Complete arcs arising from conics and cubics

G. Korchmáros

The first natural question for k-arcs in $PG(2,q)$ is if there exist complete k-arcs in $PG(2,q)$ other than conics for q odd, and hyperconics for q even.

Theorem 1 *(L. Lombardo-Radice) In $PG(2,q), q \equiv -1 \mod 4$, there exists a complete k-arc with $k = (q+5)/2$.*

Proof. Assume $q \geq 7$. Let α be a primitive element of $GF(q)$. The non-zero elements of $GF(q)$ fall into two subsets,

$$S = \{\alpha^{2i} \mid i = 0, 1, \ldots, (q-1)/2\};$$

$$N = \{\alpha^{2i+1} \mid i = 0, 1, \ldots, (q-1)/2\},$$

namely, S is the subset of squares and N is the subset of non-squares. Let C be the conic with equation $XY = 1$. The $q-1$ affine points of C fall into two branches S and N, where $\mathcal{S} = \{P(x, x^{-1}) : x \in S\}$, and $\mathcal{N} = \{P(x, x^{-1}) : x \in N\}$. The points $P(x, x^{-1})$ and $Q(-x, -x^{-1})$ belong to different branches if and only if -1 is a non-square; that is $q \equiv -1 (\mathrm{mod}\ 4)$. So, for these q, let $K = \mathcal{S} \cup \{O, X_\infty, Y_\infty\}$. Clearly K is a $(q+5)/2$-arc. It remains to show that the bisecants of K fill the affine plane. The X-axis, the Y-axis, and the infinite line are bisecants of K. The bisecants other than the X-axis and the Y-axis through O have equation $Y = mX$, with $m \in S$, and hence they cover all the affine points of C. Now, let $P(a,b)$ be a point on none of these bisecants of K. Then $ba^{-1} \in N$, and hence either a or b is in S. If $a \in S$, then $P(a, a^{-1}) \in K$, and the vertical line through P is a bisecant of K, and the same holds for $b \in S$ and the horizontal line through P. So K is complete. In a similar way, $\mathcal{N}$ may be chosen instead of $\mathcal{S}$ to obtain the complete arc $L = \mathcal{N} \cup \{O, X_\infty, Y_\infty\}$. A comparable result for q even is

Theorem 2 *(B. Segre) In $PG(2,q)$, q even and $q \geq 8$, there exists a complete k-arc with $k = (q+4)/2$.*

The above constructions suggest a quite easy way to obtain k-arcs containing approximately half the points of a conic: Choose a point r outside the conic, and one of the two points on each chord through r (for q even, and for

q odd when r is an external point, add to them the tangency point(s) of the tangent(s) from r). Clearly, $k = (q+3)/2$ or $k = (q+5)/2$, or $k = (q+2)/2$, according as q is odd, r is an internal or external point, or q is even.

It may happen that such a k-arc is not complete, and it is not clear at all how to find those points which can be added to it. Various methods depending on group theory, algebraic geometry and some properties of Galois fields have been used in investigating the completeness of such arcs, see [3, Section 9]. The following result is taken from [4]:

Theorem 3 *In $PG(2,q)$, with $(q+1)/2$ an odd prime and $q^2 \not\equiv 1 \pmod{16}$, every k–arc sharing $(q+3)/2$ points with a conic contains at most two further points.*

Remark. If $(q+1)/2$ is an odd prime, then either q is prime or $q = p^d$ with d a power of 2.

Proof. Given a set $\mathcal{U}$ of $(q+3)/2$ points on a conic C, assume that P and Q are two (external) points to C such that $\mathcal{U} \cup \{\mathcal{P}, \mathcal{Q}\}$ is a $(q+7)/2$–arc. Then the line ℓ through P and Q is disjoint from C. Let L denote the pole of ℓ with respect to C. Note that L is an internal point to C.

