On cubic curves in projective planes of characteristic two

David G. Glynn
Te Tari Tatau, Te Whare Wānanga o Waitaha,
Ōtautahi, Aotearoa*

Dedicated to the memory of Derrick Breach, 1933–1996

Abstract

The aim of this paper is to examine various interesting results from the theory of general cubic curves in projective planes of characteristic two. This leads to calculations involving nets of conics in the plane, invariants of the curves, syzygies, and Hessians. It is emphasized that classical methods, (that is those developed for geometries over fields of zero characteristic), do not always suffice for geometries of differing characteristics. For example, we give here a Hessian of a cubic curve that is a function of degree four in the coefficients of the curve for characteristic two, whereas the classical one has degree three. (The Hessian is used to calculate the points of inflection of a curve.) Particular attention is paid to the case of the planes $PG(2,q)$, where $q = 2^h$, for then the arithmetical and combinatorial properties of the curves come to the fore.

1. Introduction

Many problems in algebraic geometry are solved by reduction to special cases. For example, an inflection may be assumed to be a certain point, and this may imply that certain coefficients of a curve are zero. In this paper we emphasise "global" solutions to problems in the algebraic geometry of projective planes over fields of characteristic two. That is, many of the theorems and calculations here will be valid for *all* cubic curves, singular, non-singular, degenerate or non-degenerate. While it is of course harder to obtain results like this, the elegant simplicity and generality of the results obtained justify the labour involved. The fact that $1+1=0$ in fields of characteristic two means that it is often easier to make complicated calculations than in other fields. Also, the case of cubic curves in projective planes is the smallest non-trivial example of algebraic curves in projective spaces and so it is the natural

This research was partially supported by a von Humboldt Fellowship at the University of Erlangen-Nuremberg .

*Department of Mathematics & Statistics, University of Canterbury, Christchurch, New Zealand starting point for a global approach. Syzygies between invariants are the basis for many global properties in algebraic geometry. For example, Euler's relation for a hypersurface f of order n, $\sum x_i \partial f/\partial x_i = nf(x)$, is really a syzygy between the points x, the tangent hyperplanes, and any hypersurface f of order n. This syzygy is of degree 1 in the coefficients of f. However, there are syzygies of higher degree, each of which corresponds to a general geometric property holding for any hypersurface of order n. Of the many applications of the theory of algebraic curves that of coding theory is at present most fashionable; see [**15**] and [**20**].

Let us note a few technical points about this paper. First, the notation has been moulded to suit the special case of cubic curves of characteristic two. Also, many of the definitions and results of Chapter 2, and of some of those in Chapter 3 are standard. We calculate specific formulae that relate various geometrical (ie. invariantative) properties of the curves. Theorem 4.7 (about the xyz term of cubic curves), is well-known: it is a special case of the so-called Hasse invariant; see [**18**],[**29**]. A generalization of that theorem to hypersurfaces of degree $n+1$ in $PG(n,q)$ is given in [**14**]. Still, it is a useful exercise for the reader to follow the elementary proof that we give, being also valid for *all* cubic curves of $PG(2,q)$, q even.

There are the syzygies of Theorem 3.10, which afford generalizations to curves (and also hypersurfaces) over any field. However the author does not know the formulae for these generalizations. Then there are the more intricate calculations of Chapter 4, which tell much about the properties of pencils and nets of conics in the plane. Sometimes the properties are the same for odd and even characteristics, but often they are different.

In any case, the philosophical direction of the paper comes from various papers by Beniamino Segre — e.g. [**25,26,27**]. He was one of the first to point out that "esoteric" properties of "simple" algebraic curves and varieties, indeed of conics and quadrics, are of great use in combinatorics. However, using these properties involves an understanding of a strange mixture of classical and finite geometry. That is, one must understand when intuition fails. Indeed, for plane algebraic curves, it seems to fail when the order of the curve is at least the characteristic of the field. Thus, quadratic curves are anomalous in characteristic two, while cubics are anomalous in characteristics two and three.

Thus is produced an imbroglio from the seemingly simple algebraic object that is the cubic curve.

2. Notation and Definitions

The results we state or use without proof about points, lines and conics in planes of characteristic two may be obtained from the references [**19**], [**25**], or [**26**]. Many of the classical notions we use can be obtained from [**28**] while some of the more modern parts of the theory are contained in [**18**].

Notation 2.1. *The following notations hold throughout this paper.*

Z	the ring of integers
Z^+	the set of positive integers
K	a field of characteristic 2
K^n	the vector space of $1 \times n$ rows over K, where $n \in Z^+$
$\pi = \pi(K)$	the projective plane over K corresponding to K^3
$GF(q)$	the Galois field of order $q = 2^h$, where $h \in Z^+$
$PG(2,q)$	the same as $\pi(GF(q))$
x	a point of π; i.e. a non-zero vector (x_0, x_1, x_2) of K^3
x^t	a line of π; i.e. a non-zero 3×1 column vector over K
M	a general matrix $M = (m_{ij})$ over K
σ	a general automorphism of K
M^σ	the matrix (m^σ_{ji}) obtained from M and σ
M^2	the matrix M^σ, where $\sigma : k \mapsto k^2$, for $k \in K$
$\hat{x}$	$(x_1x_2, x_0x_2, x_0x_1)^t$, where $x = (x_0, x_1, x_2) \in K^3$

Note that a point x and a line y are incident in π if $xy = 0$ as matrices. Also, be careful not to confuse the notation M^2 with the product of M with itself. In this paper 2 always means the automorphism associated with squaring each element of a field of characteristic two. (It is possible that 2 is not an automorphism of K, but only a 1-1 mapping that preserves addition and multiplication. However for finite and many other fields of even characteristic squaring is certainly an automorphism. In any case we don't need this automorphism property very often.) Each mapping σ corresponds to a correlation of the plane to its dual, when it acts on the homogeneous (non-zero) row and column vectors in K^3. (Notice that i and j are interchanged in the notation of M^σ above.) Thus if x is a point, x^2 is a line, and vice-versa. The mapping $x \mapsto \hat{x}$, for all points $x \in \pi$, is a quadratic Cremona transformation from the plane to its dual. Also, the mapping $x \mapsto x^t$ is a polarity of π.

Definition 2.2. *A general conic of π is any set of points*

$$\mathcal{Q}(u, v) := \{x \in \pi \mid ux^2 + v\hat{x} = 0\},$$

where u and v are row vectors of K^3, not both zero. The nucleus of the conic above is defined to be the point v, (if this is non-zero).

Note. *There is a natural correspondence between the conics of π and the points of $PG(5, K)$.*

This is called the *Veronese map* :

$$\mathcal{Q}(u, v) \mapsto (u, v).$$

The conic is *non-singular*, (which is the same as *non-degenerate* in this case), if and only if its nucleus does not belong to the conic. That is, if and only if

$$uv^2 + v\hat{v} \neq 0.$$

Note that $v\hat{v}$ is equal to the product of the three coordinates of v, as $3 = 1$ in K. The singular conics are then mapped to the points of the cubic primal $\Omega : uv^2 + v\hat{v} = 0$, and the repeated line degenerate conics are mapped to the degenerate *Veronese surface* F of $PG(5, K)$. It is the plane $v = 0$ contained in Ω. This situation contrasts with the classical case, where the Veronese surface does not degenerate.

All the tangents of the conic pass through the nucleus, if it is defined. The fact is that Euler's relation for a general algebraic curve is identically zero if the characteristic of the field divides the order of the curve. This is the case for conics in characteristic two.

