# Hyperfocused Arcs

William E. Cherowitzo  Leanne D. Holder

**Abstract**

An arc in a projective plane whose secants meet some exterior line in the minimum number of points is said to be hyperfocused on that line. This is similar to a concept introduced by Simmons [9] in the design of a geometric secret sharing scheme. Drake and Keating [4] have recently rediscovered the idea under the guise of hyperovals in nets. We will answer two open questions raised by Drake and Keating. We also provide a classification of small hyperfocused arcs in Desarguesian planes using the graph-theoretic concept of 1-factorizations of complete graphs.

## 1 Introduction

A *secret sharing scheme* is a scheme where some secret can be recovered if and only if particular, predetermined groups of people collaborate and share their individual pieces of information (*shares*) related to the secret. Typically, in geometric based schemes, the secret is represented by a point, and the shares consist of geometric information, such as point coordinates, that, when correctly combined, uniquely determine the secret point.

In 1990, G. Simmons [9] designed a secret sharing scheme based on the incidence relations between subspaces of a four-dimensional projective space. In order to obtain a desirable property in this scheme, Simmons was led to investigate $k$-arcs in Desarguesian planes with the property that there existed a line exterior to the $k$-arc so that all the secants of the arc meet the line in a set of exactly $k$ points. Arcs of this type he called *sharply focused sets* and in [9] he investigated such sets with points lying on a conic in the planes $\mathrm{PG}(2, q)$ with $q = 11, 13, 17,$ and 19. In 1997, L. D. Holder [6] expanded this investigation and also considered the case

1991 *Mathematics Subject Classification :* Primary: 51E21; Secondary: 51A30, 05B25, 05C70.

*Key words and phrases :* hyperovals, nets, 1-factorizations of complete graphs, Desarguesian planes, secret sharing schemes.

where the secants of the $k$-arc meet a line in only $k-1$ points (the minimum possible number). She coined the term *super sharply focused sets* for these arcs and gave a construction for them (see Theorem 2.5). We shall use the slightly more informative term *hyperfocused arcs* for the super sharply focused sets of [6]. Recently, D. Drake and K. Keating [4] studied certain point sets, in nets that could be extended to affine Desarguesian planes, which they called *ovals and hyperovals in nets.* These sets are (when viewed in the affine plane) sharply focused sets and hyperfocused arcs. In [4] two open questions are raised concerning hyperfocused arcs, and in this note we shall answer those questions as well as provide a different approach to the subject.

## 2 Hyperfocused Arcs

We begin by reviewing some basic terminology. A *$k$-arc* in $\mathrm{PG}(2,q)$ is a set of $k$ points no three of which are collinear. It is well known that $k \le q+1$ if $q$ is odd and $k \le q+2$ if q is even. A $(q+1)$-arc is called an *oval.* When $q$ is odd, B. Segre [8] showed that every oval in $\mathrm{PG}(2,q)$ is a *conic*, meaning that all the points on the oval have coordinates which satisfy a non-degenerate quadratic equation. If $q$ is even, every oval can be completed to a $(q+2)$-arc, called a *hyperoval.* A hyperoval which consists of a conic together with its nucleus (the point at which all the tangent lines of the conic meet) is called a *hyperconic* (also known as a regular hyperoval). If $q > 4$ then a hyperconic contains a unique conic, i.e., the nucleus of this conic is a distinguished point of the hyperconic. The other ovals contained in a hyperconic, which must contain the nucleus of the conic, are called *pointed conics.* A $k$-arc $\mathcal{K}$ is *sharply focused* on a line $\ell$, which contains no point of $\mathcal{K}$, if the $\binom{k}{2}$ secants of $\mathcal{K}$ intersect $\ell$ in exactly $k$ points. If $\mathcal{K}$ is sharply focused on some line $\ell$ we say that $\mathcal{K}$ is a *sharply focused arc.* We prefer to refer to these objects as arcs, instead of "sets", since this more accurately describes them. Similarly, $k$-arcs with the property that the $\binom{k}{2}$ secants formed by pairs of these points meet an exterior line in exactly $k-1$ points will be called *hyperfocused arcs* (a.k.a. super sharply focused sets [6]). Any exterior line of an arc will be called a *focus line* of the arc, and the set of points at which the secants meet a focus line is called the *focus set* of that line. For either a sharply focused or hyperfocused $k$-arc, there exists at least one focus line of the arc whose focus set has size $k$ or $k-1$ respectively. At times we abuse the language and refer to "the" focus line in these cases, by which we mean any focus line whose focus set has the appropriate size. We shall frequently use the abbreviation *HFA* for hyperfocused arcs.

Clearly, any 2-arc is trivially a hyperfocused arc in any plane. Another obvious fact is that the number of points in a HFA is even since the number of secants of the $k$-arc through a point of the focus set is $\frac{k}{2}$. We shall therefore assume that a *non-trivial* hyperfocused arc has size at least 4. The following proposition shows that every projective plane of even order contains a hyperfocused set of size four.

