Diophantine Approximation in characteristic p

José Felipe Voloch

Abstract: We study diophantine approximations to algebraic functions in characteristic p. We precise a theorem of Osgood and give two classes of examples showing that this result is nearly sharp. One of these classes exhibits a new phenomenon.

In this note we will be concerned about the approximation of functions, algebraic over a global field K of positive characteristic by elements of K with respect to a valuation v of K. We define, for $y \in K_v \setminus K$ (although we will consider only y algebraic over K in what follows):

$$\alpha(y) = \limsup_{r \in K} v(y-r)/h(r),$$

where $h(r) = [K : k(r)]$, where k is the constant field of K. We will give some examples that exhibit pathological behaviour. Recall that $2 \leq \alpha(y) \leq d(y) := [K(y) : K]$, which are analogues of the classical theorems of Dirichlet and Liouville. Osgood [O] has shown that $\alpha(y) \leq [(d(y)+3)/2]$ if y does not satisfy a Riccati equation and we will prove the same bound if the cross ratio of any four conjugates of y over K is non constant. There are some results on $\alpha(y)$ if y satisfies $y^q = (ay+b)/(cy+d)$ where $a,b,c,d \in K, ad-bc \neq 0$ and q is a power of p, due to the author [V1] and others([BS],[dM],[MR]). One may conjecture that these are actually the only functions not satisfying Osgood's bound. We shall give examples that show that Osgood's bound is close to being best possible.

Take $K = k(x)$ and y satisfying $y^p - y = x$ and $z = y^2$ (y is a classical example of Mahler's). We have $\alpha(y) = d(y) = d(z) = p$. Also, whenever $v(y-r)/h(r)$ is near p we have $v(z-r^2)/h(r^2)$ near $p/2$. It follows (see below) that $\alpha(z) = p/2$. Note that z does not satisfy a Riccati equation. This example can be generalized as follows: Given y and $R(Y) \in K(Y)$ a rational function of degree d in Y, then $d(R(y)) \leq d(y)$ and $\alpha(R(y)) \geq \alpha(y)/d$. So if $\alpha(y)$ is large we get new examples of well approximated functions which in general do not satisfy Riccati equations. We shall also produce a very different class of examples with "large" $\alpha(y)$.

Define, for y as above and α a real number,

$$b(y,\alpha)=\limsup_{r\in K} v(y-r)-\alpha h(r).$$

(Compare [dM], but note that our definitions are minus the logarithms of those there). We have that $b(y,\alpha)=+\infty$ (resp. $-\infty$) if $\alpha<\alpha(y)$ (resp. $>\alpha(y)$). For example, Osgood actually showed that $b(y,[(d(y)+3)/2])\neq+\infty$ if y does not satisfy a Riccati equation. We need the following

Lemma 1. *Let $y\in K_v, y\notin K$. Suppose $r_n\in K$ satisfy*

$$\lim_{n\to\infty} v(y-r_n)/h(r_n)=\alpha,\ \lim_{n\to\infty} h(r_{n+1})/h(r_n)=\beta,$$

where $\alpha>\beta^{1/2}+1$. Then $\alpha(y)=\alpha$ and $b(y,\alpha)=\limsup_n v(y-r_n)-\alpha h(r_n)$.

Proof: Except for the last statement, this is proposition 5 of [V1], and the last statement also follows easily from the proof given there. All the results in [V1] are stated for $K=k(x)$ but they all immediately generalize with their proofs for general K.

We can now state

Theorem 1. *Let $y\in K_v$ satisfy $y^q=(ay+b)/(cy+d)$ where $a,b,c,d\in K, ad-bc\neq 0$ and q is a power of the characteristic of K. Let $R(Y)\in K(Y)$ be a rational function of degree d in Y. Assume that $\alpha(y)>d(q^{1/2}+1)$, Then*

$$\alpha(R(y))=\alpha(y)/d$$

and $b(R(y),\alpha(R(y)))\neq\pm\infty$.

Proof: If $R(y)=y$ this is proved in [V1] and [dM]. We may then assume $d>1$. It follows from Theorems 1 and 2 of [V1] and the above lemma that there is a sequence $r_n\in K$ as in the lemma with $\alpha(y)=\alpha$ and $\beta=q$. If we consider the sequence $R(r_n)$, then we can apply the lemma with $\alpha=\alpha(y)/d$ and $\beta=q$. Finally, it is clear that

$$v(R(y)-R(r_n))-(\alpha(y)/d)h(R(r_n))=v(y-r_n)-\alpha(y)h(r_n)+O(1).$$

This completes the proof.

