THE CYCLIC ARC OF SIZE $q-\sqrt{q}+1$

G. Korchmáros

1. Introduction

An old but still open problem in Galois geometries is to determine the maximum size of a $k-$arc in $PG(2,q)$ which is not contained in a conic (for q even, in a hyperoval). The only known infinite family of large complete $k-$arcs consists of $(q-\sqrt{q}+1)-$arcs and it contains one such an arc for each square q. This family was originally found by B.C. Kestenband [13] who observed that two non$-$degenerate Hermitian curves can meet over $GF(q)$ in a $(q-\sqrt{q}+1)-$arc. The same family was independently obtained by J.C. Fisher, J.W.P. Hirschfeld and J.A. Thas [6], E. Boros and T. Szönyi [1] and G.L. Ebert [5] who showed that a point$-$orbit under a Singer cycle of size $(q-\sqrt{q}+1)$ is an arc. For this reason, such an arc is called the *cyclic* $(q-\sqrt{q}+1)-$*arc* of $PG(2,q)$ A. Cossidente [3] showed that the existence of a cyclic $(q-\sqrt{q}+1)-$arc in $PG(2,q)$ depends on the fact that each $GF(q^3)-$rational point $P(x,y)$ of the Fermat curve $x^{q+\sqrt{q}+1}+y^{q+\sqrt{q}+1}=1$ is such that at least one of $x^{q+\sqrt{q}+1}$ and $y^{q+\sqrt{q}+1}$ belongs to $GF(q)$.

We are interested in the algebraic envelope Γ' of the cyclic $(q-\sqrt{q}+1)-$arc. To semplify the exposition we will refer to the corresponding algebraic curve Γ in the dual plane of $PG(2,q)$. As it is well known, Γ has degree either $\sqrt{q}+1$, or $2(\sqrt{q}+1)$ according as $q=2^h$ or $q=p^h$ and $p>2$. In the former case, Γ turns out to be projectively equivalent to the Hermitian curve $XY^{\sqrt{q}}+X^{\sqrt{q}}+Y=0$, see [19]. In these notes, we will discuss the properties of the cyclic $(q-\sqrt{q}+1)-$arcs.

An essential tool for the study of large arcs in Π_q is the the following result due to B. Segre [15], [10, Theorem 10.4.3]:

The Fundamental Theorem of B. Segre.

a) The $kt=(q+2-k)$ *1$-$secants through the points of a* $k-$*arc* K *in* Π_q *lie on an algebraic envelope* Γ' *of degree* t *or* $2t$*, according as* q *is even or odd;*

b) Γ' *contains no 2$-$secant of* K *and so no pencil with vertex* P *in* K*;*

c) K *is contained in a larger arc in* Π_q *if and only if* Γ' *has a linear component over* $GF(q)$*.*

In particular, for q *odd,*

d) the t *1$-$secants of* K *through a point* P *of* K *each counts twice in the intersection of* Γ' *with the pencil* $\mathcal{L}_P$ *of lines through* P*;*

e) Γ' *may contain components of multiplicity at most two, but does not consist entirely of 2$-$fold components;*

f) if $k \geq \frac{2}{3}(q+2)$, then Γ' is uniquely determined by K.

The main properties are summarized in the following theorem.

Theorem. *The algebraic envelope of the cyclic $(q-\sqrt{q}+1)$–arc in Π_q, regarded as an algebraic curve Γ_{2t} of degree $2t = 2(\sqrt{q}+2)$ in the dual plane of Π_q, has the following properties:*

i) is absolutely irreducible;
ii) has genus $\frac{1}{2}(q-\sqrt{q})$;
iii) the number of its $GF(q)$–rational points is $q\sqrt{q}+1$;
iv) is classical for the morphism Φ_1;
v) is neither classical nor Frobenius classical for the morphism Φ_2.
vi) the function field of Γ_{2t} is isomorphic to the Hermitian function field.

By ii) and iii), Γ_{2t} has the maximum number of $GF(q)$–rational points allowed by the Hasse–Weil bound. This fact is of interest for applications to coding theory, see [10].

2. Previous results on the envelope of the cyclic $(q-\sqrt{q}+1)$–arc in Π_q, and preliminary remarks to the proof of the Theorem.

Following Singer [17], the projective plane Π_q over $GF(q)$ can be represented by means of a cubic extension $GF(q^3)$ of $GF(q)$: points are non–zero elements of $GF(q^3)$ such that two elements $x, y \in GF(q^3)$ represent the same point of Π_q if and only if $x = \lambda y$, for some element $\lambda \in GF(q)$. The point represented by $x \in GF(q^3)$ will be denoted by (x). Choose a self–dual basis of $GF(q^3)$, regarded as a vector space over $GF(q)$. A scalar product with respect to such a basis is given by $Tr(a, b)$, where (a, b) is the natural scalar product and $Tr(x) = x + x^q + x^{q^2}$ is the trace linear function from $GF(q^3)$ onto $GF(q)$. Then, lines of Π_q are sets $[u]$ where

$$[u] := \{(x) : x \in GF(q^3), Tr(ux) = 0\}.$$

Let ω denote a primitive element of $GF(q^3)$. As the set $\{\omega^0 = 1, \omega^1, \omega^2, \ldots, \omega^{q^2+q}\}$ contains exactly one element from each class representing a point, one gets a representative system for points by choosing ω^i, where i ranges over $\mathcal{Z}_v$, with $v = q^2+q+1$, so that both $\sigma : \omega^i \to \omega^{i+1}$ and $\tau : \omega^i \to \omega^{\sqrt{q}i}$ become permutations on the points of Π_q. Actually, σ is a linear collineation and the group $\mathcal{S}\langle\sigma\rangle$ has order q^2+q+1; τ is a non–linear collineation of order 6. Its square τ^2 is linear, while τ^3 is a Baer involution whose fixed points are those of the subplane of order $\sqrt{q}$ consisting of the points $\omega^{j(\omega-\sqrt{\omega}+1)}$, for $j = 0, 1, \ldots, q+\sqrt{q}$. The normalizer of $\mathcal{S}$ in $PGL(3, q)$ is $\langle\mathcal{S}, \mathcal{U}\rangle$ where $\mathcal{U} = \langle\tau^2\rangle$. τ^3 also normalizes $\mathcal{S}$ and it is the only Baer involution of Π_q having this property. Now, the point–set

$$\mathrm{K} = \{\omega^{j(\omega+\sqrt{\omega}+1)} : j = 0, 1, \ldots, q-\sqrt{q}\},$$

is a $(q-\sqrt{q}+1)-$arc. Clearly, the Singer cycle of size $(q-\sqrt{q}+1)$, i.e. the subgroup $\mathcal{W} = \langle\sigma^{(\omega+\sqrt{\omega}+1)}\rangle$ of $\mathcal{S}$ of order $q-\sqrt{q}+1$, preserves K. Thus K coincides with the orbit of the point (1) under $\mathcal{W}$. The collineation τ also preserves K, and τ^2 has 1 or 3 fixed points on K according as $\sqrt{q} \equiv 0, 1 (\mathrm{mod}\ 3)$ or $\sqrt{q} \equiv 2 (\mathrm{mod}\ 3)$. We see that a collineation group preserving K is $\langle\mathcal{W}, \mathcal{T}\rangle = \mathcal{W}\mathcal{T}$, where $\mathcal{T}\langle\tau\rangle$. Its subgroup of linear collineations is $\langle\mathcal{W}, \mathcal{U}\rangle = \mathcal{W}\mathcal{U}$, where $\mathcal{U} = \langle\tau^2\rangle$. Moreover, τ^3 is a Baer involution which fixes the point (1) and preserves each one of the $\sqrt{q}+1$ 1$-$secants of K through this point. All these results together some further properties of K may be found in [1], see also [6].

