EFFECTIVE RESULTS FOR DIOPHANTINE EQUATIONS OVER FINITELY GENERATED DOMAINS: A SURVEY

JAN-HENDRIK EVERTSE AND KÁLMÁN GYŐRY

Abstract. We give a survey of our recent effective results on unit equations in two unknowns and, obtained jointly with A. Bérczes, on Thue equations and superelliptic equations over an arbitrary domain that is finitely generated over $\mathbb{Z}$. Further, we outline the method of proof.

1. Introduction

We give a survey of recent effective results for Diophantine equations with unknowns taken from domains finitely generated over $\mathbb{Z}$. Here, by a domain finitely generated over $\mathbb{Z}$ we mean an integral domain of characteristic 0 that is finitely generated as a $\mathbb{Z}$-algebra, i.e., of the shape $\mathbb{Z}[z_1, \dots, z_r]$ where the generators z_i may be algebraic or transcendental over $\mathbb{Z}$.

Lang [14] was the first to prove finiteness results for Diophantine equations over domains finitely generated over $\mathbb{Z}$. Let A be such a domain. Generalizing work of Siegel [22], Mahler [15] and Parry [17], Lang proved that if a, b, c are non-zero elements of A, then the equation $ax + by = c$, called unit equation, has only finitely many solutions in units x, y of A. Further, Lang extended Siegel's theorem [23] on integral points on curves, i.e., he proved that if $f \in A[X, Y]$ is a polynomial such that $f(x, y) = 0$ defines a curve C of genus at least 1, then there are only finitely many points $(x, y) \in A \times A$ on C. The results of Siegel, Mahler, Parry and Lang were ineffective, i.e., with their methods of proof it is not possible to determine in principle the solutions of the equations under consideration.

2010 Mathematics Subject Classification: Primary 11D61; Secondary: 11J86.

Keywords and Phrases: Unit equations, Thue equations, superelliptic equations, finitely generated domains, effective finiteness results.

K. Győry has been supported by the OTKA-grants no. 67580,75566 and 100339.

June 29, 2013.

A major breakthrough in the effective theory of Diophantine equations was established by A. Baker in the 1960's. Using his own estimates for linear forms in logarithms of algebraic numbers, he obtained effective bounds for the solutions of Thue equations [2] and hyper- and superelliptic equations [3] over $\mathbb{Z}$. Schinzel and Tijdeman [19] were the first to consider superelliptic equations $f(x) = \delta y^m$ over $\mathbb{Z}$ where also the exponent m was taken as an unknown and gave an effective upper bound for m. Győry [9], [10] showed, in the case that A is the ring of S-integers in a number field, that the solutions of unit equations can be determined effectively in principle. Their proofs also depend on Baker's linear forms estimates.

The effective results of Baker and of Schinzel and Tijdeman were extended to equations where the solutions x, y are taken from the ring of S-integers of an algebraic number field; we mention here Coates [7], Sprindžuk and Kotov [25] (Thue equations), and Trelina [26], Brindza [5] (hyper- and superelliptic equations).

In the 1980's Győry [11], [12] developed a method, which enabled him to obtain effective finiteness results for certain classes of Diophantine equations over a restricted class of finitely generated domains. The core of the method is to reduce the Diophantine equations under consideration to equations over number fields and over function fields by means of an effective specialization method, and then to apply Baker type logarithmic form estimates to the obtained equations over number fields, and results of, e.g., Mason, to the equations over function fields. Győry applied his method among others to Thue equations, and later Brindza [6] and Végső [27] to hyper- and superelliptic equations and the Schinzel-Tijdeman equation.

Recently, the two authors managed to extend Győry's method to arbitrary finitely generated domains. By means of this extended method the two authors [8] obtained an effective finiteness result for the unit equation $ax + by = c$ in $x, y \in A^*$, where A is an arbitrary domain that is finitely generated over $\mathbb{Z}$, and A^* denotes the unit group of A. By applying the same method, the authors together with Bérczes [4] obtained effective versions of certain special cases of Siegel's theorem over A. Namely, they obtained effective finiteness results for Thue equations $F(x, y) = \delta$ in $x, y \in A$ and hyper/superelliptic equations $F(x) = \delta y^m$ in $x, y \in A$, where δ is a non-zero element of A, F is a binary form, respectively polynomial with coefficients in A, and m is an integer ≥ 2. All these equations have a great number of applications. We note that the approach of the authors can be applied to various other classes of Diophantine equations as well.

In Section 2 we give an overview of our recent results. In Section 3 we give a brief outline of the method of proof.

