Effective results for Diophantine equations over finitely generated domains

Jan-Hendrik Evertse

Universiteit Leiden

Joint work with Kálmán Győry

DAYS OF TRANSCENDENCE

On-line conference in honour of Yuri Nesterenko's 75th birthday

February 1, 2022

Slides have been posted on
https://pub.math.leidenuniv.nl/∼evertsejh/lectures.shtml

Finitely generated domains

We consider Diophantine equations with solutions taken from a finitely generated domain A of characteristic 0, i.e.,

$$A = \mathbb{Z}[z_1, \ldots, z_r] = \{f(z_1, \ldots, z_r) : f \in \mathbb{Z}[Z_1, \ldots, Z_r]\} \supset \mathbb{Z}.$$

Here the z_i may be algebraic or transcendental over $\mathbb{Q}$.

Finitely generated domains

We consider Diophantine equations with solutions taken from a finitely generated domain A of characteristic 0, i.e.,

$$A = \mathbb{Z}[z_1, \ldots, z_r] = \{f(z_1, \ldots, z_r) : f \in \mathbb{Z}[Z_1, \ldots, Z_r]\} \supset \mathbb{Z}.$$

Here the z_i may be algebraic or transcendental over $\mathbb{Q}$.

Examples for finitely generated domains of char. 0:

- O_K (ring of integers of a number field K);
- $O_{K,S} = O_K[(\mathfrak{p}_1 \cdots \mathfrak{p}_t)^{-1}]$ (ring of S-integers), where $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ is a set of prime ideals of O_K;
- $\mathbb{Z}[Z_1, \ldots, Z_r]$ (polynomial ring in the variables $Z_1, \ldots, Z_r$);
- $\mathbb{Z}[Z_1, \ldots, Z_r]/\mathcal{I}$, $\mathcal{I}$ prime ideal of $\mathbb{Z}[Z_1, \ldots, Z_r]$ with $\mathcal{I} \cap \mathbb{Z} = (0)$.

Finitely generated domains

We consider Diophantine equations with solutions taken from a finitely generated domain A of characteristic 0, i.e.,

$$A = \mathbb{Z}[z_1, \ldots, z_r] = \{f(z_1, \ldots, z_r) : f \in \mathbb{Z}[Z_1, \ldots, Z_r]\} \supset \mathbb{Z}.$$

Here the z_i may be algebraic or transcendental over $\mathbb{Q}$.

Examples for finitely generated domains of char. 0:

- O_K (ring of integers of a number field K);
- $O_{K,S} = O_K[(\mathfrak{p}_1 \cdots \mathfrak{p}_t)^{-1}]$ (ring of S-integers), where $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ is a set of prime ideals of O_K;
- $\mathbb{Z}[Z_1, \ldots, Z_r]$ (polynomial ring in the variables $Z_1, \ldots, Z_r$);
- $\mathbb{Z}[Z_1, \ldots, Z_r]/\mathcal{I}$, $\mathcal{I}$ prime ideal of $\mathbb{Z}[Z_1, \ldots, Z_r]$ with $\mathcal{I} \cap \mathbb{Z} = (0)$.

Aim. To give effective upper bounds for the sizes (analogues of heights) of the solutions of Diophantine equations over an arbitrary finitely generated domain A.

With such bounds we can in principle find all solutions.

Representation of a finitely generated domain

Let $A = \mathbb{Z}[z_1, \ldots, z_r]$ be a finitely generated domain of characteristic 0.

Define the ideal $\mathcal{I} := \{f \in \mathbb{Z}[Z_1, \ldots, Z_r] : f(z_1, \ldots, z_r) = 0\}$.

By Hilbert's basis theorem, there are $f_1, \ldots, f_M \in \mathbb{Z}[Z_1, \ldots, Z_r]$ such that $\mathcal{I} = (f_1, \ldots, f_M)$. Thus,

$$A \cong \mathbb{Z}[Z_1, \ldots, Z_r]/(f_1, \ldots, f_M), \quad z_i \mapsto Z_i \bmod (f_1, \ldots, f_M)$$

We use $\{f_1, \ldots, f_M\}$ to represent A.

