Leiden University

Master Thesis

The Catalan Equation

Author:
Peter Koymans

Supervisor:
J.H. Evertse

June 24, 2015

Contents

1 Introduction

In 1844, Catalan conjectured that 8 and 9 are the only consecutive positive integers which both are perfect powers. More formally, the only solution in the natural numbers of

$$x^p - y^q = 1 \tag{1}$$

for $p, q > 1$, $x, y > 0$ is $x = 3$, $p = 2$, $y = 2$, $b = 3$. Cassels [8] made the weaker conjecture that (1) has only finitely many solutions in positive integers $x > 1$, $y > 1$, $p > 1$, $q > 1$. The latter conjecture was proven by Tijdeman [19]. His proof heavily relies on the theory of linear forms in logarithms. In section 4 we will see his proof using more recent and improved bounds for linear forms in logarithms. A key point of Tijdemans proof is that it is effective in the sense that an upper bound for the solutions can be computed.

Despite Tijdemans work, Catalan's conjecture remained unproven until 2002. The problem was that the bounds resulting from Tijdemans work were exceedingly large. In 2002, Mihăilescu [15] was able to prove Catalan's conjecture using algebraic methods.

Here, we consider Catalan's equation over other integral domains. Together with Brindza and Győry, Tijdeman was able to generalize his proof to the ring of integers of a number field K, see [6]. They showed that there exists an effectively computable number C which depends only on K such that all solutions of the equation

$$x^p \pm y^q = 1 \text{ in } x, y \in \mathcal{O}_K, p, q \in \mathbb{N}$$

with x, y not roots of unity and $p > 1$, $q > 1$, $pq > 4$ satisfy

$$\max(h(x), h(y), p, q) < C,$$

where $h(\cdot)$ denotes the absolute logarithmic height of an algebraic number.

Brindza [4] further generalized this to the ring of S-integers of a number field. However, Brindza's proof is quite technical. In section 5 we will prove Brindza's result by generalizing the proof given for the ordinary ring of integers in [6]. Furthermore, we will make the resulting upper bounds for the solutions completely explicit.

Brindza [5] also gave effective upper bounds for p and q for the Catalan equation over finitely generated domains in the case that x and y are transcendental. In section 6 we will strengthen his result by giving explicit upper bounds for p and q without restrictions on x and y. This will be our main theorem, which we state below.

Let $A = \mathbb{Z}[z_1, \ldots, z_r]$ be an integral domain finitely generated over $\mathbb{Z}$ of characteristic 0 with $r > 0$ and denote by K the quotient field of A. We have

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

where I is the ideal of polynomials $f \in \mathbb{Z}[X_1, \ldots, X_r]$ such that $f(z_1, \ldots, z_r) = 0$. Then I is prime and $I \cap \mathbb{Z} = (0)$. Furthermore, I is finitely generated. Let $d \geq 1$, $h \geq 1$ and assume that

$$I = (f_1, \ldots, f_m)$$

with $\deg f_i \leq d$, $h(f_i) \leq h$ for $i = 1, \ldots, m$. Here deg means the total degree of the polynomial f_i and $h(f_i)$ is the logarithmic height of f_i., i.e., the logarithm of the maximum of the absolute values of the coefficients of f_i.

Theorem 1. *All solutions of the equation*

$$x^p - y^q = 1$$

in positive integers p and q, $x, y \in A$ and x, y not roots of unity must satisfy

$$\max\{p, q\} < (2d)^{C_1^r}$$

if x, y are transcendental and

$$\max\{p, q\} < \exp\left(\exp\left(\exp\left((2d)^{C_2^r}(h+1)\right)\right)\right)$$

if x, y are algebraic, where C_1 and C_2 are effectively computable absolute constants.

In the case that x and y are transcendental, we will use a relatively straightforward function field argument. But the case x and y algebraic presents more difficulties. The proof uses a specialization technique. By means of a so called specialization homomorphism we embed our finitely generated domain into an algebraic number field, after which we can apply our results in section 5.

In section 7 we generalize our result to characteristic $l > 0$. We will first phrase our theorem and then make some remarks. Let $A = \mathbb{F}_l[z_1, \ldots, z_r]$ with $r > 0$ be an integral domain finitely generated over $\mathbb{F}_l$ and denote by K the quotient field of A. We have

$$A \cong \mathbb{F}_l[X_1, \ldots, X_r]/I$$

where I is the ideal of polynomials $f \in \mathbb{F}_l[X_1, \ldots, X_r]$ such that $f(z_1, \ldots, z_r) = 0$. Then I is finitely generated. Let $d \geq 1$ and assume that

$$I = (f_1, \ldots, f_m)$$

with $\deg f_i \leq d$. Here deg means the total degree of the polynomial f_i.

Theorem 2. *All solutions of the equation*

$$x^p - y^q = 1$$

in positive integers p and q coprime with l and $x, y \in A$, $x, y \notin \overline{\mathbb{F}_l}$ must satisfy

$$\max\{p, q\} < (2d)^{C_3^r},$$

where C_3 is an effectively computable absolute constant.

Note that all elements of $\overline{\mathbb{F}_l}$ are roots of unity. Hence the condition x, y not roots of unity translates to $x, y \notin \overline{\mathbb{F}_l}$. Furthermore, if we have a solution (x, y, p, q) in characteristic $l > 0$, we can apply Frobenius to get a new solution (x, y, lp, lq). So it is natural to require that p and q are coprime with l. The proof will use a similar function field argument as in section 6.

2 Preliminaries

For our proofs we will need some basic knowledge about function fields and algebraic number theory. This section covers the necessary preliminaries.

2.1 Function fields

Let k be a field. A function field K over k is a finitely generated field extension of transcendence degree 1 over k. For now we will assume that k is algebraically closed and of characteristic 0. By a valuation on K over k we mean a surjective map $v : K \to \mathbb{Z} \cup \{\infty\}$ such that

$$\begin{aligned}&v(x) = \infty \Leftrightarrow x = 0;\\ &v(xy) = v(x) + v(y),\ v(x+y) \geq \min(v(x), v(y)) \text{ for } x, y \in K;\\ &v(x) = 0 \text{ for } x \in k^*.\end{aligned}$$

Denote by M_K the set of valuations on K. Then we have the so called sum formula

$$\sum_{v \in M_K} v(x) = 0$$

for $x \in K^*$. Let $\mathbf{x} = (x_1, \dots, x_n) \in K^n \setminus \{0\}$ be a vector. We define

$$v(\mathbf{x}) := -\min(v(x_1), \dots, v(x_n)) \text{ for } v \in M_K$$

and

$$H_K^{\text{hom}}(\mathbf{x}) = H_K^{\text{hom}}(x_1, \dots, x_n) := \sum_{v \in M_K} v(\mathbf{x}).$$

We call $H_K^{\text{hom}}(\mathbf{x})$ the homogeneous height of $\mathbf{x}$ with respect to K. Let L be a finite extension of K. Then

$$H_L^{\text{hom}}(\mathbf{x}) = [L : K] H_K^{\text{hom}}(\mathbf{x})$$

Next we define the height for elements of K by

$$H_K(x) := H_K^{\text{hom}}(1, x) = -\sum_{v \in M_K} \min(0, v(x)).$$

Now we mention the most important properties of the height H_K. It is straightforward to show that

$$H_K(x) \geq 0 \text{ for } x \in K,\ H_K(x) = 0 \Leftrightarrow x \in k.$$

Furthermore, it follows from the sum formula that

$$H_K(x^m) = |m| H_K(x) \text{ for } x \in K^*, m \in \mathbb{Z},$$

$$H_K(x+y) \leq H_K(x) + H_K(y),$$

and

$$H_K(xy) \leq H_K(x) + H_K(y)$$

for $x, y \in K$. We conclude that

$$H_K(x) = \frac{1}{2}\left(H_K(x) + H_K(x^{-1})\right) = \frac{1}{2}\sum_{v \in M_K} |v(x)| \geq \frac{1}{2}|S| \text{ for } x \in K^*,$$

where S is the set of valuations $v \in M_K$ for which $v(x) \neq 0$.

Let S be a finite subset of M_K. Then the group of S-units of K is given by

$$\mathcal{O}_S^* = \{x \in K^* : v(x) = 0 \text{ for } v \in M_K \setminus S\}.$$

To each function field K over k we can associate a unique natural integer $g_{K/k}$, which is called the genus of the function field. For us the precise definition will not be important. The genus plays a key role in the following theorem.

Theorem 3. *Let K be a finite extension of $k(z)$ and S be a finite subset of M_K. Then for every solution of*

$$x + y = 1 \text{ in } x, y \in \mathcal{O}_S^* \setminus k^*$$

we have

$$\max(H_K(x), H_K(y)) \leq |S| + 2g_{K/k} - 2.$$

Proof. See Chapter I, section 3, Lemma 2 of Mason [13]. □

To apply this theorem, we need an upper bound for the genus. Such an upper bound is provided by the following lemma.

