

page 1 / 23

go back

full screen

close

quit

Semiovals from unions of conics

Jeremy M. Dover

Keith E. Mellinger*

Abstract

A semioval in a projective plane π is a collection of points \mathcal{O} with the property that for every point P of \mathcal{O} , there exists exactly one line of π meeting \mathcal{O} precisely in the point P . There are many known constructions of and theoretical results about semiovals, especially those that contain large collinear subsets.

In a Desarguesian plane π a conic, the set of zeroes of some nondegenerate quadratic form, is an example of a semioval of size $q + 1$ that also forms an arc (i.e., no three points are collinear). As conics are minimal semiovals, it is natural to use them as building blocks for larger semiovals. Our goal in this work is to classify completely the sets of conics whose union forms a semioval.

Keywords: semioval, conic

MSC 2000: 51E20

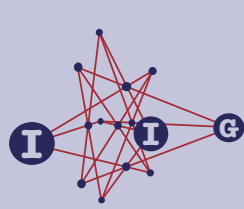
1. Introduction

Let $\text{GF}(q)$ denote the finite field of order q , and let $\text{GF}(q)^*$ denote the set of nonzero elements in this field. Let $\mathcal{PG}(2, q)$ denote the finite Desarguesian projective plane over $\text{GF}(q)$. A semioval in $\mathcal{PG}(2, q)$ is a collection of points \mathcal{O} with the property that for every point P of \mathcal{O} , there exists exactly one line meeting \mathcal{O} precisely in the point P . A well-known construction for semiovals is the vertexless triangle, the set of points formed by the union of three non-concurrent lines with the intersection points removed. Many other constructions of semiovals can be formed by taking the vertexless triangle and then adding and removing

*Author acknowledges support by a Faculty Development Grant from the University of Mary Washington.

ACADEMIA
PRESS





page 2 / 23

go back

full screen

close

quit

certain points in some clever fashion so as to maintain the semioval property. A nice survey of results on semiovals can be found in Kiss [5].

In the context of minimal blocking sets, Szőnyi [8] looked at collections of conics lying in a common conic pencil, such that their union forms a blocking set, i.e. a set disjoint from no line but also containing no line. Kiss, et. al. [6], later discovered that Szőnyi's sets are in fact semiovals. Extending the work found in these two papers, our goal here is to characterize all sets of conics in $\mathcal{PG}(2, q)$ whose union is a semioval in the plane. We summarize our principal result here.

Theorem 1.1. *Let \mathcal{O} be a semioval in $\mathcal{PG}(2, q)$ that is the union of conics. Then \mathcal{O} is a conic, or q is odd and \mathcal{O} is either the union of at most \sqrt{q} conics all lying in a common pencil, or the union of three or four conics, no three in a common pencil.*

We prove this result with a thorough case analysis in the following sections. Our analysis, using both algebraic and synthetic techniques, shows that both the existence of and spectrum of sizes for each of these types of semiovals depends on the value of q .

2. Semiovals, conics and interior points

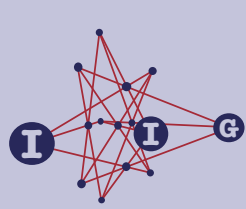
Consider $\mathcal{PG}(2, q)$ as a three-dimensional vector space over the finite field $\text{GF}(q)$ using homogenous coordinates. Letting P be any quadratic form in these homogenous coordinates, it is well known that the set of zeroes of P , denoted $V(P)$, is isomorphic to one of four sets: a point, a line, or a line pair, which occur when P is degenerate; or a conic when P is nondegenerate. Conics contain $q + 1$ points forming an arc, i.e., no three points collinear, so that lines meet a conic \mathcal{C} in at most two distinct points. We call lines *secant*, *tangent* or *disjoint* if they meet \mathcal{C} in 2, 1, or 0 points, respectively. We also use this notation to refer to how other conics meet \mathcal{C} . Note that there is a unique tangent line to a conic at each of its points, meaning that every conic is itself a semioval.

When q is even every conic \mathcal{C} in $\mathcal{PG}(2, q)$ has a unique point K not on \mathcal{C} called the *knot* (some use the term *nucleus*) which lies on all of the tangent lines to \mathcal{C} , implying every point not on \mathcal{C} , other than K , lies on a unique tangent line to \mathcal{C} . When q is odd, every point outside of a conic \mathcal{C} in $\mathcal{PG}(2, q)$ lies on either 0 or 2 tangent lines. Points lying on two tangent lines are called *exterior* to \mathcal{C} , while those lying on no tangent lines are called *interior* to \mathcal{C} .

Noting that the definition of an interior point depends only on the concept of tangent lines, we can extend the definition to semiovals.

ACADEMIA
PRESS





page 3 / 23

go back

full screen

close

quit

Definition 2.1. Let \mathcal{O} be any semioval. We call a point P off \mathcal{O} *interior* to \mathcal{O} if it lies on no tangent line of \mathcal{O} .

The importance of interior points to the problem at hand is shown in the following Lemma:

Lemma 2.2. *Let \mathcal{O}_1 and \mathcal{O}_2 be semiovals in $\mathcal{PG}(2, q)$ such that $\mathcal{O}_1 \subset \mathcal{O}_2$. Then every point of $\mathcal{O}_2 \setminus \mathcal{O}_1$ is interior to \mathcal{O}_1 .*

Proof. Let \mathcal{O}_1 and \mathcal{O}_2 be as stated and let Q be a point of \mathcal{O}_1 . Since \mathcal{O}_1 is a semioval, every line through Q except a unique \mathcal{O}_1 -tangent line ℓ contains at least two points of $\mathcal{O}_1 \subset \mathcal{O}_2$. Since \mathcal{O}_2 is a semioval this implies ℓ must be the \mathcal{O}_2 -tangent at Q as well, implying that $\ell \cap (\mathcal{O}_2 \setminus \mathcal{O}_1) = \emptyset$. Thus no point of $\mathcal{O}_2 \setminus \mathcal{O}_1$ lies on an \mathcal{O}_1 -tangent, the definition of being interior to \mathcal{O}_1 . \square

An immediate consequence of this lemma is a characterization of semiovals that contain conics in $\mathcal{PG}(2, q)$ when q is even.

Proposition 2.3. *Any semioval in $\mathcal{PG}(2, q)$, q even, containing a conic is itself a conic. Specifically any semioval that is the union of conics is itself a conic.*

Proof. It was noted earlier that a conic in $\mathcal{PG}(2, q)$, q even, has the property that every point outside the conic is on at least one tangent line, implying that a conic has no interior points. By Lemma 2.2 any semioval containing a conic, which is itself a semioval, must have any additional points interior to the conic. As no such points exist, the semioval must itself be a conic. \square

Another application of Lemma 2.2 gives us a characterization of when the union of two semiovals is a semioval.

Proposition 2.4. *Let \mathcal{O}_1 and \mathcal{O}_2 be semiovals. Then $\mathcal{O} = \mathcal{O}_1 \cup \mathcal{O}_2$ is a semioval if and only if every point of $\mathcal{O}_1 \setminus \mathcal{O}_2$ is interior to \mathcal{O}_2 , and vice versa.*

Proof. If $\mathcal{O} = \mathcal{O}_1 \cup \mathcal{O}_2$ is a semioval, then application of Lemma 2.2 immediately yields the forward direction. For the reverse assume \mathcal{O}_1 and \mathcal{O}_2 are semiovals such that every point of $\mathcal{O}_1 \setminus \mathcal{O}_2$ (resp. $\mathcal{O}_2 \setminus \mathcal{O}_1$) is interior to \mathcal{O}_2 (resp. \mathcal{O}_1). If $P \in \mathcal{O}_1$, then every line through P except its \mathcal{O}_1 -tangent ℓ meets \mathcal{O}_1 and thus \mathcal{O} in at least two points. But ℓ has to be tangent to \mathcal{O} , since ℓ meets \mathcal{O}_1 in one point and is disjoint from $\mathcal{O}_2 \setminus \mathcal{O}_1$ as those points are interior to \mathcal{O}_1 . The symmetric argument shows that \mathcal{O} has a unique tangent at points of \mathcal{O}_2 as well, completing the result. \square

ACADEMIA
PRESS





page 4 / 23

go back

full screen

close

quit

For semiovals \mathcal{O}_1 and \mathcal{O}_2 meeting the conditions of this Proposition, one consequence of the proof is that at a point $P \in \mathcal{O}_1 \cap \mathcal{O}_2$, both the \mathcal{O}_1 -tangent and the \mathcal{O}_2 -tangent at P are tangent lines to $\mathcal{O} = \mathcal{O}_1 \cup \mathcal{O}_2$ at P . But \mathcal{O} being a semioval forces these two tangent lines to be equal, proving the following

Corollary 2.5. *Let \mathcal{O}_1 and \mathcal{O}_2 be semiovals such that every point of $\mathcal{O}_1 \setminus \mathcal{O}_2$ is interior to \mathcal{O}_2 , and vice versa. If $P \in \mathcal{O}_1 \cap \mathcal{O}_2$, then the tangent lines to \mathcal{O}_1 and \mathcal{O}_2 at P are identical.*

Proposition 2.4 gives a critical tool we need to investigate unions of conics that are semiovals, leading us to make the

Definition 2.6. Let \mathcal{C}_1 and \mathcal{C}_2 be conics in $\mathcal{PG}(2, q)$, q odd. We say \mathcal{C}_1 and \mathcal{C}_2 are *mutually interior* if $\mathcal{C}_1 \setminus \mathcal{C}_2$ consists of interior points to \mathcal{C}_2 and $\mathcal{C}_2 \setminus \mathcal{C}_1$ consists of interior points to \mathcal{C}_1 . Alternatively, two conics are mutually interior if neither contains an exterior point of the other.

