Complete arcs in Galois planes of non-square order

J. F. Voloch
I.M.P.A., Rio de Janeiro

1. Introduction

Let $PG(2, q)$ be the projective plane over the field $GF(q)$ of q elements. A k-arc $K \subseteq PG(2, q)$ is a set of k points, no three of which are collinear. A k-arc is called complete if it is not contained in a $(k + 1)$-arc. It was first shown by Bose (see Hirschfeld (1979) Theorem 8.13) that a k-arc satisfies $k \leq q + 2$ if q is even and $k \leq q + 1$ if q is odd. Both bounds are sharp and arcs attaining these bounds are called ovals. A celebrated theorem of Segre (see Hirschfeld (1979) Theorem 8.24) states that, for q odd, an oval is a conic.

A fundamental quantity in the geometry of projective spaces over finite fields is the cardinality of the second largest complete arc in $PG(2, q)$ denoted by $m'(2, q)$. Equivalently one can define $m'(2, q)$ as being the smallest k_0 such that, if $k > k_0$, a k-arc is contained in an oval. The value of $m'(2, q)$ is not only important in the geometry of the plane, but also is a basic quantity in bounds for the sizes of arcs and caps in higher dimensional spaces (see Hirschfeld (1983, 1985); Hirschfeld and Thas (1987, 1991); Thas (1968)).

The basic result on $m'(2, q)$ is the following bounds, due to Segre:

$$m'(2, q) \leq q - \sqrt{(q)} + 1, \quad q \text{ even}; \tag{1}$$

$$m'(2, q) \leq q - \sqrt{(q)}/4 + 7/4, \quad q \text{ odd}. \tag{2}$$

(See Hirschfeld (1979), Theorem 10.3.3 for (1) and Theorem 10.4.4 for (2)). Segre's method of proof of these inequalities consists of associating to an arc an algebraic curve over $GF(q)$ with many rational points and then using Weil's Theorem (1948) to get an upper bound on the number of points of the algebraic curve. Thas (1983, 1987) has given an alternative approach to (1) and (2), bounding the points on the algebraic curve by using Bézout's theorem only, for q even, and the Plücker formulæ, for q odd. Thas sometimes obtains improvements to (1) or (2) but his bounds differ from (1) or (2) at most by two.

In the opposite direction, when q is a square, there exist complete k-arcs for $k = q - \sqrt{(q)} + 1$, Fisher et. al. (1986). Thus (1) is sharp when q is a square. When q is not a square, the situation is completely different. The author has shown (1990) that, for q an odd prime, $m'(2, q) \leq 44q/45 + 2$. It is the purpose of this paper to substantially improve the bounds (1) and (2) for an arbitrary non-square q, in

Theorems 1 and 2 below. Note that, for q not a square, the best lower bound for $m'(2, q)$, is at present $(q + 1)/2 + \sqrt{(q)}$, which follows from the results of Voloch (1987).

The author would like to thank James Hirschfeld for his interest in this work.

2. Bounds for the number of rational points on curves

To bound the number of rational points of algebraic curves defined over finite fields we will use the following result of Stöhr and Voloch (1986).

Theorem 1. *If $X \subseteq PG(n, q)$ is an irreducible curve of degree d, genus g, not contained in any hyperplane and with Frobenius orders $\nu_0, \ldots, \nu_{n-1}$, then the number N of $GF(q)$-rational points of X satisfies*

$$N \leq [(\nu_0 + \ldots + \nu_{n-1})(2g - 2) + d(q + n)]/n .$$

The Frobenius orders $0 = \nu_0 < \ldots < \nu_{n-1}$ is a certain well defined subset of the order sequence $0 = \varepsilon_0 < \ldots < \varepsilon_n$ of X, defined as the possible intersection multiplicities of X with hyperplanes at a generic point of X; see Stöhr and Voloch (1986) for more details.

Let us consider a plane curve X of degree d. Then

$$N \leq [\nu_1(2g - 2) + d(q + 2)]/2. \tag{3}$$

Note also that $\nu_1 = \varepsilon_1 = 1$ or $\nu_1 = \varepsilon_2$. We have that ε_2 is the order of contact of X with its tangent at a generic point and so $\varepsilon_2 \leq d$. Also, $\varepsilon_2 = 2$ or a power of the characteristic p (as follows from Garcia and Voloch (1987) Proposition 2). When $p = 2$ we conclude that ν_1 is a power of 2 and $\nu_1 \leq d$. This will be used in § 3.