Definition 2.3. *A general cubic curve of π is any set of points*

$$\mathcal{C}(A, a) := \{x \in \pi \mid xAx^2 + ax\hat{x} = 0\},$$

where A is a 3×3 matrix over K and $a \in K$, such that A and a are not both zero.

Definition 2.4. *The first polar with respect to $\mathcal{C} = \mathcal{C}(A, a)$ of a point x of π is the conic*

$$x\mathcal{C} := \mathcal{Q}(xA, ax),$$

if xA and ax are not both zero.

The tangents of $\mathcal{C}$ passing through a general point x of π are found by finding the intersection of the first polar of x with $\mathcal{C}$, then joining these points to x.

Definition 2.5. *The second polar with respect to $\mathcal{C} = \mathcal{C}(A, a)$ of a point x of π is the line*

$$\mathcal{C}x := Ax^2 + a\hat{x},$$

if this is non-zero. If $x \in \mathcal{C}$ and $\mathcal{C}x$ is non-zero, $\mathcal{C}x$ is the tangent to $\mathcal{C}$ at x. Given that $\mathcal{C}$ is fixed, let $\mathcal{C}(x) := x(\mathcal{C}x)$. Then $\mathcal{C}(x) = 0$ is the equation of $\mathcal{C}$.

The classical formula for the second polar of a point x with respect to an algebraic curve $f = 0$ in a projective plane is given by

$$\mathcal{C}x := \begin{pmatrix} \partial f/\partial x_0 \\ \partial f/\partial x_1 \\ \partial f/\partial x_2 \end{pmatrix}.$$

One can check that the two formulae for $\mathcal{C}x$ above are the same.

Definition 2.6. *A pencil of conics is a linear 1-dimensional set of conics of π. This corresponds to a line in the 5-dimensional space of all conics. A net of conics is a linear 2-dimensional set of conics of π. This corresponds to a plane in the 5-dimensional space of all conics.*

Note 2.7. *Let $\mathcal{C} = \mathcal{C}(A, a)$ with $a \neq 0$. Then*

$$\mathcal{N}(\mathcal{C}) := \{x\mathcal{C} \mid x \in \pi\}$$

is a net of conics associated with the cubic curve $\mathcal{C}$.

Clearly the net is generated by the first polars of three points of any triangle of π . Since the nucleus of $x\mathcal{C}$ is x, there is a unique conic of the net with any given nucleus point of the plane. Conversely, any such net is the set of first polar conics of a unique cubic curve $\mathcal{C}(A, a)$ with $a \neq 0$. It is important to observe that *the points of $\mathcal{C}$ are the points x for which $x\mathcal{C}$ is degenerate.*

Note 2.8. *A cubic curve $\mathcal{C}(A, 0)$, with $|A| := det(A) \neq 0$ has an associated correlation from π to its dual given by $x \mapsto \mathcal{C}x$. The cubic is the set of absolute points of this correlation. That is, it is the set of points which lie on their image-lines.*

Definition 2.9. *A point x of a cubic curve $\mathcal{C}$ is called a singularity if there is no tangent defined at x.*

Since $\mathcal{C}(x) = x(\mathcal{C}x)$, every point x with $\mathcal{C}x = 0$ is a point of $\mathcal{C}$ and so is a singularity. Hence *the set of singularities of $\mathcal{C}$* is given by

$$\mathcal{S}(\mathcal{C}) := \{x \in \pi \mid \mathcal{C}x = 0\}.$$

Also, if $a \neq 0$, every conic of the net $\mathcal{N}(\mathcal{C})$ passes through $\mathcal{S}(\mathcal{C})$. On the other hand, if $a = 0$, a cubic $\mathcal{C}(A, 0)$ is non-singular if and only if A is a non-singular matrix. The classical name for a cubic $\mathcal{C}(A, 0)$ with $|A| \neq 0$ is *equianharmonic.*

3. Properties of cubic curves in characteristic 2

Here we investigate these curves in greater detail, and show how to construct the *invariants* of a general curve. The term 'invariant' is taken in its widest sense ... it is an algebraic construction depending on the coefficients of the curve, that commutes with any linear transformation (homography) of the plane. *Syzygies*, which give global properties, are any algebraic relations that hold between the invariants.

Note 3.1. *If a point is a singularity then every line through it is considered to be a tangent.*

Theorem 3.2. *The set $\mathcal{C}'$ of tangent lines to $\mathcal{C} = \mathcal{C}(A, a)$, classically the dual of a sextic curve, is in the case of even characteristic a dual cubic curve (or cubic envelope) $\mathcal{C}' := \mathcal{C}(A', a^2)^t$. Let $A := (a_{ij}), (i, j = 0, 1, 2)$. Then A' is the 3×3 matrix over K given by*

$$A' := adj(A)^t + a \begin{pmatrix} 0 & a_{02} & a_{01} \\ a_{12} & 0 & a_{10} \\ a_{21} & a_{20} & 0 \end{pmatrix}, \text{ where}$$

$$adj(A)^t := \begin{pmatrix} a_{11}a_{22} + a_{12}a_{21} & a_{10}a_{22} + a_{12}a_{20} & a_{10}a_{21} + a_{11}a_{20} \\ a_{01}a_{22} + a_{02}a_{21} & a_{00}a_{22} + a_{02}a_{20} & a_{00}a_{21} + a_{01}a_{20} \\ a_{01}a_{12} + a_{02}a_{11} & a_{00}a_{12} + a_{02}a_{10} & a_{00}a_{11} + a_{01}a_{10} \end{pmatrix}.$$

Thus the coefficients of $\mathcal{C}'$ are homogeneous quadratic functions of those of $\mathcal{C}$.

Proof. This can be shown in various ways. One way would be to use the syzygies (algebraic identities) of Theorem 3.10. Another, more direct way would be to take a special case of a cubic curve and to show that the formula for $\mathcal{C}'$ holds in this case. Then one can use the transformation formula of Theorem 3.7 to convert to the general case. Example 5.2 gives some of the calculations for the general cubic with arbitrary j-invariant with a non-zero. When $a = 0$ things are easier because we are saying that the curve $xAx^2 = 0$ has curve of tangents $x(adjA)^t x^2 = 0$, (in dual coordinates). This follows because the tangent at a point x of $\mathcal{C}$ is $\mathcal{C}x = Ax^2$ so that one has to check that

$$(Ax^2)^t adj A^t (Ax^2)^{t2} = 0 \iff xAx^2 = 0.$$

Once the formula for $a = 0$ is known, it is only necessary to calculate the coefficient of a in A'. We leave that as an exercise.

Definition 3.3. *A point of inflection of a cubic curve is a point of the curve such that the tangent at that point meets the curve algebraically in a triple intersection.*

Definition 3.4. *A'' is the matrix of the cubic curve $\mathcal{C}'' := (\mathcal{C}')'$. Thus $\mathcal{C}'' = \mathcal{C}(A'', a^4)$ is the set of 'tangent points' of the tangent envelope of $\mathcal{C}$. We can continue this process forever, starting with $\mathcal{C}^{(0)} := \mathcal{C}$. Thus, if m is an odd positive integer, $\mathcal{C}^{(m)} = \mathcal{C}(A^{(m)}, a^{2^m})^t$ is defined to be the tangent envelope of $\mathcal{C}^{(m-1)}$, while if m is an even positive integer, $\mathcal{C}^{(m)} = \mathcal{C}(A^{(m)}, a^{2^m})$ is defined to be the set of 'tangent points' of the cubic envelope $\mathcal{C}^{(m-1)}$.*

Theorem 3.5. *If $a \neq 0$, the points of inflection of a cubic curve $\mathcal{C}$ are those points of $\mathcal{C}$ which are not singularities and are also on the cubic curve $\mathcal{C}''$. Naturally, $\mathcal{C}$ and $\mathcal{C}''$ must be independent. Thus we must have the condition that $(A'', a^4) \neq k(A, a)$; i.e. $A'' \neq a^3 A$. We shall see that this is satisfied if $\mathcal{C}$ is non-singular.*

Proof. $\mathcal{C}''$ is an invariant of $\mathcal{C}$ and since it is a cubic it intersects $\mathcal{C}$ in $3 \times 3 = 9$ points (Bézout's theorem), which must be invariant points of $\mathcal{C}$. These have to be the 9 points of inflection. (This argument is for the 'general case', but it also works for special cases if we make the assumption about singularities and about the independence of $\mathcal{C}$ and $\mathcal{C}''$.)

