Effective methods for Diophantine equations over finitely generated domains

Jan-Hendrik Evertse
Universiteit Leiden

Joint work with Kálmán Győry

On-line Research Seminar "Diophantine Number Theory"
Schiedam, December 11, 2020

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

Finitely generated domains

We consider Diophantine equations with unknowns taken from a finitely generated domain of characteristic 0 over $\mathbb{Z}$, i.e.,

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

Finitely generated domains

We consider Diophantine equations with unknowns taken from a finitely generated domain of characteristic 0 over $\mathbb{Z}$, i.e.,

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

Example 1. O_K (ring of integers of a number field K)

$O_K = \mathbb{Z}[\omega_1, \ldots, \omega_D]$, where $\{\omega_1, \ldots, \omega_D\}$ is a $\mathbb{Z}$-module basis of O_K.

Finitely generated domains

We consider Diophantine equations with unknowns taken from a finitely generated domain of characteristic 0 over $\mathbb{Z}$, i.e.,

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

Example 1. O_K (ring of integers of a number field K)

$O_K = \mathbb{Z}[\omega_1, \ldots, \omega_D]$, where $\{\omega_1, \ldots, \omega_D\}$ is a $\mathbb{Z}$-module basis of O_K.

Example 2. $O_{K,S}$ (ring of S-integers of K, $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ is a set of prime ideals of O_K)

$O_{K,S} = O_K[(\mathfrak{p}_1 \cdots \mathfrak{p}_t)^{-1}] = \mathbb{Z}[\omega_1, \ldots, \omega_D, \pi^{-1}]$,
where $(\pi) = (\mathfrak{p}_1 \cdots \mathfrak{p}_t)^{h_K}$ with h_K the class number of K.

Finitely generated domains

We consider Diophantine equations with unknowns taken from a finitely generated domain of characteristic 0 over $\mathbb{Z}$, i.e.,

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

Example 1. O_K (ring of integers of a number field K)

$O_K = \mathbb{Z}[\omega_1, \ldots, \omega_D]$, where $\{\omega_1, \ldots, \omega_D\}$ is a $\mathbb{Z}$-module basis of O_K.

Example 2. $O_{K,S}$ (ring of S-integers of K, $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ is a set of prime ideals of O_K)

$O_{K,S} = O_K[(\mathfrak{p}_1 \cdots \mathfrak{p}_t)^{-1}] = \mathbb{Z}[\omega_1, \ldots, \omega_D, \pi^{-1}]$,
where $(\pi) = (\mathfrak{p}_1 \cdots \mathfrak{p}_t)^{h_K}$ with h_K the class number of K.

We consider the most general case where $z_1, \ldots, z_r$ may be algebraic or transcendental over $\mathbb{Q}$.

Finitely generated domains

We consider Diophantine equations with unknowns taken from a finitely generated domain of characteristic 0 over $\mathbb{Z}$, i.e.,

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

Example 1. O_K (ring of integers of a number field K)

$O_K = \mathbb{Z}[\omega_1, \ldots, \omega_D]$, where $\{\omega_1, \ldots, \omega_D\}$ is a $\mathbb{Z}$-module basis of O_K.

Example 2. $O_{K,S}$ (ring of S-integers of K, $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ is a set of prime ideals of O_K)

$O_{K,S} = O_K[(\mathfrak{p}_1 \cdots \mathfrak{p}_t)^{-1}] = \mathbb{Z}[\omega_1, \ldots, \omega_D, \pi^{-1}]$,
where $(\pi) = (\mathfrak{p}_1 \cdots \mathfrak{p}_t)^{h_K}$ with h_K the class number of K.

We consider the most general case where $z_1, \ldots, z_r$ may be algebraic or transcendental over $\mathbb{Q}$.

Aim. Effective method to solve Diophantine equations with unknowns from an arbitrary finitely generated domain of char. 0 (i.e., algorithm to find all solutions in principle, we do not care about practical solubility).

Representation of finitely generated domains

To make sense of effective methods to solve Diophantine equations over finitely generated domains, we need ways to represent such a domain and to represent elements of such a domain.

Representation of finitely generated domains

To make sense of effective methods to solve Diophantine equations over finitely generated domains, we need ways to represent such a domain and to represent elements of such a 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 call such a set $\{f_1, \ldots, f_M\}$ a *representation* of A.

