J. Austral. Math. Soc. (*Series A*) **45** (1988), 275–286

THE CHARACTERIZATION OF ELLIPTIC CURVES OVER FINITE FIELDS

J. W. P. HIRSCHFELD and J. F. VOLOCH

(Received 11 March 1987)

Communicated by R. Lidl

Abstract

In a finite Desarguesian plane of odd order, it was shown by Segre thirty years ago that a set of maximum size with at most two points on a line is a conic. Here, in a plane of odd or even order, sufficient conditions are given for a set with at most three points on a line to be a cubic curve. The case of an elliptic curve is of particular interest.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*) (1985 *Revision*): 51 E 15, 14 H 25.

0. Notation

$GF(q)$	the finite field of q elements
$PG(2,q)$	the projective plane over $GF(q)$
$PG^{(1)}(2,q)$	the set of lines in $PG(2,q)$
$\mathbf{P}(X)$	the point of $PG(2,q)$ with coordinate vector X
U_0	$\mathbf{P}(1,0,0)$,
U_1	$\mathbf{P}(0,1,0)$
U_2	$\mathbf{P}(0,0,1)$
U	$\mathbf{P}(1,1,1)$
PQ	the line joining the points P and Q
$l(P,Q)$	PQ
$\langle P \rangle$	the group generated by P

1. Background

In $PG(2,q)$, a $(k;n)$-*arc* is a set of k points with at most n points on any line and with n points on some line. A $(k;2)$-arc is also called a k-*arc*. A $(k;n)$-arc is *complete* if there is no $(k+1;n)$-arc containing it. First we state some problems.

I *When is a $(k;n)$-arc an irreducible algebraic curve of degree n?*

More generally, one can ask the following.

II *When is a $(k;n)$-arc contained in an irreducible algebraic curve of degree n?*

A more restricted problem can be posed.

III *When is an irreducible algebraic curve of degree n complete as a $(k;n)$-arc?*

Much is known about these questions for $n = 2$. In this paper we consider them for $n = 3$.

For $n = 2$, some answers are by now classical. Up to projectivities, there is only one irreducible algebraic curve of degree 2, which we call a conic. The most elegant theorem, due to Segre (1956), answers problem I completely for q odd.

A *For q odd, a $(q+1)$-arc is a conic.*

A partial answer to II is given also by Segre (1967).

B1 *For q odd and $k > q - \frac{1}{4}\sqrt{q} + \frac{7}{4}$, a k-arc is contained in a unique conic.*

To show that this is not best possible there is a recent result due to the second author [23].

B2 *For q an odd prime p and $k > \frac{4}{45}(11p + 10)$, a k-arc is contained in a unique conic.*

Problem III is trivial for $n = 2$.

C *A conic is a complete $(q+1)$-arc for q odd but an incomplete $(q+1)$-arc for q even which can be completed uniquely to a $(q+2)$-arc.*

For comparable results to (A) and (B) when q is even, see [4] Chapter 10 and Thas [20], [21]; the latter contains a slight improvement on (B1) for odd q.

As an indication of the difficulty of the problem, it is worth noting that neither $m_n(2,q)$, the maximum number of points on a $(k;n)$-arc, nor $N_q(g)$, the maximum number of points on a non-singular algebraic curve of genus g, is known in general. We survey these values briefly, giving the principal results. First,

$$N_q(g) \leq q + 1 + 2g\sqrt{q}, \tag{1.1}$$

where, if a plane curve of genus g has degree n, then $2g \leq (n-1)(n-2)$. For a survey, see [6], Appendix IV and [16], [17], [18]. Also

$$m_n(2,q) \leq (n-1)q + n \tag{1.2}$$

with equality implying that $n = q+1$ or n divides q. When $q = 2^h$ and n divides q, then

$$m_n(2,q) = (n-1)q + n.$$

https://doi.org/10.1017/S1446788700030172 Published online by Cambridge University Press

Also

$$m_2(2,q) = \begin{cases} q+1, & q \text{ odd}, \\ q+2, & q \text{ even}. \end{cases}$$

Apart from the cases of $n = 2$ or q even, very few results are known. For small values of n and q,

$$m_3(2,q) = \begin{cases} 2q+3 & \text{for } q = 2,3, \\ 2q+1 & \text{for } q = 4,5,7, \\ 2q-1 & \text{for } q = 8,9, \end{cases}$$

$$m_4(2,q) = \begin{cases} 3q+1 & \text{for } q = 5,7,9, \\ 3q+4 & \text{for } q = 8, \end{cases}$$

$$m_5(2,q) = 4q+1 \quad \text{for } q = 7,8,9,$$

$$m_6(2,q) = \begin{cases} 5q+1 & \text{for } q = 7, \\ 5q+2 & \text{for } q = 8, \\ 5q+3 & \text{for } q = 9, \end{cases}$$

$$m_7(2,q) = 6q+1 \quad \text{for } q = 8.$$

For a survey on $m_n(2,q)$, see [5] and [4] Chapter 12. See also [1], [10].

