GROUP-ARCS OF PRIME POWER ORDER ON CUBIC CURVES

J.W.P. Hirschfeld and J.F. Voloch

September 18, 2015

Abstract

This article continues the characterization of elliptic curves among sets in a finite plane which are met by lines in at most three points. The case treated here is that of sets of prime-power cardinality.

1 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
PQ	the line joining the points P and Q
$\ell(P,Q)$	PQ
$\langle P\rangle$	the group generated by P.

2 Introduction

This article continues the work of [5] in considering sufficient conditions for a set of points in a finite plane to be embedded in a cubic curve. Similar results to those in [5] were obtained independently by Ghinelli, Melone and Ott [1].

For completeness the main results in [5] need to be summarized.

Definition 2.1 *A $(k;n)$-arc in $PG(2,q)$ is a set of k points with at most n points on any line of the plane.*

The fundamental problem is to decide when a $(k;n)$-arc $\mathcal{K}_n$ lies on an absolutely irreducible algebraic curve $\mathcal{C}_n$ of degree n. Here we consider the problem for $n=3$.

A crucial point is the number of points $\mathcal{K}_3$ contains and the number of rational points on $\mathcal{C}_3$. Let $m_3(2,q)$ be the maximum number of points on $\mathcal{K}_3$. Then

$$m_3(2,q) \le 2q+1 \; for \; q>3, \tag{1}$$

[10], [2, p.331], and the exact values known are given in Table 1.

For $q=11$, $2q-1 \le m_3(2,q) \le 2q+1$.

q	2, 3	4, 5, 7	8, 9
$m_3(2,q)$	$2q+3$	$2q+1$	$2q-1$

Table 1: Values for $m_3(2,q)$

For an elliptic curve, $N_q(1)$ is the maximum number of points it can contain. Its value, for $q=p^h$ with p prime, is

$$N_q(1) = \begin{cases} q+[2\sqrt{q}] & \text{when } h \text{ is odd}, h \geq 3 \text{ and } p|[2\sqrt{q}] \\ q+1+[2\sqrt{q}] & \text{otherwise,} \end{cases}$$

where $[t]$ denotes the integer part of t, [12], [3, p. 273]. The precise values that are achieved by the number of points of an elliptic curve over $GF(q)$ are also known [12], as well as the number of isomorphism classes and the number of plane projective equivalence classes for a given value, [9]. For such a value the possible structures of the abelian group the points form is also known, [8], [11].

3 Axioms

Now, we recall the axioms imposed on a $(k;3)$-arc in [5], and then solve the main case unresolved there. For further motivation and details concerning the axioms, see [5, section 2].

Let $\mathcal{K}$ be a $(k;3)$-arc in $PG(2,q)$. Four axioms (E1) - (E4) are required. For each axiom, the property that it gives to $\mathcal{K}$ is mentioned in parentheses.
(E1) There exists O in $\mathcal{K}$ such that $\ell \cap \mathcal{K} = \{O\}$ for some line ℓ. (INFLEXION)
(E2) There exists an injective map $\tau : \mathcal{K}\backslash\{O\} \to PG^{(1)}(2,q)$ such that $P \in P\tau$ and $|P\tau \cap \mathcal{K}| \leq 2$, for all $P \in \mathcal{K}\backslash\{O\}$. (TANGENT)
(E3) If $P,Q \in \mathcal{K}$ and $PQ \neq P\tau$ or $Q\tau$, then $|PQ \cap \mathcal{K}| = 3$. (FEW BISECANTS)
(E4) For$P \in \mathcal{K}$, define $\overline{P}$ to be the third point of $\mathcal{K}$ on OP. For $P,Q \in \mathcal{K}$, define $P+Q=\overline{R}$, where R is the third point of $\mathcal{K}$ on PQ. Now, let $\mathcal{K}$ be an abelian group under the operation $+$ with identity O and $-P=\overline{P}$. (ABELIAN GROUP)

Definition 3.1 *A $(k;3)$-arc $\mathcal{K}$ satisfying (E1) - (E4) is called a group-arc or k-group-arc.*

It follows from the axioms that
(a) any subgroup of a group-arc is a group-arc,
(b) $P+Q+R=O$ if and only if P,Q,R are collinear.