The plane curve X of degree d can be embedded in $PG(5, q)$ as a curve of degree $2d$ not contained in a hyperplane by the Veronese embedding $PG(2, q) \to PG(5, q)$, given by

$$(x_0 : x_1 : x_2) \mapsto (x_0x_1 : x_0x_2 : x_1x_2 : x_0^2 : x_1^2 : x_2^2).$$

It follows that

$$N \leq [(\nu_1 + \nu_2 + \nu_3 + \nu_4)(2g - 2) + 2d(q + 5)]/5. \tag{4}$$

Suppose that X, as a plane curve, is classical (that is, has order sequence 0, 1, 2). Then the orders of X in 5-space are 0, 1, 2, 3, 4, ε_5 for some $\varepsilon_5 \leq 2d$ (see Garcia and Voloch (1987) p.464). If $p \neq 2, 3$ then, by

Garcia and Voloch (1987), Proposition 2, $\varepsilon_5 = 5$ or ε_5 is a power of p. When $p = 2, 3$ then $\varepsilon_5 = 6$ is the only other possibility. Suppose now that X has a rational point P so that X meets its tangent at P with multiplicity exactly 2 at P. Then the orders at P of X in 5-space begin with 0, 1, 2, 3, 4 and it follows from Stöhr and Voloch (1986) Corollary 2.6 that $\nu_i = i$, $i \leq 3$. Thus $\nu_4 = 4$ or ε_5.

3. q even

Let q be even.

To prove his result on $m'(2, q)$, Segre showed that, with $t = q + 2 - k$, the kt unisecants to a k-arc $K \subseteq PG(2, q)$ lie, in the dual projective plane, on an algebraic curve C of degree t. (See Hirschfeld (1979) Theorem 10.3.1). Note that, given P in K, the line P^{ν} in the dual plane will intersect C in the t unisecants of K through P. It follows readily from this that the unisecants of K are simple points of C and that an irreducible component X of C of degree d contains at least kd unisecants to K. Segre then applied Weil's Theorem (1948) to X to conclude that $m'(2, q) \leq q - \sqrt{(q)} + 1$. To improve on Segre's result when q is not a square we will apply instead the results of §2.

Theorem 2. *If $q \neq 2$ is even and not a square, then*

$$m'(2, q) \leq q - \sqrt{(2q)} + 2.$$

Proof. As above, we obtain for a k-arc K, an irreducible algebraic curve X of degree $d \leq t = q + 2 - k$ containing kd unisecants to K. If $k = m'(2, q)$ and K is complete, then $d \geq 2$ (as in the proof of Theorem 10.3.3 of Hirschfeld (1979)). If X is not defined over $GF(q)$, then by Hirschfeld (1979) Lemma 10.1.1, $kd \leq d^2$. So $k \leq d \leq t = q + 2 - k$; that is, $k \leq (q + 2)/2 \leq q - \sqrt{(2q)} + 2$.

If X is of degree $d \geq 2$ and is defined over $GF(q)$, then (3) of §2 is valid. Therefore

$$kd \leq [(\nu_1(2g - 2) + d(q + 2)]/2 \leq d\,[\nu_1(d - 3) + q + 2]/2.$$

Hence

$$2k \leq \nu_1(d - 3) + q + 2 \leq \nu_1(t - 3) + q + 2$$

and, since $k = q + 2 - t$,

$$t \geq \frac{q+2+3\nu_1}{\nu_1+2}.$$

If $\nu_1 \leq \sqrt{(q/2)}$, then, for $q \neq 8$,

$$t \geq \frac{2(q+2)+3\sqrt{(2q)}}{\sqrt{(2q)}+4} > \left[\frac{2(q+2)+3\sqrt{(2q)}}{\sqrt{(2q)}+4}\right] = \sqrt{(2q)} - 1.$$

Therefore,

$$k = q + 2 - t < q + 3 - \sqrt{(2q)}.$$

As $\sqrt{(2q)}$ is an integer, we get the theorem in this case.

Recall that, as remarked in §2, $\nu_1 \leq d \leq t$ and is a power of 2. Thus if $\nu_1 > \sqrt{(q/2)}$ then $\sqrt{(2q)} \leq \nu_1 \leq t$, whence $k \leq q + 2 - \sqrt{(2q)}$, as was to be proved.

For $q = 8$, the bound in the theorem is sharp, as the only complete arcs other than ovals are 6-arcs (Hirschfeld (1979), Theorem 9.2.5).

4. q odd

In this section q is odd.

Similarly to the case q even, a k-arc K in $PG(2, q)$, q odd, has its kt unisecants ($t = q + 2 - k$) lying, in the dual plane, on an algebraic curve C. Differently from the case q even, this time C has degree $2t$ and for each P in K, the line P^{ν} meets C with a multiplicity two at each of the t unisecants of K through P (Hirschfeld (1979), Theorem 10.4.1). Again we will use the results of Stöhr and Voloch (1986) presented in §2, instead of Weil's results, to improve on Segre's bound. When q is prime, this was already done in Voloch (1990).

