Journal of Algebraic Combinatorics 1 (1992), 197–202

Completeness of Normal Rational Curves

L. STORME*
Seminar of Geometry and Combinatorics, University of Ghent, Krijgslaan 281, B-9000 Ghent, Belgium
e-mail: ls@cage.rug.ac.be

Received October 21, 1991; Revised March 20, 1992

Abstract. The completeness of normal rational curves, considered as $(q+1)$-arcs in $PG(n, q)$, is investigated. Previous results of Storme and Thas are improved by using a result by Kovács. This solves the problem completely for large prime numbers q and odd nonsquare prime powers $q = p^{2h+1}$ with p prime, $p \geq p_0(h)$, $h \geq 1$, where $p_0(h)$ is an odd prime number which depends on h.

Keywords: k-arcs, normal rational curves, M.D.S. codes

1. Introduction

Let $\Sigma = PG(n, q)$ denote the n-dimensional projective space over the field $GF(q)$. A k-arc of points in Σ (with $k \geq n+1$) is a set K of k points such that no $n+1$ points of K belong to a hyperplane. A k-arc is complete if it is not contained in a $(k+1)$-arc.

A normal rational curve in $PG(n, q)$, $2 \leq n \leq q-2$, is any $(q+1)$-arc projectively equivalent to the $(q+1)$-arc $\{(1, t, \ldots, t^n) \parallel t \in GF(q)\} \cup \{(0, \ldots, 0, 1)\} = \{(1, t, \ldots, t^n) \parallel t \in GF(q)^+\}(GF(q)^+ = GF(q) \cup \{\infty\}$; ∞ corresponds to $(0, \ldots, 0, 1))$. All $(q+1)$-arcs of $PG(q-1, q)$ are called normal rational curves of $PG(q-1, q)$.

This paper will investigate whether a normal rational curve K of $PG(n, q)$ can be extended to a $(q+2)$-arc of $PG(n, q)$. The results of [5] will be improved by using a recent result by Kovács [3]. Refer to [5] for a more detailed description of the method that is used.

2. Known results

THEOREM 2.1. (Seroussi and Roth [4]). *In* $PG(n, q)$ *every normal rational curve is complete for*

(a) q *odd and* $2 \leq n \leq (q+1)/2$,
(b) q *even and* $3 \leq n \leq (q/2) + 1$.

*Research Assistant of the National Fund for Scientific Research (Belgium).

In PG(2, q), q even, a normal rational curve is a conic and a conic is incomplete. It can be uniquely extended to a $(q + 2)$-arc by its nucleus.

THEOREM 2.2. (Storme and Thas [5]). *Let $q = p^h$, p prime. Suppose r, $r > 1$, exists such that*

(a) $2r|(q-1)$ *when q is odd and r is even, and* $r|(q-1)$ *in all other cases;*
(b) $q+1-2r^2-2r-2(r-1)^2\sqrt{q} > 0$ *when q is odd and* $q+1-r^2-2r-2(r-1)^2\sqrt{q} > 0$ *when q is even.*

Then every normal rational curve of PG(n, q) *is complete for*

(a) *q even and* $3 \leq n \leq (r-1)q/r + 1/r$,
(b) *q odd and* $2 \leq n \leq (r-1)q/r + 1/r$.

3. Completeness of normal rational curves

THEOREM 3.1. *Let C be the conic* $\{(t, t^2, 1) \| t \in \mathrm{GF}(q)^+\}$ *in* PG(2, q). *Let M be a k-arc contained in C which can only be extended to a $(k + 1)$-arc by the remaining points of C and the nucleus of C when q is even. Then every normal rational curve of* PG(n, q) *is complete for*

(a) *q even and* $3 \leq n \leq q - k + 2$,
(b) *q odd and* $2 \leq n \leq q - k + 2$.

Proof. We may assume from Theorem 2.1 that $n > q/2 + 1$. Choose the reference system in such a way that $e_0(1, 0, \ldots, 0), \ldots, e_n(0, \ldots, 0, 1), e_{n+1}(1, \ldots, 1)$ belong to the normal rational curve K. This implies that K is the set of points $\{(a_0/((a_0-1)t+1), \ldots, a_n/((a_n-1)t+1)) \| t \in \mathrm{GF}(q)^+\}$, where all elements a_i are different nonzero elements of GF(q) and where the parameter $t = -1/(a_i - 1)$ corresponds to e_i [1].

