Canonically inherited arcs in Moulton planes of odd order

Vito Abatangelo* Bambina Larato

Abstract

In this paper large complete arcs in a Moulton plane of odd order are investigated using techniques from finite geometry, number theory and algebraic geometry.

Keywords: arc, oval, Moulton plane, algebraic curve, finite field

MSC 2000: 51E21, 51E15

1. Introduction

Every finite affine plane $\mathcal{A}$ whose order n is a power of a prime p may be thought of as an alteration of the Desarguesian plane $\mathsf{AG}(2, n)$ coordinatized over the finite field $\mathsf{GF}(n)$: points and lines of $\mathcal{A}$ are identified with points and lines of $\mathsf{AG}(2, n)$ but certain (possibly all) point-line incidences in $\mathsf{AG}(2, n)$ are to be changed to define the point-line incidences in $\mathcal{A}$.

Let $\mathcal{C}_2$ be an ellipse in $\mathsf{AG}(2, n)$, that is a non-singular elliptic conic. It is well known that the set Ω consisting of all points of $\mathcal{C}_2$ is an arc, actually it is an oval in the projective closure $\mathsf{PG}(2, n)$ of $\mathsf{AG}(2, n)$. When not too many point-line incidences of $\mathsf{AG}(2, n)$ have been changed to obtain $\mathcal{A}$ and the alterations do not affect Ω dramatically, it may happen that Ω is an oval in the projective closure of $\mathcal{A}$, or a large piece of Ω may be an arc in $\mathcal{A}$.

This was first observed by Korchmáros who exhibited examples in the Hall plane and in the Moulton plane, see [9, 10]. Later on, such "inherited ovals

*Both authors are supported by the Italian Ministry MURST, Strutture geometriche, combinatoria e loro applicazioni, PRIN 2006-2007

and arcs" of the Hall and Moulton planes have been investigated by several authors, namely Glynn and Steinke [2], Korchmáros [11], Honold and Landjev [6], Menichetti [12], O'Keefe and Pascasio [13], O'Keefe, Pascasio and Penttila [14], Rinaldi [15], Rinaldi and Zironi [16], Szőnyi [18, 19, 20], and recently by the authors [1].

The new results in the present paper concern inherited arcs in a Moulton plane of odd order. Before stating and discussing them we need to recall the construction of the Moulton plane of odd order $n = q^2$ which is in turn the dual plane of the Hall plane of the same order. The quasifield coordinatizing the Moulton plane arises from the finite field $\mathsf{GF}(q^2)$ by altering the multiplication in the following manner.

Let $(\mathsf{GF}(q), +, \cdot)$ be the subfield of $\mathsf{GF}(q^2)$ of order q. Then $\mathsf{GF}(q^2)$ can be viewed as the quadratic extension of $\mathsf{GF}(q)$ with respect to a polynomial $X^2 - \tau$ irreducible over $\mathsf{GF}(q)$. Choose $i \in \mathsf{GF}(q^2)$ for which $i^2 = \tau$, and write each element $x \in \mathsf{GF}(q^2)$ as $x = \xi + i\eta$ with $\xi, \eta \in \mathsf{GF}(q)$. Then the norm of x is defined to be $\|x\| = \xi^2 - \tau\eta^2$ and $\|x\| = x \cdot x^q = (\xi + i\eta)^{q+1}$. For a non-zero element $t \in \mathsf{GF}(q)$, a new "multiplication" $\circ$ is defined as follows:

$$a \circ b = \begin{cases} a \cdot b & \text{if } \|b\| \neq t\,; \\ a^q \cdot b & \text{if } \|b\| = t\,. \end{cases}$$

With this multiplication, $(\mathsf{GF}(q^2), +, \circ)$ is a pre-quasifield which is a quasifield for $t \neq 1$. According to [8, Section 5.6], every pre-quasifield coordinatizes a translation plane. In our case this translation plane is the affine Hall plane of order q^2, and its dual plane is the affine Moulton plane of order q^2. Affine Hall planes of the same order are isomorphic, see [7, Chapter X.4], and this holds true for affine Moulton planes.

The Moulton plane $M_t(q^2)$ has the same points and the same vertical lines as $\mathsf{AG}(2, q^2)$, whereas its non-vertical lines are the graphs of the functions $y = m \circ x + b$ with $m, b \in \mathsf{GF}(q^2)$. In other words, $M_t(q^2)$ arises from $\mathsf{AG}(2, q^2)$ by altering a few point-line incidences, namely those between points $P = (x, y)$ with $\|x\| = t$ and lines of equation $y = mx + b$ with $m \in \mathsf{GF}(q^2) \setminus \mathsf{GF}(q)$. Adding to $M_t(q^2)$ its points at infinity in the usual way produces a projective plane, called the projective closure (or completion) of $M_t(q^2)$.

From previous work it has emerged that a good choice to produce large arcs in $M_t(q^2)$ (even ovals in the projective closure of $M_t(q^2)$) consists in taking $\mathcal{C}_2$ in its canonical form, that is, $\mathcal{C}_2$ has equation

$$X^2 - sY^2 = 1 \tag{1}$$

where s is a non-square element of $\mathsf{GF}(q^2)$.

ACADEMIA PRESS
UNIVERSITEIT GENT

Let Ω^* denote the set of all points P of Ω that avoid all the point-line incidence alterations at P. In other words, $P = (x, y) \in \Omega^*$ if and only if $P \in \Omega$ and $\|x\| \neq t$. Obviously, Ω^* is an arc in $M_t(q^2)$ and is called a "canonically inherited arc".

In Section 2, the following result is proven.

Theorem 1.1. *A canonically inherited k-arc is a complete k-arc in the projective closure of $M_t(q^2)$.*

Theorem 1.1 leads to investigate the spectrum consisting of all integers k such that a canonically inherited complete k-arc in $M_t(q^2)$ exists for some t. Since the equation $\|x\| = t$ has at most $q+1$ solutions, and for each x we have at most two solutions y from (1), the combinatorial bound for the lower limit of the spectrum is $q^2+1-2(q+1) = q^2-2q-1$. This bound is achieved, see below Theorem 1.2 case (iii).

For a thorough investigation, we need an algebraic characterization of the integers in the spectrum. This is done in Section 3 by showing that k is in the spectrum if and only if an affine algebraic curve Γ in AG$(4,q)$ given by explicit equations has k points in AG$(4,q)$.

Unfortunately, Γ does not belong to the meagre family of curves defined over GF(q) whose number of GF(q)-rational points N_q is known or may be computed by standard method depending on the zeta function of the curve. Nevertheless, since Γ has low genus $g \leq 5$, the Hasse-Weil theorem provides good lower and upper bounds for N_q, namely $q+1-10\sqrt{q} \leq N_q \leq q+1+10\sqrt{q}$. This bound is an ingredient in the proof of our main result.