Representation of finitely generated domains

To make sense of effective methods to solve Diophantine equations over finitely generated domains, we need ways to represent such a domain and to represent elements of such a 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 call such a set $\{f_1, \ldots, f_M\}$ a *representation* of A.

Fact

A is an integral domain of characteristic 0
$\iff \mathcal{I} = (f_1, \ldots, f_M)$ is 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

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

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 $\mathcal{I}$.

We perform computations in A by doing computations on representatives.

For this, we must be able to check whether $\widetilde{\alpha}, \widetilde{\alpha}' \in \mathbb{Z}[Z_1, \ldots, Z_r]$ represent the same element of A, i.e., $\widetilde{\alpha} - \widetilde{\alpha}' \in \mathcal{I}$.

Representatives for elements

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 $\mathcal{I}$.

We perform computations in A by doing computations on representatives.

For this, we must be able to check whether $\widetilde{\alpha}, \widetilde{\alpha}' \in \mathbb{Z}[Z_1, \ldots, Z_r]$ represent the same element of A, i.e., $\widetilde{\alpha} - \widetilde{\alpha}' \in \mathcal{I}$.

For this, we need an *ideal membership algorithm* for $\mathbb{Z}[Z_1, , \ldots, Z_r]$, that is, an algorithm to decide whether a given polynomial of $\mathbb{Z}[Z_1, \ldots, Z_r]$ belongs to a given ideal of $\mathbb{Z}[Z_1, \ldots, Z_r]$.

Such algorithms exist since the 1960s. The most recent one, due to Aschenbrenner (2004), was of crucial importance in our investigations.

Aschenbrenner's ideal membership algorithm

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

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

Theorem (Aschenbrenner, 2004)

Let $g, f_1, \ldots, f_M \in \mathbb{Z}[Z_1, \ldots, Z_r]$ have total degrees at most d and logarithmic heights at most h, where $d \geq 1$, $h \geq 1$.
Suppose there are $g_1, \ldots, g_r \in \mathbb{Z}[Z_1, \ldots, Z_r]$ with $g = g_1 f_1 + \cdots + g_M f_M$.
Then there are such $g_1, \ldots, g_M$ with

$$\deg g_i \leq C_1 := (4d)^{(6r)^r} h, \quad h(g_i) \leq C_2 := (4d)^{(6r)^{r+1}} h^{r+1}$$

for $i = 1, \ldots, M$.

Aschenbrenner's ideal membership algorithm

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

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

Theorem (Aschenbrenner, 2004)

Let $g, f_1, \ldots, f_M \in \mathbb{Z}[Z_1, \ldots, Z_r]$ have total degrees at most d and logarithmic heights at most h, where $d \geq 1$, $h \geq 1$.
Suppose there are $g_1, \ldots, g_r \in \mathbb{Z}[Z_1, \ldots, Z_r]$ with $g = g_1 f_1 + \cdots + g_M f_M$.
Then there are such $g_1, \ldots, g_M$ with

$$\deg g_i \leq C_1 := (4d)^{(6r)^r} h, \quad h(g_i) \leq C_2 := (4d)^{(6r)^{r+1}} h^{r+1}$$

for $i = 1, \ldots, M$.

To verify whether $g \in (f_1, \ldots, f_M)$ one simply has to check for all $g_1, \ldots, g_M \in \mathbb{Z}[Z_1, \ldots, Z_r]$ of total degrees at most C_1 and logarithmic heights at most C_2 whether $g = g_1 f_1 + \cdots + g_M f_M$.

Solving Diophantine equations over finitely generated domains

Let $A \cong \mathbb{Z}[Z_1, \ldots, Z_r]/\mathcal{I}$ with $\mathcal{I} = (f_1, \ldots, f_M)$ be a f.g. domain of char. 0.
Let $P \in A[X_1, \ldots, X_m]$ and suppose that representatives in $\mathbb{Z}[Z_1, \ldots, Z_r]$ for the coefficients of P are given.

Suppose that we know somehow that the Diophantine equation

$$(*) \qquad P(x_1, \ldots, x_m) = 0 \ \text{ in } x_1, \ldots, x_m \in A$$

has only finitely many solutions.

