ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 30, Number 2, Summer 2000

JACOBIANS OF CURVES OVER FINITE FIELDS

JOSÉ FELIPE VOLOCH

Let $C/\mathbf{F}_q$ be a curve over a finite field of genus g at least two. Assume C has a rational point P_0 and consider C embedded in its Jacobian J by sending P_0 to $0 \in J$. So $C(\mathbf{F}_q) \subset J(\mathbf{F}_q)$ and we can consider the subgroup G of $J(\mathbf{F}_q)$ generated by $C(\mathbf{F}_q)$. If G is not the whole of $J(\mathbf{F}_q)$, we will show that we can construct an étale cover of C where every $\mathbf{F}_q$-rational point of C splits completely into $\mathbf{F}_q$-rational points. We will prove that, if q is large enough compared to g, then $G = J(\mathbf{F}_q)$ and will give examples showing that this equality does not always hold and these examples will lead to curves over finite fields with many rational points.

Theorem. *With the notation as above, if* $q \geq (8g-2)^2$, *then* $G = J(\mathbf{F}_q)$.

Before proving the theorem, we need a lemma.

Lemma. *Let A be an abelian group and α a surjective endomorphism of A. Let G be a subgroup of* $\ker\alpha$ *and $\varphi : A \to A/G$ the canonical map and $\beta : A/G \to A/G$ the endomorphism induced by α. Finally, let $\psi : A/G \to A$ be the unique homomorphism such that $\alpha = \psi \circ \varphi$. Then* $\psi(\ker\beta) = G$.

Proof. By construction, $\beta \circ \varphi = \varphi \circ \alpha$, that is, $\beta(y) = \varphi(\alpha(x))$ for any $x, \varphi(x) = y$. Also ψ is defined by $\psi(y) = \alpha(x)$ for any $x, \varphi(x) = y$, that is, $\alpha = \psi \circ \varphi$. We also have $\beta = \varphi \circ \psi$. Indeed, given $y \in A/G$ and $x, \varphi(x) = y$, we have $\beta(y) = \beta(\varphi(x)) = \varphi(\alpha(x)) = \varphi(\psi(y))$. It follows that $\psi(\ker\beta) \subset \ker\varphi = G$. On the other hand, given $x \in \ker\varphi$, we can write $x = \alpha(y)$, $y \in A$. Then $\beta(\varphi(y)) = \varphi(\alpha(y)) = \varphi(x) = 0$, so $\varphi(y) \in \ker\beta$ and therefore $x = \psi(\varphi(y)) \in \psi(\ker\beta)$, which proves that $G \subset \psi(\ker\beta)$, proving the lemma. □

Received by the editors on March 24, 1999.

Proof of the theorem. We apply the lemma with $A = J(\bar{\mathbf{F}}_q)$ and $\alpha = 1 - F$ where F is the $\mathbf{F}_q$-Frobenius and G the group generated by $C(\mathbf{F}_q)$. So $J/G = B$ is an abelian variety and $\psi : B \to J$ is an isogeny of degree $n = [J(\mathbf{F}_q) : G]$. Note that β, as in the lemma, equals $1 - F$, where F is the $\mathbf{F}_q$-Frobenius on B, which follows since J and φ are defined over $\mathbf{F}_q$. Thus $\ker\beta = B(\mathbf{F}_q)$ and, by the lemma, $\psi(\ker\beta) = G$. Let C' be the pull-back of C under ψ, so C' is an étale cover of C of degree n defined over $\mathbf{F}_q$. (In fact, C' is the maximal étale abelian cover of C defined over $\mathbf{F}_q$ in which every rational point of C splits). Also, since $C(\mathbf{F}_q) \subset G = \psi(B(\mathbf{F}_q))$, we get that $\psi^{-1}(C(\mathbf{F}_q)) \subset C' \cap B(\mathbf{F}_q) = C'(\mathbf{F}_q)$. Therefore, $\#C'(\mathbf{F}_q) \geq n\#C(\mathbf{F}_q)$. We now use the Riemann hypothesis for curves over finite fields to estimate these cardinalities. $\#C(\mathbf{F}_q) \geq q+1-2gq^{1/2}$ and $\#C'(\mathbf{F}_q) \leq q+1+2g'q^{1/2}$, where g' is the genus of C' and, by the Hurwitz formula $g' = n(g-1)+1$. Combining these inequalities we obtain $q+1+2(n(g-1)+1)q^{1/2} \geq n(q+1-2gq^{1/2})$ which gives $n(q+1-2(2g-1)q^{1/2}) \leq q+1+2q^{1/2}$. Finally this last inequality, combined with the hypothesis $q \geq (8g-2)^2$, give $n < 2$, so $n = 1$ and we are done.