Lemma 4. *Let K be the splitting field over $k(z)$ of $F := X^m + f_1X^{m-1} + \cdots + f_m$, where $f_1, \ldots, f_m \in k[z]$. Then*

$$g_{K/k} \leq (d-1)m \cdot \max_{1 \leq i \leq m} \deg f_i,$$

where $d = [K : k(z)]$.

Proof. This is lemma H of Schmidt [16]. □

Now suppose that k is algebraically closed and of characteristic $l > 0$. As in characteristic 0 we can define the height and deduce its most important properties. Furthermore, there is the following analogue of Theorem 3.

Theorem 5. *Let K be a finite extension of $k(z)$ and S be a finite subset of M_K. Then for every solution of*

$$x + y = 1 \text{ in } x, y \in \mathcal{O}_S^* \setminus K^l$$

we have

$$\max(H_K(x), H_K(y)) \leq |S| + 2g_{K/k} - 2.$$

Proof. See Chapter VI, section 2, Lemma 10 of Mason [13]. □

We will need an upper bound for the genus in arbitrary characteristic. The following two lemmas will be sufficient for our purposes.

Lemma 6. *Let $K = k(x, y)$ be a function field over k, where x and y are related by a polynomial equation*

$$F(x, y) = 0$$

of total degree n. If F is irreducible, then we have

$$g_{K/k} \leq \frac{1}{2}(n-1)(n-2).$$

Proof. See Chapter XVI, section 6, Theorem 12 of Artin [1]. □

Lemma 7. *Let K/k be a function field. Suppose there are given two subfields F_1/k and F_2/k of K/k satisfying*

(1) $K = F_1F_2$ is the compositum of F_1 and F_2, and

(2) $[K : F_i] = n_i$ and F_i/k has genus g_i $(i = 1, 2)$.

Then the genus g of K/k is bounded by

$$g_{K/k} \leq n_1g_1 + n_2g_2 + (n_1 - 1)(n_2 - 1).$$

Proof. See Chapter III, section 3, Theorem 3.11.3 of Stichtenoth [18]. □

2.2 Algebraic number theory

We start by introducing the notion of absolute value, which makes sense for any infinite field. So let K be an infinite field. An absolute value on K is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ satisfying the following conditions

$$\begin{aligned}&|xy| = |x| \cdot |y| \text{ for } x, y \in K;\\&\text{there is } C \geq 1 \text{ such that } |x + y| \leq C \max(|x|, |y|) \text{ for } x, y \in K;\\&|x| = 0 \Leftrightarrow x = 0.\end{aligned}$$

From now on, we let K be an algebraic number field. Our goal will be to introduce a collection of absolute values $\{|\cdot|_v\}$ on K. To do this, we will use the notion of places. A real place of K is a set $\{\sigma\}$ where $\sigma : K \to \mathbb{R}$ is a real embedding of K. A complex place of K is a pair $\{\sigma, \overline{\sigma}\}$ of conjugate complex embeddings $K \to \mathbb{C}$. An infinite place is a real or complex place. A finite place of K is a non-zero prime ideal of $\mathcal{O}_K$. Denote by M_K the set of all places of K.

It turns out that we can associate to every place $v \in M_K$ an absolute value $|\cdot|_v$, which we define as follows for $\alpha \in K$

$$\begin{aligned}&|\alpha|_v := |\sigma(\alpha)| \text{ if } v = \{\sigma\} \text{ is real};\\&|\alpha|_v := |\sigma(\alpha)|^2 = |\overline{\sigma}(\alpha)|^2 \text{ if } v = \{\sigma, \overline{\sigma}\} \text{ is complex};\\&|\alpha|_v := N_K(\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(\alpha)} \text{ if } v = \mathfrak{p} \text{ is a prime ideal of } \mathcal{O}_K.\end{aligned}$$

Then we have the so called product formula over K

$$\prod_{v \in M_K} |\alpha|_v = 1$$

for $\alpha \in K^*$. Later on it will be useful to deal with all absolute values simultaneously. For this we have the useful inequality

$$|x_1 + \ldots + x_n| \leq n^{s(v)} \max(|x_1|_v, \ldots, |x_n|_v)$$

for $v \in M_K$, $x_1, \ldots, x_n \in K$, where $s(v) = 1$ if v is real, $s(v) = 2$ if v is complex and $s(v) = 0$ if v is finite. Furthermore, $|\alpha|_v^{1/2}$ satisfies the triangle inequality for all $v \in M_K$.

Let S denote a finite subset of M_K containing all infinite places. Write $s = |S|$. We define the ring of S-integers by

$$\mathcal{O}_S := \{\alpha \in K : |\alpha|_v \leq 1 \text{ for all } v \in M_K \setminus S\}.$$

This is a subring of K containing $\mathcal{O}_K$, hence it is a Dedekind domain. Concretely, this means that every non-zero proper ideal factors uniquely into prime ideals.

Let W_K denote the group of roots of unity of K. Then we have the following important generalization of the well-known Dirichlet's unit theorem.

Theorem 8. *We have*

$$\mathcal{O}_S^* \cong W_K \times \mathbb{Z}^{s-1}.$$

More explicitly, there are $\varepsilon_1, \ldots, \varepsilon_{s-1} \in \mathcal{O}_S^*$ such that every $\varepsilon \in \mathcal{O}_S^*$ can be expressed uniquely as

$$\varepsilon = \zeta \varepsilon_1^{b_1} \cdots \varepsilon_{s-1}^{b_{s-1}},$$

where ζ is a root of unity of K and $b_1, \ldots, b_{s-1}$ are rational integers.

Proof. See Corollary 1.8.2 in [10]. □

A system $\{\varepsilon_1, \ldots, \varepsilon_{s-1}\}$ as above is called a fundamental system of S-units. Write $S = \{v_1, \ldots, v_s\}$. We define the S-regulator by

$$R_S := \left|\det\left(\log|\varepsilon_i|_{v_j}\right)_{i,j=1,\ldots,s-1}\right|,$$

Then $R_S \neq 0$ and furthermore R_S is independent of the choice of $\varepsilon_1, \ldots, \varepsilon_{s-1}$ and of the choice $v_1, \ldots, v_{s-1}$ of S.

We define the absolute multiplicative height of $\alpha \in K$ by

$$H(\alpha) := \prod_{v \in M_K} \max(1, |\alpha|_v)^{1/[K:\mathbb{Q}]}.$$

Next we define the absolute logarithmic height by

$$h(\alpha) := \log H(\alpha).$$

Let $\alpha, \alpha_1, \ldots, \alpha_n \in K$ and $m \in \mathbb{Z}$. Then we have the following important properties

$$h(\alpha_1 \cdots \alpha_n) \leq \sum_{i=1}^{n} h(\alpha_i);$$

$$h(\alpha_1 + \cdots + \alpha_n) \leq \log n + \sum_{i=1}^{n} h(\alpha_i);$$

$$h(\alpha^m) = |m| h(\alpha) \text{ if } \alpha \neq 0.$$

For a proof of the above properties, see chapter 3 in [21]. Furthermore, we have Northcott's theorem.

Theorem 9. *Let D, H be positive reals. Then there are only finitely many $\alpha \in \overline{\mathbb{Q}}$ such that $\deg \alpha \leq D$ and $h(\alpha) \leq H$.*

Proof. See Theorem 1.9.3 in [10]. $\square$

3 Lemmas

In this section we will formulate the necessary lemmas. This section is subdivided into three subsections. In the first subsection we will give some algebraic lemmas. In the second and third subsection we cover advanced lemmas concerning linear forms in logarithms and the hyperelliptic equation.

Let K be a number field of degree d, discriminant D_K and denote by M_K the set of places of K. Let S be a finite subset of M_K containing all infinite places. Write $s = |S|$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ be the prime ideals in S. From now on $f_1, f_2, \ldots$ are effectively computable absolute constants and $c_1, c_2, \ldots$ are effectively computable constants depending only on K and S. Put

$$P := \max\{N(\mathfrak{p}_1), \ldots, N(\mathfrak{p}_t)\} \text{ if } t > 0, P := 2 \text{ if } t = 0$$

and

$$Q := N(\mathfrak{p}_1 \cdots \mathfrak{p}_t) \text{ if } t > 0, Q := 1 \text{ if } t = 0.$$

3.1 Algebraic lemmas

Our first lemma gives a lower bound for the height of $\alpha \in K$.

Lemma 10. *Let $\alpha \in K$, $\alpha \neq 0$, α not a root of unity. Then*

$$dh(\alpha) \geq \frac{\log 2}{(\log(3d))^3} =: c_1. \tag{1}$$

Proof. This follows from the work in [20]. □

Now we need some results on S-units.