Effectively solving $(*)$ means producing a list, consisting of a tuple of representatives $\widetilde{x_1}, \ldots, \widetilde{x_m} \in \mathbb{Z}[Z_1, \ldots, Z_r]$ for each solution $x_1, \ldots, x_m$.

Solving Diophantine equations over finitely generated domains

Let $A \cong \mathbb{Z}[Z_1, \ldots, Z_r]/\mathcal{I}$ with $\mathcal{I} = (f_1, \ldots, f_M)$ be a f.g. domain of char. 0.
Let $P \in A[X_1, \ldots, X_m]$ and suppose that representatives in $\mathbb{Z}[Z_1, \ldots, Z_r]$ for the coefficients of P are given.

Suppose that we know somehow that the Diophantine equation

$$(*) \qquad P(x_1, \ldots, x_m) = 0 \ \text{ in } x_1, \ldots, x_m \in A$$

has only finitely many solutions.

Effectively solving $(*)$ means producing a list, consisting of a tuple of representatives $\widetilde{x_1}, \ldots, \widetilde{x_m} \in \mathbb{Z}[Z_1, \ldots, Z_r]$ for each solution $x_1, \ldots, x_m$.

Győry (1983/84) developed a method to prove effective finiteness results for various classes of Diophantine equations over finitely generated domains, but his method works only for *special domains* (defined later).

Ev. and Győry (2013) extended this to arbitrary finitely generated domains of characteristic 0, using Aschenbrenner's theorem.

Solving Diophantine equations over finitely generated domains

Definition of the size

Let $A \cong \mathbb{Z}[Z_1, \ldots, Z_r]/\mathcal{I}$ with $\mathcal{I} = (f_1, \ldots, f_M)$ be a f.g. domain of char. 0.

Define the *size* of $F \in \mathbb{Z}[Z_1, \ldots, Z_r]$ by $s(F) := \max(1, \deg F, h(F))$.

Further, define the size of $\alpha \in A$ by

$$s(\alpha) := \inf \left\{ s(\widetilde{\alpha}) : \widetilde{\alpha} \in \mathbb{Z}[Z_1, \ldots, Z_r] \text{ is a representative for } \alpha \right\}$$

Solving Diophantine equations over finitely generated domains

Definition of the size

Let $A \cong \mathbb{Z}[Z_1, \ldots, Z_r]/\mathcal{I}$ with $\mathcal{I} = (f_1, \ldots, f_M)$ be a f.g. domain of char. 0.

Define the *size* of $F \in \mathbb{Z}[Z_1, \ldots, Z_r]$ by $s(F) := \max(1, \deg F, h(F))$.

Further, define the size of $\alpha \in A$ by

$$s(\alpha) := \inf \left\{ s(\widetilde{\alpha}) : \widetilde{\alpha} \in \mathbb{Z}[Z_1, \ldots, Z_r] \text{ is a representative for } \alpha \right\}$$

Fact

Let $P \in A[X_1, \ldots, X_m]$ and let $\widetilde{P}$ be a polynomial in $X_1, \ldots, X_m$ with coefficients in $\mathbb{Z}[Z_1, \ldots, Z_r]$ representing the coefficients of P.

We can solve (*) $P(x_1, \ldots, x_m) = 0$ in $x_1, \ldots, x_m \in A$ if we can compute a bound $C = C(f_1, \ldots, f_M, \widetilde{P})$ such that $s(x_1), \ldots, s(x_m) \leq C$ for all solutions of (*).

Proof. Check for all tuples $\widetilde{x_1}, \ldots, \widetilde{x_m} \in \mathbb{Z}[Z_1, \ldots, Z_r]$ of size $\leq C$ whether $\widetilde{P}(\widetilde{x_1}, \ldots, \widetilde{x_m}) \in \mathcal{I}$ using an ideal menbership algorithm. □

General idea

The general idea to estimate the sizes of the solutions of an equation

$$(*) \qquad P(x_1, \ldots, x_m) = 0 \ \text{ in } x_1, \ldots, x_m \in A$$

is as follows:

1) Derive related equations over certain function fields and certain number fields.
2) Compute upper bounds for the heights of the solutions of the equations over function fields (e.g. using Mason's abc-theorem for algebraic functions) and for the heights of the solutions over number fields (e.g., using Baker's method).
3) Combine the estimates from 2) to derive upper bounds for the sizes of the solutions of (*), using the *effective specialization lemma* (discussed later).