With this new terminology we can inductively apply Proposition 2.4 to show that the union of a set of conics forms a semioval if and only if every pair of conics in the set is mutually interior. Thus our original problem of classifying semiovals that are the unions of conics is equivalent to classifying all sets of pairwise mutually interior conics.

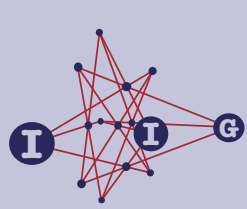
Before moving on, we wish to treat the case $q = 3$ separately, as the notion of a conic degenerates somewhat to any set of four points in general position. When $q = 3$ there are only two inequivalent semiovals in $\mathcal{PG}(2, 3)$ (see Kiss [5]), namely the conic itself and the vertexless triangle. The former obviously contains one conic while the latter contains three conics, namely the four points off any one side, for each side. These facts are not inconsistent with our results, but would require special handling. Thus in what follows we will assume $q \geq 5$.

3. Algebraic description of mutually interior conics

In this section we provide a classification of all pairs of mutually interior conics in $\mathcal{PG}(2, q)$ based on the conic pencil they generate. Any two conics $V(P)$ and $V(Q)$, with P, Q nondegenerate quadratic forms, generate a *conic pencil* defined via the quadratic forms $\langle P, Q \rangle = \{P + \lambda Q : \lambda \in \text{GF}(q)\} \cup \{Q\}$. Note that the pencil generated by two conics may very well contain points, lines or line pairs.

Abatangelo, et. al., [1] took an important step in this direction, wherein the authors determined the spectrum of sizes of the intersection of one conic with





page 5 / 23

go back

full screen

close

quit

the set of exterior points of another. From their results it is possible to derive a result similar to what follows in $\mathcal{PG}(2, q)$ for $q \geq 17$, but we provide a direct proof for all odd q . We first require a result limiting the size of the intersection of two mutually interior conics. In what follows we make use of some classical results from projective geometry, all of which can be found in Chapter 8 of the book by Coxeter [2], for instance. These results describe when a conic is uniquely determined. In particular, five points in general position, four points in general position together with a tangent line through one of these points, and three points in general position together with two tangent lines at these points all uniquely determine a conic.

Proposition 3.1. *Let \mathcal{C}_1 and \mathcal{C}_2 be distinct mutually interior conics in $\mathcal{PG}(2, q)$, q odd. Then, $|\mathcal{C}_1 \cap \mathcal{C}_2| \leq 2$.*

Proof. Since \mathcal{C}_1 and \mathcal{C}_2 are mutually interior, by Corollary 2.5 they share tangent lines at any common points. Hence if \mathcal{C}_1 and \mathcal{C}_2 share three points they must also share the three tangent lines at those points, contradicting the fact that three points and two tangent lines at these points uniquely determine a conic. Thus \mathcal{C}_1 and \mathcal{C}_2 can share at most two points. \square

Being able to determine whether a point is interior or exterior to a given conic will be an important tool in what follows. Denoting the homogeneous coordinates of the points of $\mathcal{PG}(2, q)$ with (x_0, x_1, x_2) , we define the *coefficient matrix* of a conic \mathcal{C} as $A = (a_{ij})$, $i, j \in \{0, 1, 2\}$, a symmetric nonsingular matrix such that the points of \mathcal{C} satisfy

$$\sum_{i,j=0}^2 a_{ij} x_i x_j = 0.$$

We have the following (see [4, Theorem 8.17] or [7, Section 6]).

Lemma 3.2. *Let \mathcal{C} be a conic in $\mathcal{PG}(2, q)$, q odd, with coefficient matrix A . The point (y_0, y_1, y_2) is on \mathcal{C} , exterior to \mathcal{C} , or interior to \mathcal{C} , as*

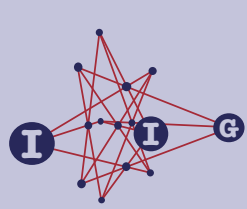
$$\Upsilon = -\det(A) \cdot \sum_{i,j=0}^2 a_{ij} y_i y_j$$

is zero, a nonzero square, or a nonsquare in $\text{GF}(q)$, respectively.

Abatangelo, et.al. [1] describe three types of conic pencils such that for any two distinct conics \mathcal{C}_1 and \mathcal{C}_2 in the pencil, either all of the points of $\mathcal{C}_2 \setminus \mathcal{C}_1$ are exterior to \mathcal{C}_1 , or they are all interior to \mathcal{C}_1 . These three conic pencils play a critical role in our classification, making it worthwhile to describe them here.

ACADEMIA
PRESS





page 6 / 23

go back

full screen

close

quit

The pencil $\langle xy, z^2 \rangle$ which we call the *secant pencil* contains $q - 1$ conics, a line and a line pair. All of the conics in the pencil contain two common points, and share the tangent lines at those two points. The line is the unique line that passes through the two common secant points, and the line pair contains the common tangent lines.

The pencil $\langle x^2 - yz, z^2 \rangle$, called the *tangent pencil*, contains q conics and a line. All of the conics in the pencil share a single point and the tangent line at that point, which is the line of the pencil. The *disjoint pencil* $\langle x^2 - sy^2, z^2 \rangle$, s a fixed nonsquare, contains $q - 1$ conics, a point and a line, with all elements pairwise disjoint.

The following theorem shows that these are the only possible conic pencils generated by a pair of mutually interior conics. Note that we are not yet asserting that these pencils actually do contain mutually interior conics, though we will see in Section 4 that they often do.

Theorem 3.3. *Let C_1 and C_2 be two mutually interior conics in $\mathcal{PG}(2, q)$, q odd. Then the pencil generated by C_1 and C_2 is isomorphic to one of*

1. $\langle xy, z^2 \rangle$, if $|C_1 \cap C_2| = 2$;
2. $\langle x^2 - yz, z^2 \rangle$, if $|C_1 \cap C_2| = 1$; or
3. $\langle x^2 - sy^2, z^2 \rangle$, for fixed nonsquare s , if $|C_1 \cap C_2| = 0$.

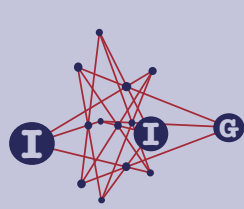
Proof. We split into cases depending on the size of $C_1 \cap C_2$, for which the spectrum of values is $\{0, 1, 2\}$ by Proposition 3.1.

C_1 and C_2 secant: Without loss of generality, we may assume that $C_1 = V(xy + z^2)$, and further that C_2 meets C_1 in the points $(1, 0, 0)$ and $(0, 1, 0)$, hence by Corollary 2.5, C_1 and C_2 also share the tangent lines $[0, 1, 0]$ and $[1, 0, 0]$ at these points. However every conic in the pencil $\langle xy, z^2 \rangle$ also shares these common points and tangents. C_2 must meet some conic $C_k = V(xy + kz^2)$ of the pencil other than C_1 in a further point, forcing C_2 to be identical to C_k as they share three points and tangent lines at two of these points. Hence C_1 and C_2 generate the pencil $\langle xy, z^2 \rangle$.

C_1 and C_2 tangent: Again without loss of generality we can assume that $C_1 = V(x^2 - yz)$ and that $C_1 \cap C_2 = \{(0, 1, 0)\}$. Using Corollary 2.5, C_2 must also share the tangent line $[1, 0, 0]$ with C_1 , and as before C_2 shares the point $(0, 1, 0)$ and the tangent line $[1, 0, 0]$ with every conic in the pencil $\langle x^2 - yz, z^2 \rangle$. Since any conic of that pencil has its noncommon points either wholly exterior or wholly interior to C_1 , the $\frac{1}{2}q(q - 1)$ interior points to C_1 are distributed among $\frac{1}{2}(q - 1)$ conics of the pencil, and the points of C_2 other than $(0, 1, 0)$ must be contained

ACADEMIA
PRESS





page 7 / 23

go back

full screen

close

quit

in the union of these conics. Using the pigeonhole principle, \mathcal{C}_2 must meet one of these conics $\mathcal{C}_k = V(x^2 - yz - kz^2)$ in at least four points, including $(0, 1, 0)$. But then \mathcal{C}_2 and \mathcal{C}_k have four common points and a common tangent at one of those points, which forces them to be equal. Hence \mathcal{C}_1 and \mathcal{C}_2 generate the pencil $\langle x^2 - yz, z^2 \rangle$.

\mathcal{C}_1 and \mathcal{C}_2 disjoint: To prove this case we appeal to a result of Dickson [3], as reported via Hirschfeld [4, Theorem 7.31], regarding the classification of pencils of conics in $\mathcal{PG}(2, q)$. From this classification there are three projectively inequivalent pencils that contain disjoint conics. One ($\langle x^2, y^2 + yz + ez^2 \rangle$, where $1 - 4e$ is a nonsquare, as reported by Hirschfeld) is isomorphic to $\langle x^2 - sy^2, z^2 \rangle$, for fixed nonsquare s ; we exclude the other two pencils here.

