Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

J. A. Thas

Normal rational curves and $(q+2)$-arcs in a Galois space $S_{q-2,q}$ $(q=2^h)$

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **47** (1969), n.5, p. 249–252.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1969_8_47_5_249_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1969.

Geometria. — *Normal rational curves and* $(q+2)$*-arcs in a Galois space* $S_{q-2,q}$ $(q=2^h)$. Nota di J. A. THAS, presentata (*) dal Socio B. SEGRE.

SUNTO. — Definito il nucleo N di una curva razionale normale C di $S_{r,q}$, dove $q=2^h$, $h\geq 3$, $r=q-2$, si dimostra che – aggregando a C il punto N – si ottiene un $(q+2)$ — arco di $S_{r,q}$.

1. INTRODUCTION.—Let GF(q) denote the Galois field of q elements, where $q=p^h$, p is a prime and h is a positive integer. Denote by $S_{n,q}$ the projective space of n dimensions defined over GF(q).

In $S_{n,q}$, $n\geq 2$, a k–arc is a set of k points such that no $l+2$ lie in an $S_{l,q}$, $l=1,2,\cdots,n-1$ (for a k–arc having $k>n$, the last condition holds for all l when it holds for $l=n-1$) [1].

If $q=2^h$ then $q+2$ is the maximum value of k for which there exist k–arcs in $S_{q-2,q}$ [2]. In [2] we give also a construction of $(q+2)$–arcs in $S_{q-2,q}$ $(p=2)$.

In this short paper we construct a $(q+2)$–arc of $S_{q-2,q}$ $(q=2^h, h\geq 3)$ adding to a normal rational curve of $S_{q-2,q}$ a point defined by it in the manner specified later on and called its nucleus.

2. THEOREM.—*Consider in* $S_{2^t-2,q}$, $q=2^h$ *and* $h\geq t-1\geq 2$, *the normal rational curve* C *which is given by* $x_i=l^{2^t-2-i}m^i$ $(i=0,1,\cdots,2^t-2)$, *where* l, m *are homogeneous parameters (the curve* C *is a* $(q+1)$*-arc of* $S_{2^t-2,q}$*). Then the intersection of the* $q+1$ *osculating hyperplanes of the curve* C *is a* $(2^{t-1}-2)$*-dimensional projective space* $S_{2^{t-1}-2,q}$. *Moreover, the* $q+1$ *tangents of* C *have a point in common with* $S_{2^{t-1}-2,q}$. *The* $q+1$ *points of* $S_{2^{t-1}-2,q}$ *obtained in this manner are those of a normal rational curve* $C^{(1)}$ *of* $S_{2^{t-1}-2,q}$.

Proof.—Consider in $S_{2^t-2,q}$, $q=2^h$ and $h\geq t-1\geq 2$, the normal rational curve C given by $x_i=l^{2^t-2-i}m^i$ $(i=0,1,\cdots,2^t-2)$. Denote by P(l,m) the point P $\in$ C which corresponds with the parameter values l, m. The osculating hyperplane of C in the point P(l,m) is given by the equation

$$\sum_{i=0}^{2^t-2}\binom{2^t-2}{i}m^{2^t-2-i}l^i x_i=0. \tag{1}$$

Now we have

$$\binom{2^t-2}{i}=\frac{(2^t-2)(2^t-3)(2^t-4)\cdots(2^t-i)(2^t-i-1)}{2\cdot 3\cdot 4\cdot\cdots\cdot i}=\theta\cdot(2^t-i-1),$$

(*) Nella seduta del 15 novembre 1969.

with θ odd. Consequently, $\binom{2^t-2}{i}$ is even when i is odd and odd when i is even. So there follows that (1) is equivalent to:

$$\sum_{i=0}^{2^{t-1}-1} m^{2^t-2-2i} l^{2i} x_{2i} = 0.$$

There results that for all l, m the osculating hyperplane of C in the point $P(l, m)$ contains the $(2^{t-1}-2)$–dimensional projective space $S_{2^{t-1}-2,q}$ defined by the equations $x_{2i} = 0$, $i = 0, 1, \cdots, 2^{t-1}-1$. Consequently, the intersection of the $q+1$ osculating hyperplanes of C is at least $(2^{t-1}-2)$–dimensional.

Next consider the 2^{t-1} osculating hyperplanes in 2^{t-1} distinct points $P_1(l_1, m_1), P_2(l_2, m_2), \cdots, P_{2^{t-1}}(l_{2^{t-1}}, m_{2^{t-1}})$ of C (this is always possible, since $2^{t-1} < 2^h + 1 = q + 1$). The intersection of these 2^{t-1} hyperplanes is a $(2^{t-1}-2)$–dimensional projective space if and only if

$$\operatorname{rank}\left[a_{ij} = \delta_j m_i^{2^t-2-j} l_i^j\right]_{1\le i\le 2^{t-1}, 0\le j\le 2^t-2} = 2^{t-1},$$

where

$$\delta_j = \begin{cases} 0 & \text{if } j \text{ is odd} \\ 1 & \text{if } j \text{ is even.} \end{cases}$$

