On Pisot's d-th root conjecture for function fields and related GCD estimates

Julie Tzu-Yueh Wang

Academia Sinica, Taiwan

Number Theory Online Conference 2020

This is a joint work with Ji Guo and Chia-Liang Sun.

Pisot's d-th root conjecture

Conjecture (Pisot)

Let $R(X) = \sum_{n=0}^{\infty} b(n)X^n$ represent a rational function in $\mathbb{Q}(X)$. If $b(n)$ is a perfect d-th power for all large $n \in \mathbb{N}$, then one can choose a d-th root $a(n)$ of $b(n)$ such that $A(X) := \sum a(n)X^n$ is again a rational function.

Exponential Polynomials

The sequence $\{b(n)\}$ coming from the rational function $R(X)$ is a linear recurrence sequence and it can be written as an *exponential polynomial*:

An *exponential polynomial over a field k* is a sequence $b : \mathbb{N} \to k$ of the form

$$b(n) = \sum_{i=1}^{r} B_i(n)\beta_i^n,$$

where $r \in \mathbb{N}$, $\beta_i \in k^*$ and $B_i \in k[T]$.

Proving Pisot's d-th root conjecture

Theorem (Zannier 2000)

Let b be an exponential polynomial over a number field k, and $d \geq 2$ be an integer. Suppose that $b(n)$ is the d-th power of some element in k for all but finitely many n. Then there exists an exponential polynomial a over $\overline{k}$ such that $a(n)^d = b(n)$ for all n.

Function Fields

k : an algebraically closed field of characteristic 0

C: an irreducible nonsingular projective curve of genus $\mathfrak{g}$ over k

$K := \mathrm{k}(C)$: the function field of C (K is a finite extension of $\mathrm{k}(t)$)

Observation

Let $a(n)$ and $c(n)$ be exponential polynomials, and $c(n) \in \mathrm{k}$ for all $n \in \mathbb{N}$. Then $c(n)a(n)^d$, $n \in \mathbb{N}$, is still an exponential polynomial whose n-th term is the d-th power of some element in K for all $n \in \mathbb{N}$.

Pisot's d-th Root Conjecture for Function Fields

Conjecture

Let $b(n) = \sum_{i=1}^{\ell} B_i(n)\beta_i^n$ be an exponential polynomial over K. If $b(n)$ is a d-th power in K for infinitely many $n \in \mathbb{N}$, then there exists an exponential polynomial $a(n) = \sum_{i=1}^{r} A_i(n)\alpha_i^n$, $A_i \in \overline{K}[T]$ and an exponential polynomial $c(n)$ with $c(n) \in \mathrm{k}$ for all $n \in \mathbb{N}$ such that

$$b(n) = c(n)a(n)^d$$

for all $n \in \mathbb{N}$.

Pisot's d-th Root Conjecture for Function Fields

Theorem (Guo-Sun-W.)

Let $b(n) = \sum_{i=1}^{\ell} B_i(n)\beta_i^n$ *be an exponential polynomial over* K*. Let* Γ *be the multiplicative subgroup of* K^* *generated by* $\beta_1, \ldots, \beta_\ell$*. Assume that* $\Gamma \cap \mathrm{k} = \{1\}$*. If* $b(n)$ *is a* d*-th power in* K *for infinitely many* $n \in \mathbb{N}$*, then there exists an exponential polynomial* $a(m) = \sum_{i=1}^{r} A_i(m)\alpha_i^m$*,* $A_i \in \overline{K}[T]$ *and a polynomial* $Q \in \mathrm{k}[T]$ *such that*

$$b(m) = Q(m)a(m)^d$$

for all $m \in \mathbb{N}$*.*

Description of the Proof

Let $u_1, \ldots, u_n$ be a (multiplicative) basis of $\Gamma = < \beta_1, \ldots, \beta_\ell >$.