For every point $A \in C$, let $L(A)$ denote the second common point of the line LA with C. Assume now that $(q+1)/2$ is a prime number. Then, $U \in \mathcal{U}$ if and only if $L(U) \in \mathcal{U}$. This shows that Φ_L preserves $\mathcal{U}$ where Φ_L is the involutory homology with center L which leaves C invariant.

To prove Theorem 3, assume that a further point R can be added to the $(q+7)/2$–arc $\mathcal{U} \cup \{\mathcal{P}, \mathcal{Q}\}$. Let S be the pole of the line PR, and T the pole of QR. Then both Φ_S and Φ_T preserve $\mathcal{U}$.

Let G be the group generated by Φ_L, Φ_S, Φ_T. This group preserves $\mathcal{U}$. From the classification of all the subgroups of $PGL(2,q)$, either $G = PGL(2,q)$, or G is a dihedral group of order m with $m \mid 2(q-1), 2(q+1)$, or $G \cong S_4$ and $q^2 \not\equiv 1 \pmod{16}$. Since G fixes $\mathcal{U}$ and $\mathcal{U}$ is a proper subset of C, we see that $G \neq PGL(2,q)$.

To show that G is not a dihedral group, we recall first a well known property of dihedral groups: Each dihedral group D_n of order $2n$ contains a coset of size n comprising involutory elements, and D_n has a further involutory element if and only if n is even (in this case this involutory element is central in D_n). In particular, if D_n is a collineation group fixing a conic, then the centers of the involutory elements (which are homologies since q is odd) in the coset are collinear, and the pole of the line $\ell(D_n)$ containing them is the center of the (eventually) central involution in D_n. This shows that if D_n contains three pairwise non commutative involutions, then their centers are not collinear. In our case, the line LT is the pole of P, and hence LT is a chord of C. If Φ_L and Φ_T were commuting then $\Phi_L \cdot \Phi_T$ would be Φ_P, and hence Φ_P would fix $\mathcal{U}$, but we know that Φ_P does not. Similarly for the pairs $\{\Phi_L, \Phi_S\}$, and $\{\Phi_S, \Phi_T\}$, whence the claim follows.

It only remains to consider the third possibility. Here, we restrict ourselves to show that if $G \cong S_4$ then no more than four points can be added to $\mathcal{U}$ in order to extend $\mathcal{U}$ to a complete arc in $PG(2,q)$. Assume that A is a point such that $\mathcal{U} \cup \{\mathcal{P}, \mathcal{Q}, \mathcal{R}, \mathcal{A}\}$ is a $\left(\frac{1}{2}(q+3)+4\right)$–arc in $PG(2,q)$. Then the four points P, Q, R, A added to $\mathcal{U}$ form six pairs (i.e., six pairwise distinct external lines to C). The corresponding six poles L, S, T, D, E, F define six pairwise distinct involutory homologies in G. Their centers are all internal points to C, because $q^2 \not\equiv 1 \pmod{16}$. Since G contains exactly six non-central involutions, no further point B can exist such that $\mathcal{U} \cup \{\mathcal{P}, \mathcal{Q}, \mathcal{R}, \mathcal{A}, \mathcal{B}\}$ is an arc.

It is still an open question to decide for what values of q this situation can actually occur (apart from the case $q = 13$, already investigated in a recent paper (A. H. Ali, J. W. P. Hirschfeld, H. Kaneta: *The automorphism group of a complete* $(q-1)$*–arc in* PG(2, q), Journal of Combinatorial Designs **2** (1994), 131–145) where the answer is affirmative). □

The complete arcs so far constructed may be regarded as special examples of a more general family, namely the family of those arcs whose points (with some exceptions) lie on a conic. To construct such arcs and investigate their completeness, the following general scheme has been proposed by V. Abatangelo, T. Szőnyi, and G. Korchmáros (see [10]):

Given a conic C in $PG(2,q)$,

1) Choose an algebraically parametrized subset $K \subset C$ in such a way that the parametrization has low degree.

