On $k$-arcs Covering a Line in Finite Projective Planes.

S. L. Ng, P. R. Wild
Maths Department, Royal Holloway
Egham, Surrey TW20 0EX, UK

**Abstract**

In a finite projective plane, a $k$-arc $\mathcal{K}$ *covers* a line $l_\infty$ if every point on $l_\infty$ lies on a secant of $\mathcal{K}$. Such $k$-arcs arises from determining sets of elements for which no linear $(n, q, t)$-perfect hash families exists ([1]), as well as from finding sets of points in $AG(2, q)$ which determine all directions ([2]). This paper provides a lower bound on $k$ and presents examples of $k$-arcs covering a line meeting the bound. This paper also gives constructions of such $k$-arcs with $k$ close to the lower bound.

*Key words:* $k$-arcs, finite projective planes, conics, perfect hash families.

*Classification:* 51E15, 51E21, 05B25

# 1 Introduction

The question of how large the smallest set of point in $PG(2, q)$ must be to cover a line disjoint from it 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 [1].

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 $\phi$ 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 $\phi$, the set of point $v \in V$ with $\phi(v) = \gamma$, where $\gamma$ is an element of $GF(q)$, forms a hyperplane of $AG(d, q)$, and $\phi$ 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 $l_\infty$, that is, every point on $l_\infty$ lies on a secant of $\mathcal{K}$. Blackburn and Wild [1] then raises the question as to how large the smallest such arcs must be.

The same question was asked by G. Ebert, mentioned in the paper by Blokhuis, Wilbrink and Sali [2], in a different guise: How large must a set of points in $AG(2, q)$ be if it determines all directions? This is equivalent to asking how large a set of points $\mathcal{K}$ in $PG(2, q)$ must be if every point on a line $l_\infty$ disjoint from $\mathcal{K}$ lies on a secant to $\mathcal{K}$, that is, $\mathcal{K}$ covers $l_\infty$. In this paper we consider $k$-arcs $\mathcal{K}$ covering a line $l_\infty$ in a projective plane of order $q$. As much of the results depend on sharply focused sets, we will give a brief description of such sets in Section 1, before proceeding to Section 2, where we determine a lower bound on the size of a $k$-arc covering a line and consider the cases when this bound is met. In Section 3, we present examples and constructions of small $k$-arcs covering a line.

## 2 Background

Let $\mathcal{K}$ be a $k$-arc in a projective plane, $k > 2$, 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 [8] showed that in $PG(2, q)$, if $\mathcal{K}$ is sharply focused on $l$ then $\mathcal{K}$ is contained in a conic. Jackson [6] showed that given a conic $\mathcal{C}$ and a line $l$, for any $s|n$, $n = |\,\mathcal{C} \backslash l\,|$, 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 $PG(2, q)$. We summarise the results on sharply focus sets from [6, Chapter 5]:

Let $\mathcal{C}$ be a conic in $PG(2, q)$ and let $l_\infty$ be a line external or secant to $\mathcal{C}$. Let $\mathcal{C}' = \mathcal{C} \setminus l_\infty$. Then the subgroup $H$ of $PGL(3, q)$ fixing both $\mathcal{C}$ and $l_\infty$ is isomorphic to the dihedral group $\mathcal{D}_{2n}$, where $n = |\mathcal{C}'|$. We write

$$H = \langle \alpha,\ \gamma \mid \alpha^2 = \gamma^n = 1,\ \alpha\gamma\alpha = \gamma^{-1} \rangle.$$

**Result 2.1** 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.

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 2.2** 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 $H_K$.

Now, let $K_i$, $K_j \in \mathcal{K}(s)$ and let $\mathrm{Int}(K_i, K_j, l_\infty) = \{AB \cap l_\infty \mid A \in K_i, B \in K_j\}$. The following result is also proved in [6]:

**Result 2.3** (a) If $K_i$, $K_j$ are distinct sharply focused sets in $\mathcal{K}(s)$ then $|\mathrm{Int}(K_i, K_j, l_\infty)| = s$.