Now we have:

$$\Delta = \left| a'_{ij} = m_i^{2^t-2-2j} l_i^{2j} \right|_{1\le i\le 2^{t-1}, 0\le j\le 2^{t-1}-1} =$$

$$\left| m_i^{2^{t-1}-1-j} l_i^j \right|^2_{1\le i\le 2^{t-1}, 0\le j\le 2^{t-1}-1} = \prod_{i,j} (l_i m_j + l_j m_i)^2,$$

where $i, j \in \{1, 2, \cdots, 2^{t-1}\}$ and $i < j$ (remark: $f : GF(2^h) \to GF(2^h)$, $a \mapsto a^2$ is an automorphism of the Galois field $GF(2^h)$). Since the points $P_1, P_2, \cdots \cdots, P_{2^{t-1}}$ are two by two different, we have $\Delta \neq 0$. It follows immediately that the intersection of the 2^{t-1} hyperplanes is $(2^{t-1}-2)$–dimensional. So we conclude that the projective space $S_{2^{t-1}-2,q}$ is the intersection of the $q+1$ osculating hyperplanes of C.

The tangent of C in the point $P(l, m)$ contains the point

$$P^{(1)}(0, l^{2^t-4}, 0, l^{2^t-6}m^2, 0, l^{2^t-8}m^4, 0, \cdots, 0, m^{2^t-4}, 0) \in S_{2^{t-1}-2,q}.$$

Since $f : GF(2^h) \to GF(2^h)$, $a \mapsto a^2$ is an automorphism of the Galois field $GF(2^h)$, we can use the new parameters l', m' defined by the equations $l' = l^2$, $m' = m^2$. So we obtain

$$P^{(1)}(0, l'^{2^{t-1}-2}, 0, l'^{2^{t-1}-3}m', 0, l'^{2^{t-1}-4}m'^2, 0, \cdots, 0, m'^{2^{t-1}-2}, 0).$$

Consequently, the point $P^{(1)}$ generates the normal rational curve $C^{(1)}$ of $S_{2^{t-1}-2,q}$ given by

$$x_{2^t-2} = x_{2i} = 0 \quad , \quad x_{2i+1} = l'^{2^{t-1}-2-i} m'^i, \qquad i = 0, 1, \cdots, 2^{t-1}-2,$$

and the theorem is proved.

3. DEFINITIONS.—We call the curve $C^{(1)}$ defined in 2. the tangent curve of C. The tangent curve $(C^{(1)})^{(1)}$ of $C^{(1)}$ is denoted by $C^{(2)}$, the tangent curve $(C^{(2)})^{(1)}$ of $C^{(2)}$ is denoted by $C^{(3)}$, etc. Evidently, the curve $C^{(t-2)}$ is an irreducible conic. The nucleus N of this conic is called the nucleus of the normal rational curve C.

Remark.—The point N is also the nucleus of the curves $C^{(1)}, C^{(2)}, \cdots, C^{(t-3)}$.

4. THEOREM.—*Consider in* $S_{q-2,q}$, $q = 2^h$ *and* $h \geq 3$, *the normal rational curve* C *given by* $x_i = l^{q-2-i} m^i$ $(i = 0, 1, \cdots, q-2)$, *where* l, m *are homogeneous parameters. Then, on adding to the* $(q+1)$*-arc* C *its nucleus* N, *there results a* $(q+2)$*-arc of* $S_{q-2,q}$.

Proof.—Consider in $S_{q-2,q}$, $q = 2^h$ and $h \geq 3$, the normal rational curve C given by $x_i = l^{q-2-i} m^i$, $i = 0, 1, \cdots, q-2$ (C is a $(q+1)$-arc of $S_{q-2,q}$). If $x_0^N, x_1^N, \cdots, x_{q-2}^N$ resp. are the coordinates of the nucleus N of C, then $x_i^N = 0$ for all $i \neq \frac{q-2}{2}$. Let us suppose that the hyperplane $S_{q-3,q} \subset S_{q-2,q}$, defined by $q-2$ distinct points $P_1, P_2, \cdots, P_{q-2}$ of C, contains the point N. From the point N we project the curve C on the hyperplane $S^*_{q-3,q}$ with equation $x_{(q-2)/2} = 0$. The projection C′ of C is given by

$$\begin{cases} x_i = l^{q-2-i} m^i \quad , \quad i \neq \frac{q-2}{2} \\ x_{(q-2)/2} = 0 . \end{cases}$$

If $P'_1, P'_2, \cdots, P'_{q-2}$ are the projections of the points $P_1, P_2, \cdots, P_{q-2}$ resp., then we have $P'_i \in S_{q-3,q} \cap S^*_{q-3,q} = S_{q-4,q}$, $i = 1, 2, \cdots, q-2$ (the points $P'_1, P'_2, \cdots, P'_{q-2}$ are two by two different). The collineation $x'_i = x_i^2$ $(i = 0, 1, \cdots, q-2)$ of $S_{q-2,q}$ transforms the curve C′ into the curve C″ with equations

$$(2) \qquad \begin{cases} x'_i = l^{2(q-2-i)} m^{2i} \quad , \quad i \neq \frac{q-2}{2} \\ x'_{(q-2)/2} = 0 . \end{cases}$$

