

Effective results for Diophantine equations over finitely generated domains

by

ATTILA BÉRCZES (Debrecen), JAN-HENDRIK EVERTSE (Leiden)
and KÁLMÁN GYÖRY (Debrecen)

1. Introduction. Let A be an arbitrary integral domain of characteristic 0 that is finitely generated over \mathbb{Z} . We consider Thue equations $F(x, y) = \delta$ in $x, y \in A$, where F is a binary form with coefficients from A , and δ is a non-zero element from A , and hyper- and superelliptic equations $f(x) = \delta y^m$ in $x, y \in A$, where $f \in A[X]$, $\delta \in A \setminus \{0\}$ and $m \in \mathbb{Z}_{\geq 2}$.

Under the necessary finiteness conditions we give effective upper bounds for the sizes (defined in Section 2) of the solutions of the equations in terms of appropriate representations for A , δ , F , f , m . These results imply that the solutions of these equations can be determined in principle. Further, we consider the Schinzel–Tijdeman equation $f(x) = \delta y^m$ where $x, y \in A$ and $m \in \mathbb{Z}_{\geq 2}$ are the unknowns and give an effective upper bound for m .

We mention that results from the existing literature deal only with equations over restricted classes of finitely generated domains, whereas we do not have to impose any restrictions on A . Further, in this generality we give upper bounds for the sizes of the solutions x, y and m that are much more precise than those obtained in the special cases considered earlier. Our proofs are a combination of existing effective results for Thue equations and hyper- and superelliptic equations over number fields and over function fields, and a recent effective specialization method of Evertse and Györy [9].

We now give a brief overview of earlier results. A major breakthrough in the effective theory of Diophantine equations was made by A. Baker in the 1960's. Using his own estimates for linear forms in logarithms of algebraic numbers, he obtained effective finiteness results, i.e., with explicit upper bounds for the absolute values of the solutions, for Thue equations [2]

2010 *Mathematics Subject Classification*: 11D41, 11D59, 11D61.

Key words and phrases: Thue equations, hyperelliptic equations, superelliptic equations, Schinzel–Tijdeman equation, effective results, Diophantine equations over finitely generated domains.

and hyper- and superelliptic equations [3] over \mathbb{Z} . Schinzel and Tijdeman [17] 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 . Their proof also depends 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 larger integral domains; we mention here Coates [8], Sprindžuk and Kotov [20] (Thue equations over \mathcal{O}_S , where \mathcal{O}_S is the ring of S -integers of an algebraic number field), Trelina [22], Brindza [6] (hyper- and superelliptic equations over \mathcal{O}_S), Győry [11] (Thue equations over a restricted class of integral domains finitely generated over \mathbb{Z} that contain transcendental elements), Brindza [7] and Végső [23] (hyper- and superelliptic equations and the Schinzel–Tijdeman equation over the class of domains considered by Győry). These last mentioned works of Győry, Brindza and Végső were based on an effective specialization method developed by Győry in the 1980's [11], [12].

Recently, Evertse and Győry [9] extended Győry's specialization method so that it can now be used to prove effective results for Diophantine equations over arbitrary finitely generated domains A over \mathbb{Z} , without any further restriction on A whatsoever. They applied this to unit equations $ax + by = c$ in units x, y of A , and gave an effective upper bound for the sizes of the solutions x, y in terms of appropriate representations for A, a, b, c . In their method of proof, Evertse and Győry used existing effective results for S -unit equations over number fields and function fields, and combined these with their general specialization method.

The approach of Evertse and Győry can be applied to various other classes of Diophantine equations. In the present paper, we have worked out the consequences for Thue equations, hyper- and superelliptic equations, and Schinzel–Tijdeman equations.

2. Results. We first introduce the necessary notation and then state our results.

2.1. Notation. Let $A = \mathbb{Z}[z_1, \dots, z_r]$ be a finitely generated integral domain of characteristic 0. We assume that $r > 0$. We have

$$A \cong \mathbb{Z}[X_1, \dots, X_r]/I$$

where I is the ideal of polynomials $f \in \mathbb{Z}[X_1, \dots, X_r]$ such that $f(z_1, \dots, z_r) = 0$. The ideal I is finitely generated, say

$$I = (f_1, \dots, f_t).$$

We may view f_1, \dots, f_t as a representation for A . Recall that a necessary and sufficient condition for A to be a domain of characteristic 0 is that I be a prime ideal with $I \cap \mathbb{Z} = (0)$. Given a set of generators $\{f_1, \dots, f_t\}$ for I

this can be checked effectively (see for instance Aschenbrenner [1, Cor. 6.7, Lemma 6.1] but this follows already from work of Hermann [14]).

Denote by K the quotient field of A . For $\alpha \in A$, we call f a *representative* for α , or we say that f *represents* α , if $f \in \mathbb{Z}[X_1, \dots, X_r]$ and $\alpha = f(z_1, \dots, z_r)$. Further, for $\alpha \in K$ we call (f, g) a *representation pair* for α , or say that (f, g) *represents* α , if $f, g \in \mathbb{Z}[X_1, \dots, X_r]$, $g \notin I$ and $\alpha = f(z_1, \dots, z_r)/g(z_1, \dots, z_r)$.

Using an ideal membership algorithm for $\mathbb{Z}[X_1, \dots, X_r]$ (see e.g., Simmons [19], Aschenbrenner [1, Theorem A]), one can decide effectively whether two polynomials $f', f'' \in \mathbb{Z}[X_1, \dots, X_r]$ represent the same element of A , i.e., $f' - f'' \in I$, and whether two representation pairs $(f', g'), (f'', g'')$ in $\mathbb{Z}[X_1, \dots, X_r]$ represent the same element of K , i.e., $g' \notin I$, $g'' \notin I$ and $f'g'' - f''g' \in I$.

Given a non-zero polynomial $f \in \mathbb{Z}[X_1, \dots, X_r]$, we denote by $\deg f$ its total degree and by $h(f)$ its *logarithmic height*, that is, the logarithm of the maximum of the absolute values of its coefficients. Then the *size* of f is defined by

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

Further, we define $s(0) := 1$. It is clear that there are only finitely many polynomials in $\mathbb{Z}[X_1, \dots, X_r]$ of size below a given bound, and these can be determined effectively.

Throughout the paper we shall use $O(\cdot)$ to denote a quantity which is c times the expression between the parentheses, where c is an effectively computable positive absolute constant which may be different at each occurrence of the O -symbol. Further, throughout the paper we write

$$\log^* a := \max(1, \log a) \quad \text{for } a > 0, \quad \log^* 0 := 1.$$

2.2. Thue equations. We consider the Thue equation over A :

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

where

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

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 representatives

$$\tilde{a}_0, \tilde{a}_1, \dots, \tilde{a}_n, \tilde{\delta} \in \mathbb{Z}[X_1, \dots, X_r]$$

of $a_0, a_1, \dots, a_n, \delta$, respectively, where $\delta \notin I$, and the discriminant $D_{\tilde{F}}$ of $\tilde{F} := \sum_{j=0}^n \tilde{a}_j X^{n-j} Y^j$ is not in I . These conditions on $\tilde{a}_0, \tilde{a}_1, \dots, \tilde{a}_n, \tilde{\delta}$ can be checked by means of the ideal membership algorithm mentioned above. Let

$$(2.2) \quad \begin{cases} \max(\deg f_1, \dots, \deg f_t, \deg \tilde{a}_0, \deg \tilde{a}_1, \dots, \deg \tilde{a}_n, \deg \tilde{\delta}) \leq d, \\ \max(h(f_1), \dots, h(f_t), h(\tilde{a}_0), h(\tilde{a}_1), \dots, h(\tilde{a}_n), h(\tilde{\delta})) \leq h, \end{cases}$$

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

THEOREM 2.1. *Every solution x, y of equation (2.1) has representatives \tilde{x}, \tilde{y} such that*

$$(2.3) \quad s(\tilde{x}), s(\tilde{y}) \leq \exp(n!(nd)^{\exp O(r)}(h+1)).$$

The exponential dependence of the upper bound on $n!$, d and $h+1$ comes from a Baker-type effective result for Thue equations over number fields that is used in the proof. The bad dependence on r comes from the effective commutative algebra for polynomial rings over fields and over \mathbb{Z} , which is used in the specialization method of Evertse and Györy mentioned above.

We immediately deduce that equation (2.1) is effectively solvable:

COROLLARY 2.1. *There exists an algorithm which, for any given f_1, \dots, f_t such that A is a domain, and any representatives $\tilde{a}_0, \dots, \tilde{a}_n, \tilde{\delta}$ such that $D_{\tilde{F}}, \tilde{\delta} \notin I$, computes a finite list consisting of one pair of representatives for each solution (x, y) of (2.1).*

Proof. Let C be the upper bound from (2.3). Check for each pair of polynomials $\tilde{x}, \tilde{y} \in \mathbb{Z}[X_1, \dots, X_r]$ of size at most C whether $\tilde{F}(\tilde{x}, \tilde{y}) - \tilde{\delta} \in I$. Then for all pairs \tilde{x}, \tilde{y} passing this test, check whether they are equal modulo I , and keep a maximal subset of pairs that are pairwise different modulo I . ■

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

$$(2.4) \quad F(x) = \delta y^m \quad \text{in } x, y \in A,$$

where

$$F(X) = a_0 X^n + a_1 X^{n-1} + \dots + a_n \in A[X],$$

$\delta \in A \setminus \{0\}$ and $a_0 \neq 0$, $D_F \neq 0$. Thus, F is a polynomial of degree n without multiple roots. We represent (2.4) by representatives

$$\tilde{a}_0, \tilde{a}_1, \dots, \tilde{a}_n, \tilde{\delta} \in \mathbb{Z}[X_1, \dots, X_r]$$

for $a_0, a_1, \dots, a_n, \delta$, respectively, where $\tilde{\delta} \notin I$, $\tilde{a}_0 \notin I$, and the discriminant of $\tilde{F} := \sum_{j=0}^n \tilde{a}_j X^{n-j}$ is not in I . We assume that either $m = 2$ and $n \geq 3$, or $m \geq 3$ and $n \geq 2$. For $m = 2$, equation (2.4) is called a *hyperelliptic equation*, while for $m \geq 3$ it is called a *superelliptic equation*. Let

$$(2.5) \quad \begin{cases} \max(\deg f_1, \dots, \deg f_t, \deg \tilde{a}_0, \deg \tilde{a}_1, \dots, \deg \tilde{a}_n, \deg \tilde{\delta}) \leq d, \\ \max(h(f_1), \dots, h(f_t), h(\tilde{a}_0), h(\tilde{a}_1), \dots, h(\tilde{a}_n), h(\tilde{\delta})) \leq h, \end{cases}$$

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

THEOREM 2.2. *Every solution x, y of equation (2.4) has representatives \tilde{x}, \tilde{y} such that*

$$(2.6) \quad s(\tilde{x}), s(\tilde{y}) \leq \exp(m^3(nd)^{\exp O(r)}(h+1)).$$

Completely similarly to the case of Thue equations, one can determine effectively a finite list consisting of one pair of representatives for each solution (x, y) of (2.4).

Our next result deals with the Schinzel–Tijdeman equation, which is (2.4) but with three unknowns $x, y \in A$ and $m \in \mathbb{Z}_{\geq 2}$.

THEOREM 2.3. *Assume that in (2.4), F has non-zero discriminant and $n \geq 2$. Let $x, y \in A$, $m \in \mathbb{Z}_{\geq 2}$ be a solution of (2.4). Then*

$$(2.7) \quad m \leq \exp((nd)^{\exp O(r)}(h+1))$$

$$(2.8) \quad m \leq (nd)^{\exp O(r)} \quad \begin{array}{l} \text{if } y \in \overline{\mathbb{Q}}, y \neq 0, y \text{ is not a root of unity,} \\ \text{if } y \notin \overline{\mathbb{Q}}. \end{array}$$

3. A reduction. We shall reduce our equations to equations of the same type over an integral domain $B \supseteq A$ of a special type which is more convenient to deal with.

