1

Diophantine Approximation in Finite Characteristic

Dinesh S. Thakur

Institute for Advanced Study, Princeton and University of Arizona, Tucson

Abstract. In contrast to Roth's theorem that all algebraic irrational real numbers have approximation exponent two, the distribution of the exponents for the function field counterparts is not even conjecturally understood. We describe some recent progress made on this issue. An explicit continued fraction is not known even for a single non-quadratic algebraic real number. We provide many families of explicit continued fractions, equations and exponents for non-quadratic algebraic laurent series in finite characteristic, including non-Riccati examples with both bounded or unbounded sequences of partial quotients.

On this occasion of Professor Abhyankar's 70th birthday conference, it might be appropriate to mention some recent applications of the 'high school algebra' [A] to the study of diophantine approximation for function fields in finite characteristic. This study is related to some of his loves: power series, continued fractions, algebraic curves, finite characteristic, resultants (and even automata).

1 What we know and don't know about the basic questions

The term 'irrational' suggests a need to 'rationalize' and one of the basic questions of diophantine approximation is how well we can approximate irrational real numbers by rationals. Since the rationals are dense in reals, we can make error arbitrarily small, so the question really is how small we can make it relative to the complexity (height) of the rational approximation measured traditionally by the size of its denominator. Let us recall some basic history. The details and references can be found in the papers in the bibliography, for example, in [S1] for the number field case, and [S2], [T] for function field case.

A simple application of the Dirichlet box principle applied to the fractional parts of multiples of α and to the boxes consisting of equal sized sub-intervals of the interval $(0, 1)$ (or approximation by convergents of continued fraction) shows that given irrational α, there are infinitely many rationals p/q satisfying $|\alpha - p/q| < 1/q^2$. On the other hand, if the irrational α is algebraic of degree $d = \deg(\alpha)$, then (as Liouville showed) applying the mean value theorem

* * Supported in part by NSA and NSF grants

to its minimal polynomial and points α and p/q gives $|\alpha - p/q| > c/q^d$ for some $c > 0$ and all rationals. (As a simple application, the first concrete examples of the transcendental numbers, such as $\sum 10^{-n!}$, whose truncation approximation eventually violates the inequality for any d, were given).

If we concentrate on the exponent

$$E(\alpha) := \limsup(-\frac{\log|\alpha - p/q|}{\log|q|})$$

we thus get $2 \leq E(\alpha) \leq \deg(\alpha)$. After successive improvements on the upper bound by Thue, Siegel, Dyson, finally Roth (in the Fields prize winning work) showed that $E(\alpha) = 2$, (for algebraic irrational α).

Let us just see the connection of this question to the arithmetic geometry. As Thue noticed, any improvement on the upper bound of d has interesting consequences to the question of integral points on curves: Consider the homogenized version $P(x, y) = y^d p(x/y)$ of the minimal polynomial $p(x)$ of α with integral coefficients. Then for a given constant c, the affine curve $P(x, y) = c$ can have only finitely many integral points, because as $p'(\alpha) \neq 0$, by the mean value theorem

$$|P(x, y)| = |y|^d |p(\alpha) - p(x/y)| = |y|^d |\alpha - p/q||p'(\beta)|$$

then tends to infinity with y. (It is easy to see that y can not stay bounded). Siegel using his improvement showed finiteness of integral points on all affine curves of genus more than 0, defined over number fields. Finally, Vojta generalized the work of Dyson and Roth in a wider context to give another proof of Mordell conjecture, which is now Faltings' theorem that curves of genus at least two, defined over number fields can have only finitely many rational points.

Now we can study similar questions by replacing integers by polynomials and using algebraic and rational functions instead of numbers. It is well-known that the case of function fields over finite constant fields is the most analogous situation, for example, there are only finitely many remainders whether we divide by an integer or a polynomial over a finite field. By completing the rational functions in a usual way we get the field of Laurent series thought of as parallel to say decimal expansion of real number, but supposedly simpler, since there is no carry over of digits now. So it is somewhat surprising that this question of the distribution of the exponents of algebraic functions looks more complicated.

As observed by Mahler [M], similar proofs do give analogs of Dirichlet and Liouville theorems in function field case implying the bounds $2 \leq E(\alpha) \leq \deg(\alpha)$, where the exponent is defined as above, but with integers p and q replaced by polynomials. Even the analog of Roth's theorem was proved by Uchida for function fields of characteristic zero. But we will now exclusively deal with function fields over finite fields (some considerations work for function fields over any finite characteristic field also).