Definition 3.2 *In $PG(2,q)$, the point set $\mathcal{S}$ is linearly determined by the set $\mathcal{T}$ of points and lines if every point of $\mathcal{S}$ is the intersection of two lines each of which is in $\mathcal{T}$ or is the join of two points of $\mathcal{T}$ or is the join of two points iteratively determined in this way.*

Lemma 3.3 *If P is a point of an arbitrary group-arc, then the cyclic group $\langle P\rangle$ is linearly determined by $\{O, \pm P, \pm 2P, 3P, (-2P)\tau\}$.*

Lemma 3.4 *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.*

Lemma 3.5 *Let $\mathcal{E}_1$ and $\mathcal{E}_2$ be cubic curves and $\mathcal{K}$ a k-group-arc which is a subgroup of both $\mathcal{E}_1$ and $\mathcal{E}_2$. If $k > 5$, then $\mathcal{E}_1 = \mathcal{E}_2$.*

Lemma 3.6 *Let $\mathcal{K}$ be a group-arc contained in a cubic curve $\mathcal{E}$ such that any cyclic subgroup of $\mathcal{K}$ is a subgroup of $\mathcal{E}$. Then $\mathcal{K}$ is a subgroup of $\mathcal{E}$.*

Theorem 3.7 *Let $\mathcal{K}$ be a k-group-arc in $PG(2, q)$ such that one of the following hold:*
(a) *$k = p_1p_2r$ where p_1 and p_2 are distinct primes ≥ 7;*
(b) *$k = 2^a3^b5^cp_1^d$, where p_1 is a prime ≥ 7, $d \geq 1$ and $2^a3^b5^c \geq 6$.*
Then $\mathcal{K}$ is a subgroup of the group of non-singular points of a cubic curve.

The theorem leaves the following values of k to be considered:
(i) $k = 2^a3^b5^c$, with $a, b, c \geq 0$; (ii) $k = ep_1^d$, with p_1 prime $\geq 7, d \geq 1, 1 \leq e \leq 5$.

In the next section we consider case (ii).

4 The main theorem

Lemma 4.1 *Suppose P, Q are elements of a group-arc $\mathcal{K}$ both of prime order $p_1 \neq 2, 3$ generating a subgroup G of order $(p_1)^2$. Then G is uniquely determined by*

$$O, \pm P, \pm Q, P \pm Q, 2P.$$

Proof: First,

$$\begin{aligned} -P - Q &= \ell(P, Q) \cap \ell(O, P + Q), \\ -P + Q &= \ell(P, -Q) \cap \ell(O, P - Q). \end{aligned}$$

Now assume, by induction on $m < p_1 - 1$, that we know

$$\pm(iP + Q), \pm iP$$

for $i = 0, \ldots, m$. This is true for $i = 1$. Now we determine these points for $i = m + 1$ as follows:

$$\begin{aligned} -(m+1)P - Q &= \ell(P, mP + Q) \cap \ell(2P, (m-1)P + Q), \\ (m+1)P + Q &= \ell(-P, -mP - Q) \cap \ell(O, -(m+1)P - Q), \\ (m+1)P &= \ell(-P, -mP) \cap \ell(Q, -(m+1)P - Q), \\ -(m+1)P &= \ell(P, mP) \cap \ell(O, (m+1)P). \end{aligned}$$

The last equality works providing the two lines are distinct; that is, providing $(m+1)P \neq O$ or $(2m+2)P \neq O$. However, the first is true since otherwise the induction would have been finished at the previous step.

In particular, $\langle P \rangle$ has been determined. Now $\langle P_1 \rangle$, where $P_1 = P + Q$, is found. From the previous step,

$$O, \pm P_1, \pm Q, P_1 \pm Q, 2P_1$$

are required. Of these, the only ones lacking are $P_1 + Q$ and $2P_1$. These are determined as follows:

$$\begin{array}{rcccl} P_1 + Q & = & P + 2Q & = & \ell(-P-Q,-Q) \cap \ell(-2P-Q, P-Q), \\ 2P_1 & = & 2P + 2Q & = & \ell(-2P-Q,-Q) \cap \ell(-3P-Q, P-Q). \end{array}$$

Now, with P_1 instead of P, we can determine $\langle P_2 \rangle$, where $P_2 = P_1 + Q = P + 2Q$. Continuing this process, $\langle P + mQ \rangle$ for $m = 0, 1, ..., p_1 - 1$ can be determined. To complete the proof, only $\langle Q \rangle$ needs to be found. By reversing the initial roles of P and Q, we require

$$O, \pm P, \pm Q, Q \pm P, 2Q.$$

Of these, only $2Q$ is missing; this is given by

$$2Q = \ell(P, -P-2Q) \cap \ell(-P, P-2Q).$$

Corollary 4.2 *A group-arc $\mathcal{K}$ isomorphic to $(\mathbf{Z}_{p_1})^2, p_1 \geq 5$, is a subgroup of a unique cubic curve.*

Proof: Given $O, \pm P, \pm Q, P \pm Q, 2P$, where $\mathcal{K} = \langle P \rangle \oplus \langle Q \rangle$, the conditions that a cubic passes through these points and has an inflexion at O are nine independent conditions and determine the cubic uniquely.