**Proposition 2.1.** *PG$(2, 2^e)$, $e \geq 1$, contains a hyperfocused set of size four.*

*Proof.* Let $\mathcal{H}$ be a hyperoval in PG$(2, 2)$ and let $\ell$ be the unique line in PG$(2, 2)$ that is exterior to $\mathcal{H}$. The six secant lines through pairs of points on $\mathcal{H}$ are hyperfocused on the three points of $\ell$. We can embed PG$(2, 2)$ in PG$(2, 2^e)$, for any $e$, thus $\mathcal{H}$ is a hyperfocused arc in PG$(2, 2^e)$. ■

**Theorem 2.2.** *Let $D$ be a division ring with char $D = 2$, $0 \in H \subseteq Z(D)$, $|H| = k < \infty$. Then $\mathcal{K} = \{(a, a^2, 1) \colon a \in H\}$ is a $k$-arc of PG$(2, D)$; $\mathcal{K}$ is hyperfocused on the line $(0, 0, 1)^\top$ if and only if $H$ is a subgroup of $(D, +)$.*

*Proof.* The line $L_{a,b} := (a + b, 1, ab)^\top$ contains a point $(x, x^2, 1)$ if and only if $0 = x^2 + (a+b)x + ab = (x+a)(x+b)$. By a theorem of Gordon and Motzkin, every root $x$ of this polynomial is a conjugate of $a$ or $b$. Thus, $a$ and $b$ are the only roots, and $\mathcal{K}$ is a $k$-arc. The secant $L_{a,b}$ of $\mathcal{K}$ meets the line $(0, 0, 1)^\top$ in the point $(1, a + b, 0)$. Thus, $\mathcal{K}$ is hyperfocused on $(0, 0, 1)^\top$ if and only if $|\{a+b \colon a, b \in H, a \neq b\}| = k - 1$ if and only if $\{a + b \colon a, b \in H\} = \{0 + b \colon b \in H\}$ if and only if $H$ is a subgroup of $(D, +)$. ■

**Corollary 2.3.** *Let $\mathcal{C}$ be a conic in PG$(2, q)$, $q = 2^e$, $\ell$ be a line tangent to $\mathcal{C}$ at a point $P$, $\mathcal{K} \subseteq \mathcal{C} \setminus \{P\}$. Then $\mathcal{K}$ is hyperfocused on $\ell$ if and only if $\mathcal{K}$ is projectively equivalent to the set $\{(a, a^2, 1) \colon a \in H\}$ for some subgroup $H$ of $(GF(q), +)$.*

*Proof.* There is a collineation mapping $\mathcal{C}$ to the conic $yz = x^2$. The collineations of PG$(2, q)$ which fix $\mathcal{C}$ are triply transitive on the points of $\mathcal{C}$, so one may map a point of $\mathcal{K}$ to $(0, 0, 1)$ while mapping $\ell$ to the line $(0, 0, 1)^\top$. ■

**Corollary 2.4.** *For each $d \leq e$, there is a hyperfocused arc of size $2^d$ in PG$(2, 2^e)$.* ■

We now give another method for constructing hyperfocused sets in PG$(2, 2^e)$.

**Theorem 2.5 (Subplane Construction [6]).** *For every divisor $d$ of $e$, there are hyperfocused arcs of size $2^d$ and $2^d + 2$ in PG$(2, 2^e)$, contained in a subplane PG$(2, 2^d)$.*

*Proof.* Since $d | e$, PG$(2, 2^e)$ contains a subplane PG$(2, 2^d)$. Let $\mathcal{H}$ be a hyperoval in PG$(2, 2^d)$ and let a secant line $\ell$ meet $\mathcal{H}$ at the points $P$ and $Q$. Then every point of $\ell \setminus \{P, Q\}$ lies on some secant line of $\mathcal{K} = \mathcal{H} \setminus \{P, Q\}$. Hence, $\mathcal{K}$ is a hyperfocused arc of size $2^d$ in PG$(2, 2^d)$, and so in PG$(2, 2^e)$.

Similarly, in PG$(2, 2^d)$, consider the hyperoval $\mathcal{H}$ with exterior line $\ell$. Since any two points in PG$(2, 2^d)$ determine a line and since there are no tangent lines to $\mathcal{H}$ in PG$(2, 2^d)$, the join of any point on $\ell$ to any point on $\mathcal{H}$ must be a secant line to $\mathcal{H}$. So the $\binom{q+2}{2}$ secants in PG$(2, 2^d)$ formed by pairs of points in $\mathcal{H}$ contain every point of $\ell$. Hence, $\mathcal{H}$ is hyperfocused arc of size $2^d + 2$ in PG$(2, 2^d)$, which can be embedded in PG$(2, 2^e)$. Thus, $\mathcal{H}$ is hyperfocused arc of size $2^d + 2$ in PG$(2, 2^e)$. ■

## 3 Two Questions Answered

In [4], two questions concerning net-hyperovals are raised, namely (in our terminology), can a hyperfocused arc exist in $\mathrm{PG}(2, q)$ with $q$ odd? and does there exist a HFA of size different from $2^d$ or $2^d + 2$ for some $d$? We shall answer these questions (no for the first and yes for the second) in this section.

Recall the following result due to A. Bichara and G. Korchmáros [1].

**Theorem 3.1 ([1]).** *Let $\Omega$ be a $q+2$-set of points in $PG(2, q)$ and let $\Phi$ be a subset of points of $\Omega$ with the property that every line containing a point of $\Phi$ intersects $\Omega$ in exactly 2 points. If $|\Phi| > 2$ then $q$ is even. Furthermore, if $|\Phi| > \frac{q}{2}$ then $\Phi = \Omega$.* ■

The proof is an application of the technique used in Segre's famous Lemma of Tangents [8]. As an immediate corollary of this result we have the following:

**Corollary 3.2.** *If $\mathcal{K}$ is a non-trivial hyperfocused $k$-arc in $PG(2, q)$ then $q$ is even. Furthermore, if $\mathcal{K}$ is not a hyperoval then $k \leq \frac{q}{2}$.*

*Proof.* Let $\mathcal{K}$ be a non-trivial hyperfocused $k$-arc in $\mathrm{PG}(2, q)$, focused on line $\ell$ with focus set $A$. Let $\Omega$ be the set $\mathcal{K} \cup \{\ell \setminus A\}$. $\Omega$ has $k + (q+1) - (k-1) = q+2$ points. With $\Phi = \mathcal{K}$, we can apply Theorem 3.1 to conclude that $q$ is even. Also, by the same result, if $k > \frac{q}{2}$ then $\mathcal{K} = \Omega$ would be a hyperoval. ■

From now on we will always assume that $q = 2^e$ with $e > 1$.