Let F be a finite field of characteristic p and let q be a power of p. As mentioned above, we consider $F[t]$, $F(t)$ and $F((1/t))$ as analogs of $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.

Mahler [M] showed that $E(\alpha) = q$ for $\alpha = \sum t^{-q^i}$, as a straight estimate of approximation by truncation of this series shows. But $\alpha^q - \alpha - t^{-1} = 0$, so that α is algebraic of degree q and hence the Liouville upper bound is best possible in this case. Mahler suggested (and it was claimed and believed for a while) that such phenomena may be special to the degrees divisible by the characteristic, but Osgood [O1] gave examples in each degree for which Liouville exponent is the best possible.

This then raises the question of the possibilities and distribution of the exponents of algebraic laurent series. A priori, the set of exponents is a countable subset of the interval $[2, \deg(\alpha)]$. How does one determine it?

The continued fractions naturally enter the picture, as the good approximations all come in by truncating the continued fraction expansions. But continued fraction expansion (or even whether the sequence of partial quotients is bounded or not) is not known even for a single algebraic real number of degree more than two. (Because of the numerical evidence and a belief that algebraic numbers are like most numbers in this respect, it is often conjectured that the sequence is unbounded.) It is hard to get such expansions for algebraic numbers, because the effect of basic algebraic operations (except for adding an integer or more generally an integral Mobius transformation of determinant ± 1), such as addition or multiplication or even multiple or power, is not at all transparent on the continued fraction expansions.

2 The first type of explicit families

In finite characteristic p, on the other hand, the algebraic operation of taking p-th power has a very transparent effect: If $\alpha = [a_0, a_1, \cdots]$, then $\alpha^p = [a_0^p, a_1^p, \cdots]$, where we use a short-form $[a_0, a_1, \cdots]$ for the expansion $a_0 + 1/(a_1 + 1/(a_2 + \cdots))$.

If $A_i(t) \in F[t]$ are any non-constant polynomials, the remark above shows that

$$\alpha := [A_1, \cdots, A_k, A_1^q, \cdots, A_k^q, A_1^{q^2}, \cdots]$$

is algebraic over $F(t)$ because it satisfies the algebraic equation

$$\alpha = [A_1, \cdots, A_k, \alpha^q]$$

So we get a variety of explicit continued fractions with explicit equations.

Once we have this explicit continued fraction, it is then just simple high school algebra to calculate the exponent in terms of the degrees of A_i and determine its possible values. It was thus proved in [S2] and [T] that

Theorem 1 *Given any rational μ between $q^{1/k} + 1$ (which tends to 2 as k tends to infinity) and $q+1$, we can find a family of α's as above with $E(\alpha) = \mu$ and $\deg(\alpha) \leq q + 1$.*

Remarks: (1) It seems thus reasonable to guess that the set of exponents is just the set of rational numbers in the Dirichlet-Liouville range. That the set can not contain any irrational number is known for degree 3, as every α of degree 3 has the property that α^q is Mobius integral transformation of α. Numbers with this property are called numbers of class I. For such numbers, the rationality of the exponent is a result of de Mathan [dM]. To show that all rationals occur, we need to control the exact degrees. Since we can always take k large, so that there is huge choice in choosing A_i's of given degree, it might be reasonable to expect that the equation above is irreducible (for example) for some choice. This has been done only in a few cases. To settle whether this happens for each degree (not necessarily of the form $q+1$) may require more complicated combinatorics.

(2) In the function field case, isolated algebraic examples with both bounded and unbounded sequences of partial quotients were known. See [BS1, BS2, MR, L] and the references in [T]. Earlier explicit examples were found by large computer searches of continued fractions starting with equations for algebraic laurent series to find examples where the patterns can be guessed and proved by ad hoc methods. The large families obtained above were obtained by starting with the continued fractions themselves. In retrospect, these were continued fractions telescoping for the q-th power operation, just as previous examples of Mahler and Osgood (and Voloch) [M, O1, O2, V] were sums and products telescoping for the q-th power operation.

(3) The theorem and easy operation of scalar multiplication by constants, takes care of explicit continued fractions as well as exponents for all α's whose some q-th power is integral linear fractional (i.e., Mobius) transformation of α of constant determinant (called α's of class Ia). Since the exponent is invariant with respect to integral Mobius transformations of non-zero determinants, we get exponents for such, but not the explicit continued fractions for these or for class I elements in general. We mention the method of automata/transducers of [MR] to generate such expansions, but it has not led to direct description of the patterns yet.