Then there exists a Laurent polynomial $f \in K[x_0, x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}]$ such that

$$b(m) = f(m, u_1^m, \ldots, u_n^m).$$

Let's assume f is a polynomial with no monomial factors. Express

$$f = QG^d \prod_{i=1}^{r} P_i^{e_i} \in K[x_0, x_1, \ldots, x_n],$$

where $Q \in \mathrm{k}[x_0]$, $G \in K[x_0, x_1, \ldots, x_n]$, and $P_1, \ldots, P_r$ are distinct irreducible non-monomial polynomials in $K[x_0, x_1, \ldots, x_n]$ but not in $\mathrm{k}[x_0]$, and $1 \leq e_i \leq d-1$.

Using GCD Estimates

Let $P := \prod_{i=1}^{r} P_i^{e_i}$. Then $P(m, u_1^m, \ldots, u_n^m)$ is a d-th power in K as long as $b(m)$ is a d-th power in K.

We will deduce from a Diophatine theorem that

$$P(m, x_1, \ldots, x_n) = Q_m(x_1, \ldots, x_n)^d, \tag{1}$$

with $Q_m \in K[x_1, \ldots, x_n]$ for m sufficiently large and such that $b(m)$ is a d-th power.

Application of Büchi's d-th Power Problem

$P \in K[x_0, x_1, \ldots, x_n] \in L[x_0]$, where $L = K(x_1, \ldots, x_n)$.

As $P(m, x_1, \ldots, x_n) = Q_m(x_1, \ldots, x_n)^d$ for infinitely many m,

$P(m)$ is a d-th power in L for infinitely many m.

Question: Is P a d-th power polynomial in $L[x_0]$?

We will use a generalized Büchi's d-th power theorem for function fields (of dimension one) repeatedly to show that P is a d-th power in $K[x_1, \ldots, x_n]$ contradicting to the assumption.

Hilbert's Tenth Problem

Is there a general algorithm to determine, given any polynomial in several variables, whether there exists a zero with all coordinates in $\mathbb{Z}$?

Ans. No, by Yu. Matiyasevich(1970)

Question (Büchi). *Does there exist an algorithm to determine, given* $m, n \in \mathbb{N}$, $a_{ij} \in \mathbb{Z}$ $(1 \leq i \leq m,\ 1 \leq j \leq n)$, $b_i \in \mathbb{Z}$ $(1 \leq i \leq m)$, *whether there exist* $x_1, ..., x_n \in \mathbb{Z}$ *satisfying the equations*

$$\sum_{j=1}^{n} a_{ij} x_j^2 = b_i, \qquad i = 1, ..., m.$$

A negative answer to this question implies Matiyasevich's result because one could take

$$P = \sum_{i=1}^{m} (\sum_{j=1}^{n} a_{ij} x_j^2 - b_i)^2.$$

Conjecture(Büchi's square problem). *There exists an integer $M > 0$ such that all $x_1, ..., x_M \in \mathbb{Z}$ satisfying the equations*

$$x_1^2 - 2x_2^2 + x_3^2 = x_2^2 - 2x_3^2 + x_4^2 = \cdots = x_{M-2}^2 - 2x_{M-1}^2 + x_M^2 = 2$$

must also satisfy

$$\pm x_1 = \pm x_2 - 1 = \cdots = \pm x_M - (M-1).$$

Negative answer to Hilbert's Tenth Problem+ truth of Büchi's square problem implies negative answer to Question (Büchi).

Büchi's square problem

The conjecture for $\mathbb{Z}$ is still open.

Vojta (2000) showed that Büchi's square problem for M sufficiently large would follow from a special case of Bombieri-Lang's conjecture on rational points on surfaces of general type.

He also proved the function field case of characteristic zero ($M \geq \max\{8, 4g+4\}$) and the case of holomorphic curves($M \geq 8$).

Büchi's square problem can be reformulated as follows.

(Büchi's square problem II). *Does there exist an integer M such that the only monic polynomials of degree two $F \in \mathbb{Z}[X]$ satisfying that $F(1), ..., F(M)$ are integer squares, are precisely of the form $F(X) = (X + c)^2$ for some $c \in \mathbb{Z}$?*

Büchi's n-th power problem over k

More generally, let k be a field.