First assume that \mathcal{C}_1 and \mathcal{C}_2 generate a pencil isomorphic to $\langle x^2 - \nu y^2, z^2 - ry^2 + 2sxy \rangle$, where ν and $r^2 - 4\nu s^2$ are nonsquares. Without loss of generality we may assume that $\mathcal{C}_1 = V(z^2 - ry^2 + 2sxy)$ and $\mathcal{C}_2 = V(z^2 - ry^2 + 2sxy + \lambda(x^2 - \nu y^2))$ for some $\lambda \in \text{GF}(q)^*$. Using Lemma 3.2 we can calculate that a point $(y_0, y_1, y_2) \in \mathcal{C}_1$ is on, exterior to, or interior to \mathcal{C}_2 as $\Upsilon = -\mu(y_2^2 - ry_1^2 + 2sy_0y_1 + \lambda(y_0^2 - \nu y_1^2))$ is zero, nonzero square or nonsquare, where $\mu = -[\lambda(\lambda\nu + r) + s^2]$, the determinant of the coefficient matrix for \mathcal{C}_2 , is nonzero. Noting that $(y_0, y_1, y_2) \in \mathcal{C}_1$ forces $y_2^2 - ry_1^2 + 2sy_0y_1 = 0$, we have $\Upsilon = -\mu\lambda(y_0^2 - \nu y_1^2)$.

Note that the two points $(1, 0, 0)$ and $(r, 2s, 0)$ both lie in \mathcal{C}_1 . Calculating the value of Υ for both of these points we obtain $-\mu\lambda$ for $(1, 0, 0)$ and $-\mu\lambda(r^2 - 4\nu s^2)$ for $(r, 2s, 0)$. Since $r^2 - 4\nu s^2$ is a nonsquare and $-\mu\lambda$ is nonzero, these two values have opposite quadratic character, meaning that one of $(1, 0, 0), (r, 2s, 0) \in \mathcal{C}_1$ is exterior to \mathcal{C}_2 , which is a contradiction.

Now assume that \mathcal{C}_1 and \mathcal{C}_2 generate a pencil isomorphic to $\langle xy, ex^2 + e'y^2 + xz + yz + z^2 \rangle$, where $1 - 4e$ and $1 - 4e'$ are nonsquares. In this case we may assume that $\mathcal{C}_1 = V(ex^2 + \frac{1}{2}xy + e'y^2 + xz + yz + z^2)$ and $\mathcal{C}_2 = V(ex^2 + \lambda xy + e'y^2 + xz + yz + z^2)$ for some $\lambda \in \text{GF}(q)$. Since the line pair $V(xy)$ is in the pencil and the elements of the pencil are pairwise disjoint, the $q + 1$ points of \mathcal{C}_1 must all be of the form $(1, y_1, y_2)$ for some $y_1, y_2 \in \text{GF}(q)$ where $y_1, y_2 \neq 0$.

Using Lemma 3.2 in the same way as before we can calculate that a point $(1, y_1, y_2) \in \mathcal{C}_1$ is on, exterior to, or interior to \mathcal{C}_2 as $\Upsilon = -\kappa(\lambda - \frac{1}{2})y_1$ is zero, a nonzero square or a nonsquare, where κ , the determinant of the coefficient matrix for \mathcal{C}_2 , is nonzero. Since \mathcal{C}_1 and \mathcal{C}_2 are mutually interior, this means that y_1 must have a fixed quadratic character as $(1, y_1, y_2)$ varies over all points of \mathcal{C}_1 , hence y_1 can take on at most $\frac{1}{2}(q - 1)$ values. But for a fixed y_1 , all points of the form $(1, y_1, y_2)$ are collinear on $[-y_1, 1, 0]$, meaning that for any value y_1 there are at most two points of the form $(1, y_1, y_2)$ in \mathcal{C}_1 . This forces \mathcal{C}_1 to contain at

ACADEMIA
PRESS





page 8 / 23

go back

full screen

close

quit

most $q - 1$ points, a contradiction. \square

The following important corollary gives us an algebraic relationship between the forms of two arbitrary mutually interior conics.

Corollary 3.4. *Let $\mathcal{C}_1 = V(P)$ and $\mathcal{C}_2 = V(Q)$ be distinct mutually interior conics in $\mathcal{PG}(2, q)$, q odd. Then there exists $\lambda \in \text{GF}(q)^*$ and a linear polynomial L such that $\mathcal{C}_2 = V(P + \lambda L^2)$.*

Proof. By Theorem 3.3, regardless of how \mathcal{C}_1 and \mathcal{C}_2 intersect the pencil they generate contains a line ($V(z^2)$ for the forms in the theorem statement). Thus there is a linear polynomial L such that the line $V(L^2)$ is in the pencil generated by \mathcal{C}_1 and \mathcal{C}_2 . Since any two distinct forms in the pencil generate the pencil, we can write $Q = \mu P + \chi L^2$ for some nonzero $\mu, \chi \in \text{GF}(q)$. Setting $\lambda = \frac{\chi}{\mu}$, this implies $\mathcal{C}_2 = V(P + \lambda L^2)$, proving the result. \square

4. Semiovals from copencilar conics

In [6], Kiss, et. al. show that the blocking sets constructed by Szőnyi [8] are semiovals. Viewed in context of the previous section, the method used is to construct a set of mutually interior conics which are contained in the tangent pencil $\langle x^2 - yz, z^2 \rangle$. In this section we generalize that result to disjoint and secant pencils and also prove a characterization of all semiovals that can be obtained from the union of copencilar conics.

Theorem 4.1. *$\mathcal{M} = \{\mathcal{C}_1, \dots, \mathcal{C}_k\}$ is a set of mutually interior, copencilar conics in $\mathcal{PG}(2, q)$, q odd, if and only if \mathcal{M} is isomorphic to one of the sets*

1. $\{V(xy + a_i z^2)\}$, where $\{a_1, \dots, a_k\} \subset \text{GF}(q)^*$ such that $a_i(a_i - a_j)$ is a nonsquare for all $i \neq j$; or
2. $\{V(x^2 - yz - a_i z^2)\}$ where $\{a_1, \dots, a_k\} \subset \text{GF}(q)$ such that $a_i - a_j$ is a nonsquare for all $i \neq j$; or
3. $\{V(x^2 - sy^2 + a_i z^2)\}$ where s is a fixed nonsquare and $\{a_1, \dots, a_k\} \subset \text{GF}(q)^*$ such that $a_i(a_i - a_j)$ is a nonzero square for all $i \neq j$.

Proof. By Theorem 3.3 we may assume without loss of generality that the conics $\mathcal{C}_1, \dots, \mathcal{C}_k$ lie in one of these three conic pencils. We split into cases:

ACADEMIA
PRESS



UNIVERSITEIT
GENT



page 9 / 23

go back

full screen

close

quit

Secant pencil $\langle xy, z^2 \rangle$: For all $i \in \{1, \dots, k\}$, $C_i = V(xy + a_i z^2)$ for some $a_i \in \text{GF}(q)^*$, as $V(xy)$ and $V(z^2)$ are the line pair and line of the pencil. For any conics $C_i, C_j \in \mathcal{M}$, C_i and C_j are mutually interior, meaning that neither contains an exterior point of the other. Using Lemma 3.2, we find that a point $(y_0, y_1, y_2) \in C_j$ is exterior to C_i if and only if $\frac{1}{4}a_i(y_0 y_1 + a_i y_2^2)$ is a nonzero square. Since $(y_0, y_1, y_2) \in C_j$ we have $y_0 y_1 = -a_j y_2^2$, so $(y_0, y_1, y_2) \in C_j$ is exterior to C_i if and only if $a_i(a_i - a_j)y_2^2$ is a nonzero square. Since C_j contains no exterior points of C_i , the expression $a_i(a_i - a_j)$ must be a nonsquare, a relationship which holds for all pairs of distinct conics in $C_i, C_j \in \mathcal{M}$.

Conversely suppose $\{a_1, \dots, a_k\} \subset \text{GF}(q)^*$ satisfies $a_i(a_i - a_j)$ nonsquare for all distinct a_i, a_j , and let $\mathcal{M} = \{C_i\}$ where $C_i = V(xy + a_i z^2)$. Let C_i and C_j be two conics in \mathcal{M} . If $(y_0, y_1, y_2) \in C_j$ then as above (y_0, y_1, y_2) is exterior to C_i if and only if $a_i(a_i - a_j)y_2^2$ is a nonzero square, implying C_j contains no exterior point of C_i . Interchanging the roles of C_i and C_j shows that C_i and C_j are mutually interior.

Tangent pencil $\langle x^2 - yz, z^2 \rangle$: The flow of the proof is the same as the previous case; the only differences are that $V(x^2 - yz)$ is a conic in this case, so a_i can be zero for some i ; and the expression used to determine when C_i and C_j are mutually interior. For all $i \in \{1, \dots, k\}$, $C_i = V(x^2 - yz - a_i z^2)$ for some $a_i \in \text{GF}(q)$. As above for conics C_i and C_j , $(y_0, y_1, y_2) \in C_i$ is exterior to C_j if and only if $\frac{1}{4}(y_0^2 - y_1 y_2 - a_j y_2^2)$ is a nonzero square, or equivalently if $(a_i - a_j)y_2^2$ is a nonzero square since $(y_0, y_1, y_2) \in C_i$. This forces $a_i - a_j$ to be a nonsquare for all distinct a_i, a_j .

