COMPLETE ARCS IN MOULTON PLANES OF ODD ORDER

VITO ABATANGELO AND BAMBINA LARATO

ABSTRACT. A complete arc of size $q^2 - 1$ is constructed in the Moulton plane of order q^2 for $q \geq 5$ odd.

Keywords: Moulton planes, complete arcs, projective spaces, finite fields

Classification: 51A35 , 51E15

1. INTRODUCTION

In a finite projective plane π, a k-arc is defined to be a set of k points no three of which are collinear. If π has order q, then a k-arc contains at most $q+1$ or $q+2$ points according as q is odd or even. If equality holds then the arc is called an oval when q is odd and a hyperoval when q is even. A k-arc is complete if it is not contained in any $(k+1)$-arc of π.

Large k-arcs in the Desarguesian plane $PG(2,q)$ have been intensively investigated also in connection with coding theory, see [7, 8, 12, 13] and [11, Chapter 13]. In $PG(2,q)$, complete k-arcs different from ovals when q is odd and from hyperovals when q is even have the following properties, see [2, 3, 5, 6, 9, 10, 15, 19, 20, 21, 22]

(1a)	$k \leq q - \sqrt{q} + 1$	if q is even;
(1b)	$k \leq q - (\sqrt{q}/2) + 5$	if q is odd;
(1c)	$k \leq (44q/45) + 2$	if q is a prime.

In particular, q-arcs in $PG(2,q)$ are not complete; this goes back to Segre for q odd and Tallini for q even. It has been conjectured that no $(q-1)$-arc for $q > 13$ is complete, but this has been proven so far for $q > 73$.

The above results on the spectrum of the sizes of large k-arcs of $PG(2,q)$ do not hold true in non-Desarguesian projective planes. Menichetti [16] constructed an infinite sequence of complete q-arcs in Hall planes of even

THIS RESEARCH WAS SUPPORTED BY GNSAGA OF THE ITALIAN CNR, WITH THE FINANCIAL SUPPORT OF THE ITALIAN MINISTRY MURST: PROJECT "STRUTTURE GEOMETRICHE, COMBINATORIA E LORO APPLICAZIONI", 2005/07

order. Examples of complete 9-arcs in non-Desarguesian planes of order 9 were given by Denniston [4] and Barlotti [1]. Szőnyi [17] gave constructions for ovals in André planes, for complete $(q-1)$-arcs in the Hall plane of odd order $q \geq 49$ and for complete arcs in André planes of square order having at least $2q/3$ points. Szőnyi [18] also showed that the set consisting of all rational numbers k/q such that there exists a complete k-arc in some projective plane of order q is dense in the interval $[0,1]$.

In this paper, we construct an arc of size (q^2-1) in the Moulton plane of odd order q^2, and prove its completeness for $q \geq 5$.

2. Notation and preliminaries

The Moulton plane of order q^2, with q a power p^h of an odd prime p, is the dual plane of the Hall plane of the same order. The quasifield coordinatizing the Moulton plane arises from the finite field $GF(q^2)$ by altering the multiplication in the following manner.

Let $(GF(q), +, \cdot)$ be the subfield of $GF(q^2)$ of order q. Then $GF(q^2)$ can be viewed as the quadratic extension of $GF(q)$ with respect to a polynomial $x^2 - \tau$ irreducible over $GF(q)$. Choose $i \in GF(q^2)$ for which $i^2 = \tau$, and write each element $x \in GF(q^2)$ as $x = \xi + i\eta$ with $\xi, \eta \in GF(q)$. Then the norm of $x = \xi + i\eta$ in $GF(q^2)$ 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 $t \in GF(q)$, 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, $(GF(q^2), +, \circ)$ is a quasifield that coordinatizes a translation plane which is in turn the affine Hall plane of order q^2, as well as its dual affine plane, called the affine Moulton plane of order q^2. Affine Hall planes of the same order are isomorphic, see [14, Chapter X.4], and this holds true for affine Moulton planes.

The affine Moulton plane has the same points and the same vertical lines as the Desarguesian plane over $GF(q^2)$, whereas its non-vertical lines are the graphs of the functions $y = m \circ x + b$ with $m, b \in GF(q^2)$. In other words, the affine Moulton plane arises from the Desarguesian plane 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 $m \in GF(q^2) \setminus GF(q)$.

Note that some collineations of the affine Desarguesian plane remain collineations in the affine Moulton plane. Those we use in this paper are

$$\varphi_x : \begin{cases} x' &= x \\ y' &= -y \end{cases}, \quad \varphi_y : \begin{cases} x' &= -x \\ y' &= y \end{cases}, \quad \varphi_O : \begin{cases} x' &= -x \\ y' &= -y \end{cases}.$$

The projective closure of this affine plane is the Moulton plane $M(q^2)$ of order q^2.