Lemma 11. *There is a fundamental system of S-units $\{\eta_1, \ldots, \eta_{s-1}\}$ and an effectively computable absolute constant f_1 such that*

(i) $\prod_{i=1}^{s-1} h(\eta_i) \leq (2s)^{f_1 s} R_S$,

(ii) $h(\eta_i) \leq (2s)^{f_1 s} R_S$ *for* $i = 1, \ldots, s-1$,

(iii) the absolute values of the entries of the inverse of the matrix $(\log |\eta_i|_{v_j})_{i,j=1,\ldots,s-1}$ *do not exceed* $(2s)^{f_1 s}$.

Proof. This is a less precise version of Lemma 1 in [7]. □

Let h denote the class number of K, let r be the unit rank and let R be the regulator of K. Put

$$c_2 := \begin{cases} 0 & \text{if } r = 0, \\ 1/d & \text{if } r = 1, \\ 29er!r\sqrt{r-1}\log d & \text{if } r \geq 2. \end{cases}$$

Define the S-norm of $\alpha \in K$ by $N_S(\alpha) := \prod_{v \in S} |\alpha|_v$. More generally, define

$$M_S(\alpha) := \max\left(\prod_{v \in M_K \setminus S} \max(1, |\alpha|_v), \prod_{v \in M_K \setminus S} \max(1, |\alpha|_v^{-1})\right)$$

for $\alpha \in K^*$. By the product formula we have

$$M_S(\alpha) = \prod_{v \in M_K \setminus S} |\alpha|_v^{-1} = N_S(\alpha) \text{ for } \alpha \in \mathcal{O}_S \setminus \{0\}.$$

Lemma 12. *Let $\alpha \in K^*$ and let n be a positive integer. Then there exists $\varepsilon \in \mathcal{O}_S^*$ such that*

$$h(\varepsilon^n \alpha) \leq \frac{1}{d} \log M_S(\alpha) + n \left(c_2 R + \frac{h}{d} \log Q \right).$$

Proof. See Proposition 4.3.12 in [10]. □

Let $\alpha, \beta \in K^*$. Put

$$H := \max\{1, h(\alpha), h(\beta)\}.$$

Lemma 13. *Every solution x, y of*

$$\alpha x + \beta y = 1 \text{ in } x, y \in \mathcal{O}_S^*$$

satisfies

$$\max(h(x), h(y)) < (2s)^{f_2 s} (P / \log P) H R_S \max\{\log P, \log^* R_S\}$$

for an effectively computable absolute constant f_2.

Proof. This is a less precise version of Corollary 4.1.5 in [10]. □

3.2 Linear forms in logarithms

Let K be an algebraic number field of degree d, and assume that it is embedded in $\mathbb{C}$. We put $\chi = 1$ if K is real, and $\chi = 2$ otherwise. Let

$$\Sigma = b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n$$

where $\alpha_1, \ldots, \alpha_n$ are $n(\geq 2)$ non-zero elements of K with some fixed non-zero values of $\log \alpha_1, \ldots, \log \alpha_n$, and $b_1, \ldots, b_n$ are rational integers, not all zero. We put

$$A_i \geq \max\{d h(\alpha_i), |\log \alpha_i|, 0.16\}, i = 1, \ldots, n$$

and

$$B = \max\{1, \max\{|b_i| A_i / A_n : 1 \leq i \leq n\}\}.$$

Theorem 14. *Suppose that $\Sigma \neq 0$. Then*

$$\log |\Sigma| > -a_1(n, d) A_1 \cdots A_n \log(eB),$$

where

$$a_1(n, d) = \min \left\{ \frac{1}{\chi} \left(\frac{1}{2} e n \right)^{\chi} 30^{n+3} n^{3.5}, 2^{6n+20} \right\} d^2 \log(ed).$$

Further, B may be replaced by $\max(|b_1|, \ldots, |b_n|)$.

Proof. This is Corollary 2.3 of [14]. □

Put

$$\Lambda = \alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1 \tag{1}$$

and

$$A_i' = dh(\alpha_i) + \pi, \quad i = 1, \dots, n.$$

Lemma 15. *Suppose that $\Lambda \neq 0$, and that B' satisfies*

$$B' \geq \max\{|b_1|, \dots, |b_n|\}.$$

Then we have

$$\log|\Lambda| > -a_2(n,d) A_1' \cdots A_n' \log\left(e(n+1)B'\right),$$

where

$$a_2(n,d) = 2\pi \min\left\{ \frac{1}{\chi}\left(\frac{1}{2}e(n+1)\right)^{\chi} 30^{n+4}(n+1)^{3.5}, 2^{6n+26} \right\} d^2 \log(ed).$$

Proof. We use the principal value of the logarithm. Let z be a complex number such that $|z-1| < \frac{1}{2}$. Then

$$|\log(z)| = \left| \sum_{n=1}^{\infty} (-1)^{n-1}(z-1)^n \right| \leq |z-1| \sum_{n=1}^{\infty} |z-1|^{n-1} = |z-1| \frac{1}{1-|z-1|} < 2|z-1|.$$

Hence

$$|z-1| > \frac{1}{2}|\log(z)|.$$

We apply this with $z = \alpha_1^{b_1} \cdots \alpha_n^{b_n}$. Because we want to give a lower bound for $|z-1|$, we may assume that $|z-1| < \frac{1}{2}$. This gives

$$|z-1| > \frac{1}{2}\left|\log\left(\alpha_1^{b_1} \cdots \alpha_n^{b_n}\right)\right| = \frac{1}{2}\left|b_1 \log(\alpha_1) + \cdots + b_n \log(\alpha_n) + 2k\pi i\right|$$

for some $k \in \mathbb{Z}$. But

$$|z-1| < \frac{1}{2},$$

so taking imaginary parts

$$|k| \leq \frac{1}{2\pi}\left(1 + |b_1|\pi + \cdots + |b_n|\pi\right) \leq (n+1)B'/2.$$

Put

$$\Sigma = b_1 \log(\alpha_1) + \cdots + b_n \log(\alpha_n) + 2k\pi i = b_1 \log(\alpha_1) + \cdots + b_n \log(\alpha_n) + 2k \log(-1).$$

We apply Theorem 14 with $n+1$, $(\alpha_1, \dots, \alpha_n, -1)$ and $(b_1, \dots, b_n, 2k)$. Then

$$|\log \alpha_i| \leq \log|\alpha_i| + \pi \leq dh(\alpha_i) + \pi.$$

So we can take $A_i = A_i'$ for $i = 1, \dots, n$, $A_{n+1} = \pi$ and $B = (n+1)B'$. Our assumption $\Lambda \neq 0$ implies $\Sigma \neq 0$. Theorem 14 gives

$$\begin{aligned} |z-1| &> \frac{1}{2}\left|b_1 \log(\alpha_1) + \cdots + b_n \log(\alpha_n) + 2k\pi i\right| \\ &> \frac{1}{2}\exp(-a_1(n+1,d) A_1 \cdots A_{n+1} \log(e(n+1)B')) \end{aligned}$$

where

$$a_1(n,d) = \min\left\{\frac{1}{\chi}\left(\frac{1}{2}en\right)^{\chi} 30^{n+3}n^{3.5}, 2^{6n+20}\right\} d^2\log(ed).$$

This implies

$$\log|z-1| > -a_2(n,d)A'_1\cdots A'_n\log\left(e(n+1)B'\right)$$

where

$$a_2(n,d) = 2\pi\min\left\{\frac{1}{\chi}\left(\frac{1}{2}e(n+1)\right)^{\chi} 30^{n+4}(n+1)^{3.5}, 2^{6n+26}\right\} d^2\log(ed)$$

as desired. □

Keep the above notation and assumptions and consider again Λ as defined by (1). Let now B and B_n be real numbers satisfying

$$B \geq \max\{|b_1|,\ldots,|b_n|\}, B \geq B_n \geq |b_n|.$$

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and denote by $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$ the ramification index and the residue class degree of $\mathfrak{p}$, respectively. Suppose that $\mathfrak{p}$ lies above the rational prime number p. Then $N_K(\mathfrak{p}) = p^{f_{\mathfrak{p}}}$.