Theorem 1.2. *A canonically inherited k-arc is a complete k-arc in the projective closure of $M_t(q^2)$ such that*

(i) $k = q^2+1$ *for* $t=-1$ *and* $q \equiv 1 \pmod 4$*;*

(ii) $k = q^2-1$ *for* $t=1$ *and* $q \equiv 3 \pmod 4$*;*

(iii) $k = q^2-2q-1$ *for either* $t=-1$ *and* $q \equiv 3 \pmod 4$ *or* $t=1$ *and* $q \equiv 1 \pmod 4$*;*

(iv) $q^2-q-10\sqrt{q}-2 \leq k \leq q^2-q+10\sqrt{q}+6$, *for* $t \neq \pm 1$ *and* $q \equiv 1 \pmod 4$*;*

(v) $q^2-q-10\sqrt{q}-4 \leq k \leq q^2-q+10\sqrt{q}+8$, *for* $t \neq \pm 1$ *and* $q \equiv 3 \pmod 4$.

Backgrounds on algebraic curves over finite fields are found in [4], see also [3, 5, 17]. For finite projective planes, see [7].

2. Completeness of canonically inherited arcs

In this section Theorem 1.1 is proven. For this purpose, notation and terminology from the introduction are maintained.

An essential tool in the proof is an "ad hoc" representation of the lines of $M_t(q^2)$ through a point P, that is, the pencil with centre P.

Lemma 2.1. *Let $\ell_0, \ldots, \ell_{q^2}$ be the lines in $\mathsf{AG}(2, q^2)$ which constitute the pencil $\mathcal{L}(P_0)$ in $M_t(q^2)$ with centre $P_0 = (x_0, y_0)$. If $\|x_0\| \neq t$, then $\mathcal{L}(P_0)$ is also the pencil in $\mathsf{AG}(2, q^2)$ with the same centre P_0. If $\|x_0\| = t$, then $\mathcal{L}(P_0)$ consists of lines of a Baer subplane in $\mathsf{PG}(2, q^2)$; more precisely, $\ell_0, \ldots, \ell_{q^2}$ plus the q vertical lines $X = c$, with $\|c\| = t$ and $c \neq x_0$, are the lines of a Baer subplane of $\mathsf{PG}(2, q^2)$.*

Proof. The assertion can be proven by direct computation. Alternatively, it can be deduced from the usual representation of the Hall plane as the derived plane of $\mathsf{AG}(2, q^2)$. In fact, a line of a derived plane is either a line or an affine Baer subplane of $\mathsf{AG}(2, q^2)$, and dualizing we obtain our assertion since the dual of the projective closure of the Hall plane is the projective closure of $M_t(q^2)$. □

In the proof of Theorem 1.1, the above lemma is combined with the following technical result of independent interest.

In $\mathsf{PG}(2, q^2)$, let $\mathcal{C}$ be a non-singular conic, and $\mathcal{B}$ a Baer subplane. For a point $Y \in \mathcal{B}$, let $\mathcal{M}(Y)$ be the pencil of lines in $\mathcal{B}$ with centre Y. These lines cover $(q+1)q^2 + 1$ points in $\mathsf{PG}(2, q^2)$. At most $2(q+1)$ points of $\mathcal{C}$ may be covered in this way. Let m denote the number of such points. Actually, we are interested in the set Δ of uncovered points in $\mathcal{C}$. Set $n = |\Delta|$. Then $n + m = q^2 + 1$ and $q^2 - 2q - 1 \leq n \leq q^2 + 1$.

Lemma 2.2. *Let $q \geq 5$. Some line in $\mathcal{B}$ has two common points with Δ.*

Proof. Take a point $T \in \Delta$. Since $T \notin \mathcal{B}$, there is a unique line ℓ_T of $\mathcal{B}$ through T. Obviously, ℓ_T does not belong to $\mathcal{M}(Y)$. It may be that ℓ_T is the tangent to $\mathcal{C}$ at T, but this may occur at most $q+1$ times when T ranges over Δ. Such a bound $q+1$ is obtained by dualizing the well known fact that a Baer subplane and a non-singular conic have at most $q+1$ common points. Discarding the points $T \in \Delta$ with ℓ_T tangent to $\mathcal{C}$, we obtain the set Δ' such that

$$\ell_T \cap \mathcal{C} = \{T, T'\}, \text{ with } T \in \Delta', \text{ and } T \neq T'.$$

Set $n' = |\Delta'|$. Then $n' \geq n - (q+1) = q^2 + 1 - m - (q+1) = q^2 - m - q$.

Every point $Q \in \mathcal{C}$ covered by $\mathcal{M}(Y)$, that is every point $Q \in \mathcal{C} \setminus \Delta$, lies on at most $q + 1 - (m-1) = q - m + 2$ lines ℓ_T with $T \in \Delta'$. The total number of lines ℓ_T which may be obtained in this way does not exceed $m(q - m + 2)$.

To prove Lemma 2.2 we may assume on the contrary that $T' \in \mathcal{C} \setminus \Delta$ for every $T \in \Delta'$. Then $n' \leq m(q-m+2)$. Hence

$$q^2 - m - q \leq m(q-m+2)\,. \tag{2}$$

Since m is a non-negative integer, this only holds for $q < 5$. □

We are now in a position to prove Theorem 1.1.

From Lemmas 2.1 and 2.2 we deduce that no point $P = (x, y)$ with $\|x\| = t$ can be added to Ω^* to obtain a larger arc in $M_t(q^2)$. For this purpose, let $\mathsf{PG}(2, q^2)$ be the projective closure of $\mathsf{AG}(2, q^2)$, and define Y_∞ to be Y. According to Lemma 2.1, define $\mathcal{B}$ to be the Baer subplane of $\mathsf{PG}(2, q^2)$ whose lines are those of the pencil $\mathcal{L}(P)$ plus the lines $X = c$ with $c \neq x_0$ and the line at infinity. Now Lemma 2.2 shows that in $M_t(q^2)$, a chord of Ω^* passes through P. This proves the assertion.

This holds true for the case when $\|x\| \neq t$. In fact, in $\mathsf{AG}(2, q^2)$ through P there are at least $(q^2-1)/2$ secants to $\mathcal{C}_2$, and hence at least $N = (q^2-1)/2 - m$ secants to Ω^*. Here $m \leq 2(q+1)$ and, for $q = 5$, $m \leq 10$. So $N > 0$ and the assertion follows.

It may be noted that the same argument also works when P is a point at infinity.

3. Spectrum of sizes of canonically inherited arcs in the Moulton plane

The combinatorial bound for the size of a canonically inherited arc Ω^* is

$$q^2 - 2q - 1 \leq |\Omega^*| \leq q^2 + 1\,. \tag{3}$$

To find the exact value of $|\Omega^*|$ in the Moulton plane $M_t(q^2)$ we need to count the solutions of the system of equations

$$\begin{cases} x^2 - sy^2 = 1 \\ \qquad \|x\| = t\,. \end{cases} \tag{4}$$

In fact, if (4) has m solutions (x, y), then Ω^* consists of q^2+1-m points showing that q^2+1-m belongs to the spectrum.