For A to be a domain of characteristic 0,
$\mathcal{I} = (f_1, \ldots, f_M)$ has to be a prime ideal of $\mathbb{Z}[Z_1, \ldots, Z_r]$ with
$\mathcal{I} \cap \mathbb{Z} = (0)$.

There are methods to check this, given $f_1, \ldots, f_M$.

Representatives for elements, sizes

Let $A = \mathbb{Z}[z_1, \ldots, z_r] \cong \mathbb{Z}[Z_1, \ldots, Z_r]/\mathcal{I}$, with $\mathcal{I} = (f_1, \ldots, f_M)$ be a finitely generated domain of characteristic 0.

We call $\widetilde{\alpha} \in \mathbb{Z}[Z_1, \ldots, Z_r]$ a *representative* for $\alpha \in A$ if $\alpha = \widetilde{\alpha}(z_1, \ldots, z_r)$, i.e., if α corresponds to the residue class $\widetilde{\alpha}$ mod $\mathcal{I}$.

Representatives for elements, sizes

Let $A = \mathbb{Z}[z_1, \dots, z_r] \cong \mathbb{Z}[Z_1, \dots, Z_r]/\mathcal{I}$, with $\mathcal{I} = (f_1, \dots, f_M)$ be a finitely generated domain of characteristic 0.

We call $\widetilde{\alpha} \in \mathbb{Z}[Z_1, \dots, Z_r]$ a *representative* for $\alpha \in A$ if $\alpha = \widetilde{\alpha}(z_1, \dots, z_r)$, i.e., if α corresponds to the residue class $\widetilde{\alpha}$ mod $\mathcal{I}$.

For $f \in \mathbb{Z}[Z_1, \dots, Z_r]$, we define

$$\begin{aligned} \deg f &:= \textit{total degree of } f, \\ h(f) &:= \textit{logarithmic height of } f \quad (\log \max |\text{coeff. of } f|), \\ s(f) &:= \textit{size of } f \ := \max(1, \deg f, h(f)). \end{aligned}$$

Representatives for elements, sizes

Let $A = \mathbb{Z}[z_1, \ldots, z_r] \cong \mathbb{Z}[Z_1, \ldots, Z_r]/\mathcal{I}$, with $\mathcal{I} = (f_1, \ldots, f_M)$ be a finitely generated domain of characteristic 0.

We call $\widetilde{\alpha} \in \mathbb{Z}[Z_1, \ldots, Z_r]$ a *representative* for $\alpha \in A$ if $\alpha = \widetilde{\alpha}(z_1, \ldots, z_r)$, i.e., if α corresponds to the residue class $\widetilde{\alpha}$ mod $\mathcal{I}$.

For $f \in \mathbb{Z}[Z_1, \ldots, Z_r]$, we define

$$\begin{aligned} \deg f &:= \textit{total degree} \text{ of } f, \\ h(f) &:= \textit{logarithmic height} \text{ of } f \quad (\log \max |\text{coeff. of } f|), \\ s(f) &:= \textit{size} \text{ of } f \ := \max(1, \deg f, h(f)). \end{aligned}$$

Subsequently, we define the size of $\alpha \in A$ by

$$s(\alpha) := \inf\{s(\widetilde{\alpha}) : \widetilde{\alpha} \text{ representative for } \alpha\}.$$

Unit equations over finitely generated domains

Let $A = \mathbb{Z}[z_1, \dots, z_r] \cong \mathbb{Z}[Z_1, \dots, Z_r]/\mathcal{I}$, with $\mathcal{I} = (f_1, \dots, f_M)$ be a finitely generated domain of characteristic 0.

Let $a, b, c \in A \setminus \{0\}$ and consider the unit equation

(U) $\quad ax + by = c \;$ in $x, y \in A^*$ (unit group of A).