Disjoint pencil $\langle x^2 - sy^2, z^2 \rangle$, s nonsquare: In this case for all $i \in \{1, \dots, k\}$, $C_i = V(x^2 - sy^2 + a_i z^2)$ for some $a_i \in \text{GF}(q)^*$, as $V(x^2 - sy^2)$ and $V(z^2)$ are the point and line of the pencil. As above for conics C_i and C_j , $(y_0, y_1, y_2) \in C_j$ is exterior to C_i if and only if $sa_i(y_0^2 - sy_1^2 + a_i y_2^2)$ is a nonzero square, or equivalently if and only if $a_i(a_i - a_j)$ is a nonsquare, since $(y_0, y_1, y_2) \in C_j$ and s is a nonsquare. This forces $a_i(a_i - a_j)$ to be a nonzero square for all distinct a_i, a_j . \square

Given these field theoretic conditions on the set $S = \{a_1, \dots, a_k\}$ of parameters for each of these cases, it is a natural question to ask how large these sets can be. Noting that the upper bound for the size of a semioval is $q\sqrt{q} + 1$, the maximum size for the secant and tangent cases is \sqrt{q} , while for the disjoint case the maximum size is $\sqrt{q} - 1$. Szőnyi [8] shows that in the tangent case, this upper bound is met when q is a square by taking $S = \{sk : k \in \text{GF}(\sqrt{q})^*\}$ for a fixed nonsquare s , and that in fact the resulting set is a unital that is the union of conics. Similarly in the disjoint case, it is not hard to see that taking

ACADEMIA
PRESS





page 10 / 23

go back

full screen

close

quit

$S = \text{GF}(\sqrt{q})^*$ yields a maximum set of $\sqrt{q} - 1$ mutually interior conics in the disjoint pencil.

The secant case does not easily generate such maximum examples. Examining the condition on the parameters for the secant case, it is easy to see that when $q \equiv 1 \pmod{4}$ any set of squares whose pairwise differences are non-squares satisfies the parameter conditions. We give one such construction in

Proposition 4.2. *Let q be an odd square, and let s be a fixed nonsquare in $\text{GF}(q)$. Then for each $x \in \text{GF}(\sqrt{q})^*$ the set $T_x = \{x + ys : y \in \text{GF}(\sqrt{q})\}$ contains $\frac{1}{2}(\sqrt{q} + 1)$ nonzero squares, denoted by S_x , whose pairwise differences are non-squares. Moreover, the set S_x is maximal subject to these conditions.*

Proof. It is clear that the pairwise differences of elements in T_x are nonsquares for all $x \in \text{GF}(\sqrt{q})$; indeed T_0 is precisely the set used to generate the maximal set of mutually interior tangent conics.

Note that $\{1, s\}$ forms a basis for $\text{GF}(q)$ over $\text{GF}(\sqrt{q})$ so that $\text{GF}(q)$ is partitioned by the sets T_x as x varies over $\text{GF}(\sqrt{q})$. If $x = 0$, T_x clearly consists entirely of nonsquares, hence the $\frac{1}{2}(q - 1)$ nonzero squares in $\text{GF}(q)$ must be in the sets T_x for nonzero $x \in \text{GF}(\sqrt{q})$.

We claim that these are distributed equally; to show this let $x_1, x_2 \in \text{GF}(\sqrt{q})^*$, and let κ be such that $x_2 = \kappa x_1$. For all $z = x_1 + ys \in T_{x_1}$, $\kappa z = x_2 + y\kappa s \in T_{x_2}$, so multiplication by κ is a bijection from T_{x_1} onto T_{x_2} . Moreover $\kappa \in \text{GF}(\sqrt{q})^*$ implies κ is a square in $\text{GF}(q)$, meaning that multiplication by κ maps the squares S_{x_1} bijectively onto the squares S_{x_2} . Hence S_{x_1} and S_{x_2} have the same cardinality, and simple division then yields that each S_x contains $\frac{1}{2}(\sqrt{q} + 1)$ squares for all $x \in \text{GF}(\sqrt{q})^*$. Note that this also implies T_x contains $\frac{1}{2}(\sqrt{q} - 1)$ nonsquares for all $x \in \text{GF}(\sqrt{q})^*$.

To show the maximality of S_x , let the elements of S_x be denoted k_i for $i \in \{1, \dots, \frac{1}{2}(\sqrt{q} + 1)\}$, and let z be a square in $\text{GF}(q)$ such that $z - k_i$ is a nonsquare for all i . We can write z uniquely as $\alpha + \beta s$ for some $\alpha, \beta \in \text{GF}(\sqrt{q})$, and for each i we can also write $k_i = x + y_i s$ for some $y_i \in \text{GF}(\sqrt{q})$.

By our assertion, $\{z - k_i\}$ is a set of $\frac{1}{2}(\sqrt{q} + 1)$ distinct nonsquares. But we can write $z - k_i = (\alpha - x) + (\beta - y_i)s$, which implies that $\{z - k_i\}$ is a set of $\frac{1}{2}(\sqrt{q} + 1)$ distinct nonsquares in $T_{\alpha - x}$. By the previous result, the only T_c which contains $\frac{1}{2}(\sqrt{q} + 1)$ distinct nonsquares is T_0 , which forces $\alpha = x$. But this implies $z \in S_x$, which proves S_x is maximal. \square

When $q \equiv 3 \pmod{4}$, we can use Theorem 4.1 to prove much tighter bounds on the size of sets of mutually interior conics in a pencil, because -1 is a non-square in this case.

ACADEMIA
PRESS





page 11 / 23

go back

full screen

close

quit

Corollary 4.3. *Let $\mathcal{M} = \{\mathcal{C}_1, \dots, \mathcal{C}_k\}$ be a set of mutually interior, copencilar conics in $\mathcal{PG}(2, q)$, $q \equiv 3 \pmod{4}$. Then $k \leq 2$, and if there are two conics in \mathcal{M} , they are either disjoint or secant.*

Proof. For the secant case suppose \mathcal{C}_1 and \mathcal{C}_2 are two distinct mutually interior conics in \mathcal{M} . Then by Theorem 4.1 we may assume $\mathcal{C}_i = V(xy + a_i z^2)$ for $i = 1, 2$ where $a_1(a_1 - a_2)$ and $a_2(a_2 - a_1)$ are both nonsquares. Since $a_1 - a_2$ and $a_2 - a_1$ have opposite quadratic character, a_1 and a_2 must have opposite quadratic character as well. This property holds true for all pairs of conics in \mathcal{M} and there are only two choices for the quadratic character, thus \mathcal{M} contains at most two conics. The proof for the disjoint case is similar.

For the tangent case suppose \mathcal{C}_1 and \mathcal{C}_2 are two distinct mutually interior conics in \mathcal{M} . Then by Theorem 4.1 we may assume $\mathcal{C}_i = V(x^2 - yz - a_i z^2)$ for $i = 1, 2$ where $a_1 - a_2$ and $a_2 - a_1$ are both nonsquares. But these two quantities have opposite quadratic character, meaning no such pair of mutually interior conics can exist in the tangent case. \square

5. Semiovals from non-copencilar conics

In this section we address the possibility that a semioval can be the union of conics that do not all lie in the same conic pencil. Our first results in this direction show that if such a semioval exists, all of the conics in the semioval must be mutually secant. We begin with a simple counting argument that calculates the number of points interior to both of a pair of mutually interior conics. For both Propositions 5.1 and 5.2, note that there are no disjoint mutually interior conics when $q < 7$, so the seemingly nonsensical negative counts that result never occur.

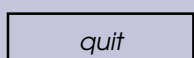
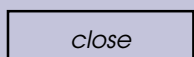
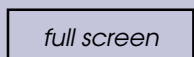
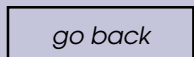
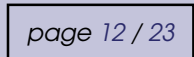
Proposition 5.1. *Let \mathcal{C}_1 and \mathcal{C}_2 be mutually interior conics in $\mathcal{PG}(2, q)$, $q \geq 5$ odd. Then the number of points interior to both \mathcal{C}_1 and \mathcal{C}_2 is $\frac{1}{4}(q^2 - 4q + 3)$, $\frac{1}{4}(q^2 - 5q)$, or $\frac{1}{4}(q^2 - 6q - 3)$ as \mathcal{C}_1 and \mathcal{C}_2 are secant, tangent or disjoint, respectively.*

Proof. Even though the results differ, the proof is practically identical for the secant, tangent and disjoint cases. Thus we treat all three cases simultaneously. Let \mathcal{C}_1 and \mathcal{C}_2 be mutually interior conics in $\mathcal{PG}(2, q)$ for q odd. We first count the number of points that are exterior to both conics. Let X be this desired number and consider the set of flags

$$\mathcal{F} = \{(P, m) : P \text{ exterior to both } \mathcal{C}_1 \text{ and } \mathcal{C}_2, m \text{ tangent to } \mathcal{C}_1\}.$$

Starting with the point P , there are X ways to pick the point, and then two choices for the tangent m to form a flag in \mathcal{F} , so $|\mathcal{F}| = 2X$.





Now we count the number of flags in \mathcal{F} by picking the tangent line first. There are two types of tangent lines to \mathcal{C}_1 : tangents at points in $\mathcal{C}_1 \cap \mathcal{C}_2$ (type I), and tangents at points in $\mathcal{C}_1 \setminus \mathcal{C}_2$ (type II). For a type I tangent, by Corollary 2.5 the tangent line m to \mathcal{C}_1 at a point of $\mathcal{C}_1 \cap \mathcal{C}_2$ must also be tangent to \mathcal{C}_2 at this point, meaning that the q points of m not in \mathcal{C}_1 are exterior to both \mathcal{C}_1 and \mathcal{C}_2 . Thus a type I tangent line is contained in q flags in \mathcal{F} .