2. Recent results

2.1. **Notation.** Let again $A \supset \mathbb{Z}$ be an integral domain which is finitely generated over $\mathbb{Z}$, say $A = \mathbb{Z}[z_1, \dots, z_r]$. Put

$$R := \mathbb{Z}[X_1, \dots, X_r], \quad I := \{f \in R : \; f(z_1, \dots, z_r) = 0\}.$$

Then I is an ideal of R, which is necessarily finitely generated. Hence

$$A \cong R/I, \quad I = (f_1, \dots, f_t)$$

for some finite set of polynomials $\{f_1, \dots, f_t\} \subset R$. We may view $\{f_1, \dots, f_t\}$ as a representation for A. For instance using Aschenbrenner [1, Prop. 4.10, Cor. 3.5], it can be checked effectively whether A is a domain containing $\mathbb{Z}$, that is to say, whether I is a prime ideal of R with $I \cap \mathbb{Z} = (0)$.

Denote by K the quotient field of A. For $\alpha \in A$, we call f a *representative* for α, or say that f represents α if $f \in R$ and $\alpha = f(z_1, \dots, z_r)$. Further, for $\alpha \in K$, we call (f, g) a *pair of representatives* for α or say that (f, g) represents α if $f, g \in R$, $g \notin I$ and $\alpha = f(z_1, \dots, z_r)/g(z_1, \dots, z_r)$. We say that $\alpha \in A$ (resp. $\alpha \in K$) is given if a representative (resp. pair of representatives) for α is given.

To do explicit computations in A and K, one needs an *ideal membership algorithm* for R, that is an algorithm that decides for any given polynomial and ideal of R whether the polynomial belongs to the ideal. Among the various algorithms of this sort in the literature we mention only those implied by work of Simmons [24] and Aschenbrenner [1]. The work of Aschenbrenner plays a vital role in our proofs. One can perform arithmetic operations on A and K by using representatives. Further, one can decide effectively whether two polynomials $f_1, f_2 \in R$ represent the same element of A, i.e., $f_1 - f_2 \in I$, or whether two pairs of polynomials $(f_1, g_1), (f_2, g_2) \in R \times R$ represent the same element of K, i.e., $f_1 g_2 - f_2 g_1 \in I$, by using one of the ideal membership algorithms mentioned above.

Given $f \in R$, we denote by $\deg f$ its total degree, and by $h(f)$ its logarithmic height, i.e., the logarithm of the maximum of the absolute values of its coefficients. The *size* of f is defined by

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

Clearly, there are only finitely many polynomials in R of size below a given bound, and these can be determined effectively.

We use the notation $O(r)$ to denote any expression of the type 'absolute constant times r', where at each occurrence of $O(r)$ the constant may be different.

2.2. **Thue equations.** We consider the *Thue equation* over A,

$$F(x, y) = \delta \quad \text{in } x, y \in A, \tag{2.1}$$

where

$$F(X, Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n \in A[X, Y]$$

is a binary form of degree $n \geq 3$ with discriminant $D_F \neq 0$, and $\delta \in A \setminus \{0\}$. We represent (2.1) by a set of representatives

$$\widetilde{a_0}, \widetilde{a_1}, \ldots, \widetilde{a_n}, \widetilde{\delta} \in \mathbb{Z}[X_1, \ldots, X_r]$$

for $a_0, a_1, \ldots, a_n, \delta$, respectively, such that $\widetilde{\delta} \notin I, D_{\widetilde{F}} \notin I$ where $D_{\widetilde{F}}$ is the discriminant of $\widetilde{F} := \sum_{j=0}^{n} \widetilde{a_j} X^{n-j}Y^j$. These last two conditions can be checked by means of the ideal membership algorithm mentioned above. Let

$$\max(\deg f_1, \ldots, \deg f_t, \deg \widetilde{a_0}, \deg \widetilde{a_1}, \ldots, \deg \widetilde{a_n}, \deg \widetilde{\delta}) \leq d,$$
$$\max(h(f_1), \ldots, h(f_t), h(\widetilde{a_0}), h(\widetilde{a_1}), \ldots, h(\widetilde{a_n}), h(\widetilde{\delta})) \leq h,$$

where $d \geq 1, h \geq 1$.

Theorem 2.1 (Bérczes, Evertse, Győry [4])**.** *Every solution x, y of equation* (2.1) *has representatives $\widetilde{x}, \widetilde{y}$ such that*

$$s(\widetilde{x}), s(\widetilde{y}) \leq \exp\left(n!(nd)^{\exp O(r)}(h + 1)\right). \tag{2.2}$$

This result implies that equation (2.1) is effectively solvable in the sense that one can compute in principle a finite list, consisting of one pair of representatives for each solution (x, y) of (2.1). Indeed, let $f_1, \ldots, f_t \in R$ be given such that A is a domain, and let representatives $\widetilde{a_0}, \widetilde{a_1}, \ldots, \widetilde{a_n}, \widetilde{\delta}$ of $a_0, \ldots, a_n, \delta$ be given such that $D_{\widetilde{F}}, \widetilde{\delta} \notin I$. Let C be the upper bound from (2.2). Then one simply has to check, for each pair of polynomials $\widetilde{x}, \widetilde{y} \in$

$\mathbb{Z}[X_1, \ldots, X_r]$ of size at most C whether $\widetilde{F}(\widetilde{x}, \widetilde{y}) - \widetilde{\delta} \in I$ and subsequently, to check for all pairs $\widetilde{x}, \widetilde{y}$ passing this test whether they are equal modulo I, and to keep a maximal subset of pairs that are different modulo I.