As mentioned above, examples where the theorem's conclusion does not hold will give examples of curves with many rational points.

Consider the Hermitian curve $C : x^{q+1} + y^{q+1} = 1$ over $\mathbf{F}_q$. As is well known, this curve attains the upper bound given by the Riemann hypothesis over $\mathbf{F}_{q^2}$, namely it has genus $g = q(q-1)/2$ and q^3+1 points over $\mathbf{F}_{q^2}$. This means that all eigenvalues of Frobenius over $\mathbf{F}_{q^2}$ are equal to $-q$. Hence the eigenvalues of Frobenius over $\mathbf{F}_{q^4}$ are equal to q^2. It follows that C has $q^4 + 1 - q(q-1)q^2 = q^3 + 1$ points over $\mathbf{F}_{q^4}$, that is, $C(\mathbf{F}_{q^2}) = C(\mathbf{F}_{q^4})$. As for the Jacobian J, Frobenius acts as $-q$ over $\mathbf{F}_{q^2}$ so $J(\mathbf{F}_{q^2}) = J[q+1]$, the $q+1$-torsion. Similarly, $J(\mathbf{F}_{q^4}) = J[q^2-1]$, which is bigger than the group generated by $C(\mathbf{F}_{q^4}) = C(\mathbf{F}_{q^2})$, since the latter is contained in $J(\mathbf{F}_{q^2})$. For any subgroup G of $J(\mathbf{F}_{q^4})$ containing $J(\mathbf{F}_{q^2})$ we can apply the construction of the proof of the theorem and obtain an étale cover of C of degree $n = [J(\mathbf{F}_{q^4}) : G]$ with at least $n(q^3+1)$ rational points over $\mathbf{F}_{q^4}$ and genus $n(g-1)+1$, and we can take n to be any divisor of $(q-1)^{2g}$.

For a numerical example take $q = 3$, so $g = 3$ and for any divisor n of 2^6 we get a curve of genus $2n+1$ over $\mathbf{F}_{81}$ with $28n$ rational points. Or, take $q = 4$, so $g = 6$ and for any divisor n of 3^{12} we get a curve of genus $5n+1$ over F_{256} with $65n$ rational points. There are no known curves with more points with the same parameters for the larger values of n, according to the tables in [**6**]. These curves get very close to the best-known upper bounds for the given parameters, which are obtained by Oesterlé's method. For example, the case $q = 3$, $n = 64$, gives a curve with 1792 points over $\mathbf{F}_{81}$ and Oesterlé's bound is 1897. The case $q = 4$, $n = 531441$ gives a curve with 34543665 points over F_{256} and Oesterlé's bound is 46069115.

Another example is the Suzuki curve $y^q - y = x^{q_0}(x^q - x)$, where $q = 2^{2m+1}$, $q_0 = 2^m$, $m \geq 1$ (see [**2**]). This curve has $q^2 + 1$ points over $\mathbf{F}_q$ and genus $g = q_0(q - 1)$. The eigenvalues of Frobenius turn out to be $2^m(-1 \pm i)$. It follows that the curve also has $q^2 + 1$ points over $\mathbf{F}_{q^2}$, that is, $C(\mathbf{F}_q) = C(\mathbf{F}_{q^2})$. The Jacobian has $(q+1+2q_0)^g$ rational points over $\mathbf{F}_q$ and $(q^2 + 1)^g$ rational points over $\mathbf{F}_{q^2}$. So we get, by taking covers, for any divisor n of $(q+1-2q_0)^g = (q^2+1)^g/(q+1+2q_0)^g$, a curve of genus $n(g - 1) + 1$ having $n(q^2 + 1)$ points over $\mathbf{F}_{q^2}$.

For a numerical example take $q = 8$, so $g = 14$, and for any divisor n of 5^{14} we get a curve of genus $13n+1$ with $65n$ rational points over $\mathbf{F}_{64}$. There are no known curves with more points with the same parameters for the larger values of n according to the tables in [**6**].

A similar class of examples can be obtained from the Ree curves in characteristic three (see [**3**]).