For the type II tangent, let m be a tangent to \mathcal{C}_1 at a point P of $\mathcal{C}_1 \setminus \mathcal{C}_2$. Since \mathcal{C}_1 and \mathcal{C}_2 are mutually interior, m must be disjoint from \mathcal{C}_2 , meaning that there are $\frac{1}{2}(q+1)$ points on m exterior to \mathcal{C}_2 . P is not one of these points, since $P \in \mathcal{C}_1$ forcing P to be interior to \mathcal{C}_2 . Hence these $\frac{1}{2}(q+1)$ exterior points to \mathcal{C}_2 are also exterior to \mathcal{C}_1 . Thus each type II tangent is contained in $\frac{1}{2}(q+1)$ flags in \mathcal{F} .

To complete our count, we must break into cases depending on how \mathcal{C}_1 and \mathcal{C}_2 meet. If \mathcal{C}_1 and \mathcal{C}_2 are secant, then there are two type I tangents and $q-1$ type II tangents, meaning $|\mathcal{F}| = 2q + \frac{1}{2}(q+1)(q-1) = \frac{1}{2}(q^2 + 4q - 1)$ from which we conclude that X , the number of points exterior to both \mathcal{C}_1 and \mathcal{C}_2 is $\frac{1}{4}(q^2 + 4q - 1)$. If \mathcal{C}_1 and \mathcal{C}_2 are tangent then there is one type I tangent, and q type II tangents, yielding $\frac{1}{4}(q^2 + 3q)$ points exterior to \mathcal{C}_1 and \mathcal{C}_2 . If \mathcal{C}_1 and \mathcal{C}_2 are disjoint all tangents are type II, and the number of points exterior to both \mathcal{C}_1 and \mathcal{C}_2 is $\frac{1}{4}(q^2 + 2q + 1)$.

There are $\frac{1}{2}q(q+1)$ exterior points to \mathcal{C}_1 . None of these points lie on \mathcal{C}_2 by the mutually interior property, and we just counted the number of these points that are also exterior to \mathcal{C}_2 . In the secant case this implies that $\frac{1}{2}q(q+1) - \frac{1}{4}(q^2 + 4q - 1) = \frac{1}{4}(q^2 - 2q + 1)$ points must be exterior to \mathcal{C}_1 but interior to \mathcal{C}_2 . The same calculation yields $\frac{1}{4}(q^2 - q)$ and $\frac{1}{4}(q^2 - 1)$ points exterior to \mathcal{C}_1 but interior to \mathcal{C}_2 in the tangent and disjoint cases respectively.

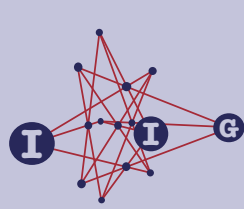
Similarly there are $\frac{1}{2}q(q-1)$ points interior to \mathcal{C}_2 , and these points are either exterior to, on, or interior to \mathcal{C}_1 . We have just counted the number of interior points to \mathcal{C}_2 that are exterior to \mathcal{C}_1 , and the points of $\mathcal{C}_1 \setminus \mathcal{C}_2$ are on \mathcal{C}_1 but interior to \mathcal{C}_2 . Thus in the secant case the number of points interior to both \mathcal{C}_1 and \mathcal{C}_2 is $\frac{1}{2}q(q-1) - \frac{1}{4}(q^2 - 2q + 1) - (q-1) = \frac{1}{4}(q^2 - 4q + 3)$. The same calculation yields $\frac{1}{4}(q^2 - 5q)$ and $\frac{1}{4}(q^2 - 6q - 3)$ points interior to both \mathcal{C}_1 and \mathcal{C}_2 in the tangent and disjoint cases respectively. \square

Now that we know the number of common interior points to two mutually interior conics, we can look at how these points are distributed amongst the elements of the pencils they generate.

Proposition 5.2. *Let \mathcal{C}_1 and \mathcal{C}_2 be mutually interior conics in $\mathcal{PG}(2, q)$, $q \geq 5$ odd.*

ACADEMIA
PRESS





page 13 / 23

go back

full screen

close

quit

- (i) If C_1 and C_2 are disjoint, then the set of points interior to both C_1 and C_2 is exactly the union of the point, $\frac{1}{2}(q+1)$ points on the line, and $\frac{1}{4}(q-9)$ conics of the pencil generated by C_1 and C_2 , if $q \equiv 1 \pmod{4}$; and the union of the point and $\frac{1}{4}(q-7)$ conics of the pencil generated by C_1 and C_2 , if $q \equiv 3 \pmod{4}$.
- (ii) If C_1 and C_2 are tangent, then the set of points interior to both C_1 and C_2 is exactly the union of the points in $\frac{1}{4}(q-5)$ conics of the pencil generated by C_1 and C_2 , less their common point of intersection.
- (iii) If C_1 and C_2 are secant, then the set of points interior to both C_1 and C_2 is exactly the union of $\frac{1}{2}(q-1)$ points on the line and $\frac{1}{4}(q-5)$ conics of the pencil generated by C_1 and C_2 , less their common points of intersection, if $q \equiv 1 \pmod{4}$; and the union of $\frac{1}{4}(q-3)$ conics of the pencil generated by C_1 and C_2 , less their common points of intersection, if $q \equiv 3 \pmod{4}$.

Proof. In the disjoint case, by Theorem 3.3 we may assume without loss of generality that the pencil generated by C_1 and C_2 is $\langle x^2 - sy^2, z^2 \rangle$ for some fixed nonsquare $s \in \text{GF}(q)$. Note that the quadratic form $x^2 - sy^2$ corresponds to the point $(0, 0, 1)$, and the form z^2 corresponds to the line $[0, 0, 1]$, so we may take $C_1 = V(x^2 - sy^2 + z^2)$ and $C_2 = V(x^2 - sy^2 + kz^2)$ for some $k \in \text{GF}(q)^*$, $k \neq 1$. Theorem 4.1 shows that $1 - k$ must be a nonzero square for all odd q , but that k is nonzero square when $q \equiv 1 \pmod{4}$, and k is a nonsquare for $q \equiv 3 \pmod{4}$.

Using the condition of Lemma 3.2, the point $(0, 0, 1)$ is interior to the conic $V(x^2 - sy^2 + tz^2)$ of our pencil if and only if st^2 is a nonsquare. Since s is a nonsquare this condition is met for all conics in the pencil, hence the point $(0, 0, 1)$ is interior to all of them. Now consider the line $[0, 0, 1]$. Again using Lemma 3.2 point $(1, a, 0)$ on this line is interior to C_1 if $s(1 - sa^2)$ is a nonsquare, and $(0, 1, 0)$ is interior to C_1 if $-s^2$ is a nonsquare. Similarly $(1, a, 0)$ is interior to C_2 if $sk(1 - sa^2)$ is a nonsquare, and $(0, 1, 0)$ is interior to C_2 if $-ks^2$ is a nonsquare. In particular the $\frac{1}{2}(q+1)$ interior points to C_1 on $[0, 0, 1]$ are also interior to C_2 if and only if k is a square. Hence when $q \equiv 1 \pmod{4}$ there are $\frac{1}{2}(q+1)$ interior points to C_1 and C_2 on $[0, 0, 1]$, while when $q \equiv 3 \pmod{4}$ there are none.

As shown in Abatangelo, et. al. [1] every conic in the pencil is either wholly interior to or wholly exterior to any other conic in the pencil. When $q \equiv 1 \pmod{4}$, the point and $\frac{1}{2}(q+1)$ points of the line are interior to both C_1 and C_2 . Using Proposition 5.1 we find that this leaves $\frac{1}{4}(q^2 - 6q - 3) - 1 - \frac{1}{2}(q+1) = \frac{1}{4}(q-9)(q+1)$ points remaining, which must be covered by $\frac{1}{4}(q-9)$ conics of the pencil generated by C_1 and C_2 . Thus the set of points interior to both C_1 and C_2 is the union of the point, $\frac{1}{2}(q+1)$ points on the line, and $\frac{1}{4}(q-9)$ conics of the pencil, as claimed. The calculation for $q \equiv 3 \pmod{4}$ is similar.

ACADEMIA
PRESS





page 14 / 23

go back

full screen

close

quit

The tangent case is substantially easier since the line of the pencil is tangent to all conics in the pencil, meaning it contains no interior points to any conics in the pencil. Excepting the common point of intersection we again have that the points of every conic in the pencil are either wholly exterior to or wholly interior to any other conic in the pencil. Thus the $\frac{1}{2}(q^2 - 5q)$ points interior to \mathcal{C}_1 and \mathcal{C}_2 must be covered by the q noncommon points of $\frac{1}{2}(q - 5)$ conics in the pencil.

In the secant case we again use Theorem 3.3 to assume without loss of generality that $\mathcal{C}_1 = V(xy + z^2)$ and $\mathcal{C}_2 = V(xy + kz^2)$, $k \in \text{GF}(q)^*$ are mutually interior conics. As above Theorem 4.1 shows that k is a nonzero square when $q \equiv 1 \pmod{4}$, and a nonsquare when $q \equiv 3 \pmod{4}$.

Since the line pair is a pair of common tangent lines to all conics in the pencil, every point on the line pair is either on or exterior to every conic of the pencil. Looking at the line $[0, 0, 1]$ we use Lemma 3.2 to see that $(1, a, 0)$ on this line is interior to \mathcal{C}_1 if a is a nonsquare (note that $(0, 1, 0)$ is contained in each conic of the pencil). Similarly $(1, a, 0)$ is interior to \mathcal{C}_2 if ka is a nonsquare. Thus the $\frac{1}{2}(q - 1)$ interior points to \mathcal{C}_1 on $[0, 0, 1]$ are also interior to \mathcal{C}_2 only if k is a square, i.e., when $q \equiv 1 \pmod{4}$.