As before, let $A = \mathbb{Z}[z_1, \dots, z_r]$ be an integral domain which is finitely generated over \mathbb{Z} and let K be the quotient field of A . Suppose that K has transcendence degree $q \geq 0$. If $q > 0$, we assume without loss of generality that $\{z_1, \dots, z_q\}$ is a transcendence basis of K/\mathbb{Q} . Write $\rho := r - q$. We define

$$\begin{array}{ll} A_0 := \mathbb{Z}[z_1, \dots, z_q], & K_0 := \mathbb{Q}(z_1, \dots, z_q) \quad \text{if } q > 0, \\ A_0 := \mathbb{Z}, & K_0 := \mathbb{Q} \quad \text{if } q = 0. \end{array}$$

The field K is a finite extension of K_0 . Further, if $q = 0$, it is an algebraic number field. In the case that $q > 0$, for $f \in A_0 \setminus \{0\}$ we define $\deg f$ and $h(f)$ to be the total degree and logarithmic height of f , viewed as a polynomial in the variables z_1, \dots, z_q . In the case that $q = 0$, for $f \in A_0 \setminus \{0\} = \mathbb{Z} \setminus \{0\}$, we put $\deg f := 0$ and $h(f) := \log |f|$.

We shall construct an integral extension B of A in K such that

$$(3.1) \quad B := A_0[w, g^{-1}],$$

where $g \in A_0 \setminus \{0\}$ and w is a primitive element of K over K_0 that is integral over A_0 . Then we give a bound for the sizes of the solutions of our equations in $x, y \in B$.

We recall that $A \cong \mathbb{Z}[X_1, \dots, X_r]/I$, where $I \subset \mathbb{Z}[X_1, \dots, X_r]$ is the ideal of polynomials f with $f(z_1, \dots, z_r) = 0$ and z_i corresponds to the residue class of X_i modulo I . The ideal I is finitely generated. Assume that

$$I = (f_1, \dots, f_t),$$

and put

$$(3.2) \quad d_0 := \max(1, \deg f_1, \dots, \deg f_t), \quad h_0 := \max(1, h(f_1), \dots, h(f_t)).$$

PROPOSITION 3.1.

- (i) *There is a $w \in A$ such that $K = K_0(w)$, w is integral over A_0 and w 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 that $D \leq d_0^p$ and

$$(3.3) \quad \deg \mathcal{F}_k \leq (2d_0)^{\exp O(r)}, \quad h(\mathcal{F}_k) \leq (2d_0)^{\exp O(r)}(h_0 + 1)$$

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

- (ii) *Let $\alpha_1, \dots, \alpha_k \in K^*$ and suppose that the pairs $u_i, v_i \in \mathbb{Z}[X_1, \dots, X_r]$, $v_i \notin I$, represent α_i for $i = 1, \dots, k$. Put*

$$\begin{aligned} d^{**} &:= \max(d_0, \deg u_1, \deg v_1, \dots, \deg u_k, \deg v_k), \\ h^{**} &:= \max(h_0, h(u_1), h(v_1), \dots, h(u_k), h(v_k)). \end{aligned}$$

Then there is a non-zero $g \in A_0$ such that

$$(3.4) \quad A \subseteq A_0[w, g^{-1}], \quad \alpha_1, \dots, \alpha_k \in A_0[w, g^{-1}]^*$$

and

$$(3.5) \quad \deg g \leq (k+1)(2d^{**})^{\exp O(r)}, \quad h(g) \leq (k+1)(2d^{**})^{\exp O(r)}(h^{**} + 1).$$

Proof. For (i) see Evertse and Györy [9, Corollary 3.4 and Lemma 3.2(i)], and for (ii) see [9, Lemma 3.6]. ■

We shall use Proposition 3.1(ii) in a special case. To state it, we introduce some further notation and prove a lemma.

We recall that $a_0, a_1, \dots, a_n \in A$ are the coefficients of the binary form $F(X, Y)$, resp. of the polynomial $F(X)$, in Section 2.2, resp. 2.3, and $\tilde{a}_0, \tilde{a}_1, \dots, \tilde{a}_n$ denote their representatives satisfying (2.2), resp. (2.5). This implies that $d_0 \leq d, h_0 \leq h$, and that \tilde{a}_i has total degree $\leq d$ and logarithmic height $\leq h$ for $i = 0, \dots, n$. Denote by \tilde{F} the binary form $F(X, Y)$, resp. the polynomial $F(X)$, with coefficients a_0, a_1, \dots, a_n replaced by $\tilde{a}_0, \tilde{a}_1, \dots, \tilde{a}_n$, and by $D_{\tilde{F}}$ the discriminant of \tilde{F} . In view of the assumption $D_F \neq 0$, we have $D_{\tilde{F}} \notin I$.

Keeping the notation and assumptions of Sections 2.2 and 2.3, we have the following lemma.

LEMMA 3.2. *For the discriminant $D_{\tilde{F}}$ the following statements are true:*

$$(3.6) \quad \deg D_{\tilde{F}} \leq (2n - 2)d,$$

$$(3.7) \quad h(D_{\tilde{F}}) \leq (2n - 2) \left(\log \left(2n^2 \binom{d+r}{r} \right) + h \right).$$

In the case $q > 0$, z_1, \dots, z_q are algebraically independent. Thus, for $q \geq 0$, A_0 is a unique factorization domain, and hence the greatest common divisor of a finite set of elements of A_0 is well defined and uniquely determined up to sign. We associate with every element $\alpha \in K$ the unique (up to sign) tuple $P_{\alpha,0}, \dots, P_{\alpha,D-1}, Q_\alpha$ of elements of A_0 such that

$$(3.11) \quad \alpha = Q_\alpha^{-1} \sum_{j=0}^{D-1} P_{\alpha,j} w^j \quad \text{with } Q_\alpha \neq 0, \gcd(P_{\alpha,0}, \dots, P_{\alpha,D-1}, Q_\alpha) = 1.$$

We put

$$(3.12) \quad \begin{cases} \overline{\deg} \alpha := \max(\deg P_{\alpha,0}, \dots, \deg P_{\alpha,D-1}, \deg Q_\alpha), \\ \bar{h}(\alpha) := \max(h(P_{\alpha,0}), \dots, h(P_{\alpha,D-1}), h(Q_\alpha)), \end{cases}$$

where as usual, $\deg P$, $h(P)$ denote the total degree and logarithmic height of a polynomial P with rational integral coefficients. Thus for $q = 0$ we have $\overline{\deg} \alpha = 0$ and $\bar{h}(\alpha) = \log \max(|P_{\alpha,0}|, \dots, |P_{\alpha,D-1}|, |Q_\alpha|)$.

LEMMA 3.4 ([9, Lemma 3.5]). *Let $\alpha \in K^*$ and let (a, b) be a representation pair for α with $a, b \in \mathbb{Z}[X_1, \dots, X_r]$, $b \notin I$. Put*

$$d^* = \max(d_0, \deg a, \deg b) \quad \text{and} \quad h^* := \max(h_0, h(a), h(b)),$$

where d_0, h_0 are defined by (3.2). Then

$$(3.13) \quad \overline{\deg} \alpha \leq (2d^*)^{\exp O(r)}, \quad \bar{h}(\alpha) \leq (2d^*)^{\exp O(r)} (h^* + 1).$$

LEMMA 3.5. *Let α be a non-zero element of A , and put*

$$\widehat{d} := \max(d_0, \overline{\deg} \alpha), \quad \widehat{h} := \max(h_0, \bar{h}(\alpha)).$$

Then α has a representative $\tilde{\alpha} \in \mathbb{Z}[X_1, \dots, X_r]$ such that

$$(3.14) \quad \begin{cases} \deg \tilde{\alpha} \leq (2\widehat{d})^{\exp O(r \log^* r)} (\widehat{h} + 1), \\ h(\tilde{\alpha}) \leq (2\widehat{d})^{\exp O(r \log^* r)} (\widehat{h} + 1)^{r+1}. \end{cases}$$

Proof. This is a special case of Lemma 3.7 of Evertse and Györy [9] with the choice $\lambda = 1$ and $a = b = 1$. The proof of this lemma is based on work of Aschenbrenner [1]. ■

3.1. Thue equations. Recall that $A_0 = \mathbb{Z}[z_1, \dots, z_q]$, $K_0 = \mathbb{Q}(z_1, \dots, z_q)$ if $q > 0$, and $A_0 = \mathbb{Z}$, $K_0 = \mathbb{Q}$ if $q = 0$, and that in the case $q = 0$ the total degrees and \deg 's are always zero. Further, we have

$$F(X, Y) = a_0 X^n + a_1 X^{n-1} Y + \dots + a_n Y^n \in A[X, Y]$$

with $n \geq 3$ and $D_F \neq 0$, and $\delta \in A \setminus \{0\}$. Recall that for $a_0, a_1, \dots, a_n, \delta$ we have chosen representatives $\tilde{a}_0, \tilde{a}_1, \dots, \tilde{a}_n, \tilde{\delta} \in \mathbb{Z}[X_1, \dots, X_r]$ satisfying (2.2).

Theorem 2.1 will be deduced from the following proposition, which makes sense also if $q = 0$. The proof of this proposition is given in Sections 4–6.

PROPOSITION 3.6. *Let w and g be as in Propositions 3.1(i) and 3.3, respectively, with the properties specified there, and consider the integral domain*

$$B := A_0[w, g^{-1}].$$

Then for the solutions x, y of the equation

$$(3.15) \quad F(x, y) = \delta \quad \text{in } x, y \in B$$

we have

$$(3.16) \quad \overline{\deg} x, \overline{\deg} y \leq (nd)^{\exp O(r)},$$

$$(3.17) \quad \bar{h}(x), \bar{h}(y) \leq \exp(n!(nd)^{\exp O(r)}(h + 1)).$$

We now deduce Theorem 2.1 from Proposition 3.6.

Proof of Theorem 2.1. Let x, y be a solution of equation (2.1). In view of (3.9), x, y is also a solution in $B = A_0[w, g^{-1}]$, where g, w have the properties specified in Propositions 3.1(i) and 3.3, respectively. Then by Proposition 3.6, the inequalities (3.16) and (3.17) hold. Applying now Lemma 3.5 to x and y , we infer that x, y have representatives \tilde{x}, \tilde{y} in $\mathbb{Z}[X_1, \dots, X_r]$ which satisfy (2.3). ■

3.2. Hyper- and superelliptic equations. Recall that the polynomial

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

has discriminant $D_F \neq 0$, that $\delta \in A \setminus \{0\}$, and that for $a_0, a_1, \dots, a_n, \delta$ we have chosen representatives $\tilde{a}_0, \tilde{a}_1, \dots, \tilde{a}_n, \tilde{\delta} \in \mathbb{Z}[X_1, \dots, X_r]$ satisfying (2.5).

Theorem 2.2 will be deduced from the following proposition, which has a meaning also if $q = 0$. Similarly to its analogue for Thue equations, its proof is given in Sections 4–6.

PROPOSITION 3.7. *Let w and g be as in Propositions 3.1(i) and 3.3, respectively, with the properties specified there, and consider the domain*

$$B := A_0[w, g^{-1}].$$

Further, let m be an integer ≥ 2 , and assume that $n \geq 3$ if $m = 2$ and $n \geq 2$ if $m \geq 3$. Then for the solutions x, y of the equation

$$(3.18) \quad F(x) = \delta y^m \quad \text{in } x, y \in B$$

we have

$$(3.19) \quad \overline{\deg} x, \overline{\deg} y \leq (nd)^{\exp O(r)},$$

$$(3.20) \quad m \leq (nd)^{\exp(r)} \quad \text{if } y \notin \overline{\mathbb{Q}},$$

$$(3.21) \quad \bar{h}(x), \bar{h}(y) \leq \exp(m^3(nd)^{\exp O(r)}(h + 1)).$$

We now deduce Theorem 2.2 from Proposition 3.7.