Unit equations over finitely generated domains

Let $A = \mathbb{Z}[z_1, \ldots, z_r] \cong \mathbb{Z}[Z_1, \ldots, Z_r]/\mathcal{I}$, with $\mathcal{I} = (f_1, \ldots, f_M)$ be a finitely generated domain of characteristic 0.

Let $a, b, c \in A \setminus \{0\}$ and consider the unit equation

(U) $\qquad ax + by = c$ in $x, y \in A^*$ (unit group of A).

Theorem 1 (Ev., Győry, 2013)

Let $\widetilde{a}, \widetilde{b}, \widetilde{c} \in \mathbb{Z}[Z_1, \ldots, Z_r]$ be representatives for a, b, c. Assume that $f_1, \ldots, f_M, \widetilde{a}, \widetilde{b}, \widetilde{c}$ have total degrees at most $d \geq 1$ and logarithmic heights at most $h \geq 1$.

Then for all solutions $x, y \in A^*$ of (U) we have

$$s(x), s(y) \leq \exp\left((2d)^{\kappa^r} h\right),$$

where κ is an effectively computable absolute constant > 1.

Recall $s(x) = \inf\{s(\widetilde{x}) : \widetilde{x}$ repr. for $x\}$, $s(\widetilde{x}) = \max(1, \deg \widetilde{x}, h(\widetilde{x}))$, $\widetilde{x}$ is a repr. for x if $\widetilde{x} \in \mathbb{Z}[Z_1, \ldots, Z_r]$ and $x = \widetilde{x}(z_1, \ldots, z_r)$.

Outline of the proof

Consider the equation (U) $ax + by = c$ in $x, y \in A^*$.
Let K be the quotient field of A.

(1) View (U) as S-unit equation over the function field K and compute an upper bound for the function field heights of x, y (using Mason's abc-theorem over function fields).

(2) A specialization, i.e., ring homomorphism $\varphi: A \to \overline{\mathbb{Q}}$, maps A^* to a group of S-units in some number field and thus (U) to an S-unit equation $\varphi(a)\varphi(x) + \varphi(b)\varphi(y) = \varphi(c)$.

Compute for various φ upper bounds for the number field heights of $\varphi(x)$, $\varphi(y)$ (using lower bounds for linear forms in ordinary, resp. p-adic logs, e.g., Győry, Yu, 2006).

(3) Estimate $s(x), s(y)$ in terms of the bounds found in (1) and (2).

Decomposable form equations

Let A be a f.g. domain of char. 0, K the quotient field of A and $\overline{K}$ an algebraic closure of K.

We consider so-called decomposable form equations

$$\text{(DF)} \qquad F(\mathrm{x}) = \delta \ \text{ in } \mathrm{x} = (x_1, \ldots, x_m) \in A^m,$$

where $\delta \in A \setminus \{0\}$ and where $F \in A[X_1, \ldots, X_m]$ is a decomposable form, that is, we can express F as a product of linear forms

$$F = \ell_1 \cdots \ell_n, \quad \ell_i = \sum_{j=1}^{m} \alpha_{i,j} X_j \ \text{ with } \alpha_{i,j} \in \overline{K}.$$

Decomposable form equations

Let A be a f.g. domain of char. 0, K the quotient field of A and $\overline{K}$ an algebraic closure of K.

We consider so-called decomposable form equations

$$\text{(DF)} \qquad F(\mathrm{x}) = \delta \ \text{ in } \mathrm{x} = (x_1, \dots, x_m) \in A^m,$$

where $\delta \in A \setminus \{0\}$ and where $F \in A[X_1, \dots, X_m]$ is a decomposable form, that is, we can express F as a product of linear forms

$$F = \ell_1 \cdots \ell_n, \quad \ell_i = \sum_{j=1}^{m} \alpha_{i,j} X_j \ \text{ with } \alpha_{i,j} \in \overline{K}.$$

Every binary form is decomposable. So Thue equations are decomposable form equations in two unknowns.

