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

Siaw-Lynn Ng, Peter 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_∞ if every point on l_∞ lies on a secant of $\mathcal{K}$. Such k-arcs arise 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 establishes exactly when the lower bound is attained. This paper also gives constructions of such k-arcs with k close to the lower bound.

1 Introduction

The question of how large the smallest set of points 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 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 $\mathcal{K}$. 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_∞ disjoint from $\mathcal{K}$ lies on a secant to $\mathcal{K}$, that is, $\mathcal{K}$ covers l_∞.

In [7] Kovács considers the question of how large a set of points must be to cover every line of the plane. A set of k points with this property is called a saturated k-set. Kovács gives an existence proof for a k-arc contained in an oval in a plane of order q with $k \leq 6\sqrt{q \log q}$ which covers all points not lying on the oval. So for all q it is possible to cover a line by a k-arc with $k \leq 6\sqrt{q \log q}$. Our methods are constructive and we show that there exist k-arcs covering a line with k approximately $2\sqrt{q}$. The lower bound for the size of a k-arc covering a line is $k \geq (1 + \sqrt{8q+9})/2$ and we establish exactly when equality occurs. No saturated k-sets are known with k close to this lower bound.

This paper is structured as follows: In Section 2, 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 some examples of k-arcs covering a line which arise from known structures and in Section 4 we present constructions of small k-arcs covering a line.

2 Arcs covering a line

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 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_∞.

We obtain the following lower bound on the size of a k-cover $\mathcal{K}$ using a counting argument:

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 $\mathcal{K}$.

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 $k(k-1)/2 \geq q+1$. Rearranging this we get the inequality. 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. □

This is no more than one less the lower bound $k \geq (3+\sqrt{8q+1})/2$ for complete arcs (see [4]). However for complete arcs this lower bound seems unsatisfactory, since the known families of complete k-arcs all have a number of points whose order of magnitude is too large compared to this lower bound. In the case of k-arcs covering a line however, the bound is attained in some cases. We determine these cases in the following.

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

Lemma 2.3 Let q be a prime power, $q = p^h$, where p a prime and $h \geq 1$. If $8q+9$ is a square then $q \in \{2, 5, 9, 27\}$.

Proof: Suppose $8q+9 = x^2$ 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, n_2) are $\{(0,3), (1,2), (2,1), (3,0)\}$. By substituting each of these values for n_1 and n_2 in equation (3), 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. □

Corollary 2.4 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 2.2 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 2.4. The definition and properties of sharply focused sets which we use in some of the proofs can be found in [6] and we include a summary at the beginning of Section 4. For the first two cases we have the following result:

Theorem 2.5 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_∞ be any line in $PG(2,2)$. Then any triangle not on l_∞ is a 3-arc in $PG(2,2)$ which covers l_∞. In $PG(2,5)$, Theorem 4.5 in the Section 4 gives a 4-cover $\mathcal{K}$ for any line l_∞ with $s = 3$. □

Theorem 2.6 There is no 5-arc in $PG(2,9)$ covering a line disjoint from it.
Proof: Let l_∞ be any line in $PG(2,9)$. Suppose $\mathcal{K}$ is a 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 4.3). 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 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_∞ in the external points. The remaining six secants are of the form P_iQ_j and they meet l_∞ in internal points (Result 4.4(b)), so at least one of the external points on l_∞ is not covered by $\mathcal{K}$. Hence if $\mathcal{K}$ is a 5-arc covering 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 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. For example, using the representation of the Hall plane of order 9 in [5, Chapter X] and writing $GF(9) = \{0, \alpha^n \mid 0 \leq n \leq 7, \alpha^2 - \alpha - 1 = 0\}$, the 5-arc $\{(0,0,1),(0,1,1),(-1,-\alpha,1),(-1,\alpha,1),(\alpha^3,\alpha,1)\}$ covers the translation line. More details can be found in [8]. Thus we have

Theorem 2.7 Let Π_9 be a projective plane of order 9. Then there is a 5-arc covering a line if and only if Π_9 is not Desarguesian.

For the last case of Corollary 2.4 we have

Theorem 2.8 There exists an 8-arc covering 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 $GF(27) = \{0, 1, \alpha^n \mid n = 1, \ldots, 25,\ \alpha^3 - \alpha + 1 = 0\}$. Then the 8-arc

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

found by computer search is an 8-arc covering l_∞. □

By Corollary 2.4 and Theorems 2.5, 2.7 and 2.8, we have

Theorem 2.9 Let q be a prime power. There is a projective plane of order q that contains a k-arc covering a line with k meeting the lower bound of Theorem 2.2 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 2.10 In $PG(2,q)$, there is a k-arc covering a line with $k = (1+\sqrt{8q+9})/2$ if and only if $q \in \{2,5,27\}$.