Note that in the classical (not characteristic two) case, the points of inflection are found by using the *Hessian* cubic curve. The Hessian, for a general plane curve f, has equation

$$det \begin{pmatrix} \partial^2 f/\partial x_0^2 & \partial^2 f/\partial x_0 \partial x_1 & \partial^2 f/\partial x_0 \partial x_2 \\ \partial^2 f/\partial x_1 \partial x_0 & \partial^2 f/\partial x_1^2 & \partial^2 f/\partial x_1 \partial x_2 \\ \partial^2 f/\partial x_2 \partial x_0 & \partial^2 f/\partial x_2 \partial x_1 & \partial^2 f/\partial x_2^2 \end{pmatrix} = 0.$$

Although the classical equations are of no use here, because the usual Hessian vanishes for characteristic two, we can still call the curve $\mathcal{C}''$ the Hessian of $\mathcal{C}$. Also, the coefficients for $\mathcal{C}''$ are homogeneous quartics in those of $\mathcal{C}$, whereas in the classical case the coefficients of the Hessian are cubics in those of the original curve. Later (after Theorem 3.13) we shall find a Hessian $\mathcal{G}$, which is a linear combination of $\mathcal{C}$ and $\mathcal{C}''$, that *is* a cubic in the coefficients of $\mathcal{C}$. The Hessian $\mathcal{C}''$ does not work when $a = 0$ because $\mathcal{C}$ and $\mathcal{C}''$ are dependent in this case. However, Theorem 3.14 solves this.

Definition 3.6. *The syzygetic pencil of a cubic curve is defined to be the pencil (or 1-dimensional space) of cubics generated by the cubic and its Hessian curve.*

Equivalently, it is the pencil of cubic curves passing through the set of inflections of a fixed cubic curve. Note that this pencil is an invariant of the curve.

It is useful to know the effect of a coordinate transformation on the equations of a cubic curve, and this is solved by the following.

Theorem 3.7. *Let $\mathcal{C} = \mathcal{C}(A, a)$, and let $y = xB$ be a general point of $\mathcal{C}$, where $|B| \neq 0$, and B is 3×3 over K. Let b_0, b_1, and b_2 be the 3 rows of B. Then x belongs to the cubic $\mathcal{C}((b_iCb_j), a|B|)$, where $|B| := det(B)$ and*

$$(b_iCb_j) := \begin{pmatrix} b_0Cb_0 & b_0Cb_1 & b_0Cb_2 \\ b_1Cb_0 & b_1Cb_1 & b_1Cb_2 \\ b_2Cb_0 & b_2Cb_1 & b_2Cb_2 \end{pmatrix}.$$

Proof. In the formula above, b_iCb_j means $b_i(Cb_j)$. Now y satisfies

$$\begin{aligned} & yAy^2 + ay\hat{y} = 0 \\ \iff & xBA(xB)^2 + axB\widehat{xB} = 0 \\ \iff & xBAB^2x^2 + axB\widehat{xB} = 0 \\ \iff & xBAB^2x^2 + ax\left(\widehat{b_ib_j}\right)x^2 + a|B|x\hat{x} = 0 \\ \iff & x\left(b_iCb_j\right)x^2 + a|B|x\hat{x} = 0. \end{aligned}$$

Note that by choosing the three "base points" b_i optimally it is possible to simplify the equations of any given cubic.

Definition 3.8.

(1) *An invariant of a general cubic curve is a rational function of the ten coordinates of the curve that permutes with any homographic transformation of the type considered in the previous theorem.*

(2) *A numerical invariant is an invariant function from the ten coordinates to $K \cup \{\infty\}$.*

Theorem 3.9. *The numerical invariants are the rational functions of Δ/a^{12}, where*

$$\Delta = \Delta[\mathcal{C}] := |a^3A + A''|.$$

Note that Δ is of degree 12 in $\mathcal{C}$. The "classical" j-invariant is just a^{12}/Δ.

Proof. It is well known that every numerical invariant is a rational function of j, so it is only necessary to verify that $j = a^{12}/\Delta$ for a special case. This is done in Example 5.2. Note that Δ must be an invariant as $\Delta = 0$ is the condition that the cubic with $a = 0$ of the syzygetic pencil of $\mathcal{C}$ is degenerate. Also, Δ is a homogeneous function of degree 12 in the coefficients of $\mathcal{C}$ and so Δ/a^{12} is a numerical invariant.

Theorem 3.10. *The following are syzygies of cubic curves in π. $\Delta[\mathcal{D}]$ denotes the Δ invariant of any cubic curve $\mathcal{D}$; Δ denotes $\Delta[\mathcal{C}]$; $\mathcal{D}(x)$ denotes the value of $\mathcal{D}$ at a general point x; for $\mathcal{C}'$, $\mathcal{C}''$, ... see Theorem 3.2 and Definition 3.4.*

(1) $\mathcal{C}'(\mathcal{C}x) = \mathcal{C}(x).\mathcal{C}''(x)$.
(The equation is of degree five in $\mathcal{C}$ and of degree six in x.)

(2) $\mathcal{C}'(a^3\mathcal{C}x + \mathcal{C}''x) = \Delta\mathcal{C}(x)^2$.
(The equation is of degree fourteen in $\mathcal{C}$ and of degree six in x.)

(3) $\mathcal{C}'((e+1)a^3\mathcal{C}x+e\mathcal{C}''x) = a^9\mathcal{C}(x)\mathcal{C}''(x)+ea^6\mathcal{C}''(x)(a^3\mathcal{C}(x)+\mathcal{C}''(x))+e^2a^3f(x)$ $+e^3\Delta\mathcal{C}(x)^2$, $\forall e \in K \cup \{\infty\}$.
(This is also of degree fourteen in $\mathcal{C}$ and degree six in x.)

(4) $(e\mathcal{C} + f\mathcal{C}'')' = e^2\mathcal{C}' + f^2\mathcal{C}^{(3)}, \forall e, f \in K$.
(This is of degree eight in $\mathcal{C}$.)

(5) $(a^3\Delta)^{2^m}\mathcal{C}^{(m)}(x) + (\Delta + a^{12})^{2^m}\mathcal{C}^{(m+2)}(x) = \mathcal{C}^{(m+4)}(x), \forall m \geq 0$.
(This is of degree 2^{m+4} in $\mathcal{C}$ and of degree three in x.)

(6) $(a^3\mathcal{C} + \mathcal{C}'')'' = \Delta(a^3\mathcal{C} + \mathcal{C}'')$.
(This is of degree sixteen in $\mathcal{C}$.)

(7) $\Delta[a^3e\mathcal{C} + (e+1)\mathcal{C}''] = \Delta(\Delta + a^{12}e + \Delta e^4)^3, \forall e \in K$.
(This equation is of degree 48 in $\mathcal{C}$.)