Decomposable form equations

Let A be a f.g. domain of char. 0, K the quotient field of A and $\overline{K}$ an algebraic closure of K.

We consider so-called decomposable form equations

$$\text{(DF)} \qquad F(\mathrm{x}) = \delta \ \text{ in } \mathrm{x} = (x_1, \ldots, x_m) \in A^m,$$

where $\delta \in A \setminus \{0\}$ and where $F \in A[X_1, \ldots, X_m]$ is a decomposable form, that is, we can express F as a product of linear forms

$$F = \ell_1 \cdots \ell_n, \quad \ell_i = \sum_{j=1}^{m} \alpha_{i,j} X_j \ \text{ with } \alpha_{i,j} \in \overline{K}.$$

Every binary form is decomposable. So Thue equations are decomposable form equations in two unknowns.

There are general finiteness theorems for (DF) (Ev., Győry, 1985, 2015) but these depend on Schmidt's Subspace Theorem, hence are *ineffective*. To get effective theorems one needs to impose stronger conditions on F.

Triangularly connected decomposable forms

Győry and Papp (1978) and Győry (1981, 1984) introduced the notion of *triangularly connected* decomposable forms, for which one can prove effective finiteness results for the corresponding decomposable form equations.

Let K be any field of characteristic 0 and $\overline{K}$ an algebraic closure of K. Consider a decomposable form

$$F = \ell_1 \cdots \ell_n \in K[X_1, \ldots, X_m], \quad \ell_i = \sum_{j=1}^{m} \alpha_{i,j} X_j \text{ with } \alpha_{i,j} \in \overline{K}.$$

Define a graph $\mathcal{G}$ with set of vertices $\{1, \ldots, n\}$ and with edges $\{p, q\}$ as follows:
$\{p, q\}$ is an edge of $\mathcal{G}$ if ℓ_p, ℓ_q are linearly dependent over $\overline{K}$ or if there is $k \notin \{p, q\}$ such that ℓ_p, ℓ_q, ℓ_k are linearly dependent over $\overline{K}$.

Then F is said to be triangularly connected if the graph $\mathcal{G}$ is connected.

Triangularly connected decomposable forms

Győry (1980/81) considered decomposable form equations

(DF) $$F(\mathrm{x}) = \delta \ \text{ in } \mathrm{x} = (x_1, \ldots, x_m) \in O_{K,S}^m$$

where $O_{K,S}$ is the ring of S-integers in a number field K.

Under the assumptions that F is a triangularly connected decomposable form and that the set of linear factors of F has rank m (to prevent easy constructions of infinitely many solutions), he gave an effective upper bound for the number field heights $h(x_1), \ldots, h(x_m)$.

Győry's proof was to reduce (DF) to a system of S'-unit equations in two unknowns in a finite extension K' of K and to apply an effective result for the latter.

We generalized his proof from $O_{K,S}$ to arbitrary finitely generated domains A of characteristic 0. For this, we needed some new machinery.

An effective result for decomposable form equations

Let $A \cong \mathbb{Z}[Z_1, \ldots, Z_r]/(f_1, \ldots, f_M)$ be a f.g. domain of characteristic 0, K the quotient field of A and $\overline{K}$ an algebraic closure of K.

Let $F \in A[X_1, \ldots, X_m]$ be a decomposable form of degree n (product of n linear forms with coeff. in $\overline{K}$) and $\delta \in A \setminus \{0\}$ and consider

(DF) $$F(\mathrm{x}) = \delta \quad \text{in } \mathrm{x} = (x_1, \ldots, x_m) \in A^m.$$

An effective result for decomposable form equations

Let $A \cong \mathbb{Z}[Z_1, \ldots, Z_r]/(f_1, \ldots, f_M)$ be a f.g. domain of characteristic 0, K the quotient field of A and $\overline{K}$ an algebraic closure of K.