(4) Most of the earlier and our examples above are of class I and thus satisfy rational Riccati equation: $d\alpha/dt = a\alpha^2 + b\alpha + c$, with $a, b, c \in F(t)$. The relevance of this equation is the important result of Osgood [O1, O2, LdM1, LdM2] that the Liouville/Mahler bound can be improved to (even effectively) $E(\alpha) \leq \lfloor \deg(\alpha)/2 \rfloor + 1$, for α not satisfying such rational Riccati differential equation.

3 The second type of explicit families

With this background, we now come to the new results giving explicitly continued fractions for many families of algebraic Laurent series which do not satisfy rational Riccati equations. We produce such families with bounded as well as unbounded sequence of partial quotients.

In fact, they are obtained by a more systematic exploitation of the idea behind another family given in [T], based on author's earlier results having to do with the continued fraction expansions of function field analog of Euler's e. (It is known to be transcendental, whereas we now apply the techniques to algebraic numbers of finite characteristic).

It is based on the following simple lemma, due to Mendes France [MF], which has been rediscovered many times.

Lemma 1. *Let* $[a_0, a_1, \cdots, a_n] = p_n/q_n$, *with the usual notation of continued fractions, then* $[a_0, \cdots, a_n, y, -a_n, \cdots, -a_1] = p_n/q_n + (-1)^n/yq_n^2$.

In words, we will refer to this pattern as a signed block reversal pattern with the new term y.

Now, if $\alpha := \sum f_i t^{-n_i} \in F((1/t))$ (where n_i is an increasing sequence of integers) is algebraic over $F(t)$ and satisfies $n_{i+1} > 2n_i$, for $i \geq i_0$ say, then the repeated applications of the lemma starting with the continued fraction of the rational function obtained by truncating at i_0-th power gives complete continued fraction of α consisting of signed block reversals, with the new y's being $t^{n_{i+1}-2n_i}$ (up to signs which are easy to calculate from the lemma). As before the exponent calculation and its range determination is routine, and we refer to [T] for it.

First we give the main examples: By taking linear combinations of Mahler's example above, we know that any

$$\alpha = \sum_{i=1}^{k} f_i (\sum_{j=0}^{\infty} t^{-m_i q^j + b_i})$$

(where $m_i \geq 0$ and b_i are rational numbers so that the exponents are integers) is algebraic. (With integral coefficients, we can write $a_i q^j + b_i(q^j - 1)/(q - 1) + c_i$). And it is easy to write down conditions on the coefficients to satisfy $n_{i+1} > 2n_i$ for large i. For example, $m_{i+1} > 2m_i$ for $1 \leq i < k$ and $qm_1 > 2m_k$ is clearly sufficient, but not necessary. With this condition, as in the Theorem 2 of [T] we see that $E(\alpha) = MAX(m_2/m_1, \cdots, m_k/m_{k-1}, qm_1/m_k)$ and that it takes any rational value between $q/2^{k-1}$ and $q^{1/k}$, if further that $q > 2^k$.

The algebraic equation for each term (corresponding to a fixed i) is immediate, since it is just a multiple of Mahler's example. So the polynomial equation satisfied by α follows, for example, by the usual elimination method using resultants. For example, when $k = 2$, we use

$$\text{Resultant}(x^q + ax + b, x^q + cx + d, x) = (d - b)^q + (ad - bc) \sum_{i+j=q-1} a^i c^j$$

The flexibility in the choice of number and coefficients m_i and b_i can be used to produce many families of α's not satisfying rational Riccati equation.

We leave the manipulation details to the interested reader and just give some examples below.

Most (every in odd characteristic, as we will see in the next section) families we thus construct have unbounded sequence of partial quotients and in fact have exponent greater than two. But we can also produce many explicit continued fraction families with bounded sequence of partial quotients in characteristic two: For example, any α as above with $q = 2^k$, $m_i = 2^{i-1}$ and $b_i > b_{i+1}/2$, for i modulo k will do.