The above examples can be used as first steps of class field towers (see [**4**]). Namely, we can consider for a curve C the cover C' given by the construction in the theorem, then apply the same construction to C' and get a cover C'' and so on. This construction may stop ($C^{(k)} = C^{(k+1)} = \cdots$) or not. It follows from [**4**, Theorem 2.3] that the sequence will not stop if, for some prime l, the l-primary component of $J(\mathbf{F}_q)/G$ has rank at least $2 + 2\sqrt{\#C(\mathbf{F}_q)}$. With the exception of finitely many values of q, the Hermitian, Suzuki and Ree curves above will lead to infinite towers. These towers are good in the sense that $\lim \#C^{(k)}(\mathbf{F}_q)/g^{(k)} > 0$, where $g^{(k)}$ is the genus of $C^{(k)}$ but not optimal in the sense that the limit attains its maximum value of $\sqrt{q}-1$.

We can consider more general class field towers as follows (see [**4**]). Take a set S of rational points of C and consider the cover C' which is the maximal unramified abelian extension of C where the points of S split completely, take for S' the pullback of S on C' and repeat with C', S' instead of C, S. The first step can be described geometrically as follows if $P_0 \in S$. Take the subgroup G_S of $J(\mathbf{F}_q)$ generated by S, apply the lemma to get an isogeny $\psi : A \to J$ with $\psi(A(\mathbf{F}_q)) = G_S$ and take C' as the pullback of C under ψ. That this construction gives the maximal such extension, follows from Rosenlicht's geometric class field theory (see [**5**]). Let us call such a set S saturated if, for any S_1, $S \subset S_1 \subset C(\mathbf{F}_q)$, if $G_S = G_{S_1}$, then $S = S_1$. For example, $S = \{P_0\}$ or $C(\mathbf{F}_q)$ are saturated. We would like to point out the following. If S is saturated, then $S' = C'(\mathbf{F}_q)$. Indeed, the points of S' are rational by construction. On the other hand, $C'(\mathbf{F}_q) = C' \cap A(\mathbf{F}_q)$ so $\psi(C'(\mathbf{F}_q)) \subset G_S$ and, since S is saturated, $\psi(C'(\mathbf{F}_q)) = S$, which gives the result.

In [**1**], Adleman et al. propose an algorithm for solving the discrete logarithm problem on Jacobians of hyperelliptic curves of high genus. In the algorithm they assume, but do not prove, that the set of rational points of the Jacobian can be generated by the image of prime divisors of small degree (their set G, see [**1**, Section 6]). From the theorem above, if $q^r \geq (8g-2)^2$, then $X(\mathbf{F}_{q^r})$ generates $J(\mathbf{F}_{q^r})$ and it follows immediately that the set of prime divisors of degree dividing r generate $J(\mathbf{F}_q)$. □

Remark. Lenstra has pointed out that, making use of the fact that the ζ function of C divides the ζ function of C' in the above proof, one can get the improved bound $q < (4g-2)^2$ in the conclusion of the theorem.

Acknowledgments. The author would like to thank J. Tate and M. Zieve for comments and K. Lauter and V. Shabat for computing the upper bounds by Oesterlé's method mentioned above. The author would also like to thank the TARP (grant no. ARP-006) and the NSA (grant MDA904-97-1-0037) for financial support.

REFERENCES

1. L.M. Adleman, J. DeMarrais and M.-D. Huang, *A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields*, in *Algorithmic number theory*, Lecture Notes in Comput. Sci., Springer, New York, 1994, 28–40.

2. J.P. Hansen, *Deligne-Lusztig varieties and group codes*, Lecture Notes in Math. **1518**, Springer, New York, 1992, 63–81.

3. J.P. Pedersen, *A function field related to the Ree group*, Lecture Notes in Math. **1518**, Springer, New York, 1992, 122–131.

4. R. Schoof, *Algebraic curves over* $\mathbf{F}_2$ *with many rational points*, J. Number Theory **41** (1992), 6–14.

5. J.-P. Serre, *Groupes algébriquest et corps de classes*, Hermann, Paris, 1959.

6. V. Shabat, *Tables of curves with many points*, available at `http://turing.wins.uva.nl/~shabat/tables.html`

Department of Mathematics, University of Texas, Austin, TX 78712
E-mail address: `voloch@math.utexas.edu`