2) For a point $P \notin C$, determine an algebraic curve $\Gamma(P)$ defined over $GF(q)$ such that non-existence of points with coordinates in $GF(q)$ on $\Gamma(P)$ expresses the condition that P can be added to K.

3) Show that $\Gamma(P)$ is absolutely irreducible for almost all points $P \notin C$, and use Weil's theorem (or, some other deep theorems from algebraic geometry) to show that if K is large enough then $\Gamma(P)$ has some points with coordinates in $GF(q)$ on Γ, and hence P cannot be added to K.

4) Extend the arc K with some exceptional points $P \notin C$, and with some points of C.

Let us illustrate this scheme on some further examples:

1. Start with the parabola $C : Y = X^2$. Let the algebraically parametrized subset K be $K = \{(u^3, u^6) : u \in GF(q) \backslash \{0\}\}$, where 3 divides $q-1$. Note

that $|K| = (q-1)/3$.

2. Take first an affine point $P(a,b)$ not on C. The collinearity of $Q : (x^3, x^6)$, $R : (y^3, y^6)$ and P means that $a(x^3+y^3) - x^3y^3 - b = 0$. This leads to consider the sextic curve of equation $a(X^3+Y^3) - X^3Y^3 - b = 0$ with $b \neq a^2$.

3. To show that F is absolutely irreducible the following criterium due to Segre can be used:

Theorem 4 *(B. Segre) Let F be a plane algebraic curve of degree k over a field E. A sufficient condition for F to be irreducible over the algebraic closure of E is the existence of a point P on F satisfying both conditions i) and ii):*

i) F has no linear component through P;

ii) there is a tangent r at P which counts once among the tangents at P and which intersects F in P with multiplicity k.

In our case, F has two infinite points, namely X_∞ and Y_∞. If $a \neq 0$ and $b \neq a^2$, then both satisfy conditions i) and ii). Hence F is indeed absolutely irreducible. Furthermore, F has exactly two ordinary singularities (X_∞ and Y_∞) and they have multiplicity 3, the genus of F is 4. The celebrated Hasse-Weil theorem implies then that there are points (x,y) on F such that $x, y \in GF(q)$ and $x^3 \neq y^3$. A similar argument works for infinite points. Now, single out the case $q = 2^h$. Then we obtain the following

Theorem 5 *(V. Abatangelo) Let $q = 2^h, h \geq 8$ and $K = \{(u^3, u^6) : u \in GF(q) \setminus \{0\}\}$. If $K \cup \{P\}$ is an arc, then either P belongs to the Y-axis or P is the nucleus X_∞ of the parabola C or $P \in C \setminus K$.*

4. We can add to K the nucleus X_∞ and the points $(0,g)$ and $(0,g^2)$ where g is a generator of the multiplicative group of $GF(q)$.

In the above construction, a subgroup of index 3 in the multiplicative group of $GF(q)$ was used to define a suitable parametrized subset. The case of an arbitrary multiplicative subgroup was investigated in [5], while Szőnyi used some additive subgroups of $GF(q)$ for the parametrization, see also [8]. These arcs have size approximately $q/3$ (in some cases $q/4$) and thus are smaller than those given in Theorems 1, 2 and 3.

