International Journal of Pure and Applied Mathematics

Volume 28 No. 4 2006, 503-506

CURVES OVER $\mathbb{F}_q$ WITH A "NICE" POINT

E. Ballico

Department of Mathematics
University of Trento
380 50 Povo (Trento) - Via Sommarive, 14, ITALY
e-mail: ballico@science.unitn.it

Abstract: Here we study the existence and abundance of genus g curves C defined over $\mathbb{F}_q$ (q as low as possible) such that there is $P \in C(\mathbb{F}_q)$ such that $h^0(C, \mathcal{O}_X((g-1)P)) = h^1(C, \mathcal{O}_C((g-1)P)) = 1$, $h^0(C, \mathcal{O}_C(gP)) = 1$, $h^1(C, \mathcal{O}_C(gP)) = 0$, and $\mathcal{O}_C((g+1)P)$ is spanned by its global sections.

AMS Subject Classification: 14H25, 14H51, 14H55
Key Words: ordinary curve, Weierstrass point, hyperelliptic curve

1. Curves Over a Finite Field with a "Nice" Point

Motivated by a construction given in [3] we study the existence and abundance of genus g curves C defined over $\mathbb{F}_q$ (q as low as possible) such that there is $P \in C(\mathbb{F}_q)$ such that $h^0(C, \mathcal{O}_X((g-1)P)) = h^1(C, \mathcal{O}_C((g-1)P)) = 1$, $h^0(C, \mathcal{O}_C(gP)) = 1$, $h^1(C, \mathcal{O}_C(gP)) = 0$, and $\mathcal{O}_C((g+1)P)$ is spanned by its global sections. First, we consider the case of hyperelliptic curves.

Theorem 1. *Fix a prime p, a p-power q, an integer $g \geq 2$, and a smooth genus g hyperelliptic curve C defined over $\mathbb{F}_q$. Let $\phi : C \to \mathbf{P}^1$ be the hyperelliptic double covering of C and $R_\phi \subset \mathbf{P}^1(\bar{\mathbb{F}}_q)$ the branch locus of ϕ. There exists $P \in C(\mathbb{F}_q)$ such that $h^0(C, \mathcal{O}_X((g-1)P)) = h^1(C, \mathcal{O}_C((g-1)P)) = 1$ and $h^0(C, \mathcal{O}_C(gP)) = 1$, $h^1(C, \mathcal{O}_C(gP)) = 0$ if and only if there is $A \in \mathbf{P}^1(\mathbb{F}_q)$ such that $A \notin R_\phi$. Furthermore, $\mathcal{O}_C((g+1)P)$ is spanned by its global sections.*

The morphism ϕ in the statement of Theorem 1 is defined over $\mathbb{F}_q$ and hence

Received: May 2, 2006

R_ϕ is defined over $\mathbb{F}_q$, i.e. it is invariant for the action on $\mathbf{P}^1(\bar{\mathbb{F}}_q)$ of the absolute Galois field of $\mathbb{F}_q$.

Corollary 1. *Fix a prime p, a p-power q and an integer $g \geq 2$. Then there exist a smooth genus g hyperelliptic curve C defined over $\mathbb{F}_q$ and $P \in C(\mathbb{F}_q)$ such that $h^0(C, \mathcal{O}_X((g-1)P)) = h^1(C, \mathcal{O}_C((g-1)P)) = 1$, $h^0(C, \mathcal{O}_C(gP)) = 1$, $h^1(C, \mathcal{O}_C(gP)) = 0$, and $\mathcal{O}_C((g+1)P)$ is spanned by its global sections.*

Corollary 2. *Fix a prime p, a p-power q and an integer $g \geq 2$. Assume $q \geq 2g-2$ if $p \neq 2$ and $q \geq g-1$ if $p = 2$. Let C be a smooth genus g hyperelliptic curve C defined over $\mathbb{F}_q$. Then there exists $P \in C(\mathbb{F}_q)$ such that $h^0(C, \mathcal{O}_X((g-1)P)) = h^1(C, \mathcal{O}_C((g-1)P)) = 10$, $h^0(C, \mathcal{O}_C(gP)) = 1$, $h^1(C, \mathcal{O}_C(gP)) = 0$ and $\mathcal{O}_C((g+1)P)$ is spanned by its global sections.*

