NEW ZEALAND JOURNAL OF MATHEMATICS
Volume 47 (2017), 1-7

ON THE NUMBER OF RATIONAL POINTS ON SPECIAL FAMILIES OF CURVES OVER FUNCTION FIELDS

Douglas Ulmer and José Felipe Voloch

(Received 23 December, 2016)

Abstract. We construct families of curves which provide counterexamples for a uniform boundedness question. These families generalize those studied previously by several authors in [**Ulm14b**], [**BHP+15**], and [**CUV12**]. We show, in detail, what fails in the argument of Caporaso, Harris, Mazur that uniform boundedness follows from the Lang conjecture. We also give a direct proof that these curves have finitely many rational points and give explicit bounds for the heights and number of such points.

1. Unboundedness of Rational Points

The question of whether there is a uniform bound for the number of rational points on curves of fixed genus greater than one over a fixed number field has been considered by several authors. In particular, in [**CHM97**] Caporaso et al. showed that this would follow from the Bombieri-Lang conjecture that the set of rational points on a variety of general type over a number field is not Zariski dense. In [**CUV12**], Conceição and the present authors gave examples over function fields of families of smooth curves of fixed genus whose number of rational points is unbounded. Our first point is that these examples are part of a more general family.

Fix a prime p and a power q of p, let $\mathbb{F}_q$ be the field of q elements, and let $\mathbb{F}_q(t)$ be the rational function field over $\mathbb{F}_q$. Choose an integer $r > 1$ and prime to p, and let $h(x) \in \mathbb{F}_q[x]$ be a polynomial of positive degree which is not the e-th power of another element of $\mathbb{F}_q(t)$ for any divisor $e > 1$ of r. We also assume that $h(0) \neq 0$. For $a \in \mathbb{F}_q(t) \setminus \mathbb{F}_q$, let $X = X_{h,r,a}$ be the smooth projective curve over $\mathbb{F}_q(t)$ associated to the equation

$$X: \quad y^r = h(x)h(a/x).$$

Our hypotheses imply that X is absolutely irreducible and its genus is independent of a. In the case where h has distinct roots and degree s with $(r, s) = 1$, the Riemann-Hurwitz formula shows that X has genus $g = (r-1)s$.

Theorem 1.1. *Assume that r divides $q^f + 1$ for some $f \geq 1$. Then as a varies through $\mathbb{F}_q(t) \setminus \mathbb{F}_q$, the number of rational points of the curve $X_{h,r,a}$ over $\mathbb{F}_q(t)$ is unbounded.*

Proof. We first note that if $d = q^n + 1$, r divides d, and $a = t^d$, then we have a rational point $(x, y) = (t, h(t)^{d/r})$ on X. Second, if m divides n and n/m is odd,

2010 *Mathematics Subject Classification* 11G30.
Key words and phrases: algebraic curves, function fields, rational points.

then $d' = q^m + 1$ divides d. If r divides d', setting $e = d/d'$, we have another rational point $(x, y) = (t^e, h(t^e)^{d'/r})$ on X. Thus if we take n to be a multiple of f such that n/f is odd and has many factors, we have many points. □

Examples 1.2. Up to change of coordinates, the case $r = 2$, $h(x) = x + 1$ is the elliptic curve studied in [**Ulm14b**], the case $r > 1$, $h(x) = x+1$ is the curve of genus $r-1$ whose Jacobian is the subject of [**BHP+15**], and the case $r = 2$, $h(x) = x^s+1$ with s odd is the curve of genus s studied in [**CUV12**].

Remark 1.3. Fixing h and r, here we consider a family of curves X_a over a fixed field $\mathbb{F}_q(t)$. It is sometimes more convenient to consider the fixed curve $y^r = h(x)h(t/x)$ over extensions $\mathbb{F}_q(u)/\mathbb{F}_q(t)$ where t is a varying rational function of u.