3. Inherited arcs in $M(q^2)$

In this section we describe a procedure for constructing a k-arc in $M(q^2)$ of size $k = q^2 - 1$. As we will see, such a procedure provides an arc with either two or zero points at infinity, according as $q \equiv 1 \pmod 4$ or $q \equiv 3 \pmod 4$. The two cases will be investigated simultaneously, although some differences in the proofs will occur.

Let s be an element of $GF(q^2)$ such that s is a square or a non-square according as $q \equiv 1 \pmod 4$ or $q \equiv 3 \pmod 4$. In the Desarguesian plane, the conic Ω of equation $x^2 - sy^2 = 1$ is irreducible, and it has either two or zero points at infinity, according as $q \equiv 1 \pmod 4$ or $q \equiv 3 \pmod 4$. Two tangents of Ω are vertical, namely the line of equation $x = 1$ with tangency point $A(1,0)$ and that of equation $x = -1$ with tangency point $B(-1,0)$.

Without loss of generality, we may assume that $t = 1$.

Lemma 3.1. *In the Desarguesian plane, no vertical line of equation $x = c$ with $\|c\| = 1$ is a secant of Ω.*

Proof. Assume on the contrary that a vertical line $x = c$ with $c \neq 1, -1$ is a secant of Ω. Then the system

$$(1) \qquad \begin{cases} x^2 - sy^2 = 1 \\ \|x\| = 1 \end{cases}$$

has two solutions, namely (c, b) and $(c, -b)$ with $c \neq 1$ and $b \neq 0$. Let $c = \xi + i\eta$. Since $c \neq 1$, we have $\eta \neq 0$.

Now, replacing $x = \xi + i\eta$ in the system (1),

$$(2) \qquad \begin{cases} \xi^2 + 2\xi\eta\, i + \tau\eta^2 - sy^2 = 1 \\ \xi^2 - \tau\eta^2 = 1 \end{cases},$$

and subtracting the second equation from the first one,

$$2\xi\eta i + 2i^2\eta^2 - sy^2 = 0,$$

that is

$$(3) \qquad 2\eta i\ (\xi + i\eta) = sy^2.$$

Raising to the $[(q^2-1)/2]$-th power,

$$(2\eta)^{(q^2-1)/2}\ i^{(q^2-1)/2}\ \|x\|^{(q^2-1)/2} = s^{(q^2-1)/2}\ y^{(q^2-1)}.$$

Since $y^{q^2-1} = 1$ and $(2\eta)^{q-1} = 1$, this implies that

$$(4) \qquad i^{(q^2-1)/2} = s^{(q^2-1)/2}.$$

To end the proof it is enough to show that (4) does not hold. Since τ is a non-square in $GF(q)$,

$$i^{(q^2-1)/2} = \tau^{(q^2-1)/4} = (\tau^{(q-1)/2})^{(q+1)/2} = (-1)^{(q+1)/2}.$$

If $q \equiv 3 \pmod 4$, then $(-1)^{(q+1)/2} = 1$ whereas s is a non-square in $GF(q^2)$ and hence $s^{(q^2-1)/2} = -1$. This contradicts (4).

Similarly, if $q \equiv 1 \pmod 4$, then $(-1)^{(q+1)/2} = -1$ whereas s is a square in $GF(q^2)$ and hence $s^{(q^2-1)/2} = 1$, again a contradiction. □

A straightforward consequence of Lemma 3.1 is the following result.

Corollary 3.2. *The set $\Omega' = \Omega \setminus \{A, B\}$ is an arc in the Moulton plane $M(q^2)$.*

For $q \equiv 1 \pmod 4$, Ω is a hyperbola in the affine Desarguesian plane, one of its infinite point P_∞ is defined by the lines of equations $y = \sigma x + b$, the other Q_∞ by those of equations $y = -\sigma x + b$ where $\sigma^2 = s^{-1}$. In the affine Desarguesian plane, each of this lines meets Ω' exactly one point, except for the four lines disjoint from Ω', these four lines join A or B to P_∞ or Q_∞. By Lemma 3.1 this holds true in the affine Moulton plane. This shows that Ω' extends to an arc of size $q^2 - 1$ in the Moulton plane by adding to it the infinite points P'_∞ and Q'_∞ defined by the parallel lines of equations $y = \sigma \circ x + b$ and $y = -\sigma \circ x + b$, respectively.

