Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Francis J. Sullivan

An iterative construction for ordinary and very special hyperelliptic curves

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **74** (1983), n.3, p. 152–155.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1983_8_74_3_152_0>

Geometria algebrica. — *An iterative construction for ordinary and very special hyperelliptic curves.* Nota di FRANCIS J. SULLIVAN, presentata (*) dal Socio G. SCORZA DRAGONI.

RIASSUNTO. — Si costruiscono famiglie di curve iperellittiche col p–rango della varietà jacobiana uguale a zero. La costruzione sfrutta le proprietà elementari dell'operatore di Cartier e delle estensioni p-cicliche dei corpi con la caratteristica p maggiore di zero.

Let k be a perfect field of characteristic $p > 2$ and let X be a hyperelliptic or elliptic curve defined over k. Then, after taking a finite extension of the base field k if necessary, one may take a defining equation for X in the form

$$\text{(1)} \qquad X : \; y^2 = f(x)$$

where $f(x) \in k[x]$, degree $(f(x)) = 2g + 1$ or $2g + 2$ with $g =$ genus of X, and $f(x)$ has no multiple roots in $\bar{k}$, the algebraic closure of k. Let J_p be the group of p-division points on the Jacobian variety of a non-singular model for X. Then, as is well known, the rank r of the elementary abelian group J_p satisfies

$$\text{(2)} \qquad 0 \leq r \leq g .$$

Indeed, r may be characterized either as the rank of the $g \times g$ matrix $AA^{(p)} \cdots A^{(p^{j-1})}$ where A is the Hasse-Witt matrix of X and $A^{(p^j)}$ is the matrix obtained from A by raising each entry to the p^j-th power, or, equivalently, as the rank of the Z/pZ-module spanned by the logarithmic differentials of the first kind on X. For these facts, and the basic properties of the Cartier operator which will be used in the sequel the reader may consult [1], [2], and [6].

X is said to be ordinary if $r = g$; otherwise X is special. In particular, if $r = 0$ X is said to be very special. This terminology also applies to curves which are not hyperelliptic. It was long part of mathematical folklore that " the generic curve of genus g is ordinary ", but a proof of this fact appeared only in 1972 [5], followed by another in 1974 [3]. In recent years special and very special curves have been studied intensively [3], [4], [7], [8] and [9], but even in very favourable cases one can rarely avoid tedious calculation in calculating r, although in light of [4] and [7] such reckoning may now be reduced to the determination of certain ramification indices in the case of Artin-Schreier curves. Such information is useful in various contexts, for example the study of stable vector bundles over curves in characteristic p, and also as a first step in the

(*) Nella seduta del 12 marzo 1983.

determination of the formal structure of the Jacobian variety of such curves. In this note we give an iterative construction for ordinary and very special hyperelliptic curves, which produces a family of curves of increasing genus with $r = 0$ and similarly a family with $r = g$. In principle our results follow from those in [7] but since our aim is clarity we give a self-contained proof which allows one to " see at a glance " why the curves in question have the stated properties. We are indebted to Claudia Metelli for pointing out the usefulness of such results.

The following lemma is well known and merely expresses the " naturality " of the Cartier operator.

LEMMA 1. *Let* L/K *be a finite separable extension of algebraic function fields of one variable over* k. *For any differential* η *of* K *let* $(\eta)_{\mathrm{L}}$ *denote the co-trace of* η *in* L. *Let* C_{K} *and* C_{L} *be the Cartier operators in* K *and* L *respectively. Then*

$$\mathrm{C}_{\mathrm{L}}\,((\eta)_{\mathrm{L}}) = (\mathrm{C}_{\mathrm{K}}\,(\eta))_{\mathrm{L}}\,.$$

In view of Lemma 1 we will dispense with the subscript on C. In the sequel $f_s(x)$ will always denote an element of $k\,[x]$ of degree s and having no multiple roots in $\bar{k}$.