Proof of Theorem 2.2. Let x, y be a solution of equation (2.4). In view of (3.9), x, y is also a solution in $B = A_0[w, g^{-1}]$, where g, w satisfy the conditions specified in Propositions 3.1(i) and 3.3, respectively. Then by Proposition 3.7, the inequalities (3.19) and (3.21) hold. Applying now Lemma 3.5 to x and y , we infer that x, y have representatives \tilde{x}, \tilde{y} in $\mathbb{Z}[X_1, \dots, X_r]$ satisfying (2.6). ■

PROPOSITION 3.8. *Suppose that equation (3.18) has a solution $x \in B$, $y \in B \cap \overline{\mathbb{Q}}$ and that also $y \neq 0$ and y is not a root of unity. Then*

$$(3.22) \quad m \leq \exp((nd)^{\exp O(r)}(h+1)).$$

The proof of Proposition 3.8 is a combination of results from Sections 4–6. It is completed at the end of Section 6.

Proof of Theorem 2.3. Immediate from (3.20) and (3.22). ■

4. Bounding the degree. In this section we prove (3.16) of Proposition 3.6 and (3.19) of Proposition 3.7.

We first recall some results on function fields in one variable. Let \mathbb{k} be an algebraically closed field of characteristic 0, z a transcendental element over \mathbb{k} and M a finite extension of $\mathbb{k}(z)$. Denote by $g_{M/\mathbb{k}}$ the genus of M , and by \mathcal{M}_M the collection of valuations of M/\mathbb{k} ; these are the discrete valuations of M with value group \mathbb{Z} that are trivial on \mathbb{k} . Recall that these valuations satisfy the sum formula

$$\sum_{v \in \mathcal{M}_M} v(\alpha) = 0 \quad \text{for } \alpha \in M^*.$$

For a finite subset S of \mathcal{M}_M , an element $\alpha \in M$ is called an S -integer if $v(\alpha) \geq 0$ for all $v \in \mathcal{M}_M \setminus S$. The S -integers form a ring in M , denoted by \mathcal{O}_S . The (homogeneous) *height* of $\mathbf{a} = (\alpha_1, \dots, \alpha_l) \in M^l$ relative to M/\mathbb{k} is defined by

$$H_M(\mathbf{a}) = H_M(\alpha_1, \dots, \alpha_l) := - \sum_{v \in \mathcal{M}_M} \min(v(\alpha_1), \dots, v(\alpha_l)),$$

and we define the height $H_M(f)$ of a polynomial $f \in M[X]$ to be the height of the vector defined by the coefficients of f . Further, we shall write $H_M(1, \mathbf{a}) := H_M(1, \alpha_1, \dots, \alpha_l)$. We note that

$$(4.1) \quad H_M(\alpha_i) \leq H_M(\mathbf{a}) \leq H_M(\alpha_1) + \dots + H_M(\alpha_l), \quad i = 1, \dots, l.$$

By the sum formula,

$$(4.2) \quad H_M(\alpha \mathbf{a}) = H_M(\mathbf{a}) \quad \text{for } \alpha \in M^*.$$

The height of $\alpha \in M$ relative to M/\mathbb{k} is defined by

$$H_M(\alpha) := H_M(1, \alpha) = - \sum_{v \in \mathcal{M}_M} \min(0, v(\alpha)).$$

It is clear that $H_M(\alpha) = 0$ if and only if $\alpha \in \mathbb{k}$. Using the sum formula, it is easy to prove that the height has the properties

$$(4.3) \quad \begin{aligned} H_M(\alpha^l) &= |l|H_M(\alpha), \\ H_M(\alpha + \beta) &\leq H_M(\alpha) + H_M(\beta), \quad H_M(\alpha\beta) \leq H_M(\alpha) + H_M(\beta) \end{aligned}$$

for all non-zero $\alpha, \beta \in M$ and for every integer l .

If L is a finite extension of M , we have

$$(4.4) \quad H_L(\alpha_0, \dots, \alpha_l) = [L : M]H_M(\alpha_0, \dots, \alpha_l) \quad \text{for } \alpha_0, \dots, \alpha_l \in M.$$

By $\deg f$ we denote the total degree of $f \in \mathbb{k}[z]$. Then for $f_0, \dots, f_l \in \mathbb{k}[z]$ with $\gcd(f_0, \dots, f_l) = 1$ we have

$$(4.5) \quad H_{\mathbb{k}[z]}(f_0, \dots, f_l) = \max(\deg f_0, \dots, \deg f_l).$$

LEMMA 4.1 ([9, Lemma 4.1]). *Let $\alpha_1, \dots, \alpha_l \in M$ and suppose that*

$$X^l + f_1 X^{l-1} + \dots + f_l = (X - \alpha_1) \dots (X - \alpha_l)$$

for certain $f_1, \dots, f_l \in \mathbb{k}[z]$. Then

$$[M : \mathbb{k}(z)] \max(\deg f_1, \dots, \deg f_l) = \sum_{i=1}^l H_M(\alpha_i).$$

LEMMA 4.2. *Let*

$$F = f_0 X^l + f_1 X^{l-1} + \dots + f_l \in M[X]$$

be a polynomial with $f_0 \neq 0$ and with non-zero discriminant. Let L be the splitting field over M of F . Then

$$g_{L/\mathbb{k}} \leq [L : M] \cdot (g_{M/\mathbb{k}} + lH_M(F)).$$

In particular, if $M = \mathbb{k}(z)$ and $f_0, \dots, f_l \in \mathbb{k}[z]$, we have

$$g_{L/\mathbb{k}} \leq [L : M] \cdot l \max(\deg f_0, \dots, \deg f_l).$$

Proof. The second assertion follows by combining the first assertion with (4.5). We now prove the first assertion. Our proof is a generalization of that of Lemma H of Schmidt [18].

For $v \in \mathcal{M}_M$, put $v(F) := \min(v(f_0), \dots, v(f_l))$. Let D_F denote the discriminant of F . Since D_F is a homogeneous polynomial of degree $2l - 2$ in f_0, \dots, f_l , we have

$$(4.6) \quad v(D_F) \geq (2l - 2)v(F).$$

Let S be the set of $v \in \mathcal{M}_M$ with $v(f_0) > v(F)$ or $v(D_F) > (2l - 2)v(F)$. We show that L/M is unramified over every valuation $v \in \mathcal{M}_M \setminus S$.

Take $v \in \mathcal{M}_M \setminus S$. Let

$$O_v := \{x \in M : v(x) \geq 0\}, \quad m_v := \{x \in M : v(x) > 0\}$$

denote the local ring at v , and the maximal ideal of O_v , respectively. The residue class field O_v/m_v is equal to \mathbb{k} since \mathbb{k} is algebraically closed. Let $\varphi_v : O_v \rightarrow \mathbb{k}$ denote the canonical homomorphism.

Without loss of generality, we assume $v(F) = 0$. Then $v(f_0) = 0$, $v(D_F) = 0$. Let $\varphi_v(F) := \sum_{j=0}^l \varphi_v(f_j)X^{l-j}$. Then $\varphi_v(f_0) \neq 0$ and $\varphi_v(F)$ has discriminant $\varphi_v(D_F) \neq 0$. Since $D_F \neq 0$, the polynomial F has l distinct zeros in L , say $\alpha_1, \dots, \alpha_l$. Further, $\varphi_v(F)$ has l distinct zeros in \mathbb{k} , say a_1, \dots, a_l .

Denote by Σ_l the permutation group on $(1, \dots, l)$. Choose $c_1, \dots, c_l \in \mathbb{k}$, such that the numbers

$$\alpha_\sigma := c_1\alpha_{\sigma(1)} + \dots + c_l\alpha_{\sigma(l)} \quad (\sigma \in \Sigma_l)$$

are all distinct, and the numbers

$$a_\sigma := c_1a_{\sigma(1)} + \dots + c_la_{\sigma(l)} \quad (\sigma \in \Sigma_l)$$

are all distinct. Let $\alpha := c_1\alpha_1 + \dots + c_l\alpha_l$. Then $L = M(\alpha)$, and the monic minimal polynomial of α over M divides $G := \prod_{\sigma \in \Sigma_l} (X - \alpha_\sigma)$, which by the theorem of symmetric functions belongs to $M[X]$. The image of G under φ_v is $\prod_{\sigma \in \Sigma_l} (X - a_\sigma)$ and this has only simple zeros. Therefore L/M is unramified at v .

For $v \in \mathcal{M}_M$ and any valuation $V \in \mathcal{M}_L$ above v , denote by $e(V|v)$ the ramification index of V over v . Recall that $\sum_{V|v} e(V|v) = [L : M]$, where the sum is taken over all valuations of L lying above v . Now the Riemann–Hurwitz formula implies that

$$(4.7) \quad 2g_{L/\mathbb{k}} - 2 = [L : M](2g_{M/\mathbb{k}} - 2) + \sum_{v \in S} \sum_{V|v} (e(V|v) - 1) \\ \leq [L : M](2g_{M/\mathbb{k}} - 2 + |S|),$$

where $|S|$ denotes the cardinality of S . It remains to estimate $|S|$. By the sum formula and (4.6) we have

$$|S| \leq \sum_{v \in S} ((v(f_0) - v(F)) + (v(D_F) - (2l - 2)v(F))) \\ = - \sum_{v \in S} (2l - 1)v(F) - \sum_{v \in \mathcal{M}_M \setminus S} v(f_0) - \sum_{v \in \mathcal{M}_M \setminus S} v(D_F) \\ \leq -(2l - 1) \sum_{v \in \mathcal{M}_M} v(F) = (2l - 1)H_M(F).$$

By inserting this into (4.7) we arrive at an inequality which is stronger than what we wanted to prove. ■

In what follows, we keep the notation of Proposition 3.1. To prove (3.16) and (3.19) we may suppose that $q > 0$ since the case $q = 0$ is trivial. Let again $K_0 := \mathbb{Q}(z_1, \dots, z_q)$, $K := K_0(w)$, $A_0 := \mathbb{Z}[z_1, \dots, z_q]$, $B := \mathbb{Z}[z_1, \dots, z_q, w, g^{-1}]$ with g, w specified in Propositions 3.1(i) and 3.3.

Fix $i \in \{1, \dots, q\}$. Let $\mathbb{k}_i := \mathbb{Q}(z_1, \dots, z_{i-1}, z_{i+1}, \dots, z_q)$ and $\overline{\mathbb{k}}_i$ be its algebraic closure. Then A_0 is contained in $\overline{\mathbb{k}}_i[z_i]$. Denote by $w^{(1)} := w, \dots, w^{(D)}$ the conjugates of w over K_0 . Let M_i denote the splitting field of the polynomial $X^D + \mathcal{F}_1 X^{D-1} + \dots + \mathcal{F}_D$ over $\overline{\mathbb{k}}_i(z_i)$, that is,

$$M_i := \overline{\mathbb{k}}_i(z_i, w^{(1)}, \dots, w^{(D)}).$$

Then

$$B_i := \overline{\mathbb{k}}_i[z_i, g^{-1}, w^{(1)}, \dots, w^{(D)}]$$

is a subring of M_i which contains $B = \mathbb{Z}[z_1, \dots, z_q, w, g^{-1}]$ as a subring. Let $\Delta_i := [M_i : \overline{\mathbb{k}}_i(z_i)]$. Further, let g_{M_i} denote the genus of $M_i/\overline{\mathbb{k}}_i$, and H_{M_i} the height taken with respect to $M_i/\overline{\mathbb{k}}_i$. Put

$$(4.8) \quad d_1 := \max(d_0, \deg f, \deg \mathcal{F}_1, \dots, \deg \mathcal{F}_D).$$

We mention that in view of Propositions 3.1 and 3.3,

$$(4.9) \quad d_1 \leq (nd)^{\exp O(r)}.$$

LEMMA 4.3 ([9, Lemma 4.4]). *Let $\alpha \in K^*$ and denote by $\alpha^{(1)}, \dots, \alpha^{(D)}$ the conjugates of α corresponding to $w^{(1)}, \dots, w^{(D)}$. Then*

$$\overline{\deg} \alpha \leq qDd_1 + \sum_{i=1}^q \Delta_i^{-1} \sum_{j=1}^D H_{M_i}(\alpha^{(j)}).$$

Conversely, we have the following:

LEMMA 4.4. *Let $\alpha \in K^*$ and $\alpha^{(1)}, \dots, \alpha^{(D)}$ be as in Lemma 4.3. Then*

$$(4.10) \quad \max_{i,j} H_{M_i}(\alpha^{(j)}) \leq \Delta_i(2D \overline{\deg} \alpha + (2d_0)^{\exp O(r)}).$$

Proof. Consider the representation of α of the form (3.11). Since $P_{\alpha,k}$ and Q are in K_0 , we have

$$\alpha^{(j)} = \sum_{k=0}^{D-1} \frac{P_{\alpha,k}}{Q} (w^{(j)})^k \quad \text{for } j = 1, \dots, D.$$

In view of (4.3) it follows that

$$(4.11) \quad H_{M_i}(\alpha^{(j)}) \leq \sum_{k=0}^{D-1} H_{M_i} \left(\frac{P_{\alpha,k}}{Q} \right) + \sum_{k=0}^{D-1} k H_{M_i}(w^{(j)}).$$

But we have

$$(4.12) \quad \begin{aligned} H_{M_i} \left(\frac{P_{\alpha,k}}{Q} \right) &\leq \Delta_i H_{\mathbb{k}_i(z)} \left(\frac{P_{\alpha,k}}{Q} \right) \leq \Delta_i (\deg_{z_i} P_{\alpha,k} + \deg_{z_i} Q) \\ &\leq \Delta_i (\deg P_{\alpha,k} + \deg Q) \leq 2\Delta_i \overline{\deg} \alpha. \end{aligned}$$

Further, applying Lemma 4.1 with $M_i, w^{(1)}, \dots, w^{(D)}$ instead of $M, \alpha_1, \dots, \alpha_l$, we get

$$(4.13) \quad H_{M_i}(w^{(j)}) \leq \Delta_i \max_{1 \leq j \leq D} (\deg_{z_i} \mathcal{F}_j) \leq \Delta_i \max_{1 \leq j \leq D} (\deg \mathcal{F}_j) \leq \Delta_i (2d_0)^{\exp O(r)}.$$

Now using the fact that $D \leq d_0^2 \leq d_0^{r-1}$ and (4.11)–(4.13), we have (4.10). ■

4.1. Thue equations. As before, \mathbb{k} is an algebraically closed field of characteristic 0, z a transcendental element over \mathbb{k} and M a finite extension of $\mathbb{k}(z)$. Further, $g_{M/\mathbb{k}}$ denotes the genus of M , \mathcal{M}_M the collection of valuations of M/\mathbb{k} , and for a finite subset S of \mathcal{M}_M , \mathcal{O}_S denotes the ring of S -integers in M . We denote by $|S|$ the cardinality of S .

Consider now the Thue equation

$$(4.14) \quad F(x, y) = 1 \quad \text{in } x, y \in \mathcal{O}_S,$$

where F is a binary form of degree $n \geq 3$ with coefficients in M and with non-zero discriminant.

PROPOSITION 4.5 ([18, Theorem 1(ii)]). *Every solution $x, y \in \mathcal{O}_S$ of (4.14) satisfies*

$$(4.15) \quad \max(H_M(x), H_M(y)) \leq 89H_M(F) + 212g_{M/\mathbb{k}} + |S| - 1.$$

We note that from Mason's fundamental inequality concerning S -unit equations over function fields (see Mason [16]) one could deduce (4.15) with smaller constants than 89 and 212. However, this is irrelevant for the bounds in (2.3).

Now we use Proposition 4.5 to prove (3.16) of Proposition 3.6.

Proof of (3.16). We denote by $w^{(1)} := w, \dots, w^{(D)}$ the conjugates of w over K_0 , and for $\alpha \in K$ we denote by $\alpha^{(1)}, \dots, \alpha^{(D)}$ the conjugates of α corresponding to $w^{(1)}, \dots, w^{(D)}$.

Next, for $i = 1, \dots, q$ we put $\mathbb{k}_i := \mathbb{Q}(z_1, \dots, z_{i-1}, z_{i+1}, \dots, z_q)$ and denote by $\overline{\mathbb{k}}_i$ its algebraic closure. Further, M_i denotes the splitting field of the polynomial $X^D + \mathcal{F}_1 X^{D-1} + \dots + \mathcal{F}_D$ over $\overline{\mathbb{k}}_i(z_i)$. We put $\Delta_i := [M_i : \overline{\mathbb{k}}_i(z_i)]$ and define

$$S_i := \{v \in \mathcal{M}_{M_i} : v(z_i) < 0 \text{ or } v(g) > 0\}.$$

The conjugates $w^{(j)}$ ($j = 1, \dots, D$) lie in M_i and are all integral over $\mathbb{k}_i[z_i]$. Hence they belong to \mathcal{O}_{S_i} . Further, $g^{-1} \in \mathcal{O}_{S_i}$. Consequently, if $\alpha \in B = A_0[w, g^{-1}]$, then $\alpha^{(j)} \in \mathcal{O}_{S_i}$ for $j = 1, \dots, D$, $i = 1, \dots, q$.

Let x, y be a solution of equation (3.15). Put $F' := \delta^{-1}F$, and let $F'^{(j)}$ be the binary form obtained by taking the j th conjugates of the coefficients of F' . Let $j \in \{1, \dots, D\}$, $i \in \{1, \dots, q\}$. Then clearly $F'^{(j)} \in M_i[X, Y]$, and

$$F'^{(j)}(x^{(j)}, y^{(j)}) = 1, \quad x^{(j)}, y^{(j)} \in \mathcal{O}_{S_i}.$$

So by Proposition 4.5 we obtain

$$(4.16) \quad \max(H_{M_i}(x^{(j)}), H_{M_i}(y^{(j)})) \leq 89H_{M_i}(F'^{(j)}) + 212g_{M_i} + |S_i| - 1.$$

We estimate the various parameters in this bound. We start with $H_{M_i}(F'^{(j)})$. We recall that $F'(X, Y) = \delta^{-1}(a_0X^n + a_1X^{n-1}Y + \dots + a_nY^n)$. Using (4.2), (4.1) and Lemma 4.4 we infer that

$$\begin{aligned} H_{M_i}(F'^{(j)}) &= H_{M_i}(a_0^{(j)}, \dots, a_n^{(j)}) \leq H_{M_i}(a_0^{(j)}) + \dots + H_{M_i}(a_n^{(j)}) \\ &\leq \Delta_i(2D(\overline{\deg} a_0 + \dots + \overline{\deg} a_n) + n(2d_0)^{\exp O(r)}). \end{aligned}$$

By Lemma 3.4 we have

$$\overline{\deg} a_i \leq (2d^*)^{\exp O(r)} \quad \text{for } i = 0, \dots, n,$$

where $d^* := \max(d_0, \deg \tilde{a}_i) \leq d$. Further, we have $d_0 \leq d$, $D \leq d_0^{r-q} \leq d^r$. Thus

$$(4.17) \quad \begin{aligned} H_{M_i}(F'^{(j)}) &\leq \Delta_i(2D(n+1)(2d)^{\exp O(r)} + n(2d)^{\exp O(r)}) \\ &\leq \Delta_i(nd)^{\exp O(r)}. \end{aligned}$$

Next, we estimate the genus. Using Lemma 4.2 with $F(X) = \mathcal{F}(X) = X^D + \mathcal{F}_1X^{D-1} + \dots + \mathcal{F}_D$, applying Proposition 3.1, and using $d_0 \leq d$, $D \leq d_0^r \leq d^r$, we infer that

$$(4.18) \quad g_{M_i} \leq \Delta_i D \max_{1 \leq k \leq D} \deg_{z_i} \mathcal{F}_k \leq \Delta_i D(2d_0)^{\exp O(r)} \leq \Delta_i(nd)^{\exp O(r)}.$$

Lastly, we estimate $|S_i|$. Each valuation of $\overline{\mathbb{k}}_i(z_i)$ can be extended to at most $[M_i : \overline{\mathbb{k}}_i(z_i)] = \Delta_i$ valuations of M_i . Thus M_i has at most Δ_i valuations v with $v(z_i) < 0$ and at most $\Delta_i \deg f$ valuations v with $v(f) > 0$. Hence, using Proposition 3.3, we get

$$(4.19) \quad |S_i| \leq \Delta_i + \Delta_i \deg_{z_i} f \leq \Delta_i(1 + \deg f) \leq \Delta_i(nd)^{\exp O(r)}.$$

By inserting the bounds (4.17), (4.18) and (4.19) into (4.16), we infer

$$(4.20) \quad \max(H_{M_i}(x^{(j)}), H_{M_i}(y^{(j)})) \leq \Delta_i(nd)^{\exp O(r)}.$$

In view of Lemma 4.3, (4.20), $D \leq d^r$, $q \leq r$ and (4.9) we deduce that

$$\overline{\deg} x, \overline{\deg} y \leq qDd_1 + \sum_{i=1}^q \Delta_i^{-1} \sum_{j=1}^D H_{M_i}(x^{(j)}) \leq (nd)^{\exp O(r)}.$$

This proves (3.16). ■

4.2. Hyper- and superelliptic equations. Recall the notation introduced at the beginning of Section 4. Again, \mathbb{k} is an algebraically closed field of characteristic 0, z a transcendental element over \mathbb{k} , M a finite extension of $\mathbb{k}(z)$, and S a finite subset of \mathcal{M}_M .

PROPOSITION 4.6. *Let $F \in M[X]$ be a polynomial with non-zero discriminant and $m \geq 3$ a given integer. Put $n := \deg F$ and assume $n \geq 2$. All solutions of the equation*

$$(4.21) \quad F(x) = y^m \quad \text{in } x, y \in \mathcal{O}_S$$

have the properties

$$(4.22) \quad H_M(x) \leq (6n + 18)H_M(F) + 6g_{M/\mathbb{k}} + 2|S|,$$

$$(4.23) \quad mH_M(y) \leq (6n^2 + 18n + 1)H_M(F) + 6ng_{M/\mathbb{k}} + 2n|S|.$$

Proof. First assume that F splits into linear factors over M , and that S consists only of the infinite valuations of M ; these are the valuations of M with $v(z) < 0$. Under these hypotheses, Mason [16, p. 118, Theorem 15] proved that for every solution x, y of (4.21) we have

$$(4.24) \quad H_M(x) \leq 18H_M(F) + 6g_{M/\mathbb{k}} + 2(|S| - 1).$$

But Mason's proof remains valid without any changes for an arbitrary finite set S of places. That is, (4.24) holds if F splits into linear factors over M , without any condition on S .

We reduce the general case, where the splitting field of M may be larger than M , to the case considered by Mason. Let L be the splitting field of F over M , and T the set of valuations of L that extend those of S . Then $|T| \leq [L : M] \cdot |S|$, and by Lemma 4.2, we have $g_{L/\mathbb{k}} \leq [L : M] \cdot (g_{M/\mathbb{k}} + nH_M(F))$. Note that (4.24) holds, but with L, T instead of M, S . It follows that

$$\begin{aligned} [L : M] \cdot H_M(x) &= H_L(x) \leq 18H_L(F) + 6g_{L/\mathbb{k}} + 2(|T| - 1) \\ &\leq [L : M]((6n + 18)H_M(F) + 6g_{M/\mathbb{k}} + 2|S|), \end{aligned}$$

which implies (4.22). Further,

$$(4.25) \quad mH_M(y) = H_M(y^m) = H_M(F(x)) \leq H_M(F) + nH_M(x),$$

which gives (4.23). ■

PROPOSITION 4.7. *Let $F \in M[X]$ be a polynomial with non-zero discriminant. Put $n := \deg F$ and assume $n \geq 3$. Then the solutions of*

$$(4.26) \quad F(x) = y^2 \quad \text{in } x, y \in \mathcal{O}_S$$

have the properties

$$(4.27) \quad H_M(x) \leq (42n + 37)H_M(F) + 8g_{M/\mathbb{k}} + 4|S|,$$

$$(4.28) \quad H_M(y) \leq (21n^2 + 19n)H_M(F) + 4ng_{M/\mathbb{k}} + 2n|S|.$$

Proof. First assume that F splits into linear factors over M , that S consists only of the infinite valuations of M , that F is monic, and that F has its coefficients in \mathcal{O}_S . Under these hypotheses, Mason [16, p. 30, Theorem 6] proved that for every solution of (4.26) we have

$$(4.29) \quad H_M(x) \leq 26H_M(F) + 8g_{M/\mathbb{k}} + 4(|S| - 1).$$

An inspection of Mason's proof shows that his result is valid for arbitrary finite sets S of valuations, not just the set of infinite valuations. This leaves only the conditions imposed on F .