Unfortunately, the above "cyclic" model of Π_q does not appear appropriate to investigate the algebraic envelope of K. Alternatively, as K coincides with the point$-$orbit under the Singer cycle of size $q-\sqrt{q}+1$, one may directly work on Π_q, regarding it, in a natural way, as the projective plane coordinatized by $GF(q)$. Although σ may be represented by the "simple" matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ a & b & c & 1 \end{pmatrix},$$

where $x^3 + ax^2 + bx + c$ is an irreducible polynomial over $GF(q)$, one cannot hope to get the equation of the algebraic envelope of K, by using standard arguments. Our method is rather different, as we adopt a special representation for σ, τ^2 and a certain collineation group $\mathcal{G}$ over $GF(q^3)$ cf. Section 3, and we assume a projective frame in the cubic extension $PG(2, q^3)$ of Π_q in such a way that σ transforms into diagonal form, and we look at algebraic curves on $PG(2, q^3)$ which are invariant under $\mathcal{G}$. Clearly, Γ_{2t} is one of them, although Π_q does not lie any longer in canonical position, i.e. Π_q is not the subplane of $PG(2, q^3)$ coordinatized over $GF(q)$. In virtue of some properties of such algebraic curves which we establish in Section 3, we will be able to prove our main Theorem. We also obtain the equation of Γ_{2t}, see (17), which appears quit simple. However, if one changes our special frame with one on Π_q, the equation becomes awful, cf. Remark 1 in Section 3. This may explain why we have said before that the "direct" approach is hopeless when one wants to study the envelope of the cyclic $(q-\sqrt{q}+1)-$arc of Π_q.

3. Preliminary results on curves invariant under a Singer cycle.

Let $\mathcal{F}_q = GF(q)$, where $q = p^r$ with r even and p an odd prime, and let $\mathcal{K} = GF(q^3)$ be a cubic extension of $\mathcal{F}_q$. We introduce the linear collineations of $PG(2, \mathcal{K})$:

$$\alpha : \begin{cases} \rho {x_1}' & = a x_1 \\ \rho {x_2}' & = a^{q+1} x_2 \\ \rho {x_3}' & = x_3, \end{cases}$$

where a denotes a primitive $(q^2+q+1)-$th root of unity over $\mathcal{K}$, and

$$\mu : \begin{cases} \rho {x_1}' & = x_3 \\ \rho {x_2}' & = x_1 \\ \rho {x_3}' & = x_2. \end{cases}$$

We put $\mathcal{A} = \langle \alpha \rangle$ and $\mathcal{M} = \langle \mu \rangle$. The following lemmas are easy to check.

Lemma 1. $\alpha^{q^2+q+1} = 1$, $\mu^3 = 1$, $\mu^{-1}\alpha\mu = \alpha^q$, $|\mathcal{A}| = q^2+q+1$, $|\mathcal{M}| = 3$.

Lemma 2. *$\mathcal{M}$ normalizes $\mathcal{A}$, and $\langle \mathcal{A}, \mathcal{M} \rangle = \mathcal{A}\mathcal{M}$.*

Lemma 3. *α fixes each vertex of the fundamental triangle $A_1A_2A_3$, while μ acts on the vertices as the cycle $(A_1A_2A_3)$.*

The point$-$orbit of the point $E(1,1,1)$ under $\mathcal{A}$ is given by

$$\Pi = \{\alpha^i(E) : i = 0, 1 \ldots, q^2+q\} = \{(a^i, a^{(q+1)i}, 1) : i = 0, 1, \ldots, q^2+q\}.$$

Π may be viewed as a subgeometry of $PG(2,\mathcal{K})$ induced by the lines meeting Π in at least two points. This subgeometry turns out to be a projective plane.

Proposition 1. *Π is isomorphic to $PG(2,\mathcal{F}_q)$. More precisely, Π is a projective subplane of $PG(2,\mathcal{K})$ lying in a non$-$classical position, i.e. $\Pi \neq PG(2,\mathcal{F}_q)$. The lines of Π have equation $tx + t^{q+1}y + 1 = 0$, with t running on the $(q^2+q+1)-$th roots of unity and form the line$-$orbit of $x+y+1=0$ under $\mathcal{A}$.*

Proof. For any two distinct points $P_i = (a^i, a^{(q+1)i}, 1)$ and $P_j = (a^j, a^{(q+1)j}, 1)$ on Π, it suffices to prove that each point $P = (\lambda a + 1, \lambda a^{q+1} + a, \lambda + a^{q+1})$, with $\lambda \in \mathcal{F}_q$ is still on Π. This and the last sentence are easily checked by straightforward calculation which we omit. $\square$

Proposition 2. *The non–linear collineation*

$$\delta : \begin{cases} \rho x_1{}' &= x_1^{\sqrt{q}} \\ \rho x_2{}' &= x_2^{\sqrt{q}} \\ \rho x_3{}' &= x_3^{\sqrt{q}}, \end{cases}$$

of $PG(2,\mathcal{K})$ preserves Π; the action of δ^3 on Π is the same of μ^{-1}, while δ^2 is a Bear involution of Π whose fixed points are $P=(a,a^{q+1},1)$ with $a^{q+\sqrt{q}+1}=1$.

By the above propositions and the previous discussion in Section 2, there is an isomorphism between Π_q and Π so that the collineations σ and τ act on Π_q as the collineations α and δ on Π, respectively. In this isomorphism, $\mathcal{SU}$ and $\mathcal{AM}$ correspond. Hence, to the collineation group $\mathcal{G}=\mathcal{BM}$ of $PG(2,\mathcal{K})$, where $\mathcal{B}=\langle\beta\rangle$,

$$\beta : \begin{cases} \rho x_1{}' &= b x_1 \\ \rho x_2{}' &= b^{q+1} x_2 \\ \rho x_3{}' &= x_3, \end{cases}$$

and b is a primitive $(q-\sqrt{q}+1)-$th root of unity over $\mathcal{K}$. This leads us to study algebraic curves of $PG(2,\mathcal{K})$ which are invariant with respect to $\mathcal{G}$. Actually, we will consider a more general situation in this Section, as we admit b to be any primitive $k-$th root of unity over $\mathcal{K}$ such that $k|(q^2+q+1)$ and $k\geq n$.
Let $\mathcal{C}^n$ denote an algebraic curve defined over $\mathcal{K}$, but viewed as a curve over the algebraic closure $\bar{\mathcal{K}}$ of $\mathcal{K}$. For a fixed non trivial divisor k of (q^2+q+1), we assume that

i) β preserves $\mathcal{C}^n$;

Moreover, we assume that

ii) μ preserves $\mathcal{C}^n$.

Note that the image curve of $\mathcal{C}^n$ under a collineation in $\mathcal{A}-\mathcal{B}$ satisfies i), but not ii) in general. This depends on the fact that an element of $\mathcal{A}$ normalizes $\mathcal{B}$ but not necessarily $\mathcal{BM}$. An exception for $\sqrt{q}\equiv 1(\mathrm{mod}\ 3)$ which will be useful in Section 3 is given by the collineation

$$\kappa : \begin{cases} \rho x_1{}' &= \epsilon x_1 \\ \rho x_2{}' &= \epsilon^2 x_2 \\ \rho x_3{}' &= x_3, \end{cases}$$

where ϵ is a primitive cubic root over $\mathcal{K}$. In fact, κ is in $\mathcal{A}$ but not in $\mathcal{B}$ as of $\epsilon^{q+1} = \epsilon^2$ and $\epsilon^{q-\sqrt{q}+1} = \epsilon \neq 1$. However, κ normalizes $\mathcal{M}$ because of $\kappa\mu\kappa^{-1} = \mu$.
Let $f(x_1, x_2, x_3) = 0$ be a (minimal) equation of $\mathcal{C}^n$. Sometimes, we will also use inhomogeneous coordinates, and write this equation in the form $f(x, y) = 0$ where $x = \frac{x_1}{x_3}$, $y = \frac{x_2}{x_3}$. Recall that each polynomial $f(x, y) \in \mathcal{K}[x, y]$ can be written as the sum of homogeneous polynomials: $f(x, y) = \phi_j(x, y) + \ldots + \phi_n(x, y)$, where ϕ_u, $(j \leq u \leq n)$, has degree u. We will denote the generic term of $\phi_u(x, y)$ by $a_{i,u-i}x^i y^{u-i}$. A surprising property of $\mathcal{C}^n$ depending on i) and ii) is that if $k \geq n$ then $\phi_u(x, y)$ consists of only one term. To prove it we need the following three lemmas.