First application: unit equations

Let $A \cong \mathbb{Z}[Z_1, \ldots, Z_r]/(f_1, \ldots, f_M)$ be a f.g. domain of char. 0 and let a, b, c be non-zero elements of A. Consider the *unit equation*

(U) $$ax + by = c \quad \text{in } x, y \in A^* \quad (\text{group of units of } A)$$

Győry (1979) gave explicit upper bounds for the heights of x, y in case that A is the ring of S-integers in a number field and Mason (1983) proved an analogue for function fields in one variable.

First application: unit equations

Let $A \cong \mathbb{Z}[Z_1, \ldots, Z_r]/(f_1, \ldots, f_M)$ be a f.g. domain of char. 0 and let a, b, c be non-zero elements of A. Consider the *unit equation*

$$\text{(U)} \qquad ax + by = c \quad \text{in } x, y \in A^* \quad \text{(group of units of } A\text{)}$$

Győry (1979) gave explicit upper bounds for the heights of x, y in case that A is the ring of S-integers in a number field and Mason (1983) proved an analogue for function fields in one variable.

Theorem (Ev., Győry, 2013)

Suppose that $f_1, \ldots, f_M$ and some representatives of a, b, c have total degrees $\leq d$ and logarithmic heights $\leq h$, where $d \geq 1$, $h \geq 1$.

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.

Further applications

Let $A \cong \mathbb{Z}[Z_1, \ldots, Z_r]/(f_1, \ldots, f_M)$ be a f.g. domain of char. 0.

Our method gives effective estimates for the sizes of the solutions of the following equations:

- (Bérczes, Ev., Győry, 2014) Thue equations $F(x, y) = \delta$ in $x, y \in A$ where $F \in A[X, Y]$ is a binary form and $\delta \in A \setminus \{0\}$;

Further applications

Let $A \cong \mathbb{Z}[Z_1, \ldots, Z_r]/(f_1, \ldots, f_M)$ be a f.g. domain of char. 0.

Our method gives effective estimates for the sizes of the solutions of the following equations:

- (Bérczes, Ev., Győry, 2014) Thue equations $F(x, y) = \delta$ in $x, y \in A$ where $F \in A[X, Y]$ is a binary form and $\delta \in A \setminus \{0\}$;
- (Bérczes, Ev., Győry, 2014) hyper- and superelliptic equations $y^n = f(x)$ in $x, y \in A$, Schinzel-Tijdeman equation $y^z = f(x)$ in $x, y \in A$, $z \in \mathbb{Z}_{>0}$ where $f \in A[X]$;

Further applications

Let $A \cong \mathbb{Z}[Z_1, \ldots, Z_r]/(f_1, \ldots, f_M)$ be a f.g. domain of char. 0.

Our method gives effective estimates for the sizes of the solutions of the following equations:

- (Bérczes, Ev., Győry, 2014) Thue equations $F(x, y) = \delta$ in $x, y \in A$ where $F \in A[X, Y]$ is a binary form and $\delta \in A \setminus \{0\}$;
- (Bérczes, Ev., Győry, 2014) hyper- and superelliptic equations $y^n = f(x)$ in $x, y \in A$, Schinzel-Tijdeman equation $y^z = f(x)$ in $x, y \in A$, $z \in \mathbb{Z}_{>0}$ where $f \in A[X]$;
- (Koymans, 2015) Catalan equation $x^m - y^n = 1$ in $x, y \in A$, $m, n \in \mathbb{Z}_{>0}$;

Further applications

Let $A \cong \mathbb{Z}[Z_1, \ldots, Z_r]/(f_1, \ldots, f_M)$ be a f.g. domain of char. 0.

Our method gives effective estimates for the sizes of the solutions of the following equations:

- (Bérczes, Ev., Győry, 2014) Thue equations $F(x, y) = \delta$ in $x, y \in A$ where $F \in A[X, Y]$ is a binary form and $\delta \in A \setminus \{0\}$;
- (Bérczes, Ev., Győry, 2014) hyper- and superelliptic equations $y^n = f(x)$ in $x, y \in A$, Schinzel-Tijdeman equation $y^z = f(x)$ in $x, y \in A$, $z \in \mathbb{Z}_{>0}$ where $f \in A[X]$;
- (Koymans, 2015) Catalan equation $x^m - y^n = 1$ in $x, y \in A$, $m, n \in \mathbb{Z}_{>0}$;
- (Bérczes, 2015) generalized unit equations $f(x, y) = 0$ in $x, y \in A^*$ where $f \in A[X, Y]$;

Further applications

Let $A \cong \mathbb{Z}[Z_1, \ldots, Z_r]/(f_1, \ldots, f_M)$ be a f.g. domain of char. 0.