The inequality in Theorem 3.1 is sharp as an example, given in [1], with $\Phi = \frac{q}{2}$ exists for all $q = 2^e$, $e > 1$. This also follows from Corollary 2.3 which determines the sizes of HFA's whose points lie on a conic and are focused on a tangent line. We can also determine the sizes of HFA's whose points lie on a hyperconic and which are focused on exterior lines or secants of the conic.

**Theorem 3.3.** *A set of points $\mathcal{K}$ with $3 < |\mathcal{K}|$ on a hyperconic in $PG(2, q)$, $q = 2^h$ which includes the nucleus $N$ of the conic is hyperfocused on a secant line to that conic which does not meet $\mathcal{K}$ if and only if $\mathcal{K} \setminus \{N\}$ is projectively equivalent to a set of points determined by a subgroup of $(GF(q)^*, \cdot)$.*

*Proof.* We may assume that the set $\mathcal{K} \setminus \{N\}$ lies on the conic $\mathcal{C}$ whose points satisfy the non-degenerate quadratic equation $yz = x^2$, and whose nucleus is $N = (1, 0, 0)$. Since the automorphism group of $\mathcal{C}$ acts triply transitively on the points of $\mathcal{C}$ we may also assume that the secant line is the line $\ell$ with affine equation $x = 0$ and that $\mathcal{K}$ contains the point $(1, 1, 1)$. Note that the point $(0, 1, 0)$ of $\mathcal{C}$, being on $\ell$, does not lie in $\mathcal{K}$. Let $H = \{a\colon (a, a^2, 1) \in \mathcal{K}\}$.

For any distinct $a, b \in H$, the secant line through the points $(a, a^2, 1)$ and $(b, b^2, 1)$ of $\mathcal{K}$ has equation $y = (a + b)x + ab$. This secant meets $\ell$ in the point $(0, ab, 1)$. The line through $N$ and a point $(a, a^2, 1)$ of $\mathcal{K}$ has affine equation $y = a^2$ and meets $\ell$ at the point $(0, a^2, 1)$. Let $\mathcal{S}_S = \{(0, ab, 1) : a, b \in H\}$ (note that there are no additional restrictions on $a$ and $b$). $\mathcal{S}_S$ is the focus set of $\mathcal{K}$ on $\ell$. We claim that $\mathcal{K}$ is hyperfocused on $\ell$ if and only if $H$ is a subgroup of $(\mathrm{GF}(q)^*, \cdot)$. From this the statement of the theorem follows.

If $H$ is a subgroup of $(\mathrm{GF}(q)^*, \cdot)$, then $|H| = |\mathcal{S}_S| = |\mathcal{K}|-1$, and $\mathcal{K}$ is hyperfocused on the line $x = 0$.

Conversely, let $T = \{d\colon (0, d, 1) \in \mathcal{S}_S\}$. Since $1 \in H$, we have that $1 \cdot b \in T$ for all $b \in H$, and hence $H \subseteq T$. As $\mathcal{K}$ is a hyperfocused set, we have that $|H| = |\mathcal{K}| - 1 = |\mathcal{S}_S| = |T|$. Thus, $T = H$ and so $H$ is closed under multiplication. Finally, as $H$ is finite, we have that $H$ is a subgroup of $(\mathrm{GF}(q)^*, \cdot)$. ∎

**Corollary 3.4.** *For each divisor $d > 1$ of $2^h - 1$ there exists a hyperfocused arc $\mathcal{K}$ of size $d + 1$, $d$ of whose points lie on a conic $\mathcal{C}$ in PG$(2, 2^h)$ and the remaining point is the nucleus of $\mathcal{C}$. Furthermore, the focus line of $\mathcal{K}$ is a secant line of $\mathcal{C}$.* ∎

**Theorem 3.5.** *A set of points $\mathcal{K}$ with $3 < |\mathcal{K}|$ on a hyperconic in PG$(2, q)$, $q = 2^h$ which includes the nucleus $N$ of the conic is hyperfocused on an exterior line to that conic if and only if $\mathcal{K} \setminus \{N\}$ is projectively equivalent to a set of points determined by a subgroup of $\mathbb{Z}_{q+1}$.*

*Proof.* Let $\mathcal{C}$ be a hyperconic in $\mathrm{PG}(2, q)$ and $\ell$ be an exterior line to $\mathcal{C}$. Let $\bar{\mathcal{C}}$ and $\bar{\ell}$ denote the hyperconic and line, respectively, in $\mathrm{PG}(2, q^2)$ obtained by embedding $\mathrm{PG}(2, q)$ in $\mathrm{PG}(2, q^2)$. As $\mathrm{PG}(2, q^2)$ is a projective plane obtained from the finite field $\mathrm{GF}(q^2)$, which is a quadratic extension of $\mathrm{GF}(q)$, we have that $\bar{\ell}$ is a secant line to $\bar{\mathcal{C}}$ [7]. By Theorem 3.3, we know that there are points of $\bar{\mathcal{C}}$, including the nucleus $N$, that are hyperfocused on $\bar{\ell}$. It remains to show that a hyperfocused arc of this type consists of points only in $\mathcal{C} \cap \bar{\mathcal{C}} = \mathcal{C}$.