As $a^q = a$, $\forall a \in \mathrm{GF}(q)$, (2) is equivalent to

$$(3) \qquad \begin{cases} x'_0 = l^{q-3} \\ x'_1 = l^{q-5} m^2 \\ x'_2 = l^{q-7} m^4 \\ \quad \vdots \\ x'_{(q-4)/2} = l m^{q-4} \\ x'_{(q-2)/2} = 0 \\ x'_{q/2} = l^{q-4} m \\ x'_{(q+2)/2} = l^{q-6} m^3 \\ \quad \vdots \\ x'_{q-2} = m^{q-3} . \end{cases}$$

Since $q-2$ distinct points of the normal rational curve (3) are linearly independent, there results that the points $P'_1, P'_2, \cdots, P'_{q-2}$ are linearly independent. Consequently, it is impossible that the points $P'_1, P'_2, \cdots, P'_{q-2}$ belong to a same $(q-4)$–dimensional projective space, such that we obtain a contradiction. So every set of $q-2$ two by two different points of C defines a hyperplane of $S_{q-2,q}$ which does not pass through the nucleus N of C. We conclude that $C \cup \{N\}$ is a $(q+2)$–arc of $S_{q-2,q}$.

5. THEOREM.—*If* $s_1, s_2, \cdots, s_{q-2}$ *are* $q-2$ *distinct elements of the Galois field* $GF(q)$, $q = 2^h$ *and* $h \geq 2$, *then*

$$F_{(q-2)/2}(s_1, s_2, \cdots, s_{q-2}) = \sum_{i_1, i_2, \cdots, i_{(q-2)/2}} s_{i_1} s_{i_2} \cdots s_{i_{(q-2)/2}} \neq 0,$$

where $i_1, i_2, \cdots, i_{(q-2)/2} \in \{1, 2, \cdots, q-2\}$ *and* $i_1 < i_2 < \cdots < i_{(q-2)/2}$.

Proof.—Since the theorem is trivial for $h = 2$, we suppose for the remainder of this proof that $h \geq 3$. In $S_{q-2,q}$, $q = 2^h$ and $h \geq 3$, we consider the normal rational curve C given by $x_i = l^{q-2-i} m^i$ $(i = 0, 1, \cdots, q-2)$ and its nucleus N. Next we take the $q-2$ distinct points $P_1(s_1, 1), P_2(s_2, 1), \cdots, P_{q-2}(s_{q-2}, 1)$ of C. Since $C \cup \{N\}$ is a $(q+2)$–arc of $S_{q-2,q}$, it follows that the points $P_1, P_2, \cdots, P_{q-2}, N$ are linearly independent such that

$$\Delta = \begin{vmatrix} 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & 0 \\ s_1^{q-2} & s_1^{q-3} & \cdots & s_1^{q/2} & s_1^{(q-2)/2} & s_1^{(q-4)/2} & \cdots & s_1 & 1 \\ s_2^{q-2} & s_2^{q-3} & \cdots & s_2^{q/2} & s_2^{(q-2)/2} & s_2^{(q-4)/2} & \cdots & s_2 & 1 \\ \cdot & \cdot & & \cdot & \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot & \cdot & & \cdot & \cdot \\ s_{q-2}^{q-2} & s_{q-2}^{q-3} & \cdots & s_{q-2}^{q/2} & s_{q-2}^{(q-2)/2} & s_{q-2}^{(q-4)/2} & \cdots & s_{q-2} & 1 \end{vmatrix} \neq 0.$$

As $\Delta = \prod_{i,j} (s_i + s_j) \cdot F_{(q-2)/2}(s_1, s_2, \cdots, s_{q-2})$, where $i, j \in \{1, 2, \cdots, q-2\}$ and $i < j$, we conclude that $F_{(q-2)/2}(s_1, s_2, \cdots, s_{q-2}) \neq 0$.

Remark.—Squaring Δ and taking account of $a^q = a$, $a \in GF(q)$, we obtain the formula

$$\boxed{F_{(q-2)/2}(s_1, s_2, \cdots, s_{q-2}) = \prod_{i,j} (s_i + s_j)^{-1/2}},$$

$i, j \in \{1, 2, \cdots, q-2\}$ and $i < j$ ($q = 2^h$, $h \geq 2$ and $s_1, s_2, \cdots, s_{q-2}$ two by two different).

BIBLIOGRAPHY.

[1] B. SEGRE, *Introduction to Galois geometries*, « Atti Accad. Naz. Lincei, Mem. Cl. Sc. Fis. Mat. Nat. », (8), *8*, sez. I^a (1967).

[2] J. A. THAS, *Connection between the Grassmannian* $G_{k-1;n}$ *and the set of the k-arcs of the Galois space* $S_{n,q}$, « Rendiconti di Matematica », (6), *2* (1969).