Proof. These are algebraic identities which can be verified by a program such as MAPLE. Another approach is to verify them for a special case, such as in Example 5.2, and then to use the fact that they are invariant under linear transformation. We leave this to the reader except for the calculation of (5), (6) and (7) ... the latter is probably out of reach for most computers at the present time.

The easiest is probably (6), which deals with the equianharmonic member of the syzygetic pencil of $\mathcal{C}$. This member has equation $xEx^2 = 0$, where $E = a^3A + A''$. Its envelope of tangents has matrix $adj(E)^t$, and so $E' = adj(E)^t$. Furthermore, $E'' = adj(adj(E)^t)^t = \det(E)E$. Since $\Delta = \det(E)$ we obtain the result.

Next, consider syzygy (6) and assume syzygy (4). Then we obtain $a^{12}\mathcal{C}''+\mathcal{C}^{(4)} = \Delta(a^3\mathcal{C} + \mathcal{C}'')$ which gives $\mathcal{C}^{(4)} = \Delta a^3\mathcal{C} + (a^{12} + \Delta)\mathcal{C}''$. This is syzygy (5) in the case $m = 0$. The cases $m > 1$ are obtained by applying (4) to the case $m = 0$.

Now we prove syzygy (7). Consider a general cubic $\mathcal{C}$ and assume that $a = 1$, which is no restriction by homegeneity. By syzygy (4) we see that

$$(e\mathcal{C} + (e+1)\mathcal{C}'')' = e^2\mathcal{C}' + (e^2+1)\mathcal{C}^{(3)}, \text{ and so}$$
$$\begin{aligned}(e\mathcal{C} + (e+1)\mathcal{C}'')'' &= (e^2\mathcal{C}' + (e^2+1)\mathcal{C}^{(3)})' = e^4\mathcal{C}'' + (e^4+1)\mathcal{C}^{(4)} \\ &= e^4\mathcal{C}'' + (e^4+1)(\Delta\mathcal{C} + (\Delta+1)\mathcal{C}''), \text{ by syzygy (5).}\end{aligned}$$

Thus

$$(e\mathcal{C} + (e+1)\mathcal{C}'') + (e\mathcal{C} + (e+1)\mathcal{C}'')'' = (e + \Delta(e^4+1))(\mathcal{C} + \mathcal{C}'').$$

Now this latter cubic is the equianharmonic member of the syzygetic pencil of $e\mathcal{C} + (e+1)\mathcal{C}''$ and so $\Delta[e\mathcal{C} + (e+1)\mathcal{C}'']$ is the determinant of the matrix of $(e + \Delta(e^4+1))(\mathcal{C} + \mathcal{C}'')$, which is

$$(e + \Delta(e^4+1))^3\Delta[\mathcal{C}] = (e + \Delta(e^4+1))^3\Delta.$$

When we introduce the appropriate powers of a for homogeneity in the coefficients of $\mathcal{C}$, we obtain Theorem 3.10(7).

Notes. *Let $\Delta \neq 0$ and let γ be the correlation*

$$x \mapsto (a^3\mathcal{C} + \mathcal{C}'')x = (a^3A + A'')x^2.$$

(1) *A point $x \in \mathcal{C}$ or $\mathcal{C}''$ if and only if its second polar $\mathcal{C}x \in \mathcal{C}'$. Thus the pre-image of $\mathcal{C}'$ under the second polar map is $\mathcal{C} \cup \mathcal{C}''$.*

(2) *A point $x \in \mathcal{C} \iff x^\gamma \in \mathcal{C}'$. Thus $\mathcal{C}'$ is isomorphic to the dual of $\mathcal{C}$, and $\mathcal{C}''$ is isomorphic by a collineation (but not in general a homography) to $\mathcal{C}$.*

(3) *This equation tells us how a certain pencil of lines defined from the syzygetic pencil is incident with $\mathcal{C}'$. The case $e = 0$ gives syzygy (1) while $e = \infty$ gives syzygy (2). The function f is an invariant of $\mathcal{C}$ for which we do not have a simple form. If we suppose that $\mathcal{C}(x)$ or $\mathcal{C}''(x) = 0$ we see that there are at most two values for e that make the equation zero. Hence it is clear that $\mathcal{C}x \cap \mathcal{C}''x$ is a point of $\mathcal{C}''$ for all points $x \in \mathcal{C} \cup \mathcal{C}''$.*

(4) *It follows that the tangent envelope of any member of the syzygetic pencil is in a dual syzygetic pencil, and vice-versa.*

(5) *$a^3\Delta\mathcal{C}(x) + (\Delta + a^{12})\mathcal{C}''(x) = \mathcal{C}^{(4)}$, and any even power of $\mathcal{C}$ is in the same syzygetic pencil.*

(6) *Any even power of the equianharmonic member of the pencil is equal to itself.*

(7) *The Δ-invariant of any member of the syzygetic pencil is given by this formula. In particular the four Maclaurin triangles of the pencil can be found from the solutions to the quartic $\Delta + a^{12}e + \Delta e^4 = 0$, and these are the only singular cubics in the pencil. The twelve lines of these four triangles are the lines of the $AG(2,3)$ that forms the configuration of the points of inflection. In this configuration each triangle is a parallel class, and the twelve vertices of the triangles are the complement of the $AG(2,3)$ in a subplane $PG(2,4)$ in the algebraic closure of π; see also Theorem 3.13 below.*

Theorem 3.11. *The number of singularities $n = n(\mathcal{C})$ of a cubic curve $\mathcal{C} := \mathcal{C}(A, a)$ with $a \neq 0$ in $\bar{\pi} := \pi(\bar{K})$, where $\bar{K}$ is the algebraic closure of K, may be calculated from the formula:*

$$n = 3 - rank(a^3A + A'').$$

Proof. Since the curve of tangents $\mathcal{C}'$ is a cubic envelope, we see that there should be at most 3 singularities on a cubic curve. Using the fact that $rank(a^3A + A'')$ is an invariant it is clear that we only have to look at special cases to prove the theorem. These cases are as follows.

(1) $\mathcal{C}$ non-singular: e.g. $x_0^3 + x_1^3 + x_2^3 + ax_0x_1x_2 = 0$;

(2) $\mathcal{C}$ irreducible, 1 singularity: e.g. $x_1^3 + x_2^3 + x_0x_1x_2 = 0$;

(3) $\mathcal{C}$ splits into line and irreducible conic: e.g. $x_0^3 + x_0x_1x_2 = 0$;

(4) $\mathcal{C}$ splits into a triangle of lines: e.g. $x_0x_1x_2 = 0$.

Every cubic with $a \neq 0$ may be transformed by a homography of $\bar{\pi}$ into one of these forms; see e.g. [**19**]. One only needs to check now that the rank of $a^3A + A''$ in (i) above is $4 - i$, $i = 1, 2, 3, 4$. The singularity of (2) is $(1, 0, 0)$; the two singularities of (3) are the intersections of the line and the conic; and the three singularities of the triangle (4) are the vertices of the triangle. It is interesting that if $\mathcal{C}$ is the case (2) above, then $\mathcal{C}'$ is the case (3), and $\mathcal{C}''$ is case (4). Thus, given any singular cubic (with $a \neq 0$), we always reach a triangle by successive application of the tangent curve mapping.

