Arcs, Ovals, and Segre's Theorem

Brian Kronenthal
Most recently updated on:

October 6, 2012

1 Preliminary Definitions and Results

Let π be a projective plane of order q.

Definition 1.1. *A* <u>*k-arc*</u> *is a set of k points in π, no three collinear.*

Proposition 1.2. *Let K be a k-arc. Then $k \leq q+2$. Furthermore, if q is odd, then $k \leq q+1$.*

Proof. Let K be a k-arc, $x \in K$. Since π has $q+1$ lines through any point, there are exactly $q+1$ lines containing x. Furthermore, since π has a unique line through any pair of points (x, y) with $y \in K \setminus \{x\}$, each of the $k-1$ pairs corresponds to a unique line of the plane (if two pairs corresponded to the same line, we would have 3 collinear points in K, a contradiction). Since the number of such lines cannot excceed the total number of lines in π that contain x, we conclude $k-1 \leq q+1$; thus, $k \leq q+2$.

We will now prove the contrapositive of the second statement. To that end, suppose $k = q+2$. Then equality holds in the above argument, and so every line L of π with $x \in L$ must also contain some $y \in K \setminus \{x\}$. Therefore, every line of π must contain either 0 or 2 points of K.

Now, choose a fixed point $z \notin K$. Since every pair in the set $S = \{(x, z) | x \in K\}$ determines a line, $|S| = q+2$. As every line contains 0 or 2 points of K, every line intersecting K is represented by exactly two pairs of the form (x, z), $x \in K$. Thus, there are $\frac{q+2}{2}$ lines through z that intersect K. This implies $2|(q-2)$, and so q is even. $\square$

Definition 1.3. *A $(q+1)$-arc is called an* <u>*oval*</u>*, while a $(q+2)$-arc (which can only exist in a plane of even order) is called a* <u>*hyperoval*</u>*.*

We now explore some properties of ovals and hyperovals.

Proposition 1.4. *Let $\mathcal{O}$ be an oval. Then there is a unique tangent line to $\mathcal{O}$ for every $x \in \mathcal{O}$.*

Proof. Let $x \in \mathcal{O}$. Then for every $y \in \mathcal{O} \setminus \{x\}$, there is a unique line containing x, y, and no other element of $\mathcal{O}$ (if the line contained a third point of $\mathcal{O}$, this would produce the contradiction of 3 collinear points in $\mathcal{O}$). But $|\mathcal{O} \setminus \{x\}| = q$ implies that there are q secant lines through x. Since π has $q+1$ lines through every point, there is exactly one line through x that remains unaccounted for. As this line is not a secant line, it must be a tangent line. $\square$

Definition 1.5. *A* <u>*conic*</u> *$\mathcal{C}$ in the projective plane $PG(2, q)$ is the set of projective points*

$$\{(x, y, z) | Q(x, y, z) = 0\}, \tag{1}$$

where $Q = Q(X, Y, Z) = aX^2 + bY^2 + cZ^2 + 2fYZ + 2gZX + 2hXY$ for some fixed $a, b, c, f, g, h \in \mathbb{F}_q$. Furthermore, we classify certain conics as follows.

1. *A conic in a projective plane of odd order is* <u>*degenerate*</u> *if the matrix* $M_Q = \begin{pmatrix} a & h & g \\ h & b & f \\ g & f & c \end{pmatrix}$ *has determinant 0.*

2. *[2] A conic is* <u>*singular*</u> *if there exists point* $T \in \mathcal{C}$ *such that* $\frac{\partial Q}{\partial X}\Big|_T = \frac{\partial Q}{\partial Y}\Big|_T = \frac{\partial Q}{\partial Z}\Big|_T = 0$.

3. *[2] A conic is* <u>*reducible*</u> *if* $Q(x, y, z)$ *can be factored into the product of two linear terms. This is equivalent to saying that* $\mathcal{C}$ *contains an entire line of* $PG(2, q)$.

4. *[1] A conic is* <u>*substitution-reducible*</u> *if there is a linear transformation*[1] *of the variables* $X, Y,$ *and* Z *with non-singular matrix representation that reduces the number of variables in* Q *from three.*

Note that if a conic does not meet these criteria, it is called non-degenerate, non-singular, irreducible, or substitution-irreducible, respectively. Furthermore, the matrix M_Q is significant because

$$(X, Y, Z)M_Q \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = (X, Y, Z) \begin{pmatrix} a & h & g \\ h & b & f \\ g & f & c \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = Q.$$

Proposition 1.6. *Let* $\mathcal{C}$ *be a conic in* $PG(2, q)$ *with* q *odd. Then the following are equivalent:*

1. $\mathcal{C}$ *is degenerate*

2. $\mathcal{C}$ *is singular*

3. $\mathcal{C}$ *is reducible*

4. $\mathcal{C}$ *is substitution-reducible*

Theorem 1.7. *Every non-degenerate conic is a* k*-arc.*

Proof. (adapted from [1]) Let $\mathcal{C}$ be a conic and L a line of $PG(2, q)$. We must show that $|\mathcal{C} \cap L| \leq 2$.