3 Examples

Before going on to our constructions we give some examples of k-arcs covering a line.

Example 3.1 Let $\mathcal{K}$ be a complete arc in a projective plane of order q, Π_q. Since every point of Π_q lies on a secant of $\mathcal{K}$, it follows that $\mathcal{K}$ covers every line of Π_q 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 with k in that range, though there are no known families of complete arcs close to the lower bound. In $PG(2,q)$, there is a complete k-arc with $k = (q+5)/2$ if $q \equiv -1 \mod 4$, and $k = (q+4)/2$ if q is even. These examples can be found in [4]. 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 magnitude of the lower bound of Theorem 2.2, 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 3.2 In [3], Giulietti constructed a family of $4(\sqrt{q}-1)$-arcs $\mathcal{K}$ in $PG(2,q)$, where $q = p^2$ and p is an 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

$$\mathcal{K}_1 = \left\{\left(\alpha, -\tfrac{\theta}{\alpha}, 1\right) \mid \alpha \in GF(p)^*\right\}, \quad \mathcal{K}_2 = \left\{\left(\beta, -\tfrac{i\theta}{\beta}, 1\right) \mid \beta \in GF(p)^*\right\},$$
$$\mathcal{K}_3 = \left\{\left(i\gamma, -\tfrac{\theta}{\gamma}, 1\right) \mid \gamma \in GF(p)^*\right\}, \quad \mathcal{K}_4 = \left\{\left(i\delta, -\tfrac{i}{\delta}, 1\right) \mid \delta \in GF(p)^*\right\}.$$

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. Nevertheless, it was shown in [8] 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 the next section we present three new families of k-arcs covering a line constructed using sharply focused sets which give examples of k-covers about half the size of the k-covers in Example 3.2.

4 Constructions

Firstly we give a brief description of sharply focused sets which will be used in the constructions.

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

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

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

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

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 [9] 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 focused sets from [6, Chapter 5]:

Let $\mathcal{C}$ be a conic in $PG(2,q)$ and let l_∞ 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_∞ 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 4.1 For any $s\,|\,n$, $s \geq 3$, 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 sharply focused on l_∞.

There is a similar result if l_∞ is a line tangent to $\mathcal{C}$ and q is odd. In this case the subgroup H fixing both $\mathcal{C}$ and l_∞ is an elementary abelian p-group.

Result 4.2 For any $s\,|\,q$, let N be a subgroup of H of with $|N| = s$. Let $\mathcal{K}(s) = \{K_1, \ldots, K_{\frac{q}{s}}\}$ be the orbits of N on $\mathcal{C} \setminus l_\infty$, each of size s. Then $K \in \mathcal{K}(s)$ is sharply focused on l_∞.

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, when l_∞ is external or secant to $\mathcal{C}$:

Result 4.3 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.

(b) If s is even and h is odd, then half of the points in $\mathrm{Int}(K, l_\infty)$ are external points.

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 4.4 (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 $K_i \in \mathcal{K}(s)\backslash\{K\}$.

(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 $l_\infty \setminus \mathcal{C}$.

Using the properties of sharply focused sets described in Result 4.4, we prove the following theorems:

Theorem 4.5 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 $s|q+1$, $s \geq 3$.

Proof: 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 4.1). 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. 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 contained in $\mathcal{C}$. Now, for any $K \in \mathcal{K}(s)$ and $P \in \mathcal{C}$, $P \notin K$, let

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

Then,

(a) The lines joining P to K meet l_∞ in s points, that is, $|\text{Int}(K, P, l_\infty)| = s$.

(b) If $P \in K' \in \mathcal{K}(s) \setminus \{K\}$, then since $\text{Int}(K, P, l_\infty)$ is a subset of $\text{Int}(K, K', l_\infty)$, and $\text{Int}(K, l_\infty) \cap \text{Int}(K, K', l_\infty) = \emptyset$ by Result 4.4(b), we have $\text{Int}(K, l_\infty) \cap \text{Int}(K, P, l_\infty) = \emptyset$.

(c) Also, if P' and P'' belong to distinct sharply focused sets K', K'', in $\mathcal{K}(s)$ different from K, then since $\text{Int}(K, K', l_\infty) \cap \text{Int}(K, K'', l_\infty) = \emptyset$, we must have $\text{Int}(K, P', l_\infty) \cap \text{Int}(K, P'', l_\infty) = \emptyset$.