Let $P$ and $Q$ be the two points in $\mathrm{PG}(2, q^2) \setminus \mathrm{PG}(2, q)$ such that $\bar{\mathcal{C}} \cap \bar{\ell} = \{P, Q\}$. The stabilizer of $\mathcal{C}$ and $\ell$ in $\mathrm{PG}(2, q)$, denoted $\mathrm{PGL}(3, q)_{\mathcal{C},l}$, fixes $\{P, Q\}$. There is a $g \in \mathrm{PGL}(3, q)_{\mathcal{C},l}$ with $P \xleftrightarrow{g} Q$, so that $|\mathrm{PGL}(3, q)_{\mathcal{C},\ell} : \mathrm{PGL}(3, q)_{\mathcal{C},P,Q}| = 2$. Hence, $\mathbb{Z}_{q+1} = \mathrm{PGL}(3, q)_{\mathcal{C},P,Q} \leqslant \mathrm{PGL}(3, q^2)_{\bar{\mathcal{C}},P,Q} = \mathbb{Z}_{q^2-1}$. If $H \leqslant \mathrm{PGL}(3, q)_{\mathcal{C},P,Q}$, then for any $X \in \mathcal{C} \setminus \{N\}$, the orbit of $X$ under $H$ together with $N$ is a hyperfocused arc in $\mathrm{PG}(2, q^2)$, and hence is contained in $\mathrm{PG}(2, q)$. ∎

**Corollary 3.6.** *For each divisor $d > 1$ of $2^h + 1$ there exists a hyperfocused arc $\mathcal{K}$ of size $d + 1$, $d$ of whose points lie on a conic $\mathcal{C}$ in PG$(2, 2^h)$ and the remaining point is the nucleus of $\mathcal{C}$. Furthermore, the focus line of $\mathcal{K}$ is an exterior line of $\mathcal{C}$.* ∎

**Example 1.** By Corollary 3.6 there exists an HFA of size 12 on a hyperconic in $\mathrm{PG}(2, 32)$ which is focused on an exterior line. This is the smallest HFA of a size not of the form $2^d$ or $2^d + 2$.

## 4 1-factorizations of complete graphs and HFA's

Let $\mathcal{K}$ be a $k$-arc hyperfocused on a line $\ell$ in $\mathrm{PG}(2, q)$. The $\binom{k}{2}$ secants of $\mathcal{K}$ meet $\ell$ in $k - 1$ points with $m = \frac{k}{2}$ secants at a point. A point of $\mathrm{PG}(2, q)$ on $n$ secants of $\mathcal{K}$ will be called an *$n$-secant point*, so each of the points of $\ell$ in the focus set is an $m$-secant point and the remaining points of $\ell$ are 0-secant points. By identifying the $k$ points of $\mathcal{K}$ with the $k$ vertices of the complete graph $K_k$, the secants of $\mathcal{K}$

are naturally identified with the edges of $K_k$. Under this identification, an $m$-secant point corresponds to a 1-factor of $K_k$ (a set of disjoint edges which cover the vertices of a graph) and the $k-1$ points of the focus set provide a 1-factorization of $K_k$ (a set of mutually disjoint 1-factors whose union covers all the edges of the graph).

Our aim is to use information about 1-factorizations of $K_k$ to classify the hyperfocused $k$-arcs for small values of $k$. This is a (lax) embedding problem with the restrictions that the vertices of $K_k$ are embedded in $\mathrm{PG}(2,q)$ as the points of a $k$-arc and the 1-factors of a given 1-factorization of $K_k$ are embedded as collinear points. Throughout this section the term "embedding" shall mean an embedding of this type. One-factorizations of complete graphs have been intensively studied and we refer the reader to Wallis [10] for more details.

To fix some notation we shall use the numbers $0,1,\dots,k-1$ to denote both the points of $\mathcal{K}$ and the corresponding vertices of $K_k$. On occasion these will be bold-faced to avoid confusion with numerical values. The secant lines of $\mathcal{K}$ and corresponding edges of $K_k$ will be denoted by $(XY)$ where $XY$ indicates an unordered pair of distinct points of $\mathcal{K}$. An $n$-secant point of $\mathrm{PG}(2,q)$ will be denoted by concatenating the names of the secants passing through the point. Thus, for example, the notation for the 4-secant point $P=(01)(23)(45)(67)$ indicates that $P$ is the intersection of the secants $(01),(23),(45)$ and $(67)$ and simultaneously denotes the 1-factor associated to $P$.

The union of two distinct 1-factors of a 1-factorization of $K_k$ is a subgraph which is the disjoint union of cycles of even length (greater than two). If the union of $n$ distinct 1-factors is a disconnected subgraph, we say that these 1-factors form an *$n$-division* of $K_k$. Clearly, any subset of $s$ 1-factors of the $n$ 1-factors that form an $n$-division will form an $s$-division of $K_k$. If a 1-factorization contains no two-divisions, i.e., the union of any pair of 1-factors of this 1-factorization is a single cycle (a Hamiltonian cycle), then the 1-factorization is called *perfect*. If $k \geq 12$ there are non-isomorphic perfect 1-factorizations of $K_k$ [10].