By taking y as in the theorem with $\alpha(y) = d(y)$ (see above or [V1] for specific examples) and R as in the theorem with $d = 2$, we get examples $R(y)$ such that $\alpha(R(y)) = d(y)/2$ and $b(R(y), \alpha(R(y))) \neq \pm\infty$. In general, $R(y)$ will not satisfy a Riccati equation which shows that Osgood's theorem is nearly sharp. Our next examples will also show that Osgood's theorem is nearly sharp but will be of a different nature.

Suppose that k is a finite field with q elements and let E be an elliptic curve defined over k. Let $K = k(E)$ be its function field. A point in $E(K)$ corresponds to a rational map $E \to E$ defined over k. Let $P_0 \in E(K)$ correspond to the identity I and $P_n \in E(K)$ correspond to the n-th iterate of the k-Frobenius map F. Note that P_n belong to the subgroup of $E(K)$ generated by P_0 and P_1, which is of finite index on $E(K)$ if and only if E is ordinary. For example $P_2 + aP_1 - qP_0 = 0$, where $a = q + 1 - \#E(k)$. The Néron-Tate height of a point of $E(K)$ is the degree of the corresponding map. For example, $P_n - P_0$ correspond to $F^n - I$ hence $h(P_n - P_0) = q^n + 1 - a_n = \#E(k_n)$, where $[k_n : k] = n$ and $|a_n| \leq 2q^{n/2}$.

Fix now an integer $m \geq 2, (m, q) = 1$ and assume that $E(k)$ contains the m-torsion on E. Then $P_n - P_0 = mQ_n, Q_n \in E(K)$. Note that P_0 is not divisible by m in $E(K)$ but let Q be the point on E defined over the algebraic closure of K which satisfies $mQ = -P_0$ and $K(Q)/K$ corresponds to the isogeny multiplication by m. Choose a Weierstrass equation for E and let s be the x-coordinate of Q. Let v be the place of K corresponding to the point at infinity of E.

Theorem 2. *Notation as above. The function s belongs to K_v and is algebraic of degree $d(s) = m^2$ over K. Moreover, if $m^2 > 2(q^{1/2}+1)$, then $\alpha(s) = d(s)/2$ and $b(s, \alpha(s)) = +\infty$.*

Proof: The first claim of the theorem is standard. Let r_n be the x-coordinate of Q_n as above. Note that $P_n \to 0$ v-adically so $Q_n \to Q$. Moreover, $h(r_n) = 2h(Q_n) = (2/m^2)h(P_n - P_0)$ and since multiplication by m is an étale map, it follows easily that $v(r_n - s) = q^n$. The theorem now follows from lemma 1 and the (well-known) fact that

$a_n/2q^{n/2}$ gets arbitrarily close to 1 as $n \to \infty$.

Note that the examples given by theorem 2 are genuinely different from those in theorem 1, as attested by the behaviour of "b". The conditions above impose some restrictions on m, q, namely $m^2 \le q + 1 + 2q^{1/2}, m^2 > 2(q^{1/2} + 1), m|(q-1)$ (see [V2]) but these conditions are satisfied by some values of q as soon as $m > 2$. For example $m = 3, q = 4, 7, m = 4, q = 9, 13, 17, 25, 29, 37, 41$. Another interesting remark is that these examples seem to be the only known algebraic functions s with $b(s, \alpha(s)) = \pm\infty$. Finally note that the above examples can be modified to work over $k(x)$ as follows. If E has equation $Y^2 = f(X)$ (assume q odd), consider the elliptic curve E' defined over $k(x)$ by the equation $f(x)Y^2 = f(X)$. E' is a twist of E and the K-rational points of E considered above will give points on $E'(k(x))$ to which one can apply the same arguments and get the examples over $k(x)$. This trick already occurs in Manin's elementary proof of the Riemann hypothesis for elliptic curves over finite fields.