Let $F \in A[X_1, \ldots, X_m]$ be a decomposable form of degree n (product of n linear forms with coeff. in $\overline{K}$) and $\delta \in A \setminus \{0\}$ and consider

(DF) $$F(\mathrm{x}) = \delta \quad \text{in } \mathrm{x} = (x_1, \ldots, x_m) \in A^m.$$

Theorem 2 (Ev., Győry, hopefully 2022)

Suppose that F is triangularly connected and the linear factors of F have rank m over $\overline{K}$ (effectively decidable),

An effective result for decomposable form equations

Let $A \cong \mathbb{Z}[Z_1, \ldots, Z_r]/(f_1, \ldots, f_M)$ be a f.g. domain of characteristic 0, K the quotient field of A and $\overline{K}$ an algebraic closure of K.

Let $F \in A[X_1, \ldots, X_m]$ be a decomposable form of degree n (product of n linear forms with coeff. in $\overline{K}$) and $\delta \in A \setminus \{0\}$ and consider

(DF) $$F(\mathrm{x}) = \delta \ \text{ in } \mathrm{x} = (x_1, \ldots, x_m) \in A^m.$$

Theorem 2 (Ev., Győry, hopefully 2022)

Suppose that F is triangularly connected and the linear factors of F have rank m over $\overline{K}$ (effectively decidable),

let $f_1, \ldots, f_M$ have total degree at most d and logarithmic height at most h, where $d \geq 1$, $h \geq 1$,

suppose δ and the coefficients of F have representatives of total degree at most d and logarithmic height at most h.

An effective result for decomposable form equations

Let $A \cong \mathbb{Z}[Z_1, \dots, Z_r]/(f_1, \dots, f_M)$ be a f.g. domain of characteristic 0, K the quotient field of A and $\overline{K}$ an algebraic closure of K.

Let $F \in A[X_1, \dots, X_m]$ be a decomposable form of degree n (product of n linear forms with coeff. in $\overline{K}$) and $\delta \in A \setminus \{0\}$ and consider

(DF) $$F(\mathrm{x}) = \delta \text{ in } \mathrm{x} = (x_1, \dots, x_m) \in A^m.$$

Theorem 2 (Ev., Győry, hopefully 2022)

Suppose that F is triangularly connected and the linear factors of F have rank m over $\overline{K}$ (effectively decidable),

let $f_1, \dots, f_M$ have total degree at most d and logarithmic height at most h, where $d \geq 1$, $h \geq 1$,

suppose δ and the coefficients of F have representatives of total degree at most d and logarithmic height at most h.

Then for every solution $\mathrm{x} = (x_1, \dots, x_m) \in A^m$ of (DF) we have

$$s(x_1), \dots, s(x_m) \leq \exp\left((n^{mn^2} d)^{\kappa^r} h\right)$$

where κ is an effectively computable absolute constant > 1.

Applications

Let A be a f.g. domain of char. 0. We give some equations for which we can deduce effective upper bounds for the sizes of the solutions:

Applications

Let A be a f.g. domain of char. 0. We give some equations for which we can deduce effective upper bounds for the sizes of the solutions:

1. Thue equations $F(x, y) = \delta$ in $x, y \in A$.

Here $\delta \in A \setminus \{0\}$ and $F \in A[X, Y]$ is a binary form of degree $n \geq 3$ and non-zero discriminant. So F is a triangularly connected dec. form.

Applications

Let A be a f.g. domain of char. 0. We give some equations for which we can deduce effective upper bounds for the sizes of the solutions:

1. Thue equations $F(x, y) = \delta$ in $x, y \in A$.

Here $\delta \in A \setminus \{0\}$ and $F \in A[X, Y]$ is a binary form of degree $n \geq 3$ and non-zero discriminant. So F is a triangularly connected dec. form.