Our method gives effective estimates for the sizes of the solutions of the following equations:

- (Bérczes, Ev., Győry, 2014) Thue equations $F(x, y) = \delta$ in $x, y \in A$ where $F \in A[X, Y]$ is a binary form and $\delta \in A \setminus \{0\}$;
- (Bérczes, Ev., Győry, 2014) hyper- and superelliptic equations $y^n = f(x)$ in $x, y \in A$, Schinzel-Tijdeman equation $y^z = f(x)$ in $x, y \in A$, $z \in \mathbb{Z}_{>0}$ where $f \in A[X]$;
- (Koymans, 2015) Catalan equation $x^m - y^n = 1$ in $x, y \in A$, $m, n \in \mathbb{Z}_{>0}$;
- (Bérczes, 2015) generalized unit equations $f(x, y) = 0$ in $x, y \in A^*$ where $f \in A[X, Y]$;
- (Ev., Győry, 202?) decomposable form equations $F(x_1, \ldots, x_m) = \delta$ in $x_1, \ldots, x_m \in A$ where $\delta \in A \setminus \{0\}$ and $F \in A[X_1, \ldots, X_m]$ is a decomposable form, i.e., it factorizes into linear forms over an algebraic extension of the quotient field of A.

Explanation of the method

As mentioned before, we can estimate the sizes of the solutions of a Diophantine equation over a finitely generated integral domain A of characteristic 0 in terms of estimates for the heights of the solutions of related equations over number fields and over function fields.

We would like to explain this in more detail.

Our method has three ingredients:

1) construction of a special domain $B \supseteq A$;

2) construction of specializations (ring homomorphisms) $B \to \overline{\mathbb{Q}}$;

3) effective specialization lemma.

Construction of a special domain $B \supset A$

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 and K its quotient field.

Suppose that $f_1, \ldots, f_M$ have total degrees at most d and logarithmic heights at most h, where $d \geq 1$, $h \geq 1$.

We assume that $z_1, \ldots, z_q$ are algebraically independent and that $z_{q+1}, \ldots, z_r$ are algebraic over $K_0 := \mathbb{Q}(z_1, \ldots, z_q)$.
Note that $[K : K_0] =: D \leq d^r$.

Construction of a special domain $B \supset A$

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 and K its quotient field.

Suppose that $f_1, \ldots, f_M$ have total degrees at most d and logarithmic heights at most h, where $d \geq 1$, $h \geq 1$.

We assume that $z_1, \ldots, z_q$ are algebraically independent and that $z_{q+1}, \ldots, z_r$ are algebraic over $K_0 := \mathbb{Q}(z_1, \ldots, z_q)$.
Note that $[K : K_0] =: D \leq d^r$.

Let $A_0 := \mathbb{Z}[z_1, \ldots, z_q]$. Then

$$A \subseteq B := A_0[\theta, g^{-1}] = \mathbb{Z}[z_1, \ldots, z_q, \theta, g^{-1}],$$

where $g \in A_0 \setminus \{0\}$, $\theta \in K$ and θ has minimal polynomial $\mathcal{F}(X) = X^D + \mathcal{F}_1 X^{D-1} + \cdots + \mathcal{F}_D \in A_0[X]$ over K_0.
Such a domain B is called *special*.

Construction of a special domain $B \supset A$

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 and K its quotient field.

Suppose that $f_1, \ldots, f_M$ have total degrees at most d and logarithmic heights at most h, where $d \geq 1$, $h \geq 1$.

We assume that $z_1, \ldots, z_q$ are algebraically independent and that $z_{q+1}, \ldots, z_r$ are algebraic over $K_0 := \mathbb{Q}(z_1, \ldots, z_q)$.
Note that $[K : K_0] =: D \leq d^r$.