Consider the case $r = 2$, $h(x) = x^s + 1$ with s odd. Let $\mathcal{X}$ be the smooth projective surface with affine model

$$y^2 = x(x^s + 1)(x^s + t^s)$$

and consider the fibration $\mathcal{X} \to \mathbb{P}^1$, $(x, y, t) \mapsto t$. Its generic fiber is isomorphic to $X_{h,r,t}$ over $\mathbb{F}_q(t)$. As remarked in [**CUV12**], the results of [**CHM97**] show that the fibration has a fibered power which covers a variety of general type. However, since this fibration is defined over a finite field, the variety of general type will also be defined over a finite field. Moreover it may have a Zariski dense set of $\mathbb{F}_p(t)$-rational points, so the rest of the argument of [**CHM97**] does not apply. (See [**AV96**] for a general discussion, including the function field case).

We can be more specific: In the next section, we will see that for many choices of h and r, $X_{h,r,t}$ has a model over $\mathbb{P}^1_t$ which is already a variety of general type.

2. Geometry of a Regular Proper Model of X

When a curve X over $\mathbb{F}_q(t)$ has a model $\mathcal{X} \to \mathbb{P}^1_t$ such that $\mathcal{X}$ is dominated by a product of curves, many questions about X become much simpler. For example, the Tate conjecture on divisors holds for $\mathcal{X}$, the conjecture of Birch and Swinnerton-Dyer holds for the Jacobian of X, and it is often possible to compute or estimate the rank of the Néron-Severi group of $\mathcal{X}$ and the rank of group of rational points on the Jacobian. (This observation is mainly due to Shioda [**Shi86**] with further elaboration in [**Ulm07**].)

Fix a polynomial $h(x) \in \mathbb{F}_q[t]$ and an integer r with hypotheses as in the first section. Fix also an integer d prime to p, and let $X = X_{h,r,t^d}$ be the smooth projective curve over $\mathbb{F}_q(t)$ associated to the equation

$$y^r = h(x)h(t^d/x).$$

Let $\mathcal{X}$ be a smooth projective surface equipped with a morphism to $\mathbb{P}^1$ whose generic fiber is isomorphic to X. (The construction is elementary; see [**Ulm14a**, Ch. 2] for details.) In this section, we will show that $\mathcal{X}$ is dominated by a product of curves and give two applications: $\mathcal{X}$ is often of general type, and X is non-isotrivial.

Let $\mathcal{C} = \mathcal{C}_{h,r,d}$ be the smooth projective curve over $\mathbb{F}_q$ associated to

$$w^r = h(z^d).$$

Our hypotheses on h and r imply that $\mathcal{C}$ is absolutely irreducible. Note that $\mathcal{C}$ admits an action (over $\overline{\mathbb{F}}_q$) of the group $G := \mu_r \times \mu_d$.

Proposition 2.1. *The surface $\mathcal{X}$ is birational to the quotient of $\mathcal{C}\times\mathcal{C}$ by the action of G, where G acts "anti-diagonally," i.e., by the action above on the first factor and by its inverse on the second factor.*

Proof. The surface $\mathcal{X}$ is birational to the (quasi-) affine surface given by

$$\mathcal{Y}: \quad y^r = h(x)h(t^d/x).$$

We define a rational map ϕ from $\mathcal{C}\times\mathcal{C}$ to $\mathcal{Y}$ by setting

$$\begin{aligned}\phi^*(x) &= z_1^d,\\ \phi^*(y) &= w_1w_2,\\ \phi^*(t) &= z_1z_2.\end{aligned}$$

It is evident that ϕ factors through $(\mathcal{C}\times\mathcal{C})/G$ where G acts anti-diagonally, and a consideration of degrees shows that the induced rational map from $(\mathcal{C}\times\mathcal{C})/G$ to $\mathcal{Y}$ is birational. □

We note that $(\mathcal{C}\times\mathcal{C})/G$, and therefore $\mathcal{X}$, contains infinitely many rational curves. Indeed the images in the quotient of the graphs of q^n-power Frobenius maps $\mathcal{C}\to\mathcal{C}$ and their transposes are rational curves. This gives a Zariski dense set of rational curves on $\mathcal{X}$.