Theorem 4.3 *Let $\mathcal{K}$ be a k-group-arc in $PG(2, q)$ such that k is divisible by a prime $p_1 \geq 7$. Then $\mathcal{K}$ is a subgroup of a unique cubic curve.*

Proof: By Theorem 3.7, it suffices to consider the case that $k = ep_1^d$ with $1 \leq e \leq 5$.

Consider first the case that the p_1-Sylow subgroup $\mathcal{P}_1$ of $\mathcal{K}$ is cyclic so that $\mathcal{P}_1 = \langle P_1 \rangle$. Now, $\mathcal{K} = \mathcal{P}_1 \oplus G$, where $|G| = e$ and $|\mathcal{P}_1| = p_1^d$. As $\mathcal{P}_1$ is cyclic it is contained in a cubic curve $\mathcal{E}_1$. For any point P in $\mathcal{P}_1$, the subgroup $\langle P \rangle$ is contained in a cubic curve $\mathcal{E}$, which coincides with $\mathcal{E}_1$ by Lemma 3.5. If Q is any point of $\mathcal{K}$, then $Q = P + R$ for some $P \in \mathcal{P}_1$ and $R \in G$. By Lemma 3.4, $\langle Q \rangle$ is contained in an cubic curve $\mathcal{E}'$; also, since the orders of P and R are coprime, $\langle Q \rangle$ contains both $\langle P \rangle$ and $\langle R \rangle$. Again, by Lemma 3.5, $\mathcal{E}' = \mathcal{E}_1$. Hence $\mathcal{K} \subset \mathcal{E}_1$.

Now consider the non-cyclic case and let $\mathcal{K}_1 \subset \mathcal{K}$ with $\mathcal{K}_1$ isomorphic to $(\mathbf{Z}_{p_1})^2$. Then, by the previous corollary, $\mathcal{K}_1$ is contained in a cubic $\mathcal{E}$. As in the previous case, $\mathcal{K} = \mathcal{K}_0 \oplus G$ where $|G| = e$ and $|\mathcal{K}_0| = p_1^d$. If P in $\mathcal{K}_0 \backslash \mathcal{K}_1$ has order p_1^λ, then $\langle P \rangle$ is contained in a cubic $\mathcal{E}'$ and, for $Q \in \mathcal{K}_1 \backslash \{O\}$, the sum $\langle p_1^{\lambda-1} P \rangle \oplus \langle Q \rangle$ is contained in a cubic $\mathcal{E}''$. Now $\mathcal{E}'' \cap \mathcal{E} \supset \langle Q \rangle$, whence $\mathcal{E}'' = \mathcal{E}$ by Lemma 3.5. Also, $\mathcal{E}' \cap \mathcal{E}'' \supset \langle p_1^{\lambda-1} P \rangle$ and so $\mathcal{E}' = \mathcal{E}''$. Hence $\mathcal{E} = \mathcal{E}'$ and therefore $\mathcal{K}_0 \subset \mathcal{E}$.

Now, let $R \in G$. Then there is a cubic $\mathcal{E}'''$ containing $\langle R + Q \rangle$. As $e(R + Q) = eQ \in \mathcal{E}$ and $eQ \neq O$, so $\langle eQ \rangle = \langle Q \rangle$ and $\mathcal{E}''' \cap \mathcal{E} \supset \langle Q \rangle$. Therefore $\mathcal{E}''' = \mathcal{E}$ by Lemma 3.5 and $\langle R + Q \rangle \subset \mathcal{E}$, whence $p_1(R + Q) = p_1 R \in \mathcal{E}$. So $R \in \mathcal{E}$. It has now been shown that both G and $\mathcal{K}_0$ lie in $\mathcal{E}$, whence $\mathcal{K} \subset \mathcal{E}$.