We know[2] that any two points in $PG(2, q)$ may be mapped to any two points via a linear transformation with non-singular matrix representation. Since two points determine a unique line, there is a linear transformation that maps L to the line $z = 0$. Therefore, we may assume without loss of generality that L is $z = 0$.

Now, suppose to the contrary that $a = b = h = 0$. Then $\mathcal{C} = \{(x, y, z)|(2gx + 2fy + cz)z = 0\}$, where at least one of $c, f,$ and g is non-zero; suppose without loss of generality that $g \neq 0$. Consider the linear transformation φ defined by $\varphi(x) = 2gx + 2fy + cz$, $\varphi(y) = y$, and $\varphi(z) = z$. This transformation has matrix $\begin{pmatrix} 2g & 2f & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, which has determinant $2g \neq 0$. Therefore, this transformation is invertible. Furthermore,

$$\varphi^{-1}(\mathcal{C}) = \{(x, y, z)|xz = 0\},$$

which contains only two variables. As φ^{-1} is a linear transformation with non-singular matrix representation, this contradicts the assumption that $\mathcal{C}$ is non-degenerate, and thus substitution-irreducible by Proposition 1.6. Thus, we conclude that at least one of $a, b,$ and h is non-zero.

[1] More specifically, this transformation is between degree one polynomials of $x, y,$ and z.

[2] This is because the action of $PGL(V)$ on $P(V)$ (i.e. the points of the projective plane corresponding to an n-dimensional vector space V) is 2-transitive. To see this, let $\langle u_1 \rangle \neq \langle u_2 \rangle$ and $\langle v_1 \rangle \neq \langle v_2 \rangle$ be elements of $P(V)$. Since u_1 and u_2 are linearly independent, we may extend u_1, u_2 to a basis $\{u_1, u_2, u_3, ..., u_n\}$ of V. Similarly, the linear independence of v_1 and v_2 implies we may extend v_1, v_2 to a basis $\{v_1, v_2, v_3, ..., v_n\}$ of V. Since there is always a linear transformation $f \in GL(V)$ that maps one basis to another, $f(u_i) = v_i$ for all i; thus, $f(\langle u_1 \rangle) = \langle v_1 \rangle$ and $f(\langle u_2 \rangle) = \langle v_2 \rangle$, as desired, where $f \in PGL(V)$.

Assume first that $a \neq 0$. All points on the line $z = 0$ have form $(1, 0, 0)$ or $(x, 1, 0)$ for some x. Note that $(1, 0, 0) \notin \mathcal{C}$ because $a \neq 0$. Furthermore, $(x, 1, 0) \in \mathcal{C}$ if and only if $ax^2 + 2hx + b = 0$; since this is a quadratic equation in x, it has at most 2 solutions. Therefore, $|\mathcal{C} \cap L| \leq 2$.

Next, assume $b \neq 0$. Note that all points on the line $z = 0$ have form $(0, 1, 0)$ or $(1, y, 0)$ for some y, and that $(0, 1, 0) \notin \mathcal{C}$ because $b \neq 0$. Furthermore, $(1, y, 0) \in \mathcal{C}$ if and only if $by^2 + 2hy + a = 0$; since this is a quadratic equation in y, it has at most 2 solutions. Therefore, $|\mathcal{C} \cap L| \leq 2$.

Finally, if we assume $a = b = 0$ and $h \neq 0$, then any $(x, y, z) \in \mathcal{C} \cap L$ satisfies $2hxy = 0$. Since $h \neq 0$, we know $x = 0$ or $y = 0$. As we are only considering points on the line $z = 0$, the only solutions are $(1, 0, 0)$ and $(0, 1, 0)$. Therefore, $|\mathcal{C} \cap L| = 2$.

Thus, for every line L of $PG(2, q)$, $|\mathcal{C} \cap L| \leq 2$. Therefore, no three points of $\mathcal{C}$ are collinear, and so $\mathcal{C}$ is a k-arc. □

In general, it can be inconvenient to prove a result for all non-degenerate conics in $PG(2, q)$. The next result is a powerful tool that allows one to consider a particular conic instead.

Proposition 1.8. *Let q be odd. Every non-degenerate conic in $PG(2, q)$, is equivalent to the conic $XY - Z^2 = 0$.*

Proof. (adapted primarily from [7]) Let $\mathcal{C}$ be the conic as defined by (1). Let P be a point of $\mathcal{C}$. Assume without loss of generality (via a non-singular linear transformation, if necessary) that $P = (1, 0, 0)$. Since $P \in \mathcal{C}$ implies $Q(1, 0, 0) = 0$, we know $a = 0$. Therefore,

$$Q = bY^2 + cZ^2 + 2fYZ + 2gXZ + 2hXY.$$

Now, note that any line through P has equation $\beta Y + \gamma Z = 0$, where $\beta, \gamma \in \mathbb{F}_q$ are not both 0. Let L be one such line, and let T be a point on L. Then[3] $T = (t, \gamma, -\beta)$ for some $t \in \mathbb{F}_q$. Now, we know $T \in \mathcal{C}$ if and only if:

$$Q(t, \gamma, -\beta) = b\gamma^2 + c\beta^2 - 2f\gamma\beta - 2gt\beta + 2ht\gamma = 0,$$

or equivalently

$$b\gamma^2 + c\beta^2 - 2f\beta\gamma + 2(h\gamma - g\beta)t = 0. \tag{2}$$

We now consider two cases:

1. Assume there is no $\lambda \in \mathbb{F}_q$ such that $\beta = \lambda h$ and $\gamma = \lambda g$. Then[4] $h\gamma - g\beta \neq 0$; so (2) produces a unique solution for t. Therefore, every line $L : \beta y + \gamma z$ through P in this case contains a unique additional point on $\mathcal{C}$.