By (a), (b) and (c), the set $\mathcal{K}$ covers the disjoint sets $\text{Int}(K_i, l_\infty)$ and $\text{Int}(K_i, P, l_\infty)$, $P \in \mathcal{P}(K_i)$, on l_∞, which together constitute the whole of l_∞. Hence $\mathcal{K}$ is an $(s + (q+1)/s - 1)$-arc covering l_∞. □

For this construction we have $2\sqrt{q+1} - 1 \leq k \leq q+1$. In fact, this construction gives smallest possible k-covers for some small q and gives examples close to the bound whenver $q+1$ has a factor close to $\sqrt{q}$. This will certainly be the case when q has many small factors. 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 3.1.

The following constructions show that we can get within a factor $\sqrt{2}$ of the bound when q is a square. This is twice as good as the construction in Example 3.2 by Ughi and Giulietti.

Theorem 4.6 In $PG(2,q)$, q odd, there is a k-arc covering any given line l_∞ with

$$k = \begin{cases} p^h(p+1) & \text{if } q = p^{2h+1},\ h \geq 1, \\ 2\sqrt{q} & \text{if } q \text{ is a square.} \end{cases}$$

Proof: Let $\mathcal{C}$ be a conic tangent to l_∞ and let $l_\infty \cap \mathcal{C} = \{Q\}$. Let

$$s = \begin{cases} p^h & \text{if } q = p^{2h+1},\ h \geq 1, \\ \sqrt{q} & \text{if } q \text{ is a square.} \end{cases}$$

Then, by Result 4.2, there is a partition of the points of $\mathcal{C} \setminus l_\infty$ into sharply focused sets $\mathcal{K}(s) = \{K_1, \ldots, K_{\frac{q}{s}}\}$, each of size s. Let $K_i \in \mathcal{K}(s)$ and let $P \in K_i$. Let R be a point on the line PQ not lying on $\mathcal{C}$. Then PR covers Q. There are at most $s-1$ secants to $\mathcal{C}$ through R which join a point of $K_i \setminus \{P\}$ to a point of $\mathcal{C} \setminus K_i$. Let these points on $\mathcal{C} \setminus K_i$ be called bad points and the remaining points on $\mathcal{C} \setminus K_i$ good points. Since there are at most $s-1$ bad points and each sharply focused set in $\mathcal{K}(s)$ has s points, we can always pick a good point in each sharply focused set as a representative. Using the same notation as in the proof of Theorem 4.5, let $\mathcal{P}(K_i)$ be a system of distinct representative of the sharply focused sets in $\mathcal{K}(s)$ different from K_i consisting entirely of good points. Then $\mathcal{K} = \{K_i\} \cup \{P \mid P \in \mathcal{P}(K_i)\} \cup \{R\}$ is an $(s + q/s)$-arc. By the same argument as in the proof of Theorem 4.5, it can be shown that $\mathcal{K}$ covers l_∞. □

Now, a conic covers every line disjoint from it. Using sharply focused sets again, 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.

Theorem 4.7 In $PG(2,q)$, q a square, $\sqrt{q} > 5$, there is a k-arc covering any given line l_∞ with $2\sqrt{q} - 1 \leq k \leq 2\sqrt{q} + 1$.

Proof: 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 $2(\sqrt{q}+1)$. 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 the same argument as in the proof of Theorem 4.5, 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 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 $P_1 A_1$. 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_∞.

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 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 4.4(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 $i \le h$. 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 $(h+1)^{\mathrm{th}}$ orbit. Let $\mathcal{K} = \mathcal{C}_o \cup \{R, A, A_1, A_2, \ldots, A_{\sqrt{q}-3}\}$. Then

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

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 $\{A_3, \ldots, A_{n+2}\}$ 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 $l_\infty \setminus \mathcal{C}$ 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 $2\sqrt{q}+1$. □

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 for $q = 2, 5, 9$ and 27. 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 2.2 is best possible. For q a square, Theorem 4.7 gives k-covers of order $2\sqrt{q}$. For arbitrary q, the smallest examples we have are the complete arcs, and those constructed in Theorem 4.5, 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] J.W.P. Hirschfeld. *Projective Geometries over Finite Fields.* Oxford University Press, Oxford, second edition, 1998.

[5] D. R. Hughes and F. C. Piper. *Projective Planes.* Springer-Verlag, New York, 1973.

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

[7] S. J. Kovács. Small saturated sets in finite projective planes. *Rend. Mat. (Roma) Series* VII, 12:157–164, 1992.

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

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