2.3. **Hyper- and superelliptic equations.** We now consider the equation

$$F(x) = \delta y^m \quad \text{in } x, y \in A, \tag{2.3}$$

where

$$F(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \in A[X]$$

is a polynomial degree n with discriminant $D_F \neq 0$, and where $\delta \in A \setminus \{0\}$. We assume that either $m = 2$ and $n \geq 3$, or $m \geq 3$ and $n \geq 2$. For $m = 2$, equation (2.3) is called a *hyperelliptic equation*, while for $m \geq 3$ it is called a *superelliptic equation*. Similarly as for the Thue equation, we represent (2.3) by means of a tuple of representatives

$$\widetilde{a_0}, \widetilde{a_1}, \ldots, \widetilde{a_n}, \widetilde{\delta} \in \mathbb{Z}[X_1, \ldots, X_r]$$

for $a_0, a_1, \ldots, a_n, \delta$, respectively, such that $\widetilde{\delta}$ and the discriminant of $\widetilde{F} := \sum_{j=0}^{n} \widetilde{a_j} X^{n-j}$ do not belong to I. Let

$$\max(\deg f_1, \ldots, \deg f_t, \deg \widetilde{a_0}, \deg \widetilde{a_1}, \ldots, \deg \widetilde{a_n}, \deg \widetilde{\delta}) \leq d$$
$$\max(h(f_1), \ldots, h(f_t), h(\widetilde{a_0}), h(\widetilde{a_1}), \ldots, h(\widetilde{a_n}), h(\widetilde{\delta})) \leq h,$$

where $d \geq 1, h \geq 1$.

Theorem 2.2 (Bérczes, Evertse, Győry [4]). *Every solution x, y of equation* (2.3) *has representatives $\widetilde{x}, \widetilde{y}$ such that*

$$s(\widetilde{x}), s(\widetilde{y}) \leq \exp\left(m^3 (nd)^{\exp O(r)} (h+1)\right).$$

Completely similarly as for Thue equations, one can determine effectively a finite list, consisting of one pair of representatives for each solution (x, y) of (2.3).

Our next result deals with the *Schinzel-Tijdeman equation*, which is (2.3) but with three unknowns $x, y \in A$ and $m \in \mathbb{Z}_{\geq 2}$.

Theorem 2.3 (Bérczes, Evertse, Győry [4]). *Assume that in* (2.3)*, F has non-zero discriminant and $n \geq 2$. Let $x, y \in A, m \in \mathbb{Z}_{\geq 2}$ be a solution of* (2.3)*. Then*

$$m \leq \exp\left((nd)^{\exp O(r)} (h+1)\right)$$

$$\text{if } y \in \overline{\mathbb{Q}}, y \neq 0, \ y \text{ is not a root of unity,}$$

and

$$m \leq (nd)^{\exp O(r)} \qquad \text{if } y \notin \overline{\mathbb{Q}}.$$

2.4. **Unit equations.** Finally, consider the *unit equation*

$$ax + by = c \ \text{ in } x, y \in A^* \tag{2.4}$$

where A^* denotes the unit group of A, and a, b, c are non-zero elements of A.

Theorem 2.4 (Evertse and Győry [8]). *Assume that $r \geq 1$. Let $\widetilde{a}, \widetilde{b}, \widetilde{c}$ be representatives for a, b, c, respectively. Assume that $f_1, \dots, f_t$ and $\widetilde{a}, \widetilde{b}, \widetilde{c}$ all have degree at most d and logarithmic height at most h, where $d \geq 1$, $h \geq 1$. Then for each solution (x, y) of (2.4), there are representatives $\widetilde{x}, \widetilde{x}', \widetilde{y}, \widetilde{y}'$ of x, x^{-1}, y, y^{-1}, respectively, such that*

$$s(\widetilde{x}),\ s(\widetilde{x}'),\ s(\widetilde{y}),\ s(\widetilde{y}') \leq \exp\Big((2d)^{\exp O(r)}(h+1)\Big).$$

Again, similarly as for Thue equation, one can determine effectively a finite list, consisting of one pair of representatives for each solution (x, y) of (2.4).

By a theorem of Roquette [18], the unit group of an integral domain finitely generated over $\mathbb{Z}$ is finitely generated. In the case that $A = O_S$ is the ring of S-integers of a number field it is possible to determine effectively a system of generators for A^*, and this was used by Győry in his effective finiteness proof for (2.4) with $A = O_S$. However, no general algorithm is known to determine a system of generators for the unit group of an arbitrary finitely generated domain A. In our proof of Theorem 2.4, we did not need any information on the generators of A^*.