The idea is to rewrite (4) in terms of equations over the subfield $\mathsf{GF}(q)$ of $\mathsf{GF}(q^2)$. As in the preceding Sections, $\mathsf{GF}(q^2)$ is assumed to be the algebraic extension of $\mathrm{GF}(q)$ with respect to the irreducible polynomial $X^2 - \tau$ with $\tau \in \mathrm{GF}(q)$, and $i \in \mathrm{GF}(q^2)$ denotes a root of $X^2 - \tau$, so $i^2 = \tau$. Let

$$x = x_1 + ix_2\,, \quad y = y_1 + iy_2\,, \quad s = s_1 + is_2$$

with $x_i, y_i, s_i \in \mathrm{GF}(q)$ for $i = 1, 2$. Now, (4) becomes

$$\begin{cases} (x_1 + ix_2)^{q+1} = t \\ (x_1 + ix_2)^2 - (s_1 + is_2)(y_1 + iy_2)^2 = 1\,. \end{cases}$$

Since $\|x\| = t$ means that $x^{q+1} = x_1^2 - \tau x_2^2 = t$, we obtain the system of equations

$$\begin{cases} x_1^2 - \tau x_2^2 = t \\ x_1^2 + \tau x_2^2 - 1 = s_1 y_1^2 + 2\tau s_2 y_1 y_2 + \tau s_1 y_2^2 \\ 2x_1 x_2 = s_2 y_1^2 + 2 s_1 y_1 y_2 + \tau s_2 y_2^2 \end{cases}$$

which is equivalent to the system of equations

$$\begin{cases} 2x_1^2 = s_1 y_1^2 + 2\tau s_2 y_1 y_2 + \tau s_1 y_2^2 + 1 + t \\ 2\tau x_2^2 = s_1 y_1^2 + 2\tau s_2 y_1 y_2 + \tau s_1 y_2^2 + 1 - t \\ 2x_1 x_2 = s_2 y_1^2 + 2 s_1 y_1 y_2 + \tau s_2 y_2^2\,. \end{cases} \tag{5}$$

Let K be the algebraic closure of $\mathrm{GF}(q)$ containing $\mathrm{GF}(q^2)$, and $\mathrm{AG}(4, K)$ the four-dimensional affine space over $\mathrm{GF}(q)$ with coordinates (x_1, x_2, y_1, y_2). Then the equations in (5) define an affine algebraic set Γ in $\mathrm{AG}(4, K)$ defined over $\mathrm{GF}(q)$. From the above discussion we have the following lemma.

Lemma 3.1. *The number of solutions of (4) is equal to the number of points of Γ whose coordinates lie over $\mathrm{GF}(q)$.*

So we are led to investigate Γ and its points in $\mathrm{AG}(4, q)$.

The equation

$$(s_1^2 - \tau s_2^2)(y_1^2 - \tau y_2^2)^2 + 2(s_1 y_1^2 + 2\tau s_2 y_1 y_2 + \tau s_1 y_2^2) + (1 - t^2) = 0 \tag{6}$$

together with the first equation in (5) define a (possibly reducible and singular) affine algebraic curve Γ_1 in $\mathrm{AG}(3, K)$ equipped with affine coordinates (x_1, y_1, y_2). Similarly, (6) together with the second equation in (5) define Γ_2 in $\mathrm{AG}(3, K)$ equipped with affine coordinates (x_2, y_1, y_2).

To investigate Γ_1 and Γ_2, some results on the absolutely irreducible plane quartic curve defined by (6) are needed.

Lemma 3.2. *Let $\mathcal{C}$ be the projective plane curve with homogeneous equation $F(X,Y,Z)=0$ with*

$$F(X,Y,Z)=(s_1^2-\tau s_2^2)(X^2-\tau Y^2)^2+2(s_1X^2+2\tau s_2XY+\tau s_1Y^2)Z^2 \\ +(1-t^2)Z^4\,.$$

(i) *$\mathcal{C}$ is absolutely irreducible.*

(ii) *For $t=\pm1$, $\mathcal{C}$ has three singular points, namely the origin and the points at infinity $T=(i,1,0)$ and $U=(-i,1,0)$. They are nodes, and the two places centred at the origin are defined over $\mathsf{GF}(q)$ or $\mathsf{GF}(q^2)$ according as $q\equiv1 \pmod 4$ or $q\equiv 3 \pmod 4$. Furthermore, $\mathcal{C}$ has genus 0.*

(iii) *For $t\neq\pm1$, $\mathcal{C}$ has genus 1 and two singular points $T=(i,1,0)$ and $U=(-i,1,0)$. Both are nodes and defined over $\mathsf{GF}(q^2)$.*

(iv) *The linear collineation $\psi:(X,Y,Z)\to(-X,-Y,Z)$ preserves $\mathcal{C}$ and fixes both T and U.*

Proof. After computing the partial derivatives of the above homogeneous polynomial $F=F(X,Y,Z)$, we find the singular points of $\mathcal{C}$ solving the system of equations

$$\begin{aligned} F_X&=4(s_1^2-\tau s_2^2)X(X^2-\tau Y^2)+4(s_1X+\tau s_2Y)Z^2 &&=0\,;\\ F_Y&=-4\tau(s_1^2-\tau s_2^2)Y(X^2-\tau Y^2)+4\tau(s_2X+s_1Y)Z^2 &&=0\,;\\ F_Z&=4(s_1X^2+2\tau s_2XY+\tau s_1Y^2)Z+4(1-t^2)Z^3 &&=0\,. \end{aligned}$$

For $Z=0$ the system has two solutions, namely $(i,1,0)$ and $(-i,1,0)$. The corresponding points $T=(i,1,0)$ and $U=(-i,1,0)$ are double points of $\mathcal{C}$, and the tangents to $\mathcal{C}$ at these points are the lines

$$\ell_T^+: X-iY+\sqrt{\frac{s_1+s_2i}{s_1^2-\tau s_2^2}}=0\,;\qquad \ell_T^-: X-iY-\sqrt{\frac{s_1+s_2i}{s_1^2-\tau s_2^2}}=0\,;$$

$$\ell_U^+: X+iY+\sqrt{\frac{s_1-s_2i}{s_1^2-\tau s_2^2}}=0\,;\qquad \ell_U^-: X+iY-\sqrt{\frac{s_1-s_2i}{s_1^2-\tau s_2^2}}=0\,.$$

For $t=\pm1$, the origin $O=(0,0,1)$ is also a double point and the tangents to $\mathcal{C}$ at O are

$$Y=\left(\tau s_2\pm\sqrt{-\tau(s_1^2-\tau s_2^2)}\right)X\,.$$

In particular, the tangents are defined over $\mathsf{GF}(q)$ or $\mathsf{GF}(q^2)$ according as -1 is a square or a non-square element in $\mathsf{GF}(q)$. Assume on the contrary that $\mathcal{C}$ has a further singular point P. Since the line ℓ_∞ of equation $Z=0$ is not a component of $\mathcal{C}$, P is not on ℓ_∞. So, affine coordinates with respect to the infinite line ℓ_∞ are used, and $P = (x, y)$ is assumed.