Lemma 4. *For every i, $(0 \leq i \leq k-1)$, $f(b^i x, b^{(q+1)i} y) = \rho f(x, y)$ holds.*

Lemma 5. *$f(x_1, x_2, x_3) = \rho f(x_2, x_3, x_1) = \tau f(x_3, x_1, x_2)$.*

Lemma 6. *If $a_{i,j-i}x^i y^{j-i}$, $a_{l,m-l}x^l y^{m-l}$ are (non zero) terms in $f(x, y)$, then*

$$m - j \equiv (q+1)(l-i)(mod\ k). \tag{1}$$

Lemma 4 and Lemma 5 are easily checked, and we limite ourselves to give a proof for Lemma 6. By Lemma 4, we have $b^{i+(q+1)(j-i)} = b^{l+(q+1)(m-l)}$, hence $i + (q+1)(j-i) \equiv l + (q+1)(m-l)(\mathrm{mod}\ k)$. Since $q^2 + q + 1 \equiv 0(\mathrm{mod}\ k)$, we get $m - j \equiv (q+1)(l-i)(\mathrm{mod}\ k)$.
¿From now on we assume

iii) $k > n$.

Proposition 3. *For every m $(0 \leq m \leq n)$, $f(x, y)$ has at most one term of degree m.*

Proof. ¿From $m - j \equiv (q+1)(l-i)(\mathrm{mod}\ k)$ and $m - j \equiv (q+1)(l^* - i)(\mathrm{mod}\ k)$, it follows $(q+1)(l^* - l) \equiv 0(\mathrm{mod}\ k)$. As k and $q+1$ are coprime, the latter congruence shows that $l \equiv l^*(\mathrm{mod}\ k)$. As $l, l^* \leq n \leq k$, this implies $l = l^*$. $\square$

Similarly, one may prove

Proposition 4. *For every l, $(0 \leq l \leq n)$, $f(x, y)$ has at most one term of degree l in x and at most one term of degree $n - l$ in y.*

Next we examine the case where

iv) no fundamental line is a component of $\mathcal{C}^n$.

By Proposition 4, $f(x, y)$ has only one linear term in x, and the same is true for x. Hence,

$$f(x, y) = a_{m_1,0}x^{m_1} + \ldots + a_{0,m_2}y^{m_2}.$$

¿From (1) we get immediately

Lemma 7. *For any two integers i,j, if $a_{i,j-i}\neq 0$ we have*

$$m_1 \equiv j + q(j-i)(mod\ k); \tag{2}$$

$$m_2 \equiv j - i(q+1)(mod\ k); \tag{3}$$

$$m_1 - m_2 \equiv i + jq(mod\ k). \tag{4}$$

Now, we deduce from iii) some relations among the coefficients of $f(x,y)$.

Lemma 8. *For any two integers l,m $(0\leq l,m\leq n)$, we have*

$$a_{l,m-l} = \epsilon a_{n-m,l} = \epsilon^2 a_{m-l,n-m}, \tag{5}$$

with $\epsilon^3 = 1$.

Proof. Since μ preserves $\mathcal{C}^n$, we have $a_{l,m-l} = \epsilon a_{m-l,n-m}$, and $a_{m-l,n-m} = \epsilon a_{l,m-l}$, for every m with $j\leq m\leq n$. Now (5) follows immediately because these relations imply $\epsilon^3 = 1$. □

¿From (1) and (5) we get some other relations

$$(n-m+l) - j \equiv (q+1)(n-m-i)(\text{mod } k); \tag{6}$$

$$(n-l) - j \equiv (q+1)(m-l-i)(\text{mod } k); \tag{7}$$

$$2l - m \equiv (q+1)(n-2m+l)(\text{mod } k). \tag{8}$$

As the algebraic envelope of a $k-$arc has degree $2t$ with $k = q-t+2$, we specify our curve $\mathcal{C}^n$ by assuming from now on that

v) $n = 2t$, $k = q+2-t$, $t > 2$.

Clearly, this implies

$$2(q+2) \equiv n(\text{mod } k). \tag{9}$$

We prove that $\mathcal{C}^n$ has a $2-$fold point at the origin.

Lemma 9.

$$m_1 = n-2, \quad m_2 = 2. \tag{10}$$

Proof. For $l = 0$ (and $m = m_2$), from (8) we have that $(2q+1)m_2 \equiv n(q+1) (\mathrm{mod}\ k)$. As $q^2+q+1 \equiv 0 (\mathrm{mod}\ k)$, this implies $n \equiv (q+2)m_2 (\mathrm{mod}\ k)$. By (9), then $2(q+2) \equiv (q+2)m_2 (\mathrm{mod}\ k)$. If $(k,q+2)= 1$, this yields $m_2 \equiv 2 (\mathrm{mod}\ k)$, and hence $m_2 = 2$. Otherwise, $(k,q+2)= 3$, and either $m_2 \equiv 2 (\mathrm{mod}\ k)$ or $m_2 \equiv 6 (\mathrm{mod}\ k)$ holds. Since $m_2 \leq n$ and, by iii), $n < k$, we see that either $m_2 = 2$ or $m_2 = 6$. We prove now that the latter case cannot occour. In fact, from $m_2 = 6$ it would follow $4(q+2) \equiv 0 (\mathrm{mod}\ k)$, and hence $q+2 \equiv 0 (\mathrm{mod}\ k)$ because k is odd. But this contradicts $(k,q+2)$=3. Thus, $m_2 = 2$, that is $a_{0,2} \neq 0$. Putting $l = 0$, $m = 2$, (5) becomes $a_{0,2} = \epsilon a_{n-2,0}$, which shows that $m_1 = n-2$. □

Lemma 10.

$$i = 0, \quad j = 2. \tag{11}$$

Proof. We have to prove that the term $a_{i,j-i}x^i y^{j-i}$ of lowest degree in $f(x,y)$ is $a_{0,2}y^2$, with $a_{0,2} = a_{0,m_2}$. Assume on the contrary that $f(x,y)$ has a non−zero term of degree one, i.e. either $a_{1,1}x$ or $a_{0,1}y$. By (2), we have in the former case $n \equiv 3 (\mathrm{mod}\ k)$, in the latter case $m_2 \equiv 1 (\mathrm{mod}\ k)$. In both cases, we get a contradiction with v).
In virtue of (11), (1) becomes

$$m \equiv (q+1)l + 2 (\mathrm{mod}\ k), \tag{12}$$

or, equivalently,

$$m \equiv (t-1)l + 2 (\mathrm{mod}\ k). \tag{13}$$

□

Proposition 5. *Each vertex of the fundamental triangle is a 2−fold cuspidal point of $\mathcal{C}^n$ such that one of the fundamental lines through the vertex is the tangent and has intersection multiplicity $n-2$ with $\mathcal{C}^n$ at the vertex, namely*

$$I(\mathcal{C}^n, x_1 = 0; A_2) = I(\mathcal{C}^n, x_2 = 0; A_3) = I(\mathcal{C}^n, x_3 = 0; A_1) = n-2$$