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

(c) If $K$, $K_i$, $K_j$ are distinct sharply focused sets in $\mathcal{K}(s)$ then $\mathrm{Int}(K, K_i, l_\infty) \cap \mathrm{Int}(K, K_j, l_\infty) = \emptyset$.

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

As a corollary to these results we have

**Lemma 2.4** Let $K \in \mathcal{K}(s)$ and $P \in \mathcal{C}' \setminus K$, where $\mathcal{C}' = \mathcal{C} \setminus l_\infty$. Let

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

Then,

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

(b) If $P \in \mathcal{C}' \setminus K$, then $\text{Int}(K, l_\infty) \cap \text{Int}(K, P, l_\infty) = \emptyset$, that is, $\text{Int}(K, l_\infty)$ and $\text{Int}(K, P, l_\infty)$ are disjoint subsets of points on $l_\infty$ if $P$ belongs to a sharply focused set in $\mathcal{K}(s)$ different from $K$.

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

We will use these results in some of the proofs and constructions in the next two sections.

# 3 Arcs covering a line

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

**Definition 3.1** 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** $l_\infty$ if every point on $l_\infty$ lies on at least one secant of $\mathcal{K}$, and we call $\mathcal{K}$ a ***k*-cover** for $l_\infty$.

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

**Theorem 3.2** If $\mathcal{K}$ is a $k$-cover for $l_\infty$ in $\Pi_q$, then

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

with equality if and only if every point on $l_\infty$ 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 $l_\infty$ exactly once. Hence, if $\mathcal{K}$ covers $l_\infty$ 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 $l_\infty$ 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. $\square$

If $k = (1+\sqrt{8q+9})/2$ then $8q+9$ must be a square. We determine when this happens if $q$ is a prime power.

**Lemma 3.3** 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

$$x - 3 = 2^{n_1} p^{h_1} \tag{1}$$

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

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 (1) from equation (2) we have

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

The only possible values for $n_1$ and $n_2$ are $(n_1, n_2) \in \{(0,3), (1,2), (2,1), (3,0)\}$.

Now, consider the case when $(n_1, n_2) = (0, 3)$. Equation (3) becomes $2^3 p^{h_2} - p^{h_1} = 2 \cdot 3$. 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 $h_1$.

On the other hand, 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 $q = 2$.

Using a similar argument for the three other cases, 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. $\square$

**Corollary 3.4** Let $\mathcal{K}$ be a $k$-arc in a projective plane of prime power order $q$ covering a line disjoint from it. If $k$ meets the lower bound of Theorem 3.2 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 discuss the existence of such $k$-arcs in each of the four cases of Corollary 3.4. For the first two cases we have the following result:

**Theorem 3.5** There exists a 3-arc in $PG(2,2)$ and a 4-arc in $PG(2,5)$ each covering a line disjoint from it.

**Proof:** Let $l_\infty$ be any line in $PG(2,2)$. Then any triangle not on $l_\infty$ is a 3-arc in $PG(2,2)$ which covers $l_\infty$.

In $PG(2,5)$, Construction 4.4 described in the next section gives a 4-cover $\mathcal{K}$ for any line $l_\infty$ with $s=3$, that is, $\mathcal{K}$ lies on a conic $\mathcal{C}$ disjoint from $l_\infty$, 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. □

**Theorem 3.6** There is no 5-arc in $PG(2,9)$ covering a line disjoint from it.

**Proof:** Let $l_\infty$ be any line in $PG(2,9)$. Suppose $\mathcal{K}$ is a 5-arc covering $l_\infty$ in $PG(2,9)$. Then $\mathcal{K}$ lies on a conic $\mathcal{C}$ disjoint from $l_\infty$, for every 5-arc lies on a conic in $PG(2,q)$, and if $\mathcal{C}$ is not disjoint from $l_\infty$ 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 $l_\infty$ (Result 2.2). 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 $l_\infty$. 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 $l_\infty$ in only the five external points. Hence at least one of the external points on $l_\infty$ lie on more than one secant and so one of the internal points is not covered. 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 $l_\infty$ in the external points. The remaining six secants are of the form $P_iQ_j$ and they meet $l_\infty$ in internal points (Result 2.3(b)), so at least one of the external points on $l_\infty$ is not covered by $\mathcal{K}$. Hence if $\mathcal{K}$ is a 5-arc covering $l_\infty$ 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 5-arc covering a line 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 5-arc in $PG(2,9)$ covering a line by the above result, it is possible that such a 5-arc exists in one of the other planes. By a computer search we found 5-covers in each of the non-Desarguesian planes of order 9. The details can be found in [7]. Thus we have