2. Assume that there exists $\lambda \in \mathbb{F}_q$ such that $\beta = \lambda h$ and $\gamma = \lambda g$. Then $h\gamma - g\beta = 0$, and so $T \in \mathcal{C}$ if and only if
$$Q(t, \gamma, -\beta) = Q(t, \lambda g, -\lambda h) = 0 \Longrightarrow bg^2 - 2fgh + ch^2 = 0. \tag{3}$$
But recall that every point $T \in L$ (besides P) has form $(t, \gamma, -\beta)$, and is therefore on $\mathcal{C}$ by (3). This implies that $\mathcal{C}$ contains the entire line L, and so $\mathcal{C}$ is reducible; this contradicts the non-degeneracy of $\mathcal{C}$. Thus, P is the only point of $\mathcal{C}$ on L in this case.

Therefore, we conclude that the $q + 1$ lines through P may be described as follows:

1. The line $hy + gz = 0$ (from the case 2 equalities $\beta = \lambda h$ and $\gamma = \lambda g$) contains only one point of $\mathcal{C}$ and is thus a tangent line.

[3] This is because we may assume without loss of generality that the y-coordinate of T is 1. Then T must satisfy $\beta + \gamma z = 0$, or equivalently $z = -\beta\gamma^{-1}$. So $T = (t', 1, -\beta\gamma^{-1}) = (t, \gamma, -\beta)$ for arbitrary $t' \in \mathbb{F}_q$ and $t = t'\gamma$.

[4] If $h\gamma - g\beta = 0$, then $h\gamma = g\beta$. If $g \neq 0$, then $\beta = (\gamma g^{-1})h$ and $\gamma = (\gamma g^{-1})g$. If instead $g = 0$, then either $h = 0$ (which implies the contradiction $\beta = \gamma = 0$) or $\gamma = 0$, in which case $\beta = \lambda h$ and $\gamma = 0 = \lambda g$ for some λ. Our statement follows by contrapositive, where $\lambda = \gamma g^{-1}$ in the $g \neq 0$ case.

2. The other q lines through P (from case 1) are secant lines to $\mathcal{C}$.

Since $q \geq 2$, there are at least 3 lines through P. This means that there exist noncollinear points $P, Q, R \in \mathcal{C}$. Define L to be the tangent line to $\mathcal{C}$ at P, L' to be the tangent line to $\mathcal{C}$ at Q, and $S = L \cap L'$; see Figure 1. Now, since P, Q, R, S are in general position (i.e. no three of these points are collinear), we may assume

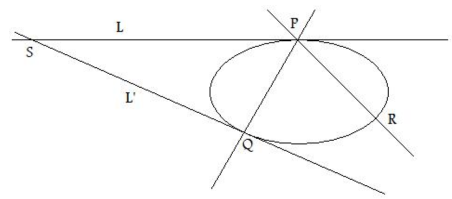

Figure 1: S is the intersection of the tangent lines to $\mathcal{C}$ at P and Q.

without loss of generality (via a linear transformation[5]) that $P = (1,0,0), Q = (0,1,0), S = (0,0,1)$, and $R = (1,1,1)$. Define $\widetilde{b}, \widetilde{c}, \widetilde{d}, \widetilde{e}$, and $\widetilde{f}$ to be the respective images of b, c, d, e, and f under this transformation.

Now, we have $\widetilde{Q} = \widetilde{b}Y^2 + \widetilde{c}Z^2 + 2\widetilde{f}YZ + 2\widetilde{g}XZ + 2\widetilde{h}XY$. Since $Q = (0,1,0) \in \mathcal{C}$, we know $\widetilde{b} = 0$, and so

$$\widetilde{Q} = \widetilde{c}Z^2 + 2\widetilde{f}YZ + 2\widetilde{g}XZ + 2\widetilde{h}XY.$$

Let T denote an arbitrary point of $\mathcal{C}$. Then by page 139 of [2], the tangent line to $\mathcal{C}$ at T has equation

$$\left.\frac{\partial \widetilde{Q}}{\partial X}\right|_T X + \left.\frac{\partial \widetilde{Q}}{\partial Y}\right|_T Y + \left.\frac{\partial \widetilde{Q}}{\partial Z}\right|_T Z = 0,$$

which for $T = (x_0, y_0, z_0)$ and $\widetilde{Q} = \widetilde{c}Z^2 + 2\widetilde{f}YZ + 2\widetilde{g}XZ + 2\widetilde{h}XY$ is

$$(2\widetilde{h}y_0 + 2\widetilde{g}z_0)X + (2\widetilde{h}x_0 + 2\widetilde{f}z_0)Y + (2\widetilde{g}x_0 + 2\widetilde{f}y_0 + 2\widetilde{c}z_0)Z = 0.$$

