Effective results for Diophantine equations over finitely generated domains (I)

Jan-Hendrik Evertse
Universiteit Leiden

Specialization and Effectiveness in Number Theory

BIRS, August 30, 2022

Reference: J.-H. E. & K. Győry: *Effective results and methods for Diophantine equations over finitely generated domains,* London Math. Soc. Lecture Notes 475

Finitely generated domains

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

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

In case that $z_1, \dots, z_r$ are all algebraic over $\mathbb{Q}$, then A is a subring of the ring of S-integers of a number field K, i.e.,

$$O_{K,S} = O_K[(\mathfrak{p}_1 \cdots \mathfrak{p}_t)^{-1}],$$

where O_K is the ring of integers of K and $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_t\}$ a finite set of prime ideals of O_K.

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

Equations over finitely generated domains

Lang (1960, see his 'Fundamentals of Diophantine geometry') was the first to prove finiteness results for various classes of Diophantine equations over arbitrary f.g. domains A of char. 0, e.g., unit equations $ax + by = c$ in $x, y \in A^*$ with $a, b, c \in A \setminus \{0\}$, polynomial equations $P(x, y) = 0$ in $x, y \in A$ with $P \in A[X, Y]$ but his proofs are ineffective.

Aim. To prove *effective* finiteness results over an arbitrary finitely generated domain of char. 0 for certain classes of equations (i.e., results that imply algorithms to find all solutions in principle, we do not care about practical solubility).

Equations over finitely generated domains

Lang (1960, see his 'Fundamentals of Diophantine geometry') was the first to prove finiteness results for various classes of Diophantine equations over arbitrary f.g. domains A of char. 0, e.g., unit equations $ax + by = c$ in $x, y \in A^*$ with $a, b, c \in A \setminus \{0\}$, polynomial equations $P(x, y) = 0$ in $x, y \in A$ with $P \in A[X, Y]$ but his proofs are ineffective.

Aim. To prove *effective* finiteness results over an arbitrary finitely generated domain of char. 0 for certain classes of equations (i.e., results that imply algorithms to find all solutions in principle, we do not care about practical solubility).

There are various effective results for Diophantine equations over the S-integers of a number field (e.g., unit equations, Thue equations, hyper- and superelliptic equations, ...), all obtained by means of Baker's method (lower bounds for linear forms in logarithms).

Győry (1983/84) developed a method to prove effective results over a more general class of f.g. domains containing transcendental elements. Ev. and Győry (2013) extended Győry's method to arbitrary f.g. domains of char. 0.

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 its elements.

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

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

By Hilbert's basis theorem, there are $f_1, \dots, f_M \in \mathbb{Z}[Z_1, \dots, Z_r]$ such that $\mathcal{I} = (f_1, \dots, f_M)$. We use $\{f_1, \dots, f_M\}$ to represent A.

Note that

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

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 its elements.

Let $A = \mathbb{Z}[z_1, \ldots, z_r]$ be a f.g. domain of char. 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 $\mathcal{I} = (f_1, \ldots, f_M)$. We use $\{f_1, \ldots, f_M\}$ to represent A.

Note that

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

Fact. A is an integral domain of characteristic 0
$\Longleftrightarrow \mathcal{I} = (f_1, \ldots, f_M)$ 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., $\widetilde{\alpha} - \widetilde{\alpha}' \in \mathcal{I}$.

This can be done by an *ideal membership algorithm* for $\mathbb{Z}[Z_1, \ldots, Z_r]$, i.e., an algorithm that decides for any given $g, f_1, \ldots, f_M \in \mathbb{Z}[Z_1, \ldots, Z_r]$ whether g belongs to the ideal $(f_1, \ldots, f_M)$ 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

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

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 that $g \in (f_1, \ldots, f_M)$.

Then there are $u_1, \ldots, u_r \in \mathbb{Z}[Z_1, \ldots, Z_r]$ with $g = u_1 f_1 + \cdots + u_M f_M$ and

$$\deg u_i \leq C_1 := (4d)^{(6r)^r} h, \quad h(u_i) \leq C_2 := (4d)^{(6r)^{r+1}} h^{r+1}$$
for $i = 1, \ldots, M$.

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.

We consider Diophantine equations

$$(*) \quad P(x_1, \ldots, x_m) = 0 \ \text{ in } x_1, \ldots, x_m \in A \ \text{ where } P \in A[X_1, \ldots, X_m].$$

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 $x_1, \ldots, x_m$.

To find all solutions of (*) it suffices to give an explicit upper bound for the *sizes* (to be defined) of $x_1, \ldots, x_m$.