Note that when $d = q^n+1$, the image of the graph of the q^n-power Frobenius $\mathcal{C}\to\mathcal{C}$ in $\mathcal{X}$ is the section of $\mathcal{X}\to\mathbb{P}^1$ corresponding to the point $(t, h(t)^{d/r})$, and the image of the transpose of Frobenius corresponds to the point $(t^{d-1}, h(t)^{d/r})$. In some sense, this "explains" these points.

Our next result shows that $\mathcal{X}$ has general type as soon as $\mathcal{C}$ has genus >1. (See also [**Gra07**, §7.1] for another proof of this fact.) If h has degree s with $(r,s)=1$ and distinct, non-zero roots, and if $r|d$, then the genus of $\mathcal{C}$ is $(r-1)(ds-2)/2$ which is >1 for large d as soon as $r>1$ and $s\geq 1$.

Lemma 2.2. *Let C be a curve of genus $g(C)>1$ over a field k. Let G be a finite abelian group of automorphisms of C with the order of G prime to the characteristic of k. Let $Y = C\times C$ and let G act on Y "anti-diagonally": $g(y_1,y_2) = (gy_1, g^{-1}y_2)$. Then the quotient Y/G is of general type.*

Note that Y/G is normal with isolated singular points, so it makes sense to speak of the canonical bundle and the plurigenera of Y/G.

Proof. We will show that Y/G has Kodaira dimension 2, i.e., that the plurigenera of Y/G grow quadratically. Let $V_n = H^0(C, K_C^{\otimes n})$. Since $g(C)>1, \dim V_n$ grows linearly with $n: \dim V_n \geq cn$ for some $c>0$.

Decompose V_n into eigenspaces for the action of G. At least one of them has dimension $\geq \dim(V_n)/|G|$. Call it $V_{n,\rho}$ (where ρ is the character by which G acts on this subspace).

Since G acts anti-diagonally, the image of $V_{n,\rho}\otimes V_{n,\rho}\to H^0(Y, K_Y^{\otimes n})$ (via pull-back and wedge product) lands in the G-invariant subspace, which we denote $H^0(Y,K_Y^{\otimes n})^G$. The map is injective, so

$$\dim H^0(Y,K_Y^{\otimes n})^G \geq (\dim(V_n)/|G|)^2.$$

This last expression is $\geq c'n^2$ for some $c'>0$.

Since $|G|$ is prime to the characteristic of k, we have

$$H^0(Y/G, K_{Y/G}^{\otimes n}) = H^0(Y, K_Y^{\otimes n})^G.$$

Thus $\dim H^0(Y/G, K_{Y/G}^{\otimes n}) \geq c'n^2$, as required. □

Now we show that X is not isotrivial, i.e., there does not exist a curve X_0 defined over a finite field k and an isomorphism

$$X \times_{\mathbb{F}_q(t)} \overline{\mathbb{F}_q(t)} \cong X_0 \times_k \overline{\mathbb{F}_q(t)}.$$

Proposition 2.3. *The curve $X = X_{h,r,a}$ is not isotrivial for any $a \in \mathbb{F}_q(t) \setminus \mathbb{F}_q$.*

Proof. From the definition of isotrivial, it clearly suffices to prove that $X_{h,r,t}$ is not isotrivial, so we assume $a = t$ for the rest of the proof. We will use the domination of a regular proper model $\mathcal{X}$ of X by $\mathcal{C} \times \mathcal{C}$ where $\mathcal{C}$ is the curve associated to $w^r = h(z)$.

Let $Z \subset \mathcal{C} \times \mathcal{C}$ be the locus where $z_1 z_2 = 0$. Since $h(0) \neq 0$, this is the union of $2r$ curves each isomorphic to $\mathcal{C}$ meeting transversally at r^2 points.