Lemma 16. *Assume that $ord_p b_n \leq ord_p b_i$ for $i = 1,\ldots,n$ and set*

$$h'_i := \max\{h(\alpha_i), 1/16e^2d^2\}, \quad i = 1,\ldots,n.$$

If $\Lambda \neq 0$, then for any real δ with $0 < \delta \leq 1/2$ we have

$$ord_{\mathfrak{p}}\Lambda < a_3(n,d)\frac{e_{\mathfrak{p}}^n N(\mathfrak{p})}{(\log N(\mathfrak{p}))^2}\max\left\{h'_1\cdots h'_n\log(M\delta^{-1}), \frac{\delta B}{B_n a_4(n,d)}\right\},$$

where

$$a_3(n,d) = (16ed)^{2(n+1)}n^{3/2}\log(2nd)\log(2d),$$
$$a_4(n,d) = (2d)^{2n+1}\log(2d)\log^3(3d),$$

and

$$M = B_n a_5(n,d)N(\mathfrak{p})^{n+1}h'_1\cdots h'_{n-1}$$

with

$$a_5(n,d) = 2e^{(n+1)(6n+5)}d^{3n}\log(2d).$$

Proof. This is the second consequence of the Main Theorem in [22]. □

3.3 The super- and hyperelliptic equation

Let

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_0 \in \mathcal{O}_S[X]$$

be a polynomial of degree $n \geq 2$ without multiple roots and let b be a non-zero element of $\mathcal{O}_S$. Put

$$\hat{h} := \frac{1}{d}\sum_{v\in M_K}\log\max(1, |b|_v, |a_0|_v, \ldots, |a_n|_v).$$

Our next lemma concerns the superelliptic equation

$$f(x) = by^m \tag{1}$$

in $x, y \in \mathcal{O}_S$ with a fixed exponent $m \geq 3$.

Lemma 17. *Assume that $m \geq 3$, $n \geq 2$. If $x, y \in \mathcal{O}_S$ is a solution to equation (1) then we have*

$$h(x), h(y) \leq (6ns)^{14m^3n^3s}|D_K|^{2m^2n^2}Q^{3m^2n^2}e^{8m^2n^3d\hat{h}}.$$

Proof. See Theorem 2.1 in [3]. □

We now consider the hyperelliptic equation

$$f(x) = by^2 \tag{2}$$

in $x, y \in \mathcal{O}_S$.

Lemma 18. *Assume that $n \geq 3$. If $x, y \in \mathcal{O}_S$ is a solution to equation (2) then we have*

$$h(x), h(y) \leq (4ns)^{212n^4s}|D_K|^{8n^3}Q^{20n^3}e^{50n^4d\hat{h}}.$$

Proof. See Theorem 2.2 in [3]. □

The following lemma is an explicit version of the Schinzel-Tijdeman theorem over the S-integers.

Lemma 19. *Assume that (1) has a solution $x, y \in \mathcal{O}_S$ where y is neither 0 nor a root of unity. Then*

$$m \leq (10n^2s)^{40ns}|D_K|^{6n}P^{n^2}e^{11nd\hat{h}}.$$

Proof. See Theorem 2.3 in [3]. □

4 A special case

In this section we will bound p and q for the Catalan equation over $\mathbb{Z}$. We will follow [19].

Setup
Consider the equation

$$x^p - y^q = 1 \tag{1}$$

in integers $p > 1$, $q > 1$, $x > 1$, $y > 1$. Our goal will be to prove the following theorem.

Theorem 20. *The equation (1) has only finitely many solutions in integers $p > 1$, $q > 1$, $x > 1$, $y > 1$. Effective bounds for the solutions p, q, x, y can be given.*

Auxiliary results
The proof of Theorem 20 is rather short, but it contains three applications of the theory of linear forms in logarithms. At the end of the proof we obtain that there are absolute bounds for p and q for every solution p, q, x, y of (1). We then complete our proof by using Lemma 17 and 18. Before we start the proof of the theorem, we first state and prove a simple lemma.

Lemma 21. *Let a be a real number such that $0 \leq a \leq \frac{1}{2}$ and let $n \geq 1$ be an integer. Then*

$$(1-a)^n + a^n \leq 1.$$

Proof. Define

$$f(a) := (1-a)^n + a^n.$$

Then f is differentiable and $f(0) = 1$. So it suffices to prove that

$$f'(a) = -n(1-a)^{n-1} + na^{n-1} \leq 0,$$

or equivalently

$$a^{n-1} \leq (1-a)^{n-1}.$$

But this is clear by our assumption on a. □

Proof of Theorem 20
We are now ready to prove Theorem 20.

Proof. Without loss of generality we may assume that p and q are different primes. Further we assume that q is odd. This last assumption is justified by Lebesgue's result that $q \neq 2$, see [11].

We have

$$x^p = y^q + 1 = (y+1)(y^{q-1} - y^{q-2} + \cdots + 1).$$

Let $d = \gcd(y+1, y^{q-1} - y^{q-2} + \cdots + 1)$. Then $y \equiv -1 \mod d$ and, hence,

$$y^{q-1} - y^{q-2} + \cdots + 1 \equiv q \mod d.$$

It follows that $d \mid q$, and therefore $d = 1$ or $d = q$. Since the product of $y + 1$ and $y^{q-1} - y^{q-2} + \cdots + 1$ is a p-th power, we find that there is a $\delta_2 \in \{-1, 0, 1\}$ and a positive integer σ such that

$$y + 1 = q^{\delta_2}\sigma^p. \tag{2}$$

In a similar way we derive from

$$y^q = x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + 1)$$

that there is a $\delta_1 \in \{-1, 0, 1\}$ and a positive integer ρ such that

$$x - 1 = p^{\delta_1}\rho^q. \tag{3}$$

On substituting (2) and (3) in (1) we obtain

$$(p^{\delta_1}\rho^q + 1)^p - (q^{\delta_2}\sigma^p - 1)^q = 1. \tag{4}$$

The equation is almost symmetrical in (p, ρ, δ_1) and (q, σ, δ_2). Since we have to distinguish the cases $p > q$ and $p < q$ and the proofs in both cases are similar in virtue of this symmetry, we assume $p > q$ in the sequel. In particular we have that $p > 2$.

We shall first prove that there exist two absolute constants C_1 and C_2 such that

$$q \leq C_1(\log p)^{C_2}. \tag{5}$$

Throughout we will use the well-known inequality

$$|\log(1 + a)| \leq a$$

for $a \geq 0$. We distinguish two cases, (a) and (b).

(a) $\rho = 1$ or $\sigma = 1$. The following argument shows that $x \leq p^2$ in both cases. Indeed, if $\sigma = 1$, then we get from (2) that $\delta_2 = 1$ and $y = q - 1$. Now it follows from (1) and $p > q$ that $x < y < q < p$. If $\rho = 1$, then we have from (3) that either $x = 2$ or $x = p+1$. We conclude that in both cases $x \leq p^2$.

By (1)

$$0 < |p \log x - q \log y| = |\log(1 + x^p y^{-q} - 1)| \leq x^p y^{-q} - 1 = \exp(-q \log y).$$

We apply Theorem 14 with $K = \mathbb{Q}$, $n = 2$, $\alpha_1 = x$, $\alpha_2 = y$, $b_1 = p$ and $b_2 = q$. Then we can choose

$$A_1 = 2\log p \geq \log x, \quad A_2 = \log y, \quad B = \max\{p, q\} = p.$$

This gives

$$|p \log x - q \log y| > \exp(-2C_3 \log p \log y \log(ep)) > \exp(-4C_3 \log y (\log p)^2)$$

for some absolute constant C_3, where we used that $p > 2$. The combination of both inequalities yields (5) in case (a).

(b) $\rho > 1$ and $\sigma > 1$. It follows from (4) and $(x-1)^p < y^q + 1 < (y+1)^q$ that

$$1 > p^{\delta_1 p}\rho^{pq}q^{-\delta_2 q}\sigma^{-pq} = \left(1 + \frac{1}{p^{\delta_1}\rho^q}\right)^{-p}((1 - q^{-\delta_2}\sigma^{-p})^q + q^{-\delta_2 q}\sigma^{-pq}).$$

Using Lemma 21 we get for $0 \le a \le \frac{1}{2}$

$$\begin{aligned}|\log((1-a)^q + a^q)| &\le |\log((1-a)^q)| = -q\log(1-a)\\ &= q\log\left(\frac{1}{1-a}\right) = q\log\left(1+\frac{a}{1-a}\right)\\ &\le \frac{aq}{1-a} \le 2aq.\end{aligned}$$

This gives

$$\begin{aligned}\left|\delta_1 p\log p - \delta_2 q\log q + pq\log\frac{\rho}{\sigma}\right| &= \left|-p\log\left(1+\frac{1}{p^{\delta_1}\rho^q}\right) + \log((1-q^{-\delta_2}\sigma^{-p})^q + q^{-\delta_2 q}\sigma^{-pq})\right|\\ &\le \frac{p}{p^{\delta_1}\rho^q} + \frac{2q}{q^{\delta_2}\sigma^p}.\end{aligned}$$