Let $S = \{x_1, \ldots, x_k\}$ ($S \subseteq \mathrm{GF}(q)^+$) be the set of parameters associated with the points of M in C. Since the conic C has a 3-transitive projective group [1], we may assume that $x_1 = 0$, $x_2 = \infty$, and $x_3 = 1$.

Select a_i in $\mathrm{GF}(q) \setminus \{0, 1\}$ in such a way that $-1/(a_i - 1) \notin S$, $i = 0, \ldots, n-2$. This is possible if $n - 1 \leq q - 2 - (k - 3) \Leftrightarrow n \leq q - k + 2$. So if $n \leq q - k + 2$, it is possible to select the parameters $t_i = -1/(a_i - 1)$ of the points e_i ($i = 0, \ldots, n-2$) of K in such a way that $t_i \notin S$.

We now proceed as in the proof of Theorem 26 of [5]. This proof uses the one-to-one correspondence between the involutions ϕ ($\phi \neq 1$) of PGL(2, q) on a conic $C = \{(t, t^2, 1) \| t \in \mathrm{GF}(q)^+\}$ and the points r of PG(2, q) not belonging to C and different from the nucleus of C when q is even. Each point r of PG(2, q) not belonging to C and different from the nucleus of C when q is even corresponds to an unique involution $\phi : t \mapsto (at + b)/(ct - a)$, $a^2 + bc \neq 0$, on C. Two points $p_1(t_1, t_1^2, 1)$ and $p_2(t_2, t_2^2, 1)$ are each others image under ϕ if and only if $p_1 \in rp_2$.

Since M can only be extended to a larger arc in PG(2, q) by the remaining points of C and the nucleus of C when q is even, for each involution ϕ of PGL(2, q) on C ($\phi \neq 1$) there exist two distinct parameters t_1 and t_2 in S for which $\phi(t_1) = t_2$ (see also the introduction of Section 6 in [5]).

Consider the subspace $\alpha : X_{n-1} = X_n = 0$ generated by the $n-1$ points $e_0, \ldots, e_{n-2}$ of K. Project from $\alpha_i : X_i = X_{n-1} = X_n = 0$ $(0 \leq i \leq n-2)$ onto the plane $\beta_i : X_j = 0$ for all $j \neq i, n-1, n$. The points of K which do not belong to α_i are projected onto points of the conic $C_i = \{(a_i/((a_i - 1)t + 1), a_{n-1}/((a_{n-1} - 1)t + 1), a_n/((a_n - 1)t + 1)) \parallel t \in \mathrm{GF}(q)^+\}$ in β_i. The points of K not belonging to α_i are projected onto the points of a $(q + 3 - n)$-arc K_i on C_i. The parameters of the points of K_i are the elements of $\mathrm{GF}(q)^+ \setminus \{-1/(a_j - 1) \parallel j = 0, \ldots, n-2; j \neq i\}$. Since $-1/(a_j - 1) \notin S\,(j = 0, \ldots, n-2)$, K_i contains the points of C_i with parameters in S. This implies that for each involution $\phi\,(\phi \neq 1)$ of PGL(2, q) on C_i there exist two distinct parameters t_1, t_2 of points of K_i for which $\phi(t_1) = t_2$. As a consequence of the one-to-one correspondence between the involutions $\phi\,(\phi \neq 1)$ of PGL(2, q) on C_i and the points r of β_i not belonging to C_i and different from the nucleus of C_i when q is even (see also the introduction of Section 6 in [5]), this arc K_i can only be extended to a larger arc in β_i by the remaining points of C_i and the nucleus of C_i when q is even.

If there exists a point p of PG(n, q) which extends K to a $(q+2)$-arc, then p is projected from α_i onto a point p_i of β_i which extends K_i to a $(q+4-n)$-arc in β_i. Thus p is projected onto C_i or possibly to the nucleus of C_i if q is even. This is precisely the same situation as in the proof of Theorem 15 of [5]. Therefore, when the proof of Theorem 15 is combined with Lemma 21 of [5], it follows that p belongs to K.

This is impossible. This shows that K is complete when $q/2 + 1 < n \leq q - k + 2$. □

THEOREM 3.2. (Kovács [3]). *Consider the conic* $C = \{(t, t^2, 1) \parallel t \in \mathrm{GF}(q)^+\}$ *in* PG(2, q). *Then for at least one* $k \leq 6\sqrt{q \ln q}$ *there exists on* C *a* k*-arc* K *which can only be extended to a larger arc in* PG(2, q) *by the remaining points of* C *and the nucleus of* C *when* q *is even.*

THEOREM 3.3. *In* PG(n, q) *every normal rational curve is complete for*

(a) q *even and* $3 \leq n \leq q + 2 - 6\sqrt{q \ln q}$,
(b) q *odd and* $2 \leq n \leq q + 2 - 6\sqrt{q \ln q}$.