Proof. Putting $a_{0,2} = 1$, from Lemmas 9, 10 and (5) we get

$$f(x,y) = y^2 + \epsilon x^{n-2} + \epsilon^2 x^2 y^{n-2} + \ldots$$

Hence, A_3 is a 2−fold point. By Proposition 3, $f(x,y)$ has only one term of degree 2. By Lemma 2, this term is $a_{0,2}y^2$, and we may put $a_{0,2} = 1$. This shows that A_3 is a 2−fold cuspidal point such that the tangent line is $x = 0$. From Proposition 4 we know that ϵx^{n-2}

is the only term which does not contain y, so we see that the intersection multiplicity of $\mathcal{C}^n$ with $x=0$ is $n-2$, i.e. $I(\mathcal{C}^n, x_2=0; A_3)=n-2$. As $\mathcal{M}$ acts transitively on the vertices of the fundamental triangle, the same holds for A_1 and A_2.
By Proposition 4, we have either two linear branches or one quadratic branch centered at A_3.
Let

$$\xi(t)=t, \quad \eta(t)=a_0t^d+\ldots+a_it^{d+\alpha_i}+\ldots \tag{14}$$

where $a_0\neq 0$, be a primitive representation of a linear branch γ of $\mathcal{C}^n$ centered at A_3. As β preserves $\mathcal{C}^n$ and fixes A_3, either β preserves γ or β interchanges γ with the other linear branch of $\mathcal{C}^n$ centered at A_3. Since β has odd order, the latter case is not possible, and hence β preserves γ. Therefore, β maps the pair $(\xi(t),\eta(t))$ into the pair $(b\xi(t), b^{q+1}\eta(t))$. Since the latter pair is still a primitive representation of γ, there exixts a linear substitution in $\mathcal{K}[[t]]$, say $t\to ct+\ldots$, such that $b\xi(t)=\xi(ct+\ldots)$ and $b^{q+1}\eta(t)=\eta(ct+\ldots)$. We see that this substitution must be $t\to bt$. Then $b^{q+1}=b^d$, and hence $q+1\equiv d(\mathrm{mod}\ k)$. In virtue of (9), this yields $2d+2\equiv n(\mathrm{mod}\ k)$. Since $d\leq n$, from iii) we get $2d+2=n$, and

$$\xi(t)=t \quad \eta(t)=a_0t^{(n/2)-1}+a_1t^{(n/2)-1+\alpha_1}+a_2t^{(n/2)-1+\alpha_1+\alpha_2}+\ldots \tag{15}$$

where $\alpha_i\equiv 0(\mathrm{mod}\ k)$, for $i\geq 1$.
A similar argument shows that if γ is assumed to be a quadratic branch of $\mathcal{C}^n$ centered at A_3, then a primitive representation of γ is given by

$$\xi(t)=t^2 \quad \eta(t)=a_0t^{n-2}+a_1t^{n-2+\alpha_1}+a_2t^{n-2+\alpha_1+\alpha_2}+\ldots \tag{16}$$

where $\alpha_i\equiv 0(\mathrm{mod}\ k)$. $\square$

4. Some properties of the envelope of the cyclic $(q-\sqrt{q}+1)$−arc in Π_q.

The envelope of the cyclic $(q-\sqrt{q}+1)$−arc in Π_q may be regarded as an algebraic curve Γ_{2t} of degree $2t=2(\sqrt{q}+1)$ over $GF(q)$, and hence on $PG(2,\mathcal{F}_q)$. Choose three points A_1', A_2', A_3', on Π such that $A_1'A_2'A_3'E$ is a non degenerate quadrangle. Let κ be a linear collineation which sends A_i to A_i', $(i=1,2,3)$ and fixes E. Since A_i' lies on $PG(2,\mathcal{K})$, the image of Γ_{2t} under κ is an algebraic curve $\mathcal{C}^n$ of degree $n=2(\sqrt{q}+1)$ over $GF(q^3)$. As we will see, $\mathcal{C}^n$ satisfies all the conditions i) − v). Moreover, $\mathcal{C}^n$ satisfies the extra condition of having some t−tangents, because of the Fundamental Theorem of B. Segre.
Let us write this extra condition in terms of $PG(2,\mathcal{K})$. By a) of the Fundamental Theorem of B. Segre, every point of K, viewed as a line in the dual plane, is a t−tangent of Γ_{2t}. As we have seen in Section 2, one of the points on K, namely (1), is also a fixed point of τ^2. Hence, to identify the corresponding line in $PG(2,\mathcal{K})$, we have only to look for fixed lines of δ^2 on Π. Since, by Proposition 2, δ^2 and μ^{-1} have the same action on Π, this may be done by determining the fixed lines of μ^{-1}. An easy calculation shows that for $p=3$, μ^{-1}

fixes only one line $r_0 : x_1 + x_2 + x_3 = 0$, while, for $p > 3$, there are other two lines fixed by μ^{-1}, namely $r_1 : \epsilon x_1 + \epsilon^2 x_2 + x_3 = 0$, and $r_2 : \epsilon^2 x_1 + \epsilon x_2 + x_3 = 0$, where ϵ is a primitive cubic root of unity over $\mathcal{K}$. Note that both r_1 and r_2 belong to Π because of $\epsilon^{q^2+q+1} = 1$. Thus, for $p = 3$, r_0 is the $t-$tangent corresponding to the point (1).
For $p > 3$, we only know that one of the lines r_0, r_1, r_2 corresponds to (1), and hence at least one of them is a $t-$tangent to $\mathcal{C}^n$. This depends on the fact that the collineation $\kappa \in \mathcal{A}$ introduced in Section 2, preserves the set of these three lines and acts on it as the cycle $(r_0 r_1 r_2)$. In fact, for $\sqrt{q} \equiv 2(\text{mod } 3)$, κ belongs to $\mathcal{B}$ and by i) preserves $\mathcal{C}^n$; hence, each of the three lines r_0, r_1, r_2, is a $t-$tangent of $\mathcal{C}^n$. For $\sqrt{q} \equiv 1(\text{mod } 3)$, κ does not belong to $\mathcal{B}$, but we may replace $\mathcal{C}^n$ by its image under κ, as we explained in Section 2; therefore, by applying κ we may obtain that r_0 becomes a $t-$tangent of a curve projectively equivalent with $\mathcal{C}^n$ which still satisfies all the conditions i), ii), iii) and v). We prove that iv) is also satisfied. Clearly, if $\mathcal{C}^n$ had a linear component $\mathcal{L}$, then $\mathcal{L}$ would coincide with one of the fundamental lines. As we have seen, some lines r are $t-$tangents to $\mathcal{C}^n$ such that each one of the t tangency points of $\mathcal{C}^n$ with r is on Π. Hence, the above linear component $\mathcal{L}$ meets r on Π. Actually, this does not occour because Π is disjoint from the fundamental lines, a contradiction.
We are able to determine the equation of $\mathcal{C}^n$.