Note that indeed $0 \le q^{-\delta_2}\sigma^{-p} \le \frac{1}{2}$, since

$$\sigma^p \ge 2^p \ge 2p \ge 2q \ge 2q^{-\delta_2}$$

by our assumption $\sigma > 1$. Because $p > q$, we have $y > x$ by (1). Hence $q^{\delta_2}\sigma^p > p^{\delta_1}\rho^q$ by (2) and (3). It follows that

$$\left|\delta_1 p\log p - \delta_2 q\log q + pq\log\frac{\rho}{\sigma}\right| \le \frac{3p^2}{\rho^q}.$$

We want to prove (5). We may therefore assume that

$$q > 10\log p. \tag{6}$$

Hence, from $\rho > 1$,

$$\rho^{q/2} > \rho^{5\log p} = p^{5\log\rho} \ge p^{5\log 2} > p^3 \ge 3p^2,$$

where we used that $p > 2$. Thus,

$$0 < \left|\delta_1 p\log p - \delta_2 q\log q + pq\log\frac{\rho}{\sigma}\right| < \exp\left(-\frac{1}{2}q\log\rho\right). \tag{7}$$

It is an easy consequence of (3) and (7) that

$$\left|\log\frac{\rho}{\sigma}\right| \le \frac{2\log p}{q} + 1 < 2.$$

Hence, $\sigma < e^2\rho < \rho^4$. We can therefore apply Theorem 14 to the left-hand side of (7) with $K = \mathbb{Q}$, $n = 3$, $\alpha_1 = p$, $\alpha_2 = q$, $\alpha_3 = \rho/\sigma$, $b_1 = \delta_1 p$, $b_2 = -\delta_2 q$ and $b_3 = pq$. Then we can choose

$$A_1 = \log p, \quad A_2 = \log p \ge \log q, \quad A_3 = 4\log\rho \ge \log\max\{\sigma,\rho\}, \quad B = p^2 \ge \max\{p, q, pq\}.$$

This gives

$$\begin{aligned}\left|\delta_1 p\log p - \delta_2 q\log q + pq\log\frac{\rho}{\sigma}\right| &> \exp(-4C_4\log p\log p\log(ep^2)\log\rho) &(8)\\ &> \exp(-12C_4(\log p)^3\log\rho). &(9)\end{aligned}$$

for some absolute constant C_4, where we used that $p > 2$. The combination of (7) and (9) gives (5) in case (b). This completes the proof of (5).

Subsequently we show that there is an absolute constant C such that $p \leq C$ for every solution x, y, p, q of (1). Again we distinguish two cases, (a) and (b).

(a) $\sigma = 1$. We see from (2) that $\delta_2 = 1$ and $y = q - 1$. By (1) we obtain

$$p \log 2 \leq p \log x < q \log y + 1 < q \log q + 1.$$

It now follows from (5) that

$$p < 2q \log q < C_5 (\log p)^{C_6}$$

for some absolute constants C_5 and C_6. Hence, there is an absolute upper bound C for p in this case.

(b) $\sigma > 1$. It follows from (4) that

$$(p^{\delta_1} \rho^q + 1)^p q^{-\delta_2 q} \sigma^{-pq} = \left(1 - \frac{1}{q^{\delta_2} \sigma^p}\right)^q + \frac{1}{q^{\delta_2 q} \sigma^{pq}} < 1$$

Using our earlier estimate

$$|\log((1-a)^q + a^q)| \leq 2aq,$$

we obtain

$$\left|\delta_2 q \log q - p \log \frac{p^{\delta_1} \rho^q + 1}{\sigma^q}\right| \leq \frac{2q}{q^{\delta_2} \sigma^p} < \frac{2q^2}{\sigma^p}.$$

If $p \geq 32$, then $2q^2 < 2p^2 < 2^{p/2} \leq \sigma^{p/2}$, and

$$0 < \left|\delta_2 q \log q - p \log \frac{p^{\delta_1} \rho^q + 1}{\sigma^q}\right| \leq \exp\left(-\frac{1}{2} p \log \sigma\right). \tag{10}$$

It follows from this inequality in combination with (5) that

$$\left|\log \frac{p^{\delta_1} \rho^q + 1}{\sigma^q}\right| \leq \frac{q \log q}{p} + \frac{1}{p} \leq \frac{2C_1^2 (\log p)^{2C_2}}{p} \leq 1,$$

if $p \geq p_0$, where p_0 is some absolute constant. Since we want to prove that p is bounded, we can assume that $p \geq 32$ and $p \geq p_0$ without loss of generality.

We apply Theorem 14 with $K = \mathbb{Q}$, $n = 2$, $\alpha_1 = q$, $\alpha_2 = \frac{p^{\delta_1} \rho^q + 1}{\sigma^q}$, $b_1 = \delta_2 q$ and $b_2 = p$. Then we can choose

$$A_1 = \log p \geq \log q, \quad A_2 = \log \sigma^{2q} \geq \log e\sigma^q \geq \log \max\{p^{\delta_1} \rho^q + 1, \sigma^q\}, \quad B = \max\{p, q\} = p.$$

On using (5) we obtain absolute constants C_7 and C_8 such that

$$\left|\delta_2 q \log q - p \log \frac{p^{\delta_1} \rho^q + 1}{\sigma^q}\right| \geq \exp\left(-C_7 (\log p)^{C_8} \log \sigma\right). \tag{11}$$

The combination of (10) and (11) yields

$$p \leq 2C_7 (\log p)^{C_8}.$$

Hence, in both cases (a) and (b) there exists an effectively computable upper bound for p. By (5) this gives at the same time an effectively computable upper bound for q. The case $q > p$ leads similarly to effective upper bounds for p and q. □

5 The algebraic case

We will give bounds for the solutions of the Catalan equation over the ring of S-integers of a number field K. This was already proven in [4], but our proof is less technical. We will also make the bounds explicit. Instead of following [4], we generalize the proof in [6] dealing with the Catalan equation for the ordinary ring of integers.

Setup
Let K be a number field of degree d, discriminant D_K and denote by M_K the set of places of K. Let S be a finite subset of M_K containing all infinite places. Write $s = |S|$. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ be the prime ideals in S. Put

$$P := \max\{2, N(\mathfrak{p}_1), \dots, N(\mathfrak{p}_t)\}$$

and

$$Q := N(\mathfrak{p}_1 \cdots \mathfrak{p}_t) \text{ if } t > 0, Q := 1 \text{ if } t = 0.$$

Consider the equation

$$x^p \pm y^q = 1 \tag{1}$$

in $x, y \in \mathcal{O}_S$, $p, q \in \mathbb{N}$ with x, y not roots of unity and $p > 1$, $q > 1$, $pq > 4$.

Theorem 22. *Suppose that p and q are prime. Then there exists an effectively computable absolute constant f_3 such that all solutions of (1) satisfy*

$$\max\{p, q\} < (P^2 s)^{f_3 P s} |D_K|^{6P} P^{P^2} =: c_3 \tag{2}$$

and

$$\max\{h(x), h(y)\} < (c_3 s)^{c_3^6} |D_K|^{c_3^4} Q^{c_3^4}. \tag{3}$$

Furthermore, if p and q are arbitrary natural integers, we have

$$\max\{p, q\} < (c_3 s)^{c_3^6} |D_K|^{c_3^4} Q^{c_3^4}. \tag{4}$$

Basic lemmas
We will need an elementary lemma to make our estimates easier. Let us start by proving a prepatory lemma.

Lemma 23. *Let $A > e$, $z > 2A \log A$. Then*

$$\frac{z}{\log z} > A.$$

Proof. The function $f(z) = \frac{z}{\log z}$ is increasing for $z > e$. By our assumptions we get

$$z > 2A \log A > 2e$$

and hence

$$f(z) > f(2A \log A) = \frac{2A \log A}{\log A + \log 2 + \log \log A}.$$

So it suffices to prove

$$\frac{2A\log A}{\log A+\log 2+\log\log A} > A,$$

which is equivalent to

$$2\log A > \log A+\log 2+\log\log A.$$

But this is equivalent to

$$f(A)=\frac{A}{\log A} > 2,$$

which follows from $A>e$ and our observation that $f(z)$ is increasing for $z>e$. □

We are now ready to state and prove our final lemma.

Lemma 24. *Let $a>0$, $b>1$, $c>0$ and $x>0$. Assume that*

$$\frac{a}{\log b}c^{1/a} > e$$

and

$$b^{x/a} > 2\frac{a}{\log b}c^{1/a}\log\left(\frac{a}{\log b}c^{1/a}\right).$$

Then

$$\frac{x^a}{b^x} < c^{-1}.$$

Proof. Take $z := b^{x/a} = e^{x\log b/a}$. Then

$$\begin{aligned}\frac{x^a}{b^x} < c^{-1} \Leftrightarrow \frac{x}{z} < c^{-1/a} \Leftrightarrow \frac{\log z}{z} < \frac{\log b}{a}c^{-1/a}\\ \Leftrightarrow \frac{z}{\log z} > \frac{a}{\log b}c^{1/a}.\end{aligned}$$

Now apply Lemma 23 with z and $A := \frac{a}{\log b}c^{1/a}$. □

5.1 A key theorem

Before proving theorem 22, we generalize Lemma 6 in [6]. The proof is a more modern and simplified version of Theorem 9.3 in [17].