Since (x, y) is a common zero of F_X and F_Y, we have that (x, y) is also a zero of $\tau Y F_X - X F_Y$. Hence

$$(x^2 - \tau y^2)(2xy(s_1^2 - \tau s_2^2)(x^2 - \tau y^2) - s_2) = 0\,. \tag{7}$$

Similarly, from $\tau Y F_X + X F_Y$,

$$2s_1xy + s_2(x^2 + \tau y^2) = 0\,. \tag{8}$$

Also, from $F(x, y, 1) = 0$ and $F_Z(x, y, 1) = 0$,

$$(s_1^2 - \tau s_2^2)(x^2 - \tau y^2)^2 - (1 - t^2) = 0\,. \tag{9}$$

If $x^2 - \tau y^2 = 0$, then (9) implies that $t = \pm 1$. Further, $F_X(x, y, 1) = 0$ reads $s_1x + \tau s_2 y = 0$, and $F_Y(x, y, 1) = 0$ reads $s_2x + s_1y = 0$. Since $s_1^2 - \tau s_2^2 \neq 0$, this implies that $(x, y) = (0, 0)$, a contradiction.

So we may assume that $x^2 - \tau y^2 \neq 0$. Then (7) implies that

$$2xy(s_1^2 - \tau s_2^2)(x^2 - \tau y^2) - s_2 = 0\,. \tag{10}$$

Note that both x and y must be distinct from zero, otherwise $(x, y) = (0, 0)$ by (8) and $t = \pm 1$ by $F(0, 0, 1) = 1 - t^2$. From (10),

$$2xy(s_1^2 - \tau s_2^2)(x^2 - \tau y^2)^2 - s_2(x^2 - \tau y^2) = 0\,. \tag{11}$$

This together with (9) implies that

$$2xy(1 - t^2) = s_2(x^2 - \tau y^2)\,. \tag{12}$$

The sum and the difference of (8) and (12) give after simplification by y and x, respectively:

$$x(1 - t^2 + s_1) = -s_2\tau y\,,$$
$$y(1 - t^2 - s_1) = s_2 x\,.$$

Since $x \neq 0$ and $y \neq 0$, this implies that $(1 - t^2)^2 = s_1^2 - \tau s_2^2$, a contradiction as $s_1^2 - \tau s_2^2$ is a non-square element in $\mathrm{GF}(q)$. This proves that the singular points of $\mathcal{C}$ are those in the statement.

We prove that $\mathcal{C}$ is absolutely irreducible. Let $\mathcal{G}$ be an absolutely irreducible component of $\mathcal{C}$.

If $\mathcal{G}$ is a line, then it is distinct from the infinity line and its infinity point is either U or V. Since $\mathcal{C}$ is defined over $\mathrm{GF}(q)$, the conjugate $\mathcal{G}'$ of $\mathcal{G}$ over $\mathrm{GF}(q)$

ACADEMIA PRESS
UNIVERSITEIT GENT

is also a component of $\mathcal{C}$. Since U and V are conjugate points over $\mathrm{GF}(q)$, it follows that $\mathcal{G} \neq \mathcal{G}'$. Let P be its common point. Then P is a singular point of $\mathcal{C}$ distinct from U and V. Therefore, $t = \pm 1$ and P is the origin. But no line through the origin is a component of $\mathcal{C}$, a contradiction.

If $\mathcal{C}$ is reducible without linear components, then it splits into two absolutely irreducible conics, say $\mathcal{G}_1$ and $\mathcal{G}_2$. Since U and V are nodes, this can only happen when $\mathcal{G}_1$ and $\mathcal{G}_2$ have different tangents at U and V. In particular, $I(U, \mathcal{G}_1 \cap \mathcal{G}_2) = I(V, \mathcal{G}_1 \cap \mathcal{G}_2) = 1$. By Bézout's theorem, $\mathcal{G}_1$ and $\mathcal{G}_2$ have at least one more common point, say P. Since P is a singular point of $\mathcal{C}$, this implies that $t = \pm 1$ and that P is the origin. Since the origin is also a node, $\mathcal{G}_1$ and $\mathcal{G}_2$ have different tangents at the origin. Hence, $I(P, \mathcal{G}_1 \cap \mathcal{G}_2) = 1$. Again, from Bézout's theorem, $\mathcal{G}_1$ and $\mathcal{G}_2$ must have at least one more common point. But such a point would be a singular point of $\mathcal{C}$ distinct from U, V and the origin, a contradiction. $\square$

The number of points of Γ may be computed from the number of points of Γ_1 (or Γ_2) in $\mathrm{AG}(3, q)$.

Lemma 3.3. *Let N, N_1, N_2 denote the number of points with coordinates over $\mathrm{GF}(q)$ lying on Γ, Γ_1, Γ_2, respectively.*

(i) $N = N_1 - 2$ *for* $t \neq \pm 1$ *and* $q \equiv 1 \pmod 4$;

(ii) $N = N_1$ *or* $N = N_1 - 4$ *for* $t \neq \pm 1$ *and* $q \equiv 3 \pmod 4$;

(iii) $N = N_1 - 1$ *for* $t = -1$;

(iv) $N = N_2 + 1$ *for* $t = 1$.

Proof. Let $t \neq 1$. Every point $P = (x_1, x_2, y_1, y_2) \in \mathrm{AG}(4, q)$ of Γ defines a point $P' = (x_1, y_1, y_2) \in \mathrm{AG}(3, q)$ of Γ_1. We show that $x_1 \neq 0$. If $x_1 = 0$, then from the first equation in (5), $s_1 y_1^2 + 2\tau y_1 y_2 + \tau s_1 y_2^2 = -1 - t$. Now, from (6),

$$(s_1^2 - \tau s_2^2)(y_1^2 - \tau y_2^2)^2 = (1 + t)^2 .$$

But this is impossible, since s is a non-square in $\mathrm{GF}(q^2)$, its norm $s_1^2 - \tau s_2^2$ is a non-square in $\mathrm{GF}(q)$. Hence $x_1 \neq 0$. So x_2 is uniquely determined from x_1, y_1, y_2 by the third equation in (5). Thus, distinct points $P \in \mathrm{AG}(4, q)$ of Γ define distinct points $P' \in \mathrm{AG}(3, q)$ of Γ_1. Conversely, let $P' = (x_1, y_1, y_2) \in \mathrm{AG}(3, q)$ be a point of Γ_1. If $x_1 \neq 0$, the third equation in (5) is used to define x_2 and with this definition we have that $P = (x_1, x_2, y_1, y_2) \in \mathrm{AG}(4, q)$ is a point of Γ. If $x_1 = 0$ then x_2 may be defined by the second equation in (5), but then the point $P = (x_1, x_2, y_1, y_2) \in \Gamma$ is in $\mathrm{AG}(4, q^2) \setminus \mathrm{AG}(4, q)$. Points $P' = (0, y_1, y_2) \in$

AG$(3,q)$ of Γ_1 come from the common points $Q = (y_1, y_2) \in$ AG$(2,q)$ of the plane quartic $\mathcal{C}$ in Lemma 3.2 and the conic $\mathcal{D}$ with equation

$$s_1X^2 + 2\tau s_2XY + \tau s_1Y^2 + (1+t) = 0\,.$$

For $t = -1$, we have only one such a common point, namely $Q = (0,0)$. Therefore, assertion (iii) holds.