Does there exist integer M such that the *only* monic polynomials $F \in k[X]$ of degree n satisfying that $F(1), \ldots, F(M)$ are n-th power rational numbers, are precisely of the form $F(X) = (X + c)^n$ for some $c \in k$.

Büchi's n-th power problem in zero characteristic

- Pheidas and Vidaux(2006): $n = 2$, rational functions
- Pheidas and Vidaux(2008): $n = 3$, polynomials,
- An, Huang and W. (2012): general n, function fields and meromorphic functions
- Hector Pasten (2012): number fields by assuming abc conjecture, function fields(zero characteristic)

Generalized Büchi's n-th power problem

Theorem (Pasten-W. 2015)

Let $n \geq 2$ and $M > 4n \max\{\mathfrak{g} - 1, 0\} + 11n - 3$.
Let $F \in K[x] \setminus \mathrm{k}[x]$ be a monic polynomial of degree n. Write $F = PH$ where $P \in \mathrm{k}[x]$ is monic, $H \in K[x]$ is monic and H is not divisible by any non-constant polynomial in $\mathrm{k}[x]$. Let $G_1, \ldots, G_\ell \in K[x]$ be the distinct monic irreducible factors of H and let $e_1, \ldots, e_\ell \geq 1$ be integers such that $H = \prod_{j=1}^{\ell} G_j^{e_j}$. Let $\mu \geq \max_j e_j$ be an integer and let $a_1, \ldots, a_M$ be distinct elements of k.
If for each $1 \leq i \leq M$, the zero multiplicity of $F(a_i) \in K$ at every point $\mathfrak{p} \in C$ is divisible by μ, then $\mu = e_1 = \cdots = e_\ell$ and $H = (\prod_{j=1}^{\ell} G_j)^{\mu}$.

Diophatine Equations: The First Step

Theorem (Guo-Sun-W.)

Let $d \geq 2$ be an integer and F be polynomial in $K[x_1, \ldots, x_n]$ which is not a d-th power free in $K[x_1, \ldots, x_n]$ and has no monomial factors. Let $u_1, \ldots, u_n \in \mathcal{O}_S^*$. Then there exist positive integer m and constants c_1, c_2 all depending only on d, $\deg F$ and $h(u_i)$, $1 \leq i \leq n$, such that if

$$F(u_1^\ell, \ldots, u_n^\ell) = y_\ell^d \quad \text{for some } y_\ell \in K^*$$

with $\ell \geq c_1 \tilde{h}(F) + c_2 \max\{1, 2\mathfrak{g} - 2 + |S|\}$, then $u_1^{m_1} \cdots u_n^{m_n} \in \mathrm{k}$ for some $(m_1, \ldots m_n) \in \mathbb{Z}^n \setminus \{(0, \ldots, 0)\}$ with $\sum |m_i| \leq 2m$.

Here $\tilde{h}(F)$ is the relevant height of F.

Ideas of the Proof

Let's take the example $F = x_1^2 + \cdots + x_n^2$ with $y^d = F(u_1, \ldots, u_n)$.

Take $G = 2\frac{u_1'}{u_1}x_1^2 + \ldots + 2\frac{u_n'}{u_n}x_n^2$. Then $(y^d)' = G(u_1, \ldots, u_n)$.

When $d \geq 2$, the number of common zeros of y^d and $(y^d)'$ is *usually* large as y^{d-1} is a common factor.

On the other hand, we expect the number of common zeros of $F(u_1, \ldots, u_n)$ and $G(u_1, \ldots, u_n)$ to be small unless something special happens.

What do we need?