This motivates to consider the point-set in $M(q^2)$

$$(5) \qquad \Delta = \begin{cases} \Omega' & \text{when } q \equiv 3 \pmod 4 \\ \Omega' \cup \{P'_\infty, Q'_\infty\} & \text{when } q \equiv 1 \pmod 4 \end{cases} .$$

From the above results, the following theorem follows.

Theorem 3.3. *The point-set Δ is an arc of size $q^2 - 1$ in $M(q^2)$.*

4. The completeness of the arc Δ in $M(q^2)$ for $q \geq 5$

To show that Δ is complete for $q \geq 5$, we must prove that no point $P(u, v)$ with $\|u\| = 1$ can be added to Δ. For $q \equiv 3 \pmod 4$, we must also show that this holds true for every point at infinity.

Lemma 4.1. *Neither A nor B can be added to Δ.*

Proof. Since $\|1\| = 1$, every non vertical line r through A has equation $y = m \circ x - m^q$ with $m \in GF(q^2)$. Choose $m \in GF(q^2) \setminus GF(q)$ in such a way that $m^2 \in GF(q)$ but $m \neq -m^q$, and, for $q \equiv 1 \pmod 4$, also $m^2 \neq 1/s$. The existence of such an element m follows from the hypothesis that $q \geq 5$.

To show that the line r of equation $y = m \circ x - m^q$ is a secant of Δ, note that the set of common points of r and Δ consists of the points $P(x, y)$ of $M(q^2)$ satisfying the system

$$(6) \qquad \begin{cases} x^2 - sy^2 = 1 \\ y = m \circ x - m^q \end{cases} .$$

From this,

$$(1 - sm^2)\, x^2 + 2\, s\, m^{q+1}x - (1 + sm^{2q}) = 0. \tag{7}$$

By hypothesis $1 - sm^2 \neq 0$. The discriminant d of (7) divided by 4 is

$$d/4 = sm^{2q} - sm^2 + 1 = 1 + s(m^{2q} - m^2)$$

and it is equal to 1 since $m^2 \in GF(q)$. Therefore, the equation (7), and also the system (6) have two distinct solutions

$$\begin{cases} x_1 &= (1 - sm^{q+1})/(1 - sm^2) \\ y_1 &= (m - m^q)/(1 - sm^2) \end{cases}, \quad \begin{cases} x_2 &= (-1 - sm^{q+1})/(1 - sm^2) \\ y_2 &= -(m + m^q)/(1 - sm^2) \end{cases}$$

By the choice of m, neither $y_1 = 0$ nor $y_2 = 0$. Hence, both points $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ lie on the line r showing that A cannot be added to Δ. The same argument works for the point B. □

Lemma 4.2. *No point $P(u, 0)$ of $M(q^2)$ with $\|u\| = 1$ can be added to Δ.*

Proof. Since Δ is a $(q^2 - 1)$-arc in $M(q^2)$, through every point $C \in \Delta$ there are exactly three 1-secants to Δ. Two of these join C to A and B, the third being the tangent line ℓ to the conic Ω at C. Let it be $C(x_1, y_1)$. Then ℓ has equation

$$y = \frac{1}{s}\frac{x_1}{y_1} \circ x - \frac{1}{s} y_1\,,$$

and it passes through the point $P(u, 0)$ if and only if

$$u = \frac{y_1^{q-1} s^{q-1}}{x_1^q}. \tag{8}$$

Assume that $P(u, 0)$ can be added to Δ. Then (8) holds for every point $C \in \Omega$ distinct from A and B. But then

$$x_1 y_1^{q-1} - x_2 y_2^{q-1} = 0$$

for every two points $C(x_1, y_1)$ and $D(x_2, y_2)$ of Ω distinct from A and B. Therefore, the function xy^{q-1} is constant on the points of Ω distinct from A and B. If c is this constant, then the algebraic curve Γ of equation $xy^{q-1} = c$ contains at least $q^2 - 3$ points from Ω. On the other hand, since Γ has degree q, the number of common points of Γ and Ω is at most $2q$. Since $q^2 - 3 > 2q$, this is a contradiction with Bézout's theorem. □

Lemma 4.3. *No point $P(u, v)$ of $M(q^2)$ can be added to Δ.*

Proof. If $\|u\| \neq 1$, the point P cannot be added since Ω' is an arc in the Desarguesian plane such that A and B are the only points which can be added to Ω'.