For $t \neq \pm 1$, $\mathcal{C}$ and $\mathcal{D}$ have four common points. This will be proven later, see Lemma 3.8. The common points are of the form

$$Q_1 = (\xi_1, \eta_1)\,, \quad Q_2 = (-\xi_1, -\eta_1)\,, \quad Q_3 = (\xi_2, \eta_2)\,, \quad Q_4 = (-\xi_2, -\eta_2)\,,$$

with $\xi_1, \xi_2, \eta_1, \eta_2$ defined as in Lemma 3.8. In particular, $\xi_1\xi_2 = c_1\sqrt{-\tau}$ and $\eta_1\eta_2 = c_2\sqrt{-\tau}$ with $c_1, c_2 \in$ GF(q) and $c_1c_2 \neq 0$. Therefore, the number of common points $Q \in$ AG$(2,q)$ of $\mathcal{C}$ and $\mathcal{D}$ is equal to 2 for $q \equiv 1 \pmod 4$ and to 0 or 4 for $q \equiv 3 \pmod 4$. From this, assertions (i) and (ii) follow.

Let $t = 1$. Every point $P = (x_1, x_2, y_1, y_2) \in$ AG$(4,q)$ of Γ defines a point $P' = (x_2, y_1, y_2) \in$ AG$(3,q)$ of Γ_2. We show that $x_2 = 0$ occurs in two cases only, namely when $P_1 = (1,0,0,0)$, $P_2 = (-1,0,0,0)$. To do this, assume on the contrary that $x_2 = 0$. Then from the second equation in (5),

$$s_1y_1^2 + 2\tau y_1y_2 + \tau s_1y_2^2 = t - 1\,.$$

Now, from (6),

$$(s_1^2 - \tau s_2^2)(y_1^2 - \tau y_2^2)^2 = (t-1)^2\,.$$

But this is a contradiction, $s_1^2 - \tau s_2^2$ being a non-square element in GF(q). If $x_2 \neq 0$, x_1 is uniquely determined from x_2, y_1, y_2 by the third equation in (5). So distinct points $P \in$ AG$(4,q)$ of Γ other than P_1, P_2 define distinct points $P' \in$ AG$(3,q)$ of Γ_2. Conversely, let $P' = (x_2, y_1, y_2) \in$ AG$(3,q)$ be a point of Γ_2. If $x_2 \neq 0$, the third equation in (5) is used to define x_1 and with this definition we have that $P = (x_1, x_2, y_1, y_2) \in$ AG$(4,q)$ is a point of Γ. If $x_2 = 0$ then x_1 may be defined by the first equation in (5) yielding $x_1^2 = 1$. But then $-sy^2 = 0$, and hence $y_1 = y_2 = 0$. Therefore, the corresponding points are P_1 and P_2. From this, assertion (iv) follows. $\square$

Now, three cases are investigated separately according as either $t = -1$ or $t = 1$, or $t \neq \pm 1$.

Proposition 3.4. *For $t = -1$, Γ_1 is reducible being split into two absolutely irreducible rational curves both defined over* GF(q) *or* GF(q^2) *according as $q \equiv 3 \pmod 4$ or $q \equiv 1 \pmod 4$. Furthermore, N_1 is equal to either $2q+3$ or 1 according as $q \equiv 3 \pmod 4$ or $q \equiv 1 \pmod 4$.*

Proof. For $t=-1$, Γ_1 is defined by the equations

$$\begin{cases} 2x_1^2 = s_1y_1^2 + 2\tau s_2 y_1 y_2 + \tau s_1 y_2^2\,; \\ (s_1^2-\tau s_2^2)(y_1^2-\tau y_2^2)^2 = -2(s_1y_1^2 + 2\tau s_2 y_1 y_2 + \tau s_1 y_2^2)\,. \end{cases}$$

Eliminating $s_1y_1^2 + 2\tau s_2 y_1 y_2 + \tau s_1 y_2^2$ gives

$$4x_1^2 = -(s_1^2-\tau s_2^2)\,(y_1^2-\tau y_2^2)^2\,.$$

This shows that Γ_1 splits into the two affine curves, namely Γ_1^+ and Γ_1^- defined by (6) together with

$$\begin{aligned} x_1 &= \tfrac{1}{2}\sqrt{-(s_1^2-\tau s_2^2)}\;(y_1^2-\tau y_2^2) \;\text{ and} \\ x_1 &= -\tfrac{1}{2}\sqrt{-(s_1^2-\tau s_2^2)}\;(y_1^2-\tau y_2^2)\,, \end{aligned}$$

respectively. Both Γ_1^+ and Γ_1^- are absolutely irreducible and birationally equivalent to $\mathcal{C}$. In particular, they have genus zero. From Lemma 3.2(i), the origin $O=(0,0,0)$ in $\mathsf{AG}(3,q)$ is a double point for both Γ_1^+ and Γ_1^-.

Actually, P is the centre of two places $\mathcal{P}_1^+$ and $\mathcal{P}_1^-$ of the function field $K(\Gamma_1^+)$. A primitive representation of $\mathcal{P}_1^+$ (and $\mathcal{P}_1^-$) is of the form

$$\begin{cases} y_1 = y_1(\lambda) \\ y_2 = y_2(\lambda) \\ x_1 = \pm\,\tfrac{1}{2}\sqrt{-(s_1^2-\tau s_2^2)}\,\left(y_1(\lambda)^2-\tau y_2(\lambda)^2\right) \end{cases}$$

where

$$\begin{aligned} &-(s_1^2-\tau s_2^2)\,\left(y_1(\lambda)^2-\tau y_2(\lambda)^2\right)^2 \\ &\qquad = -2\left(s_1y_1(\lambda)^2 + 2\tau s_2 y_1(\lambda)y_2(\lambda) + \tau s_1 y_2(\lambda)^2\right)\,. \end{aligned}$$

From Lemma 3.2(i), we get that $y_1(\lambda)$ and $y_2(\lambda)$ are contained in $\mathsf{GF}(q)[\lambda]$ or in $\mathsf{GF}(q^2)[\lambda]\setminus\mathsf{GF}(q)[\lambda]$ according as $q\equiv 1 \pmod 4$ or $q\equiv 3 \pmod 4$. Since τ is a non-square in $\mathsf{GF}(q)$, if $q\equiv 1 \pmod 4$, then $x_1(\lambda)\in\mathsf{GF}(q^2)[\lambda]\setminus\mathsf{GF}(q)[\lambda]$. Therefore $\mathcal{P}_1^+$ (and, similarly, $\mathcal{P}_1^-$) are not $\mathsf{GF}(q)$-rational places. Furthermore, no point at infinity of Γ_1 has all coordinates over $\mathsf{GF}(q)$. Therefore, the $\mathsf{GF}(q)$-rational places of Γ_1^+ are the affine points of Γ_1^+ in $\mathsf{AG}(3,q)$ which are distinct from the origin, and their total number is equal to $q+1$ or 0 according as Γ_1^+ is defined over $\mathsf{GF}(q)$ or $\mathsf{GF}(q^2)$. The same holds true for Γ_1^-. $\square$

Proposition 3.4 has the following corollary.