Let $\gamma_1, \dots, \gamma_s$ be multiplicatively independent elements of K^*. There exist algorithms to check effectively the multiplicative independence of elements of a finitely generated field of characteristic 0; see for instance Lemma 7.2 of [8]. Let again a, b, c be non-zero elements of A and consider the equation

$$a\gamma_1^{v_1} \cdots \gamma_s^{v_s} + b\gamma_1^{w_1} \cdots \gamma_s^{w_s} = c \ \text{ in } v_1, \dots, v_s,\ w_1, \dots, w_s \in \mathbb{Z}. \tag{2.5}$$

Theorem 2.5 (Evertse and Győry [8]). *Let $\widetilde{a}, \widetilde{b}, \widetilde{c}$ be representatives for a, b, c and for $i = 1, \dots, s$, let (g_{i1}, g_{i2}) be a pair of representatives for γ_i.*

Suppose that $f_1, \dots, f_t$, $\widetilde{a}, \widetilde{b}, \widetilde{c}$, *and* g_{i1}, g_{i2} $(i = 1, \dots, s)$ *all have degree at most* d *and logarithmic height at most* h, *where* $d \geq 1$, $h \geq 1$. *Then for each solution* $(v_1, \dots, w_s)$ *of* (2.5) *we have*

$$\max\left(|v_1|, \dots, |v_s|, |w_1|, \dots, |w_s|\right) \leq \exp\left((2d)^{\exp O(r+s)}(h+1)\right).$$

An immediate consequence of Theorem 2.5 is that for given $f_1, \dots, f_t$, a, b, c and $\gamma_1, \dots, \gamma_s$, the solutions of (2.5) can be determined effectively. Theorem 2.5 is a consequence of Theorem 2.4.

3. A sketch of the method

Let $A = \mathbb{Z}[z_1, \dots, z_r] \supset \mathbb{Z}$ be a domain that is finitely generated over $\mathbb{Z}$. Let K be the quotient field of A. As usual we write $R := \mathbb{Z}[X_1, \dots, X_r]$, and take $f_1, \dots, f_t \in R$ such that $f_1, \dots, f_t$ generate the ideal of $f \in R$ with $f(z_1, \dots, z_r) = 0$.

The general idea is to reduce our given Diophantine equation over A to Diophantine equations over function fields and over number fields by means of a specialization method. We first recall the lemmas which together constitute our specialization method, and then give a brief explanation how this can be used to prove the results mentioned in the previous section.

If K is algebraic over $\mathbb{Q}$ then no specialization argument is needed. We assume throughout that K has transcendence degree $q > 0$ over $\mathbb{Q}$. We assume without loss of generality that $z_1, \dots, z_q$ are algebraically independent over $\mathbb{Q}$. Put

$$A_0 := \mathbb{Z}[z_1, \dots, z_q], \quad K_0 := \mathbb{Q}(z_1, \dots, z_q).$$

Thus, $A = A_0[z_{q+1}, \dots, z_r]$, $K = K_0(z_{q+1}, \dots, z_r)$ and K is algebraic over K_0. Given $a \in A_0$ we let $\deg a$, $h(a)$ be the total degree and logarithmic height of a viewed as polynomial in the variables $z_1, \dots, z_q$.

Let $\widehat{d_0}$ be an integer ≥ 1 and $\widehat{h}_0$ a real ≥ 1. Assume that

$$\deg f_i \leq \widehat{d_0}, \quad h(f_i) \leq \widehat{h}_0 \quad \text{for } i = 1, \dots, t.$$

Lemma 3.1. *There are* w, f *with* $w \in A$, $f \in A_0 \setminus \{0\}$ *such that*

$$A \subseteq B := A_0[w, f^{-1}],$$
$$\deg f \leq (2\widehat{d_0})^{\exp O(r)}, \quad h(f) \leq (2\widehat{d_0})^{\exp O(r)}(\widehat{h}_0 + 1),$$

and such that w has minimal polynomial $X^D+\mathcal{F}_1X^{D-1}+\cdots+\mathcal{F}_D$ over K_0 of degree $D\le \widehat{d}_0^{\,r-q}$ with

$$\mathcal{F}_i\in A_0,\quad \deg\mathcal{F}_i\le (2\widehat{d}_0)^{\exp O(r)},\quad h(\mathcal{F}_i)\le (2\widehat{d}_0)^{\exp O(r)}(\widehat{h}_0+1)$$

for $i=1,\dots,D$.