Therefore, L (the tangent line to $\mathcal{C}$ at $P = (1,0,0)$) has equation

$$L : \widetilde{h}Y + \widetilde{g}Z = 0$$

and L' (the tangent line to $\mathcal{C}$ at $Q = (0,1,0)$) has equation

$$L' : \widetilde{h}X + \widetilde{f}Z = 0.$$

Since $S = (0,0,1) = L \cap L'$, we know $\widetilde{f} = 0$ and $\widetilde{g} = 0$. This implies $\widetilde{Q} = \widetilde{c}Z^2 + 2\widetilde{h}XY$. Since $R = (1,1,1) \in \mathcal{C}$, we know $\widetilde{c} + 2\widetilde{h} = 0$, and so $\widetilde{c} = -2\widetilde{h} \neq 0$ ($\widetilde{c} = \widetilde{h} = 0$ would produce the contradiction $\widetilde{Q} = 0$). Therefore, $\mathcal{C}$ consists of all solutions to

$$-2\widetilde{h}Z^2 + 2\widetilde{h}XY = 0,$$

or equivalently to the desired equation

$$XY - Z^2 = 0$$

because $\widetilde{h} \neq 0$. $\square$

[5]Let A, B, C be three noncollinear points, and let $D = aA + bB + cC$ for some scalars a, b, c. Define $f \in GL(2, q)$ such that $f(A) = a^{-1}(1,0,0), f(B) = b^{-1}(0,1,0)$, and $f(C) = c^{-1}(0,0,1)$. Then

$$f(D) = f(aA + bB + cC) = af(A) + bf(B) + cf(C) = (1,0,0) + (0,1,0) + (0,0,1) = (1,1,1).$$

Corollary 1.9. *Let q be odd. Every non-degenerate conic in $PG(2,q)$ contains exactly $q+1$ points.*

Proof. By Proposition 1.8, we need only consider the conic $xy - z^2 = 0$. If $z \neq 0$, then there are $q-1$ choices for z. Since $xy = z^2$, $z \neq 0$ implies $x \neq 0$ and $y \neq 0$. So there are $q-1$ choices for x, and choosing x and z uniquely determines y. Thus, this case produces $(q-1)^2$ points (x, y, z).

Alternatively, if $z = 0$, then $x = 0$ or $y = 0$. If $x = 0$, then y is unrestricted and there are thus q choices. Similarly, there are q choices for x if $y = 0$. This case therefore produces $2q-1$ points, where we subtract one because we have counted the point $(0,0,0)$ twice.

Therefore, we have a total of $(q-1)^2 + 2q - 1 = q^2$ triples. But since we are in projective space, $(0,0,0)$ is not an option and we must divide by $q-1$ to account for the fact that (x,y,z) and $\lambda(x,y,z)$ are equivalent points for all $\lambda \in \mathbb{F}_q^*$. This yields a total of $\frac{q^2-1}{q-1} = q+1$ points on a non-degenerate conic. □

Now, we will consider an example that illustrates the power of Proposition 1.8.

Example 1.10. *These results yield a simple way to count the number of solutions $(x,y,z) \in PG(2,q)$ to the equation $x^2+y^2=z^2$. Since $x^2+y^2=z^2$ is a non-degenerate conic (note that if $Q = X^2+Y^2-Z^2$, then* $\det(M_Q) = -1 \neq 0$*), it is equivalent to $xy = z^2$ by Proposition 1.8. By Corollary 1.9, there are precisely $q+1$ solutions.*

Corollary 1.11. *Every non-degenerate conic in $PG(2,q)$ (q odd) is an oval.*

Proof. Let $\mathcal{C}$ be a non-degenerate conic. Then $\mathcal{C}$ is a k-arc by Theorem 1.7 and has $q+1$ points by Corollary 1.9. Therefore, $\mathcal{C}$ is an oval. □

We now shift our attention to properties of hyperovals. Recall that an arc in a projective plane of order q can only have size $q+2$ for q even; the remainder of this section will therefore focus exclusively on such planes.

Proposition 1.12. *Let $\mathcal{H}$ be a hyperoval in a projective plane π of order q even. Choose arbitrary $u \in \mathcal{H}$, and define the oval $\mathcal{O} = \mathcal{H} \setminus \{u\}$. Label the points of $\mathcal{H}$ by $\{x_1, x_2, ..., x_{q+1}, u\}$, and let L_i denote the unique tangent line to $\mathcal{O}$ through x_i. Then the lines $L_1, L_2, ..., L_{q+1}$ meet at the point u.*

Proof. Consider $x_1 \in \mathcal{O}$. Then we classify all lines containing x_1:

1. There is a unique line through x_1 and y for every $y \in \mathcal{O}$; this accounts for q lines secant to $\mathcal{O}$. Note that none of these lines contain u, as otherwise three points of $\mathcal{O}$ would be collinear.