Apart from the central results (A) and (B), there have been characterizations of other rational curves ($g = 0$) obtained by using birational transformations of a conic and then applying (B1). See [4], Chapter 12, Tallini Scafati [19], Keedwell [7], [8], Raguso and Rella [12], [13], [14].

2. Cubic arcs and cubic curves

We now turn to the case of $(k;3)$-arcs, also called cubic arcs, and cubic curves. It is desired to solve problem I when $n = 3$. Tallini Scafati used (B1) of §1 to solve the problem for rational cubic curves with the following result.

D *Let $\mathscr{K}$ be a $(k;3)$-arc in $PG(2,q)$, q odd and $q > 11$, with the following properties*:

(i) *$\mathscr{K}$ contains four distinct points P, P_1, P_2, P_3 such that*

(a) *there is no 3-secant of $\mathscr{K}$ through P,*

(b) *any conic through P and one P_i meets $\mathscr{K}$ in at most three other points*;

(ii) $k > q - \frac{1}{4}\sqrt{q} + 19/4$.

Then $\mathscr{K}$ is contained in a rational cubic with a double point at P.

It therefore remains to look at $(k;3)$-arcs and elliptic cubic curves. Firstly it must be noted that there are many $(k;3)$-arcs which are not elliptic curves.

The number of projectively distinct elliptic cubics in $PG(2,q)$ is roughly $3q$. More precisely, if P_q is this number and A_q is the number with at least one inflexion, then the numbers are given by Table 1, in which $q \equiv m \pmod{12}$.

https://doi.org/10.1017/S1446788700030172 Published online by Cambridge University Press

TABLE 1

m	3	9	2, 8	4	1	7	5	11
A_q	$2q+2$	$2q+4$	$2q+1$	$2q+5$	$2q+6$	$2q+4$	$2q+2$	$2q$
P_q	$3q+1$	$3q+3$	$3q$	$3q+6$	$3q+7$	$3q+5$	$3q+1$	$3q-1$

The number $C(k,q)$ of projectively distinct $(k;3)$-arcs is hard to calculate. By way of example, $C(11,5) = 2$, [11]; $C(7,8) = 98$, [25]. In contrast, if $E(k,q)$ is the number of projectively distinct elliptic cubics with precisely k points, then $E(11,5) = 0$, $E(7,8) = 0$. In fact, the number k of points on an elliptic curve satisfies

$$q+1-2\sqrt{q} \leq k \leq q+1+2\sqrt{q}$$

and can take every value in this interval other than $q+1+mp$, where $q = p^h$ with p prime. For these results, see [24], [15], [2], [9]. In [15] the value of $E(k,q)$ is calculated.

The most important property of an elliptic cubic $\mathscr{E}$ is that it is an abelian group. Choose any point O as the zero. If P, Q are any points of $\mathscr{E}$, then PQ meets $\mathscr{E}$ in a further point R, which is taken as P if PQ is the tangent at P. Then RO meets $\mathscr{E}$ again at $P+Q$. If O is an inflexion, then P_1, P_2, P_3 are collinear if and only if $P_1+P_2+P_3 = O$.

From the above properties it follows that certain restrictions must be placed on a $(k;3)$-arc $\mathscr{K}$ to make it an elliptic curve. Certain axioms evolve naturally. Firstly, $\mathscr{K}$ requires a zero and we make it an inflexion:

(E1) there exists O in $\mathscr{K}$ such that $l \cap \mathscr{K} = \{O\}$ for some line l.

Next, we require a specific tangent at each point of $\mathscr{K}$ other than O:

(E2) there exists an injective map $\tau: \mathscr{K} \setminus \{O\} \to PG^{(1)}(2,q)$ such that $P \in P\tau$ and $|P\tau \cap \mathscr{K}| = 1$ or 2.

Note that (E2) does not specify a tangent at O. The axiom (E1) says that more than one such tangent may exist. This is naturally weaker than specifying the tangent at O. It would be unsatisfactory to show that $\mathscr{K}$ lies in a cubic curve $\mathscr{E}$ when one unisecant of $\mathscr{K}$ is chosen as a tangent at O but not one other is chosen. Now, it is necessary to ensure that there are no bisecants of $\mathscr{K}$ other than tangents:

(E3) if P, $Q \in \mathscr{K}$ and $PQ \neq P\tau$ or $Q\tau$, then PQ meets $\mathscr{K}$ in three distinct points P, Q, R.