THEOREM 1. *Let* $\mathrm{X} : y^2 = f_{2g+1}(x)$ *be a very special hyperelliptic curve, and let* X^* *be the hyperelliptic curve obtained from* X *by the substitution* $x = z^p - z$. *Then* X^* *is also very special.*

Proof. The genus of X^* is $pg + (p - 1)/2$, and since $dz = - dx$ we may take a basis for the holomorphic differentials on X^* in the form

$$\begin{array}{ccccccccc}
\mathrm{d}x/y & , & x\,\mathrm{d}x/y & , & \cdots & , & x^{g-1}\,\mathrm{d}x/y & , & x^{g}\,\mathrm{d}x/y \\
\vdots & & \vdots & & & & \vdots & & \vdots \\
z\,\mathrm{d}x/y & & \vdots & & & & \vdots & & z^{\frac{1}{2}(p-3)}\,x^{g}\,\mathrm{d}x/y\,. \\
\vdots & & \vdots & & & & \vdots & & \\
z^{p-1}\,\mathrm{d}x/y & , & z^{p-1}\,x\,\mathrm{d}x/y & , & \cdots & , & z^{p-1}\,g^{g-1}\,\mathrm{d}x/y\,. & &
\end{array}$$

Order these differentials lexicographically with respect to the exponents of x and z. By the hypothesis on X and Lemma 1, $\mathrm{d}x/y$ is not logarithmic. Hence we may assume inductively that there is no non-zero logarithmic differential in the k-space W spanned by $\mathrm{d}x/y\,,\ z\mathrm{d}x/y\,, \cdots,\ x^i z^j\,\mathrm{d}x/y$. Consider the space V spanned over k by W and the next differential appearing in the basis. We show that V also contains no nonzero logarithmic differential. We proceed by cases:

Case 1: $\qquad \mathrm{V} = \mathrm{W} \oplus k \cdot x^i z^{j+1}\,\mathrm{d}x/y\,, \qquad$ that is $j \neq p - 1\,.$

Suppose that $\omega = a_{00}\,\mathrm{d}x/y + \cdots + a_{i,j+1}\,x^i y^{j+1}\,\mathrm{d}x/y$ is a non-zero logarithmic differential, say $\omega = \mathrm{d}f/f$. Then, by assumption, $a_{i,j+1} \neq 0$. Furthermore if σ is the $k(x)$-automorphism of $k(y, z)$ defined by $\sigma(y) = y$, $\sigma(z) = z + 1$ we see that $\omega = \mathrm{d}f^{\sigma}/f^{\sigma}$ is also logarithmic and of the first kind, whence the same is true for $\omega - \omega^{\sigma}$. However it can be easily seen that the assumptions $j \neq p - 1$ and $a_{i,j+1} \neq 0$ entail that $\omega - \omega^{\sigma}$ is a non-zero element of W. This contradicts the assumption that W has no non-trivial logarithmic differentials.

Case 2: $\quad V = W \oplus k \cdot x^{i+1}\,\mathrm{d}x/y\,, \quad$ that is $j = p - 1$.

As above we consider a non-zero logarithmic differential ω in V. If $\omega \neq \omega^{\sigma}$ we can argue as in case 1. Otherwise ω is fixed under the action of σ and so ω is (the cotrace of) a differential on X. If $i + 1 < g$, Lemma 1 again contradicts a contradiction to the assumed very special character of X. The only remaining possibility is that $\omega = a_{00}\,\mathrm{d}x/y + a_{10}\,x\,dx/y + \cdots + a_{g\,0}\,x^{g}\,\mathrm{d}x/y$.

Now each summand appearing in the expression for ω, except the last, is the cotrace of a differential of the first on X. The space of differentials of the first kind is stable under the action of C. Thus, to obtain a contradiction of the assumption that ω is logarithmic (which is to say fixed by C), it will suffice to show that C $(x^{g}\,\mathrm{d}x/y)$ lies in the k-space spanned by $\mathrm{d}x/y$, $x\mathrm{d}x/y, \cdots, x^{g-1}\,dx/y$. We calculate:

$$\text{(3)} \qquad C\,(x^{g}\,\mathrm{d}x/y) = y^{-1}\,C\,(x^{g+1}\,y^{p-1}\,\mathrm{d}x/x) = y^{-1}\,C\,(x^{g+1}\,f_{2g+1}\,(x)^{\frac{1}{2}(p-1)}\,\mathrm{d}x/x)\,.$$

The argument of C in the last term is a polynomial in x of degree $pg + \frac{1}{2}(p+1) < p(g + 1)$ multiplying $\mathrm{d}x/x$. All terms of $x^{g+1}f_{2g+1}(x)^{\frac{1}{2}(p-1)}$ which do not have exponents divisible by p give differentials annihilated by C, while $C(x^{jp}\mathrm{d}x/x) = x^{j}\mathrm{d}x/x = x^{j-1}\mathrm{d}x$. But we have just seen that the j which occur are less that or equal to g. Hence $C(x^{g}\,\mathrm{d}x/x)$ doe indeed lie in the k-space spanned by $\mathrm{d}x/y, \cdots, x^{g-1}\,\mathrm{d}x/y$. This provides the required contradiction and proves the theorem. QED

Remark: Starting from a supersingular elliptic curve E : $y^2 = x(x - 1)(x - \lambda)$ Theorem 1 gives an inductive procedure for constructing very special hyperelliptic curves of genera $p^{i} + \frac{1}{2}(p^{i} - 1)$.