Sizes

The size of a polynomial $f \in \mathbb{Z}[Z_1, \dots, Z_r]$ is defined by

$$s(f) := \max(1, \deg f, h(f)),$$

where

$\deg f$ is the total degree of f,
$h(f) := \log \max |\text{coeff. of } f|$ is the logarithmic height of f.

The size of $\alpha \in A \cong \mathbb{Z}[Z_1, \dots, Z_r]/(f_1, \dots, f_M)$ is given by

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

Solving Diophantine equations over finitely generated domains by means of size bounds

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. Consider the Diophantine equation

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

where $P = \sum a(\mathrm{i}) X_1^{i_1} \cdots X_m^{i_m} \in A[X_1, \ldots, X_m]$.

Suppose we are given a representative $\widetilde{a}(\mathrm{i}) \in \mathbb{Z}[Z_1, \ldots, Z_r]$ for each $a(\mathrm{i})$, and put $\widetilde{P} := \sum \widetilde{a}(\mathrm{i}) X_1^{i_1} \cdots X_m^{i_m}$.

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

Solving Diophantine equations over finitely generated domains by means of size bounds

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. Consider the Diophantine equation

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

where $P = \sum a(\mathrm{i}) X_1^{i_1} \cdots X_m^{i_m} \in A[X_1, \ldots, X_m]$.

Suppose we are given a representative $\widetilde{a}(\mathrm{i}) \in \mathbb{Z}[Z_1, \ldots, Z_r]$ for each $a(\mathrm{i})$, and put $\widetilde{P} := \sum \widetilde{a}(\mathrm{i}) X_1^{i_1} \cdots X_m^{i_m}$.

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

Indeed, finding the solutions $x_1, \ldots, x_m \in A$ of (*) is equivalent to finding representatives $\widetilde{x}_1, \ldots, \widetilde{x}_m \in \mathbb{Z}[Z_1, \ldots, Z_r]$ of size $\leq C$ such that
$(+)$ $\widetilde{P}(\widetilde{x}_1, \ldots, \widetilde{x}_m) \in \mathcal{I}$.

These can be found by going through the finitely many tuples $\widetilde{x}_1, \ldots, \widetilde{x}_m \in \mathbb{Z}[Z_1, \ldots, Z_r]$ of size $\leq C$ and check whether they satisfy $(+)$ using an ideal membership algorithm for $\mathbb{Z}[Z_1, \ldots, Z_r]$.

How to compute size bounds

Given an equation over a f.g. domain A of char. 0, one maps this by means of specializations to a finite number of equations over number fields and over function fields, computes upper bounds for the heights of the image equations (e.g., by Baker's method for number fields and Mason's abc-theorem for function fields), and combines these into an upper bound for the sizes of the solutions of the equation over A by means of the *effective specialization lemma* (discussed later).

Roughly speaking, if one can compute height bounds for the solutions of Diophantine equations of a particular type over number fields and also over function fields, then one can compute size bounds for the solutions of such equations over f.g. domains.

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*

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

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 (by Baker's method) and Mason (1983) proved an analogue for function fields in one variable (following from his celebrated abc-theorem). By combining these with the effective specialization lemma we obtain size bounds for the solutions of (U).

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) $\qquad ax + by = c \;$ in $x, y \in A^*$ (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 (by Baker's method) and Mason (1983) proved an analogue for function fields in one variable (following from his celebrated abc-theorem). By combining these with the effective specialization lemma we obtain size bounds for the solutions of (U).

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 results

For the equations listed below, there are height bounds for the solutions over the S-integers of a number field, and also over function fields, obtained via Baker's method and Mason's abc-theorem.

Using the effective specialization lemma these can be combined to size bounds similar to those for unit equations for the solutions of the equations over a f.g. domain A of char. 0.

Further results

For the equations listed below, there are height bounds for the solutions over the S-integers of a number field, and also over function fields, obtained via Baker's method and Mason's abc-theorem.

Using the effective specialization lemma these can be combined to size bounds similar to those for unit equations for the solutions of the equations over a f.g. domain A of char. 0.

- (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 results

For the equations listed below, there are height bounds for the solutions over the S-integers of a number field, and also over function fields, obtained via Baker's method and Mason's abc-theorem.

Using the effective specialization lemma these can be combined to size bounds similar to those for unit equations for the solutions of the equations over a f.g. domain A of char. 0.

- (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 results

For the equations listed below, there are height bounds for the solutions over the S-integers of a number field, and also over function fields, obtained via Baker's method and Mason's abc-theorem.