Corollary 3.12. *A cubic curve $\mathcal{C}(A, a)$ is non-singular $\iff \Delta = |a^3A + A''| \neq 0$.*

Theorem 3.13. *If $\mathcal{C}$ is a non-singular cubic, then the set of inflections $\mathcal{C} \cap \mathcal{C}''$ of $\mathcal{C}$ is a set of 9 points in the plane $\bar{\pi}$. The configuration of these 9 points forms an affine plane $AG(2, 3)$ of order 3, embedded in a subplane $PG(2, 4)$ of $\bar{\pi}$. The four parallel classes of lines of the $AG(2, 3)$ are triangles of $\bar{\pi}$ and these are the four degenerate cubics of the syzygetic pencil through the points of inflection. The nine inflections may also be found as the subgroup of order nine in the abelian group of the cubic (over $\bar{\pi}$). This subgroup is isomorphic to $Z_3 \times Z_3$. Also, there is a unique syzygetic pencil corresponding to every non-singular cubic with $a = 0$, and vice-versa.*

Proof. The configuration formed by the points of inflection is $AG(2, 3)$; see [**18**], [**19**]. The new part of this theorem is the fact about the points of inflection being contained in $PG(2, 4)$. However, this is trivial in the case of characteristic 2, since any $AG(2, 3)$ configuration is contained in a subplane of order 4 in this case. (One can also check it for special cases and use the property of invariance of inflection points; see Example 5.1.)

Although we have found a Hessian $\mathcal{C}''$ that is of fourth degree in $\mathcal{C}$ it is still possible to find one of degree 3. This can be done as follows. Let $\mathcal{C} = \mathcal{C}(A, a)$ as usual. Let $\mathcal{G} := \mathcal{C}((A'' + |A|A)/a, a^3 + |A|)$. Then $\mathcal{G}$ is in the syzygetic pencil of $\mathcal{C}$ since $a\mathcal{G}(x) = |A|\mathcal{C}(x) + \mathcal{C}''(x)$. Suppose we expand A'' as a quartic in a. Then the constant term is $|A|A$ so that a does divide $A'' + |A|A$. Thus $\mathcal{G}$ is a cubic in $\mathcal{C}$, which we could take for a Hessian for $\mathcal{C}$. However it is not clear that $\mathcal{G}$ is an invariant of $\mathcal{C}$. Any cubic curve of the form $\mathcal{G} + p\mathcal{C}$, where p is a quadratic polynomial in the 10 coefficients of $\mathcal{C}$ could also be taken as a Hessian for $\mathcal{C}$. In [**8**], Dickson investigated cubic curves over $GF(2)$ and also found a Hessian, which he called $\mathcal{H}$. We leave it to the reader to check that $\mathcal{H} = (a_{01}a_{02} + a_{10}a_{12} + a_{20}a_{21})\mathcal{C} + \mathcal{G}$. He obtained his $\mathcal{H}$ by a direct calculation of a line intersecting $\mathcal{C}$ triply. So this is a double check of our calculations, and of his. He actually stated that $\mathcal{H}$ was an invariant (or covariant) of $\mathcal{C}$, although his calculations only appear to prove that the syzygetic pencil formed by $\mathcal{C}$ and $\mathcal{H}$ is an invariant.

Theorem 3.14. *Let $\mathcal{C} = \mathcal{C}(A, 0)$, $(a = 0)$, where $|A| \neq 0$, so that $\mathcal{C}$ is a general non-singular equianharmonic plane cubic curve. Then the syzygetic pencil of $\mathcal{C}$ is generated by $\mathcal{C}$ and $\mathcal{G} := \mathcal{C}(ABA, |A|)$, where*

$$B = \begin{pmatrix} 0 & a_{12} & a_{21} \\ a_{02} & 0 & a_{20} \\ a_{01} & a_{10} & 0 \end{pmatrix}$$

Proof. We just put $a = 0$ in the formula $\mathcal{G} := \mathcal{C}((A'' + |A|A)/a, a^3 + |A|)$. Then we find that ABA is the coefficient of a in $A'' + |A|A$.

Note that B is also related to the general formula for $\mathcal{C}'$, for if $\mathcal{D} = \mathcal{C}(A, a)$, then $\mathcal{D}' = \mathcal{C}(A', a^2)^t$, where $A' = adj(A)^t + aB^t$. Also, $A\ adj(A) = |A|I$, so that $|A|\mathcal{C}(A, 0) = \mathcal{C}(A\ adj(A)A, 0)$. Thus a general member of the syzygetic pencil of $\mathcal{C}(A, 0)$ is given by

$$|A|\mathcal{C}(A, 0) + a\mathcal{C}(ABA, |A|) = \mathcal{C}(A[adj(A) + aB]A, a|A|).$$

We see that another Hessian for $\mathcal{C}(A, 0)$ could be given by

$$\mathcal{C}(AA'^t A, a|A|).$$

4. Arithmetic Results

In this section we investigate the case of cubics in the finite projective planes over the Galois fields $GF(q)$, where $q = 2^h$. These are the only finite fields of characteristic two. Let $\pi = PG(2, q)$, with $q = 2^h, h \in Z^+$, from now on.

From the general theory of the preceding chapter it is clear that the investigation can be split into two major cases: $a = 0$ and $a \neq 0$. However the case $a \neq 0$ is more interesting because of its association with nets of conics, so we shall look at that case in far greater detail.

Note 4.1. *The theory of cubics with $a \neq 0$ is equivalent to that of nets of conics of π such that every point is the nucleus of a unique conic of the net. See Note 2.7.*

We now give a detailed analysis of these kinds of nets.

Theorem 4.2. *Here we list the various kinds of conics. There are up to homographies four kinds of conics $\mathcal{Q}(u, v)$ of the plane π.*

(1) *$uv^2 + v\hat{v} \neq 0$: the non-degenerate conic has $q + 1$ points no three collinear. There is a unique point not on the conic, called the nucleus of the conic, such that the $q + 1$ lines through the nucleus are the tangents to the conic.*
(2) *$uv^2 + v\hat{v} = 0, v \neq 0$: the degenerate conic has two real lines intersecting in v. We call this type of conic a line-pair. It has $2q + 1$ points.*
(3) *$uv^2 + v\hat{v} = 0, v \neq 0$: the degenerate conic has two imaginary conjugate lines r and r^q intersecting in v. We call this type of conic an imaginary line-pair. It has just the single real point v.*
(4) *$v = 0$: the degenerate conic is made up of a line of π repeated twice. This is called a repeated line-pair. Since there is no well-defined nucleus to such a conic it does not appear in the net of a cubic curve $\mathcal{C}(A, a)$ with $a \neq 0$.*

Theorem 4.3. *In Tables 1 and 2 we give the classification of pencils of conics in the plane π.*

There are two main cases: those containing at least one non-degenerate conic and those containing only degenerate conics. In the first case it turns out that the pencils are completely specified by the type of quartic polynomial that is given by the intersection of the quadratic curves. In Table 1 below, the column headed by α gives the number of *real* points of intersection of the conics of the pencil. Note that we use the word 'real' to denote actual algebraic objects that occur over the field, and not over some algebraic extension of the field.

Let $i1$, $j1$, $k1$, and $m1$ denote general different linear polynomials over $GF(q)$. Let $i2$ and $j2$ denote a general independent irreducible quadratic polynomials over $GF(q)$. Let $i3$ denote a general irreducible cubic polynomial over $GF(q)$ and $i4$ a general irreducible quartic polynomial over $GF(q)$.