Theorem 3. *Let q be odd, not a square or a prime. Then, if q is a power of the prime p,*

$$m'(2, q) \leq q - \sqrt{(pq)}/4 + 29p/16 + 1.$$

Proof. Let K be a complete k-arc in $PG(2, q)$, q odd, not a square, $k = m'(2, q)$. Let X be an irreducible component of the curve C constructed above. It follows from the argument in Voloch (1990) that

$$k \leq 44q/45 + 2 \leq q - \sqrt{(pq)}/4 + 29p/16 + 1,$$

unless X is degree $d \geq 3$ defined over $GF(q)$ and with the Veronese embedding of X in $PG(5, q)$ having $\nu_4 > 4$. Suppose that we are in this last case. If the $kd/2$ unisecants of K which are in X are double points of X, then

$$kd/2 \leq (d-1)(d-2)/2 \leq d^2/2;$$

so $k \leq d \leq 2t$, and hence $k \leq 2(q+2)/3 \leq 44q/45 + 2$, as desired. Otherwise, X has a point, corresponding to a unisecant ℓ to K through P in K, which is simple, and therefore, P^{ν} meets X at ℓ with multiplicity two. It follows from the discussion in §2 that $X \subseteq PG(5, q)$ has order sequence $0, 1, 2, 3, 4, \varepsilon_5 \leq 2d$ and Frobenius orders $0, 1, 2, 3, \varepsilon_5$. Finally ε_5 is a power of p unless $p = 3$ and $\varepsilon_5 = 6$. From (4) and the argument in Voloch (1990) it follows that

$$kd/2 \leq [(\varepsilon_5 + 6)\, d(d-3) + 2d(q+5)]/5\,.$$

Hence

$$k \leq 2/5[(\varepsilon_5 + 6)(d-3) + 2(q+5)] \leq 2/5[(\varepsilon_5 + 6)(2t-3) + 2(q+5)].$$

As $k = q + 2 - t$, it follows that

$$t \geq \frac{q}{4\varepsilon_5 + 29} + \frac{6\varepsilon_5 + 26}{4\varepsilon_5 + 29} \geq \frac{q}{4\varepsilon_5 + 29} + 1. \tag{5}$$

Write $q = p^{2h+1}$, $h \geq 1$. If $\varepsilon_5 \geq p^{h+1}$ then, as $\varepsilon_5 \leq 2d \leq 4t$, it follows that $k \leq q + 2 - p^{h+1}/4$ and the theorem is proved. Suppose now that $\varepsilon_5 < p^{h+1}$. If $p \neq 3$ then ε_5 is a power of p; so $\varepsilon_5 \leq p^h$ and, from (5), $t \geq q/(4p^h + 29) + 1$, which proves the theorem. If $p = 3$, the same argument gives the result unless $\varepsilon_5 = 6$, which also satisfies $\varepsilon_5 \leq p^h$ unless $h = 1$, that is, $q = 27$. However, the result is trivially true for $q = 27$.

References

J. C. Fisher, J.W.P. Hirschfeld and J. A. Thas (1986), Complete arcs in planes of square order, *Ann. Discrete Math.* **30**, 243-250.

A. Garcia and J. F. Voloch (1987), Wronskians and linear independence in fields of prime characteristic, *Manuscripta Math.* **59**, 457-469.

J. W. P. Hirschfeld (1979), *Projective Geometries over Finite Fields*, Oxford University Press, Oxford.

J. W. P. Hirschfeld (1983), Caps in elliptic quadrics, *Ann. Discrete Math.* **18**, 449-466.
J. W. P. Hirschfeld (1985), *Finite Projective Spaces of Three Dimensions* , Oxford University Press, Oxford.
J. W. P. Hirschfeld and J. A. Thas (1987), Linear independence in finite spaces, *Geom. Dedicata* **23**, 15-31.
J. W. P. Hirschfeld and J. A. Thas (1991), *General Galois Geometries*, Oxford University Press, Oxford, to appear.
K. O. Stöhr and J. F. Voloch (1986), Weierstrass points and curves over finite fields, *Proc. London Math. Soc.* **52**, 1-19.
J. A. Thas (1968), Normal rational curves and k-arcs in Galois spaces, *Rend. Mat.* **1**, 331-334.
J. A. Thas (1983), Elementary proofs of two fundamental theorems of B. Segre without using the Hasse-Weil theorem, *J. Combin. Theory Ser. A* **34**, 381-384.
J. A. Thas (1987), Complete arcs and algebraic curves in $PG(2, q)$, *J. Algebra* **106**, 457-464.
J. F. Voloch (1987), On the completeness of certain plane arcs, *European J. Combin.* **8**, 453-456.
J. F. Voloch (1990), Arcs in projective planes over prime fields, *J. Geom.* **38**, 198-200.
A. Weil (1948), *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Hermann, Paris.