Let $\widetilde{\mathcal{C} \times \mathcal{C}}$ be the blow up of $\mathcal{C} \times \mathcal{C}$ at the closed points where either $(z_1 = 0, z_2 = \infty)$ or $(z_1 = \infty, z_2 = 0)$. Let $\tilde{Z}$ be the strict transform of Z in $\widetilde{\mathcal{C} \times \mathcal{C}}$.

The anti-diagonal action of $G := \mu_r$ on $\mathcal{C} \times \mathcal{C}$ lifts uniquely to $\widetilde{\mathcal{C} \times \mathcal{C}}$, it preserves $\tilde{Z}$, and it has no fixed points on $\tilde{Z}$. (Again we use that $h(0) \neq 0$.) It follows that $\tilde{Z}/G$ is the union of two copies of $\mathcal{C}$ meeting transversally at r points. In particular, $\tilde{Z}/G$ is a semistable curve. It also follows that $\widetilde{\mathcal{C} \times \mathcal{C}}/G$ is regular in a neighborhood of $\tilde{Z}/G$.

Let $\mathcal{C} \times \mathcal{C} \dashrightarrow \mathbb{P}^1_t$ be the rational map defined by $t = z_1 z_2$. This induces a morphism $\widetilde{\mathcal{C} \times \mathcal{C}} \to \mathbb{P}^1$ which factors through $\pi : \widetilde{\mathcal{C} \times \mathcal{C}}/G \to \mathbb{P}^1_t$. Moreover, the generic fiber of π is X, and $\pi^{-1}(0)$ is precisely $\tilde{Z}/G$.

We have thus constructed a regular proper model of X in a neighborhood of $t = 0$ such that the special fiber is a non-smooth, semi-stable curve. This proves that the moduli map $\mathbb{P}^1_t \to \overline{\mathcal{M}}_g$ associated to X is non-constant, and so X is non-isotrivial. □

3. Height Bounds

The finiteness of $X(\mathbb{F}_q(t))$ when X has genus > 1 is of course a consequence of the Mordell conjecture for function fields. We will use the ABC theorem to give a direct, effective proof of this fact for a subclass of the curves studied above, namely a common generalization of the curves in [**CUV12**] and [**BHP+15**].

For the rest of the paper, we fix positive integers r and s prime to one another and to p, we let $h(x) = x^s + 1$, and we study the curve

$$X: \quad y^r = h(x)h(t^d/x) = \frac{(x^s+1)(x^s+t^{ds})}{x^s}$$

over $\mathbb{F}_q(t)$ where d is prime to p. As noted above, the genus g of X is $(r-1)s$.

Note that if (x, y) is an $\mathbb{F}_q(t)$-rational point on X and x is a p-th power, then $(t^d/x, y)$ is another point and t^d/x is not a p-th power.

In this section, we prove the following height bound.

Theorem 3.1. *Suppose that the genus g of X is > 2. Let (x, y) be an $\mathbb{F}_q(t)$-rational point on X, write $x = u/v$ with $u, v \in \mathbb{F}_q[t]$, $(u, v) = 1$, and let $\delta = max\{\deg u, \deg v\}$. If x is not a p-th power, then*

$$\delta \leq \frac{dg - 1}{g - 2}$$

and if x is a p-th power, then

$$\delta \leq \frac{2d(g-1) - 1}{g - 2}.$$

Proof. The case when x is a p-th power follows immediately from the case when x is not a p-th power after replacing x with t^d/x, so we may assume x is not a p-th power.