5 Small cases

I. k = 8

Lemma 5.1 *An 8-group-arc $\mathcal{K}$ isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ exists in $PG(2,q)$ if and only if $q = 2^h, h \geq 3$. Such a group-arc lies on a unique cuspidal cubic.*

Proof: Let $O = \mathbf{P}(1,0,0), P = \mathbf{P}(0,1,0), Q = \mathbf{P}(0,0,1), R = \mathbf{P}(1,1,1)$ be points of $\mathcal{K}$. Then

$$\begin{aligned} R+Q &= \mathbf{P}(t,t,1), t \neq 0,1; \\ P+R &= \mathbf{P}(1,s,1), s \neq 1. \end{aligned}$$

Also

$$\begin{aligned} P+Q &= \ell(P,Q) \cap \ell(Q+R, P+R) &= \mathbf{P}(0, t-ts, 1-t); \\ P+Q+R &= \ell(P+R, Q) \cap \ell(P, Q+R) &= \mathbf{P}(1, s, t^{-1}). \end{aligned}$$

Now, $P+Q+R \in \ell(P+Q, R) \Rightarrow$

$$\begin{vmatrix} 1 & 1 & 1 \\ 0 & t-ts & 1-t \\ 1 & s & t \end{vmatrix} = 0$$

$\Rightarrow 1 - s + 1 - t - (t - ts) - s(1-t) = 0$
$\Rightarrow 2(1-s)(1-t) = 0$
$\Rightarrow 2 = 0.$

Since O is on none of the lines

$$\ell(Q, P+R), \ell(R+Q, P+R), \ell(P+Q, P+Q+R),$$

it follows that $s \neq 0, s \neq t, s \neq t^{-1}$; hence $q > 4$. Also the 7 points of $\mathcal{K}\backslash\{O\}$ form a $PG(2,2)$. The 8 points lie on the unique cubic $\mathcal{C}$ with equation

$$(s+1)x^2y + s(t+1)x^2z + (t+1)y^2z + t(s+1)yz^2 = 0.$$

This is irreducible when $(s+t)(st+1) \neq 0$, which is satisfied in this case. It has a cusp at $\mathbf{P}(\sqrt{t}, \sqrt{st}, 1)$ and all tangents to $\mathcal{C}$ are concurrent at O.

For more on cuspidal cubics, see [2, section 11.3].

Lemma 5.2 *An 8-group-arc $\mathcal{K}$ isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_4$ exists in $PG(2,q)$ if and only if q is odd with $q \geq 5$. Such a group-arc lies on a unique cubic curve, which is elliptic.*

Proof: The eight points of $\mathcal{K}$ written as elements of $\mathbf{Z}_2 \times \mathbf{Z}_4$ are

$O = (0,0), P_1 = (0,2), P_2 = (1,0), P_3 = (1,2), Q_1 = (0,1), Q_2 = (0,3), Q_3 = (1,1), Q_4 = (1,3).$

Hence

$$2P_1 = 2P_2 = 2P_3 = O,\ P_1 + P_2 + P_3 = O,\ 2Q_1 = 2Q_2 = 2Q_3 = 2Q_4 = P_1.$$

So P_1, P_2, P_3 are the points of contact of the tangents through O, and Q_1, Q_2, Q_3, Q_4 the points of contact of the tangents through P_1.

Let $O = \mathbf{P}(0,0,1)$ with tangent $y = 0$. Let $P_1 = \mathbf{P}(0,1,0), P_2 = \mathbf{P}(1,1,1), P_3 = \mathbf{P}(\alpha,1,\alpha)$ with respective tangents $x = 0, x = y, x = \alpha y$; so $\alpha \neq 0, 1$. Then, if $\mathcal{K}$ lies on the cubic curve $\mathcal{E}$, consider the intersection divisors in which $\mathcal{E}$ meets the two curves with equations

$$y(x-z)^2 = 0 \text{ and } x(x-y)(x-\alpha y) = 0.$$

In both cases the divisor is

$$O \oplus O \oplus O \oplus P_1 \oplus P_1 \oplus P_2 \oplus P_2 \oplus P_3 \oplus P_3,$$

where $\oplus$ has been used to denote the formal sum to distinguish it from the sum on a cubic curve elsewhere in this paper. So $\mathcal{E}$ has equation

$$y(x-z)^2 + \lambda x(x-y)(x-\alpha y) = 0. \tag{2}$$

The common points of a line $z = tx$ through P_1 and $\mathcal{C}$ are determined by

$$(1-t)^2 x^2 y + \lambda x(x-y)(x-\alpha y) = 0; \tag{3}$$

that is, apart from P_1 , the points defined by

$$\lambda x^2 + xy\{(1-t)^2 - \lambda(1+\alpha)\} + \lambda\alpha y^2 = 0. \tag{4}$$