Using the effective specialization lemma these can be combined to size bounds similar to those for unit equations for the solutions of the equations over a f.g. domain A of char. 0.

- (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 results

For the equations listed below, there are height bounds for the solutions over the S-integers of a number field, and also over function fields, obtained via Baker's method and Mason's abc-theorem.

Using the effective specialization lemma these can be combined to size bounds similar to those for unit equations for the solutions of the equations over a f.g. domain A of char. 0.

- (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 $f \in A[X, Y]$ (see his talk);

Further results

For the equations listed below, there are height bounds for the solutions over the S-integers of a number field, and also over function fields, obtained via Baker's method and Mason's abc-theorem.

Using the effective specialization lemma these can be combined to size bounds similar to those for unit equations for the solutions of the equations over a f.g. domain A of char. 0.

- (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 $f \in A[X, Y]$ (see his talk);
- (Ev., Győry, 2022) 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.

Ingredients of the effective specialization lemma

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

Specializations.
If $\varphi : A \to \overline{\mathbb{Q}}$ is a specialization, then $\varphi(A)$ is contained in the ring of S_φ-integers of a number field L_φ for some L_φ, S_φ depending on φ.

Most of our applications require that $\varphi(e) \neq 0$ for a particular non-zero element e of A.

Ingredients of the effective specialization lemma

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

Specializations.
If $\varphi : A \to \overline{\mathbb{Q}}$ is a specialization, then $\varphi(A)$ is contained in the ring of S_φ-integers of a number field L_φ for some L_φ, S_φ depending on φ.

Most of our applications require that $\varphi(e) \neq 0$ for a particular non-zero element e of A.

Function fields.
Assume wlog that $z_1, \ldots, z_q$ are algebraically independent and that $z_{q+1}, \ldots, z_r$ are algebraic over $\mathbb{Q}(z_1, \ldots, z_q)$. Let

$$\Bbbk_i := \overline{\mathbb{Q}(z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_q)}, \quad L_i := \Bbbk_i K \quad (i = 1, \ldots, q).$$

Note that $A \subset L_i$, and that L_i is a finite extension of $\Bbbk_i(z_i)$, i.e., a function field of transcendence degree 1 over $\Bbbk_i$.
The function field height associated to L_i is given by
$H_{L_i}(\alpha) := [L_i : \Bbbk_i(\alpha)]$ for $\alpha \in L_i \setminus \Bbbk_i$.

Effective specialization lemma

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

Let $L_1, \dots, L_q$ be the function fields from the previous slide.

Let $e \in A \setminus \{0\}$ and $\widetilde{e} \in \mathbb{Z}[Z_1, \dots, Z_r]$ a representative for e.
Suppose $f_1, \dots, f_M, \widetilde{e}$ have total degrees $\leq d$ and log. heights $\leq h$.

Further, let
H_{L_i} the function field height on L_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 $\max_{1 \leq i \leq q} H_{L_i}(\alpha) \leq T$. Then one can compute:

- a finite set $\mathcal{S}$ of specializations $\varphi : A \to \overline{\mathbb{Q}}$ depending only on r, d, h, T such that $\varphi(e) \neq 0$ for $\varphi \in \mathcal{S}$;

- an effective upper bound for $s(\alpha)$ depending only on $r, d, h,$ T and $\max\left\{h_{\overline{\mathbb{Q}}}(\varphi(\alpha)) : \varphi \in \mathcal{S}\right\}$.

Effective specialization lemma

Effective specialization lemma

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

- a finite set $\mathcal{S}$ *of specializations* $\varphi : A \to \overline{\mathbb{Q}}$ *depending only on* r, d, h, T *such that* $\varphi(e) \neq 0$ *for* $\varphi \in \mathcal{S}$*;*

- an effective upper bound for $s(\alpha)$ *depending only on* r, d, h, T *and* $\max\left\{h_{\overline{\mathbb{Q}}}(\varphi(\alpha)) : \varphi \in \mathcal{S}\right\}$.

$$\begin{tikzcd} \alpha \arrow[r] & T \arrow[r] \arrow[dr] & \mathcal{S} \arrow[r] & \max\left\{h_{\overline{\mathbb{Q}}}(\varphi(\alpha)) : \varphi \in \mathcal{S}\right\} \arrow[dl] \\ & & \text{bound for } s(\alpha) & \end{tikzcd}$$

Győry (1983/84) basically proved a version of this lemma for a special class of domains A.

We extended this to arbitrary finitely generated domains A of characteristic 0 using the work of Aschenbrenner (2004).