In Table 1, y denotes the number of line-pairs, z denotes the number of imaginary line-pairs, and w denotes the number of repeated lines in the pencil. The last column gives the number of non-degenerate conics in the plane intersecting a fixed non-degenerate conic in the given intersection type. Thus the sum of the numbers in the final column is one less than the number of non-degenerate conics in the plane — it is $q^5 - q^2 - 1$. This table can be found in the author's Ph.D thesis, and is valid also for odd q; see [**11**]. It shows that such a pencil is determined by the type of quartic invariant given by the four (possibly imaginary) points of intersection of the conics. The pencils (h') and (h'') are the only pencils where the numbers of degenerate conics in the pencil do not precisely determine the type.

TABLE 1. **Pencils containing non-degenerate conics**

type	α	*intersection*	y	z	w	*fixed conic*
(a)	0	$i4$	1	2	0	$(q+1)q(q-1)(q-2)(q-3)/8$
(b)	0	$i2.i2$	0	1	1	$q(q-1)(q-2)/2$
(c)	0	$i2.j2$	0	1	0	$(q+1)q^2(q-2)^2/4$
(d)	1	$i1.i1.i2$	1	1	0	$(q+1)q(q-1)(q-2)/2$
(e)	1	$i1.i1.i1.i1$	0	0	1	$(q+1)(q-1)$
(f)	1	$i1.i3$	0	0	0	$(q+1)^2q^2(q-1)/3$
(g)	2	$i1.i1.j1.j1$	1	0	1	$(q+1)q(q-2)/2$
(h')	2	$i1.i1.i1.j1$	1	0	0	$(q+1)q(q-1)$
(h'')	2	$i1.j1.i2$	1	0	0	$(q+1)q^2(q-1)^2/4$
(i)	3	$i1.i1.j1.k1$	2	0	0	$(q+1)q(q-1)(q-2)/2$
(j)	4	$i1.j1.k1.m1$	3	0	0	$(q+1)q(q-1)(q-2)(q-3)/24$

There are four types of pencil containing only degenerate conics given by the following Table 2.

TABLE 2. **Pencils containing only degenerate conics**

type	α	y	z	w
(1)	1	0	0	$q+1$
(2)	$q+2$	$q+1$	0	0
(3)	$q+1$	q	0	1
(4)	1	$q/2$	$q/2$	1

Note. We omit the proofs for the above Tables 1 and 2 as they require many messy calculations. Table 2 is not valid for q odd, as can be seen from the type (4) pencils. The four normal forms for the pencils of type (1), (2), (3) and (4) respectively are:

(1) $x_0^2 + \lambda x_1^2 = 0$;
(2) $x_0 x_1 + \lambda x_0 x_2 = 0$;
(3) $x_0^2 + \lambda x_0 x_2 = 0$;
(4) $x_0^2 + \lambda x_1(x_0 + x_1) = 0$.

See [**2**] for further information about quadric pencils.

Lemma 4.4. *We consider now only those pencils that contain no repeated line-pairs, for repeated line-pairs do not occur in a net $\mathcal{N}(\mathcal{C})$ of a cubic curve. Let such a pencil contain x non-degenerate conics, y line-pairs, and z imaginary line-pairs. Suppose the conics of the pencil have α common points. Then the following equations hold.*

(1) $x + y + z = q + 1$
(2) $x + 2y = q + \alpha$
(3) $\alpha = y - z + 1$

Proof. The number of conics in a pencil is $q+1$, so (1) holds. Since a non-degenerate conic contains $q+1$ points, a line-pair $2q+1$ points, and an imaginary line-pair 1 point, counting point-conic incidences gives

$$(q+1)\alpha + q^2 + q + 1 - \alpha = x(q+1) + y(2q+1) + z.$$

Subtracting equation (1) from both sides and dividing by q gives equation (2), while (3) is obtained by subtracting (1) from (2).

From now on let $n = n(\mathcal{C}) = |S(\mathcal{C})|$ be the number of *real* singularities of a general cubic curve $\mathcal{C}$ with $a \neq 0$, and let $y(\mathcal{C})$ and $z(\mathcal{C})$ be the number of real and imaginary line-pairs respectively in the net $\mathcal{N}(\mathcal{C})$.

Theorem 4.5. *The number of points on a cubic curve $\mathcal{C} = \mathcal{C}(A, a)$ with $a \neq 0$ is given by*

$$|\mathcal{C}| = y(\mathcal{C}) + z(\mathcal{C}) = qn + 2z(\mathcal{C}).$$

Proof. First, a point p is in $\mathcal{C}$ if and only if the conic $p\mathcal{C}$ is degenerate. Thus we have the equation

$$|\mathcal{C}| = y(\mathcal{C}) + z(\mathcal{C}).$$

Let r be a general line of π. The points on r are the nuclei of a pencil of conics of $\mathcal{N}(\mathcal{C})$ given by $P_r := \{x\mathcal{C} \mid x \in r\}$. Suppose there are x_r, y_r, and z_r conics of type non-degenerate, line-pair, and imaginary line-pair, respectively in P_r. Consider a general point g of π. Let $m(g)$ be the size of the set

$$\{(u, v\mathcal{C}) \mid u, v \in \pi, u \in g\mathcal{C}, u \in v\mathcal{C}, v \neq g\}.$$

Since a point u of π has q^2+q+1 or $q+1$ conics of $\mathcal{N}(\mathcal{C})$ through it depending on whether $u \in S(\mathcal{C})$ or not, then

$$m(g) = n(q^2+q) + (|g\mathcal{C}| - n)q = q^2 n + q|g\mathcal{C}|.$$

Also, each conic $v\mathcal{C} \neq g\mathcal{C}$ is in a unique pencil P_r, where r is the line joining g and v. Hence

$$m(g) = q \sum_{r \text{ on } g} \alpha_r = q^2 n + q|g\mathcal{C}|,$$

where α_r is the number of points common to every conic of P_r. Thus, dividing by q and using Lemma 4.4(3) we obtain

$$\begin{aligned} \sum_{r \text{ on } g} \alpha_r &= qn + |g\mathcal{C}| \\ &= \sum_{r \text{ on } g} (y_r - z_r) + (q+1), \end{aligned}$$

where y_r and z_r are the numbers of real and imaginary line-pairs in the pencil P_r. Then

$$\begin{aligned} g \notin \mathcal{C} &\Rightarrow |g\mathcal{C}| = q+1 \\ &\Rightarrow \sum_{r \text{ on } g} (y_r - z_r) = qn \\ &\Rightarrow \sum_{r \text{ on } g} (y_r + z_r) = |\mathcal{C}| = qn + 2 \sum_{r \text{ on } g} z_r \\ &\Rightarrow |\mathcal{C}| = qn + 2z(\mathcal{C}). \end{aligned}$$

One can also check that if $g\mathcal{C}$ is a real or imaginary line-pair we still get the same formula for $|\mathcal{C}|$.

Next we consider the properties of nets of conics such that every point of the plane is the nucleus of a unique conic of the net. We have seen that this study is equivalent to that of the cubic curves in the plane which have $a \neq 0$. The set of points of the cubic corresponds to those points of the plane for which the conic with that nucleus is degenerate. If the number of degenerate conics of the net of the line-pair type is y and the number of imaginary line-pair type is z then the number of points on the corresponding cubic is clearly $y+z$. The possible types of pencils of conics contained in the net are given by the pencils with no repeated lines in Tables 1 and 2 above. These are: $(a), (c), (d), (f), (h'), (h''), (i), (j)$ and (2). The net contains a pencil of type (2) if and only if the cubic curve contains a line and is therefore degenerate. So we consider for the moment only those nets containing no pencils of type (2).