2. There is a unique line L_1 through x_1 and u. This accounts for one line tangent to $\mathcal{O}$.

We have thereby accounted for all lines of π containing x_1. Note that the unique tangent line to $\mathcal{O}$ containing x_1 (i.e. L_1) contains u. Repeat this process for every x_i, $2 \leq i \leq n+1$. This shows every L_i contains u, as claimed. □

Definition 1.13. *Let π be a projective plane of order q even. The <u>nucleus</u> of an oval $\mathcal{O}$ in π is the intersection of the $q+1$ tangent lines to $\mathcal{O}$ (labeled u in the previous proposition).*

Definition 1.14. *A hyperoval is called <u>regular</u> if its points consist of the $q+1$ points of an oval $\mathcal{O}$ and the nucleus of $\mathcal{O}$. Otherwise, a hyperoval is called <u>irregular</u>.*

Example 1.15. *Consider the Fano Plane (i.e. $PG(2,2)$) as pictured in Figure 2. Then $\{A, C, E\}$ forms an oval with nucleus G. Therefore, $\{A, C, E, G\}$ is a regular hyperoval.*

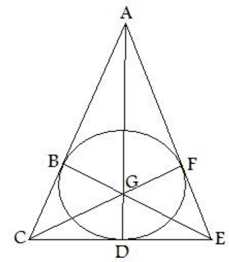

Figure 2: The Fano Plane

Example 1.16. *All hyperovals in $PG(2,2), PG(2,4)$, and $PG(2,8)$ are regular. However, irregular hyperovals exist in $PG(2,2^e)$ for all $e \geq 4$; for justification of these facts, see Lemma 8.21, Corollary 8.32, and Theorem 8.37 of [4]. For example, Lunelli and Sce proved [6] that if $\eta \in \mathbb{F}_{16}$ such that $\eta^4 = \eta + 1$, then*

$$\{(1, t, \eta^{12}t^2 + \eta^{10}t^4 + \eta^3 t^8 + \eta^{12}t^{10} + \eta^9 t^{12} + \eta^4 t^{14} | t \in \mathbb{F}_{16} \cup \{(0,1,0),(0,0,1)\}\}$$

is an irregular hyperoval in $PG(2,16)$. Furthermore, Hall proved [3] (using a computer), and later O'Keefe and Penttila proved [8] (without a computer), that every irregular hyperoval of $PG(2,16)$ is equivalent to the Lunelli-Sce hyperoval. For additional results about hyperovals, see e.g. [4] or Penttila [9].

Since every conic is an oval (Corollary 1.11), we could define the nucleus of a conic using the corresponding definition for the nucleus of an oval (Definition 1.13). However, the coordinates of the nucleus of a conic in a projective plane of even order may be determined precisely.

Proposition 1.17. *Suppose $\mathcal{C}$ is a conic in $PG(2,q)$, $q = 2^e$ for some $e \in \mathbb{N}$, defined by*

$$Q = aX^2 + bY^2 + cZ^2 + fYZ + gXZ + hXY = 0.$$

Then the nucleus of $\mathcal{C}$ is (f,g,h).

Proof. (Uses [2], in part)

Calculating partial derivatives of Q, and remembering that we are in characteristic 2, we have:

$$\begin{aligned}\frac{\partial Q}{\partial X} &= gZ + hY,\\ \frac{\partial Q}{\partial Y} &= fZ + hX, \text{ and}\\ \frac{\partial Q}{\partial Z} &= fY + gX.\end{aligned}$$

Then the tangent line to this conic at the point $T = (x_0, y_0, z_0)$ is:

$$\begin{aligned}0 &= \left.\frac{\partial Q}{\partial X}\right|_T X + \left.\frac{\partial Q}{\partial Y}\right|_T Y + \left.\frac{\partial Q}{\partial Z}\right|_T Z\\ 0 &= (gz_0 + hy_0)X + (fz_0 + hx_0)Y + (fy_0 + gx_0)Z, \qquad (4)\end{aligned}$$

To show that (f,g,h) lies on every tangent line, we need only show that (f,g,h) is a solution to (4) for any (x_0, y_0, z_0). This follows immediately, as

$$(gz_0 + hy_0)f + (fz_0 + hx_0)g + (fy_0 + gx_0)h = 2fgz_0 + 2fhy_0 + 2ghx_0 = 0.$$

Therefore, (f,g,h) is the nucleus of $\mathcal{C}$ (note that we can say "the" nucleus because in a projective plane, two lines intersect in a unique point; so if all tangent lines intersect at (f,g,h), this is the only place they can intersect). $\square$

2 Segre's Theorem

The purpose of this section is to prove Segre's Theorem, which is Theorem 2.4 below. We start with some preliminary results. Let $\mathcal{O}$ be an oval in $PG(2,q)$, q an odd prime power. We will need a lemma to prove Proposition 2.3.

Lemma 2.1. *If q is an odd prime power, then*

$$\prod_{a\in\mathbb{F}_q^*} a = -1$$

We will present two proofs of this result.

