Ovals and conics in a finite projective plane

1 Arcs, ovals and hyperovals

Consider a projective plane Π of order n. It has n^2+n+1 points, and as many lines; there are $n+1$ points on each line and as many lines on each point.

An *arc* in Π is a set of points, no three collinear.

If A is an arc, then $|A| \leq n+2$. (Indeed, choose a point P on the arc. Each of the $n+1$ lines on P contains at most 1 other point of A.) We see that if equality holds then each line meets A in either 0 or 2 points.

If n is odd and $n > 1$, and A is an arc, then $|A| \leq n+1$. (Indeed, choose a point Q outside A. If $|A| = n+2$ then precisely $(n+2)/2$ lines on Q meet A, but this number is not integral.)

An *oval* in Π is an arc of size $n+1$. A *hyperoval* is an arc of size $n+2$. Hyperovals can exist only in planes of even order n.

A line is called *tangent* to an oval if it meets the oval in precisely one point. If A is an oval then there is a unique tangent in each if its points.

Proposition 1.1 *If n is even, every oval is contained in a unique hyperoval.*

Proof: Consider an oval A, and let there be n_i points outside that are on precisely i tangents. We find

$$\sum n_i = n^2$$

(namely $n^2+n+1-|A|$),

$$\sum in_i = n(n+1)$$

(namely n outside points on each of the $n+1$ tangents) and

$$\sum \binom{i}{2} n_i = \binom{n+1}{2}$$

(the pairs of tangents). Combining these three equations yields

$$\sum (i-1)(i-n-1)n_i = 0.$$

But each outside point is on at least one tangent (since $|A|$ is odd) and on at most $n+1$ tangents, so all terms are nonpositive. It follows that all terms are zero, and $n_1 = n^2 - 1$, $n_{n+1} = 1$. Add the single point that is on $n+1$ tangents to A to get a hyperoval. $\square$

The intersection point of all tangents to an oval in a plane of even order is called the *nucleus* of the oval.

Of course one can go in the other direction, and obtain an oval from a hyperoval by removing an arbitrary point.

2 Conics

Now let Π be the finite projective plane of order q that is coordinatized by the field $\mathbf{F}_q$.

Every nondegenerate conic in Π is an oval. (If a line and a conic meet in at least three points, then the line is contained in the conic, so the conic is the union of two lines, and is degenerate. Also, the conic has precisely $q+1$ points since there is at least one point by Chevalley-Warning, and there is a unique tangent at each point.)

A famous theorem by Segre says that the reverse holds if q is odd.

Theorem 2.1 *Let q be odd. Then each oval in the projective plane Π over $\mathbf{F}_q$ is a conic.*

We first need a lemma.

Lemma 2.2 *Let O be an oval in the projective plane over $\mathbf{F}_q$, q odd. Let P, Q, R be three distinct points of O. Let ABC be the triangle of which the sides AB, BC, CA are tangent to O in the points R, P, Q, respectively. Then the three lines AP, BQ and CR are concurrent.*

Proof: Choose coordinates such that $P = (1, 0, 0)$, $Q = (0, 1, 0)$, $R = (0, 0, 1)$. Then the equations for the lines AB, BC, CA are $Y = cX$, $Z = aY$, $X = bZ$ for certain nonzero constants a, b, c. Let $T = (x, y, z)$ be a point of the oval distinct from P, Q, R. (Then x, y, z are nonzero.) The three lines TP, TQ, TR have equations $Z = \frac{z}{y}Y$, $X = \frac{x}{z}Z$, $Y = \frac{y}{x}X$, respectively. If we vary the point T we see all lines through P, Q, R this way, except for the three tangent lines and the sides of the triangle PQR. Now the product of all nonzero elements of $\mathbf{F}_q$ is -1 (since we can pair w and w^{-1} for $w \neq \pm 1$), and multiplying all directions of the lines containing precisely one of P, Q, R we find $(-1)^3 = abc \prod \frac{z}{y} \frac{x}{z} \frac{y}{x}$, so that $abc = -1$. Now $A = (b, bc, 1)$, $B = (1, c, ac)$, $C = (ab, 1, a)$ and the three lines AP, BQ and CR all pass through the point $(1, -c, ac) = (-b, bc, 1) = (ab, 1, -a)$. $\square$

The result $abc = -1$ of the proof of the above lemma can also be phrased as: Suppose an oval passes through three points P, Q, R, and has the tangents at P and Q in common with a conic through P, Q, R. Then it also has the tangent at R in common with that conic. (Indeed, a conic through P, Q, R

has equation $pXY + qYZ + rXZ = 0$, and the tangents at these points are $Z = -\frac{p}{r}Y$, $X = -\frac{q}{p}Z$ and $Y = -\frac{r}{q}X$. If $-\frac{p}{r} = a$ and $-\frac{q}{p} = b$, then $-\frac{r}{q} = c$.)

Proof (of the theorem): Choose three distinct points P, Q, R on the oval O, and let S be the common point constructed in the above lemma. Choose coordinates such that $P = (1, 0, 0)$, $Q = (0, 1, 0)$, $R = (0, 0, 1)$, $S = (1, 1, 1)$. We are in the case $a = b = c = -1$ of the proof of the lemma, so the tangents at P, Q, R are $Y + Z = 0$, $X + Z = 0$, $X + Y = 0$, respectively.

Now choose a point $T = (x, y, z)$ distinct from P, Q, R on the oval.

The conic $XY + YZ + XZ + sZ^2 = 0$ passes through P and Q and has tangents $Y + Z = 0$, $X + Z = 0$. Choose s so that it also passes through T. Then conic and oval have the same tangent at T, and that tangent is $(y+z)X + (x+z)Y + (y+x+2sz)Z = 0$.

The conic $XY + YZ + XZ + tY^2 = 0$ passes through P and R and has tangents $Y + Z = 0$, $X + Y = 0$. Choose t so that it also passes through T. Then conic and oval have the same tangent at T, and that tangent is $(y+z)X + (z+x+2ty)Y + (x+y)Z = 0$.

Since both equations must coincide we have $s = t = 0$, and each point of the oval lies on the conic with equation $XY + XZ + YZ = 0$. $\square$