Theorem 4.6. *Suppose that $\mathcal{C}$ is non-singular and that it corresponds to a net $\mathcal{N}(\mathcal{C})$ of conics. Let the number of pencils of the net of type (a) be a, the number of type (b) be b, etc. Also let $y = y(\mathcal{C})$. (This is equal to $z(\mathcal{C})$ since $n = 0$, by Theorem 4.5.) Then the following equations are satisfied:*

$$\begin{aligned} a &= \binom{y}{2}, \\ c &= y(q+1-y), \\ d &= y, \\ f &= q^2+q+1+(4y^2-6qy-6y+2h')/3, \\ h'' &= y(q-y), \\ i &= y-h', \\ j &= (y(y-3)+2h')/6. \end{aligned}$$

Proof. We refer closely to Table 1 of pencils containing non-degenerate conics above. Note that the set of points p of $\mathcal{C}$ such that $p\mathcal{C}$ is an imaginary line-pair, is a z-arc — it is a set of $z = y(\mathcal{C})$ points such that no three are collinear. We can see this from the z-column in Table 1, because there are entries of only 0, 1, or 2 there. Call any point of this z-arc a z-point and the remaining y points on $\mathcal{C}$ y-points.

Then we see that any chord of the z-arc is a line l corresponding to the pencil P_l of type (a). Hence $a = \binom{y}{2}$.

Next, any line corresponding to a pencil of type (d), is the tangent to $\mathcal{C}$ at a z-point. Thus $d = y$.

Then only remaining lines that intersect the z-arc are the lines of type (c), which intersect in just one point. Since there are $y-1$ chords, and a unique tangent to $\mathcal{C}$ through each of these points, there remain $q+1-y$ lines of type (c) through each z-point. Thus $c = y(q+1-y)$.

h' is clearly the number of inflections on $\mathcal{C}$, because a line of this type intersects $\mathcal{C}$ triply. The remaining tangents at y-points are lines of type (i), so that we obtain the equation $i = y - h'$.

To obtain the value of j we count the number of unordered pairs of points of type y on lines of π. Thus

$$\binom{y}{2} = 3j + i \implies j = \left[(y^2-y)/2 - y + h'\right]/3$$

which gives the equation for j.

To calculate h'' we count the number of flags of points of type y on lines of π. Thus

$$\begin{aligned} &yq + y = a + d + h' + h'' + 2i + 3j \\ &\Rightarrow h'' = (yq+y) - (y^2-y)/2 - y - h' - 2(y-h') - (y^2-3y+2h')/2 \end{aligned}$$

which gives the equation for h''.

Finally, the total number of lines of π is $q^2+q+1 = a+c+d+f+h'+h''+i+j$. From this we obtain the formula for f.

Theorem 4.7. *The number of points on a $\mathcal{C}(A,a)$ of π is odd if $a=0$, or even if $a \neq 0$. Thus the parity of the number of points is determined by having an $x_0x_1x_2$ term or not.*

Proof. Every plane cubic curve $\mathcal{C}(A,a)$ belongs to one of the following cases:

(1) *Degenerate*

We can list all the degenerate cubics and check directly that the theorem holds. Note that there is really no need to list those degenerate cubics with $a \neq 0$, since they are covered by case (3) below.

(2) $\mathcal{C}(A,0)$ *non-singular*

$\mathcal{C}(A,0)$ is the set of absolute points of the correlation (or duality) $x \mapsto Ax^2$. From the paper by Ball [**1, Theorem 2.1**] it follows that every correlation of π has an odd number of absolute points, since 2 divides the order q of π.

(3) $\mathcal{C}(A,a)$, $a \neq 0$

In this case Theorem 4.5 shows that the cubic has an even number of points, since q is even.

Note that there is no case with $\mathcal{C}(A,0)$ singular and non-degenerate, since

$$\begin{aligned}\mathcal{C}(A,0)\text{ singular } &\Longrightarrow |A|=0\\ &\Longrightarrow Ax^2=0 \text{ for some point } x\in\pi\\ &\Longrightarrow \text{the line } Ax^2 \subseteq \mathcal{C}.\end{aligned}$$

Observation 4.8. *It was known by L.E. Dickson that the only cubic curves with no real points in $PG(2,q)$, (q even or odd), are those that are made up of three imaginary lines of a triangle, that are conjugate over the cubic extension of $GF(q)$. In our case of q even, we see that such a cubic has $a \neq 0$ (as it has an even number of points). Also, we substitute $y=h'=0$ in the equations of Theorem 4.6 to see that every line of $PG(2,q)$ is the set of nuclei of a pencil of conics of type (f). An alternative is to note that pencils of type (f) always correspond to external lines to the cubic curve. The quadratic mapping $x \mapsto Cx$ is in this case a bijective Cremona transformation from the points to the lines of $PG(2,q)$. Also, every conic of the net of conics of the cubic is non-singular. Every net of conics with this property comes from such a cubic with no real points.*

5. Examples

Example 5.1. *The non-conic oval of PG(2,16)*

Lunelli and Sce discovered by computer that there is an oval (or 18-arc) of $PG(2,16)$, that does not contain a conic. There are only two types of 18-arcs in $PG(2,16)$: the conic plus nucleus, and this unusual oval; see [**16**] and [**22**]. Here we shall show that it can be given very simply by two cubic curves in a syzygetic pencil. See [**12**], [**13**] and [**24**] for the theory of ovals in $PG(2,q)$.

Consider the cubic $\mathcal{C}(I,\delta)$. Then its tangent curve $\mathcal{C}' = \mathcal{C}(I,\delta^2)^t$, while $\mathcal{C}'' = \mathcal{C}(I,\delta^4)$. Thus $\Delta(\mathcal{C}) = det(\delta^3+1)I = (\delta^3+1)^3$. $\mathcal{C}$ is non-singular if $\Delta \neq 0$ and so we assume that

$$\delta \in GF(16) \setminus GF(4).$$

Certainly $\mathcal{C}$ and $\mathcal{C}''$ are two distinct non-singular cubics. It is easy to check that the set of inflection points on both curves is just the curve $\mathcal{C} \cap \mathcal{C}'' = \mathcal{C}(I,0)$, which is contained in the subplane $PG(2,4)$, and that there is the full set of nine inflections forming the configuration $AG(2,3)$. Both $\mathcal{C}$ and $\mathcal{C}''$ have 18 points in $PG(2,16)$, so the subgroup of index 2 in the group of each curve is the set of inflections (isomorphic to $Z_3 \times Z_3$). The complement of this subgroup in each curve is therefore a 9-arc. It can be checked that the Lunelli-Sce oval is given by the symmetric difference of the two cubics $\mathcal{C}$ and $\mathcal{C}''$.

This representation makes it easy to construct the automorphism group of the oval. Clearly the automorphic collineation corresponding to taking fourth powers of elements of $GF(16)$ is an automorphism of the oval. Also, the matrices

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & b+1 \end{pmatrix},$$

where $b \in GF(4)\backslash GF(2)$, generate a group of order 18 transitive on the points of each 9-arc. Thus the all collineations of $PG(2,16)$ given above generate a group of order 36 which is transitive on the 18 points of the oval. Note that each of the automorphisms of the oval fixes $\mathcal{C}(I,0)$, and hence also fixes the $PG(2,4)$ that contains these inflections.