Proof 1. Let $a \in \mathbb{F}_q^*$. Then

$$a = a^{-1} \Leftrightarrow a^2 = 1 \Leftrightarrow a = \pm 1.$$

Therefore,

$$\prod_{a\in\mathbb{F}_q^*} a = \left(a_1 a_1^{-1}\right)\left(a_2 a_2^{-1}\right)...\left(a_{\frac{q-3}{2}} a_{\frac{q-3}{2}}^{-1}\right)(1)(-1) = (1)(1)...(1)(1)(-1) = -1$$

□

Proof 2. We know that $a \in \mathbb{F}_q^*$ if and only if a is a root of $x^{q-1}-1$. Therefore,

$$x^{q-1}-1 = \prod_{a\in\mathbb{F}_q^*}(x-a) = x^{q-1} - \left(\sum a\right)s^{q-2} + \left(\sum a_i a_j\right)x^{q-3} - ... - \left(\sum a_{i_1}...a_{i_{q-2}}\right)x + a_1...a_{q-1},$$

with the second equality holding by Viete's Theorem. Comparing corresponding terms, we find that $a_1...a_{q-1} = -1$. □

Definition 2.2. *A triangle with its vertices on $\mathcal{O}$ is called an* <u>*inscribed triangle of $\mathcal{O}$*</u>*. A triangle whose sides are tangent to $\mathcal{O}$ is called a* <u>*circumscribed triangle of $\mathcal{O}$*</u>*. If the sides of a circumscribed triangle are tangent to $\mathcal{O}$ at the vertices of an inscribed triangle, these two triangles may be called* <u>*mates*</u>*.*

Proposition 2.3. *[5] Every inscribed triangle of $\mathcal{O}$ and its mate are in perspective.*

Proof. Without loss of generality, suppose that the inscribed triangle is the triangle of reference (i.e. has vertices $A_1 = (1,0,0), A_2 = (0,1,0)$, and $A_3 = (0,0,1)$). For $i = 1,2,3$, define a_i to be the tangent line to $\mathcal{O}$ at A_i. Then a_1 has equation $y = k_1 z$, a_2 has equation $z = k_2 x$, and a_3 has equation $x = k_3 y$ for some $k_1, k_2, k_3 \in \mathbb{F}^*$. See Figure 3.

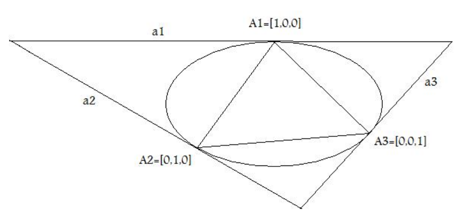

Figure 3: The triangle of reference and its mate.

Choose arbitrary $B = (c_1, c_2, c_3) \in \mathcal{O} \setminus \{A_1, A_2, A_3\}$. If we assume to the contrary that $c_1 = 0$, then the line containing B and A_3 is $x = 0$. However, this would imply that B, A_2, and A_3 are all on the line $x = 0$, violating the requirement that no three points on an oval are collinear. Therefore, we conclude $c_1 \neq 0$. By similar reasoning, $c_2 \neq 0$ and $c_3 \neq 0$. Now, note that:

1. The line containing A_1 and B has equation $y = h_1 z$, where $h_1 = c_2 c_3^{-1}$.
2. The line containing A_2 and B has equation $z = h_2 x$, where $h_1 = c_3 c_1^{-1}$.
3. The line containing A_3 and B has equation $x = h_3 y$, where $h_3 = c_1 c_2^{-1}$.

In addition, note that $h_1 h_2 h_3 = c_2 c_3^{-1} c_3 c_1^{-1} c_1 c_2^{-1} = 1$. Therefore, using $\overline{XY}$ to denote the line containing the points X and Y, we have the following result:

Conclusion: Let $A_1 A_2 A_3$ be the triangle of reference and $B \in \mathcal{O} \setminus \{A_1, A_2, A_3\}$. Then if the lines $\overline{A_1 B}, \overline{A_2 B}$, and $\overline{A_3 B}$ have equations $y = h_1 z$, $z = h_2 x$, and $x = h_3 y$ respectively, then $h_1 h_2 h_3 = 1$.

Claim: $k_1 k_2 k_3 = -1$, where we recall that $y = k_1 z$, $z = k_2 x$, and $x = k_3 y$ are the tangent lines to $\mathcal{O}$ at A_1, A_2, and A_3 respectively.

Proof: (adapted from Step 4 on page 140 of [1]) Label the $q+1$ points of $\mathcal{O}$ by $A_1, A_2, A_3, p_4, p_5, ..., p_{q+1}$. Note that $L := \overline{A_2 A_3}$ must be the line $x = 0$. Consider the point $A_1 = (1, 0, 0)$. It lies on:

1. The tangent at A_1, which has equation $y = k_1 z$ and intersects L at $(0, k_1, 1)$.
2. The secant containing A_1 and A_2.
3. The secant containing A_1 and A_3.
4. The secants containing A_1 and p_i, $4 \leq i \leq q+1$, which intersect L at $(0, k_i, 1)$ with $k_i \in \mathbb{F}_q^*$.