It follows from (E1)–(E3) that $\mathscr{K}$ has at most $k-1$ bisecants. Also there is no cubic curve whose tangents are concurrent at a point of the curve. So (E3) ensures that a cubic curve containing $\mathscr{K}$ has no double point in $\mathscr{K}$. Further, (E1)–(E3) are insufficient to ensure that the group law holds on $\mathscr{K}$; for an example, see the Appendix. It is therefore necessary to introduce a further axiom.

https://doi.org/10.1017/S1446788700030172 Published online by Cambridge University Press

For each point P in $\mathscr{K}$, define the point $\overline{P}$ as follows.

(i) $\overline{O} = O$;

(ii) if $P \neq O$ and $P\tau \neq PO$, define $\overline{P}$ to be the third point of $PO \cap \mathscr{K}$ other than P and O;

(iii) if $P \neq O$ and $P\tau = PO$, define $\overline{P} = P$.

Now, for each pair of points P, Q in $\mathscr{K}$, define the point $P * Q$:

(i) $P * P = \overline{P}$ if $P\tau \cap \mathscr{K} = \{P\}$;

(ii) $P * P = \overline{R}$ if $P\tau \cap \mathscr{K} = \{P, R\}$;

(iii) $P * Q = \overline{P}$ if $P_\tau \cap \mathscr{K} = \{P, Q\}$;

(iv) $P * Q = \overline{R}$ if $PQ \cap \mathscr{K} = \{P, Q, R\}$.

The final axiom for $\mathscr{K}$ is the strongest:

(E4) $\mathscr{K}$ is an abelian group with identity O such that $-P = \overline{P}$ and $P + Q = P * Q$.

DEFINITION. A $(k; 3)$-arc $\mathscr{K}$ satisfying (E1)–(E4) is called a *group-arc* or a *k-group-arc*.

EXAMPLES. (1) The prototype of a group-arc is the set of points of an elliptic cubic curve with inflexion at O.

(2) The set of non-singular points of a singular cubic with an inflexion at O is also a group-arc.

REMARKS. (1) The axiom (E4) is necessary as it is not possible to prove the associative law on the basis of (E1)–(E3).

(2) Any subgroup of a group-arc is a group-arc.

(3) $P + Q + R = O$ if and only if P, Q, R are collinear.

The main purpose of this paper is to show that these two examples are the only ones and thus to provide a characterization of elliptic curves.

THEOREM 2.1. *If $\mathscr{K}$ is a k-group-arc in $PG(2, q)$ such that either*

(a) *k is divisible by at least two distinct primes other than 2, 3, 5, or*

(b) *$k = 2^a 3^b 5^c p^d$, where $p \geq 7$ is a prime, $d \geq 1$ and $2^a 3^b 5^c \geq 6$,*

then $\mathscr{K}$ is a subgroup of the set of non-singular points of a cubic curve.

Note. The only values of k excluded are $k = 2^a 3^b 5^c, a, b, c \geq 0$, $k = ep^d$, p prime, $p \geq 7$ and $1 \leq e \leq 5$. This theorem is proved in §4.

3. Preliminary lemmas for the main theorem

Four lemmas are required.

LEMMA 3.1. *If P is a point of an arbitrary group-arc, then $\langle P \rangle$ is uniquely determined by O, $\pm P$, $\pm 2P$, $3P$ and $(-2P)\tau$.*

https://doi.org/10.1017/S1446788700030172 Published online by Cambridge University Press

PROOF. Let n be the order of P. If $n \leq 6$, there is nothing to prove; so, assume that $n \geq 7$. Then

$$-3P = l(P, 2P) \cap l(O, 3P).$$

If $n = 7$, all points of $\langle P \rangle$ have been obtained. If $n > 7$,

$$4P = l(-P, -3P) \cap (-2P)\tau.$$

If $n = 8$, again all points of $\langle P \rangle$ have been determined. If $n > 8$,

$$-4P = l(P, 3P) \cap l(O, 4P).$$

Now proceed by induction and assume that $O, \pm P, \ldots, \pm mP$ have been determined for $m \geq 4$. Then

$$-(m+1)P = l(P, mP) \cap l(2P, (m-1)P),$$
$$(m+1)P = l(-P, -mP) \cap l(O, -(m+1)P),$$

providing each pair of lines is distinct. If the opposite occurs, then $\langle P \rangle$ is already determined by the induction hypothesis.