There are two families of 1-factorizations which play a significant role in the sequel. The first is the family of *affine line parallelisms* [2]. In this family, the vertices of $K_{2^e}$ are identified with the points of the affine space $\mathrm{AG}(e,2)$. The lines of this space, which contain only two points, are naturally identified with the edges of the graph. A parallel class of lines (associated with a point in the hyperplane at infinity of the projective extension of this space) corresponds to a 1-factor of the graph, and the $2^e-1$ parallel classes give a 1-factorization. The union of any two 1-factors in this 1-factorization consists of a disjoint union of 4-cycles (see [2]). The second family consists of the patterned 1-factorizations $\mathcal{GK}_{2n}$ of the complete graphs $K_{2n}$ ([10]). The vertices of $K_{2n}$ are identified with the elements of $\mathbb{Z}_{2n-1}$ together with the symbol $\infty$. For each $x \in \mathbb{Z}_{2n-1}$ a 1-factor of the 1-factorization is given by $P_x=(x,\infty)(x-1,x+1)(x-2,x+2)\cdots(x-n+1,x+n-1)$. This 1-factorization is perfect if and only if $2n=p+1$ for some prime $p$.

We will now classify the small HFA's. As every 4-arc is an HFA (Proposition 2.1) we start with $k=6$. This classification has already been done for $k=6$ and 8, but our aim here is to use 1-factorizations to obtain these results.

## 4.1 6-arcs

Let $\mathcal{K}$ be a 6-arc hyperfocused on a line $\ell$ in $\mathrm{PG}(2,q)$. The 15 secants of $\mathcal{K}$ meet $\ell$ in five points, each a 3-secant point. The union of any two disjoint 1-factors of $K_6$ is necessarily a 6-cycle. The unique (up to isomorphism) 1-factorization of $K_6$ is thus the perfect 1-factorization $\mathcal{GK}_6$. We may thus assume, without loss of generality, that the points on $\ell$ are given by $P = (05)(14)(23)$, $Q = (15)(20)(34)$, $S = (25)(31)(40)$, $T = (35)(42)(01)$, and $U = (45)(03)(12)$.

The classification of the hyperfocused 6-arcs was done by Drake and Keating [4] and our approach here is not essentially different from theirs.

**Theorem 4.1 ([4]).** *A 6-arc $\mathcal{K}$ is a hyperfocused arc in PG$(2,q)$, if and only if $q = 2^{2k}$ and $\mathcal{K}$ is a hyperconic in a subplane of order 4.*

*Proof.* Assume $\mathcal{K}$ is hyperfocused on $\ell$ in $\mathrm{PG}(2,q)$. We may assume that the points of the focus set on $\ell$ consists of the points $P, Q, S, T$ and $U$.

We introduce coordinates in $\mathrm{PG}(2,q)$ so that $P = (1,0,0)$, $Q = (0,1,0)$, $\mathbf{0} = (1,1,1)$ and $\mathbf{4} = (0,0,1)$. Then we must have that $\mathbf{5} = (a,1,1)$, $\mathbf{1} = (a,0,1)$, $\mathbf{3} = (0,b,1)$, and $\mathbf{2} = (1,b,1)$ with $a, b \in \mathrm{GF}(q) \setminus \{0,1\}$. The lines through the 3-secant points $P$ and $Q$ have slopes 0 and $\infty$ respectively. By calculating the slopes of the the lines through $S = (25)(31)(40)$ (which must be 1), we obtain the equations $a + b = 0$ and $a + b = 2$. These equations imply that $0 = 2$, so $\mathrm{GF}(q)$ has characteristic 2 and $a = b$.

Since $a = b$, the slopes of the secant lines through $T$ are $(1+a)/a$, $1/(1+a)$, $a$, and the slopes of the secant lines through $U$ are $a/(1+a)$, $1+a$, and $1/a$. By equating the slopes of the lines through $T$ (or $U$) we obtain the equation $a^2 + a + 1 = 0$. It follows that $\{0, 1, a, a^2\}$ is a subfield $\mathbf{F}$ of $\mathrm{GF}(q)$. Hence, $q = 2^{2k}$. Furthermore, since the points of $\mathcal{K}$ lie in the subplane $\mathrm{PG}(2,\mathbf{F})$ of $\mathrm{PG}(2,q)$, they form a hyperoval in that subplane which must be a hyperconic (regular hyperoval) in a subplane of order 4. The focus line $\ell$ is an external line of this hyperconic, so $\mathcal{K}$ is the hyperfocused 6-arc given by the subplane construction (Theorem 2.5).

Theorem 2.5 gives the converse of this proposition. ■

## 4.2 8-arcs

The classification of the hyperfocused 8-arcs was also done by Drake and Keating [4]. We will use a different technique and obtain a slight improvement of their result.

There are six non-isomorphic 1-factorizations of $K_8$ ([3], but also see [11]) and we will examine these using the notation and terminology of [11]. [We note that the 1-factorization $\mathcal{F}_5$ given in [11] and repeated in [10] is not correct, but the properties of this 1-factorization that we require are correctly reported.] Taking the union of two disjoint 1-factors of $K_8$, we obtain either a single cycle of length eight or two cycles of length four (the latter are the "quads" of [4]). The points corresponding to the two 1-factors which form a two-division are common diagonal points of two disjoint quadrangles of points of $\mathcal{K}$. A point corresponding to any 1-factor of a three-division is the meet of the four diagonal lines of the two quadrangles determined by the other two 1-factors. The six non-isomorphic 1-factorizations of $K_8$ are denoted by $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_6$. The only structural properties of these 1-factorizations that we will mention are the following. Every 1-factor in $\mathcal{F}_1$ is in three three-divisions. In fact, with the 1-factors as points and the three-divisions as blocks, $\mathcal{F}_1$ forms a Steiner Triple System, STS(7) (the Fano plane). $\mathcal{F}_1$ is an affine line parallelism. $\mathcal{F}_1 - \mathcal{F}_4$ contain three-divisions. $\mathcal{F}_2 - \mathcal{F}_5$ contain two-divisions which are not contained in a three-division. $\mathcal{F}_6$ is a perfect 1-factorization (i.e., it contains no two-divisions). The following result eliminates all the possibilities except for $\mathcal{F}_1$ and $\mathcal{F}_6$.