2. Double Pell equations $x^2 - b_1 y^2 = c_1$, $x^2 - b_2 z^2 = c_2$ in $x, y, z \in A$.

Here $b_1, b_2, c_1, c_2 \in A \setminus \{0\}$, $c_1 \neq c_2$.

Apply Thm. 2 to the triangularly connected dec. form equation
$F(x, y, z) = (x^2 - b_1 y^2)(x^2 - b_2 z^2)(b_1 y^2 - b_2 z^2) = c_1 c_2 (c_2 - c_1)$.

Applications

Let A be a f.g. domain of char. 0. We give some equations for which we can deduce effective upper bounds for the sizes of the solutions:

1. Thue equations $F(x, y) = \delta$ in $x, y \in A$.

Here $\delta \in A \setminus \{0\}$ and $F \in A[X, Y]$ is a binary form of degree $n \geq 3$ and non-zero discriminant. So F is a triangularly connected dec. form.

2. Double Pell equations $x^2 - b_1 y^2 = c_1$, $x^2 - b_2 z^2 = c_2$ in $x, y, z \in A$.

Here $b_1, b_2, c_1, c_2 \in A \setminus \{0\}$, $c_1 \neq c_2$.

Apply Thm. 2 to the triangularly connected dec. form equation
$F(x, y, z) = (x^2 - b_1 y^2)(x^2 - b_2 z^2)(b_1 y^2 - b_2 z^2) = c_1 c_2 (c_2 - c_1)$.

3. Discriminant form equation

$$D(\mathrm{x}) = (x_1 \cdots x_m)^2 \cdot \prod_{1 \leq i < j \leq m} (x_i - x_j)^2 = \delta \text{ in } \mathrm{x} = (x_1, \ldots, x_m) \in A^m.$$

Here $\delta \in A \setminus \{0\}$. Recall that $D(\mathrm{x})$ is the discriminant of $X(X - x_1) \cdots (X - x_m)$. Note that D is triangularly connected.

Proof of Theorem 2: reduction to unit equations

Let A be a f.g. domain of char. 0, K the quotient field of A and $\overline{K}$ an algebraic closure of K. Consider the dec. form equation

(DF) $$F(\mathbf{x}) = \ell_1(\mathbf{x}) \cdots \ell_n(\mathbf{x}) = \delta \quad \text{in } \mathbf{x} = (x_1, \dots, x_m) \in A^m$$

where $F \in A[X_1, \dots, X_m]$, and the ℓ_i are the linear factors of F, with coefficients in $\overline{K}$.

Suppose that F is triangularly connected and $\ell_1, \dots, \ell_n$ have rank m.

Then there are many relations $\lambda_k \ell_k = \lambda_p \ell_p + \lambda_q \ell_q$ between the linear forms, arising from the edges of the associated graph $\mathcal{G}$.

Proof of Theorem 2: reduction to unit equations

Let A be a f.g. domain of char. 0, K the quotient field of A and $\overline{K}$ an algebraic closure of K. Consider the dec. form equation

$$\text{(DF)} \qquad F(\mathrm{x}) = \ell_1(\mathrm{x}) \cdots \ell_n(\mathrm{x}) = \delta \ \text{ in } \mathrm{x} = (x_1, \ldots, x_m) \in A^m$$

where $F \in A[X_1, \ldots, X_m]$, and the ℓ_i are the linear factors of F, with coefficients in $\overline{K}$.

Suppose that F is triangularly connected and $\ell_1, \ldots, \ell_n$ have rank m.

Then there are many relations $\lambda_k \ell_k = \lambda_p \ell_p + \lambda_q \ell_q$ between the linear forms, arising from the edges of the associated graph $\mathcal{G}$.