Note that since no two of these lines will intersect L at the same place (otherwise, the lines would be the same, forcing 3 collinear points of $\mathcal{O}$), the k_i ($i = 1$ or $4 \leq i \leq q+1$) are distinct. Therefore,

$$k_1 \prod_{i=4}^{q+1} k_i = \prod_{x \in \mathbb{F}_q^*} x = -1,$$

with the last equality following from Lemma 2.1.

Now, we switch our perspective from lines containing A_1 to lines containing A_2. Let L' denote the line containing A_1 and A_3, and proceed as above. We find

$$k_2 \prod_{i=4}^{q+1} k_i' = \prod_{x \in \mathbb{F}_q^*} x = -1.$$

Finally, we use a similar approach on lines containing A_3. Letting L'' be the line containing A_1 and A_2, we have

$$k_3 \prod_{i=4}^{q+1} k_i'' = \prod_{x \in \mathbb{F}_q^*} x = -1.$$

Multiplying these three results together yields:

$$
\begin{aligned}
-1 &= (-1)^3 = \left(k_1 \prod_{i=4}^{q+1} k_i\right)\left(k_2 \prod_{i=4}^{q+1} k_i'\right)\left(k_3 \prod_{i=4}^{q+1} k_i''\right) \\
&= k_1k_2k_3 \prod_{i=4}^{q+1} k_ik_i'k_i'' \\
&= k_1k_2k_3 \prod_{i=4}^{q+1} 1 \\
&\quad \text{(This is because the lines } y = k_iz,\ z = k_i'x, \text{ and } x = k_i''y \text{ all intersect } \mathcal{O} \text{ at } p_i. \\
&\quad \text{Therefore, } k_ik_i'k_i'' = 1 \text{ by above conclusion.)} \\
&= k_1k_2k_3
\end{aligned}
$$

Thus, $k_1k_2k_3 = -1$, as claimed.

$\diamond$

Now, let $a \cap b$ denote the intersection of the lines a and b. Then define the points $A_1' := a_2 \cap a_3 = (k_3, 1, k_2k_3)$, $A_2' := a_1 \cap a_3 = (k_1k_3, k_1, 1)$, and $A_3 := a_1 \cap a_2 = (1, k_1k_2, k_2)$. Futhermore, we note that $\overline{A_1A_1'}$ has equation $z = k_2k_3y$, $\overline{A_2A_2'}$ has equation $x = k_1k_3z$, and $\overline{A_3A_3'}$ has equation $y = k_1k_2x$. Each of these three lines contains the point $K = (1, k_1k_2, -k_2)$. Therefore, the triangles $A_1A_2A_3$ and $A_1'A_2'A_3'$ are in perspective with respect to the point K, as in Figure 4. $\square$

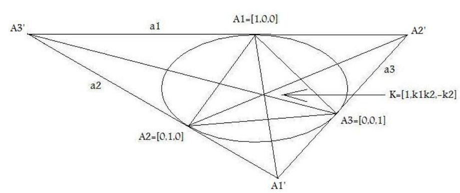

Figure 4: Triangles in perspective

Theorem 2.4 (Segre's Theorem). *Let q be an odd prime power. Then every oval in $PG(2, q)$ is a conic.*

Proof. (adapted primarily from [5]) Let $\mathcal{O}$ be an oval in $PG(2, q)$, where q is an odd prime power. Recall from the proof of Proposition 2.3 that $K = (1, k_1k_2, -k_2)$ is the point of concurrency for the lines $\overline{A_1A_1'}$, $\overline{A_2A_2'}$, and $\overline{A_3A_3'}$. Assume without loss of generality that $k_1 = k_2 = k_3 = -1$, and so $K = (1, 1, 1)$.

Choose $B = (c_1, c_2, c_3) \in \mathcal{O} \setminus \{A_1, A_2, A_3\}$, and let b denote the tangent line $b_1x + b_2y + b_3z = 0$ to $\mathcal{O}$ at B. Since B is on b, we know that

$$b_1c_1 + b_2c_2 + b_3c_3 = 0. \tag{5}$$

By Proposition 2.3, the triangle BA_2A_3 and the triangle with sides b, a_2, and a_3 are in perspective.

Let point P denote the intersection of the lines $x = 0$ and b; it is therefore the unique point determined by the equation $b_2y + b_3z = 0$, namely $P = (0, b_3, -b_2)$. Similarly, let point Q denote the intersection of the line $a_2 : z = -x$ and the line $\overline{BA_3}$. $\overline{BA_3}$ has equation $c_2x - c_1y = 0$, and intersects $z = -x$ at the point $Q = (c_1, c_2, -c_1)$. Finally, we let R denote the intersection of the line $a_3 : x = -y$ and the line $\overline{BA_2}$. $\overline{BA_2}$ has equation $c_3x - c_1z = 0$, and intersects $x = -y$ at the point $R = (c_1, -c_1, c_3)$. See Figure 5.