LEMMA 3.2. *Let P be a point of order at least six of a group-arc. Then $\langle P \rangle$ is a subgroup of a unique cubic curve with inflexion O.*

PROOF. By a suitable choice of coordinates we may take (i) $O = U_1$, (ii) $P = U_2$, (iii) $-2P = U_0$, (iv) $3P = U$. Since $P\tau = l(P, -2P)$, (v) $P\tau = U_0U_2$. As $2P \in l(O, -2P)$ and $2P \neq O$, $4P \neq O$, so (vi) $2P = \mathbf{P}(1, c, 0)$, $c \neq 0$. Since $-P = l(3P, -2P) \cap l(O, P)$, (vii) $-P = \mathbf{P}(0, 1, 1)$. Now, let (viii) $(-2P)\tau$ have equation $x_2 = dx_1$. From conditions (i)–(iii) and (vi)–(vii), the cubic has equation

$$A(x_1^2x_2 - x_1x_2^2) + B_1x_0^2x_2 + B_2x_0x_2^2 + C(cx_0^2x_1 - x_0x_1^2) + Dx_0x_1x_2 = 0.$$

Now, (iv) gives $B_1 + B_2 + (c-1)C + D = 0$; from (v), $B_2 = 0$; from (viii), $B_1d + Cc = 0$. The fact that O is an inflexion gives $D + cA - C = 0$. Hence $A = d - 1$, $B_2 = 0$, $B_1 = -c$, $C = d$, $D = c + (1-c)d$. Thus the cubic is determined.

LEMMA 3.3. *Let $\mathscr{E}_1$ and $\mathscr{E}_2$ be cubic curves and $\mathscr{K}$ a k-group-arc which is a subgroup of both $\mathscr{E}_1$ and $\mathscr{E}_2$. If $k > 5$, then $\mathscr{E}_1 = \mathscr{E}_2$.*

PROOF. The curves $\mathscr{E}_1$ and $\mathscr{E}_2$ intersect in the points of $\mathscr{K}$ with multiplicity at least two in the points P of $\mathscr{K}$ other than O, since $P\tau$ is the tangent at P of both $\mathscr{E}_1$ and $\mathscr{E}_2$. Hence, if $\mathscr{E}_1 \neq \mathscr{E}_2$, Bézout's theorem gives $9 \geq 1 + 2(k-1)$, whence $k \leq 5$.

https://doi.org/10.1017/S1446788700030172 Published online by Cambridge University Press

LEMMA 3.4. *Let $\mathscr{K}$ be a group-arc contained in a cubic curve $\mathscr{E}$ such that any cyclic subgroup of $\mathscr{K}$ is a subgroup of $\mathscr{E}$. Then $\mathscr{K}$ is a subgroup of $\mathscr{E}$.*

PROOF. Tangents at P depend only on $\langle P\rangle$; so tangents are the same in $\mathscr{K}$ and $\mathscr{E}$. Also, inverses depend only on $\langle P\rangle$; so inverses are the same in $\mathscr{K}$ and $\mathscr{E}$. If $P, Q \in \mathscr{K}$, then it must be shown that $P+Q$ is the same in $\mathscr{K}$ and $\mathscr{E}$. If $P = -Q$, then $P+Q = O \in \langle P\rangle$. If $PQ = P\tau$, then $Q = -2P$ and $P+Q = -P \in \langle P\rangle$; similarly, when $PQ = Q\tau$. Otherwise $PQ \cap \mathscr{K} = \{P, Q, R\} \subset \mathscr{E}$; so $R \in \mathscr{E}$. As $R = -(P+Q)$ in $\mathscr{K}$ and $\mathscr{E}$, so $P+Q$ is the same in $\mathscr{K}$ and $\mathscr{E}$.

4. Proof of the main theorem

(i) *Assume condition* (a). Let p, q be distinct primes dividing k with $p, q \geq 7$. Let P in $\mathscr{K}$ be a point of order p and Q in $\mathscr{K}$ a point of order q. Then $P+Q$ has order pq and, by Lemma 3.2, we may take $\mathscr{E}$ to be the unique cubic containing $\langle P+Q\rangle$. We shall prove that $\mathscr{K}$ is a subgroup of $\mathscr{E}$.

Let R in $\mathscr{K}$ be a point of order n and suppose first that $p \nmid n$. Let $\mathscr{E}_1$ be the cubic containing $\langle P+R\rangle$. As P, R have coprime orders, so both $\langle P\rangle$ and $\langle R\rangle$ are contained in $\langle P+R\rangle$ and hence in $\mathscr{E}_1$. Similarly, $\langle P\rangle$ is contained in $\langle P+Q\rangle$ and in $\mathscr{E}$. As P has order $p \geq 7$, so $\mathscr{E} = \mathscr{E}_1$ by Lemma 3.3. So $\langle R\rangle$ is contained in $\mathscr{E}_1 = \mathscr{E}$.