Proposition 6. *The algebraic envelope associated to the cyclic $(q-\sqrt{q}+1)-$arc, regarded as an algebraic curve $\mathcal{C}^n$ in $PG(2,\mathcal{K})$, has equation*

$$f(x,y) = y^2 + x^2y^{2\sqrt{q}} + x^{2\sqrt{q}} - 2(x^{\sqrt{q}+1}y^{\sqrt{q}} + x^{\sqrt{q}}y + xy^{\sqrt{q}+1}) = 0. \tag{17}$$

Proof. For any term $a_{l,m-l}x^l y^{m-l}$ in the equation $f(x,y) = 0$ of $\mathcal{C}^n$, we find by (5) two more terms in $f(x,y)$, namely $a_{n-m,l}x^{n-m}y^l$, and $a_{m-l,n-m}x^{m-1}y^{n-m}$. Relabelling indices we may suppose that $a_{l,m-l}x^l y^{m-l}$, with $0 \le l \le \frac{1}{3}n$, is a term in $f(x,y)$. As in our case, $n = 2t$ with $t = \sqrt{+1}$, we have

$$(t-1)l + 2 \le \frac{2}{3}(t-1)t + 2 = \frac{2}{3}(q-\sqrt{q}) + 2 < q - \sqrt{q} + 1 = k.$$

By $m \le 2t < k$ and (13), $m = \sqrt{q}l + 2$ follows. Hence, $\sqrt{q}l + 2 \le 2\sqrt{q} + 2$, which implies $l \le 2$. We see that the pair $(l, m-l)$ coincides with one of the pairs $(0,2)$, $(1, \sqrt{q}+1)$, $(2, 2\sqrt{q})$. This shows that

$$f(x,y) = y^2 + \epsilon_1 x^2 y^{2\sqrt{q}} + \epsilon^2 x^{2\sqrt{q}} + c(x^{\sqrt{q}+1}y^{\sqrt{q}} + \epsilon_2 x^{\sqrt{q}}y + {\epsilon_2}^2 xy^{\sqrt{q}+1}) = 0, \tag{18}$$

where $c \in \mathcal{K}$ and ${\epsilon_1}^3 = 1$, ${\epsilon_2}^3 = 1$. We distinguish three cases according as $p = 3$, $\sqrt{q} \equiv 1(\text{mod } 3)$, and $\sqrt{q} \equiv 2(\text{mod } 3)$. If $p = 3$, we have obviously $\epsilon_1 = \epsilon_2 = 1$. As we have previously noted, $r_0 : x_1 + x_2 + x_3 = 0$ is a $t-$tangent to $\mathcal{C}^n$. Let $y = -(x+1)$. Then $f(x,y)$ becomes the polynomial $h(x) = f(x, -(x+1))$ of degree $2t = 2\sqrt{q} + 2$ where

$$h(x)=1+(2+c)x+(2+c)x^2-cx^{\sqrt{q}}-cx^{\sqrt{q}+1}+(2+c)x^{\sqrt{q}+2}+x^{2\sqrt{q}}-cx^{2\sqrt{q}+1}+x^{2\sqrt{q}+2}.$$

As $h(x)$ must have t two−fold roots, $h(x)$ must be the square of a polynomial in x over $\bar{\mathcal{K}}$. A straightforward calculation shows that this holds if and only if either $c=-2$, and $h(x)=(1+x^{\sqrt{q}}+x^{\sqrt{q}+1})^2$, or $c=2$, and $h(x)=(1+2x-x^{\sqrt{q}}+x^{\sqrt{q}+1})^2$. In the latter case $f(x,y)$ turns out to be the square of $y+xy^{\sqrt{q}}+x^{\sqrt{q}})$. But this would mean that $\mathcal{C}^n$ consists entirely of double components contradicting e) of the Fundamental Theorem of k−arcs. This completes the proof for $p=3$.
If $\sqrt{q}\equiv 2(\mathrm{mod}\ 3)$, $\epsilon^{\sqrt{q}}=\epsilon^2$ holds for a primitive cubic root ϵ of unity over $\mathcal{K}$. Thus ϵ does not belong to $\mathcal{F}_q$. Since the collineation δ preserves $\mathcal{C}^n$, in the sense that the image curve of $\mathcal{C}^n$ under δ coincides with $\mathcal{C}^n$ counted $\sqrt{q}$ times, we see that both $\epsilon_1=\epsilon_1^{\sqrt{q}}$, $\epsilon_2=\epsilon^{\sqrt{q}}$ hold. Hence, $\epsilon_1=\epsilon_2=1$, and we may argue as before to prove Proposition 6.
Finally, suppose $\sqrt{q}\equiv 1(\mathrm{mod}\ 3)$. Note that then $\epsilon^{\sqrt{q}}=\epsilon$. The linear collineation μ fixes both $\mathcal{C}^n$ and r_0, and hence preserves the set of the t tangency points of $\mathcal{C}^n$ on the line r_0. As $t\equiv 2(\mathrm{mod}\ 3)$ in our case, two of these points are left fixed. Since μ has only three fixed points, namely $P(\epsilon,\epsilon^2,1)$, $Q(\epsilon^2,\epsilon,1)$, $E(1,1,1)$, and $E(1,1,1)$ does not lie on r_0, these two points are P and Q. For $\epsilon_1=1$, since P lies on $\mathcal{C}^n$, from (18) $\epsilon_2=1$, $c=-2$ follow. Hence, to complete the proof of Proposition 6, it suffices to show that $\epsilon_1=1$. If, instead, $\epsilon_1\neq 1$, let us change the frame by the substitutions $x=\epsilon_1 x'$, $y={\epsilon_1}^2 y'$. Then (18) becomes

$$f(x',y')=y'^2+x'^2y'^{2\sqrt{q}}+x'^{2\sqrt{q}}+c(x'^{\sqrt{q}+1}y'^{\sqrt{q}}+\epsilon x'^{\sqrt{q}}y'+\epsilon^2x'y'^{\sqrt{q}+1})=0 \qquad (19)$$

with $\epsilon^3=1$ and P (or Q) has coordinates $(1,1)$ with respect to the new frame. Moreover, one of r_1 and r_2 becomes the line of equation $x'+y'+1=0$. Since both points P and Q lie on $\mathcal{C}^n$, this implies that $(1,1)$ satisfies (18), and hence $\epsilon=1$, $c=-2$. As we have already seen, the line $x'+y'+1=0$ is then a t−tangent to $\mathcal{C}^n$. But this is not possible because neither r_1 nor r_2 is a t−tangent to $\mathcal{C}^n$. □

Remark 1.

To get a (minimal) equation of the algebraic envelope of the cyclic $(q-\sqrt{q}+1)$−arc, regarded as an algebraic curve Γ_{2t} over Π_q, one needs to bring Π into canonical position by mapping a frame of Π onto the frame $\{A_1,A_2,A_3,E\}$ of $PG(2,\mathcal{K})$. For a primitive (q^2+q+1)−root of unity a over $\mathcal{K}$, one may take the points ${A_1}'=(a,a^{q+1},1)$, ${A_2}'=(1,a,a^{q+1})$, ${A_3}'=(a^{q+1},1,a)$, and E as vertices of a frame of Π, so that the map which has matrix

$$\begin{pmatrix} a & 1 & a^{q+1}\\ a^{q+1} & a & 1\\ 1 & a^{q+1} & a \end{pmatrix},$$

sends $\{A_1, A_2, A_3, E\}$ to $\{A_1', A_2', A_3', E\}$. Hence, writing (17) in homogeneous coordinates, say $f(x_1, x_2, x_3) = 0$, and substituting (x_1, x_2, x_3) by (x_1', x_2', x_3') where

$$x_1' = ax_1 + x_2 + a^{q+1}x_3$$
$$x_2' = a^{q+1}x_1 + ax_2 + x_3$$
$$x_3' = x_1 + a^{q+1}x_2 + ax_3,$$

one may find the "canonical" equation $f(x_1', x_2', x_3')$ of Γ_{2t}. We do not report this tedious calculation, neither do we write $f(x_1', x_2', x_3')$ explicitely.

Proposition 7. *The algebraic envelope of the cyclic $(q - \sqrt{q} + 1)-$arc, regarded as an algebraic curve $\mathcal{C}^n$ in $PG(2, \mathcal{K})$, is not a component of its Hessian curve.*

Proof. It is straightforward to prove that the Hessian curve $\mathcal{C}^n$ has only linear components, namely the fundamental lines each counted $2\sqrt{q}$ times. □

Next we determine the branches of $\mathcal{C}^n$ which are centered at singular points.