Since the points $P = (0, b_3, -b_2)$, $Q = (c_1, c_2, -c_1)$, and $R = (c_1, -c_1, c_3)$ are collinear by Desargue's Theorem, we know that:

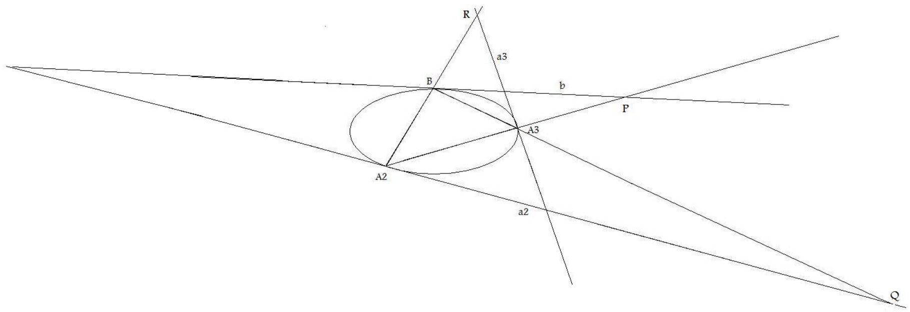

Figure 5: Triangles in perspective implies colllinear points

$$\begin{aligned}
0 &= \det\begin{pmatrix} 0 & b_3 & -b_2 \\ c_1 & c_2 & -c_1 \\ c_1 & -c_1 & c_3 \end{pmatrix} \\
&= -b_3(c_1c_3 + c_1^2) - b_2(-c_1^2 - c_1c_2) \\
&= -b_3c_1c_3 - b_3c_1^2 + b_2c_1^2 + b_2c_1c_2
\end{aligned}$$

This means that $b_2c_1^2 + b_2c_1c_2 = b_3c_1c_3 + b_3c_1^2$, and so

$$b_2(c_1 + c_2) = b_3(c_1 + c_3). \tag{6}$$

If we similarly apply Desargue's Theorem to the triangles BA_1A_3 and BA_1A_2 we find that

$$b_3(c_2 + c_3) = b_1(c_1 + c_2) \text{ and } b_1(c_1 + c_3) = b_2(c_2 + c_3). \tag{7}$$

Now, we have:

$$\begin{aligned}
(b_1, b_2, b_3) &= (c_1 + c_2)(b_1, b_2, b_3) \\
&= (b_1(c_1 + c_2), b_2(c_1 + c_2), b_3(c_1 + c_2)) \\
&= (b_3(c_2 + c_3), b_3(c_1 + c_3), b_3(c_1 + c_2)) \qquad \text{(by (6) and (7))} \\
&= b_3(c_2 + c_3, c_1 + c_3, c_1 + c_2) \\
&= (c_2 + c_3, c_1 + c_3, c_1 + c_2). \qquad (8)
\end{aligned}$$

Plugging (8) into (5) yields:

$$\begin{aligned}
0 &= (c_2 + c_3)c_1 + (c_1 + c_3)c_2 + (c_1 + c_2)c_3 \\
&= 2(c_1c_2 + c_2c_3 + c_1c_3)
\end{aligned} \tag{9}$$

and since q is odd,

$$c_1c_2 + c_2c_3 + c_1c_3 = 0 \tag{10}$$

for all points of the oval (besides A_1, A_2 and A_3). Now, consider the conic

$$\mathcal{C} := \{(x, y, z) | xy + yz + xz = 0\}.$$

Clearly, $A_1, A_2, A_3 \in \mathcal{C}$. Furthermore, (10) proves that each of the $q - 2$ points $(c_1, c_2, c_3) \in \mathcal{O} \setminus \{A_1, A_2, A_3\}$ lies on $\mathcal{C}$. Therefore, $\mathcal{C}$ contains the $q + 1$ points of $\mathcal{O}$. But Corollary 1.9 showed that $\mathcal{C}$ contains exactly $q + 1$ points. Therefore, $\mathcal{O} = \mathcal{C}$, and thus $\mathcal{O}$ is a conic. $\square$

References

[1] Peter J. Cameron. *Combinatorics: topics, techniques, algorithms.* Cambridge University Press, Cambridge, 1994.

[2] Rey Casse. *Projective geometry: an introduction.* Oxford University Press, Oxford, 2006.

[3] Marshall Hall, Jr. Ovals in the Desarguesian plane of order 16. *Ann. Mat. Pura Appl. (4)*, 102:159–176, 1975.

[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] Daniel R. Hughes and Fred C. Piper. *Projective planes.* Springer-Verlag, New York, 1973. Graduate Texts in Mathematics, Vol. 6.

[6] L. Lunelli and M. Sce. *k-archi completi nei piani proiettivi desarguesiani di rango* 8 *e* 16. Centro di Calcoli Numerici, Politecnico di Milano, Milan, 1958.

[7] Eric Moorhouse. Incidence geometry. August 2007.

[8] Christine M. O'Keefe and Tim Penttila. Hyperovals in $\mathrm{PG}(2, 16)$. *European J. Combin.*, 12(1):51–59, 1991.

[9] Tim Penttila. Configurations of ovals. *J. Geom.*, 76(1-2):233–255, 2003. Combinatorics, 2002 (Maratea).