Now suppose that $p|n$ and that q^r is the highest power of q dividing n. Let $m = n/q^r$. Note that $p|m$ and so $m \geq 7$. Let $\mathscr{E}_2, \mathscr{E}_3, \mathscr{E}_4$ be the cubics containing respectively $\langle R\rangle$, $\langle q^r R\rangle$, $\langle q^r R+Q\rangle$. It will be shown that $\mathscr{E} = \mathscr{E}_2$. Since $R \in \mathscr{E}_2$, this will complete the proof.

The group $\langle q^r R\rangle$ is in both $\mathscr{E}_2$ and $\mathscr{E}_3$. As $q^r R$ has order $m \geq 7$, again by Lemma 3.3 it follows that $\mathscr{E}_2 = \mathscr{E}_3$. Since $q^{r+1}R = q(q^r R + Q)$, the group $\langle q^{r+1}R\rangle$ lies in both $\mathscr{E}_3$ and $\mathscr{E}_4$. As m and q are coprime, $q^{r+1}R$ has order m; Lemma 3.3 delivers that $\mathscr{E}_3 = \mathscr{E}_4$. Finally, $mQ = m(q^r R + Q)$. Since there exist integers u, v such that $um + vq = 1$, so $Q = umQ$. Hence $\langle Q\rangle$ is in both $\mathscr{E}$ and $\mathscr{E}_4$; so $\mathscr{E} = \mathscr{E}_4$ as $q \geq 7$. Thus $\mathscr{E} = \mathscr{E}_4 = \mathscr{E}_3 = \mathscr{E}_2$.

(ii) *Assume condition* (b). By the fundamental theorem for finite abelian groups,

$$\mathscr{K} = G \oplus G_1 \oplus \cdots \oplus G_r,$$

where $G_i \cong \mathbf{Z}/p^{c_i}$, $c_i \geq 1$, $c_1 + \cdots + c_r = d$, $|G| = 2^a 3^b 5^c \geq 6$. Let P_i be a generator of G_i, $i = 1, \ldots, r$. If $Q \in G$, then the order of $P_i + Q$ is divisible by $p^{c_i} \geq 7$; so $\langle P_i + Q\rangle$ is contained in a unique cubic $\mathscr{E}_{i,Q}$. As P_i and Q have coprime orders, both $\langle P_i\rangle$ and $\langle Q\rangle$ lie in $\langle P_i + Q\rangle$ and hence in $\mathscr{E}_{i,Q}$. Since P_i has order $p^{c_i} \geq 7$, it follows from Lemma 3.3 that, for a fixed i, the $\mathscr{E}_{i,Q}$ are all

https://doi.org/10.1017/S1446788700030172 Published online by Cambridge University Press

equal as Q runs through the points of G. Let this common curve be $\mathscr{E}_i$; then $G \subset \mathscr{E}_i$. So, by Lemma 3.3, all $\mathscr{E}_i$ are equal to the cubic $\mathscr{E}$, say. Thus, G and $G_1, G_2, \ldots, G_r$ are subgroups of $\mathscr{E}$.

It remains to show that $\langle R \rangle$ is a subgroup of $\mathscr{E}$ for any R in $\mathscr{H}$. Firstly, $\mathscr{E}$ does not depend on the decomposition of $H = G_1 \oplus \cdots \oplus G_r$, since the uniqueness of $\mathscr{E}$ follows from the fact that $G \subset \mathscr{E}$ and Lemma 3.3. So, given any point P in H of order p^{c_i} for some i, we may assume that $G_i = \langle P \rangle$; hence $\langle P \rangle$ is a subgroup of $\mathscr{E}$. Also, given any point Q in H we can find P in H of order p^{c_i}, some i, such that $\langle Q \rangle$ is a subgroup of $\langle P \rangle$, which in turn is a subgroup of $\mathscr{E}$. Hence $\langle Q \rangle$ is a subgroup of $\mathscr{E}$ for all Q in H.

Finally, given R in $\mathscr{H}$, we have $R = P + Q$ with P in G and Q in H. If R is not in G or H, then R has order at least $2p$ and so $\langle R \rangle$ is contained in a unique cubic $\mathscr{E}_1$. Further, $\mathscr{E} \cap \mathscr{E}_1$ contains mR where m is the order of P. As mR has order at least p, so $\mathscr{E} = \mathscr{E}_1$ and $\langle R \rangle$ is a subgroup of $\mathscr{E}$. Lemma 3.4 now shows that $\mathscr{H}$ is a subgroup of $\mathscr{E}$.