When $q \equiv 1 \pmod{4}$ the $\frac{1}{4}(q^2 - 4q + 3) - \frac{1}{2}(q - 1) = \frac{1}{4}(q^2 - 6q + 5)$ points interior to both \mathcal{C}_1 and \mathcal{C}_2 but not on $[0, 0, 1]$ must be covered by the $q - 1$ noncommon points of $\frac{1}{4}(q - 5)$ conics of the pencil. When $q \equiv 3 \pmod{4}$, all $\frac{1}{4}(q^2 - 4q + 3)$ points interior to both \mathcal{C}_1 and \mathcal{C}_2 must be covered by $\frac{1}{4}(q - 3)$ conics of the pencil. \square

With these two propositions in hand, we are in position to prove our key nonexistence result.

Theorem 5.3. *Let $\mathcal{M} = \{\mathcal{C}_1, \dots, \mathcal{C}_k\}$ be a set of mutually interior conics in $\mathcal{PG}(2, q)$, q odd. If any pair of conics \mathcal{C}_i and \mathcal{C}_j in \mathcal{M} is either disjoint or tangent, then all of the conics contained in \mathcal{M} are in the pencil generated by \mathcal{C}_i and \mathcal{C}_j .*

Proof. Suppose first that we have two disjoint conics in \mathcal{M} , which we can assume are \mathcal{C}_1 and \mathcal{C}_2 . If there are no additional conics in \mathcal{M} we are done, so let \mathcal{C}_i be any other conic in \mathcal{M} . By definition \mathcal{C}_i is mutually interior to both \mathcal{C}_1 and \mathcal{C}_2 . By Proposition 3.1 \mathcal{C}_i could meet both \mathcal{C}_1 and \mathcal{C}_2 in up to two points each, implying that at least $q - 3$ points of \mathcal{C}_i must be interior to both \mathcal{C}_1 and \mathcal{C}_2 .

We wish to use Proposition 5.2, but must split into cases depending on q . If $q \equiv 1 \pmod{4}$ at least $q - 3$ points of \mathcal{C}_i must be contained in the disjoint union of the point, $\frac{1}{2}(q + 1)$ points on the line, and $\frac{1}{4}(q - 9)$ conics of the pencil generated by \mathcal{C}_1 and \mathcal{C}_2 . If \mathcal{C}_i is one of the conics in the pencil we are done, so assume not. Then \mathcal{C}_i could contain the point, at most 2 points of the line, and





page 15 / 23

go back

full screen

close

quit

at most 4 points of each of the $\frac{1}{4}(q-9)$ conics above. But this means \mathcal{C}_i has at most $4 + 1 + 2 + (q-9) = q-2$ points, a contradiction. Hence \mathcal{C}_i must be a conic of the pencil generated by \mathcal{C}_1 and \mathcal{C}_2 . The argument when $q \equiv 3 \pmod{4}$ is similar, where \mathcal{C}_1 could possibly contain the point and at most four points from each of $\frac{1}{4}(q-7)$, again yielding a maximum possible size of $q-2$ points, and forcing \mathcal{C}_i to be a conic of the pencil generated by \mathcal{C}_1 and \mathcal{C}_2 .

Suppose now that \mathcal{C}_1 and \mathcal{C}_2 are tangent, and again suppose \mathcal{C}_i is another conic in \mathcal{M} . As above \mathcal{C}_i could contain up to two points each of \mathcal{C}_1 and \mathcal{C}_2 , meaning at least $q-3$ points of \mathcal{C}_i must be interior to both \mathcal{C}_1 and \mathcal{C}_2 . Using Proposition 5.2 we see that at least $q-3$ points of \mathcal{C}_i must be contained in the union of $\frac{1}{4}(q-5)$ conics. Thus either \mathcal{C}_i is one of these conics, or \mathcal{C}_i contains at most $4 + (q-5) = q-1$ points, again a contradiction. This again forces \mathcal{C}_i to be a conic in the pencil generated by \mathcal{C}_1 and \mathcal{C}_2 . \square

So to this point we have shown that any semioval that is the union of non-copencilar conics must have the property that any two conics in the semioval are pairwise secant, which is about as far as combinatorics can get us. We now move toward a more algebraic approach, which allows to classify all of the conics that are mutually interior to a pair of mutually interior secant conics, but not in the pencil they generate.

Theorem 5.4. *Let \mathcal{C}_1 and \mathcal{C}_2 be distinct mutually interior secant conics in $\mathcal{PG}(2, q)$, q odd. By Theorem 4.1, we may assume without loss of generality that $\mathcal{C}_1 = V(xy + z^2)$ and $\mathcal{C}_2 = V(xy + kz^2)$ for some fixed $k \in \text{GF}(q)^*$ where k is a square, $k-1$ is a nonsquare when $q \equiv 1 \pmod{4}$, or k is a nonsquare with $k-1$ a square when $q \equiv 3 \pmod{4}$. Then the set of conics mutually interior to both \mathcal{C}_1 and \mathcal{C}_2 but not in the pencil $\langle xy, z^2 \rangle$ they generate is*

$$\{V(xy + z^2 + \lambda(ax + y)^2)\}$$

where $\lambda a = \frac{1-k}{4k}$ with $-\lambda$ a nonsquare.

Proof. Let \mathcal{C}_1 and \mathcal{C}_2 be as in the theorem statement, and suppose \mathcal{D} is mutually interior to both, but not in the pencil they generate. Using Corollary 3.4, since \mathcal{D} is mutually interior with \mathcal{C}_1 we have $\mathcal{D} = V(xy + z^2 + \lambda_1(a_1x + b_1y + c_1z)^2)$ for some $\lambda_1 \in \text{GF}(q)^*$ and $a_1, b_1, c_1 \in \text{GF}(q)$. But \mathcal{D} is also mutually interior with \mathcal{C}_2 , implying $\mathcal{D} = V(xy + kz^2 + \lambda_2(a_2x + b_2y + c_2z)^2)$ for some $\lambda_2 \in \text{GF}(q)^*$ and $a_2, b_2, c_2 \in \text{GF}(q)$. These two quadratic forms defining \mathcal{D} must be scalar multiples of each other, hence the two polynomials

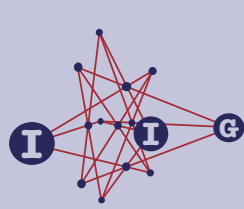
$$xy + z^2 + \lambda_1(a_1x + b_1y + c_1z)^2 \tag{1}$$

and

$$xy + kz^2 + \lambda_2(a_2x + b_2y + c_2z)^2 \tag{2}$$

ACADEMIA
PRESS





page 16 / 23

go back

full screen

close

quit

are proportional.

We first wish to show that c_1 , and thus c_2 must be zero. Proceeding by contradiction assume that $c_1 \neq 0$, allowing us to normalize $c_1 = 1$ by absorbing the value into λ_1 . If $c_1 = 1$, then we cannot have $a_1 = b_1 = 0$ since that would give (by Polynomial (1)) $\mathcal{D} = V(xy + (1 + \lambda_1)z^2)$, which forces \mathcal{D} to be in the pencil generated by \mathcal{C}_1 and \mathcal{C}_2 . Hence Polynomial (1) has at least one of the xz and yz cross-terms nonzero. This forces Polynomial (2) to have at least one of its xz and yz cross-terms nonzero, which implies $c_2 \neq 0$ and at least one of a_2 and b_2 is nonzero. As above, since $c_2 \neq 0$, we may assume without loss of generality that $c_2 = 1$.

Expanding Polynomials (1) and (2) and equating the coefficients with a constant of proportionality μ , we obtain the following six equations:

$$\lambda_1 a_1^2 = \mu(\lambda_2 a_2^2), \quad (3)$$

$$1 + 2\lambda_1 a_1 b_1 = \mu(1 + 2\lambda_2 a_2 b_2), \quad (4)$$

$$\lambda_1 b_1^2 = \mu(\lambda_2 b_2^2), \quad (5)$$

$$2\lambda_1 a_1 = \mu(2\lambda_2 a_2), \quad (6)$$

$$2\lambda_1 b_1 = \mu(2\lambda_2 b_2), \quad (7)$$

$$1 + \lambda_1 = \mu(k + \lambda_2). \quad (8)$$

Equations (6) and (7) let us solve for a_1 and b_1 in terms of a_2 and b_2 respectively, yielding $a_1 = \frac{\mu\lambda_2}{\lambda_1} a_2$ and $b_1 = \frac{\mu\lambda_2}{\lambda_1} b_2$. Plugging these into Equations (3) and (5) respectively, shows that $\frac{\mu\lambda_2}{\lambda_1} a_2^2 = a_2^2$ and $\frac{\mu\lambda_2}{\lambda_1} b_2^2 = b_2^2$. Since we cannot have both $a_2 = 0$ and $b_2 = 0$ we must have $\mu\lambda_2 = \lambda_1$. Utilizing this fact in Equations (6) and (7) shows that $a_1 = a_2$ and $b_1 = b_2$, and in Equation (8) shows that $\mu k = 1$. But plugging $\mu\lambda_2 = \lambda_1$, $a_1 = a_2$ and $b_1 = b_2$ into Equation (4) forces $\mu = 1$. Thus we must have $k = 1$ implying \mathcal{C}_1 and \mathcal{C}_2 are identical, which is our contradiction.