For this example $F = x_1^2 + \cdots + x_n^2$ with $y^d = F(u_1, \ldots, u_n)$,
we take $G = 2\frac{u_1'}{u_1}x_1^2 + \ldots + 2\frac{u_n'}{u_n}x_n^2$.
Notice that $\frac{u_i'}{u_i} \notin \mathrm{k}$ if $u_i \notin \mathrm{k}$, and the number of poles (counting multiplicity) of $\frac{u_i'}{u_i}$ is bounded by the number of zeros and poles (without counting multiplicity) of u_i plus a constant related to $\mathfrak{g}$.

We need to consider GCD of two polynomials F and G in $K[x_1, \ldots, x_n]$, i.e. a moving target case.

We will take $F = P(m, x_1, \ldots, x_n)$ for infinitely m. Therefore, it is important to be able to trace the height of the coefficients.

Notation

$\mathfrak{p} \in C$

$v_{\mathfrak{p}}$: normalized valuation at $\mathfrak{p}$

S: a finite set of points in C

$\mathcal{O}_S = \{f \in K \mid v_{\mathfrak{p}}(f) \geq 0$ for all $\mathfrak{p} \notin S\}$, the ring of S-integers

$\mathcal{O}_S^* = \{f \in K \mid v_{\mathfrak{p}}(f) = 0$ for all $\mathfrak{p} \notin S\}$, the set of S-units

For $f \in K^\star$, we let

$$v_{\mathfrak{p}}^0(f) := \max\{0, v_{\mathfrak{p}}(f)\}, \qquad \text{and} \qquad v_{\mathfrak{p}}^\infty(f) := -\min\{0, v_{\mathfrak{p}}(f)\}.$$

$$h(f) := \sum_{\mathfrak{p} \in C} v_{\mathfrak{p}}^\infty(f),$$

$$N_S(f) := \sum_{\mathfrak{p} \notin S} v_{\mathfrak{p}}^0(f).$$

Notation

Let $f_0, ..., f_m \in K$ not all zeros.

$$h(\mathrm{f}) := h(f_0, ..., f_m) := \sum_{\mathfrak{p} \in C} - \min\{v_{\mathfrak{p}}(f_0), ..., v_{\mathfrak{p}}(f_m)\}.$$

For $g_1, \ldots, g_n \in K$, we let

$$\begin{aligned} & N_{S,\mathrm{gcd}}(F(g_1, \ldots, g_n), G(g_1, \ldots, g_n)) \\ & := \sum_{\mathfrak{p} \notin S} \min\{v_{\mathfrak{p}}^0(F(g_1, \ldots, g_n)), v_{\mathfrak{p}}^0(G(g_1, \ldots, g_n))\}, \end{aligned}$$

$$\begin{aligned} & h_{\mathrm{gcd}}(F(g_1, \ldots, g_n), G(g_1, \ldots, g_n)) \\ & := \sum_{\mathfrak{p} \in C} \min\{v_{\mathfrak{p}}^0(F(g_1, \ldots, g_n)), v_{\mathfrak{p}}^0(G(g_1, \ldots, g_n))\}. \end{aligned}$$

Theorem (Guo-Sun-W.)

Let F, $G \in K[x_1, \ldots, x_n]$ be nonconstant coprime polynomials. For any $\epsilon > 0$, there exist an integer m, positive constants c_i, $0 \le i \le 4$, all depending only on ϵ, such that for all n-tuple $(g_1, \ldots, g_n) \in (\mathcal{O}_S^*)^n$ either

$$h(g_1^{m_1} \cdots g_n^{m_n}) \le c_1(\tilde{h}(F) + \tilde{h}(G)) + c_2 \max\{0, 2\mathfrak{g} - 2 + |S|\}$$

for some integers $m_1, \ldots, m_n$, not all zeros with $\sum |m_i| \le 2m$, or the following two statements holds

(i) $N_{S,\mathrm{gcd}}(F(g_1, \ldots, g_n), G(g_1, \ldots, g_n)) \le \epsilon \max_{1 \le i \le n} h(g_i)$;

(ii) $h_{\mathrm{gcd}}(F(g_1, \ldots, g_n), G(g_1, \ldots, g_n)) \le \epsilon \max_{1 \le i \le n} h(g_i)$, *if we further assume that not both of F and G vanish at $(0, \ldots, 0)$,*

if

$$\max_{1 \le i \le n} h(g_i) \ge c_3(\tilde{h}(F) + \tilde{h}(G)) + c_4 \max\{1, 2\mathfrak{g} - 2 + |S|\}.$$

Description of the proof

The methods in Levin's 2019 GCD theorem for number fields and the complex case of Levin-W. in 2020.