Proposition 8. *The algebraic envelope of the cyclic $(q - \sqrt{q} + 1)-$arc, regarded as an algebraic curve $\mathcal{C}^n$ in $PG(2, \mathcal{K})$, has exactly three singular points, namely, A_1, A_2 and A_3. Each of them is a $2-$fold point and is the center of a quadratic branch of $\mathcal{C}^n$.*

Proof. ¿From Proposition 5, each fundamental point A_1, A_2, A_3 is singular, and a fundamental line meets $\mathcal{C}^n$ in only two fundamental points. For a singular point $P(x, y)$, we have $f(x, y) = 0$, and both

$$f_x(x, y) = 2(xy^{2\sqrt{q}} - x^{\sqrt{q}}y^{\sqrt{q}} - y\sqrt{q} + 1) = 2y^{\sqrt{q}}(xy^{\sqrt{q}} - x^{\sqrt{q}} - y) = 0;$$

$$f_y(x, y) = 2(y - x^{\sqrt{q}} - xy^{\sqrt{q}}) = 0.$$

It is easily seen that then $(x, y) = (0, 0)$. This shows that A_1, A_2 and A_3 are the only singular points of $\mathcal{C}^n$. Assume that there exists a linear branch of $\mathcal{C}^n$ centered at A_3. Then, as we have seen, a primitive representation is given by (15) with $n = 2(\sqrt{q} + 1)$ and $k = q - \sqrt{q} + 1$. But a straightforward calculation shows that no elements a_0, a_1, $a_2, \cdots \in \bar{\mathcal{K}}$ exist such that

$$f(t, a_0t^{2\sqrt{q}} + a_1t^{2\sqrt{q}-1+k_1(q-\sqrt{q}+1)} + a_2t^{2\sqrt{q}-1+k_2(q-\sqrt{q}+1)} \ldots) = 0.$$

for some positive integers k_1, k_2, ... Therefore, $\mathcal{C}^n$ has a quadratic branch centered at A_3, and the same holds for the other two fundamental points. Note that a primitive representation of the quadratic branch of $\mathcal{C}^n$ is given by

$$x = t^2, \quad y = t^{2\sqrt{q}} + t^{q+\sqrt{q}+1} + \dots \tag{20}$$

□

5. Proofs of i), ii) and iii) of the Theorem.

Assume on the contrary that $\mathcal{C}^n$ has a non trivial component $\mathcal{C}^d$ over $\bar{\mathcal{K}}$. Then $\mathcal{C}^d$ cannot be linear, because such a linear component would be a fundamental line contradicting iv). Without loss of generality, we may assume that $d \le \sqrt{q}+1 = \frac{n}{2}$. By Proposition 8, $\mathcal{C}^d$ passes through a fundamental point, say A_3. By Lemma 4, for every i, $(0 \le i \le q-\sqrt{q})$, the image curve ${\mathcal{C}_i}^d$ of $\mathcal{C}^d$ under β^i is still a component of $\mathcal{C}^n$. Then ${\mathcal{C}_i}^d$ also is. Since A_3 is only a $2-$fold point of $\mathcal{C}^n$, we infer that ${\mathcal{C}_i}^d = {\mathcal{C}_{i+2}}^d$. As $q-\sqrt{q}+1$ is odd, $\mathcal{C}^d = {\mathcal{C}_i}^d$ follows. This shows that β preserves $\mathcal{C}^d$. By Lemma 6 (which depends only on i) and thus is valid for $\mathcal{C}^d$), for any two non$-$zero terms $a_{i,j-l}x^iy^{j-i}$, $a_{l,m-l}x^ly^{m-l}$ in a minimal equation $d(x,y)=0$ of $\mathcal{C}^d$,

$$m - j \equiv 2\sqrt{q}(l-i)(\bmod\ q-\sqrt{q}+1). \tag{21}$$

Assume firstly that A_3 is a simple point of of $\mathcal{C}^d$. If $y=0$ is the tangent line of $\mathcal{C}^d$ at A_3, then we put $i=0$, $j=1$ in (21) and infer from it

$$j \equiv 2\sqrt{q}i + 1(\bmod\ q-\sqrt{q}+1). \tag{22}$$

Since $0 \le i \le j \le d \le \sqrt{q}+1$, (22) yields only three pairs (i,j), namely $(0,1)$, $(1,\sqrt{q}+1)$ and $(\sqrt{q},\sqrt{q})$. Hence, $\mathcal{C}^d$ has equation $d(x,y) = y + uxy^{\sqrt{q}} + vx^{\sqrt{q}}$, $u,v \in \bar{\mathcal{K}}$. Here $u \ne 0$, as one may easily check that $y + vx^{\sqrt{q}}$ does not divide the polynomial $f(x,y)$ given in (17). Thus, each fundamental point belongs to $\mathcal{C}^d$. By Lemma 5, the image $\bar{\mathcal{C}_1}^d$ (resp. $\bar{\mathcal{C}_2}^d$) of $\mathcal{C}^d$ under μ (resp. μ^2) is still a component of $\mathcal{C}^n$. This implies that $\mathcal{C}^d = \bar{\mathcal{C}_1}^d = \bar{\mathcal{C}_2}^d$. In fact, if two of them were different, then they would be $3-$fold for $\mathcal{C}^n$. On the other hand, from what we have seen above, $\mathcal{C}^d$ satisfies i)$-$iv). By Lemma 10, this would imply that A_3 is a $2-$fold point of $\mathcal{C}^d$ which contradicts our hypothesis. We may suppose that each fundamental point belonging to $\mathcal{C}^d$ is a $2-$fold point. If $\mathcal{C}^m$ is a non$-$trivial component of $\mathcal{C}^n$ different from $\mathcal{C}^d$, then the common points of $\mathcal{C}^d$ and $\mathcal{C}^m$ are fundamental points, and because of Proposition 8, no other point of $\mathcal{C}^n$ is singular. Thus, at least one fundamental point must be $3-$fold for $\mathcal{C}^n$ contradicting Proposition 8. This completes the proof of i). To show ii), we have to evaluate the lowering of the genus g of $\mathcal{C}^n$, (which is certainly equal to the genus of Γ_{2t}) due to the three singular points A_1, A_2 and A_3. As it is known (see [16]), every singular point Q of an irreducible plane curve Γ lowers the genus not only by a quantity depending on the nultiplicity of Q, but also in the points infinitely close to Q. More precisely, if Q is a point of multiplicity r of γ, viewed as a branch of order r, and $Q_1,\dots,Q_m$ are the points infinitely near to Q (also called successive points of Q) of respective multiplicities $\rho_1,\dots,\rho_m$, then g is lowered by $\frac{1}{2}\sum_{i=0}^m \rho_i(\rho_i-1)$, where $\rho_0 = r$. The formula for the genus of Γ is

$$g = \frac{1}{2}(n-1)(n-2) - \frac{1}{2}\sum_{Q\in\Gamma}\sum_{i=0}^{m}\rho_i(\rho_i - 1)$$

where n denotes the degree of Γ.
Clearly, the successive points of the branch of $\mathcal{C}^n$ centered at A_3, given by the primitive representation (20), are still 2−fold and their total number equals $\frac{1}{2}(q+\sqrt{q})$, see [2]. The same holds for the two other fundamental points. Thus we get $g = (2\sqrt{q}+1)\sqrt{q} - \frac{3}{2}(q+\sqrt{q}) = \frac{1}{2}(q-\sqrt{q})$. By a) of the Fundamental Theorem of k−arcs, we know that the algebraic envelope, regarded as an algebraic curve of degree $2\sqrt{q}+2$ on the dual plane, has at least $q\sqrt{q}+1$ points on Π_q, each of them is a simple point by Proposition 8. Since $q+1-2g\sqrt{q} = q\sqrt{q}+1$, the Hasse−Weil bound shows that this is the maximum.