We reduce the general case to the special case to which (4.29) is applicable. Let $F = a_0X^n + \cdots + a_n$. Let L be the splitting field of $F \cdot (X^2 - a_0)$ over M . Let T be the set of valuations of L that extend the valuations of S , and also the valuations $v \in \mathcal{M}_M$ such that $v(F) < 0$. Further, let $F' = X^n + a_1X^{n-1} + a_0a_1X^{n-2} + \cdots + a_0^{n-1}a_n$, and let b be such that $b^2 = a_0^{n-1}$. Then for every solution x, y of (4.26) we have

$$F'(a_0x) = (by)^2, \quad a_0x, by \in \mathcal{O}_T,$$

and moreover $F' \in \mathcal{O}_T[X]$, F' is monic, and F' splits into linear factors over L . So by (4.29),

$$(4.30) \quad H_L(a_0x) \leq 26H_L(F') + 8g_{L/\mathbb{k}} + 4(|T| - 1).$$

First notice that

$$H_L(F') = [L : M]H_M(F') \leq [L : M] \cdot nH_M(F).$$

Further,

$$|T| \leq [L : M] \left(|S| - \sum_{v \in \mathcal{M}_M} \min(0, v(F)) \right) \leq [L : M] (|S| + H_M(F)).$$

Finally, from $H_M(F \cdot (X^2 - a_0)) \leq 2H_M(F)$ and Lemma 4.2, we have

$$g_{L/\mathbb{k}} \leq [L : M](g_{M/\mathbb{k}} + (n + 2)2H_M(F)).$$

By inserting these bounds into (4.30), we infer

$$\begin{aligned} [L : M]H_M(x) &\leq [L : M](H_M(a_0x) + H_M(F)) = H_L(a_0x) + [L : M]H_M(F) \\ &\leq [L : M]((42n + 37)H_M(F) + 8g_{M/\mathbb{k}} + 4|S|). \end{aligned}$$

This implies (4.27). The other inequality (4.28) follows by combining (4.27) with (4.25) with $m = 2$. ■

The final step of this subsection is to prove (3.19) of Proposition 3.7.

Proof of (3.19). We closely follow the proof of (3.16) of Proposition 3.6, and use the same notation. In particular, $\mathbb{k}_i, M_i, S_i, \Delta_i$ have the same meaning, and for $\alpha \in B$, $j = 1, \dots, D$, the j th conjugate $\alpha^{(j)}$ is the one corresponding to $w^{(j)}$. Put $F' := \delta^{-1}F$, and let $F'^{(j)}$ be the polynomial obtained by taking the j th conjugates of the coefficients of F' .

We keep the argument together for both hyper- and superelliptic equations by using the worse bounds everywhere. Let $x, y \in B$ be a solution of (2.4), where $m, n \geq 2$ and $n \geq 3$ if $m = 2$. Then

$$F'^{(j)}(x^{(j)}) = (y^{(j)})^m, \quad x^{(j)}, y^{(j)} \in \mathcal{O}_{S_i}.$$

By combining Propositions 4.6 and 4.7 we obtain the generous bound

$$H_{M_i}(x^{(j)}), mH_{M_i}(y^{(j)}) \leq 80n^2(H_{M_i}(F'^{(j)}) + g_{M_i/\mathbb{k}_i} + |S_i|).$$

For $H_{M_i}(F'^{(j)})$, g_{M_i/\mathbb{k}_i} , $|S_i|$ we have precisely the same estimates as (4.17)–(4.19). Then a similar computation as in the proof of (3.16) leads to

$$(4.31) \quad H_{M_i}(x^{(j)}), mH_{M_i}(y^{(j)}) \leq \Delta_i(nd)^{\exp O(r)}.$$

Now employing Lemma 4.3 and ignoring m for the moment we get, similarly to the proof of (3.16),

$$\overline{\deg} x, \overline{\deg} y \leq (nd)^{\exp O(r)},$$

which is (3.19). ■

Proof of (3.20). Assume that $y \notin \overline{\mathbb{Q}}$. Then $y \notin \mathbb{k}_i$ for at least one index i . Since $y \in B \subset \mathbb{k}_i(z_i, w)$ and $[\mathbb{k}_i(z_i, w) : \mathbb{k}_i(z_i)] \leq D$, we have

$$H_{M_i}(y) = [M_i : \mathbb{k}_i(z_i, w)]H_{\mathbb{k}_i(z_i, w)}(y) \geq [M_i : \mathbb{k}_i(z_i, w)] \geq \Delta_i/D.$$

Together with (4.31) and $D \leq d^r$ this implies

$$m \leq (nd)^{\exp O(r)},$$

which gives (3.20). ■

5. Specializations. In this section we consider specialization homomorphisms from the domain B to $\overline{\mathbb{Q}}$, and using these specializations together with earlier results concerning our equations in the number field case we finish the proof of Propositions 3.6 and 3.7.

We start with some notation. The set of places of \mathbb{Q} is $\mathcal{M}_{\mathbb{Q}} = \{\infty\} \cup \{\text{primes}\}$. By $|\cdot|_{\infty}$ we denote the ordinary absolute value on \mathbb{Q} and by $|\cdot|_p$ (p prime) the p -adic absolute value with $|p|_p = p^{-1}$. More generally, let L be an algebraic number field with set of places \mathcal{M}_L . Given $v \in \mathcal{M}_L$, we define the absolute value $|\cdot|_v$ in such a way that its restriction to \mathbb{Q} is $|\cdot|_p$ if v lies above $p \in \mathcal{M}_{\mathbb{Q}}$. These absolute values satisfy the product formula

$$\prod_{v \in \mathcal{M}_L} |\alpha|_v^{d_v} = 1 \quad \text{for } \alpha \in L^*,$$

where $d_v := [L_v : \mathbb{Q}_p]/[L : \mathbb{Q}]$, with $p \in \mathcal{M}_{\mathbb{Q}}$ the place below v , and \mathbb{Q}_p and L_v the completions of \mathbb{Q} at p and of L at v . Note that we have $\sum_{v|p} d_v = 1$ for every $p \in \mathcal{M}_{\mathbb{Q}}$. The *absolute logarithmic height* of $\alpha \in L$ is

defined by

$$h(\alpha) := \log \prod_{v \in \mathcal{M}_L} \max(1, |\alpha|_v^{d_v}).$$

This depends only on α and not on the choice of the number field L containing α , hence it defines a height on $\overline{\mathbb{Q}}$. For properties of the height we refer to Bombieri and Gubler [5].

LEMMA 5.1 ([9, Lemma 5.2]). *Let $m \geq 1$ and let $\alpha_1, \dots, \alpha_m \in \overline{\mathbb{Q}}$ be distinct, and suppose that $G(X) := \prod_{j=1}^m (X - \alpha_j) \in \mathbb{Z}[X]$. Let q, p_0, \dots, p_{m-1} be integers with $\gcd(q, p_0, \dots, p_{m-1}) = 1$ and put*

$$\beta_j := \sum_{i=0}^{m-1} \frac{p_j}{q} \alpha_j^i, \quad j = 1, \dots, m.$$

Then

$$\log \max(|q|, |p_0|, \dots, |p_{m-1}|) \leq 2m^2 + (m-1)h(G) + \sum_{j=1}^m h(\beta_j).$$

We now consider our specializations $B \mapsto \overline{\mathbb{Q}}$ and prove some of their properties. These specializations were introduced by Györy [11], [12] and, in a refined form, by Evertse and Györy [9].

We assume $q > 0$ and apart from that keep the notation and assumptions from Section 3. In particular, $K_0 := \mathbb{Q}(z_1, \dots, z_q)$, $K := \mathbb{Q}(z_1, \dots, z_q, w)$, $A_0 := \mathbb{Z}[z_1, \dots, z_q]$. Further, $B := \mathbb{Z}[z_1, \dots, z_q, w, g^{-1}]$ where g is a non-zero element of A_0 with the properties specified in Proposition 3.3, and w is integral over A_0 and has minimal polynomial

$$\mathcal{F}(X) = X^D + \mathcal{F}_1 X^{D-1} + \dots + \mathcal{F}_D \in A_0[X]$$

over K_0 as in Proposition 3.1(i). In the case $D = 1$ we take $w = 1$, $\mathcal{F}(X) = X - 1$.

Let $\mathbf{u} = (u_1, \dots, u_q) \in \mathbb{Z}^q$. Then the substitution $z_1 \mapsto u_1, \dots, z_q \mapsto u_q$ defines a ring homomorphism (specialization) from K_0 to \mathbb{Q} :

$$\varphi_{\mathbf{u}} : \alpha \mapsto \alpha(\mathbf{u}) : \{\alpha = g_1/g_2 : g_1, g_2 \in A_0, g_2(\mathbf{u}) \neq 0\} \rightarrow \mathbb{Q}.$$

To extend this to a ring homomorphism from B to $\overline{\mathbb{Q}}$ we have to impose some restrictions on \mathbf{u} . Let $\Delta_{\mathcal{F}}$ be the discriminant of \mathcal{F} (with $\Delta_{\mathcal{F}} = 1$ if $D = 1$), and let

$$(5.1) \quad \mathcal{H} := \Delta_{\mathcal{F}} \cdot \mathcal{F}_D \cdot g.$$

Put

$$(5.2) \quad \begin{cases} d_0^* := \max(\deg \mathcal{F}_1, \dots, \deg \mathcal{F}_D), & d_1^* := \max(d_0^*, \deg g), \\ h_0^* := \max(h(\mathcal{F}_1), \dots, h(\mathcal{F}_D)), & h_1^* := \max(h_0^*, h(g)). \end{cases}$$

Clearly $\mathcal{H} \in A_0$ and since $\Delta_{\mathcal{F}}$ is a homogeneous polynomial in $\mathcal{F}_1, \dots, \mathcal{F}_D$

of degree $2D - 2$, we have

$$(5.3) \quad \deg \mathcal{H} \leq (2D - 1)d_0^* + d_1^*.$$

Further, by Propositions 3.1(i), 3.3 and by (2.2) we also have

$$(5.4) \quad \begin{cases} d_0^* \leq (2d)^{\exp O(r)}, & h_0^* \leq (2d)^{\exp O(r)}(h + 1), \\ d_1^* \leq (nd)^{\exp O(r)}, & h_1^* \leq (nd)^{\exp O(r)}(h + 1). \end{cases}$$

Next assume that

$$(5.5) \quad \mathcal{H}(\mathbf{u}) \neq 0.$$

Then $g(\mathbf{u}) \neq 0$, $\Delta_F(\mathbf{u}) \neq 0$, hence the polynomial

$$\mathcal{F}_{\mathbf{u}} := X^D + \mathcal{F}_1(\mathbf{u})X^{D-1} + \dots + \mathcal{F}_D(\mathbf{u})$$

has D distinct zeros which are all different from 0, say $w^{(1)}(\mathbf{u}), \dots, w^{(D)}(\mathbf{u})$. Consequently, for $j = 1, \dots, D$ the assignment

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

defines a ring homomorphism $\varphi_{\mathbf{u},j}$ from B to $\overline{\mathbb{Q}}$; if $D = 1$ it is just $\varphi_{\mathbf{u}}$. The image of $\alpha \in B$ under $\varphi_{\mathbf{u},j}$ is denoted by $\alpha^{(j)}(\mathbf{u})$. It is important to note that if α is a unit in B , then its image under a specialization cannot be 0. Thus by Proposition 3.3, $\delta(\mathbf{u}) \neq 0$ and $D_F(\mathbf{u}) \neq 0$.