5. Elliptic curves as complete arcs

A conic in $PG(2, q)$ is a complete $(q+1)$-arc when q is odd and is an incomplete $(q+1)$-arc when q is even. The question now is to decide when a non-singular cubic $\mathscr{E}$ with k points is a complete $(k; 3)$-arc.

THEOREM 5.1. *If $q \geq 79$ and q is not a power of 2 or 3, then a non-singular cubic $\mathscr{E}$ with k points is a complete $(k; 3)$-arc unless $j(\mathscr{E}) = 0$ in which case the completion of $\mathscr{E}$ has at most $k + 3$ points.*

PROOF. Let $f(x, y) = 0$ be an affine equation for $\mathscr{E}$ and let $P_0 \in PG(2, q) \backslash \mathscr{E}$. The j-invariant of $\mathscr{E}$ gives the six cross-ratios of the four tangents from a point of $\mathscr{E}$ to other points of $\mathscr{E}$. Then $j(\mathscr{E}) = 0$ when there are only two distinct values among the six cross-ratios; the curve is called *equianharmonic* in this case. We shall show that if $j(\mathscr{E}) \neq 0$ there exists a line through P_0 cutting $\mathscr{E}$ in three distinct points.

Let K be the function field of $\mathscr{E}$. Suppose $P_0 = (x_0, y_0)$ and let

$$F(z) = \frac{1}{z - x} f(z, (y - y_0)(z - x_0)/(x - x_0) + y_0).$$

Then $F(z)$ is a polynomial of degree 2 in z, lying in $K[z]$, whose roots give the two points of $\mathscr{E}$ lying on the line through $P = (x, y)$ and P_0 where $P \in \mathscr{E}$ and P is excluded. If $F(z)$ is irreducible over L, the function field of $\mathscr{E}$ consider over the algebraic closure $\overline{GF(q)}$ of $GF(q)$, then $F(z) = 0$ defines a *double cover* of $\mathscr{E}$, which we denote by $\mathscr{F}$. The curve $\mathscr{F}$ is *ramified* over $\mathscr{E}$ at those points (x, y)

https://doi.org/10.1017/S1446788700030172 Published online by Cambridge University Press

where $F(z)$ has a double root, that is where PP_0 is a tangent to $\mathscr{E}$ at the other intersection; hence there are at most six such points. It follows from Hurwitz's formula ([3], p. 299) that the genus of $\mathscr{F}$ satisfies $2g-2 \leq 6$, whence $g \leq 4$.

An unramified rational point of $\mathscr{F}$ corresponds to a point P in $\mathscr{E}$ for which $F(z)$ splits into two distinct linear factors over $GF(q)$; that is, PP_0 meets $\mathscr{E}$ in three distinct points. So it suffices to show that $\mathscr{F}$ has an unramified rational point. This will happen if $\mathscr{F}$ has at least 7 points, which is true if $q+1-8\sqrt{q} \geq 7$ by the Hasse-Weil theorem; that is $q \geq 79$.

It remains to deal with the case that $F(z)$ splits into linear factors over L. So P_0P meets $\mathscr{E}$ in two further points P_1, P_2 corresponding to the roots of $F(z)$. Choosing P_1, say, we define an automorphism $\phi: \mathscr{E} \to \mathscr{E}$, given by $P\phi = P_1$, which permutes the points on the lines through P_0; the choice of P_2 gives ϕ^{-1}. As ϕ permutes P, P_1, P_2, it has order 2 or 3. It cannot have order 2, as this would imply that ϕ has a fixed point on every line through P_0, which is impossible. So ϕ has order 3. Since ϕ has a fixed point on every line through P_0 tangent to $\mathscr{E}$, we can already conclude that $j(\mathscr{E}) = 0$ ([3], p. 321), proving the first part of the theorem.

Suppose now that $j(\mathscr{E}) = 0$. The equation of $\mathscr{E}$ can be put in the form $y^2 = x^3 + 1$ and its automorphisms fixing $(0,0)$ are given by $(x,y) \to (bx, cy)$, where $b = 1$, ω, or ω^2 with $\omega^2 + \omega + 1 = 0$ and $c = 1$ or -1. Let ϕ be as above and let $P_1 = O\phi$. Then $\psi = \phi - P_1$ fixes O. Note that P_0 is determined by P_1, since P_0 is collinear with P, $P\phi$, $P\phi^{-1}$ for all P in $\mathscr{E}$. Also