6. Proofs of iv) and v) of the Theorem.

We need some previous results from [8] and [18]. We start by summarizing them. Let $\mathcal{L}$ denote an algebraically closed field of characteristic $p \geq 0$. Let X be an irreducible algebraic curve in $PG(r,\mathcal{L})$ which is not contained in a hyperplane. Points on X will be viewed as branches. The order−sequence at a point$P \in X$ is defined to be the set $\{j_0 = 0, j_1, \ldots, j_r\}$ of intersection multiplicities at the point P of X with the hyperplanes of $PG(r,\mathcal{L})$. Almost all points of X have the same order−sequence which is called the order−sequence of X and is denoted by $\{\epsilon_0 = 0, \epsilon_1 \ldots, \epsilon_r\}$, where $\epsilon_0 < \epsilon_1 < \ldots < \epsilon_r$. In characteristic 0, this order−sequence is $\{0,1,\ldots,r\}$. For this reason, X is said to have classical orders if $\epsilon_i = i$, $(i = 0,1,\ldots,r)$. The order−sequence of X is also characterized as the smallest sequence of natural numbers (in the lexicographic order) for which the Wronskian $\det({D_t}^{(\epsilon_i)}x_j) \neq 0$, where ${D_t}^{(j)}$ id the j−th Hasse derivative with respect to the separating variable t and $x_0, x_1, \ldots, x_r$ are the coordinate functions. Now, let $\mathcal{L}$ be the algebraic closure of the Galois field $\mathcal{F}_q$, and suppose that X is defined over $\mathcal{L}$. ¿From the sequence $\{\epsilon_0 = 0, \ldots, \epsilon_r\}$ one can select a subsequence $\{\nu_0 = 0, \nu_1, \ldots, \nu_{r-1}\}$ (the so−called Frobenius order−sequence over $\mathcal{F}_q$ of X) with the property of being the smallest sequence in the lexicographic order for which the following determinant does not vanish identically

$$\left\| \begin{matrix} {x_0}^q & \ldots & \ldots & {x_r}^q \\ {D_t}^{(\nu_0)}x_0(P) & \ldots & \ldots & {D_t}^{(\nu_0)}x_r(P) \\ \vdots & \vdots & \vdots & \vdots \\ {D_t}^{(\nu_{r-1})}x_0(P) & \ldots & \ldots & {D_t}^{(\nu_{r-1})}x_r(P) \end{matrix} \right\|. \tag{23}$$

X is said to have Frobenius order−sequence over $\mathcal{F}_q$ if $\nu_i = i$, $(i = 0,1,\ldots,r-1)$. In this case, the image P' of a generic point of X under the Frobenius collineation $(x_0,\ldots,x_r) \to (x_0^q,\ldots,x_r^q)$ does not lie on the osculating hyperplane $\mathcal{H}_P$ at P. On the contrary, when $P' \in \mathcal{H}_P$ for each $P' \in \mathcal{H}_P$ for each $P \in X$, the curve if Frobenius non−classical. THe interest in Frobenius order−sequences comes from a deep result due to Stöhr and Voloch [18, Theorem 21.3 and Proposition 2.4] which gives an upper bound for the number N of $\mathcal{F}_q$−rational points of X:

$$N \leq \frac{1}{r}[(\nu_1+\ldots,\nu_r)(2g-2)+(q+r)m], \tag{24}$$

where m is the degree of X. This upper−bound improve the Hasse−Weil bound in several circumstances.
In the simplest case, $r=2$, X is non−classical if and only if X is a component of its Hessian curve, see [18]. Hence, from Proposition 7 we get that $\mathcal{C}^n$ is classical, i.e. classical with respect to the trivial morphism $\Phi_1:(x,y,1)\to(x,y,1)$. This proves iv).
Now we focus our attention to the Veronese morphism $\Phi_2: PG(2,\mathcal{L})\to PG(5,\mathcal{L})$ given by $(x,y,1)\to(1,x,x^2,y,xy,y^2)$. Note that, the order−sequence $\{j_0=0,j_1,\ldots,j_5\}$ gives the intersection multiplicities at P with the conics of $PG(2,\mathcal{L})$. Given a Φ_1−classical curve of equation $f(x,y)=0$, if there exist $h,z_0,\ldots,z_5\in\mathcal{L}[x,y]$ such that $hf=z_0+z_1^{p^\nu}+z_2^{p^\nu}x^2+z_3^{p^\nu}y+z_4^{p^\nu}xy+z_5^{p^\nu}y^2$, then this curve is non−classical with respect to Φ_2, its order sequence being $(0,1,2,3,4,p^\nu)$. This was proved in [7, Theorem 1 and discussion in Section 2]. Thus, the first statement of v) follows immediately from (17). ¿From (24) we obtain

$$q+\sqrt{q}+1\leq\frac{1}{5}[(\nu_1+\ldots+\nu_4)(q-\sqrt{q}-2)+4(q+5)(\sqrt{q}+1)],$$

whence, $\nu_1+\ldots,\nu_4\geq 3+\sqrt{q}$. Thus $\nu_i=i$, $(i=1,2,3)$, but $\nu_4=\sqrt{q}$. Our last observation is that an alternative proof of v) independing of (24) may be done following Garcia and Voloch [8] although their approach needs the canonical equation of Γ_{2t}, see Remark 1.

7. The Function Field of Γ_{2t}.

We have seen that the algebraic envelope of the cyclic $(q-\sqrt{q}+1)$−arc in Π_q, regarded as an algebraic curve Γ_{2t} has the maximum number of $GF(q)$−rational points allowed by the Hasse−Weil bound. Using an algebraic terminology, we say that the function field of Γ_{2t} is maximal. A necessary condition for maximality is that q is a square. For instance a Hermitian function field is maximal. Conversely, in [14] Rück and Stichtenoth proved that the Hermitian function field is the only maximal function field over $\mathcal{F}_q$, q square of genus $\frac{1}{2}(q-\sqrt{q})$. As a consequence we conclude from our Theorem that the function field of Γ_{2t} is isomorphic but actually not projectively equivalent to a Hermitian curve. We give a direct proof of this isomorphism. We begin by establishing some intersection properties of Π_q with conics and other curves of $PG(2,\bar{\mathcal{K}})$.

Proposition 9. *The conic $\mathcal{C}$ of equation*

$$X^2+Y^2+1=0 \tag{25}$$

and the algebraic curve $\mathcal{D}$ of equation

$$X=Y^{\sqrt{q}+1} \tag{26}$$

meet in $2(\sqrt{q}+1)$ pairwise different points, and half of these points lie on Π.

Proof.

Substituting X by $Y^{\sqrt{q}+1}$ in (25) we obtain $Y^{2(\sqrt{q}+1)}+Y^2+1=0$. The latter equation has pairwise different roots since the polynomial $f(Y)=Y^{2(\sqrt{q}+1)}+Y^2+1$ and its derivative $f(Y)'=Y(Y^{2\sqrt{q}}+1)=Y(Y^2+1)^{\sqrt{q}}$ have no common roots. We have to show that $\sqrt{q}+1$ of these roots have the property that the arising common point also lies on Π. Since $f(Y)^{\sqrt{q}}Y^2=Y^{2(q+\sqrt{q}+1)}+Y^{2(\sqrt{q}+1)}+Y^2$ and $Y^{2(\sqrt{q}+1)}+Y^2+1=0$, each root of $F(Y)$ is also a root of the polynomial $g(Y)=Y^{2(q+\sqrt{q}+1)}-1$. Since $f(Y)=f(-Y)$, and $g(Y)=g(-Y)$, half of the roots of $f(Y)$ are also roots of the polynomial $h(Y)=Y^{q+\sqrt{q}+1}-1$. This shows that the corresponding $\sqrt{q}+1$ points lie on Π. $\square$

Proposition 10. *The conic $\mathcal{C}$ of equation (25) and the Hermitian curve $\mathcal{H}$ of equation $XY^{\sqrt{q}}+X^{\sqrt{q}}+Y=0$ have $\sqrt{q}+1$ pairwise different points, each of them lies on Π_q. Furthermore, the curves $\mathcal{C}$ and $\mathcal{H}$ have the same tangent line at each of their common points.*