Proof. It follows from Theorem 3.2 that there exists a k-arc K on the conic $C = \{(t, t^2, 1) \parallel t \in \mathrm{GF}(q)^+\}$ with $k \leq 6\sqrt{q \ln q}$, which can only be extended to a larger arc in PG(2, q) by the remaining points of C and the nucleus of C when q is even.

We apply Theorem 3.1 when $k = 6\sqrt{q \ln q}$, so in PG(n, q) every normal rational curve is complete when

(a) q is even and $3 \le n \le q + 2 - 6\sqrt{q \ln q}$,
(b) q is odd and $2 \le n \le q + 2 - 6\sqrt{q \ln q}$. □

THEOREM 3.4. *For each prime number* p, $p > 1007215$, *every normal rational curve in* PG(n, p), $2 \le n \le p - 1$, *is complete.*

Proof. Theorem 3.3 states that in PG(n, p), $p \neq 2$, $2 \le n \le p + 2 - 6\sqrt{p \ln p}$, every normal rational curve is complete.

Voloch [10] proved that if K is a k-arc of PG(2, p), p prime, $p > 2$, with $k > (44/45)p + 8/9$, then K is contained in a conic. The arguments used by Thas in [7] then show that a k-arc K of PG(n, p), p prime, $p > 2$, $n \ge 2$, for which $p + 1 \ge k > (44/45)p + n - 10/9$, is contained in a unique normal rational curve of PG(n, p). Hence, every $(p + 1)$-arc of PG(n, p), p prime, $p > 2$, $(p + 95)/45 > n \ge 2$, is a normal rational curve. Theorem 4 in [2] then implies that $k \le p + 1$ for any k-arc K of PG(n, p), $(p + 140)/45 > n \ge 2$.

Assume that there exists a $(p + 2)$-arc K in PG(n, p), p prime, $p > 2$, $p - 2 \ge n > (44p - 140)/45$. Then there exists a dual $(p + 2)$-arc $\hat{K}$ in PG($p - n$, p) [6], [8], [9]. So, $\hat{K}$ is a $(p + 2)$-arc in PG(m, p), $(p + 140)/45 > m \ge 2$. This contradicts the previous calculations. Hence, $k \le p + 1$ for any k-arc K of PG(n, p), p prime, $p > 2$, $p - 2 \ge n > (44p - 140)/45$.

Every $(p + 1)$-arc of PG($p - 1$, p), p prime, $p > 2$, is complete. A $(p + 1)$-arc of PG($p - 1$, p) is projectively equivalent to the set $L = \{e_0(1, 0, \dots, 0), \dots, e_{p-1}(0, \dots, 0, 1), e_p(1, \dots, 1)\}$. If a point $r(a_0, \dots, a_{p-1})$ of PG($p - 1$, p) extends L to a $(p + 2)$-arc, then all p coordinates a_i, $i = 0, \dots, p - 1$, must be nonzero and distinct from each other. This is impossible. So L is complete.

We conclude that for p an odd prime, when $(44p - 140)/45 < p + 2 - 6\sqrt{p \ln p}$, then in PG($n$, p), $2 \le n \le p - 1$, every normal rational curve is complete.

This inequality $(44p - 140)/45 < p + 2 - 6\sqrt{p \ln p}$ is satisfied for all prime numbers $p > 1007215$. □

THEOREM 3.5. *For a fixed integer* $h \ge 1$ *let* $p_0(h)$ *be the smallest odd prime number satisfying*

$$p^{h+1} > 24p^h\sqrt{p(2h + 1) \ln p} + \frac{29}{4}p - 20.$$

Then for each odd prime number $p \ge p_0(h)$ *in* PG(n, q), $q = p^{2h+1}$, $2 \le n \le q - 1$, *every normal rational curve is complete.*

Proof. Voloch [11] proved that in PG$(2, q)$, $q = p^{2h+1}$, $h \geq 1$, p prime, $p \neq 2$, any k-arc K for which $q + 1 \geq k > q - \sqrt{pq}/4 + 29p/16 + 1$ is contained in a unique conic.

