Mathematical Research Letters **4**, 663–666 (1997)

PURELY INSEPARABLE POINTS ON CURVES OF HIGHER GENUS

Minhyong Kim

1.

Let k be a field of characteristic $p > 0$ and let K be a function field of one variable over k, i.e., $K \simeq k(t)[s]/(h(t,s))$ where $h \in k[t,s]$ is a polynomial irreducible in $\bar{k}[t,s]$. Now let $f(x,y)$ be a polynomial with coefficients in K. We are interested in K-rational solutions to the equation

$$f(x,y) = 0.$$

For example, the equation

$$x^l - y^l = t^l - 1$$

has solution $(t,1)$ in $K = k(t)$.

Given any such f we can keep 'twisting' its coefficients with the Frobenius map of K and get new polynomials $f^{(n)}(x,y)$ (by which we denote the nth twist) and new equations $f^{(n)}(x,y) = 0$.

The question we wish to ask is whether $f^{(n)} = 0$ can keep having new solutions as we increase n. An 'old' solutions for the twisted equation means the following: If (x,y) is a solution for $f = 0$, then obviously, $(x,y)^{(n)} := (x^{p^n}, y^{p^n})$ is a solution for $f^{(n)} = 0$; in the example above, the equation $f^{(1)} = 0$ is

$$x^l - y^l = t^{lp} - 1$$

and we have the twisted solution $(t^p, 1)$.

By *new solutions* to $f^{(n)} = 0$ then, we mean solutions which *don't* arise by twisting solutions to $f^{(n-1)} = 0$.

One way in which infinitely many $f^{(n)} = 0$ can have new solutions is if f has coefficients in some finite field (f is a 'constant' polynomial). For then, infinitely many $f^{(n)}$ will be equal to f, and hence, have solutions which are not Frobenius twists (if f does).

For example, if $K = k(t)[s]/(s^l - t^l + 1)$ (with l prime to p), then the equation $x^l - y^l = 1$ has the $K-$rational solution (t,s), and all its twists have the new solution (t,s). Obviously, such a thing can happen also with an f which admits a K-rational change of variables to such a constant polynomial. The purpose of this note is to show that this is essentially all that can happen for higher genus equations, that is:

Received May 15, 1997.

Theorem 1. *Suppose $f(x,y)=0$ defines a curve over K whose genus over $\bar{K}$ is at least 2 and suppose infinitely many of the equations $f^{(n)}(x,y)=0$ have new solutions. Then there is a change of variables in some finite extension of K (including a possible extension of k) which sends f to a polynomial with coefficients in a finite field.*

More precisely, the 'change of variables' here refers to a birational map of curves.

By combining this with standard finiteness for each individual curve $f^{(n)}=0$ (geometric Mordell conjecture), we get the following

Corollary 1. *Suppose $f(x,y)=0$ defines a curve over K whose genus over $\bar{K}$ is at least 2 and suppose it is not birational over any finite extension to a curve defined over a finite field. Then the set of its solutions in the field $K^{1/p^{\infty}} := \lim_n K^{1/p^n}$ is finite.*

For the theorem, our two examples above illustrate such a change of variables, and why an extension may be necessary. The field K in this case is $k(t)$ and the extension is $k(t)[s]/(s^l - t^l + 1)$ while the change of variables is $(x,y) \mapsto (x/s, y/s)$. The existence of such a 'constant form' for the equation over some extension may cause infinitely many new solutions as follows: Let l be a prime different from p and let n range over integer multiples of $l-1$. Then we see that $p^n - 1 = ml$ for some m, and hence,

$$[(t^l-1)^m t]^l - [(t^l-1)^m]^l = (t^l-1)^{p^n-1}t^l - (t^l-1)^{p^n-1} = t^{lp^n} - 1,$$

so that $((t^l-1)^m t, (t^l-1)^m)$ are new solutions to $f^{(n)}=0$. One checks easily that the constant form is responsible for these solutions.

2.

Proof of Theorem:

It suffices to prove the theorem after a finite extension of K (which may include a finite extension of k), so we may assume that there is a projective smooth model for $f(x,y)=0$ which has *semistable reduction*. That is, the curve $f(x,y)=0$ over K is birational to the generic fiber of a map $\pi : X \to B$ where X is a projective smooth surface and B a projective smooth curve over k, such that

i) π has smooth generic fiber of genus at least two,
ii) all of its geometric fibers are reduced with at worst normal crossing singularities;
iii) and its fibers contain no (-1)-curves.

Then a new solution to $f^{(n)} = 0$ will give rise to a diagram

$$\begin{array}{ccc} & & X \\ & \overset{P}{\nearrow} & \downarrow \\ B & \overset{F^n}{\to} & B \end{array}$$

with the property that the map $P^*\Omega_X \to \Omega_B$ is non-zero.

Most of the proof is contained in the following

Claim: Suppose the fibration $\pi : X \to B$ is not isotrivial. Then a diagram as above exists for at most finitely many n.

Proof. Assume that we have a separable map $P : B \to X$ such that $\pi \circ P = F^n$ for $n \geq 1$. Let $S \subset B$ be the set of singular values of the fibration and let $D \subset X$ be the union of the singular fibers, that is, $D = \pi^{-1}(S)$. Let $\Omega(\log D)$ be the sheaf of differentials with log poles along the normal crossing divisor D. This fits into an exact sequence

$$0 \to \pi^*\Omega_B(S) \to \Omega(\log D) \to \omega \to 0$$

since the dualizing sheaf is isomorphic to the sheaf of relative log differentials. To see this, note that both are invertible sheaves and $c_1(\Omega(\log D)) = K_X + D$ so that $c_1(\Omega(\log D)) - c_1(\pi^*\Omega_B(S)) = K_X - \pi^* K_B$.

We have a non-zero map $P^*\Omega(\log D) \to \Omega_B((F^n)^{-1}S) = \Omega_B(S)$ which factors to $P^*\omega \to \Omega_B(S)$, by the inseparability. Thus, $\deg P^*\omega \leq 2g_B - 2 + s$, where $s = |S|$.

Now, since ω is a big line bundle [Sz], this degree bound implies that the divisor $P_*(B)$ lies inside a bounded algebraic family. In particular, only finitely many degrees for the intersection with a fiber is possible. This implies that in $\pi \circ P = F^n$, n is bounded.

Suppose $f^{(n)} = 0$ has new solutions for infinitely many n. By the claim above this implies that X/B is isotrivial. So replacing B by a base change, we can assume that X is birational to $B \times C$, where C is a smooth projective curve over k of genus at least 2. Then a new solution of degree p^n corresponds to a (non-constant) separable map $g : B \to (F^n)^*C$, where the Frobenius in this case is the Frobenius of k. This must exist for infinitely many n. By a theorem of Severi [S], there are only finitely many function fields of genus at least two separably contained in the function field of B. That is, infinitely many of the $(F^n)^*C$ are isomorphic. This implies that some Frobenius pull-back of C is defined over a finite field (by considering the corresponding moduli points).

Acknowledgement

I am grateful to Felipe Voloch for discussions related to this paper.

References

[S] P. Samuel, *Compléments á un article de Hans Grauert sur la conjecture de Mordell*, Publ. Math. I.H.E.S. (1965), 311–318.

[Sz] L. Szpiro, *'Propriétés numériques du faisceaux dualisant relatif,' in 'Pinceaux de courbes de genre au moins deux'*, Astérisque **86** (1981).

Department of Mathematics, University of Arizona, Tucson, AZ 85721
E-mail address: kim@math.arizona.edu