Let us show that most of these do not satisfy the rational Riccati equation (and so are of degree more than 3): Take $f_i = 1$ for simplicity, and write α_i for the i-th term of the sum expression for the α above. Then $\alpha = \sum_{i=1}^{k} \alpha_i$, and $\alpha_i = \alpha_1^{2^{i-1}} p_i$ with $p_i := t^{b_i - 2^{i-1} b_1}$. Again for simplicity, take b_1 odd and other b_i's even, so that $\alpha' = \alpha_1/t + t^{b_1 - 2}$. If α were to satisfy rational Riccati equation $\alpha' = a\alpha^2 + b\alpha + c$, then we would have

$$\alpha_1/t + t^{b_1-2} = a(\alpha_1^2 + \alpha_1^4 p_1^2 + \cdots + \alpha_1^{2^k} p_k^2) + b(\alpha_1 + \alpha_1^2 p_1 + \cdots + \alpha_1^{2^{k-1}} p_k) + c.$$

But by the degree comparison, this equation has to be the Mahler type irreducible equation $\alpha_1^{2^k} = t^{b_1(q-1)}\alpha_1 + t^{qb_1-1}$, which is clearly impossible for most choices of p_i for $k > 2$. The same construction in characteristic $p > 2$, with say exponent p, gives examples (now $k > 1$ is fine) which are non-Riccati (in fact not of the form α' equals polynomial of degree $\leq p$).

Remarks: (1) Since we are allowed to modify finitely many terms of the series for α, we can construct examples with almost arbitrary partial quotients occurring infinitely often.

(2) We can relax $n_{i+1} > n_i$ to $n_{i+1} \geq n_i$ by changing from resulting degenerate expansion to a proper one, as explained in [T].

(3) If we just assume the inequality above for infinitely many i rather than for all large i, we do not get full continued fraction, but the resulting continued fraction has infinitely many signed block reversal places and we thus get a lower bound on its exponent.

(4) There is one more flexibility in the method, which allows for additional families, not satisfying our conditions: Usually we can substitute everywhere some polynomial $P(t)$ for each occurrence of t. But here, satisfying certain mild conditions, you can make different substitutions $P_i(t)$ for t for different i in the formula for α. Rather than giving general conditions, we will just write down a very simple illustrative example, for $q > 8$:

$$\sum (t(t+1))^{-q^j} + (t^2(t+1))^{-2*q^j}.$$

By the lemma, we again get the complete continued fraction, with block reversals at each stage with the new partial quotients y's being (up to signs) powers of t and powers of t times those of $t+1$ mixed alternately.

(5) Choosing suitable m_i and b_i, we can clearly construct explicit non-quadratic elements whose sums or various rational multiples are also explicit having signed block reversal patterns.

4 Classification and automata

Then arises the question of the classification of all algebraic α's satisfying the conditions above. For F a finite field, this has been done by computer scientists!:

First, there is a theorem of Christol [C, CKMR] which (combined with earlier work of Cobham [Co] and others) says that a power series $\sum f_n t^{-n} \in F((1/t))$ is algebraic over $F(t)$, if for each $f \in F$, the subsequence of n's for which $f_n = f$ considered as sequence of words in the alphabet of base q digits is produced by a finite state automata or equivalently generated by a regular grammar. (See [E, HU] for detailed discussions of these notions).

Second, the asymptotics of such automatic sequences have been classified by Cobham [Co], Theorem 12, according to which, our condition of exponential growth implies the sparsest possible automatic sequences (excluding the finite ones which correspond to just rational functions).

Third, by the main result of [SYZS] (we give this as a convenient reference, but for our special case, there are earlier references given in this paper and Shallit tells me that he later found even earlier references in the computer science literature) we see that sequence with such a density is a finite union of regular expressions of the form xy^*z for strings x, y , z in the base q alphabet. Translated in our language of numbers, it means that such a sequence is union of sequences $n_i := a_j p^{id} + b_j(p^{id}-1)/(p^d-1)+c_j$ over finitely many j. (Several d's can be combined by least common multiple, by elementary manipulation).

Putting these together, we see that our examples in the last section take care of all the examples satisfying the conditions.

Next, we show that if α of the type in the last section has bounded sequence of partial quotients, then the characteristic p is two:

Let n_i be a p-automatic sequence of positive integers. By [E], chapter V, corollary 4.2, there are rational $a > 0$ and b and a power q of p such that $aq^m + b = n_{i_m}$ for all m and a subsequence i_m. Now assume that $c > n_{i+1} - 2n_i > 0$ for all i. If we fix $i = i_{m_0}$ and let l_m run through values so that $i + l_m = i_m$, then $(2^{l_m} - 1)n_i < a(q^m - q^{m_0}) < (2^{l_m} - 1)(n_i + c)$. Hence for all large enough m, we have

$$\log_2(n_i/a) < m \log_2(q) - l_m < \log_2((n_i + c)/a).$$

Now for large enough i, the two extremes of this inequality are sufficiently close, whereas if p were odd, then $\log_2(q)$ would be an irrational and the fractional part of $m \log_2(q)$ would be dense in the interval $(0, 1)$, leading to a contradiction.