An effective second main theorem with moving targets for function fields.

The theorem implies the following.

Theorem (Corvaja-Zannier 2005)

Let F, $G \in \mathrm{k}[x_1, x_2]$ be nonconstant coprime polynomials. For any $\epsilon > 0$, there exist an integer m, constant c, both depending only on ϵ, such that for all pairs $(g_1, g_2) \in (\mathcal{O}_S^*)^2$ with $\max\{h(g_1), h(g_2)\} \geq c \max\{1, 2\mathfrak{g} - 2 + |S|\}$, *either $g_1^{m_1} g_2^{m_2} \in \mathrm{k}$ for some integers m_1, m_2, not all zeros with $|m_1| + |m_2| \leq 2m$, or the following two statements holds*

(i) $N_{S,\mathrm{gcd}}(F(g_1, g_2), G(g_1, g_2)) \leq \epsilon \max\{h(g_1), h(g_2)\}$;

(ii) $h_{\mathrm{gcd}}(F(g_1, g_2), G(g_1, g_2)) \leq \epsilon \max\{h(g_1), h(g_2)\}$, *if we further assume that not both of F and G vanish at $(0, 0)$.*

Asymptotic GCD bounds

Theorem (Guo-Sun-W.)

Let F, $G \in K[x_1, \ldots, x_n]$ be nonconstant coprime polynomials. Let $g_1, \ldots, g_n \in K^*$, not all constant. Then for any $\epsilon > 0$, there exist an integer m and constant c_1 and c_2 depending only on ϵ, such that for

$$\ell > c_1(\tilde{h}(F) + \tilde{h}(G)) + c_2(\mathfrak{g} + n \max_{1 \le i \le n} \{h(g_i)\}),$$

either $g_1^{m_1} \cdots g_n^{m_n} \in \mathrm{k}$ for some integers $m_1, \ldots, m_n$, not all zeros with $\sum |m_i| \le 2m$, or the following two statements holds.

(i) $N_{S,\mathrm{gcd}}(F(g_1^\ell, \ldots, g_n^\ell), G(g_1^\ell, \ldots, g_n^\ell)) \le \epsilon \max_{1 \le i \le n} h(g_i^\ell)$;

(ii) $h_{\mathrm{gcd}}(F(g_1^\ell, \ldots, g_n^\ell), G(g_1^\ell, \ldots, g_n^\ell)) \le \epsilon \max_{1 \le i \le n} h(g_i^\ell)$, *if we further assume that not both of F and G vanish at $(0, \ldots, 0)$.*

Remarks

When $F,\ G \in \mathbb{C}[x_1, \ldots, x_n]$ be coprime polynomials and $g_1, \ldots, g_n \in \mathbb{C}[z]$ are multiplicatively independent modulo $\mathbb{C}$, then the results in [Levin-W.] also imply the gcd inequalities (i) and (ii). Our statement here is stronger since we have formulated effective bounds on ℓ and the m_i such that $g_1^{m_1} \cdots g_n^{m_n} \in \mathbb{C}$.

When $n > 2$, the only other previous result in this direction appears to be a result of Ostafe in 2016, which considers special polynomials such as $F = x_1 \cdots x_r - 1, G = x_{r+1} \cdots x_n - 1$, but proves a stronger uniform bound independent of ℓ. In the $n = 2$ case, previous results include the original theorem of Ailon-Rudnick (2004) in this setting, i.e. $F = x_1 - 1$, $G = x_2 - 1$, and extensions of Ostafe (both with uniform bounds).