Proof. This is a combination of Corollary 3.4 and Lemma 3.6 of [8]. □

Since A_0 is a unique factorization domain with unit group $\{\pm1\}$, for every non-zero $\alpha\in K$ there is an up to sign unique tuple $P_{\alpha,0},\dots,P_{\alpha,D-1},Q_\alpha\in A_0$ such that

$$\alpha=Q_\alpha^{-1}\sum_{j=0}^{D-1}P_{\alpha,j}w^j. \tag{3.1}$$

We define

$$\overline{\deg}\,\alpha:=\max(\deg P_{\alpha,0},\dots,\deg P_{\alpha,D-1},\deg Q_\alpha),$$
$$\overline{h}(\alpha):=\max(h(P_{\alpha,0}),\dots,h(P_{\alpha,D-1}),h(Q_\alpha)).$$

We observe here that $\alpha\in B$ if and only if Q_α divides a power of f.

Lemma 3.2. *Let $\alpha\in A\setminus\{0\}$.*
(i) Let $\widetilde{\alpha}\in R$ be a representative for α. Put $\widehat{d}_1:=\max(\widehat{d}_0,\deg\widetilde{\alpha})$, $\widehat{h}_1:=\max(\widehat{h}_0,h(\widetilde{\alpha}))$. Then

$$\overline{\deg}\,\alpha\le (2\widehat{d}_1)^{\exp O(r)},\quad \overline{h}(\alpha)\le (2\widehat{d}_1)^{\exp O(r)}(\widehat{h}_1+1). \tag{3.2}$$

(ii) Put $\widehat{d}_2:=\max(\widehat{d}_0,\overline{\deg}\,\alpha)$, $\widehat{h}_2:=\max(\widehat{h}_0,\overline{h}(\alpha))$. Then α has a representative $\widetilde{\alpha}\in R$ such that

$$\deg\widetilde{\alpha}\le (2\widehat{d}_2)^{\exp O(r\log^* r)}(\widehat{h}_2+1),\quad h(\widetilde{\alpha})\le (2\widehat{d}_2)^{\exp O(r\log^* r)}(\widehat{h}_2+1)^{r+1}. \tag{3.3}$$

Proof. This is a combination of Lemmas 3.5 and 3.7 of [8]. The proof is based on effective commutative linear algebra for polynomial rings over fields (Seidenberg, [21]) and over $\mathbb{Z}$ (Aschenbrenner, [1]). □

The next lemma relates $\overline{\deg}\,\alpha$ to certain function field heights. We use the notation from Lemma 3.1. Let $\alpha\mapsto\alpha^{(i)}$ $(i=1,\dots,D)$ denote the K_0-isomorphic embeddings of K in the algebraic closure of K_0. For $i=1,\dots,q$, let $\mathbf{k}_i$ be the algebraic closure of $\mathbb{Q}(z_1,\dots,z_{i-1},z_{i+1},\dots,z_q)$, and $M_i=$

$\mathbf{k}_i(z_i, w^{(1)}, \ldots, w^{(D)})$. Thus, K may be viewed as a subfield of $M_1, \ldots, M_q$. Given $\alpha \in K$, define the height of α with respect to $M_i/\mathbf{k}_i$,

$$H_{M_i/\mathbf{k}_i}(\alpha) := \sum_{v \in V_{M_i/\mathbf{k}_i}} \max(0, -v(\alpha)),$$

where $V_{M_i/\mathbf{k}_i}$ is the set of normalized discrete valuations of M_i that are trivial on $\mathbf{k}_i$. Put $\Delta_i := [M_i : \mathbf{k}_i(z_i)]$.

Lemma 3.3. *Let $\alpha \in K^*$. Then*

$$\overline{\deg}\,\alpha \leq qD \cdot (2\widehat{d}_0)^{\exp O(r)} + \sum_{i=1}^{q} \Delta_i^{-1} \sum_{j=1}^{D} H_{M_i/\mathbf{k}_i}(\alpha^{(j)}), \tag{3.4}$$

and

$$\max_{i,j} \Delta_i^{-1} H_{M_i/\mathbf{k}_i}(\alpha^{(j)}) \leq 2D\overline{\deg}\,\alpha + (2\widehat{d}_0)^{\exp O(r)}. \tag{3.5}$$

Proof. The first assertion is Lemma 4.4 of [8], where we have estimated from above the quantity d_1 from that lemma by the upper bound $(2\widehat{d}_0)^{\exp O(r)}$ for $\deg f$ and $\deg \mathcal{F}_i$ from Lemma 3.1 of the present paper. The second assertion is Lemma 4.4 of [4]. □

We define ring homomorphisms $B \to \overline{\mathbb{Q}}$, where $B \supseteq A$. Let $\alpha_1, \ldots, \alpha_k \in K^*$. For $i = 1, \ldots, k$, choose a pair of representatives $(a_i, b_i) \in R \times R$ for α_i and put

$$\widehat{d}_3 := \max(\widehat{d}_0, \deg a_1, \deg b_1, \ldots, \deg a_k, \deg b_k),$$
$$\widehat{h}_3 := \max(\widehat{h}_0, h(a_1), h(b_1), \ldots, h(a_k), h(b_k)).$$