Hence $c_1 = 0$, from which it follows that c_2 must also be zero. We claim b_1 and b_2 are both nonzero. First note that if b_1 is zero then Polynomial (1) has no y^2 term, which forces b_2 to be zero as well, and vice versa, so either both b_1 and b_2 are zero, or neither are. In the former case, the coefficients of z^2 in the Polynomials (1) and (2) are 1 and k respectively, while the coefficients of xy are both 1; since the polynomials are proportional this forces $k = 1$, which yields the same contradiction as before. Thus b_1 and b_2 are both nonzero and we may normalize so that $b_1 = b_2 = 1$. We again expand our polynomials and equate coefficients with a constant of proportionality μ to obtain four equations (since

ACADEMIA
PRESS





page 17 / 23

go back

full screen

close

quit

the xz and yz cross-terms have coefficient zero):

$$\lambda_1 a_1^2 = \mu \lambda_2 a_2^2, \quad (9)$$

$$1 + 2\lambda_1 a_1 = \mu(1 + 2\lambda_2 a_2), \quad (10)$$

$$\lambda_1 = \mu \lambda_2, \quad (11)$$

$$1 = \mu k. \quad (12)$$

From Equation (12) we have $\mu = \frac{1}{k}$, which plugged into Equation (11) yields $\lambda_2 = k\lambda_1$. Combined with Equation (9) we obtain $a_1^2 = a_2^2$. If $a_1 = a_2$, then Equation (10) forces $\mu = 1$ and thus $k = 1$, which is again false. If $a_1 = -a_2$, Equation (10) yields $k(1 + 2\lambda_1 a_1) = 1 - 2k\lambda_1 a_1$, which we simplify to obtain $\lambda_1 a_1 = \frac{1-k}{4k}$.

At this point, we have shown that if there exists a conic mutually interior to \mathcal{C}_1 and \mathcal{C}_2 but not in the pencil they generate, it must be of the form $\mathcal{D} = V(xy + z^2 + \lambda(ax + y)^2)$, or alternatively $\mathcal{D} = V(xy + kz^2 + k\lambda(-ax + y)^2)$, where $\lambda a = \frac{1-k}{4k}$. We now need to determine which conics \mathcal{D} of this form are in fact mutually interior with both \mathcal{C}_1 and \mathcal{C}_2 , which involves showing that \mathcal{D} contains no exterior point of \mathcal{C}_1 or \mathcal{C}_2 , and vice versa. Suppose (y_0, y_1, y_2) is a point of $\mathcal{D} = V(xy + z^2 + \lambda(ax + y)^2)$. Appealing to Lemma 3.2 as before (y_0, y_1, y_2) is exterior to \mathcal{C}_1 if $-\frac{1}{4}\lambda(ay_0 + y_1)^2$ is a nonzero square, which occurs if and only if $-\lambda$ is a nonzero square. Hence \mathcal{D} contains no exterior point of \mathcal{C}_1 if and only if $-\lambda$ is a nonsquare. Repeating the calculation for the other three cases shows that

1. \mathcal{C}_1 contains no exterior point of \mathcal{D} if and only if $\frac{\lambda}{k}$ is a nonsquare.
2. \mathcal{D} contains no exterior point of \mathcal{C}_2 if and only if $k\lambda$ is a nonsquare.
3. \mathcal{C}_2 contains no exterior point of \mathcal{D} if and only if $k\lambda$ is a nonsquare.

When $q \equiv 1 \pmod{4}$ both -1 and k are nonzero squares, so these conditions are satisfied if and only if λ , and thus $-\lambda$, is a nonsquare. When $q \equiv 3 \pmod{4}$ both -1 and k are nonsquares, implying these conditions are met if and only if λ is a nonzero square, or equivalently $-\lambda$ is a nonsquare. This proves the result. \square

Theorem 5.4 limits the number and structure of conics mutually interior to both \mathcal{C}_1 and \mathcal{C}_2 , allowing us to press on to determine if there are any sets of four non-copencilar conics that are mutually interior. There are two possible configurations of such conics: $\mathcal{C}_1, \mathcal{C}_2$ and \mathcal{C}_3 mutually interior in a pencil, with \mathcal{C}_4 not in the pencil they generate, or no three of the conics in a common pencil. We first show that the former case can never happen.





page 18 / 23

go back

full screen

close

quit

Theorem 5.5. Suppose \mathcal{C}_1 , \mathcal{C}_2 and \mathcal{C}_3 are mutually interior secant copencilar conics in $\mathcal{PG}(2, q)$, q odd. Then any conic \mathcal{C}_4 mutually interior to \mathcal{C}_1 , \mathcal{C}_2 and \mathcal{C}_3 is in the pencil they generate.

Proof. First we note that by Corollary 4.3 no such configuration of three copencilar mutually interior conics exists when $q \equiv 3 \pmod{4}$, so we may assume $q \equiv 1 \pmod{4}$. Let \mathcal{C}_1 , \mathcal{C}_2 and \mathcal{C}_3 be as stated. By Proposition 5.2, the set of points interior to both \mathcal{C}_1 and \mathcal{C}_2 consists of $\frac{1}{2}(q-1)$ points on the line in the pencil, plus the points on $\frac{1}{4}(q-5)$ conics in the pencil, of which \mathcal{C}_3 is one.

\mathcal{C}_4 is mutually interior to both \mathcal{C}_1 and \mathcal{C}_2 , so other than its points of intersection with \mathcal{C}_1 and \mathcal{C}_2 , of which there are at most 4, the remaining at least $q-3$ points of \mathcal{C}_4 must be interior to \mathcal{C}_1 and \mathcal{C}_2 . Up to two of these can lie on the line of the pencil, but then at least $q-5$ points of \mathcal{C}_4 must lie in the union of the $\frac{1}{4}(q-5)$ conics above. One possibility is that \mathcal{C}_4 equals one of these conics, in which case it lies in the same pencil as \mathcal{C}_1 , \mathcal{C}_2 and \mathcal{C}_3 . If \mathcal{C}_4 is not a conic of the pencil, then \mathcal{C}_4 must meet each of the $\frac{1}{4}(q-5)$ conics in the pencil containing the points interior to both \mathcal{C}_1 and \mathcal{C}_2 in exactly four points, since distinct conics can meet in at most four points. But \mathcal{C}_3 is one of these conics meaning \mathcal{C}_4 meets \mathcal{C}_3 in exactly four points, contradicting the fact that mutually interior conics can meet in at most two points (Proposition 3.1). Thus \mathcal{C}_4 must be contained in the same pencil as the other three conics, as claimed. \square

We now address the final case, namely that we could have a set of mutually interior conics such that no three are copencilar. We do find that this happens, but only in one special case which shows immediately that no larger sets of mutually interior conics can occur.

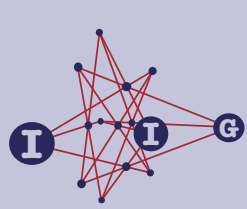
Theorem 5.6. Let \mathcal{C}_1 , \mathcal{C}_2 , \mathcal{C}_3 and \mathcal{C}_4 be distinct mutually interior secant conics in $\mathcal{PG}(2, q)$, q odd, such that no three are copencilar. Then $q \equiv 5 \pmod{8}$ and any such set of conics is isomorphic to

$$\begin{aligned}\mathcal{C}_1 &= V(xy + z^2), \\ \mathcal{C}_2 &= V(xy - z^2), \\ \mathcal{C}_3 &= V\left(xy + z^2 + \lambda \left(\frac{-1}{2\lambda}x + y\right)^2\right) \text{ and} \\ \mathcal{C}_4 &= V\left(xy + z^2 - \lambda \left(\frac{1}{2\lambda}x + y\right)^2\right),\end{aligned}$$

where λ is a nonsquare. Moreover for fixed \mathcal{C}_1 , \mathcal{C}_2 and \mathcal{C}_3 of this form, \mathcal{C}_4 is the unique conic that is mutually interior to all three.

Proof. By Theorem 4.1, we may assume without loss of generality that $\mathcal{C}_1 = V(xy + z^2)$ and $\mathcal{C}_2 = V(xy + kz^2)$ for some fixed $k \in \text{GF}(q)^*$ where k is a





page 19 / 23

go back

full screen

close

quit

nonzero square, $k - 1$ is a nonsquare when $q \equiv 1 \pmod{4}$, or k is a nonsquare with $k - 1$ a nonzero square when $q \equiv 3 \pmod{4}$. Then by Theorem 5.4

$$\mathcal{C}_3 = V\left(xy + z^2 + \lambda_3 \left(\frac{1-k}{4k\lambda_3}x + y\right)^2\right) \quad \text{and}$$

$$\mathcal{C}_4 = V\left(xy + z^2 + \lambda_4 \left(\frac{1-k}{4k\lambda_4}x + y\right)^2\right)$$

for some $\lambda_3, \lambda_4 \in \text{GF}(q)^*$ such that $-\lambda_3, -\lambda_4$ are nonsquares.

The conics \mathcal{C}_3 and \mathcal{C}_4 are also mutually interior, so Corollary 3.4 implies that \mathcal{C}_4 can also be written as

$$V\left(xy + z^2 + \lambda_3 \left(\frac{1-k}{4k\lambda_3}x + y\right)^2 + \chi(ax + by + cz)^2\right)$$

for some $\chi \in \text{GF}(q)^*$ and $a, b, c \in \text{GF}(q)$. Hence the polynomials

$$xy + z^2 + \lambda_4 \left(\frac{1-k}{4k\lambda_4}x + y\right)^2 \tag{13}$$

and

$$xy + z^2 + \lambda_3 \left(\frac{1-k}{4k\lambda_3}x + y\right)^2 + \chi(ax + by + cz)^2 \tag{14}$$

are proportional.