ACADEMIA PRESS
UNIVERSITEIT GENT

Theorem 3.5. *For $t = -1$, the number of solutions of the system (4) in* $\mathsf{GF}(q)$ *is either $2q + 2$ or 0 according as $q \equiv 3 \pmod 4$ or $q \equiv 1 \pmod 4$.*

It should be noted that Theorem 3.5 for $q \equiv 1 \pmod 4$ was originally due to Korchmáros, see [10].

Proposition 3.6. *For $t = 1$, Γ_2 is reducible being split into two absolutely irreducible rational curves both defined over* $\mathsf{GF}(q)$ *or* $\mathsf{GF}(q^2)$ *according as $q \equiv 3 \pmod 4$ or $q \equiv 1 \pmod 4$. Furthermore, N_2 is equal to either $2q + 3$ or 1 according as $q \equiv 3 \pmod 4$ or $q \equiv 1 \pmod 4$.*

Proof. The arguments are analogous to those used in the preceding proof. The affine curve Γ_2 has two irreducible components, namely the affine curves Γ_2^+ and Γ_2^- defined by (6) together with

$$x_2 = \tfrac{1}{2}\sqrt{-\frac{1}{\tau}(s_1^2 - \tau s_2^2)}\,(y_1^2 - \tau y_2^2) \text{ and}$$
$$x_2 = -\tfrac{1}{2}\sqrt{-\frac{1}{\tau}(s_1^2 - \tau s_2^2)}\,(y_1^2 - \tau y_2^2),$$

respectively. □

Theorem 3.7. *For $t = 1$, the number of solutions of the system (4) in* $\mathsf{GF}(q)$ *is either $2q + 4$ or 2 according as $q \equiv 3 \pmod 4$ or $q \equiv 1 \pmod 4$.*

It should be noted that Theorem 3.7 for $q \equiv 1 \pmod 4$ was originally due to the authors, see [1].

The next step is to show that if $t \neq \pm 1$ then Γ_1 is an absolutely irreducible curve in $\mathsf{AG}(3, q)$.

Let $K(\mathcal{C}) = K(y_1, y_2)$ be the function field of $\mathcal{C}$ which is the field of transcendency degree 1 over K generated by y_1, y_2 such that (6) holds. From Lemma 3.2 the point T is the centre of two distinct places of $K(\mathcal{C})$, say $\mathcal{T}^+$ and $\mathcal{T}^-$, both defined over an extension of $\mathsf{GF}(q)$. The same holds for U and for the places $\mathcal{U}^+$ and $\mathcal{U}^-$ centred at U. The linear collineation ψ induces an involutory K-automorphism of $K(\mathcal{C})$ which interchanges $\mathcal{T}^+$ with $\mathcal{T}^-$ and $\mathcal{U}^+$ with $\mathcal{U}^-$.

Let $K(\Gamma_1) = K(y_1, y_2, x_1)$ be the function field of Γ_1 such that both (6) and the first equation in (5) hold.

To show the absolute irreducibility of Γ_1 for $t \neq \pm 1$, we also need a result on quadratic Kummer extensions of $K(y_1, y_2)$. Let $\delta \in K(y_1, y_2)$ be a non-square element in $K(y_1, y_2)$. Then the polynomial $X^2 - \delta$ is irreducible over $K(y_1, y_2)$ and the arising algebraic extension of $K(y_1, y_2)$ is a Kummer extension which is the function field $\Sigma = K(y_1, y_2, x_1)$ such that both (6) and $x_1^2 = \delta$ hold. The arising absolutely irreducible affine curve is defined in AG$(3, K)$ equipped with coordinates (y_1, y_2, x_1) by the equations (6) and $x_1^2 = \delta$.

From what we have observed, it is enough to show that δ may be chosen to be

$$\delta = s_1 y_1^2 + 2\tau s_2 y_1 y_2 + \tau s_1 y_2^2 + 1 + t\,, \tag{13}$$

δ being the square of no element in $K(y_1, y_2)$.

In terms of curves, this requires a preliminary investigation of the intersection number $I_{\mathcal{P}}(\mathcal{C}, \mathcal{D}) \geq 2$, where $\mathcal{D}$ is the non-singular conic of equation

$$G(X, Y, Z) = s_1 X^2 + 2\tau s_2 XY + \tau s_1 Y^2 + (1 + t) Z^2\,. \tag{14}$$

Lemma 3.8. *The curves $\mathcal{C}$ and $\mathcal{D}$ have four common points, namely the affine points $Q_1 = (\xi_1, \eta_1)$, $Q_2 = (-\xi_1, -\eta_1)$, $Q_3 = (\xi_2, \eta_2)$, $Q_4 = (-\xi_2, -\eta_2)$ with*

$$\xi_1 = \sqrt{-2\tau(t+1)\frac{\sqrt{s_1^2 - \tau s_2^2} + s_1}{s_1^2 - \tau s_2^2}}\,, \quad \xi_2 = \sqrt{-2\tau(t+1)\frac{\sqrt{s_1^2 - \tau s_2^2} - s_1}{s_1^2 - \tau s_2^2}}\,,$$
$$\eta_1 = \sqrt{2\tau(t+1)\frac{\sqrt{s_1^2 - \tau s_2^2} - s_1}{s_1^2 - \tau s_2^2}}\,, \quad \eta_2 = \sqrt{2\tau(t+1)\frac{\sqrt{s_1^2 - \tau s_2^2} + s_1}{s_1^2 - \tau s_2^2}}\,.$$

At each of the common points, $\mathcal{C}$ and $\mathcal{D}$ have the same tangent. In particular, if Q_i is the place of $K(y_1, y_2)$ centred at Q_i, then $v_{Q_i}(\delta) = 2$ with δ as in (13).

Proof. It is straightforward to check that $\mathcal{C}$ and $\mathcal{D}$ have no common point at infinity. Also, both $\mathcal{C}$ and $\mathcal{D}$ contains the point Q_i, for $i = 1, 2, 3, 4$. It remains to show that these curves have the same tangent at Q_i. The partial derivatives of $G(X, Y, Z)$ are

$$\begin{aligned} G_X &= 2s_1 X + 2\tau s_2 Y\,;\\ G_Y &= 2\tau s_2 X + 2\tau s_1 Y\,;\\ G_Z &= 2(t+1)Z\,. \end{aligned}$$

Now, to show the assertion, it is enough to verify that the matrix

$$\begin{pmatrix} F_X & F_Y & F_Z \\ G_X & G_Y & G_Z \end{pmatrix}$$

evaluated at Q_i has rank one. Let $Q_i = (\xi, \eta)$; to avoid tedious computations, we may argue as follows. The above matrix has rank one if and only if

$$\begin{cases} \xi^2 + \tau\eta^2 + 2\tau\dfrac{s_2}{s_1}\xi\eta + \dfrac{t+1}{s_1} & = 0 \\ \xi^2 + \tau\eta^2 + 2\dfrac{s_1}{s_2}\xi\eta & = 0 \\ \xi^2 - \tau\eta^2 \pm \dfrac{t+1}{\sqrt{s_1^2 - \tau s_2^2}} & = 0\,. \end{cases} \tag{15}$$