Example 5.2. *Deuring's normal form for a cubic*

In [**6**], Deuring gave the following normal form for an affine cubic curve $\mathcal{C}$ with j-invariant ($j \neq 0$):

$$y^2 - y = jx^2 + (jx)^{-1}.$$

Suppose we homogenise this and substitute $\delta = j^{-1}$. Thus

$$\delta^{-1}x^3 + xy^2 + \delta z^3 + xyz = 0.$$

Then we see that

$$\mathcal{C} = \mathcal{C}(A,1), \text{ where } A = \begin{pmatrix} \delta^{-1} & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \delta \end{pmatrix}, \text{ so that}$$

$$A' = \begin{pmatrix} 0 & 0 & 1 \\ \delta & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \text{ and } A'' = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & \delta \\ 1 & \delta & 0 \end{pmatrix}$$

$$\Longrightarrow \Delta = det(A + A'') = det \begin{pmatrix} \delta^{-1} & 0 & 0 \\ 0 & 0 & \delta \\ 1 & \delta & \delta \end{pmatrix} = \delta.$$

Deuring's normal form for $j = 0$ was:

$$y^2 - y = x^3, \text{ or equivalently } x^3 + y^2z + yz^2 = 0.$$

This corresponds to the cubic $\mathcal{C}(A, 0)$, where

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

If we wanted to find the syzygetic pencil formed by this $\mathcal{C}(A, 0)$, we refer to Theorem 3.14 and find that a Hessian curve is $\mathcal{C}(ABA, |A|)$, where

$$B = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Since $ABA = B$, all the inflection points of $\mathcal{C}(A, 0)$ lie on the Hessian $\mathcal{C}(B, 1)$: $xy^2 + xz^2 + xyz = 0$. This happens to be one of the four Maclaurin triangles of the syzygetic pencil. The line $x = 0$ intersects $\mathcal{C}(A, 0)$ in the three points

$$(0, 1, 0), (0, 0, 1), (0, 1, 1).$$

Thus these points are all inflections of Deuring's normal form.

Exercise 5.3. *Prove that $\mathcal{C} = \mathcal{C}''$ if and only if $\mathcal{C}$ is a triangle.*

6. Some Further Problems

We have obtained some results, especially about syzygetic pencils of cubic curves in characteristic 2, that lead naturally to further problems.

(1) What are the formulae for fields of characteristic 0 and 3 corresponding to the syzygies of Theorem 3.10? Generalize the formulas for curves of any order and any characteristic.

(2) Do there exist other ovals of $PG(2, q)$, $q = 2^h$, that are partially made up by the arc contained in a cubic curve? Note that q cannot be too large, by results in [**21**] and [**30**].

(3) Prove that 1 is the average number of inflections of a non-singular cubic of $PG(2, q)$ with fixed j-invariant, or "of the same type". Referring to [**19, Table 11.22, pp. 314–315**] one sees that

$$\sum n/o = 1,$$

for cubics of the same type in each row.

(4) Prove that for any field of characteristic not equal to three, the number of inflections of a non-singular plane cubic is equal to $2r - t + 1$, where r is the number of real triangles and t is the number of completely imaginary triangles (made up of three imaginary lines with no real points), in the syzygetic pencil.

References

1. R.W. Ball, *Dualities of finite projective planes*, Duke Math. J. **15** (1948), 929–940.
2. A.A. Bruen and J.W.P. Hirschfeld, *Intersections in projective space, II. Pencils of quadric surfaces*, European J. Combin. **9** (1988), 275–286.
3. A.D. Campbell, *Plane cubic curves in the Galois fields of order* 2^n*'*, Ann. of Math. **27** (1926), 395–406.
4. M. Cicchese, *Sulle cubiche di un piano di Galois*, Rend. Mat. Pura ed Appl **24** (1965), 291–330.
5. ______, *Sulle cubiche di un piano lineare* $S_{2,q}$ *con* $q \equiv 1$ *(mod 3)*, Rend. Mat **4** (1971), 249–283.
6. M. Deuring, *Invarianten und Normalformen elliptischer Funktionkörper*, Math. Z. **47** (1940), 47–56.
7. L.E. Dickson, *On the canonical forms and automorphs of ternary cubic forms*, Amer. J. Math **30** (1908), 117–128.
8. ______, *Invariantive theory of plane cubic curves modulo 2*, Amer. J. Math. **37** (1915), 107–116.
9. F. Enriques and O. Chisini, *Lezioni sulla teoria geometrica delle equazioni e delle funzioni algebraiche*, vol. I & II, Zanichelli, Bologna, 1915.
10. A. Garcia and J.F. Voloch, *Duality for projective curves*, Instituto de matemática pura e aplicada, Série A, Informes de Matemática **085** (1989).
11. D.G. Glynn, *Finite Projective Planes and Related Combinatorial Systems*, Ph.D Thesis, University of Adelaide, South Australia, 1978.
12. ______, *Two new sequences of ovals in finite Desarguesian planes of even order*, Comb. Math. **X** (Adelaide 1982), Lecture Notes in Math. **1036** (1983), 217–229, Springer, Berlin, Heidelberg, New York and Tokyo.
13. ______, *A condition for the existence of ovals in* $PG(2,q)$*,* q *even*, Geometriae Ded. **32** (1989), 247–252.
14. ______, *On the number of points on a hypersurface in* $PG(n,q)$ *and the modular counterparts of Cayley's hyperdeterminants*, submitted for publication.
15. V.D. Goppa, *Algebraico-geometric codes*, Math. USSR Izvestiya **21** (1983), 75–91.
16. M. Hall, Jr., *Ovals in the Desarguesian plane of order 16*, Ann. di Mat. Pura ed Appl. **102** (1975), 159–176.
17. R.W. Hartley, *Determination of the ternary collineation groups whose coefficients lie in the* $GF(2^n)$, Ann. Math. (2) **2** (1926), 140–158.
18. R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Maths, 52, Springer, New York, Heidelberg, Berlin, 1983.
19. J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford Uni. Press, Oxford, 1979.
20. ______, *Linear codes and algebraic curves*, Geometrical Combinatorics §4, (eds. F.C. Holroyd & R.J. Wilson), Pitman, Research Notes in Mathematics **114** (1984), 35–53.
21. J.W.P. Hirschfeld and J.F. Voloch, *The characterization of elliptic curves over finite fields*, J. Austral. Math. Soc. (Series A) **45** (1988), 275–286.

22. L. Lunelli and M. Sce, *k-archi completi nei piani proiettivi desarguesiani di rango 8 e 16*, Politecnico Milano, Centro Calcol. Numerici (1958), 1–15.

23. R. Schoof, *Non-singular plane cubic curves over finite fields*, PhD thesis, Uni. of Amsterdam, 1985.

24. B. Segre, *Sulle ovali nei piani lineari finiti*, Atti Accad. Naz. Lincei Rend **17** (1954), 1–2.

25. ______, *Intorno alla geometria sopra un campo di caratteristica due*, Istanbul Uni. Fen Fakueltesi Mecmnasi, Seri A Sirfi ve Talbiki Matematik **21** (1956), 97–123.

26. ______, *Le geometrie di Galois*, Ann. Mat. Pura Appl **48** (1959), 1–97.

27. ______, *Arithmetische Eigenschaften von Galois-Räumen. I*, Math. Annalen **154** (1964), 195–256.

28. J.G. Semple and L. Roth, *Introduction to Algebraic Geometry*, Clarendon Press, Oxford, 1985.

29. J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Maths, 106, Springer, New York, Berlin, Heidelberg, Tokyo, 1986.

30. J.F. Voloch, *On the completeness of certain plane arcs*, European J. Combinatorics **8** (1987), 453–456.

31. ______, *A note on elliptic curves over finite fields*, Bull. Soc. math. France **116** (1988), 455–458.

32. ______, *On the completeness of certain plane arcs II*, European J. Combinatorics **11** (1990), 491–496.

33. W.C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. **2** (1969), 521–560.

(Received 10/5/96)