Now, consider a point $P_1(u, v)$ with $\|u\| = 1$, $v \neq 0$. If P_1 can be added to Δ, then the same is true for its images $P_2(u, -v)$, $P_3(-u, v)$ and $P_4(-u, -v)$ under the collineations quoted in Section 2. Since the line joining P_1 and P_2 is disjoint from Δ, we see that $\Delta_{12} = \Delta \cup \{P_1, P_2\}$ is an oval, that is an arc of size q^2+1. Similarly, $\Delta_{34} = \Delta \cup \{P_3, P_4\}$ is an oval. It turns out that the ovals Δ_{12} and Δ_{34} in $M(q^2)$ have q^2-1 common points, but this is not possible for $q \geq 5$. □

Lemma 4.4. *No point at infinity can be added to* Δ .

Proof. The assertion is certainly true for $q \equiv 1 \pmod 4$ as Δ has two infinite points for such values of q. For $q \equiv 3 \pmod 4$, every parallel class of lines contains at least one secant of Ω that does not pass either through A or B. This proves the assertion. □

From the above lemmas together with Theorem 3.3, we obtain the following result.

Theorem 4.5. *In the Moulton plane* $M(q^2)$ *of order* q^2 *with* $q \geq 5$, *there exists a complete* (q^2-1)*-arc.*

REFERENCES

[1] A. Barlotti, Un'osservazione intorno ad un teorema di B. Segre sui q-archi, *Le Matematiche*, **21** (1966), 23-29.

[2] E. Boros and T. Szőnyi, On the sharpness of a theorem of B. Segre, *Combinatorica* **6** (1986), 261–268.

[3] A. Cossidente, A new proof of the existence of (q^2-q+1)-arcs in $PG(2, q^2)$, *J. Geom.* **53** (1995), 37–40; correction **59** (1997), 32–33.

[4] R.H.F. Denniston, On arcs in projective planes of order 9, *Manuscripta Math.*, **4** (1971), 61-89.

[5] G. Ebert, Partitioning projective geometries into caps, *Canad. J. Math.* **37** (1985), 1163–1175.

[6] J.C. Fisher, J.W.P. Hirschfeld and J.A. Thas, Complete arcs in planes of square order, *Combinatorics '84*, North-Holland Math. Stud. **123**, North-Holland, Amsterdam, 1986, 243–250.

[7] J.W.P. Hirschfeld, The main conjecture for MDS codes, *Cryptography and Coding*, Lecture Notes in Comput. Sci. **1025**, Springer, Berlin, 1995, 44–52.

[8] J.W.P. Hirschfeld, Complete arcs, *Discrete Math.* **174** (1997), 177–184.

[9] J.W.P. Hirschfeld and G. Korchmáros, On the embedding of an arc into a conic in a finite plane, *Finite Fields Appl.* **2** (1996), 274–292.

[10] J.W.P. Hirschfeld and G. Korchmáros, On the number of rational points on an algebraic curve over a finite field, *Bull. Belg. Math. Soc. Simon Stevin* **5** (1998), 313–340.

[11] J.W.P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic curves over a finite field,* Princetone University Press, pp. i-xviii, pp. 691.

[12] J. W. P. Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces, *J. Statist. Plann. Inference* **72** (1998), 355–380.

[13] J.W.P. Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces: update 2001, *Finite Geometries*, Kluwer, Dordrecht, 2001, 201–246.

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

[15] B. Kestenband, Unital intersections in finite projective planes, *Geom. Dedicata* **11** (1981), 107–117.

[16] G. Menichetti, q-archi completi nei piani di Hall di ordine $q = 2^k$, *Rend. Accad. Naz. Lincei*, **56** (1974), 518-525.
[17] T. Szőnyi, Arcs and k-sets with large prime-set in Hall planes, *J. Geom.*, **34** (1989), 187-194.
[18] T. Szőnyi, Complete arcs in non-Desarguesian planes, *Ars Combin.*, **25**, (1988), C , 169-178.
[19] J.F. Voloch, On the completeness of certain plane arcs, *European J. Combin.* **8** (1987), 453–456.
[20] J.F. Voloch, Arcs projective planes over prime fields, *J. Geometry*, **38** (1990), 198–200.
[21] J.F. Voloch, On the completeness of certain plane arcs II, *European J. Combin.* **11** (1990), 491–496.
[22] J.F. Voloch, Complete arcs in Galois planes of nonsquare order, *Advances in Finite Geometries and Designs*, Oxford University Press, Oxford, 1991, 401–406.

V. Abatangelo and B. Larato,
Dipartimento di Matematica
Politecnico di Bari,
Via Orabona 4,
I-70125 Bari, Italy.

e-mail: abatvito@poliba.it
larato@poliba.it