Remark 1. By Riemann-Roch the conditions "$h^0(C, \mathcal{O}_C((g-1)P)) = 1$" and "$h^1(C, \mathcal{O}_C((g-1)P)) = 1$" are equivalent. By Riemann-Roch the conditions "$h^0(C, \mathcal{O}_C(gP)) = 1$" and "$h^1(C, \mathcal{O}_C(gP)) = 1$" are equivalent and the union of them with the condition of them means that P is not a Weierstrass points of C. For examples of genus g curves C' defined over a finite field $\mathbb{F}_q$ such that all points are Weierstrass points, see [1]. Such example exists only when $p < 2g-2$ (see [1], [2]). If $h^0(C, \mathcal{O}_C((g-1)P)) = 0$", then $h^0(C, \mathcal{O}_C((g+1)P)) = 2$ and $h^1(C, \mathcal{O}_C((g+1)P)) = 0$.

Remark 2. Take C, P as in the statements of Theorem 1 or Corollary 1 and Corollary2 and set $D := (g+1)P$. The last part of Remark 1 shows that the pair $(C, \mathcal{O}_C(D))$ may be used in the proof of [3], Th. 1.1. Hence we get such an example over the finite field $\mathbb{F}_q$ with a reasonable control of q. It is very easy to construct similar examples over any infinite field.

For arbitrary curves we have the following result.

Theorem 2. *Fix a prime p, a p-power q, an integer $g \geq 2$ and a smooth and geometrically connected genus g curve C defined over $\mathbb{F}_q$ such that the general $Q \in C(\bar{\mathbb{F}}_q)$ is not a classical Weierstrass point of C (i.e. $h^0(C, \mathcal{O}_C(gQ)) = 1$, i.e. $h^1(C, \mathcal{O}_C(gQ)) = 0$). Assume $\sharp(C(\mathbb{F}_q)) \geq (g+1)g(g-1)/6$. Then there exists $P \in C(\mathbb{F}_q)$ such that $h^0(C, \mathcal{O}_X((g-1)P)) = h^1(C, \mathcal{O}_C((g-1)P)) = 1$ and $h^0(C, \mathcal{O}_C(gP)) = 1$, $h^1(C, \mathcal{O}_C(gP)) = 0$ and the line bundle $\mathcal{O}_C((g+1)P)$ is spanned by its global sections.*

Remark 3. Let C be a smooth and geometrically connected genus g curve defined over $\mathbb{F}_q$. By Hasse-Weil inequality we have $\sharp(C(\mathbb{F}_q)) \geq q+1-2g\sqrt{q}$. Hence for fixed p, g the assumption $\sharp(C(\mathbb{F}_q)) \geq (g+1)g(g-1)/6$ in the statement of Theorem 2 is satisfied when $q \gg 0$.

Remark 4. The assumption "the general $Q \in C(\bar{\mathbb{F}}_q)$ is not a classical Weierstrass point of C" in the statement of Theorem 2 is satisfied for all smooth and geometrically connected curves if $p > 2g-2$ (see [1] or [2]). When p is low with respect to g, this assumption is not always satisfied (see examples in [1] and the quotations of the classical examples due to Hasse).

Remark 5. There are many classes of smooth genus g curves for which it is known that they have far less than $(g+1)g(g-1)/6$ Weierstrass points (bielliptic curves, cyclic coverings of $\mathbf{P}^1$, double coverings of a genus > 0 curve, multiple coverings with a total ramification point, and so on). For each of these classes it is easy to give a small improvement of Theorem 2. We singled out the case of hyperelliptic curves because it is the only case in which we have a fairly complete picture.