Let $g := \prod_{i=1}^{k}(Q_{\alpha_i} Q_{\alpha_i^{-1}})$ and define the ring $B := A_0[w, (fg)^{-1}]$. Then by Lemma 3.1 and (3.1),

$$A \subseteq B, \quad \alpha_1, \ldots, \alpha_k \in B^*. \tag{3.6}$$

Define

$$\mathcal{H} := \Delta_{\mathcal{F}} \cdot \mathcal{F}_D \cdot fg,$$

where $\Delta_{\mathcal{F}}$ is the discriminant of $\mathcal{F}$. Clearly, $\mathcal{H} \in A_0$ and by Lemmas 3.1, 3.2, the additivity of the total degree and the 'almost additivity' of the logarithmic height for products of polynomials, we have

$$\deg \mathcal{H} \leq (k+1)(2\widehat{d}_3)^{\exp O(r)}, \quad h(\mathcal{H}) \leq (k+1)(2\widehat{d}_3)^{\exp O(r)}(\widehat{h}_3 + 1). \tag{3.7}$$

Any $\mathbf{u} = (u_1, \dots, u_q) \in \mathbb{Z}^q$ gives rise to a ring homomorphism $\varphi_{\mathbf{u}} : A_0 \to \mathbb{Z}$ by substituting u_i for z_i, for $i = 1, \dots, q$, and we write $a(\mathbf{u}) := \varphi_{\mathbf{u}}(a)$ for $a \in A_0$. We extend $\varphi_{\mathbf{u}}$ to B. Choose $\mathbf{u} \in \mathbb{Z}^q$ such that

$$\mathcal{H}(\mathbf{u}) \neq 0.$$

Let $\mathcal{F}_{\mathbf{u}} := X^D + \mathcal{F}_1(\mathbf{u})X^{D-1} + \cdots + \mathcal{F}_D(\mathbf{u})$. By our choice of $\mathbf{u}$, the polynomial $\mathcal{F}_{\mathbf{u}}$ has non-zero discriminant, hence it has D distinct roots, $w^{(1)}(\mathbf{u}), \dots, w^{(D)}(\mathbf{u}) \in \overline{\mathbb{Q}}$, which are all non-zero, since also $\mathcal{F}_D(\mathbf{u}) \neq 0$. Further, $f(\mathbf{u})g(\mathbf{u}) \neq 0$. Hence the substitutions

$$z_1 \mapsto u_1, \dots, z_q \mapsto u_q,\ w \mapsto w^{(j)}(\mathbf{u}) \quad (j = 1, \dots, D)$$

define ring homomorphisms $\varphi_{\mathbf{u}}^{(j)} : B \to \overline{\mathbb{Q}}$. We write $\alpha^{(j)}(\mathbf{u}) := \varphi_{\mathbf{u}}^{(j)}(\alpha)$ for $\alpha \in B$, $j = 1, \dots, D$. Notice that by (3.6) we have

$$\alpha_i^{(j)}(\mathbf{u}) \neq 0 \text{ for } i = 1, \dots, k,\ j = 1, \dots, D. \tag{3.8}$$

The image $\varphi_{\mathbf{u}}^{(j)}(B)$ is contained in the algebraic number field $K_{\mathbf{u}}^{(j)} := \mathbb{Q}(w^{(j)}(\mathbf{u}))$ and $[K_{\mathbf{u}}^{(j)} : \mathbb{Q}] \leq D \leq \widehat{d}_0^{\,r-q}$.

In the Lemma below, we denote by $h^{\mathrm{abs}}(\xi)$ the absolute logarithmic Weil height of $\xi \in \overline{\mathbb{Q}}$. For $\mathbf{u} = (u_1, \dots, u_q) \in \mathbb{Z}^q$ we write $|\mathbf{u}| := \max(|u_1|, \dots, |u_q|)$.

Lemma 3.4. *Let $\alpha \in B \setminus \{0\}$.*
(i) Let $\mathbf{u} \in \mathbb{Z}^q$ with $\mathcal{H}(\mathbf{u}) \neq 0$ and $j \in \{1, \dots, D\}$. Then

$$h^{\mathrm{abs}}(\alpha^{(j)})(\mathbf{u})) \leq C_1(\overline{\deg}\,\alpha, \overline{h}(\alpha), \mathbf{u}), \tag{3.9}$$

where $C_1(\overline{\deg}\,\alpha, \overline{h}(\alpha), \mathbf{u}) :=$

$$(2\widehat{d}_0)^{\exp O(r)}(\widehat{h}_0 + 1) + \overline{h}(\alpha) + \Big((2\widehat{d}_0)^{\exp O(r)} + q\overline{\deg}\,\alpha\Big) \log\max(1, |\mathbf{u}|).$$