Note that Polynomial (13) has no xz and yz cross terms, so the proportionality shows that Polynomial (14) also has zero coefficients for its xz and yz cross-terms. Therefore either $c = 0$, or $a = b = 0$; we first show that c cannot be zero. Assume by way of contradiction that $c = 0$. Expanding Polynomials (13) and (14) and equating the coefficients with a constant of proportionality μ , we obtain the following four equations:

$$\frac{(1-k)^2}{16k^2\lambda_4} = \mu \left(\frac{(1-k)^2}{16k^2\lambda_3} + \chi a^2 \right), \tag{15}$$

$$\frac{1-k}{2k} + 1 = \mu \left(1 + \frac{1-k}{2k} + 2\chi ab \right), \tag{16}$$

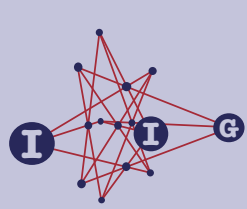
$$\lambda_4 = \mu(\lambda_3 + \chi b^2), \tag{17}$$

$$1 = \mu. \tag{18}$$

Equation (18), equating the z^2 coefficients, shows immediately that $\mu = 1$. Equation (17) then shows that $\lambda_4 = \lambda_3 + \chi b^2$; since λ_3 and λ_4 being equal would force $\mathcal{C}_3 = \mathcal{C}_4$, we must have $\chi b^2 \neq 0$ implying $b \neq 0$. On the other hand Equation (16) shows $2\chi ab = 0$, which forces $a = 0$. Finally we plug $a = 0$ and

ACADEMIA
PRESS





page 20 / 23

go back

full screen

close

quit

$\mu = 1$ into Equation (15), and use the fact that k cannot be 1 as that would force $\mathcal{C}_1 = \mathcal{C}_2$, yielding $\lambda_3 = \lambda_4$, again a contradiction. Hence c is nonzero, and $a = b = 0$.

Normalizing $c = 1$, we again expand Polynomials (13) and (14) and equate coefficients with a constant of proportionality μ to get the following equations:

$$\frac{(1-k)^2}{16k^2\lambda_4} = \mu \frac{(1-k)^2}{16k^2\lambda_3}, \quad (19)$$

$$\frac{1-k}{2k} + 1 = \mu \left(\frac{1-k}{2k} + 1 \right), \quad (20)$$

$$\lambda_4 = \mu\lambda_3, \quad (21)$$

$$1 = \mu(\chi + 1). \quad (22)$$

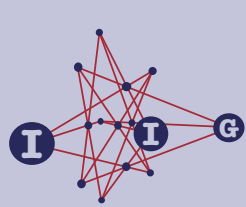
Examining Equation (20), we see immediately that either $\mu = 1$ or $\frac{1-k}{2k} + 1 = 0$. However $\mu = 1$ combined with Equation (21) would force $\lambda_3 = \lambda_4$, yet another contradiction, so we must have $\frac{1-k}{2k} + 1 = 0$ which forces $k = -1$. Equation (19) then yields $\lambda_3 = \mu\lambda_4$, which combined with Equation (21) shows that $\mu = -1$. Finally from Equation (22) we determine that $\chi = -2$.

First notice that λ_3 and λ_4 are opposites, which means that for $q \equiv 3 \pmod{4}$ λ_3 and λ_4 have opposite quadratic character, meaning not both $-\lambda_3$ and $-\lambda_4$ are nonsquares. Hence no such mutually interior conics \mathcal{C}_3 and \mathcal{C}_4 can exist when $q \equiv 3 \pmod{4}$. Assuming $q \equiv 1 \pmod{4}$, we must check the constraints on $k = -1$, namely that k is a nonzero square and $k - 1$ is a nonsquare. The former condition is clearly true, but the latter is only true when $k - 1 = -2$ is a nonsquare, or equivalently when 2 is a nonsquare, which occurs only for $q \equiv 5 \pmod{8}$.

Thus only in the case where $q \equiv 5 \pmod{8}$ is it possible that a set of four non-copencilar, mutually interior conics can exist, and if it exists the conics in the set must be isomorphic to $\mathcal{C}_1 = V(xy + z^2)$, $\mathcal{C}_2 = V(xy - z^2)$, $\mathcal{C}_3 = V(xy + z^2 + \lambda(\frac{-1}{2\lambda}x + y)^2)$ and $\mathcal{C}_4 = V(xy + z^2 - \lambda(\frac{1}{2\lambda}x + y)^2)$ for some nonsquare λ . However we need to check that these conics are actually mutually interior. We can use Theorems 4.1 and 5.4 to show all pairs are mutually interior, except \mathcal{C}_3 and \mathcal{C}_4 . Using Lemma 3.2 as in Theorem 5.4 quickly shows that \mathcal{C}_3 and \mathcal{C}_4 are mutually interior if $\frac{1}{2}$ is a nonsquare, which is true when $q \equiv 5 \pmod{8}$. Thus $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ and \mathcal{C}_4 are a set of non-copencilar mutually interior conics when $q \equiv 5 \pmod{8}$, and uniqueness of \mathcal{C}_4 given $\mathcal{C}_1, \mathcal{C}_2$ and \mathcal{C}_3 follows immediately from the form of \mathcal{C}_4 . \square

ACADEMIA
PRESS





page 21 / 23

go back

full screen

close

quit

6. Conclusion

We summarize the sets of mutually interior conics in $\mathcal{PG}(2, q)$ in Table 1.

While the semiovals discussed in this paper are interesting in their own right, we are very interested in finding examples of blocking semiovals, i.e., semiovals that are also blocking sets. While some of the sets we constructed here are blocking semiovals in small order planes, the only infinite family arises from the tangent pencils discovered by Szőnyi [8]. However we are hopeful of using our results here to find blocking semiovals that contain some of the sets constructed in this paper.

The authors would like to take this opportunity to thank the reviewers and editors for their many useful comments and constructive criticism.

ACADEMIA
PRESS



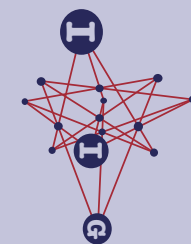
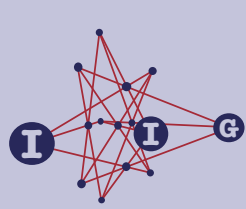


Table 1: Sets of mutually interior conics

canonical forms	restrictions	# of conics	pencil structure	intersections
$xy + z^2$	all q	1	n/a	n/a
$\{xy + a_i z^2\}$	$q \equiv 1 \pmod{4}$	$\leq \sqrt{q}$	copencilar	secant
	$q \equiv 3 \pmod{4}$	2	copencilar	secant
$\{x^2 - yz - a_i z^2\}$	$q \equiv 1 \pmod{4}$	$\leq \sqrt{q}$	copencilar	tangent
$\{x^2 - sy^2 + a_i z^2\}$ s nonsquare	$q \equiv 1 \pmod{4}$	$\leq \sqrt{q} - 1$	copencilar	disjoint
	$q \equiv 3 \pmod{4}$	2	copencilar	disjoint
$xy + z^2, xy + kz^2,$ $xy + z^2 + \lambda(\frac{1-k}{4k\lambda}x + y)^2$	q odd	3	non-copencilar	pairwise secant
$xy + z^2, xy - z^2,$ $xy + z^2 + \lambda(\frac{-1}{2\lambda}x + y)^2,$ $xy + z^2 - \lambda(\frac{1}{2\lambda}x + y)^2$	$q \equiv 5 \pmod{8}$	4	non-copencilar	pairwise secant



page 23 / 23

go back

full screen

close

quit

References

- [1] **V. Abatangelo, J.C. Fisher, G. Korchmaros and B. Larato**, On the mutual position of two irreducible conics in $\text{PG}(2, q)$, q odd, *Adv. Geom.* **11** (2011), 603–614.
- [2] **H.S.M. Coxeter**, “Projective geometry”, Blaisdell Publishing Co. Ginn and Co. New York-London-Toronto, 1964.
- [3] **L.E. Dickson**, On families of quadratic forms in a general field, *Quarterly J. Pure Appl. Math.* **39** (1908), 316–333.
- [4] **J. W. P. Hirschfeld**, “Projective geometries over finite fields”, Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, second edition, 1998.
- [5] **G. Kiss**, A survey on semiovals, *Contrib. Discrete Math.* **3** (2008), 81–95.
- [6] **G. Kiss, S. Marcugini and F. Pambianco**, On the spectrum of the sizes of semiovals in $\text{PG}(2, q)$, q odd, *Discrete Math.* **310** (2010), 3188–3193.
- [7] **B. Segre**, Proprietà elementari relative ai segmenti ed alle coniche sopra un campo qualsiasi ed una congettura di Seppo Ilkka per il caso dei campi di Galois, *Ann. Mat. Pura Appl. (4)* **96** (1972), 289–337.
- [8] **T. Szőnyi**, Note on the existence of large minimal blocking sets in Galois planes, *Combinatorica* **12** (1992), 227–235.

Jeremy M. Dover

DOVER NETWORKS LLC, 445 POPLAR LEAF DR., EDGEWATER, MD 21037

e-mail: jeremy@dovernetworks.com

Keith E. Mellinger

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MARY WASHINGTON, 1301 COLLEGE AVENUE, FREDERICKSBURG, VA 22401-5300

e-mail: kmelling@umw.edu

ACADEMIA
PRESS