Let A' be the domain obtained by adjoining δ^{-1} and the coefficients of the ℓ_i to A. Then for every solution $\mathrm{x} \in A^m$ of (DF),

$$\lambda_p \cdot \frac{\ell_p(\mathrm{x})}{\ell_k(\mathrm{x})} + \lambda_q \cdot \frac{\ell_q(\mathrm{x})}{\ell_k(\mathrm{x})} = \lambda_k, \quad \frac{\ell_p(\mathrm{x})}{\ell_k(\mathrm{x})}, \ \frac{\ell_q(\mathrm{x})}{\ell_k(\mathrm{x})} \in A'^*.$$

Now apply Theorem 1 on unit equations, with A' instead of A.

Proof of Theorem 2: reduction to unit equations

Let A be a f.g. domain of char. 0, K the quotient field of A and $\overline{K}$ an algebraic closure of K. Consider the dec. form equation

$$\text{(DF)} \qquad F(\mathrm{x}) = \ell_1(\mathrm{x}) \cdots \ell_n(\mathrm{x}) = \delta \ \text{ in } \mathrm{x} = (x_1, \ldots, x_m) \in A^m$$

where $F \in A[X_1, \ldots, X_m]$, and the ℓ_i are the linear factors of F, with coefficients in $\overline{K}$.

Suppose that F is triangularly connected and $\ell_1, \ldots, \ell_n$ have rank m.

Then there are many relations $\lambda_k \ell_k = \lambda_p \ell_p + \lambda_q \ell_q$ between the linear forms, arising from the edges of the associated graph $\mathcal{G}$.

Let A' be the domain obtained by adjoining δ^{-1} and the coefficients of the ℓ_i to A. Then for every solution $\mathrm{x} \in A^m$ of (DF),

$$\lambda_p \cdot \frac{\ell_p(\mathrm{x})}{\ell_k(\mathrm{x})} + \lambda_q \cdot \frac{\ell_q(\mathrm{x})}{\ell_k(\mathrm{x})} = \lambda_k, \quad \frac{\ell_p(\mathrm{x})}{\ell_k(\mathrm{x})}, \ \frac{\ell_q(\mathrm{x})}{\ell_k(\mathrm{x})} \in A'^*.$$

Now apply Theorem 1 on unit equations, with A' instead of A.

To work this out, we have to do computations in $\overline{K}$ and for this we use suitable measures for elements of $\overline{K}$, so-called *degree-height estimates*.

Degree-height estimates

Let $A = \mathbb{Z}[z_1, \ldots, z_r] \cong \mathbb{Z}[Z_1, \ldots, Z_r]/(f_1, \ldots, f_M)$ be a f.g. domain of char. 0, K the quotient field of A and $\overline{K}$ an algebraic closure of K.

Let $\alpha \in \overline{K}$ be of degree n over K.

We can express the minimal polynomial of α over K as

$$X^n + \frac{g_1(z_1, \ldots, z_r)}{g_0(z_1, \ldots, z_r)} X^{n-1} + \cdots + \frac{g_n(z_1, \ldots, z_r)}{g_0(z_1, \ldots, z_r)}$$

where $g_0, \ldots, g_n \in \mathbb{Z}[Z_1, \ldots, Z_r]$ and $g_0 \notin (f_1, \ldots, f_M)$.

We call (d, h) a *degree-height estimate* for α if $g_0, \ldots, g_n$ can be chosen such that

$$\deg g_i \leq d, \quad h(g_i) \leq h \quad \text{for } i = 0, \ldots, n$$

(here deg denotes total degree and $h(\cdot)$ logarithmic height).

Degree-height estimates

Let $A = \mathbb{Z}[z_1, \ldots, z_r] \cong \mathbb{Z}[Z_1, \ldots, Z_r]/(f_1, \ldots, f_M)$ be a f.g. domain of char. 0, K the quotient field of A and $\overline{K}$ an algebraic closure of K.

Let $\alpha \in \overline{K}$ be of degree n over K.

We can express the minimal polynomial of α over K as

$$X^n + \frac{g_1(z_1, \ldots, z_r)}{g_0(z_1, \ldots, z_r)} X^{n-1} + \cdots + \frac{g_n(z_1, \ldots, z_r)}{g_0(z_1, \ldots, z_r)}$$

where $g_0, \ldots, g_n \in \mathbb{Z}[Z_1, \ldots, Z_r]$ and $g_0 \notin (f_1, \ldots, f_M)$.