(ii) There exist $\mathbf{u} \in \mathbb{Z}^q$, $j \in \{1, \dots, D\}$ such that

$$\begin{cases} |\mathbf{u}| \leq \max\big(\overline{\deg}\,\alpha, (2\widehat{d}_3)^{\exp O(r)}\big), \quad \mathcal{H}(\mathbf{u}) \neq 0, \\ \overline{h}(\alpha) \leq C_2\big(\overline{\deg}\,\alpha, h^{\mathrm{abs}}(\alpha^{(j)}(\mathbf{u}))\big) \end{cases} \tag{3.10}$$

where $C_2\big(\overline{\deg}\,\alpha, h^{\mathrm{abs}}(\alpha^{(j)}(\mathbf{u}))\big) :=$

$$(2\widehat{d}_3)^{\exp O(r)}\Big((k+1)^6(\widehat{h}_3 + 1)^2(\overline{\deg}\,\alpha)^4 + (k+1)(\widehat{h}_3 + 1)h^{\mathrm{abs}}(\alpha^{(j)}(\mathbf{u}))\Big).$$

Proof. This is a combination of Lemmas 5.6 and 5.7 from [8]. Observe that the quantities D, d_0 occurring in Lemmas 5.6 and 5.7 of [8], can be estimated from above by the upper bounds for D and $\deg \mathcal{F}_i$ $(i = 1, \dots, D)$

from Lemma 3.1 of the present paper, i.e., by $\widehat{d}_0^{r-q}$ and $(2\widehat{d}_0)^{\exp O(r)}$. The polynomial f from [8] corresponds to fg in the present paper. In [8], the degree and the logarithmic height of f are estimated from above by d_1, h_1. We have to replace these by the upper bounds for $\deg fg$, $h(fg)$ implied by (3.7) of the present paper. As a consequence, the lower bound for N in Lemma 5.7 of [8] is replaced by the upper bound for $|\mathbf{u}|$ in (3.10) of the present paper, while the upper bound for $\overline{h}(\alpha)$ in Lemma 5.7 of [8] is replaced by C_2 in the present paper. □

We now sketch briefly, how to obtain an upper bound for the sizes of representatives for solutions $x, y \in A$ of the Thue equation $F(x,y) = \delta$, where F is a binary form in $A[X,Y]$ of degree $n \geq 3$ with non-zero discriminant and where $\delta \in A \setminus \{0\}$.

Let $x, y \in A$ be a solution. Using Lemma 3.2 one obtains upper bounds for the $\overline{\deg}$-values and $\overline{h}$-values of the coefficients of F and of δ. Next, by means of Lemma 3.3 one obtains upper bounds for the $H_{M_i/\mathbf{k}_i}$-values of the coefficients of F and of δ and their conjugates over K_0. Using for instance effective results of Mason [16, Chapter 2] or Schmidt [20, Theorem 1, (ii)] for Thue equations over function fields, one can derive effective upper bounds for $H_{M_i/\mathbf{k}_i}(x^{(j)})$ and $H_{M_i/\mathbf{k}_i}(y^{(j)})$ for all i, j and subsequently, upper bounds for $\overline{\deg}\, x$, $\overline{\deg}\, y$ from our Lemma 3.3.

Next, let $\{\alpha_1, \dots, \alpha_k\}$ consist of the discriminant of F and of δ. Choose $\mathbf{u} \in \mathbb{Z}^q$, $j \in \{1, \dots, D\}$ such that $|\mathbf{u}| \leq \max\big(\overline{d}, (2\widehat{d}_3)^{\exp O(r)}\big)$, $\mathcal{H}(\mathbf{u}) \neq 0$, and subject to these conditions, $H := \max\big(h^{\text{abs}}(x^{(j)}(\mathbf{u})),\, h^{\text{abs}}(x^{(j)}(\mathbf{u}))\big)$ is maximal; here $\overline{d}$ is the maximum of the $\overline{\deg}$-values of x, y, the coefficients of F and δ. Let $F_{\mathbf{u}}^{(j)}$ be the binary form obtained by applying $\varphi_{\mathbf{u}}^{(j)}$ to the coefficients of F. By (3.8) and our choice of $\{\alpha_1, \dots, \alpha_k\}$, this binary form is of non-zero discriminant, and also $\delta^{(j)}(\mathbf{u}) \neq 0$.

Clearly, $F_{\mathbf{u}}^{(j)}\big(x^{(j)}(\mathbf{u}), y^{(j)}(\mathbf{u})\big) = \delta^{(j)}(\mathbf{u})$. Now we can apply an existing effective result for Thue equations over number fields (e.g, from Győry and Yu [13]) to obtain an effective upper bound for H. Inequality (3.10) then implies an effective upper bound for $\overline{h}(x)$, $\overline{h}(y)$. Finally, Lemma 3.2 gives effective upper bounds for the sizes of certain representatives for x, y.