ACADEMIA PRESS
UNIVERSITEIT GENT

Therefore, if this is the case, then $(\xi^2, \eta^2, \xi\eta)$ must be a solution of linear system

$$\begin{cases} X_1 + \tau X_2 + 2\tau \dfrac{s_2}{s_1} X_3 = -\dfrac{t+1}{s_1} \\ X_1 + \tau X_2 + \ 2\dfrac{s_1}{s_2} X_3 = 0 \\ X_1 - \tau X_2 \qquad\qquad\quad = \mp \dfrac{t+1}{\sqrt{s_1^2 - \tau s_2^2}} \,. \end{cases}$$

This system has non-zero determinant $4\tau(s_1^2 - \tau s_2^2)/s_1 s_2$, and hence a unique solution (X_1, X_2, X_3) by the Cramer rule, for both choices "$+$" and "$-$" in the third equation. A straightforward computation shows that

$$\begin{cases} X_1 = (t+1)(-s_1 \mp \sqrt{s_1^2 - \tau s_2^2})/2(s_1^2 - \tau s_2^2) \\ X_2 = (t+1)(-s_1 \pm \sqrt{s_1^2 - \tau s_2^2})/2\tau(s_1^2 - \tau s_2^2) \\ X_3 = (t+1)s_2/2(s_1^2 - \tau s_2^2)\,. \end{cases}$$

From this, $X_1 X_2 = X_3^2$. Therefore, each of the four points $P = (\xi, \eta, 1)$ with $\xi = \pm\sqrt{X_1}$ and $\eta = \pm\sqrt{X_2}$ is a singular point of Γ_1. This completes the proof. $\square$

Lemma 3.8 has the following consequence.

Lemma 3.9. *Let*

$$u = y_1^2 - \tau y_2^2 + \frac{t+1}{\sqrt{s_1^2 - \tau s_2^2}}\,, \qquad w = y_1^2 - \tau y_2^2 - \frac{t+1}{\sqrt{s_1^2 - \tau s_2^2}}\,.$$

Then

$$\begin{aligned} v_{Q_1}(u) &= v_{Q_2}(u) = 2\,, \qquad & v_{Q_1}(w) &= v_{Q_2}(w) = 0\,, \text{ and} \\ v_{Q_3}(u) &= v_{Q_4}(u) = 0\,, \qquad & v_{Q_3}(w) &= v_{Q_4}(w) = 2\,, \end{aligned}$$

and each of the places $\mathcal{T}^+, \mathcal{T}^-, \mathcal{U}^+, \mathcal{U}^-$ is a pole of multiplicity 1 of both u and w.

Proof. By the definitions of δ, u, v, we have that

$$(s_1^2 - \tau s_2^2)uv = 2\delta\,.$$

From the third equation (15), $v_{Q_1}(w) = v_{Q_2}(w) = v_{Q_3}(u) = v_{Q_4}(u) = 0$. The remaining assertions follow from Lemma 3.8. $\square$

In $K(y_1, y_2)$, consider the Riemann-Roch space $\mathcal{L}(\mathbf{D})$ of the divisor

$$\mathbf{D} = \mathcal{T}^+ + \mathcal{T}^- + \mathcal{U}^+ + \mathcal{U}^- .$$

By Lemma 3.9, $u, w \in \mathcal{L}(\mathbf{D})$. Furthermore, $1, y_1, y_2 \in \mathcal{L}(\mathbf{D})$. Since $\deg \mathbf{D} = 4$ and $K(y_1, y_2)$ has genus 1, it follows that $\{1, y_1, y_2, u\}$ is a basis of $\mathcal{L}(\mathbf{D})$.

Now suppose that δ as in (13) is a square in $K(y_1, y_2)$, and let $\varepsilon \in K(y_1, y_2)$ such that $\varepsilon^2 = \delta$. From Lemma 3.8, $\varepsilon \in \mathcal{L}(\mathbf{D})$. Therefore, there exist c_0, c_1, c_2, c_3 in K such that

$$\varepsilon = c_0 + c_1 x + c_2 y + c_3 \left(y_1^2 - \tau y_2^2 + \frac{t+1}{\sqrt{s_1^2 - \tau s_2^2}} \right) .$$

But this is inconsistent with $\delta = \varepsilon^2$.

Therefore, we have shown the following result.

Proposition 3.10. *For $t \neq \pm 1$, the algebraic curve Γ_1 is absolutely irreducible.*

Next we determine the singular points of Γ_1.

Lemma 3.11. *For $t \neq \pm 1$, Γ_1 has eight singular points, namely*

$$\begin{aligned} T_1 &= (i, 1, \sqrt{\tfrac{1}{2}(s_1 + i s_2)}, 0) , & T_2 &= (i, 1, -\sqrt{\tfrac{1}{2}(s_1 + i s_2)}, 0) , \\ U_1 &= (-i, 1, \sqrt{\tfrac{1}{2}(s_1 - i s_2)}, 0) , & U_2 &= (-i, 1, -\sqrt{\tfrac{1}{2}(s_1 - i s_2)}, 0) , \\ R_1 &= (\xi_1, \eta_1, 0, 1) , & R_2 &= (-\xi_1, -\eta_1, 0, 1) , \\ R_3 &= (\xi_2, \eta_2, 0, 1) , & R_4 &= (-\xi_2, -\eta_2, 0, 1) . \end{aligned}$$

The first four points lie over a proper extension of $\mathsf{GF}(q)$*, but this may fail for the other four points.*

Proof. In the projective closure $\mathsf{PG}(3, q)$ equipped with homogeneous coordinates (X, Y, W, Z) the projective curve Γ_1 has equations $F(X, Y, Z) = 0$ and $H(X, Y, W, Z) = 0$ with

$$H = H(X, Y, Z, W) = 2W^2 - \left(s_1 X^2 + 2\tau s_2 XY + \tau s_1 Y^2 + (1+t) Z^2 \right) .$$

The partial derivatives of H are

$$\begin{aligned} H_X &= -2 s_1 X - 2\tau s_2 Y ; \\ H_Y &= -2\tau s_2 X - 2\tau s_1 Y ; \\ H_W &= 2W ; \\ H_Z &= 2(t+1) Z . \end{aligned}$$

A point $P = (x, y, w, z)$ of Γ_1 is singular if and only if the matrix

$$\begin{pmatrix} F_X & F_Y & 0 & F_Z \\ H_X & H_Y & H_W & H_Z \end{pmatrix}$$

evaluated at P has rank one. Obviously, this certainly occurs when the first row consists of zeros giving rise to the points T_1, T_2, U_1, U_2. Otherwise, $w = 0$ and we show that Γ_1 has four more singular points. Since the points T_1, T_2, U_1, U_2 are the only points at infinity of Γ_1, we may assume that $z = 1$. A point $P = (x, y, 0, 1)$ is a singular point of Γ_1 if and only if the matrix

$$\begin{pmatrix} F_X & F_Y & F_Z \\ H_X & H_Y & H_Z \end{pmatrix}$$

evaluated at $P' = (x, y, 1)$ has rank one. Geometrically, P' is a common point of the quartic $\mathcal{C}$ and the non-singular conic $\mathcal{D}$ and they have the same tangent at P'. From Lemma 3.8, P must be one of the points R_1, R_2, R_3 and R_4. □

Lemma 3.12. Γ_1 *has genus at most* 5.