Since there are four tangents through P_1 , so q is odd. For a tangent, the discriminant $\Delta = 0$. Here

$$\Delta = \{(1-t)^2 - \lambda(1+\lambda)\}^2 - 4\lambda^2\alpha = (1-t)^4 - 2\lambda(1+\alpha)(1-t)^2 + \lambda^2(1-\alpha^2).$$

Since $\Delta = 0$ has four solutions for t, so the discriminant Δ' of Δ considered as a quadratic in $(1-t)^2$ is a square. Now,

$$\Delta' = \lambda^2(1+\alpha)^2 - \lambda^2(1-\alpha)^2 4\lambda^2\alpha.$$

Hence $\alpha = \beta^2$; this incidentally means that $GF(q)$ contains a square other than 0 and 1, whence $q \neq 3$. Solving $\Delta = 0$ for $(1-t)^2$ gives

$$(1-t)^2 = \lambda(1+\beta^2) \pm 2\lambda\beta = \lambda(1 \pm \beta)^2.$$

Hence $\lambda = \gamma^2$. Thus

$$1 - t = \pm\gamma(1 \pm \beta).$$

Therefore, (4) becomes $(x \pm \beta y)^2 = 0$. This gives for Q_1, Q_2, Q_3, Q_4 the points

$$\mathbf{P}(e\beta, 1, e\beta + f\beta\gamma - ef\beta^2\gamma)$$

where $e, f = \pm 1$. Also $\mathcal{C}$ has equation

$$y(x-z)^2 + \gamma^2 x(x-y)(x-\beta^2 y) = 0,$$

which is elliptic.

For the calculation of the equations of cubic curves with a precise number of points, see also [4], [6], [7].

II. k = 25

Each case not covered in this paper can be reduced to a finite calculation. An arbitrary group-arc $\mathcal{K}$ of a given order is given by a set of points, where some of the coordinates are elements of $GF(q)$ and some are indeterminates. The necessary collinearities are given by a set of polynomial equations in the indeterminates. An algebraic manipulation programme can then determine the consistency of these equations, and check whether or not $\mathcal{K}$ lies on a cubic curve. For example, A. Simis (personal communication) has verified that if $\mathcal{K}$ is isomorphic to $(\mathbf{Z}_5)^2$, then this works, as one expects from Corollary 4.2.

References

[1] Ghinelli, D., Melone, N. and Ott, U. (1989) On abelian cubic arcs, *Geom. Dedicata* **32**, 31-52.

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

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

[4] Hirschfeld, J.W.P. and Thas, J.A. (1990) Sets with more than one representation as an algebraic curve of degree three. *Finite Geometries and Combinatorial Designs*, American Mathematical Society, Providence, pp. 99-110.

[5] Hirschfeld, J.W.P. and Voloch, J.F. (1988) The characterization of elliptic curves over finite fields, *J. Austral. Math. Soc. Ser. A* **45**, 275-286.

[6] Keedwell, A. (1988) Simple constructions for elliptic cubic curves with specified small numbers of points, *European J. Combin.* **9**, 463-481.

[7] Keedwell, A. (1991) More simple constructions for elliptic cubic curves with small numbers of points, preprint.

[8] Rück, H.-G. (1987) A note on elliptic curves over finite fields, *Math. Comput.* **49**, 301-304.

[9] Schoof, R. (1987) Non-singular plane cubic curves over finite fields, *J. Combin. Theory Ser. A* **46**, 183-211.

[10] Thas, J.A. (1975) Some results concerning $\{(q+1)(n-1);n\}$-arcs and $\{(q+1)(n-1)+1;n\}$-arcs in finite projective planes of order q, *J. Combin. Theory Ser. A* **19**, 228-232.

[11] Voloch, J.F. (1988) A note on elliptic curves over finite fields, *Bull. Soc. Math. France* **116**, 455-458.

[12] Waterhouse, W.G. (1969) Abelian varieties over finite fields, *Ann. Sci. Ecole Norm. Sup.* **2**, 521-560.

School of Mathematical and Physical Sciences
University of Sussex
Brighton BN1 9QH
United Kindom

Department of Mathematics
University of Texas at Austin
Austin
TX 78712
U S A