Setup
Consider the equation

$$x_1+x_2=y^q \tag{1}$$

in $q\in\mathbb{Z}_{>0}$, $x_1,x_2\in\mathcal{O}_S^*$ and $y\in\mathcal{O}_S$ not zero and not a S-unit.

Theorem 25. *Equation (1) implies that*

$$P(q)\le (2s)^{f_4 s}P^2R_S^4$$

for an effectively computable absolute constant f_4. Here $P(q)$ denotes the greatest prime factor of q.

Simplifications

To prove theorem 25, we first make some simplifications. We may assume $q > 1$. Further, since every power of y is a non-zero non-unit in $\mathcal{O}_S$, there is no loss of generality in assuming that q is prime.

We have the useful inequality

$$d \leq 2s,$$

which we will use throughout without further mention. We write R_S for the S-regulator. Then we have by Lemma 3 in [7]

$$R_S \geq 0.2052(\log 2)^t. \tag{2}$$

Choose a fundamental system of S-units $\{\eta_1, \ldots, \eta_{s-1}\}$ as in Lemma 11. We may write

$$x_1 = \zeta_1 \eta_1^{a_1} \cdots \eta_{s-1}^{a_{s-1}}, \quad x_2 = \zeta_2 \eta_1^{b_1} \cdots \eta_{s-1}^{b_{s-1}}$$

where $a_1, \ldots, a_{s-1}, b_1, \ldots, b_{s-1} \in \mathbb{Z}$ and $\zeta_1, \zeta_2 \in \mathcal{O}_K$ roots of unity. For $1 \leq i \leq s-1$,write

$$b_i = q b_{i,1} + b_{i,2}, \quad 0 \leq b_{i,2} < q$$

and

$$\varepsilon_1 = \eta_1^{b_{1,1}} \cdots \eta_{s-1}^{b_{s-1,1}}, \quad \varepsilon_2 = \eta_1^{b_{1,2}} \cdots \eta_{s-1}^{b_{s-1,2}}.$$

Thus $x_2 = \zeta_2 \varepsilon_2 \varepsilon_1^q$. On dividing both the sides of (1) by ε_1^q and observing that $y \varepsilon_1^{-1}$ is a non-zero non-unit in $\mathcal{O}_S$, we may assume that

$$0 \leq b_i < q \quad (1 \leq i \leq s-1).$$

Set

$$W = \max(|a_1|, \ldots, |a_{s-1}|, b_1, \ldots, b_{s-1}, e).$$

We will need two lemmas before proving the main theorem.

Lemmas

Here we will state and prove the necessary lemmas. We take $c_4 := (2s)^{f_5 s} P^2 R_S^2$ with f_5 sufficiently large.

Lemma 26. *Assume the above simplifications and $q > c_4$. Then*

$$W \leq c_5 q h(y) \tag{3}$$

with $c_5 := (2s)^{f_6 s} R_S q h(y)$.

Proof. By $\max(b_1, \ldots, b_{s-1}, e) < q$, (2) and Lemma 10, we may assume that

$$W = \max(|a_1|, \ldots, |a_{s-1}|).$$

Fix $v \in S$. Then we have

$$|x_1|_v = |y - x_2|_v \leq 4 \max(|y|_v, |x_2|_v).$$

Hence

$$\log |x_1|_v \leq \log 4 + \max(\log |y|_v, \log |x_2|_v) \leq \log 4 + |\log |y|_v| + |\log |x_2|_v|.$$

But

$$|\log|x_2|_v| = \left|\sum_{i=1}^{s-1} \log|\eta_i^{b_i}|_v\right| \leq \sum_{i=1}^{s-1} |b_i||\log|\eta_i|_v| \leq q\sum_{i=1}^{s-1} 2dh(\eta_i) \leq (2s)^{f_7 s} qR_S$$

by our choice of the fundamental system $\{\eta_1, \ldots, \eta_{s-1}\}$ of S-units. We conclude that

$$\log|x_1|_v \leq \log 4 + |\log|y|_v| + (2s)^{f_7 s} qR_S \leq (2s)^{f_8 s} qR_S + |\log|y|_v|.$$

Also, by the product formula,

$$-\log|x_1|_v = \sum_{\substack{w \in S \\ w \neq v}} \log|x_1|_w \leq (2s)^{f_9 s} qR_S + \sum_{\substack{w \in S \\ w \neq v}} |\log|y|_w| \leq (2s)^{f_9 s} qR_S + 2dh(y).$$

But then

$$|a_1 \log|\eta_1|_v + \cdots + a_{s-1} \log|\eta_{s-1}|_v| = |\log|x_1|_v| \leq (2s)^{f_9 s} qR_S + 2dh(y),$$

for all $v \in S$. Then in view of Lemma 11 (iii), we obtain a system of linear inequalities whose coefficient matrix has an inverse of which the elements have absolute values at most $(2s)^{f_1 s}$. Consequently,

$$W = \max(|a_1|, \ldots, |a_{s-1}|) \leq s(2s)^{f_1 s}((2s)^{f_9 s} qR_S + 2dh(y)) \leq (2s)^{f_6 s} R_S qh(y)$$

by (2) and Lemma 10. □

Lemma 27. *Assume the above simplifications and $q > c_4$. Then*

$$h(y) \leq (2s)^{f_{10} s} R_S =: c_6. \tag{4}$$

Proof. Fix $v \in S$. By (1)

$$|x_2|_v = |y^q - x_1|_v = |y^q|_v |1 - x_1 y^{-q}|_v = |y^q|_v |1 - \zeta_1 \eta_1^{a_1} \cdots \eta_{s-1}^{a_{s-1}} y^{-q}|_v.$$

We distinguish two cases, namely v archimedean and v non-archimedean. First suppose that v is archimedean. We apply Lemma 15 with $n = s+2$, $(\alpha_1, \ldots, \alpha_n) = (\zeta_1, \eta_1, \ldots, \eta_{s-1}, -1, y)$ and $(b_1, \ldots, b_n) = (1, a_1, \ldots, a_{s-1}, 2k, -q)$. For $i = 2, \ldots, s$, we use

$$dh(\alpha_i) + \pi \leq d(1 + \pi c_1^{-1})h(\alpha_i).$$

So we can take $A_i = dh(\alpha_i) + \pi$ for $i \notin \{2, \ldots, s\}$ and $A_i = d(1 + \pi c_1^{-1})h(\alpha_i)$ for $i \in \{2, \ldots, s\}$. Because we need to prove that $h(y)$ is bounded, we may suppose that $h(y) > \pi$. Then it follows that $h(y) < A_n < (d+1)h(y)$ and $B < (2s)^{f_{11} s} R_S^2 q$. Lemma 15 gives

$$|1 - x_1 y^{-q}| > \frac{1}{2}|\log\zeta_1 + a_1 \log\eta_1 + \cdots + a_{s-1}\log\eta_{s-1} + 2k\log(-1) - q\log y| > \exp(-c_7 h(y)\log q)$$

with

$$c_7 = (2s)^{f_{12} s} R_S \frac{\log(e(2s)^{f_{11} s} R_S^2 q)}{\log q}.$$

By taking f_5 sufficiently large, we get $q > e(2s)^{f_{11} s} R_S^2$ and hence

$$c_7 \leq 2(2s)^{f_{12} s} R_S.$$

Next suppose that v is non-archimedean. Suppose that v corresponds to a prime ideal $\mathfrak{p}$. We may assume that $\mathrm{ord}_{\mathfrak{p}}(q) = 0$ since $q > c_4$. We apply Lemma 16 with $n = s+1$, $(\alpha_1, \ldots, \alpha_n) = (\zeta_1, \eta_1, \ldots, \eta_{s-1}, y)$ and $(b_1, \ldots, b_n) = (1, a_1, \ldots, a_{s-1}, -q)$. Take $\delta = \frac{1}{2}$. Then $B \leq c_5 q h(y)$, $B_n = q$, $h'_n = h(y)$ by assuming $h(y) \geq \frac{1}{16} e^2 d^2$ and

$$M \leq f_{13} f_{14}^{s^2} P^{s+3} R_S q.$$

This gives

$$\begin{aligned}|1 - x_1 y^{-q}|_v &= \exp(-\log N(\mathfrak{p}) \mathrm{ord}_{\mathfrak{p}}(1 - \zeta_1 \eta_1^{a_1} \cdots \eta_{s-1}^{a_{s-1}} y^{-q})) \\ &> \exp\Big(-(2s)^{f_{15}s} P \max\Big((2s)^{f_{16}s} R_S h(y) \log(2M), c_5 h(y)\Big)\Big)\end{aligned}$$