Let $A_0 := \mathbb{Z}[z_1, \ldots, z_q]$. Then

$$A \subseteq B := A_0[\theta, g^{-1}] = \mathbb{Z}[z_1, \ldots, z_q, \theta, g^{-1}],$$

where $g \in A_0 \setminus \{0\}$, $\theta \in K$ and θ has minimal polynomial $\mathcal{F}(X) = X^D + \mathcal{F}_1 X^{D-1} + \cdots + \mathcal{F}_D \in A_0[X]$ over K_0.
Such a domain B is called *special*.

Viewing the $\mathcal{F}_i$ and g as polynomials in the variables $z_1, \ldots, z_q$, we can choose them such that their total degrees and logarithmic heights are effectively bounded in terms of r, d and h.

Specializations

Let $A = \mathbb{Z}[z_1, \ldots, z_r]$ be a f.g. domain of char. 0.

Let $z_1, \ldots, z_q$ be algebraically independent, $z_{q+1}, \ldots, z_r$ algebraic over $K_0 = \mathbb{Q}(z_1, \ldots, z_q)$, $A_0 = \mathbb{Z}[z_1, \ldots, z_q]$ and $A \subseteq B = A_0[\theta, g^{-1}]$, where $g \in A_0 \setminus \{0\}$ and θ has minimal polynomial $\mathcal{F}(X) = X^D + \mathcal{F}_1 X^{D-1} + \cdots + \mathcal{F}_D \in A_0[X]$ over K_0.

For $\mathrm{u} = (u_1, \ldots, u_q) \in \mathbb{Z}^q$, let $\mathcal{F}_\mathrm{u}$ be the polynomial in $\mathbb{Z}[X]$ obtained by substituting u_i for z_i $(i = 1, \ldots, q)$ in the $\mathcal{F}_j$, and let $\theta_{\mathrm{u},1}, \ldots, \theta_{\mathrm{u},D}$ be the zeros of $\mathcal{F}_\mathrm{u}$ in $\overline{\mathbb{Q}}$.

Specializations

Let $A = \mathbb{Z}[z_1, \ldots, z_r]$ be a f.g. domain of char. 0.

Let $z_1, \ldots, z_q$ be algebraically independent, $z_{q+1}, \ldots, z_r$ algebraic over $K_0 = \mathbb{Q}(z_1, \ldots, z_q)$, $A_0 = \mathbb{Z}[z_1, \ldots, z_q]$ and $A \subseteq B = A_0[\theta, g^{-1}]$, where $g \in A_0 \setminus \{0\}$ and θ has minimal polynomial $\mathcal{F}(X) = X^D + \mathcal{F}_1 X^{D-1} + \cdots + \mathcal{F}_D \in A_0[X]$ over K_0.

For $\mathsf{u} = (u_1, \ldots, u_q) \in \mathbb{Z}^q$, let $\mathcal{F}_\mathsf{u}$ be the polynomial in $\mathbb{Z}[X]$ obtained by substituting u_i for z_i $(i = 1, \ldots, q)$ in the $\mathcal{F}_j$, and let $\theta_{\mathsf{u},1}, \ldots, \theta_{\mathsf{u},D}$ be the zeros of $\mathcal{F}_\mathsf{u}$ in $\overline{\mathbb{Q}}$.

Now for $\mathsf{u} \in \mathbb{Z}^q$ with $g(\mathsf{u}) \neq 0$ and $j = 1, \ldots, D$, we can define a ring homomorphism $\varphi_{\mathsf{u},j} : B \to \overline{\mathbb{Q}}$ by

$$z_1 \mapsto u_1, \ldots, z_q \mapsto u_q, \theta \mapsto \theta_{\mathsf{u},j}.$$

$\varphi_{\mathsf{u},j}(B)$ is contained in the ring of S-integers of a number field, where S and the number field depend on u and j.

Hence also $\varphi_{\mathsf{u},j}(A)$ is contained in this ring of S-integers.

Effective specialization lemma

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 and K its quotient field.

Suppose that $f_1, \ldots, f_M$ have total degrees at most d and logarithmic heights at most h, where $d \geq 1$, $h \geq 1$.

Let $z_1, \ldots, z_q$ be alg. ind., $z_{q+1}, \ldots, z_r$ alg. over $K_0 = \mathbb{Q}(z_1, \ldots, z_q)$.