$$P + P\phi + P\phi^{-1} = O. \tag{5.1}$$

Now,

$$P\phi = P\psi + P_1. \tag{5.2}$$

Putting $P\phi^{-1}$ for P in (5.2) gives $P = P\phi^{-1}\psi + P_1$, whence

$$P\psi^{-1} = P\phi^{-1} + P_1\psi^{-1}, \tag{5.3}$$

Hence (5.1) gives

$$P + (P\psi + P_1) + (P\psi^{-1} - P_1\psi^{-1}) = O.$$

Finally, putting $P = O$ gives $P_1 = P_1\psi^{-1}$. As ψ can be taken as one of the above automorphisms with $b \neq 1$ so $P_1 = (0,1)$, $(0,-1)$ or the point at infinity on $x = 0$. So there are at most three choices for P_0.

Apart from the possibility of an elliptic curve $\mathscr{E}$ being a complete $(k;3)$-arc as in the theorem, it can also contain complete $(\frac{1}{2}k;2)$-arcs when k is even. In [22], the second author used a similar argument to that of Theorem 5.1 to prove this. However, the possibility that a certain quadratic polynomial might be reducible was overlooked. Exactly as in Theorem 5.1, the polynomial is irreducible if $j(\mathscr{E}) \neq 0$. So the main result of [22] should read as follows.

THEOREM 5.2. *If q is odd and $q \geq 301$, then an elliptic cubic curve $\mathscr{E}$ in $PG(2,q)$ with $j(\mathscr{E}) \neq 0$ and comprising $2k$ points contains a complete k-arc.*

6. Appendix

We give here an example of a $(k;3)$-arc in $PG(2,4)$ satisfying (E1), (E2), (E3) but not (E4).

Let l_1, l_2, l_3 be three lines in $PG(2,4)$ concurrent at P_0 and let P_1, P_2, P_3 be non-collinear points on l_1, l_2, l_3 respectively. The nine points on l_1, l_2, l_3 other than these four form a $(9;3)$-arc $\mathscr{K}$ with the following list of properties.

(1) $\mathscr{K} = \mathscr{K} \cup \{Q_1, Q_2, Q_3\}$, where $\mathscr{K}$ is a 6-arc and Q_1, Q_2, Q_3 are the three collinear points completing the $PG(2,2)$ containing P_0, P_1, P_2, P_3.

(2) The six points R_i, $i = 1, \ldots, 6$, of $\mathscr{K}$ can be regarded as a hexagon $\mathscr{K}'$ where each side of $\mathscr{K}'$ is a 2-secant of $\mathscr{K}$ and any bisecant of $\mathscr{K}$ which is not a side of $\mathscr{K}'$ contains some Q_i. If ρ_i is the number of i-secants of $\mathscr{K}$ through one of its points P, then

$$\rho_3 = 4, \rho_1 = 1 \quad \text{for } P = Q_i,\ i = 1,2,3;$$
$$\rho_3 = 3, \rho_2 = 2 \quad \text{for } P = R_i,\ i = 1, \ldots, 6;$$

(3) The only cubic curve containing $\mathscr{K}$ consists of the three lines l_1, l_2, l_3.

(4) With $\mathscr{K}' = R_1R_2R_3R_4R_5R_6$, choose $R_i\tau = R_iR_{i+1}$, where $R_7 = R_1$.

(5) $\mathscr{K}$ is not a group-arc.

Let l_1, l_2, l_3 have respective equations $x_1 = 0$, $x_2 = 0$, $x_1 = x_2$. Define P_i, Q_i, R_i as follows, where $\omega^2 + \omega + 1 = 0$:

$$P_0 = U_0, \quad P_1 = U_2, \quad P_2 = U_1, \quad P_3 = U,$$
$$Q_0 = \mathbf{P}(1,0,1), \quad Q_2 = \mathbf{P}(1,1,0), \quad Q_3 = \mathbf{P}(0,1,1),$$
$$R_1 = \mathbf{P}(\omega,0,1), \quad R_4 = \mathbf{P}(\omega^2,0,1),$$
$$R_2 = \mathbf{P}(\omega^2,1,0), \quad R_5 = \mathbf{P}(\omega,1,0),$$
$$R_3 = \mathbf{P}(\omega^2,1,1), \quad R_6 = \mathbf{P}(\omega,1,1).$$

The 3-secants of $\mathscr{K}$ other than $Q_1Q_2Q_3$ are

$$\begin{array}{ccccccccc} Q_1 & Q_1 & Q_1 & Q_2 & Q_2 & Q_2 & Q_3 & Q_3 & Q_3 \\ R_1 & R_2 & R_5 & R_2 & R_1 & R_4 & R_3 & R_1 & R_2 \\ R_4 & R_6 & R_3 & R_5 & R_3 & R_6 & R_6 & R_5 & R_4. \end{array}$$

Choose Q_1 as the zero of $\mathscr{K}$. Then

$$(R_1 + R_4) + R_2 = Q_1 + R_2 = R_2,$$
$$R_1 + (R_4 + R_2) = R_1 + Q_2 = R_5.$$

https://doi.org/10.1017/S1446788700030172 Published online by Cambridge University Press

So $\mathscr{K}$ satisfies (E1), (E2), (E3) but not (E4) and therefore cannot be contained in an irreducible cubic curve.