By taking f_5 sufficiently large again, we find thanks to our assumption $q > c_4$

$$q > \sqrt[s]{2 f_{13} f_{14}^{s^2} P^{s+3} R_S}$$

and therefore

$$|1 - x_1 y^{-q}|_v > \exp\Big(-(2s)^{f_{17}s} P R_S h(y) \log q\Big).$$

We conclude that

$$|1 - x_1 y^{-q}|_v > \exp(-c_8 h(y) \log q)$$

for all $v \in S$ with

$$c_8 := (2s)^{f_{18}s} P R_S.$$

Define $S_1 = \{v \in S : |y|_v > 1\}$. Then it follows by

$$\prod_{v \in S_1} |y|_v = \prod_{v \in M_K} \max(1, |y|_v) = \exp(dh(y))$$

that

$$\begin{aligned}\exp(s(2s)^{f_7 s} q R_S) &\geq \prod_{v \in S_1} |x_2|_v = \exp(qdh(y)) \prod_{v \in S_1} |1 - x_1 y^{-q}|_v \\ &> \exp(qdh(y) - sc_8 h(y) \log q).\end{aligned}$$

Making f_5 sufficiently large gives

$$\sqrt{q} > \frac{2sc_8}{d}.$$

But we have the well-known inequality

$$\frac{q}{\log q} > \sqrt{q},$$

so

$$qdh(y) > 2sc_8 h(y) \log q.$$

We conclude that

$$\exp(s(2s)^{f_7 s} q R_S) > \exp\left(\frac{1}{2} qdh(y)\right),$$

hence

$$h(y) \leq \frac{2s}{d} (2s)^{f_7 s} R_S \leq (2s)^{f_{19}s} R_S.$$

So we can take

$$c_6 = \max\left(\pi, \frac{1}{16}e^2d^2, (2s)^{f_{19}s}R_S\right) \leq (2s)^{f_{10}s}R_S$$

proving (4). □

Proof of Theorem 25
It will now be straightforward to prove Theorem 25.

Proof. We showed earlier that

$$|1 - x_1y^{-q}|_v > \exp(-c_8h(y)\log q)$$

for all $v \in S$. We may assume that $q > c_4$ with c_4 sufficiently large so that (4) is valid. Then, because $x_2 = y^q(1 - x_1y^{-q})$ is a S-unit, we have

$$\begin{aligned} 1 &= \prod_{v\in S} |x_2|_v \\ &= \prod_{v\in S} |y|_v^q \prod_{v\in S} |1 - x_1y^{-q}|_v \\ &\geq N_S(y)^q \exp(-sc_6c_8 \log q), \end{aligned}$$

where

$$N_S(y) = \prod_{v\in S} |y|_v.$$

Because y is a non-zero non-unit in $\mathcal{O}_S$, we have $|N_S(y)| \geq 2$. Hence

$$1 \geq 2^q \exp(-sc_6c_8 \log q)$$

giving

$$sc_6c_8\sqrt{q} \geq sc_9c_8 \log q \geq q \log 2.$$

We conclude that

$$q \leq \left(\frac{sc_6c_8}{\log 2}\right)^2 \leq (2s)^{f_{20}s}P^2R_S^4.$$

This gives the desired bound for q, completing the proof. □

5.2 Proof of Theorem 22

We will now prove Theorem 22 in several steps.

A: simplifications
Let x, y, p, q be a solution of (1) satisfying the conditions of the theorem. We first show that we can make certain assumptions without loss of generality.

Note that (4) is an easy consequence of (3). So from now on we may assume that p and q are prime and our goal will be to show (2). If we have (2), then (3) follows from Lemma 17 and 18. We may further assume that $p > 2$ and $q > 2$. Indeed, if e.g. $p = 2$, then we apply Lemma 19 with $f(X) = \pm(X^2 - 1)$ to conclude that q is bounded.

If q is a prime with $q > 2$, then q is odd. Hence we may restrict our attention to the equation

$$x^p + y^q = 1 \tag{1}$$

in $x, y \in \mathcal{O}_S$, $p, q \in \mathbb{N}$ with p and q primes, since we can replace y by $-y$ when necessary.

It is further no restriction to assume that neither x nor y is an S-unit. Indeed, if both x and y are S-units, then (1) and Lemma 13 with $\alpha = \beta = 1$ imply

$$h(x^p) = ph(x) \leq (2s)^{f_{21}s} P^2 R_S^2$$

and

$$h(y^q) = qh(y) \leq (2s)^{f_{21}s} P^2 R_S^2,$$

whence we are done by Lemma 10. If exactly one of x, y is an S-unit, x say, then by applying Theorem 25 with $x_1 = -x^p$, $x_2 = 1$ to $-x^p + 1 = y^q$, we obtain

$$q \leq (2s)^{f_{22}s} P^2 R_S^4$$

and

$$p \leq (2s)^{f_{23}s} P^2 R_S^6,$$

giving us the desired bounds.

We may also assume that $h(x) > 3$ and $h(y) > 3$. Indeed, suppose e.g. that $h(y) \leq 3$. Observe that there are only finitely many $y \in K$ such that $h(y) \leq 3$. Now take S' large enough such that all $y \in K$ with $h(y) \leq 3$ become S'-units. If x becomes an S'-unit, we apply Lemma 13. Otherwise we apply Theorem 25.

If $p = q$, then x^p, $-xy$ is a solution of the equation

$$u(u-1) = v^p$$

in $u, v \in \mathcal{O}_S$. But xy is not an S-unit so certainly not a root of unity. Hence, by Lemma 19, we have

$$p = q \leq (2s)^{f_{24}s} |D_K|^{12} P^4.$$

So we may assume without loss of generality that $p > q$.

Finally, we may assume that $q > c_{10} := P \geq 2$. Indeed, if $q \leq c_{10}$, then we apply Lemma 19 with $f(Y) = 1 - Y^q$ to conclude that

$$p \leq (P^2 s)^{f_{25}Ps} |D_K|^{6P} P^{P^2}. \tag{2}$$

B: a special case

By A) we may restrict our attention to equation (1) in non-zero non-S-units $x, y \in \mathcal{O}_S$ with $h(x) > 3$ and $h(y) > 3$ and primes p, q with $p > q > c_{10} \geq 2$. We first deal with the special case that

$$(x-1)^p + (y-1)^q = 0, \tag{3}$$

which can be dealt with in an elementary way.

If $\mathfrak{p} \mid x - 1$ for some prime ideal $\mathfrak{p}$ in $\mathcal{O}_S$, then (3) implies $\mathfrak{p} \mid y - 1$. But it follows then from (1) that $\mathfrak{p} \mid x$. Hence $\mathfrak{p} \mid 1$ which is impossible. Thus $x - 1$ is an S-unit and, by (3), $y - 1$ is also an S-unit.

Subsequently we show that there is an S-unit ε such that

$$x = 1 - \varepsilon^q \text{ and } y = 1 + \varepsilon^p.$$

Let $w \in \overline{\mathbb{Q}}$ be such that $w^q = 1 - x$. Then $w^{pq} = (y-1)^q$. Hence $w^p = \rho(y-1)$ with ρ a qth root of unity. For any qth root of unity ζ we have $(\zeta w)^q = 1 - x$ and $(\zeta w)^p = \zeta^p \rho(y-1)$. By $\gcd(p,q) = 1$ we can choose ζ such that $\zeta^p = \rho^{-1}$. Put $\varepsilon = \zeta w$. Then $\varepsilon^q = 1 - x$ and $\varepsilon^p = y - 1$. Hence $\varepsilon^p, \varepsilon^q \in K$. Since $\gcd(p,q) = 1$, we find $\varepsilon \in K$ by applying Euclid's algorithm to the exponents. But ε^p is an S-unit, thus ε is also an S-unit. Furthermore,

$$3 < h(y) \leq h(1) + h(\varepsilon^p) + \log 2 = ph(\varepsilon) + \log 2$$

hence ε is not a root of unity. Therefore we have by Lemma 10

$$dh(\varepsilon) > c_1. \tag{4}$$

Let $\mathfrak{p}$ be an arbitrary prime ideal divisor of q in $\mathcal{O}_S$. (1) and (3) imply that

$$(x-1)^p \equiv 1 - y^q \equiv x^p \mod \mathfrak{p}. \tag{5}$$

Since $x - 1$ is an S-unit, we have $\mathfrak{p} \nmid x - 1$ and so, by (5), $\mathfrak{p} \nmid x$. There is an $x' \in \mathcal{O}_S$ with $\mathfrak{p} \nmid x'$ and $xx' \equiv 1 \mod \mathfrak{p}$. Hence (5) gives