Let $\Bbbk_i = \overline{\mathbb{Q}(z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_q)}$, $L_i := \Bbbk_i K$.
Then L_i is a finite extension of $\Bbbk_i(z_i)$ and thus a function field in one variable over $\Bbbk_i$.

Effective specialization lemma

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 and K its quotient field.

Suppose that $f_1, \ldots, f_M$ have total degrees at most d and logarithmic heights at most h, where $d \geq 1$, $h \geq 1$.

Let $z_1, \ldots, z_q$ be alg. ind., $z_{q+1}, \ldots, z_r$ alg. over $K_0 = \mathbb{Q}(z_1, \ldots, z_q)$.

Let $\Bbbk_i = \overline{\mathbb{Q}(z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_q)}$, $L_i := \Bbbk_i K$.
Then L_i is a finite extension of $\Bbbk_i(z_i)$ and thus a function field in one variable over $\Bbbk_i$. Further, let

H_{L_i} the function field height on L_i (0 on $\Bbbk_i^*$),
$h_{\overline{\mathbb{Q}}}$ the absolute logarithmic Weil height on $\overline{\mathbb{Q}}$,
$s(\alpha) := \inf\{\max\left(1, \deg \widetilde{\alpha}, h(\widetilde{\alpha})\right) : \widetilde{\alpha} \text{ repr. of } \alpha\}$ the size of $\alpha \in A$.

Effective specialization lemma

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 and K its quotient field.

Suppose that $f_1, \ldots, f_M$ have total degrees at most d and logarithmic heights at most h, where $d \geq 1$, $h \geq 1$.

Let $z_1, \ldots, z_q$ be alg. ind., $z_{q+1}, \ldots, z_r$ alg. over $K_0 = \mathbb{Q}(z_1, \ldots, z_q)$.

Let $\Bbbk_i = \overline{\mathbb{Q}(z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_q)}$, $L_i := \Bbbk_i K$.
Then L_i is a finite extension of $\Bbbk_i(z_i)$ and thus a function field in one variable over $\Bbbk_i$. Further, let

H_{L_i} the function field height on L_i (0 on $\Bbbk_i^*$),
$h_{\overline{\mathbb{Q}}}$ the absolute logarithmic Weil height on $\overline{\mathbb{Q}}$,
$s(\alpha) := \inf\{\max\left(1, \deg \widetilde{\alpha}, h(\widetilde{\alpha})\right) : \widetilde{\alpha} \text{ repr. of } \alpha\}$ the size of $\alpha \in A$.

Effective specialization lemma

Let $\alpha \in A$. Let $\max_{1 \leq i \leq q} H_{L_i}(\alpha) \leq R$. Then one can compute:

- a finite set $\mathcal{S} \subset \mathbb{Z}^q$ depending only on r, d, h, R;

- an effective upper bound for $s(\alpha)$ depending only on r, d, h, R and $\max\left\{h_{\overline{\mathbb{Q}}}(\varphi_{u,j}(\alpha)) : u \in \mathcal{S}, j = 1, \ldots, D\right\}$.

Effective specialization lemma

Effective specialization lemma

Let $\alpha \in A$. Let $\max_{1\le i\le q} H_{L_i}(\alpha) \le R$. Then one can compute:

- a finite set $\mathcal{S} \subset \mathbb{Z}^q$ depending only on r, d, h, R;

- an effective upper bound for $s(\alpha)$ depending only on r, d, h, R and $\max\left\{h_{\overline{\mathbb{Q}}}(\varphi_{\mathsf{u},j}(\alpha)) : \mathsf{u} \in \mathcal{S}, j = 1, \dots, D\right\}$.

$$
\begin{array}{ccccc}
R & \to & \mathcal{S} & \to \max\left\{h_{\overline{\mathbb{Q}}}(\varphi_{\mathsf{u},j}(\alpha)) : \mathsf{u} \in \mathcal{S}, j = 1, \dots, D\right\} \\
 & \searrow & & \swarrow & \\
 & & s(\alpha) & &
\end{array}
$$

Győry (1983/84) basically proved a version of this effective specialization lemma in the case that A is a special domain.

We extended this to arbitrary finitely generated domains A of characteristic 0 using Aschenbrenner's theorem mentioned before (a result of this type was not available when Győry obtained his result).