Proof. The map

$$\varphi\colon (y_1, y_2, x_1) \mapsto (y_1, y_2, -x_1)$$

is an involutory K-automorphism of the function field $K(\Gamma_1)$ of Γ_1, and $K(y_1, y_2)$ is the subfield fixed by φ elementwise. We show that the associated covering of degree 2 may only ramify at the places centred at the points R_1, R_2, R_3 and R_4. In fact, φ acts on the points of Γ_1 as the linear collineation $(X, Y, Z) \mapsto (X, Y, -Z)$ which is a symmetry with axis $Z = 0$. Also, φ does not fix any of the four points at infinity of Γ_1. Each of the points R_1, R_2, R_3, R_4 is the centre of two places of Γ_1. Therefore, the number k of fixed places of φ is at most eight. From the Riemann-Hurwitz formula,

$$2g - 2 = 2(2g' - 2) + k$$

where g' is the genus of the subfield $K(\Gamma_1)^\varphi$ of $K(\Gamma_1)$. Obviously, $K(\mathcal{C})$ is a subfield of $K(\Gamma_1)^\varphi$. Since $[K(\Gamma_1) : K(\mathcal{C})] = 2$, this implies that $K(\Gamma_1)^\varphi = K(\mathcal{C})$. From this and Lemma 3.2, $g' = 1$ and the assertion follows. □

In the above proof we have also shown that the points at infinity of Γ_1 are not defined over GF(q). From this and the Hasse-Weil theorem, we obtain the following result.

Theorem 3.13. *For* $t \neq \pm 1$,

$$q - 10\sqrt{q} - 3 \le N_1 \le q + 10\sqrt{q} + 5\,. \qquad (16)$$

ACADEMIA PRESS
UNIVERSITEIT GENT

Proof. Let N_q be the number of all GF(q)-rational places of Γ_1, that is the number of all points in PG(r,q) of a non-singular model $\mathcal{X}$ of Γ_1 embedded in PG(r,q) by a birational map defined over GF(q). The non-singular points of Γ_1 in PG$(3,q)$ are GF(q)-rational points, but a singular point $P \in$ PG$(3,q)$ of Γ_1 may happen not to define a GF(q)-rational point. More precisely, let $\mathcal{P}_1, \ldots, \mathcal{P}_k$ be the places of Γ_1 centred at P. If m of them are defined over GF(q), then P counts with weight m in N_q. From Lemma 3.11, Γ_1 has four singular points which may happen to be in AG$(3,q)$, namely R_1, R_2, R_3 and R_4. Since each R_i is a doubly point, R_i is the centre of one or two places of Γ_1. If $R_i \in$ AG$(3,q)$, then one or two or none of the places centred at R_i are GF(q)-rational. Thus $-4 \le N_q - N_1 \le 4$, whence

$$N_q - 4 \le N_1 \le N_q + 4\,.$$

From the Hasse-Weil theorem, $|N_q - (q+1)| \le 2g\sqrt{q} \le 10\sqrt{q}$. This completes the proof. □

Theorem 1.2(iv) and (v) follow from Lemma 3.3 and Theorem 3.13.

Our final remark is that for $q \le 11$, an exhaustive computer aided argument shows that Γ_1 has genus 1. Therefore, if $q \le 11$ then (16), and hence (iv) of Theorem 1.2 may be replaced by

$$q - 2\sqrt{q} - 3 \le N_1 \le q + 2\sqrt{q} + 5\,. \tag{17}$$

References

[1] **V. Abatangelo** and **B. Larato**, Complete arcs on Moulton planes of odd order, *Ars Combin.*, to appear.

[2] **D. G. Glynn** and **G. F. Steinke**, On conics that are ovals in a Hall plane, *European J. Combin.* **14** (1993), 521–528.

[3] **J. W. P. Hirschfeld**, *Projective Geometries over Finite Fields*, second ed., Oxford Univ. Press, Oxford, 1998, xiv+555 pp.

[4] **J. W. P. Hirschfeld**, **G. Korchmáros** and **F. Torres**, *Algebraic Curves over a Finite Field*, Princeton Univ. Press, Princeton and Oxford, 2008, xx+696 pp.

[5] **W. V. D. Hodge** and **D. Pedoe**, *Methods of Algebraic Geometry, Vols. I,II,III*, Cambridge Univ. Press, Cambridge, 1953, viii+440 pp.; 1952, x+394 pp.; 1954, x+336 pp.

[6] **T. Honold** and **I. Landjev**, Arcs in projective Hjelmslev planes, *Discrete Math. Appl.* **11** (2001), 53–70.

[7] **D. R. Hughes** and **F. C. Piper**, *Projective planes*, Springer, Berlin, 1973.

[8] **N. L. Johnson**, **V. Jha**, and **M. Biliotti**, *Handbook of Finite Translation Planes*, Pure and Applied Mathematics (Boca Raton) **289**, Chapman & Hall/CRC, Boca Raton, FL, 2007. xxii+861 pp.

[9] **G. Korchmáros**, Ovali nei piani di Hall di ordine dispari, *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8)* **56** (1974), 315–317.

[10] ———, Ovali nei piani di Moulton di ordine dispari, *Atti Convegni Lincei*, **17**, Vol. II (1976), 395–398.

[11] ———, Inherited arcs in finite affine planes, *J. Combin. Theory Ser. A* **42** (1986), 140–143.

[12] **G. Menichetti**, q-archi completi nei piani di Hall di ordine $q = 2^k$, *Rend. Accad. Naz. Lincei*, **56** (1974), 518–525.

[13] **C. M. O'Keefe** and **A. A. Pascasio**, Images of conics under derivation, Graph theory and combinatorics, *Discrete Math.* **151** (1996), 189–199.

[14] **C. M. O'Keefe**, **A. A. Pascasio** and **T. Penttila**, Hyperovals in Hall planes, *European J. Combin.* **13** (1992), 195–199.

[15] **G. Rinaldi**, Arcs in the Hall planes, *Results Math.* **29** (1996), 149–152.

[16] **G. Rinaldi** and **F. Zironi**, Complete unital-derived arcs in the Hall plane of order 9, *Bull. Inst. Combin. Appl.* **36** (2002), 29–36.

[17] **A. Seidenberg**, *Elements of the Theory of Algebraic Curves*, Addison-Wesley, Reading, 1968, viii+216 pp.

[18] **T. Szőnyi**, Complete arcs in non-Desarguesian planes, *Ars Combin.*, **25**, (1988), C , 169-178.

[19] ———, Arcs and k-sets with large prime-set in Hall planes, *J. Geom.* **34** (1989), 187-194.

[20] ———, Complete arcs in non-Desarguesian planes, *Confer. Sem. Mat. Univ. Bari* **233** (1989), pp. 1-22.

Vito Abatangelo
Dipartimento di Matematica, Politecnico di Bari, Via Orabona 4, I-70125 Bari, Italy
e-mail: abatvito@poliba.it

Bambina Larato
Dipartimento di Matematica, Politecnico di Bari, Via Orabona 4, I-70125 Bari, Italy
e-mail: larato@poliba.it