**Theorem 3.7** Let $\Pi_9$ be a projective plane of order 9. Then there is a 5-arc covering a line if and only if $\Pi_9$ is not the Desarguesian plane of order 9.

For the last case of Corollary 3.4 we have

**Theorem 3.8** There exists an 8-arc covering the line $z=0$ in $PG(2,27)$.

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

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

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 an 8-arc covering $l_\infty$. □

By Corollary 3.4, Theorem 3.5, Theorem 3.7 and Theorem 3.8, we have

**Theorem 3.9** Let $q$ be a prime power. Then there is a projective plane of order $q$ that contains a $k$-arc covering a line with $k$ meeting the lower bound of Theorem 3.2 if and only if $q \in \{2, 5, 9, 27\}$.

In response to the questions raised in [1] and [2], however, we have the following result:

**Theorem 3.10** In $PG(2, q)$, there is a $k$-arc covering a line with $k = (1 + \sqrt{8q + 9})/2$ if and only if $q \in \{2, 5, 27\}$.

## 4 Examples and constructions

**Example 4.1** Let $\mathcal{K}$ be a complete arc in a projective plane of order $q$, $\Pi_q$, that is, every point of $\Pi_q$ lies on a secant of $\mathcal{K}$. It follows that $\mathcal{K}$ covers every point of $\Pi_q$ and hence every line of $\Pi_q$ disjoint from it. In $\Pi_q$, 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 with $k$ in that range. The upper bounds are well-known. The lower bound is obtained as follows (see [5]): 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 with the following values:

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

These examples can be found in [5]. Hence there is a $k$-cover with $k$ the order of a fraction of $q$. □

Now, the $k$-covers which are also complete arcs have sizes the order of $q/2$, which far exceeds the order of the lower bound of Theorem 3.2, 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 4.2** In [4], 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 [3], 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 $\theta$ 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 $\theta$. Nevertheless, it was shown in [7] that $\mathcal{K}$ covers the line $z=0$ for all $q$. Essentially the proof consists of partitioning the line $z=0$ into several parts and showing that each part is covered by a union of some of the $\mathcal{K}_i$'s. In fact, it was also shown that at least one eighth of the points can be removed from $\mathcal{K}$ without affecting the ability of the remaining points to cover $z=0$. The details of the proof can be found in [7]. □

Next we present two new families of $k$-arcs covering a line constructed using sharply focused sets, one of which gives examples of $k$-covers about half the size of the $k$-covers in Example 4.2. To begin with we deduce the following lemma from Lemma 2.4

**Lemma 4.3** Let $\mathcal{C}$ be a conic in $PG(2,q)$ and $l_\infty$ 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 2.4 and Result 2.3(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 4.4 follows from Lemma 4.3:

**Construction 4.4** In $PG(2,q)$, there is a $k$-arc $\mathcal{K}$ covering any given line $l_\infty$ 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 $l_\infty$. Let $\langle\gamma\rangle$ be the (unique) cyclic group of order $q+1$ in $PGO(3,q)_{l_\infty}$ fixing $\mathcal{C}$ and $l_\infty$. 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 $l_\infty$ (Result 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 Lemma 4.3, $\mathcal{K}$ covers $l_\infty$.