Recall that we may express elements of B as

$$(5.6) \quad \alpha = \sum_{i=1}^{D-1} (P_i/Q)w^i$$

where $P_0, \dots, P_{D-1}, Q \in A_0$, $\gcd(P_0, \dots, P_{D-1}, Q) = 1$.

Because of $\alpha \in B$, Q must divide a power of g ; hence $Q(\mathbf{u}) \neq 0$. So we have

$$(5.7) \quad \alpha^{(j)}(\mathbf{u}) = \sum_{i=1}^{D-1} (P_i(\mathbf{u})/Q(\mathbf{u}))(w^{(j)}(\mathbf{u}))^i, \quad j = 1, \dots, D.$$

Clearly, $\varphi_{\mathbf{u},j}$ is the identity on $B \cap \mathbb{Q}$. Hence if $\alpha \in B \cap \overline{\mathbb{Q}}$ then $\varphi_{\mathbf{u},j}(\alpha)$ has the same minimal polynomial as α and so it is a conjugate of α .

For $\mathbf{u} = (u_1, \dots, u_q) \in \mathbb{Z}^q$, put $|\mathbf{u}| := \max(|u_1|, \dots, |u_q|)$. It is easy to check that for any $g \in A_0$, $\mathbf{u} \in \mathbb{Z}^q$,

$$(5.8) \quad \log |g(\mathbf{u})| \leq q \log \deg g + h(g) + \deg g \log \max(1, |\mathbf{u}|).$$

In particular,

$$(5.9) \quad h(\mathcal{F}_{\mathbf{u}}) \leq q \log d_0^* + h_0^* + d_0^* \log \max(1, |\mathbf{u}|)$$

and so by Lemma 5.1 of Evertse and Györy [9] we have

$$(5.10) \quad \sum_{j=1}^D h(w^{(j)}(\mathbf{u})) \leq D + 1 + q \log d_0^* + h_0^* + d_0^* \log \max(1, |\mathbf{u}|).$$

We define the algebraic number fields $K_{\mathbf{u},j} = \mathbb{Q}(w^{(j)}(\mathbf{u}))$ for $j = 1, \dots, D$. We denote by Δ_L the the discriminant of an algebraic number field L . We derive an upper bound for the absolute value of the discriminant $\Delta_{K_{\mathbf{u},j}}$ of $K_{\mathbf{u},j}$.

LEMMA 5.2 ([9, Lemma 5.5]). *Let $\mathbf{u} \in \mathbb{Z}^q$ with $\mathcal{H}(\mathbf{u}) \neq 0$. Then for $j = 1, \dots, D$ we have $[K_{\mathbf{u},j} : \mathbb{Q}] \leq D$ and*

$$|\Delta_{K_{\mathbf{u},j}}| \leq D^{2D-1}((d_0^*)^q e^{h_0^*} \max(1, |\mathbf{u}|^{d_0^*}))^{2D-2}.$$

The following two lemmas relate the height of $\alpha \in B$ to the heights of $\alpha^{(j)}(\mathbf{u})$ for $\mathbf{u} \in \mathbb{Z}^q$.

LEMMA 5.3 ([9, Lemma 5.6]). *Let $\mathbf{u} \in \mathbb{Z}^q$ with $\mathcal{H}(\mathbf{u}) \neq 0$, and let $\alpha \in B$. Then for $j = 1, \dots, D$,*

$$\begin{aligned} h(\alpha^{(j)}(\mathbf{u})) &\leq D^2 + q(D \log d_0^* + \log \overline{\deg} \alpha) \\ &\quad + Dh_0^* + \bar{h}(\alpha) + (Dd_0^* + \overline{\deg} \alpha) \log \max(1, |\mathbf{u}|). \end{aligned}$$

LEMMA 5.4 ([9, Lemma 5.7]). *Let $\alpha \in B$, $\alpha \neq 0$, and let N be an integer with*

$$(5.11) \quad N \geq \max(\overline{\deg} \alpha, 2Dd_0^* + 2(q+1)(d_1^* + 1)).$$

Then the set

$$\mathcal{S} := \{\mathbf{u} \in \mathbb{Z}^q : |\mathbf{u}| \leq N, \mathcal{H}(\mathbf{u}) \neq 0\}$$

is non-empty, and

$$(5.12) \quad \bar{h}(\alpha) \leq 5N^4(h_1^* + 1)^2 + 2D(h_1^* + 1)H,$$

where $H := \max\{h(\alpha^{(j)}(\mathbf{u})) : \mathbf{u} \in \mathcal{S}, j = 1, \dots, D\}$.

6. Bounding the height and the exponent m . We shall derive the height bounds (3.17) in Proposition 3.6 and (3.21) in Proposition 3.7, as well as the upper bound for m in Proposition 3.8, by combining the specialization techniques from the previous section with existing effective results for Diophantine equations over S -integers of a number field, namely Györy and Yu [13] for Thue equations, and the three authors [4] for hyper- and superelliptic equations and the Schinzel–Tijdeman equation.

6.1. Thue equations. To state the result of Györy and Yu we need some notation.

For an algebraic number field L , we denote by d_L , \mathcal{O}_L , \mathcal{M}_L , Δ_L , h_L , r_L and R_L the degree, ring of integers, set of places, discriminant, class number, unit rank and regulator of L . The absolute norm of an ideal \mathfrak{a} of \mathcal{O}_L is denoted by $N(\mathfrak{a})$.

Let L be an algebraic number field and let S be a finite set of places of L which contains all infinite places. Denote by s the cardinality of S . Recall

that the ring of S -integers \mathcal{O}_S is defined as

$$\mathcal{O}_S = \{\alpha \in L : |\alpha|_v \leq 1 \text{ for } v \in \mathcal{M}_L \setminus S\}.$$

If S consists only of the infinite places of L , we put $P := 2$, $Q := 2$. If S contains also finite places, we denote by $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ the prime ideals corresponding to the finite places of S , and we put

$$P := \max(N(\mathfrak{p}_1), \dots, N(\mathfrak{p}_t)), \quad Q := N(\mathfrak{p}_1 \dots \mathfrak{p}_t).$$

The S -regulator associated with S is denoted by R_S . If S consists only of the infinite places of L it is just R_L , while otherwise

$$R_S = h_S R_L \prod_{i=1}^t \log N(\mathfrak{p}_i),$$

where h_S is a (positive) divisor of h_L . It is an easy consequence of formula (2) of Louboutin [15] that

$$(6.1) \quad h_L R_L \leq |\Delta_L|^{1/2} (\log^* |\Delta_L|)^{d_L-1}$$

(cf. formula (59) of Györy and Yu [13]). Further, we have

$$(6.2) \quad R_S \leq |\Delta_L|^{1/2} (\log^* |\Delta_L|)^{d_L-1} (\log^* Q)^s$$

(see [9, (6.1)]). In view of (6.1) above, this is true also if $t = 0$.

6.1.1. Results in the number field case. Let $F(X, Y) \in L[X, Y]$ be a binary form of degree $n \geq 3$ with splitting field L and with at least three pairwise non-proportional linear factors. Further, let $\beta \in L \setminus \{0\}$ and consider the Thue equation

$$(6.3) \quad F(\xi, \eta) = \beta \quad \text{in } \xi, \eta \in \mathcal{O}_S.$$

For a polynomial G with algebraic coefficients, we denote by $h(G)$ the maximum of the logarithmic heights of its coefficients.

PROPOSITION 6.1 ([13, Corollary 3]). *All solutions $(\xi, \eta) \in \mathcal{O}_S^2$ of (6.3) satisfy*

$$(6.4) \quad \max(h(\xi), h(\eta)) \leq c_1 P R_S (1 + (\log^* R_S) / \log^* P) \\ \times \left(c_2 R_L + \frac{h_L}{d_L} \log Q + 2nd_L H_1 + H_2 \right),$$

where

$$H_1 = \max(1, h(F)), \quad H_2 = \max(1, h(\delta)), \\ c_1 = 250n^6 s^{2s+3.5} \cdot 2^{7s+27} (\log 2s) d_L^{2s+4} (\log^*(2d_L))^3, \\ c_2 = \begin{cases} 0 & \text{if } r_L = 0, \\ 1/d_L & \text{if } r_L = 1, \\ 29e r_L! r_L \sqrt{r_L - 1} \log d_L & \text{if } r_L \geq 2. \end{cases}$$

We shall also need the following.

LEMMA 6.2 ([21]). *If L is the compositum of the algebraic number fields L_1, \dots, L_k with degrees d_{L_1}, \dots, d_{L_k} and discriminants $\Delta_{L_1}, \dots, \Delta_{L_k}$, then Δ_L divides $\Delta_{L_1}^{d_L/d_{L_1}} \dots \Delta_{L_k}^{d_L/d_{L_k}}$ in \mathbb{Z} .*

LEMMA 6.3. *Let L be an algebraic number field and θ a zero of a polynomial $G \in L[X]$ of degree n without multiple roots. Then*

$$|\Delta_{L(\theta)}| \leq n^{(2n-1)d_L} e^{(2n^2-2)h(G)} |\Delta_L|^{[L(\theta):L]}.$$

Proof. This is a slight modification of the second assertion of [4, Lemma 4.1]. In fact, this lemma gives the same bound but with an exponent $(2n-2)h'(G)$ on e , where for $G = \sum_{k=0}^n b_k X^{n-k}$ we define

$$h'(G) = \sum_{v \in \mathcal{M}_L} d_v \log \max(1, |b_0|_v, \dots, |b_n|_v).$$

This height is easily estimated from above by $\sum_{k=0}^n h(b_k) \leq (n+1)h(G)$. Our lemma follows. ■

6.1.2. *Concluding the proof of Proposition 3.6.* What remains is the proof of (3.17). We first consider the case $q > 0$. Let x, y be a solution of (3.15) in B . We keep the notation introduced in Section 5. Recall that $\mathcal{H} := \Delta_{\mathcal{F}} \cdot \mathcal{F}_D \cdot g$. From (5.3) and (5.4) we easily deduce

$$(6.5) \quad \deg \mathcal{H} \leq (nd)^{\exp O(r)}.$$

Choose $\mathbf{u} \in \mathbb{Z}^q$ with $\mathcal{H}(\mathbf{u}) \neq 0$, choose $j \in \{1, \dots, D\}$, and denote by $F_{\mathbf{u},j}$, $\delta^{(j)}(\mathbf{u})$, $x^{(j)}(\mathbf{u})$, $y^{(j)}(\mathbf{u})$, the images of F, δ, x, y under $\varphi_{\mathbf{u},j}$. Then $F_{\mathbf{u},j}$ has its coefficients in $K_{\mathbf{u},j}$. Further, let L denote the splitting field of $F_{\mathbf{u},j}$ over $K_{\mathbf{u},j}$, and S the set of places of L which consists of all infinite places and all finite places lying above the rational prime divisors of $g(\mathbf{u})$. Note that $w^{(j)}(\mathbf{u})$ is an algebraic integer and $g(\mathbf{u}) \in \mathcal{O}_S^*$. Thus $\varphi_{\mathbf{u},j}(B) \subseteq \mathcal{O}_S$ and it follows from (3.15) that

$$(6.6) \quad F_{\mathbf{u},j}(x^{(j)}(\mathbf{u}), y^{(j)}(\mathbf{u})) = \delta^{(j)}(\mathbf{u}), \quad x^{(j)}(\mathbf{u}), y^{(j)}(\mathbf{u}) \in \mathcal{O}_S.$$

We already proved in Section 4 that (3.16) of Proposition 3.6 holds, i.e.

$$\overline{\deg x}, \overline{\deg y} \leq (nd)^{\exp O(r)}.$$

Hence we can apply Lemma 5.4 with

$$N = \max((nd)^{\exp O(r)}, 2Dd_0^* + 2(q+1)(d_1^* + 1)).$$

In view of (5.4), $D \leq d^r$ and $q \leq r$ we get

$$(6.7) \quad N \leq (nd)^{\exp O(r)}.$$

By applying Lemma 5.4 with $\alpha = x$ and $\alpha = y$, and inserting $D \leq d^r$ and the upper bound $h_1^* \leq (nd)^{\exp O(r)}(h+1)$ from (5.4), it follows that there

are $\mathbf{u} \in \mathbb{Z}^q$, $j \in \{1, \dots, D\}$ with

$$(6.8) \quad |\mathbf{u}| \leq (nd)^{\exp O(r)}, \quad \mathcal{H}(\mathbf{u}) \neq 0$$

and

$$(6.9) \quad \max(\bar{h}(x), \bar{h}(y)) \leq (nd)^{\exp O(r)} [(h+1)^2 + d^r (h+1) \max(h(x^{(j)}(\mathbf{u})), h(y^{(j)}(\mathbf{u}))].$$

We proceed further with these \mathbf{u} , j and apply Proposition 6.1 to equation (6.6) to derive an upper bound for $h(x^{(j)}(\mathbf{u}))$ and $h(y^{(j)}(\mathbf{u}))$. To do so we have to bound from above the parameters corresponding to those which occur in Proposition 6.1.