We write a for t^d. The hypotheses imply that

$$\frac{(u^s + v^s)(u^s + a^s v^s)}{u^s v^s}$$

is an r-th power in $\mathbb{F}_q(t)$. Since u and v are relatively prime, we have

$$\gcd(u^s, u^s + a^s v^s) \,|\, a^s$$

and

$$\gcd(u^s + v^s, u^s + a^s v^s) \,|\, (a^s - 1),$$

and all of the other terms in the displayed quantity are pairwise relatively prime, i.e.,

$$\gcd(u^s, v^s) = \gcd(u^s, u^s + v^s) = \gcd(v^s, u^s + v^s) = \gcd(v^s, u^s + a^s v^s) = 1.$$

Therefore, v is an r-th power, $t^i u$ is an r-th power for some $i \in \{0, \ldots, r-1\}$, and $f(u^s + v^s)$ is an r-th power for some f dividing $(a^s - 1)^{r-1}$.

Next, we recall the ABC theorem in the following form (a special case of [**Mas84**, Chapter 6, Lemma 10]).

ABC Theorem. *If $A, B \in \mathbb{F}_q[t]$ are not both p-th powers, $(A, B) = 1$, and $C = A + B$, then we have*

$$\max\{\deg A, \deg B, \deg C\} \leq \deg N(ABC) - 1,$$

where $N(P)$ is the product of irreducible factors of P.

Apply this with $A = u^s$, $B = v^s$. We have $\deg N(A) \leq (\delta + r - 1)/r$, $\deg N(B) \leq \delta/r$, and

$$\deg N(C) \leq (\delta s + \deg f)/r \leq (\delta s + ds(r-1))/r.$$

Since A and B are relatively prime, $N(ABC) = N(A)N(B)N(C)$ and we find that

$$\delta s \leq \frac{\delta(s+2) + ds(r-1) - 1}{r}$$

and so

$$\frac{\delta((r-1)s - 2)}{r} \leq \frac{ds(r-1) - 1}{r}.$$

Assuming that $g - 2 = (r-1)s - 2 > 0$, we find that

$$\delta \leq \frac{ds(r-1) - 1}{(r-1)s - 2} = \frac{dg - 1}{g - 2}$$

as desired. □

We note that when $d = p^n + 1$, we have points on $X(\mathbb{F}_p(t))$ with x coordinate equal to $t^{(p^n+1)/(p^m+1)}$, which are not p-th powers, and for $m|n$, with n/m odd, equal to $t^{(p^n+1)p^m/(p^m+1)}$, which are p-th powers. This shows that no major improvement of the inequality of the theorem can be expected.

4. Cardinality Bounds

We continue to study the curve

$$X: \quad y^r = \frac{(x^s+1)(x^s+t^{ds})}{x^s}$$

over $\mathbb{F}_q(t)$ where p, r, and s are pairwise relatively prime and d is prime to p. Theorem 3.1 yields an explicit bound on the number of points on $X(\mathbb{F}_q(t))$ which is independent of q:

Corollary 4.1. *There is a constant C depending only on r and s, such that, for any power q of p and any d prime to p, we have $\#X(\mathbb{F}_q(t)) \leq C^d$.*

Proof. Theorem 3.1 shows that the x coordinate of any affine point has degree $O(d)$ and likewise the y coordinate. A curve that has infinitely many points of bounded height (with coefficients in the algebraic closure of $\mathbb{F}_q$) is isotrivial by [**Lan60**, Proposition 2] and the remark that immediately follows, so we get finiteness this way without appealing to the Mordell conjecture. But we get more: The conditions on the $O(d)$ coefficients of the numerator and denominator of x and y for the point to lie on X is a system of $O(d)$ equations in $O(d)$ variables and each equation has degree at most $r+2s$. We can consider this system over the algebraic closure of $\mathbb{F}_p$ and, by the above argument, it has finitely many solutions, so by Bézout's theorem it has at most $(r+2s)^{O(d)}$ solutions, proving the corollary. □

The main result of [**PP13**] implies a bound similar to that of the theorem but with C depending on r, s, and p. The cardinality of the set of points constructed in [**CUV12**] (and reviewed in Section 1 above) when $d = p^n + 1$ is bounded by a multiple of the number of divisors of n, so there is a huge gap between the known upper bounds for the number of points and the number of points we can produce. It would be very interesting to narrow this gap or perhaps identify all the rational points.