One might expect a similar result when the defining equation for X is of the form $y^2 = f_{2g+2}(x)$, but a glance at the proof of the last step in Theorem 1 shows that this is emphatically not the case. There is, however, a " dual " to Theorem 1:

THEOREM 2. *Let* X : $y^2 = f_{2g+2}(x)$ *be an ordinary hyperelliptic curve, and let* X^* *be obtained from* X *by the substitution* $x = z^{p} - z$. *Then* X^* *is also ordinary.*

Proof. Note that the genus of X^* is now $pg + (p - 1)$, so that the basis analogous to that used in Theorem 1 has $x^{g}\,z^{p-2}\,\mathrm{d}x/y$ as the last entry in the last column. Now repeat the proof of Theorem 1 replacing the word " logarithmic " by the word " exact ". To obtain the desired contradiction in the final step in this situation it now suffices to show that $C(x^g \, dx/y)$ does NOT lie in the k-space spanned by $dx/y, xdx/y, \cdots, x^{g-1} dx/y$. Now, however the degree of the polynomial appearing in the argument of C in the final term of equation (3) is exactly $p(g+1)$. This shows that $x^g \, dx/y$ appears with non-zero coefficient in $C(x^g \, dx/y)$ and provides the desired contradiction. QED

We can subsume the inductive procedure mentioned above in the following simple generalization of the preceding results, when $k = \bar{k}$.

Theorem 3. *Let $a(z)$ be an additive separable polynomial, that is, let*

$$a(z) = \sum_{m=0}^{t} c_m z^{p^m} \quad \text{with } c_0 \neq 0 \;,\; c_m \in k . \qquad \text{Let } X_1 : \; y^2 = f_{2g+1}(x)$$

be a very special hyperelliptic curve, $X_2 : y^2 = f_{2g+2}(x)$, an ordinary hyperelliptic curve, and let X_1^* and X_2^* be the curves obtained from X_1 and X_2 respectively by the substitution $x = a(z)$. Then X_1^* is very special and X_2^* is ordinary.

Proof. If u is a root of $a(z)$ then $z \to z + u$, $y \to +y$ define automorphisms of $k(y, z)$ over $k(x)$, and every automorphism can be so obtained. Using these automorphisms in place of the powers of σ one sees easily that the proofs of Theorems 1 and 2 carry over with the sole modification that in Case 2 we can argue as in Case 1 whenever ω is not fixed by at least one automorphism which fixes y. (The Galois group of $k(y, z)$ over $k(x, y)$ is now not cyclic but elementary abelian of order p^t = degree $a(z)$). QED.

References

[1] P. Cartier (1957) – *Une nouvelle operation sur les formes differentielles.* « C. R. Acad. Science », Paris, *244*, 426.

[2] H. Hasse and E. Witt (1936) – *Zyklische unverzweigte Erweiterungskorper von Primzahlgrade p uber einem algebraischen Funktionenkorper der Charaketeistik p, Monathft.* « Math. Phs. », *43*, 477.

[3] N. Koblitz (1975) – *p–adic variation of the zeta–function over families of varieties defined over finite fields.* « Compositio Math. », *31*, 119–218.

[4] D. Madden (1978) – *Arithmetic in Generalized Artin–Schreier Extensions of k (x).* « Journ. Number Theory », *17*, 303–323.

[5] L. Miller (1972) – *Curves with Invertible Hasse–Witt Matrix.* « Math. Ann. », *197*, 123.

[6] J. P. Serre (1956) – *Sur la topologie des variete algebriques en characteristique p.* « Symp. Int. Top. Alg. », 43.

[7] D. Subrao (1975) – *The p–rank of Artin–Schreier curves.* « Manuscripta Math. », *16*, 169–193.

[8] N. Yui (1978) – *On the Jacobian varieties of hyperelliptic curves over fields od characteristic p 2.* « J. Algebra », *52*, 378–400.

[9] N. Yui (1980) – *On the Jacobian Variety of the Fermat Curve.* « J. Algebra », *65*, 1–34.