**Proposition 4.2.** *Let $\mathcal{F}$ be the 1-factorization obtained from the focus set of an HFA in PG$(2, 2^e)$. If the union of two 1-factors of $\mathcal{F}$ contains a 4-cycle, then there exists a unique third 1-factor of $\mathcal{F}$ such that the union of these three 1-factors has a connected component which is the $K_4$ that contains the 4-cycle.*

*Proof.* Let $\mathcal{K}$ be an HFA in PG$(2, 2^e)$ which is focused on line $\ell$. Let $\mathcal{F}$ be the 1-factorization associated with the focus set of $\ell$. Let $P$ and $Q$ be the two points of the focus set that are associated with the two 1-factors of $\mathcal{F}$ whose union contains a 4-cycle. We may assume then that these points have the form $P = (AB)(CD)\cdots$ and $Q = (AC)(BD)\cdots$, where $A, B, C$ and $D$ are points of $\mathcal{K}$. Since $\mathcal{K}$ is an arc, these points form a quadrangle. The diagonal line of this quadrangle contains $P$ and $Q$, and so, is the line $\ell$. The third diagonal point of the quadrangle is $R = (AD)(BC)\cdots$, and is a point of the focus set on $\ell$. The 1-factor of $\mathcal{F}$ associated with the point $R$ has the required property. ■

Note that in the case of 8-arcs, this proposition implies that any two-division of the corresponding 1-factorization must be contained in a three-division. Thus, the 1-factorizations $\mathcal{F}_2 - \mathcal{F}_5$ can not correspond to embeddings of $K_8$.

**Theorem 4.3.** *An 8-arc $\mathcal{K}$ is a hyperfocused arc in PG$(2, q)$ if and only if the $\mathcal{K}$ is constructed as in Corollary 2.3 or Theorem 2.5 and the points of $\mathcal{K}$ lie on a hyperconic. In particular, if the hyperconic is $\mathcal{H} = \mathcal{C} \cup N$, where $\mathcal{C}$ is a conic with nucleus $N$, then*

*(a) $N \notin \mathcal{K}$ if, and only if, $q = 2^e$ with $e \geq 3$ and the focus line is a tangent of $\mathcal{C}$, or*

*(b) $N \in \mathcal{K}$ if, and only if, $q = 2^{3k}$, $k \geq 1$ and the points of $\mathcal{K}$ lie in a subplane of order 8 with focus line a secant of the conic in that subplane.*

*Proof.* Let $\ell$ be a line on which $\mathcal{K}$ is hyperfocused. There are two cases to consider. The 1-factorization corresponding to the points of the focus set on $\ell$ is either $\mathcal{F}_1$ or $\mathcal{F}_6$.

If the 1-factorization is the affine line parallelism $\mathcal{F}_1$ we may assume that the points of the focus set are given by:

$$\begin{aligned} P &= (01)(23)(45)(67) & S &= (04)(15)(26)(37) & V &= (07)(16)(25)(34). \\ Q &= (02)(13)(46)(57) & T &= (05)(14)(27)(36) & & \\ R &= (03)(12)(47)(56) & U &= (06)(17)(24)(35) & & \end{aligned}$$

The intersection points of the opposite sides of the hexagon 046513 are $R, Q$ and $S$ and so, by the converse of Pascal's theorem, the six vertices of this hexagon lie on a conic. Similarly we obtain that the vertices of the hexagons 047512 and 046157 also lie on conics. Since the first two of these conics have five points in common with the third one, all three are the same conic and all the points of $\mathcal{K}$ lie on this single conic. The quadrangle 0123 has $\ell$ as its diagonal line. In a Desarguesian plane of even order, the diagonal line of any quadrangle of points on a conic is a tangent line to that conic. This hyperfocused 8-arc is thus constructed by Corollary 2.3.

Now assume that the 1-factorization is $\mathcal{F}_6$, the perfect 1-factorization $\mathcal{GK}_8$. We may thus assume that the focus set on $\ell$ contains the points:

$$\begin{array}{lll} P = (07)(16)(25)(34) & S = (37)(42)(51)(60) & V = (67)(05)(14)(23). \\ Q = (17)(20)(36)(45) & T = (47)(53)(62)(01) & \\ R = (27)(31)(40)(56) & U = (57)(64)(03)(12) & \end{array}$$

Arguing as in the previous case, the vertices of the hexagons 520163 and 516243 lie on conics, which, having five points in common, are the same conic. The point $\mathbf{7}$ does not lie on this conic as an examination of the hexagon 523706 will show.

The diagonal points of the quadrangle $16TS$ are the collinear points $P, \mathbf{0}$ and $W = (15)(26)\cdots$ and this line contains the point $\mathbf{7}$. $P$ and $W$ are also diagonal points of the quadrangle 5216 and so, these two diagonal lines are the same. However, in the latter case, the four points lie on a conic $\mathcal{C}$ and therefore the diagonal line is a tangent line of $\mathcal{C}$. Similarly, the quadrangles $02TU$ and 6302 have a common diagonal line containing the points $Q$, $\mathbf{1}$ and $\mathbf{7}$ which must be a tangent line of $\mathcal{C}$. $\mathbf{7}$ is therefore the nucleus of $\mathcal{C}$.