References

[1] J. Bierbrauer, 'Sets of maximal size in the plane of order eight', preprint.

[2] R. De Groote and J. W. P. Hirschfeld, 'The number of points on an elliptic cubic curve over a finite field', *European J. Combin.* **1** (1980), 327–333.

[3] R. Hartshorne, *Algebraic geometry* (Springer, 1977).

[4] J. W. P. Hirschfeld, *Projective geometries over finite fields* (Oxford University Press, 1979).

[5] J. W. P. Hirschfeld, 'Maximum sets in finite projective spaces', *Surveys in combinatorics*, pp. 55–76 (London Math. Soc. Lecture Note Series 82, 1983).

[6] J. W. P. Hirschfeld, *Finite projective spaces of three dimensions* (Oxford University Press, 1985).

[7] A. D. Keedwell, 'When is a (k, n)-arc of $PG(2, q)$ embeddable in a unique algebraic plane curve of order n?', *Rend Mat.* **12** (1979), 397–410.

[8] A. D. Keedwell, 'A theorem concerning the embedding of graphic arcs in algebraic plane curves', preprint.

[9] A. D. Keedwell, 'Simple constructions for elliptic cubic curves with specified small numbers of points', preprint.

[10] J. R. M. Mason, 'A class of $((p^n - p^m)(p^n - 1), p^n - p^m)$-arcs in $PG(2, p^n)$', *Geom. Dedicata* **15** (1984), 355–361.

[11] M. Oraee Yazdi, *The classification of $(k; 3)$-arcs over the Galois field of order five* (Thesis, University of Sussex, 1986).

[12] G. Raguso and L. Rella, 'Graphic arcs of order 5, 6 embeddable in algebraic plane curves of the same order', *Mitt. Math. Sem. Giessen* **166** (1984), 167–176.

[13] G. Raguso and L. Rella, 'On the graphic arcs embeddable in an algebraic plane curves', *Mitt. Math. Sem. Giessen* **169** (1985), 45–53.

[14] G. Raguso and L. Rella, 'Sugli archi grafici di ordine 3 di un piano di Galois di caratteristica 2', *Boll. Un. Mat. Ital.* **4-D** (1985), 161–166.

[15] R. J. Schoof, ' Nonsingular plane cubic curves over finite fields' *J. Combin. Theory, Ser. A* **46** (1987), 183–211.

[16] J.-P. Serre, *Nombres de points des courbes algébriques sur F_q*', Séminaire de Théorie des Nombres de Bordeaux, exposé no. 22, 1983).

[17] J.-P. Serre, 'Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini', *C. R. Acad. Sci. Paris Sér. I* **296** (1983), 397–402.

[18] K.-O. Stöhr and J. F. Voloch, 'Weierstrass points and curves over finite fields', *Proc. London Math. Soc.* **52** (1986), 1–19.

[19] M. Tallini Scafati, 'Graphic curves on a Galois plane', *Atti del Convegno di Geometria Combinatoria e sue Applicazioni*, Università di Perugia, 1970, pp. 413–419 (Università di Perugia, 1971).

[20] J. A. Thas, 'Elementary proofs of two fundamental theorems of B. Segre without using the Hasse-Weil theorem', *J. Combin. Theory Ser. A* **34** (1983), 381–384.

[21] J. A. Thas, 'Complete arcs and algebraic curves in $PG(2, q)$', preprint.

[22] J. F. Voloch, 'On the completeness of certain plane arcs', *European J. Combin.*, to appear.

[23] J. F. Voloch, 'Arcs in projective planes over prime fields', *J. Geom.*, to appear.
[24] W. G. Waterhouse, 'Abelian varieties over finite fields', *Ann. Sci. École Norm. Sup.* **2** (1969), 521–560.
[25] A. L. Yasin, *Cubic arcs in the projective plane of order eight* (Thesis, University of Sussex, 1986).

Mathematics Division
University of Sussex
Brighton BN1 9QH
United Kingdom

I.M.P.A.
Est. D. Castorina 110
Rio de Janeiro 22460
Brazil