The above general construction scheme still works provided that the conic C is replaced by a cubic curve. However, some explanation is needed, especially in the case where a non-singular cubic is taken for C. Firstly, the point set K must be itself an arc and hence the possible large set K must be chosen on C in such a way that no three points of K are collinear. For a singular cubic curve C, the additive or the multiplicative group of $GF(q)$ still provides an algebraic parametrization and technical details to define good choices for K may be worked out in a simple way. For a non-singular cubic C no rational parametrization is possible. To define algebraic point sets K on C, the following result from classical algebraic geometry is useful: A non-singular cubic can be made into a commutative group G such that collinearity of three pairwise distinct points a_1, a_2, and a_3 of the cubic C is expressed by $a_1 + a_2 + a_3 = \delta$ in G, for a certain element δ. If the neutral element coincides with an inflexion, then $\delta = 0$ can be chosen. In particular, if the number of points on C (with coordinates in $GF(q)$) is even, these points form a subgroup H of even order, and the coset of the subgroup of index 2 in H will be an arc K containing half the points of C. Voloch proved that if the j-invariant of a non-singular cubic is non-zero and $q \geq 175$ (for q odd) or $q \geq 256$ (for q even), then these arcs are complete. Using this approach, Szőnyi constructed a k-arc with $k \leq cq^{3/4}$. Very recently, Kim and Vu used a sophistical version of the probabilistic method, the so-called Rödl nibble, to show the existence of k-arcs of size $d\sqrt{q}\log^c q$, where d and c are absolute constants.

A difficult question is to determine the spectrum of complete arcs, that is to decide which are the possible sizes of complete k-arcs in $PG(2,q)$. We point out the spectrum can even contain whole intervals.

Theorem 6 *(Hadnagy, Voloch, Szőnyi) Let $p > 5^{10}$ be a prime number. For every integer k satisfying*

$$[2.46 \cdot p^{3/4} \cdot \log p] \leq k \leq (\sqrt{p} + 1)^2/2,$$

there exists a complete k-arc in $PG(2,p)$.

Voloch proved the part $(\sqrt{p} - 1)^2 \leq k \leq (\sqrt{p} + 1)^2$ by using the complete arcs consisting of half the points of a non-singular cubic. Taking points of a conic, Szőnyi showed that for every integer k satisfying $[p/3]+3 \leq k \leq [p/2]+1$ there exists a complete k-arc in $PG(2,q)$ provided that p is a sufficiently large prime. Finally, Hadnagy dealt with the longest part of the interval. For the completeness, Hadnagy uses a theorem of Smith about small solutions of congruences.

References

[1] V. Abatangelo, A class of complete $((q+8)/3)$-arcs of $PG(2,q)$, with $q = 2^h$ and $h (> 6)$ even, *Ars Combinatoria*, **16** (1983), 103-111.

[2] E. Hadnagy, Small complete arcs in Galois-planes of prime order, manuscript, 1996.

[3] J.W.P. Hirschfeld, *Projective geometries over finite fields*, Oxford University Press, Oxford, 1998 (Second Edition).

[4] G. Korchmáros, Osservazioni sui risultati di B. Segre relativi ai k-archi contenenti $k-1$ punti di un ovale, *Atti Accad. Naz. Lincei Rend.*, **56** (1974), 690-697.

[5] G. Korchmáros, New examples of complete k-arcs in $PG(2,q)$. *Europ. J. Combin.* **4** (1983), 329-334.

[6] L. Lombardo-Radice, Sul problema dei k-archi completi di $S_{2,q}$, *Boll. Un. Mat. Ital.*, **11** (1956), 178-181.

[7] B. Segre, Introduction to Galois geometries, *Atti Accad. Naz. Lincei Mem.*, **8** (1967), 133-236 (edited by J.W.P. Hirschfeld).

[8] T. Szőnyi, Small complete arcs in Galois planes. *Geom. Dedicata* **18** (1985), 161-172.

[9] T. Szőnyi, Arcs in cubic curves and 3-independent subsets of abelian groups, in *Combinatorics, Eger, Colloquia Mathematica Societatis János Bolyai*, **52** North Holland, Amsterdam (1987), 499-508.

[10] T. Szőnyi, Some Applications of algebraic curves in finite geometries and combinatorics, in *Surveys in Combinatorics, 1997* LMS, Lecture Note Series 241, (1997), 197-236.

[11] J.F. Voloch, On the completeness of certain plane arcs II, *European Journal of Combinatorics*, **11** (1990), 491-496.