Since $\mathbf{7}$ is not on $\ell$, $\ell$ can not be a tangent line of $\mathcal{C}$. As $7 \nmid 2^e + 1$ for any natural number $e$, $\ell$ can not be an exterior line of $\mathcal{C}$ (Theorem 3.5). Thus, $\ell$ must be a secant of $\mathcal{C}$ containing no point of $\mathcal{K}$. By Theorem 3.3, $7 \mid q - 1$ and so, $q = 2^{3k}$ for some natural number $k$. We can introduce coordinates so that the two points of $\mathcal{C}$ on $\ell$ are $(0,1,0)$ and $(0,0,1)$, $\mathbf{7} = (1,0,0)$ and $\mathbf{4} = (1,1,1)$. The conic $\mathcal{C}$ then has equation $yz = x^2$. Let $\mathbf{3} = (a, a^2, 1)$. As in the proof of Theorem 3.3, the first coordinates of the points of $\mathcal{K} \setminus \{\mathbf{7}\}$ form a multiplicative group, which being of order seven, is cyclic and generated by any of its non-identity elements, in particular, $a$. Thus, $a^7 = 1$ and the points of $\mathcal{K} \setminus \{\mathbf{7}\}$ have coordinates of the form $(a^i, a^{2i}, 1)$ for $0 \leq i \leq 6$. As $1 \neq a \in \mathrm{GF}(q)$ and $a^8 = a$, $a$ is in a subfield $\mathbf{F}$ of $\mathrm{GF}(q)$ of order eight. The subplane $\mathrm{PG}(2, \mathbf{F})$ of $\mathrm{PG}(2, q)$ contains $\mathcal{K} \cup \{(0,1,0), (0,0,1)\}$. Thus, $\mathcal{K}$ arises from the subplane construction (Theorem 2.5). ■

### 4.3 10-arcs

There are 396 non-isomorphic 1-factorizations of $K_{10}$ determined by Gelling [5]. The union of two 1-factors of any of these 1-factorizations is either a 10-cycle or the union of a 4-cycle and a 6-cycle. Only one of these 1-factorizations is perfect, and it is given by:

$$\begin{array}{lll} A = (01)(23)(45)(67)(89) & D = (04)(18)(26)(35)(79) & G = (07)(12)(39)(46)(58) \\ B = (02)(16)(34)(59)(78) & E = (05)(19)(24)(37)(68) & H = (08)(15)(29)(36)(47) \\ C = (03)(17)(25)(48)(69) & F = (06)(13)(28)(49)(57) & I = (09)(14)(27)(38)(56). \end{array}$$

Assuming that this 1-factorization can be embedded, the converse of Pascal's theorem shows, by using the hexagons 231549, 239458 and 153804, that the points $0-5, 8$ and 9 lie on the same conic. However, the hexagon 230548 fails to satisfy Pascal's theorem, so this 1-factorization does not embed.

By Proposition 4.2 a necessary condition for any of the non-perfect 1-factorizations to be embeddable is that every two-division is contained in a three-division. Examining Gelling's list shows that only two of the 1-factorizations have this property. One of these is:

$$\begin{array}{lll} A=(01)(23)(45)(67)(89) & D=(04)(15)(29)(36)(78) & G=(07)(16)(28)(35)(49) \\ B=(02)(13)(48)(56)(79) & E=(05)(14)(27)(38)(69) & H=(08)(19)(25)(37)(46) \\ C=(03)(12)(47)(59)(68) & F=(06)(17)(24)(39)(58) & I=(09)(18)(26)(34)(57). \end{array}$$

Triangles 024 and 135 are perspective from point $A$. The sides (02) and (13) meet at $B$, and the sides (04) and (15) meet at $D$. Since the sides (24) and (35) do not meet on $\ell$, Desargues' theorem is violated and this 1-factorization does not embed.

Thus, there is only one (up to isomorphism) 1-factorization that can embed in a Desarguesian plane of even order and it is given by:

$$\begin{array}{lll} A=(01)(23)(45)(67)(89) & D=(04)(17)(25)(38)(69) & G=(07)(19)(24)(36)(58) \\ B=(02)(13)(48)(56)(79) & E=(05)(16)(29)(34)(78) & H=(08)(14)(26)(39)(57) \\ C=(03)(12)(47)(59)(68) & F=(06)(18)(27)(35)(49) & I=(09)(15)(28)(37)(46). \end{array}$$

The hexagons 452769, 462739, 452896 and 136485 show that the points of $\mathcal{K}$ other than $\mathbf{0}$ lie on a single conic, $\mathcal{C}$, and the hexagon 018672 shows that $\mathbf{0}$ does not lie on this conic. The triangles 405 and 716 are perspective from the line $\ell$, so the secants $(01), (47)$ and $(56)$ meet at a point $X$. The quadrangle 4567 has diagonal line $AX$, showing that (01) is a tangent line of the conic $\mathcal{C}$. Similarly, triangles 437 and 509 are perspective from $\ell$, and so, secants $(03), (45)$ and $(79)$ meet at a point $Y$. The quadrangle 4759 has diagonal line $CY$ and so (03) is a tangent line of $\mathcal{C}$. Therefore, $\mathbf{0}$ is the nucleus of the conic $\mathcal{C}$.