Application to unit equations

Let $A \cong \mathbb{Z}[Z_1, \ldots, Z_r]/(f_1, \ldots, f_M)$ be a f.g. domain of char. 0 and let a, b, c be non-zero elements of A. Consider the equation

(U) $$ax + by = c \quad \text{in } x, y \in A^* \quad \text{(group of units of } A\text{)}$$

Let $d \geq 1$ be an upper bound for the total degrees and $h \geq 1$ an upper bound for the logarithmic heights of $f_1, \ldots, f_M$ and for representatives for a, b, c.

Application to unit equations

Let $A \cong \mathbb{Z}[Z_1, \ldots, Z_r]/(f_1, \ldots, f_M)$ be a f.g. domain of char. 0 and let a, b, c be non-zero elements of A. Consider the equation

$$\text{(U)} \qquad ax + by = c \quad \text{in } x, y \in A^* \quad \text{(group of units of } A\text{)}$$

Let $d \geq 1$ be an upper bound for the total degrees and $h \geq 1$ an upper bound for the logarithmic heights of $f_1, \ldots, f_M$ and for representatives for a, b, c.

1. Compute an upper bound R for $H_{L_i}(x)$, $H_{L_i}(y)$ for $i = 1, \ldots, q$, using Mason's abc-theorem for function fields;
2. Compute the set $\mathcal{S} \subset \mathbb{Z}^q$; the specializations $\varphi_{\mathrm{u},j}$ ($\mathrm{u} \in \mathcal{S}$, $j = 1, \ldots, D$) map (U) to S-unit equations in number fields;
3. Compute an upper bound for $\max\{h_{\overline{\mathbb{Q}}}(\varphi_{\mathrm{u},j}(x)), h_{\overline{\mathbb{Q}}}(\varphi_{\mathrm{u},j}(y)) : \mathrm{u} \in \mathcal{S}, j = 1, \ldots, D\}$ using Baker theory (e.g., Győry, Yu (2006));
4. Using the effective specialization lemma, compute upper bounds

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

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

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

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

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

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.
But forms in more than two variables need not be decomposable.

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

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

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

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

Every binary form is decomposable. So Thue equations are decomposable form equations in two unknowns.
But forms in more than two variables need not be decomposable.

There are general finiteness theorems for (DFE) (Ev., Győry, 1985, 2015) but these depend on Schmidt's Subspace Theorem, hence are *ineffective*.
To get effective finiteness results 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.

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.

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

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

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.

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

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

Theorem (Ev., Győry, 202?)

Suppose that F is triangularly connected and the linear factors of F have rank m (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.

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

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

where κ is an effectively computable absolute constant > 1.

About the proof

Győry proved in 1980/81 a version of the above theorem for decomposable form equations over the ring of S-integers of a number field.

We generalized his proof to decomposable form equations over arbitrary finitely generated domains A. This required some new machinery.

The idea is that thanks to the triangular connectedness condition, the decomposable form equation can be reduced to a system of unit equations in two unknowns over a finitely generated domain $A' \supset A$.

Applying our effective result on unit equations we eventually deduce our theorem.

About the proof

The reduction to unit equations is as follows.

Let $A = \mathbb{Z}[z_1, \ldots, z_r]$, K the quotient field of A and $\overline{K}$ an algebraic closure of K.

Let $F = \ell_1 \cdots \ell_n \in A[X_1, \ldots, X_m]$ with the ℓ_i linear forms with coefficients in $\overline{K}$ be the decomposable form under consideration, and suppose that F is triangularly connected.

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 $\mathcal{G}$.

About the proof

The reduction to unit equations is as follows.

Let $A = \mathbb{Z}[z_1, \ldots, z_r]$, K the quotient field of A and $\overline{K}$ an algebraic closure of K.

Let $F = \ell_1 \cdots \ell_n \in A[X_1, \ldots, X_m]$ with the ℓ_i linear forms with coefficients in $\overline{K}$ be the decomposable form under consideration, and suppose that F is triangularly connected.

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 $\mathrm{x} = (x_1, \ldots, x_m) \in A^m$ be a solution of $F(\mathrm{x}) = \delta$.

By adjoining to A a finite number of elements from $\overline{K}$, and denoting by A' the resulting f.g. domain, we obtain

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

Now apply the result on unit equations mentioned before, with A' instead of A.

Thank you for your attention.