Finally, we note that it is possible to improve the exponent when d is large with respect to q. Indeed, the degree of conductor of the Jacobian of X is $O(d)$ (with a constant depending only on r and s). It follows from the arguments in [**Ulm07**, §11] (generalizing [**Bru92**]) that the order of vanishing at $s = 1$ of the L-function of X, and therefore the rank of the Mordell-Weil group of the Jacobian of X, is $O(d/\log d)$ (with a constant depending on r, s, and q). Applying [**BV96**], we find that the number of points on X is at most $C_1^{d/\log d}$ where C_1 depends on r, s, and q. These bounds, and in particular the exact value of the rank, can in many cases be determined more precisely using the domination by a product of curves in Section 3 and arguments as in [**Ulm13**].

Acknowledgements: Both authors thank the Simons Foundation for financial support under grants #359573 and #234591. We also thank Igor Shparlinski for comments on an earlier version of the paper.

References

[AV96] D. Abramovich and J. F. Voloch. *Lang's conjectures, fibered powers, and uniformity.* New York J. Math., **2** (1996), 20–34, electronic.

[BHP+15] L. Berger, C. Hall, R. Pannekoek, J. Park, R. Pries, S. Sharif, A. Silverberg, and D. Ulmer. *Explicit arithmetic of Jacobians of generalized Legendre curves over global function fields.* Preprint, arXiv:1505.00021, (2015).

[Bru92] A. Brumer. *The average rank of elliptic curves. I.* Invent. Math., **109** (1992), 445–472.

[BV96] A. Buium and J. F. Voloch. *Lang's conjecture in characteristic p: an explicit bound.* Compositio Math., **103** (1996), 1–6.

[CHM97] L. Caporaso, J. Harris, and B. Mazur. *Uniformity of rational points.* J. Amer. Math. Soc., **10** (1997), 1–35.

[CUV12] R. Conceição, D. Ulmer, and J. F. Voloch. *Unboundedness of the number of rational points on curves over function fields.* New York J. Math., **18** (2012), 291–293.

[Gra07] A. Granville. *Rational and integral points on quadratic twists of a given hyperelliptic curve.* Int. Math. Res. Not. IMRN, Art. ID 027 (2007), 1–25.

[Lan60] S. Lang. *Integral points on curves.* Inst. Hautes Études Sci. Publ. Math., **6** (1960), 27–43.

[Mas84] R. C. Mason. *Diophantine Equations Over Function Fields*, volume 96 of London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1984.

[PP13] A. Pacheco and F. Pazuki. *Bounds for the number of rational points on curves over function fields.* New York J. Math., **19** (2013), 131–144.

[Shi86] T. Shioda. *An explicit algorithm for computing the Picard number of certain algebraic surfaces.* Amer. J. Math., **108** (1986), 415–432.

[Ulm07] D. Ulmer. *L-functions with large analytic rank and abelian varieties with large algebraic rank over function fields.* Invent. Math., **167** (2007), 379–408.

[Ulm13] D. Ulmer. *On Mordell-Weil groups of Jacobians over function fields.* J. Inst. Math. Jussieu, **12** (2013), 1–29.

[Ulm14a] D. Ulmer. *Curves and Jacobians over function fields.* In G. Boeckle et al., editor, *Arithmetic Geometry over Global Function Fields*, Advanced Courses in Mathematics CRM Barcelona, pages 281–337. Springer, Basel, 2014.

[Ulm14b] D. Ulmer. *Explicit points on the Legendre curve.* J. Number Theory, **136** (2014), 165–194.

Douglas Ulmer
School of Mathematics,
Georgia Institute of Technology,
Atlanta, GA 30332,
USA
douglas.ulmer@math.gatech.edu

José Felipe Voloch
School of Mathematics and Statistics,
University of Canterbury,
Private Bag 4800, Christchurch 8140,
New Zealand
felipe.voloch@canterbury.ac.nz