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 3.2, 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 3.2.

| $s$ | $q$ | $k = \sqrt{4q+5} - 1$ | $\lfloor \frac{1}{2} + \frac{\sqrt{8q+9}}{2} \rfloor$ |
|---|---|---|---|
| 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 3.2 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 4.1. $\square$

Now, a conic covers every line disjoint from it. Using sharply focused sets, 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 4.5** Let $\Pi_q = PG(2,q)$, $q$ a square, $\sqrt{q} > 5$, and let $l_\infty$ be a line of $\Pi_q$. Let $\Pi_o$ be a Baer subplane secant to $l_\infty$. Let $\mathcal{C}_o$ be a conic in $\Pi_o$ disjoint from $l_\infty \cap \Pi_o$ and $\mathcal{C}$ the conic containing $\mathcal{C}_o$ in $\Pi_q$. Since $l_\infty$ 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 $2(\sqrt{q}+1)$. Let $G$ be the cyclic subgroup of order $\sqrt{q}+1$ fixing both $\mathcal{C}_o$ and $l_\infty$. Then $G$ acts regularly on the points of $\mathcal{C}_o$ and, as a subgroup of $PGO(3,q)_{l_\infty}$ acting on $\Pi_q$, 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 $l_\infty$ and, by Corollary 4.3, 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 $l_\infty$. Note that, by part (c) of Lemma 2.4, 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 $\mathcal{C}\cap RP_2$. 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. 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 $l_\infty$.

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

Suppose there are $\sqrt{q}+1$ bad points all in one orbit $\omega$. 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 $\omega$ 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 2.3(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 $l_\infty$ covered by the secants joining points of $\omega$ 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 $\omega$ to cover $\mathrm{Int}(\mathcal{C}_o,\omega,l_\infty)$ on $l_\infty$, since these points are covered by the secants joining $R$ to points of $\mathcal{C}_o$. We then choose $\{A_2,\dots,A_{\sqrt{q}-3}\}$ 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 $A_{h+1}$, $h=1,\dots,\sqrt{q}-4$, successively from each of the remaining $\sqrt{q}-4$ orbits on $\mathcal{C}\setminus\mathcal{C}_o$ which are not $\omega$ and do not contain $A_1$, such that $A_{h+1}$ does not lie on $RA_i$ for all $i\le h$. 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 $\mathcal{K}=\mathcal{C}_o\cup\{R,A,A_1,A_2,\dots,A_{\sqrt{q}-3}\}$. Then

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

If $A$ and $A_1$ belong to different orbits and $A\notin\mathcal{C}_o$, let $A_2=A$ and choose $\{A_3,\dots,A_{\sqrt{q}-3}\}$ as before. Then $\mathcal{K}=\mathcal{C}_o\cup\{R,A_1,A_2,\dots,A_{\sqrt{q}-3}\}$ 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 $\omega_1,\dots,\omega_n$, $2\le n\le\sqrt{q}-2$, then every one of $\omega_i$ 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 $\omega_n$ must have at most $\sqrt{q}+1-n$ bad points and hence at least $n$ good points, and $\omega_1,\dots,\omega_{n-1}$ 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 $\omega_1$, then pick $A_{i+1}$ from the good points of $\omega_i$, $i = 2, \ldots, n$, 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 $\omega_n$ 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 4.3 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 $l_\infty$ of order at most $2\sqrt{q}+1$. □

We have shown that if $\mathcal{K}$ is a $k$-arc covering a line disjoint from it in a projective plane of order $q$ then $k \geq (1+\sqrt{8q+9})/2$, and this bound is sharp. We have also presented examples of small $k$-covers. We see that for small $q$ there are examples for which the lower bound in Theorem 3.2 is best possible. For $q$ a square, Construction 4.5 gives $k$-covers of order $2\sqrt{q}$. For arbitrary $q$, the smallest examples we have are the complete arcs, and those constructed in Construction 4.4, of order a fraction of $q$. It will be of interest to construct a family of $k$-covers with smaller order for arbitrary $q$.

## References


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

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

[3] M. Giulietti. Some small complete arcs in $PG(2,q)$, $q$ odd square. Submitted to the Journal of Geometry.

[4] M. Giulietti and E. Ughi. A small complete arc in $PG(2,q)$, $q = p^2$, $p \equiv 3 \bmod 4$. Submitted to Discrete Maths, Proceedings of Combinatorics '96.

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

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

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

[8] F. Wettl. On the nuclei of a pointset of a finite projective plane. *Journal of Geometry*, 30:157–163, 1987.