Obviously, the same procedure applies to equations $F(x) = \delta y^m$. As for unit equations $ax + by = c$, one may apply the above procedure to systems of equations $ax + by = c$, $x \cdot x' = 1$, $y \cdot y' = 1$ in $x, y, x', y' \in A$.

References

[1] M. Aschenbrenner, *Ideal membership in polynomial rings over the integers*, J. Amer. Math. Soc. **17** (2004), 407–442.

[2] A. Baker, *Contributions to the theory of Diophantine equations*, Philos. Trans. Roy. Soc. London, Ser. A **263**, 173–208.

[3] A. Baker, Bounds for the solutions of the hyperelliptic equation, *Proc. Cambridge Philos. Soc.*, **65** (1969), 439–444.

[4] A. Bérczes, J.-H. Evertse and K. Győry, Effective results for Diophantine equations over finitely generated domains, submitted.

[5] B. Brindza, On S-integral solutions of the equation $y^m = f(x)$, *Acta Math. Hungar.*, **44** (1984), 133–139.

[6] B. Brindza, On the equation $f(x) = y^m$ over finitely generated domains, *Acta Math. Hungar.*, **53** (1989), 377–383.

[7] J. Coates, *An effective p-adic analogue of a theorem of Thue*, Acta Arith. **15** (1968/69), 279–305.

[8] J.-H. Evertse and K. Győry, Effective results for unit equations over finitely generated integral domains, *Math. Proc. Camb. Phil. Soc.*, **154** (2013), 351–380.

[9] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné* II, Publ. Math. Debrecen **21** (1974), 125–144.

[10] K. Győry, *On the number of solutions of linear equations in units of an algebraic number field*, Comment. Math. Helv. **54** (1979), 583–600.

[11] K. Győry, *Bounds for the solutions of norm form, discriminant form and index form equations in finitely generated domains*, Acta Math. Hung. **42** (1983), 45–80.

[12] K. Győry, *Effective finiteness theorems for polynomials with given discriminant and integral elements with given discriminant over finitely generated domains*, J. reine angew. Math. **346**, 54–100.

[13] K. Győry, Kunrui Yu, *Bounds for the solutions of S-unit equations and decomposable form equations*, Acta Arith. **123** (2006), 9–41.

[14] S. Lang, *Integral points on curves*, Inst. Hautes Études Sci. Publ. Math. **6** (1960), 27–43.

[15] K. Mahler, *Zur Approximation algebraischer Zahlen, I. (Über den größten Primteiler binärer Formen)*, Math. Ann. **107** (1933), 691–730.

[16] R. C. Mason, *Diophantine equations over function fields*, Cambridge University Press, 1984.

[17] C.J. Parry, *The* $\mathfrak{p}$*-adic generalisation of the Thue-Siegel theorem*, Acta Math. **83** (1950), 1–100.

[18] P. Roquette, *Einheiten und Divisorenklassen in endlich erzeugbaren Körpern*, Jber. Deutsch. Math. Verein **60** (1958), 1–21.

[19] A. Schinzel and R. Tijdeman, On the equation $y^m = P(x)$, *Acta Arith.*, **31** (1976), 199–204.
[20] W.M. Schmidt, *Thue's equation over function fields*, J. Austral. Math. Soc. Ser. A **25** (1978), 385–422.
[21] A. Seidenberg, *Constructions in algebra*, Trans. Amer. Math. Soc. **197** (1974), 273–313.
[22] C.L. Siegel, *Approximation algebraischer Zahlen*, Math. Zeitschrift **10** (1921), 173–213.
[23] C. L. Siegel, Über einige Anwendungen diophantischer Approximationen, *Preuss. Akad. Wiss., Phys.-math. Kl.*, **1** (1929), 70 pages.
[24] H. Simmons, *The solution of a decision problem for several classes of rings*, Pacific J. Math. **34** (1970), 547–557.
[25] V. G. Sprindžuk and S. V. Kotov, An effective analysis of the Thue-Mahler equation in relative fields (Russian), *Dokl. Akad. Nauk. BSSR*, **17** (1973), 393–395, 477.
[26] L. A. Trelina, S-integral solutions of Diophantine equations of hyperbolic type (in Russian), *Dokl. Akad. Nauk. BSSR*, **22** (1978), 881–884; 955.
[27] J. Végső, On superelliptic equations, *Publ. Math. Debrecen*, **44** (1994), 183–187.

J.-H. Evertse
Leiden University, Mathematical Institute,
P.O. Box 9512, 2300 RA Leiden, The Netherlands

E-mail address: evertse@math.leidenuniv.nl

K. Győry
Institute of Mathematics, University of Debrecen
Number Theory Research Group, Hungarian Academy of Sciences and University of Debrecen
H-4010 Debrecen, P.O. Box 12, Hungary

E-mail address: gyory@science.unideb.hu