Effective specialization lemma

Effective specialization lemma

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

- a finite set $\mathcal{S}$ of specializations $\varphi : A \to \overline{\mathbb{Q}}$ depending only on r, d, h, T such that $\varphi(e) \neq 0$ for $\varphi \in \mathcal{S}$;

- an effective upper bound for $s(\alpha)$ depending only on r, d, h, T and $\max\left\{h_{\overline{\mathbb{Q}}}(\varphi(\alpha)) : \varphi \in \mathcal{S}\right\}$.

$$\begin{tikzcd}
\alpha \arrow[r] & T \arrow[r] \arrow[dr] & \mathcal{S} \arrow[r] & \max\left\{h_{\overline{\mathbb{Q}}}(\varphi(\alpha)) : \varphi \in \mathcal{S}\right\} \arrow[dl] \\
& & \text{bound for } s(\alpha) &
\end{tikzcd}$$

To estimate $s(x_1), \ldots, s(x_m)$ for the solutions $(x_1, \ldots, x_m) \in A^m$ of a Diophantine equation, one first computes an upper bound T for $\max_{i,j} H_{L_i}(x_j)$, then $\mathcal{S}$, then an upper bound for $\max_{j, \varphi \in \mathcal{S}} h_{\overline{\mathbb{Q}}}(\varphi(x_j))$, and finally an upper bound for $\max_j s(x_j)$.

The proof of the result on 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

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

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.

The proof of the result on 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) $\quad ax + by = c$ in $x, y \in A^*$ (group of units of A)

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 T for the function field heights $H_{L_i}(x)$, $H_{L_i}(y)$ for $i = 1, \ldots, q$, using Mason's abc-theorem for function fields.
2. Take $e = abc$ and compute the finite set $\mathcal{S}$ of specializations $A \to \overline{\mathbb{Q}}$ from the effective specialization lemma, with $\varphi(abc) \neq 0$ for $\varphi \in \mathcal{S}$; each of these specializations maps (U) to an S-unit equation in some number field.

The proof of the result on 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

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

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 T for the function field heights $H_{L_i}(x)$, $H_{L_i}(y)$ for $i = 1, \ldots, q$, using Mason's abc-theorem for function fields.
2. Take $e = abc$ and compute the finite set $\mathcal{S}$ of specializations $A \to \overline{\mathbb{Q}}$ from the effective specialization lemma, with $\varphi(abc) \neq 0$ for $\varphi \in \mathcal{S}$; each of these specializations maps (U) to an S-unit equation in some number field.
3. Compute an upper bound for $\max\{h_{\overline{\mathbb{Q}}}(\varphi(x)), h_{\overline{\mathbb{Q}}}(\varphi(y)) : \varphi \in \mathcal{S}\}$ using Baker theory (e.g., Győry, Yu (2006)).
4. Using the effective specialization lemma, compute upper bounds

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

Future plans

Theorem (Siegel, Lang)

Let $A = \mathbb{Z}[z_1, \ldots, z_r]$ be a f.g. domain of char. 0, $P \in A[X, Y]$ an absolutely irreducible polynomial and $\mathcal{C}_P$ the algebraic curve given by $P(x, y) = 0$.
Suppose either $\mathcal{C}_P$ is of genus ≥ 1, or $\mathcal{C}_P$ is of genus 0 and has at least three points at infinity. Then $P(x, y) = 0$ has only finitely many solutions in $x, y \in A$.

Siegel proved this in 1929 for A the ring of integers of a number field, and Lang proved in 1960 the general case. The proofs of Siegel and Lang are ineffective.

Future plans

Theorem (Siegel, Lang)

Let $A = \mathbb{Z}[z_1, \ldots, z_r]$ be a f.g. domain of char. 0, $P \in A[X, Y]$ an absolutely irreducible polynomial and $\mathcal{C}_P$ the algebraic curve given by $P(x, y) = 0$.
Suppose either $\mathcal{C}_P$ is of genus ≥ 1, or $\mathcal{C}_P$ is of genus 0 and has at least three points at infinity. Then $P(x, y) = 0$ has only finitely many solutions in $x, y \in A$.

Siegel proved this in 1929 for A the ring of integers of a number field, and Lang proved in 1960 the general case. The proofs of Siegel and Lang are ineffective.

In certain cases, with A the ring of S-integers of a number field, there are effective results, with bounds for the heights of x, y, e.g., if $\mathcal{C}_P$ is of genus 0 or 1.

We would like to extend these to arbitrary f.g. domains A of char. 0, with bounds for the sizes $s(x), s(y)$. Our effective specialization lemma is not sufficient in this case.

Thank you for your attention.