. Let P be any point of Π_q not on $\mathcal{K}$. If P lies on a line missing $\mathcal{K}$ then $P \in \mathcal{L}$ and hence must lie on a secant of $\mathcal{K}$. If all the points of $\Pi_q \setminus \mathcal{K}$ lie on a line missing $\mathcal{K}$ then $\mathcal{K}$ is a complete arc. Suppose that there is a point P that does not lie on a line missing $\mathcal{K}$. Then all the $q+1$ lines through P must meet $\mathcal{K}$ in one or two points. If a line through P meets $\mathcal{K}$ in two points then $\mathcal{K}$ must have at least $q+2$ points, so $\mathcal{K}$ is a $(q+2)$-arc and q is even. However, this means that some line through P must miss $\mathcal{K}$, and this contradicts our assumption. Hence if P does not lie on any line missing $\mathcal{K}$ then P must lie on $q+1$ tangents of $\mathcal{K}$, so $\mathcal{K}$ is a $(q+1)$-arc, q even, with P as the nucleus. Hence if $\mathcal{K}$ is not a complete arc then $\mathcal{K}$ must be a $(q+1)$-arc with q even. The converse is obvious. □

Now, a set of points $\mathcal{K}$ covers a set of points $\mathcal{L}$ if every point on $\mathcal{L}$ lies on a t-secant of $\mathcal{K}$, $t \geq 2$. It is clear then that a set $\mathcal{K}$ of more than one point always covers itself, since every point of $\mathcal{K}$ lies on a secant of $\mathcal{K}$. In view of this, we consider a set $\mathcal{K}$ covering a set $\mathcal{L}$ containing it.

Definition 3.4 Let $\mathcal{K}$, $\mathcal{L}$ be sets of points in Π_q, $\mathcal{K} \subseteq \mathcal{L}$. We say that $\mathcal{K}$ covers $\mathcal{L}$ if every point in $\mathcal{L}$ lies on a secant to $\mathcal{K}$. (By secant we mean a line meeting $\mathcal{K}$ in at least two points.)

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

Theorem 3.5 A set $\mathcal{L}$ of k points in a projective plane of order q is not covered by any proper subset of itself if and only if $\mathcal{L}$ is a k-arc. □

Again, if $\mathcal{L}$ is the whole plane then $\mathcal{K}$ must be a complete arc.

We see that a set $\mathcal{K}$ always covers all the points lying on its secants by definition. Conversely we may ask, if $\mathcal{L}$ is a set of points lying on a union of α lines, what is the minimal number of points in a set $\mathcal{K} \subseteq \mathcal{L}$ that could "generate" $\mathcal{L}$ (that is, $\mathcal{L}$ lies wholly in the secants of $\mathcal{K}$)? By "minimal" we mean that for every point P of $\mathcal{K}$, the set of points $\mathcal{K} \setminus \{P\}$ does not generate $\mathcal{L}$.

We conjecture that if $\mathcal{L}$ is a set of α lines and $\mathcal{K}$ is a minimal set of k points contained in $\mathcal{L}$ such that $\mathcal{K}$ generates $\mathcal{L}$, then

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

where the lower bound is met when $\mathcal{L}$ is the set of secants of a k-arc, and the upper bound is met when $\mathcal{L}$ is a set of α concurrent lines. The lower bound is easily proved, since a set of k points has at most $k(k-1)/2$ secants. The upper bound is yet to be proved. At present we have only proof that $k \leq 2\alpha$, by observing the fact that if $\mathcal{K}$ is minimal then through every point of $\mathcal{K}$ there must be a line of $\mathcal{L}$ which contains exactly one other point of $\mathcal{K}$. There is hence a "skeleton" graph G in $\mathcal{L}$ whose vertices V are the points of $\mathcal{K}$ and whose edges E are the lines of $\mathcal{L}$ containing exactly two points of $\mathcal{K}$. 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 $k \leq 2\alpha$.

4 Covers of hyperplanes 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 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 4.1 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 $\mathcal{H}_\infty$.

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 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 4.1 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, 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:

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.

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, [4]) 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 4.1. 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 [1, 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

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

5 Discussions

To conclude we discuss some ideas and results related to the results in this paper as well as those in [9].

In [9], a few families of small k-arcs covering a line were constructed using conics in $PG(2,q)$. One of these families has k the order of $2\sqrt{q}$, while the lower bound is of the order $\sqrt{2q}$. The question was raised as to whether there are families of k-arcs covering a line with smaller order for arbitrary q. Here we discuss some of the ideas related to k-arcs covering a line.

In [7], it was shown that the points on a conic can be identified with the integers modulo n as follows: 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 $P \in l_\infty \backslash \mathcal{C}$, 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 $[P]$, $P \in l_\infty \backslash \mathcal{C}$, 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 [7] 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 $l_\infty \backslash \mathcal{C}$ 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 $i + j \equiv k \bmod n$.

In view of the fact that points on a conic in $PG(2,q)$ may be identified with $\boldsymbol{Z}_{q+1}$, 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. The results of [9] 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 [5], 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 the result in [9].

There are examples of A and $\boldsymbol{Z}_{q+1}$ for small q given in [5] 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 2.2. 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 by the case of a 1-regular 8-cover in $PG(2,27)$ which can be shown not to lie on a conic.

In [3], 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. It is not clear if the method of proof for this 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.

References

[1] A. Beutelspacher. Blocking sets and partial spreads in finite projective spaces. *Geometriae Dedicata*, 9:425–449, 1980.

[2] S. R. Blackburn and P. R. Wild. Optimal linear perfect hash families. *Journal of Combinatorial Theory Series A*, 83(2):233–250, 1998.

[3] A. Blokhuis, H. A. Wilbrink and A. Sali. Perfect sumsets in finite abelian groups. *Linear Algebra and its Applications*, 226–228:47–56, 1995.

[4] A. A. Bruen. Blocking sets in finite projective planes. *SIAM Journal of Applied Mathematics*, 21:380–392, 1971.

[5] 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.

[6] J.W.P. Hirschfeld. *Projective Geometries over Finite Fields.* Oxford University Press, Oxford, second edition, 1998.

[7] W. A. Jackson. *On designs which admits certain automorphisms.* PhD thesis, University of London, 1989.

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

[9] S. L. Ng and P. R. Wild. On k-arcs covering a line in finite projective planes. To appear in *Ars Combinatoria.*