Proof. In the previous proof we found $\sqrt{q}+1$ different points $P(y^{\sqrt{q}+1},y)$ in the intersection $\mathcal{C}\cap\Pi$, such that y is a root of both $f(Y)$ and $h(Y)$. Each of these points also lies on $\mathcal{H}$ since

$$y^{2(\sqrt{q}+1)}+y^{q+\sqrt{q}}+y=\frac{1}{y}(y^{q+\sqrt{q}+1}+y^{2(\sqrt{q}+1)}+y^2)=\frac{1}{y}(1+y^{2(\sqrt{q}+1)}+y^2)=0.$$

An easy calculation shows that the tangent line to $\mathcal{H}$ at the point $P(y^{\sqrt{q}+1},y)$ has slope equal to $-\sqrt{y}$. The same value is obtained when $\mathcal{H}$ is replaced by $\mathcal{C}$. Hence $\mathcal{C}$ and $\mathcal{H}$ are tangent at each of the above $\sqrt{q}+1$ points. By the classical Bézout theorem, no further common point of $\mathcal{C}$ and $\mathcal{H}$ exists, and this completes the proof of Proposition 10. $\square$

Now, consider the set of conics $\mathcal{C}_t$ of equation

$$tX^2+t^{q+1}Y^2+1=0 \tag{27}$$

with t running on the $(q^2+q+1)-$th roots of unity. Actually, this set consists of all conics which are images of the conic $\mathcal{C}$ of equation (2) under the group $\mathcal{A}$ of order $q-\sqrt{q}+1$. Let $\mathcal{B}$ denote the subgroup of $\mathcal{A}$ of order $q-\sqrt{q}+1$. Note that the orbit of $\mathcal{C}$ under $\mathcal{B}$ consists of the conics $\mathcal{C}_t$ where t ranges over the $(q-\sqrt{q}+1)-$roots of unity.

Proposition 11. *The conics $\mathcal{C}_t$ with t running over the $(q-\sqrt{q}+1)-$th roots of unity partition $\mathcal{H}\cap\Pi_q$ in $(q-\sqrt{q}+1)$ point$-$sets each of size $\sqrt{q}+1$.*

Proof. It is straightforward to check that $\mathcal{B}$ leaves $\mathcal{H}$ invariant. This shows that Proposition 10 remains valid when $\mathcal{C}$ is replaced by any conic $\mathcal{C}_t$ with t a $(q-\sqrt{q}+1)-$th root of unity. From this we infer at first that no point on $\mathcal{H}$ lies on more than one of such conics. In fact, if both t and u are $(q-\sqrt{q}+1)-$th roots of unity, and $P(x,y)$ is a point in $\mathcal{H}\cap\mathcal{C}_t\cap\mathcal{C}_u$, from Proposition 3 it follows that $\mathcal{C}_t$ and $\mathcal{C}_u$ must have the same tangent at $P(x,y)$. But, this can only occur when $-t^q=-u^q$, and hence $t=u$. From Proposition 10 we also infer that each conic $\mathcal{C}_t$ with t a $(q-\sqrt{q}+1)-$th root of unity meets $\mathcal{H}\cap\Pi_q$ in $\sqrt{q}+1$ points. Since $\mathcal{H}\cap\Pi$ has size $q\sqrt{q}+1$, the assertion follows. $\square$

A relationship between conics $\mathcal{C}_t$ and lines l_t is given in the following

Proposition 12. *The quadratic transformation T defined by $X' = X^2$ and $Y' = Y^2$, induces a one–to–one correspondence on Π_q and turns the conic $\mathcal{C}_t$ into the line l_t.*

Proof. The transformation T is one–to–one on Π_q since the mapping $x \to x^2$ is a bijection on the set of all (q^2+q+1)–th roots of unity. The second half of the assertion is easy to check. $\square$

Now we are in a position to show that the transformation T turns $\mathcal{H}$ into Γ. Let $T(\mathcal{H})$ denote the image curve of $\mathcal{H}$ under T. From Propositions 10, 11 and 12, it follows that each line l_t with t a $(q-\sqrt{q}+1)$–th root of unity is a $(\sqrt{q}+1)$–tangent to $T(\mathcal{H})$, i.e. l_t is the tangent line to $T(\mathcal{H})$ at each of their common points. Since such lines form a dual arc, we see that $T(\mathcal{H})$ viewed on the dual plane is the algebraic envelope associated to the cyclic $(q-\sqrt{q}+1)$–arc.

To complete the proof of the Theorem we have to check that the transformation T maps $\mathcal{H}$ onto Γ birationally. Consider the linear system Φ of all conics of equations $\lambda X^2 + \mu Y^2 + \tau = 0$, with $\lambda, \mu, \tau \in \mathcal{L}$. We have to show that if $P(x,y)$ is a point of $\mathcal{H}$ in a generic position, and Φ_P is the linear subsystem of Φ consisting of all conics through $P(x,y)$, then the conics of Φ_P have no further common point on $\mathcal{H}$. As $P(x,y)$ is in generic position, both x and y must be different from 0. On the other hand, the conics of Φ_P have exactly four common points on the plane $PG(2,\bar{\mathcal{K}})$, namely, $P(x,y)$, $P_1(x,-y)$, $P_2(-x,-y)$ and $P_3(-x,-y)$. It is easily checked that no of the latter three points lies on $\mathcal{H}$. Thus, the point $P(x,y)$ is the only common point of the conics of Φ_P which lies on $\mathcal{H}$.

So $vi)$ is completely proved.

References

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

[2] A. Campillo, *Algebroid curves in positive characteristic*, Lecture Notes in Math, Springer–Verlag, 1985.

[3] A. Cossidente, *A new proof of the existence of (q^2-q+1)–arcs in $PG(2,q^2)$*, J. Geometry **53** (1995), 37-40.

[4] A. Cossidente, *J. Geometry* **59** (1997), 32-33.

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

[6] C. Fisher, J.W.P. Hirschfeld and J.A. Thas, *Complete arcs in plane of square orders*, Ann. Discrete Math. **30** (1986), 243-250.

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

[8] A. Garcia and J.F. Voloch, *Fermat curves over finite fields*, J. Number Theory **30** (1988), 345-356.

[9] A. Hefez and J.F. Voloch, *Frobenius non classical curves*, Arch. Math. **54** (1990), 263-273.

[10] J.W.P. Hirschfeld, *Projective geometries over finite fields*, Oxford University Press, Oxford, 1979.

[11] J.W.P. Hirschfeld and J.A. Thas, *General Galois Geometries*, Oxford University Press, Oxford, 1991.

[12] J.W.P. Hirschfeld and G. Korchmaros, *On the embedding of an arc into a conic in a finite plane*, Finite Fields and their Applications **2** (1996), 274-292.

[13] B.C. Kestenband, *A family of complete arcs in finite projective planes*, Colloq. Math. **17** (1989), 59-67.

[14] H.-G. Rück and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. reine angew. Math. **457** (1994), 185-188.

[15] B. Segre, *Introduction to Galois geometries (edited by J.W.P. Hirschfeld)*, Atti Accad. Naz. Lincei Mem. **8** (1967), 133-236.
[16] A. Seidenberg, *Elements of the theory of curves*, Addison–Wesley, 1969.
[17] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. **43** (1938), 377-385.
[18] K.O. Stöhr and J.F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. **52** (1986), 1-19.
[19] J.A. Thas, *Complete arcs and algebraic curves in* $PG(2,q)$, J. Algebra **106** (1987), 457-464.
[20] J.F. Voloch, *Arcs in projective planes on prime fields*, J. Geometry **38** (1990), 198-200.
[21] J.F. Voloch, *Complete arcs in Galois planes of non–square order*, in Advances in Finite Geometries, Oxford University Press (1991), 401-405.

Dipartimento di Matematica, Università della Basilicata via N. Sauro 85, 85100 Potenza (Italy)