Write $F = \sum_{k=0}^n a_k X^{n-k} Y^k$ and put

$$\overline{\deg} F := \max_{0 \leq k \leq n} \overline{\deg} a_k, \quad \bar{h}(F) := \max_{0 \leq k \leq n} \bar{h}(a_k).$$

Notice that by Lemma 3.4, applied to δ and the coefficients of F with the choice $d^* = d$, $h^* = h$, we have

$$(6.10) \quad \overline{\deg} F, \overline{\deg} \delta \leq (2d)^{\exp O(r)},$$

$$(6.11) \quad \bar{h}(F), \bar{h}(\delta) \leq (2d)^{\exp O(r)} (h+1).$$

It follows from Lemma 5.3, $q \leq r$, $D \leq d^r$, (5.4), (6.10), (6.11), and lastly (6.8), that

$$(6.12) \quad \begin{aligned} h(F_{\mathbf{u},j}) &\leq D^2 + q(D \log d_0^* + \log \overline{\deg} F) + Dh_0^* \\ &\quad + \bar{h}(F) + (Dd_0^* + \overline{\deg} F) \log \max(1, |\mathbf{u}|) \\ &\leq (nd)^{\exp O(r)} (h+1). \end{aligned}$$

In a similar way, replacing F by δ , we also obtain

$$(6.13) \quad h(\delta^{(j)}(\mathbf{u})) \leq (nd)^{\exp O(r)} (h+1).$$

We recall that d_L and Δ_L denote the degree and the discriminant of L over \mathbb{Q} . Since $[K_{\mathbf{u},j} : \mathbb{Q}] \leq D$, we have $d_L \leq Dn!$. Let $G(X) := F(X, 1)$, and let $\theta_1, \dots, \theta_{n'}$ be the roots of G . We have $n' = n$ if $a_0 \neq 0$ and $n' = n - 1$ otherwise. Then $L = K_{\mathbf{u},j}(\theta_1, \dots, \theta_{n'})$. Denote by d_{L_i} the degree and by Δ_{L_i} the discriminant of the number field $L_i := K_{\mathbf{u},j}(\theta_i)$, $i = 1, \dots, n'$. Then by Lemma 6.2 we have

$$(6.14) \quad |\Delta_L| \leq \prod_{i=1}^{n'} |\Delta_{L_i}|^{d_L/d_{L_i}}.$$

We estimate $|\Delta_L|$. First notice that by Lemma 5.2, inserting the estimates

$q \leq r$, $D \leq d^r$, (5.4), (6.8),

$$(6.15) \quad |\Delta_{K_{\mathbf{u},j}}| \leq D^{2D-1} ((d_0^*)^q e^{h_0^*} \max(1, |\mathbf{u}|^{d_0^*}))^{2D-2} \\ \leq \exp\{(nd)^{\exp O(r)}(h+1)\}.$$

Further, by Lemma 6.3 and the estimates $D \leq d^r$, (6.12), (6.15),

$$|\Delta_{L_i}| \leq n^{(2n-1)D} e^{(2n^2-2)h(F_{\mathbf{u},j})} |\Delta_{K_{\mathbf{u},j}}|^{[L_i:K_{\mathbf{u},j}]} \\ \leq \exp\{[L_i:K_{\mathbf{u},j}] \cdot (nd)^{\exp O(r)}(h+1)\}.$$

By inserting this into (6.14), using $[L:K_{\mathbf{u},j}] \leq n!$, we obtain

$$(6.16) \quad |\Delta_L| \leq \exp\{(nd)^{\exp O(r)}(h+1) \cdot nd_L/d_{K_{\mathbf{u},j}}\} \\ \leq \exp\{n!(nd)^{\exp O(r)}(h+1)\}.$$

By assumption (5.2), g has degree at most d_1^* and logarithmic height at most h_1^* . Further, $g(\mathbf{u}) \neq 0$ and by $q \leq r$, (5.4), (6.8),

$$(6.17) \quad |g(\mathbf{u})| \leq (d_1^*)^q e^{h_1^*} \max(1, |\mathbf{u}|^{d_1^*}) \leq \exp\{(nd)^{\exp O(r)}(h+1)\}.$$

The cardinality s of S is at most $d_L(1+\omega)$, where ω denotes the number of distinct prime divisors of $f(\mathbf{u})$. By prime number theory,

$$(6.18) \quad s = O(d_L \log^* |g(\mathbf{u})| / \log^* |g(\mathbf{u})|).$$

From this estimate and (6.17), $D \leq d^r$, $d_L \leq n!d^r$, one easily deduces that for c_1 coming from Proposition 6.1 we have

$$(6.19) \quad c_1 \leq \exp\{n!(nd)^{\exp O(r)}(h+1)\}.$$

Next, we estimate P, Q and R_S . By (6.17), $d_L \leq n!d^r$ we have

$$(6.20) \quad P \leq Q \leq |g(\mathbf{u})|^{d_L} \leq \exp\{n!(nd)^{\exp O(r)}(h+1)\}.$$

To estimate R_S , we use (6.2). Then, in view of (6.16) and $d_L \leq n!d^r$, we have

$$(6.21) \quad |\Delta_L|^{1/2} (\log^* |\Delta_L|)^{d_L-1} \leq \exp\{n!(nd)^{\exp O(r)}(h+1)\}.$$

Further, by (6.18) and (6.20),

$$(\log Q)^s \leq \exp \left\{ O \left(d_L \frac{\log^* |g(\mathbf{u})|}{\log^* \log^* |g(\mathbf{u})|} \cdot (\log d_L + \log^* \log^* |g(\mathbf{u})|) \right) \right\}.$$

Together with (6.17), this leads to

$$(6.22) \quad R_S \leq |\Delta_L|^{1/2} (\log^* |\Delta_L|)^{d_L-1} (\log Q)^s \leq \exp\{n!(nd)^{\exp O(r)}(h+1)\}.$$

Combining (6.1) with (6.21) and $R_L > 0.2052$ (see Friedman [10]) we get

$$(6.23) \quad \max(h_L, R_L) \leq \exp\{n!(nd)^{\exp O(r)}(h+1)\}.$$

Finally, using $r_L < d_L \leq n!d^r$, we infer that

$$(6.24) \quad c_2 \leq \exp O(d_L \log^* d_L) \leq \exp\{n!(nd)^{\exp O(r)}\}.$$

We now apply Proposition 6.1 to equation (6.6). From the estimates (6.12), (6.13), (6.19), (6.20), (6.22), (6.23), (6.24), it follows that the upper bound in Proposition 6.1 is a sum and product of terms, which are all bounded above by $\exp\{n!(nd)^{\exp O(r)}(h+1)\}$. Consequently,

$$h(x^{(j)}(\mathbf{u})), h(y^{(j)}(\mathbf{u})) \leq \exp\{n!(nd)^{\exp O(r)}(h+1)\}.$$

By inserting this into (6.9), we obtain the upper bound (3.17) for $q > 0$.

Now assume $q = 0$. In this case $K_0 = \mathbb{Q}$, $A_0 = \mathbb{Z}$ and $B = \mathbb{Z}[w, g^{-1}]$, where w is an algebraic integer with minimal polynomial $\mathcal{F}(X) = X^D + \mathcal{F}_1 X^{D-1} + \dots + \mathcal{F}_D \in \mathbb{Z}[X]$ over \mathbb{Q} , and g is a non-zero rational integer. In view of Propositions 3.1(i) and 3.3 we may assume that

$$\log |g| \leq h_1^* \quad \text{and} \quad \log |\mathcal{F}_k| \leq h_0^* \quad \text{for } k = 1, \dots, D,$$

where h_0^*, h_1^* satisfy (5.4). Denote by $w^{(1)}, \dots, w^{(D)}$ the conjugates of w , and let $K_j := \mathbb{Q}(w^{(j)})$ for $j := 1, \dots, D$. By a similar argument to the proof of Lemma 5.5 of Evertse and Györy [9], we have $|\Delta_{K_j}| \leq D^{2D-1} e^{(2D-2)h_0^*}$, which is the estimate from Lemma 5.2 with $q = 0$ and $\max(1, |\mathbf{u}|)$ replaced by 1. For $\alpha \in K$, we denote by $\alpha^{(j)}$ the conjugate of α corresponding to $w^{(j)}$.

Instead of Lemma 5.4 we use Lemma 5.1, applied with $G = \mathcal{F}$, $m = D$ and $\beta^{(j)} = x^{(j)}$, resp. $y^{(j)}$. Inserting (5.4), this leads to an estimate

$$(6.25) \quad \max(\bar{h}(x), \bar{h}(y)) \leq (nd)^{\exp O(r)} \max_{1 \leq j \leq D} \max(h(x^{(j)}), h(y^{(j)})).$$

We proceed further with the j for which the maximum is attained.

Now we can follow the argument for the case $q > 0$, except that in all estimates we have to take $q = 0$, and replace $\max(1, |\mathbf{u}|)$ by 1, $K_{\mathbf{u},j}$ by K_j , $f(\mathbf{u})$ by f , $F_{\mathbf{u},j}$ by $F^{(j)}$, where $F^{(j)}$ is the binary form obtained by taking the j th conjugates of the coefficients of F , and $g(\mathbf{u})$ by g . This leads to an estimate

$$h((x^{(j)})), h((y^{(j)})) \leq \exp\{n!(nd)^{\exp O(r)}(h+1)\},$$

and combined with (6.25) this gives again (3.17), completing the proof of Proposition 3.6. ■

6.2. Hyper- and superelliptic equations

6.2.1. Results in the number field case. Let L be a number field, and denote as usual by $d_L, \Delta_L, h_L, R_L, \mathcal{O}_L, \mathcal{M}_L$ its degree, discriminant, class number, regulator, ring of integers, and set of places. Further, let S be a finite set of places of L containing all infinite places. If S consists only of the infinite places of L , put $P := 2, Q := 2$. Otherwise, denote by $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ the prime ideals corresponding to the finite places of S , and put

$$P := \max(N(\mathfrak{p}_1), \dots, N(\mathfrak{p}_t)), \quad Q := N(\mathfrak{p}_1 \dots \mathfrak{p}_t).$$

Let

$$(6.26) \quad F(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n \in \mathcal{O}_S[X]$$

be a polynomial of degree $n \geq 2$ and of non-zero discriminant, $\delta \in \mathcal{O}_S \setminus \{0\}$, and m a positive integer. Put

$$\hat{h} := \sum_{v \in \mathcal{M}_L} d_v \log \max(1, |\delta|_v, |a_0|_v, \dots, |a_n|_v),$$

where $d_v := [L_v : \mathbb{Q}_p]/[L : \mathbb{Q}]$, with $p \in \mathcal{M}_{\mathbb{Q}}$ the place below v .

PROPOSITION 6.4 ([4, Theorem 2.1]). *Assume $n \geq 2$, $m \geq 3$. If $x, y \in \mathcal{O}_S$ is a solution to the equation*

$$(6.27) \quad F(x) = \delta y^m, \quad x, y \in \mathcal{O}_S,$$

then

$$h(x), h(y) \leq c_3^{m^3} |\Delta_L|^{2m^2 n^2} Q^{3m^2 n^2} e^{8m^2 n^3 d_L \hat{h}},$$

where $c_3 := (6ns)^{14n^3 s}$.