We may assume that the conic $\mathcal{C}$ has equation $yz = x^2$ and coordinatize so that $\mathbf{0} = (1,0,0)$, $\mathbf{1} = (0,1,0)$, $\mathbf{2} = (0,0,1)$, $\mathbf{3} = (1,1,1)$ and $\mathbf{4} = (a, a^2, 1)$ with $a \in \mathrm{GF}(q) \setminus \{0,1\}$. Furthermore, we obtain $A = (1,1,0)$, $B = (1,0,1)$ and $C = (0,1,1)$. The focus line $\ell$ is thus $(1,1,1)^\top$. We can continue assigning coordinates using the points $\mathbf{0}$ and $\mathbf{1}$ to obtain $D = (a^2+1, a^2, 1)$, $\mathbf{7} = (a^2+1, a^4+1, 1)$, $G = (a^4, a^4+1, 1)$, $\mathbf{9} = (a^4, a^8, 1)$ and $H = (a, a+1, 1)$. From the fact that the secant (79) passes through the point $B$, we obtain the equation $a^6 = a^2 + 1$, i.e., $a^3 = a + 1$. Now, $a^7 = a(a^6) = a^3 + a = a + 1 + a = 1$. Thus, $7 \mid q - 1$ and so, $q = 2^{3k}$ and $\mathcal{K}$ is a hyperconic in a subplane of order 8. If $k$ is odd, $\ell$ is an exterior line of the conic $\hat{\mathcal{C}}$ of $\mathrm{PG}(2,q)$ which is the extension of $\mathcal{C}$. If $k$ is even, $\ell$ is a secant line of $\hat{\mathcal{C}}$. We summarize these results in:

**Theorem 4.4.** *A* 10*-arc* $\mathcal{K}$ *is a hyperfocused arc in* $PG(2,q)$ *if and only if* $q = 2^{3k}$ *and* $\mathcal{K}$ *is a hyperconic in a subplane of order* 8 *with focus line an exterior line of the conic in that subplane. If* $k$ *is odd, the focus line is an exterior line of the extension of this hyperconic in the full plane, and if* $k$ *is even it is a secant line of the extended hyperconic.*

## 5 Open Problems

This work leads naturally to the following open problems and conjectures concerning HFA's in Desarguesian projective planes.

1. Find necessary and sufficient conditions on a 1-factorization of $K_{2n}$ so that it may be embedded in $\mathrm{PG}(2, 2^e)$ in the manner we have been discussing.

2. Related to the above would be theorems of the form, when a 1-factorization $\mathcal{F}$ has been embedded, then the points of the arc lie on a hyperoval(?) of type $X$.

3. Provide graph-theoretic descriptions of the 1-factorizations associated to different types of hyperovals.

4. While the classification of the small HFA's may be misleading, there is some evidence that would imply that the points of an HFA which does not arise from the subplane construction must lie on a hyperconic. This would not be a very surprising result considering the fact that a high degree of structure is needed to obtain such highly focused arcs.

*Acknowledgment.* The authors would like to thank Gábor Korchmáros and Aart Blokhuis for pointing out the significance of Theorem 3.1 to this work. We also wish to express our gratitude to David Drake for his many helpful suggestions and the reworking of Theorem 2.2. Finally, we wish to thank Art Hanna for his help in verifying the 1-factorizations of $K_{10}$.

## References

[1] A. Bichara and G. Korchmáros, *Note on (q+2)-sets in a galois plane of order q*, Annals of Discrete Math. **14** (1982), 117–122.

[2] P.J. Cameron, *Parallelisms of complete designs*, London Mathematical Society Lecture Note Series, vol. 23, Cambridge University Press, London-New York-Melbourne, 1976.

[3] L.E. Dickson and F.H. Safford, *Solution to problem 8 (group theory)*, American Mathematical Monthly **13** (1906), 150–151.

[4] D. Drake and K. Keating, *Ovals and hyperovals in Desarguesian nets*, Designs, Codes and Cryptography **31** (2004), 195–212.

[5] E. N. Gelling, *On one-factorizations of a complete graph and the relationship to round-robin schedules*, Master's thesis, Univeristy of Victoria, Canada, 1973.

[6] L. D. Holder, *The Construction of Geometric Threshold Schemes with Projective Geometry*, Master's thesis, Univeristy of Colorado at Denver, 1997.

[7] P. Kleidman and M. Liebeck, *The subgroup structure of finite classical groups*, The London Mathematical Society Lecture Note Series, vol. 129, Cambridge University Press, 1990.

[8] B. Segre, *Sulle ovali nei piani lineari finite*, Rend. Accad. Naz. Lincei **17** (1954), 141 – 142.

[9] G. Simmons, *Sharply Focused Sets of Lines on a Conic in PG(2,q)*, Congressus Numerantium, vol. 73, January 1990, pp. 181–204.

[10] W.D. Wallis, *One-factorizations*, Mathematics and Its Applications, vol. 390, Kluwer Academic Publishers, Dordrecht-Boston-London, 1997.

[11] W.D. Wallis, A.P. Street, and J.S. Wallis, *Combinatorics: Room squares, sum-free sets, hadamard matrices*, Lecture Notes in Mathematics, vol. 292, Springer-Verlag, Berlin-Heidelberg-New York, 1972.

Department of Mathematics
University of Colorado at Denver
Campus Box 170
P.O. Box 173364
Denver, Colorado 80217-3364
USA
email: william.cherowitzo@cudenver.edu

Mathematics Department
St. Mary's University
One Camino Santa Maria
San Antonio, Texas 78228-8560
USA
email:lholder@stmarytx.edu