We call (d, h) a *degree-height estimate* for α if $g_0, \ldots, g_n$ can be chosen such that

$$\deg g_i \leq d, \quad h(g_i) \leq h \text{ for } i = 0, \ldots, n$$

(here deg denotes total degree and $h(\cdot)$ logarithmic height).

Main tool. Given $\alpha_1, \ldots, \alpha_m \in \overline{K}$ and $\beta \in \overline{K}$ satisfying $P(\alpha_1, \ldots, \alpha_m, \beta) = 0$ for some $P \in \mathbb{Z}[X_1, \ldots, X_m, Y]$, we want a degree-height estimate for $\beta \in \overline{K}$ in terms of degree-height estimates for $\alpha_1, \ldots, \alpha_m \in \overline{K}$.

A result for degree-height estimates

Let $A = \mathbb{Z}[z_1, \ldots, z_r] \cong \mathbb{Z}[Z_1, \ldots, Z_r]/(f_1, \ldots, f_M)$ be a f.g. domain of char. 0, K the quotient field of A and $\overline{K}$ an algebraic closure of K.

Theorem 3 (Ev., Győry, 2022 (?))

Suppose $f_1, \ldots, f_M$ have total degree $\leq d$ and log. height $\leq h$, where $d \geq 1$, $h \geq 1$.

Let $\alpha_1, \ldots, \alpha_m \in \overline{K}$ be such that $[K(\alpha_i) : K] = n_i$, and α_i has degree-height estimate (d, h) for $i = 1, \ldots, m$.

Let $P \in \mathbb{Z}[X_1, \ldots, X_m, Y]$ be such that $P(\alpha_1, \ldots, \alpha_m, Y)$ is of degree ≥ 1 in Y.

Let $\beta \in \overline{K}$ with $P(\alpha_1, \ldots, \alpha_m, \beta) = 0$.

A result for degree-height estimates

Let $A = \mathbb{Z}[z_1, \ldots, z_r] \cong \mathbb{Z}[Z_1, \ldots, Z_r]/(f_1, \ldots, f_M)$ be a f.g. domain of char. 0, K the quotient field of A and $\overline{K}$ an algebraic closure of K.

Theorem 3 (Ev., Győry, 2022 (?))

Suppose $f_1, \ldots, f_M$ have total degree $\leq d$ and log. height $\leq h$, where $d \geq 1$, $h \geq 1$.

Let $\alpha_1, \ldots, \alpha_m \in \overline{K}$ be such that $[K(\alpha_i) : K] = n_i$, and α_i has degree-height estimate (d, h) for $i = 1, \ldots, m$.

Let $P \in \mathbb{Z}[X_1, \ldots, X_m, Y]$ be such that $P(\alpha_1, \ldots, \alpha_m, Y)$ is of degree ≥ 1 in Y.

Let $\beta \in \overline{K}$ with $P(\alpha_1, \ldots, \alpha_m, \beta) = 0$.

Then β has degree-height estimate

$$\big(R,\ R\cdot(h(P) + h)\big), \quad \text{where } R = \big(2 \deg P \cdot m \cdot n_1 \cdots n_m \cdot d\big)^{\kappa^r},$$

with κ an effectively computable absolute constant > 1.

Open problems

- The proof of Theorem 3 is technical and clumsy.

  Is there a good alternative for the very naive degree-height estimates, with an analogue for Theorem 3 that can be proved more smoothly? (Compare naive heights and Weil heights for algebraic numbers.)

- In 2000, Moriwaki introduced height functions, based on Arakelov intersection theory, for $\overline{K}$, where K is a finitely generated field over $\mathbb{Q}$.

  Can these be compared to our degree-height estimates?

Congratulations, Yuri!