PROPOSITION 6.5 ([4, Theorem 2.2]). *Let $n \geq 3$. If $x, y \in \mathcal{O}_S$ is a solution to*

$$(6.28) \quad F(x) = \delta y^2, \quad x, y \in \mathcal{O}_S,$$

then

$$h(x), h(y) \leq c_4 |\Delta_L|^{8n^3} Q^{20n^3} e^{50n^4 d_L \hat{h}},$$

where $c_4 := (4ns)^{212n^4 s}$.

PROPOSITION 6.6 ([4, Theorem 2.3]). *Let $n \geq 2$. If x, y, m is a solution to*

$$F(x) = \delta y^m, \quad x, y \in \mathcal{O}_S, m \in \mathbb{Z}_{\geq 2},$$

such that $y \neq 0$ and y is not a root of unity, then

$$m \leq c_5 |\Delta_L|^{6n} P^{n^2} e^{11nd_L \hat{h}},$$

where $c_5 := (10n^2 s)^{40ns}$.

6.2.2. Concluding the proofs of Propositions 3.7 and 3.8

Proof of (3.21) of Proposition 3.7. The computations will be similar to those in the proof of (3.17) but with some simplifications.

First we suppose $q > 0$. Take a solution x, y of (3.18) in B . We use once more the polynomial $\mathcal{H} := \Delta_{\mathcal{F}} \cdot \mathcal{F}_D \cdot g$ from Section 5. Take again $\mathbf{u} \in \mathbb{Z}^q$ with $\mathcal{H}(\mathbf{u}) \neq 0$, choose $j \in \{1, \dots, D\}$, and denote by $F_{\mathbf{u},j}$, $\delta^{(j)}(\mathbf{u})$, $x^{(j)}(\mathbf{u})$, $y^{(j)}(\mathbf{u})$, the images of F, δ, x, y under the specialization $\varphi_{\mathbf{u},j}$. In contrast to our argument for Thue equations, we do not have to deal with the splitting field of F now. So we take for S the set of places of $K_{\mathbf{u},j}$ consisting of all

infinite places and all finite places lying above the rational prime divisors of $g(\mathbf{u})$. Then $\varphi_{\mathbf{u},j}(B) \subseteq \mathcal{O}_S$, and

$$(6.29) \quad F_{\mathbf{u},j}(x^{(j)}(\mathbf{u})) = \delta^{(j)}(\mathbf{u})y^{(j)}(\mathbf{u})^m, \quad \mathbf{x}^{(j)}(\mathbf{u}), y^{(j)}(\mathbf{u}) \in \mathcal{O}_S.$$

Note that by the choice of \mathcal{H} and $\mathcal{H}(\mathbf{u}) \neq 0$ we have $\delta_j(\mathbf{u}) \neq 0$, and $F_{\mathbf{u},j}$ has non-zero discriminant. So $F_{\mathbf{u},j}$ has the same number of zeros and the same degree as F , that is, the degree of $F_{\mathbf{u},j}$ is $n \geq 2$ if $m \geq 3$ and $n \geq 3$ if $m = 2$. Hence Propositions 6.4 and 6.5 are applicable.

By precisely the same argument as in the case of Thue equations, there are $\mathbf{u} \in \mathbb{Z}^q$ and $j \in \{1, \dots, D\}$ satisfying (6.8) and (6.9). We proceed further with these \mathbf{u}, j .

We estimate the parameters corresponding to those in the bounds from Propositions 6.4, 6.5. First, we get precisely the same estimates as in (6.12) and (6.13). These imply

$$(6.30) \quad \widehat{h} \leq (n+1)h(F_{\mathbf{u},j}) + h(\delta^{(j)}(\mathbf{u})) \leq (nd)^{\exp O(r)}(h+1).$$

Further we have, similarly to (6.15),

$$(6.31) \quad |\Delta_{K_{\mathbf{u},j}}| \leq \exp\{(nd)^{\exp O(r)}(h+1)\}.$$

Next, similarly to (6.17),

$$(6.32) \quad |g(\mathbf{u})| \leq \exp\{(nd)^{\exp O(r)}(h+1)\}.$$

The set S now consists of places of $K_{\mathbf{u},j}$ instead of the splitting field of $F_{\mathbf{u},j}$ over K . So since $[K_{\mathbf{u},j} : \mathbb{Q}] \leq D$ we now have $s \leq D(1 + \omega)$, where ω is the number of distinct prime divisors of $g(\mathbf{u})$. This gives, instead of (6.18),

$$(6.33) \quad s = O(D \log^* |g(\mathbf{u})| / \log^* \log^* |g(\mathbf{u})|).$$

By inserting (6.32), and $D \leq d^r$, we obtain for the quantities c_3, c_4 in Propositions 6.4 and 6.5 the upper bounds

$$(6.34) \quad c_3, c_4 \leq \exp\{(nd)^{\exp O(r)}(h+1)\}.$$

Lastly, instead of (6.20) we have

$$(6.35) \quad P \leq Q \leq |g(\mathbf{u})|^D \leq \exp\{(nd)^{\exp O(r)}(h+1)\},$$

where we have used (6.32) and $D \leq d^r$.

We now apply Propositions 6.4 and 6.5 to (6.29). Note that we must take $L = K_{\mathbf{u},j}$; so $d_L \leq D \leq d^r$. By inserting this and (6.30), (6.31), (6.34), (6.35) into the upper bounds from these propositions, we get

$$(6.36) \quad h(x^{(j)}(\mathbf{u})), h(y^{(j)}(\mathbf{u})) \leq \exp\{m^3(nd)^{\exp O(r)}(h+1)\}.$$

By inserting this into (6.9), we obtain (3.21) in the case $q > 0$.

Now let $q = 0$. For $\alpha \in K$, write $\alpha^{(j)}$ for the conjugate of α corresponding to $w^{(j)}$, and let $F^{(j)}$ be the polynomial obtained by taking the j th conjugates of the coefficients of F . We simply have to follow the above arguments,

replacing everywhere q by 0, $\max(1, |\mathbf{u}|)$ by 1, $K_{\mathbf{u},j}$ by $K^{(j)} = \mathbb{Q}(w^{(j)})$, $F_{\mathbf{u},j}$ by $F^{(j)}$, $x^{(j)}(\mathbf{u})$, $y^{(j)}(\mathbf{u})$ by $x^{(j)}$, $y^{(j)}$, and $g(\mathbf{u})$ by $g \in \mathbb{Z}$. Instead of (6.9) we have to use (6.25). Thus, we obtain the same estimate as (6.36), but with $x^{(j)}$, $y^{(j)}$ instead of $x_j(\mathbf{u})$, $y_j(\mathbf{u})$. Via (6.25) we obtain (3.21) in the case $q = 0$. This completes our proof of Proposition 3.7. ■

Proof of Proposition 3.8. Assume for the moment $q > 0$. Let $x \in B$, $y \in B \cap \overline{\mathbb{Q}}$, $m \in \mathbb{Z}_{\geq 2}$ be a solution of (3.18), such that $y \neq 0$ and y is not a root of unity. Choose again \mathbf{u} , j satisfying (6.8), (6.9). Note that $y^{(j)}(\mathbf{u})$ is a conjugate of y since $y \in \overline{\mathbb{Q}}$; hence it is not 0 or a root of unity.

We apply Proposition 6.6 to (6.29). By (6.32), (6.33), we find that the constant c_5 in Proposition 6.6 satisfies

$$c_5 \leq \exp\{(nd)^{\exp O(r)}(h+1)\}.$$

Further, we have the upper bounds (6.30) for \widehat{h} , (6.31) for $|\Delta_{K_{\mathbf{u},j}}|$, and (6.35) for P . By inserting these estimates into the upper bound for m from Proposition 6.6, we obtain $m \leq \exp\{(nd)^{\exp O(r)}(h+1)\}$. In the case $q = 0$, we obtain the same estimate, by making the same modifications as in the proof of Proposition 3.7. This finishes our proof of Proposition 3.8. ■

Acknowledgments. This research was supported in part by the University of Debrecen (J.-H.E., A.B.), by the Hungarian Academy of Sciences (J.-H.E., K.G.), and by grants K100339, NK104208 and K75566 (A.B., K.G.) of the Hungarian National Foundation for Scientific Research. This work was also partially supported by the European Union and the European Social Fund through project Supercomputer, the national virtual lab (grant no. TAMOP-4.2.2.C-11/1/KONV-2012-0010).

We would like to thank the referee for his careful scrutiny of our paper and for his useful comments.

References

- [1] M. Aschenbrenner, *Ideal membership in polynomial rings over the integers*, J. Amer. Math. Soc. 17 (2004), 407–441.
- [2] A. Baker, *Contributions to the theory of Diophantine equations I. On the representation of integers by binary forms*, Philos. Trans. Roy. Soc. London Ser. A 263 (1967/68), 173–191.
- [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. Györy, *Effective results for hyper- and superelliptic equations over number fields*, Publ. Math. Debrecen 82 (2013), 727–756.
- [5] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge Univ. Press, 2006.
- [6] B. Brindza, *On S -integral solutions of the equation $y^m = f(x)$* , Acta Math. Hungar. 44 (1984), 133–139.

- [7] B. Brindza, *On the equation $f(x) = y^m$ over finitely generated domains*, Acta Math. Hungar. 53 (1989), 377–383.
- [8] J. Coates, *An effective p -adic analogue of a theorem of Thue*, Acta Arith. 15 (1968/69), 279–305.
- [9] J.-H. Evertse and K. Győry, *Effective results for unit equations over finitely generated integral domains*, Math. Proc. Cambridge Philos. Soc. 154 (2013), 351–380.
- [10] E. Friedman, *Analytic formulas for the regulator of a number field*, Invent. Math. 98 (1989), 599–622.
- [11] K. Győry, *Bounds for the solutions of norm form, discriminant form and index form equations in finitely generated integral domains*, Acta Math. Hungar. 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 (1984), 54–100.
- [13] K. Győry and K. Yu, *Bounds for the solutions of S -unit equations and decomposable form equations*, Acta Arith. 123 (2006), 9–41.
- [14] G. Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. 95 (1926), 736–788.
- [15] S. Louboutin, *Explicit bounds for residues of Dedekind zeta functions, values of L -functions at $s = 1$, and relative class numbers*, J. Number Theory 85 (2000), 263–282.
- [16] R. C. Mason, *Diophantine Equations over Function Fields*, Cambridge Univ. Press, 1984.
- [17] A. Schinzel and R. Tijdeman, *On the equation $y^m = P(x)$* , Acta Arith. 31 (1976), 199–204.
- [18] W. M. Schmidt, *Thue’s equation over function fields*, J. Austral. Math. Soc. Ser. A 25 (1978), 385–442.
- [19] H. Simmons, *The solution of a decision problem for several classes of rings*, Pacific J. Math. 34 (1970), 547–557.
- [20] V. G. Sprindžuk and S. V. Kotov, *An effective analysis of the Thue–Mahler equation in relative fields*, Dokl. Akad. Nauk BSSR 17 (1973), 393–395, 477 (in Russian).
- [21] H. M. Stark, *Some effective cases of the Brauer–Siegel theorem*, Invent. Math. 23 (1974), 135–152.
- [22] L. A. Trelina, *S -integral solutions of Diophantine equations of hyperbolic type*, Dokl. Akad. Nauk BSSR 22 (1978), 881–884, 955 (in Russian).
- [23] J. Végső, *On superelliptic equations*, Publ. Math. Debrecen 44 (1994), 183–187.
- [24] M. Waldschmidt, *Diophantine Approximation on Linear Algebraic Groups*, Springer, 2000.

Attila Bérczes, Kálmán Győry
 Institute of Mathematics
 University of Debrecen
 H-4010 Debrecen, P.O. Box 12, Hungary
 E-mail: berczesa@science.unideb.hu
 gyory@science.unideb.hu

Jan-Hendrik Evertse
 Mathematisch Instituut
 Universiteit Leiden
 Postbus 9512
 2300 RA Leiden, The Netherlands
 E-mail: evertse@math.leidenuniv.nl

Received on 22.8.2013
 and in revised form on 22.10.2013

(7563)