Proof of Theorem 1. Let $f : C \to \mathbf{P}^{g-1}$ be the canonical morphism of C. The morphism f is defined over $\mathbb{F}_q$, $f(C)$ is a rational normal curve of $\mathbf{P}^{g-1}$ defined over $\mathbb{F}_q$ and we may take f as ϕ. Since $f(C)$ is a rational normal curve, for any $O \in f(C)(\bar{\mathbb{F}}_q)$ the $(g-2)$-dimensional osculating hyperplane of $f(C)$ at O has contact order $g-1$ at 0, i.e. $\mathbf{P}^{g-1}$ is spanned by the Cartier divisor gP of $f(C)$. Alternatively, the Brill-Noether theory of hyperelliptic curves gives that if $Q \in C$ and $\phi(Q) \in R_\phi$, then $h^0(C, \mathcal{O}_C(gP)) = 1 + \lfloor g/2 \rfloor > 1$, while if $f(Q) \notin R_\phi$, then $h^0(C, \mathcal{O}_C(gP)) = 1$ and hence $h^1(C, \mathcal{O}_C((g-1)P)) = 1$ and $h^1(C, \mathcal{O}_C(gP)) = 0$ (Remark 1), concluding the first part. Now we will check the "furthermore" part. Take any $Q \in C(\bar{\mathbb{F}}_q)$ such that $h^0(C, \mathcal{O}_C(gQ)) = 1$. Hence $h^0(C, \mathcal{O}_C((g+1)Q)) = 2$. For any $B \in C(\bar{\mathbb{F}}_q)$ the line bundle $\mathcal{O}_C((g+1)B)$ is spanned outside B. Since $h^0(C, \mathcal{O}_C((g+1)Q)) = h^0(C, \mathcal{O}_C((g+1)Q - Q)) + 1$, $\mathcal{O}_C((g+1)Q)$ is spanned at Q. □

Proof of Corollary 1. We have $\sharp(R_\phi) = 2g+2$ if $p \neq 2$ and $\sharp(R_\phi) = g+1$ if $p = 2$. Set $e := 2g-2$ if $p \neq 2$ and $e := g-1$ if $p = 2$. Take $B \in \mathbf{P}^1(\mathbb{F}_{q^e}) \backslash \mathbf{P}^1(\mathbb{F}_{q^{e-1}})$ and call S the orbit of B in $\mathbf{P}^1(\bar{\mathbb{F}}_q)$ for the action of the Galois group of the cyclic field extension $\mathbb{F}_{q^e}/\mathbb{F}_q$. There is a unique smooth hyperelliptic genus g curve C with S as branch locus R_ϕ and C is defined over $\mathbb{F}_q$. By Theorem 1 C gives a solution of Corollary 1. □

Proof of Corollary 2. We have $\sharp(R_\phi) = 2g+2$ if $p \neq 2$ and $\sharp(R_\phi) = g+1$ if $p = 2$. Since $\sharp(\mathbf{P}^1(\mathbb{F}_q)) = q+1 > \sharp(R_\phi)$, we may apply the proofs of Theorem 1 and Corollary 1. □

Proof of Theorem 2. By assumption the canonical morphism of C has the classical Hasse sequence in the sense of [2]. By the Plücker formula for the canonical morphism [2] C has at most $(g+1)g(g-1)/6$ Weierstrass points. Take as P any point of $C(\mathbb{F}_q)$ which is not a Weierstrass point of C. □

Acknowledgements

The author was partially supported by MIUR and GNSAGA of INdAM (Italy).

References

[1] D. Laksov, Weierstrass points on curves, *Astérisque 87-88* (1981), 221-247.

[2] D. Laksov, Wronskians and Plücker formulas for linear systems on curves, *Ann. Sc. École Norm. Sup.*, **17**, No. 1 (1984), 45-56.

[3] R. Takahashi, K.-I. Watanabe, Totally reflexive modules constructed from smooth projective curves of genus $g \geq 2$, *E-print* arXiv:math.AC/061407.