As for the promised improvement on Osgood's result we have

Theorem 3. *Suppose that $y \in K_v$ is algebraic over K of degree d. If $b(y, [(d+3)/2]) = +\infty$ then the cross ratio of any four conjugates of y lies in k.*

By definition, the cross ratio of $x_1, \ldots, x_4$ is

$$[x_1, x_2, x_3, x_4] = (x_4 - x_1)(x_3 - x_2)/(x_4 - x_2)(x_3 - x_1).$$

Proof: By Osgood's theorem [O], y satisfies a Riccati differential equation $dy/dx = ay^2 + by + c$ where $a, b, c, x \in K$ and x a separating variable (Osgood only states the result for $K = k(x)$ but it is true in general). Let $\mathcal{D}(Y) = dY/dx - (aY^2 + bY + c)$. Suppose $r_n \in K$ are such that $\lim_{n\to\infty} v(y - r_n) - [(d+3)/2]h(r_n) = +\infty$. Then $v(\mathcal{D}(r_n)) = v(\mathcal{D}(r_n) - \mathcal{D}(y)) = v(y - r_n) + O(1)$ and $h(\mathcal{D}(r_n)) \le 2h(r_n) + O(1)$. On the other hand $v(\mathcal{D}(r_n)) \le h(\mathcal{D}(r_n))$ unless $\mathcal{D}(r_n) = 0$. It follows that $\mathcal{D}(r_n) = 0$ for n sufficiently large. We may assume that $1, 2, 3$ are "sufficiently large" after renumbering and it follows from classical properties of Riccati equations that

$$d/dx[y, r_1, r_2, r_3] = d/dx[r_n, r_1, r_2, r_3] = 0$$

for all n. $[Y, r_1, r_2, r_3] = \gamma Y$ is a fractional linear transformation with coefficients in K and from the above we have that $\gamma y = y_2^p, \gamma r_n = s_n^p, y_2 \in K(y), s_n \in K$, where p is the characteristic of K. It follows readily that $\lim_{n\to\infty} v(y_2 - s_n) - [(d+3)/2]h(s_n) = +\infty$ and it follows that y_2 also satisfies a Riccati differential equation. We can then iterate this procedure and find fractional linear transformations γ_n with coefficients in K such that $\gamma_n y = y_n^{p^n}, y_n \in K(y)$. If y, y', y'', y''' are any four conjugates of y then

$$[y, y', y'', y'''] = [\gamma_n y, \gamma_n y', \gamma_n y'', \gamma_n y'''] \in K^{p^n}$$

and this implies the theorem.

Remark: Let D be the divisor on $\mathbf{P}^1$ formed by the conjugates of y over K, so D is of degree d and is defined over K. Let X be the affine curve $\mathbf{P}^1 \setminus D$. It can be checked that y satisfies a Riccati equation if and only if the Kodaira-Spencer class of X, in the sense of [K], vanishes. It can also be checked that the cross ratio of any four conjugates of y lies in k if and only if X is isotrivial, that is, isomorphic to an affine curve defined over k perhaps after field extension. It then follows from theorem 3 that, when X is non-isotrivial, it has only finitely many integral points.

Acknowledgments: This research was partly supported by the NSF and by the Univ. of Texas's URI.

References.

[BS] L. E. Baum and M. M. Sweet, *Badly approximable power series in characteristic 2*, Ann. Math. **105** (1977), 573-580.

[K] N. M. Katz, *Algebraic solutions of differential equations (p-curvature and the Hodge filtration)*, Inventions Math. **18**, (1972) 1-118.

[dM] B. de Mathan, *Approximation exponents for algebraic functions in positive characteristic*, Acta Arith. **LX** (1992), 359-370.

[MR] W. H. Mills and D. P. Robbins, *Continued fractions of certain algebraic power series*, J. Number Theory **23** (1986), 388-404.

[O] C. F. Osgood, *Effective bounds on the "diophantine approximation" of algebraic functions over fields of arbitrary characteristics and applications to differential equations*, Indag. Math. **37**, (1975), 105- 119.

[V1] J. F. Voloch, *Diophantine approximation in positive characteristic*, Periodica Math. Hungarica **19** (1988), 217-225.

[V2] J. F. Voloch, *A note on elliptic curves over finite fields*, Bull. Soc. Math. France **116** (1988), 455-458.

Dept. of Mathematics, Univ. of Texas, Austin, TX 78712, U.S.A.