The method described by Thas in [7] once again implies that a k-arc K of PG(n, q), $q = p^{2h+1}$, $h \geq 1$, p prime, $p > 2, n \geq 2$, for which $q + 1 \geq k > q - \sqrt{pq}/4 + 29p/16 + n - 1$, is contained in a unique normal rational curve of PG(n, q). Therefore, any $(q + 1)$-arc of PG(n, q), $\sqrt{pq}/4 - 29p/16 + 2 > n \geq 2$, is a normal rational curve. Theorem 4 in [2] then shows that $k \leq q + 1$ for any k-arc K in PG(n, q), $q = p^{2h+1}$, $h \geq 1$, p prime, $p > 2$, $\sqrt{pq}/4 - 29p/16 + 3 > n \geq 2$.

The existence of a $(q + 2)$-arc K in PG(n, q), $q = p^{2h+1}$, $h \geq 1$, p prime, $p > 2, q - 2 \geq n > q - \sqrt{pq}/4 + 29p/16 - 3$, implies the existence of a dual $(q + 2)$-arc $\hat{K}$ in PG$(q - n, q)$, $\sqrt{pq}/4 - 29p/16 + 3 > q - n \geq 2$ [6], [8], [9]. This contradicts the previous calculations.

Thus all k-arcs of PG(n, q), $q = p^{2h+1}$, $h \geq 1$, p prime, $p > 2, q - 2 \geq n > q - \sqrt{pq}/4 + 29p/16 - 3$, satisfy $k \leq q + 1$.

Every $(q + 1)$-arc of PG$(q - 1, q)$ is complete. This is proven in the same way as in the proof of Theorem 3.4.

In PG(n, q), q odd, $2 \leq n \leq q + 2 - 6\sqrt{q \ln q}$, every normal rational curve is complete (Theorem 3.3).

Hence, when

$$q - \frac{\sqrt{pq}}{4} + \frac{29}{16}p - 3 < q + 2 - 6\sqrt{q \ln q}, \tag{1}$$

then in PG(n, q), q odd, $q = p^{2h+1}$, $2 \leq n \leq q - 1$, every normal rational curve is complete.

Since $q = p^{2h+1}$, (1) is equivalent to

$$p^{h+1} > 24p^h\sqrt{p(2h + 1)\ln p} + \frac{29}{4}p - 20. \tag{2}$$

This inequality (2) is satisfied for large prime numbers p. Hence, there exists a lower bound $p_0(h)$ such that (2) is valid for all prime numbers greater than or equal to $p_0(h)$. $\square$

Example 3.6. In PG(n, q), $q = p^3$, p prime, $p > 16830, q - 1 \geq n \geq 2$, every normal rational curve is complete.

Acknowledgment

I especially thank T. Szőnyi for introducing me to the result of S.J. Kovács.

References

1. J.W.P. Hirschfeld, *Finite Projective Spaces of Three Dimensions*, Clarendon Press, Oxford, 1985.
2. H. Kaneta and T. Maruta, "An elementary proof and an extension of Thas' theorem on k-arcs," *Math. Proc. Cambridge Philos. Soc.* **105** (1989), 459–462.
3. S.J. Kovács, "Small saturated sets in finite projective planes," *Rend. Mat.*, to appear.
4. G. Seroussi and R.M. Roth, "On M.D.S. extensions of generalized Reed–Solomon codes," *IEEE Trans. Inform. Theory* **IT-32** (1986), 349–354.
5. L. Storme and J.A. Thas, "Generalized Reed-Solomon codes and normal rational curves: an improvement of results by Seroussi and Roth," in *Advances in Finite Geometries and Designs*, J.W.P. Hirschfeld, D.R. Hughes, and J.A. Thas, eds., Oxford University Press, Oxford, 1991, pp. 369–389.
6. L. Storme and J.A. Thas, "k-arcs and dual k-arcs," *Ann. Discrete Math.*, to appear.
7. J.A. Thas, "Normal rational curves and k-arcs in Galois spaces," *Rend. Mat.* **1** (1968), 331–334.
8. J.A. Thas, "Connection between the Grassmannian $G_{k-1;n}$ and the set of the k-arcs of the Galois space $S_{n,q}$," *Rend. Mat.* **2** (1969), 121–134.
9. J.A. Thas, "Projective geometry over a finite field," in *Handbook of Geometry*, F. Buekenhout, ed., North-Holland, Amsterdam, to appear.
10. J.F. Voloch, "Arcs in projective planes over prime fields," *J. Geom.* **38** (1990), 198–200.
11. J.F. Voloch, "Complete arcs in Galois planes of non-square order," *Advances in Finite Geometries and Designs*, J.W.P. Hirschfeld, D.R. Hughes, and J.A. Thas, eds., Oxford University Press, Oxford, 1991, pp. 401–406.