Another immediate implication of this classification is that any of our examples with exponent two has bounded sequence of partial quotients.

5 Connections with deformations and more open questions

Finally, we briefly mention some other recent related results obtained in joint work with Kim and Voloch, which now involves 'university algebra' in the terminology of [A].

Following up on the initial result of Osgood mentioned above, in [KTV], we study the influence of differential equations on diophantine approximation properties. We give diophantine approximation exponent bound hierarchy corresponding to the rank hierarchy of Kodaira-Spencer map (which controls deformation theory) for some curves, such as Thue curve $P(x, y) = 1$ or curves $y^k = p(x)$, associated to α.

Roughly speaking, if α corresponds to a curve which is general, in the sense of having many deformations, then its exponent is low (approaching the Roth bound of two, assuming (as we suggest) that Vojta height inequalities hold under maximal deformation assumptions).

There are many open questions left about precise bounds and hierarchies and exponent distribution with respect to heights and degrees of α's, as well as whether there are simpler generalizations of Riccati equations generalizing Osgood's result by pushing the bound down, if you exclude their solutions.

This paper is dedicated to Professor Shreeram Abhyankar on his 70th birthday. It is the written and expanded version of the talk delivered at Purdue University in July 2000 at the 'Conference on algebra and algebraic geometry with applications' celebrating it.

References

[A] S. Abhyankar, *Historical ramblings in algebraic geometry and related algebra*, Amer. Math. Monthly 83 (1976), no. 6, 409-448.

[BS1] L. Baum and M. Sweet, *Continued fractions of algebraic power series in characteristic 2*, Ann. of Math **103** (1976), 593-610.

[BS2] L. Baum and M. Sweet, *Badly approximable power series in characteristic 2*, Ann. of Math **105** (1977), 573-580.

[C] G. Christol, *Ensembles presque-périodiques k-reconnaissables*, Theoret. Comput. Sci. **9** (1979), 141–145.

[CKMR] G. Christol, T. Kamae, M. Mendès France, G. Rauzy, *Suites algébriques, automates et substitutions*, Bull. Soc. Math. France **108** (1980), 401–419.

[Co] A. Cobham, *Uniform tag sequences*, Math. Systems Theory **6** (1972), 164–192.

[E] S. Eilenberg, *Automata, Languages and Machines*, vol. A, Academic Press, New York (1974).

[HU] J. E. Hopcroft, J. D. Ullman, *Introduction to automata theory, languages and computation*, Addison-Wesley Pub. London (1979).

[KTV] M. Kim, D. Thakur and J. F. Voloch, *Diophantine approximation and deformation*, Bull. Math. Soc. France, 128 (2000), 585-598.

[L] A. Lasjaunias, *Diophantine approximation and continued fraction expansions of algebraic power series in positive characteristic*, J. Number Theory **65** (1997), 206-225.

[LdM1] A. Lasjaunias and B. de Mathan, *Thue's theorem in positive characteristic*, J. Reine Angew. Math **473** (1996), 195-206.

[LdM2] A. Lasjaunias and B. de Mathan, *Differential equations and Diophantine approximation in positive characteristic*, Montash. Mat. **128** (1999), 1-6.

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

[M] K. Mahler, *On a theorem of Liouville in fields of positive characteristic*, Can. J. Math. **1** (1949), 397-400.

[MF] M. Mendes France, *Sur les continues fractions limitées*, Acta Arith. 23 (1973), 207-215.

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

[O1] C. Osgood, *An effective lower bound on the diophantine approximation of algebraic functions by rational functions*, Mathematika **20** (1973), 4-15.

[O2] C. Osgood, *Effective bounds on the diophantine approximation of algebraic functions over fields of arbitrary characteristic and applications to differential equations*, Indag. Math **37** (1975), 104-119.

[S1] W. Schmidt, *Diophantine approximation*, Lecture notes in Math. 785 (1980), Springer Verlag, Berlin.

[S2] W. Schmidt, *On continued fractions and diophantine approximation in power series fields*, Acta Arith. XCV.2 (2000), 139-166.

[SYZS] A. Szilard, S. Yu, K. Zhang, J. Shallit, *Characterizing regular languages with polynomial densities*, 494-503, in Mathematical Foundations of Computer Science 1992, 17th International symposium, Prague, August 1992, Lecture notes in Computer Science 629, Springer-Verlag, Berlin.

[T] D. Thakur, *Diophantine approximation exponents and continued fractions for algebraic power series*, J. Number Theory 79 (1999), 284-291.

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