$$((x-1)x')^p \equiv 1 \mod \mathfrak{p}.$$

Here $(x-1)x' \equiv 1 - x' \not\equiv 0$ and $\not\equiv 1 \mod \mathfrak{p}$. This means that p is the smallest positive integer t for which

$$(1 - x')^t \equiv 1 \mod \mathfrak{p}.$$

But

$$(1 - x')^{N(\mathfrak{p})-1} \equiv 1 \mod \mathfrak{p},$$

hence $p \mid N(\mathfrak{p}) - 1$ in $\mathbb{Z}$. Since $N(\mathfrak{p}) = q^f$ with some positive integer $f \leq d$, we obtain

$$p \leq q^d. \tag{6}$$

Using (4) and (6), we shall now prove that q is bounded. Take a place $v \in S$ such that $|\varepsilon|_v \geq H(\varepsilon)^{d/s}$. Then

$$|\varepsilon|_v \geq H(\varepsilon)^{d/s} = \exp(h(\varepsilon)d/s) \geq 1 + h(\varepsilon)d/s > 1 + c_1/s \tag{7}$$

by (4). Put

$$f(z) = (1 - z^q)^p + (1 + z^p)^q - 1.$$

Then

$$0 = f(\varepsilon) = \sum_{k=0}^{p} \binom{p}{k} (-\varepsilon^q)^k + \sum_{l=0}^{q} \binom{q}{l} \varepsilon^{pl} - 1. \tag{8}$$

The leading term of f is $pz^{(p-1)q}$. First suppose that v is infinite and let $\sigma : K \to \mathbb{C}$ be an embedding corresponding to v. We may suppose that σ is the identity. Then $|\varepsilon|_v = |\varepsilon|^{s(v)}$ with $s(v) = 1$ if v is real and $s(v) = 2$ if v is complex, hence by (7)

$$|\varepsilon| > \sqrt{1 + c_1/s} =: 1 + c_{11}. \tag{9}$$

So by (8), we have

$$\begin{aligned} p|\varepsilon|^{(p-1)q} &= \left|\sum_{k=0}^{p-2}\binom{p}{k}(-\varepsilon^q)^k + \sum_{l=0}^{q-1}\binom{q}{l}\varepsilon^{pl} - 1\right| \\ &\leq q|\varepsilon|^{p(q-1)} + \sum_{k=0}^{p-2}\binom{p}{k}|\varepsilon|^{kq} + \sum_{l=1}^{q-2}\binom{q}{l}|\varepsilon|^{lp}. \end{aligned}$$

Combined with $p > q$ and (9) this gives

$$\begin{aligned} 1 &\leq |\varepsilon|^{q-p} + \frac{1}{p}\sum_{k=0}^{p-2}\binom{p}{k}|\varepsilon|^{(k-p+1)q} + \frac{1}{p}\sum_{l=1}^{q-2}\binom{q}{l}|\varepsilon|^{(l-q)p+q} \\ &\leq \frac{1}{|\varepsilon|} + \frac{1}{p}\sum_{k=1}^{p-1}\binom{p}{k+1}|\varepsilon|^{-kq} + \frac{1}{p}\sum_{l=1}^{q-2}\binom{q}{l+1}|\varepsilon|^{-lp} \\ &< \frac{1}{|\varepsilon|} + \sum_{k=1}^{\infty}p^k|\varepsilon|^{-kq} + \sum_{l=1}^{\infty}q^l|\varepsilon|^{-lp}, \end{aligned} \tag{10}$$

and subsequently, by (6) and (9),

$$\frac{p}{|\varepsilon|^p} \leq \frac{p}{|\varepsilon|^q} \leq \frac{q^d}{(1+c_{11})^q} < \frac{c_{11}}{4(1+c_{11})} < \frac{1}{2} \tag{11}$$

after taking q sufficiently large. To find a suitable lower bound for q, we want to apply Lemma 24 with $x = q$, $a = d$, $b = 1 + c_{11}$ and $c = \frac{4(1+c_{11})}{c_{11}}$. So we need to check that

$$\frac{2d}{\log(1+c_1/s)}c^{1/d} = \frac{d}{\log(1+c_{11})}c^{1/d} > e.$$

Observe that $c_1/s < 1$, hence $c_{11} < 1$. This gives

$$2dc^{1/d} \geq 4,$$

so we can apply Lemma 24. Lemma 24 tells us that we can take

$$q > (2ds)^{f_{26}}. \tag{12}$$

If $q \leq (2ds)^{f_{26}}$, then (6) gives us the desired bound for p. So from now on we may assume (12) and hence (11).

It follows from (9), (10) and (11) that

$$\frac{c_{11}}{1+c_{11}} \leq 1 - \frac{1}{|\varepsilon|} < \sum_{k=1}^{\infty}p^k|\varepsilon|^{-kq} + \sum_{l=1}^{\infty}q^l|\varepsilon|^{-lp} \leq \frac{2p}{|\varepsilon|^q} + \frac{2q}{|\varepsilon|^p} < \frac{c_{11}}{1+c_{11}},$$

a contradiction.

Now suppose that v is finite. Then (8) implies

$$\begin{aligned}|p|_v|\varepsilon|_v^{(p-1)q} &= \left|\sum_{k=0}^{p-2}\binom{p}{k}(-\varepsilon^q)^k + \sum_{l=0}^{q-1}\binom{q}{l}\varepsilon^{lp} - 1\right|_v \\ &= \left|q\varepsilon^{p(q-1)} + \sum_{k=0}^{p-2}\binom{p}{k}(-\varepsilon^q)^k + \sum_{l=1}^{q-2}\binom{q}{l}\varepsilon^{lp}\right|_v \\ &\leq \max_{i,j}\left(|q|_v|\varepsilon|_v^{p(q-1)}, \left|\binom{p}{i}(-\varepsilon^q)^i\right|_v, \left|\binom{q}{j}\varepsilon^{jp}\right|_v\right),\end{aligned}$$

where the maximum is taken over $i = 0, \dots, p-2$ and $j = 1, \dots, q-2$. Hence

$$1 \leq \max_{i,j}\left(\left|\frac{q}{p}\right|_v |\varepsilon|_v^{q-p}, \left|\frac{1}{p}\binom{p}{i}\right|_v |\varepsilon|_v^{(i-p+1)q}, \left|\frac{1}{p}\binom{q}{j}\right|_v |\varepsilon|_v^{(j-q)p+q}\right).$$

If p is sufficiently large as we may assume, we have

$$\left|\frac{1}{p}\right|_v = 1.$$

So we get by $p > q$

$$1 \leq |\varepsilon|_v^{-1},$$

a contradiction.

C: ideal arithmetic
In view of A) and B) we restrict our further attention to equation (1) in non-zero non-S-units $x, y \in \mathcal{O}_S$ with $h(x) > 3$ and $h(y) > 3$ and primes p, q with $p > q > c_{10} \geq 2$ such that

$$(x-1)^p + (y-1)^q \neq 0. \tag{13}$$

For any $\alpha \in K$ we denote by $[\alpha]$ the fractional principal ideal of $\mathcal{O}_S$ generated by α. We have, by (1),

$$[y]^q = [1-x][1 + x + \cdots + x^{p-1}] = [x-1][\beta(x-1) + p]$$

for some $\beta \in \mathcal{O}_S$. Assuming $p > P$, we can write

$$[p] = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$$

where $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are distinct prime ideals in $\mathcal{O}_S$, $r \leq d$, and $a_1, \dots, a_r$ are positive integers not exceeding d. If, for some prime ideal $\mathfrak{p}$ and positive integer a, $\mathfrak{p}^a$ is a common divisor of $[x-1]$ and $[\beta(x-1) + p]$ then $\mathfrak{p}^a \mid [p]$ and therefore $a \leq d$. Hence we can write

$$[x-1] = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_r^{b_r}\mathfrak{a}^q$$

where $\mathfrak{a}$ is an integral ideal and $b_1, \dots, b_r$ are rational integers with absolute values at most d. Since $N(\mathfrak{p}_i) = p^{f_i}$ for some positive integer $f_i \leq d$, we have

$$p^{-d^2} \leq N(\mathfrak{p}_i^{b_i}) \leq p^{d^2} \quad (i = 1, \dots, r).$$

Let h denote the class number of K. We have

$$[x-1]^h = (\mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_r^{b_r})^h \mathfrak{a}^{hq}. \tag{14}$$

Here $\mathfrak{a}^h = [\kappa]$ and $(\mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_r^{b_r})^h = [\pi_0]$ for some $\kappa \in \mathcal{O}_S$ and $\pi_0 \in K$ such that $\pi_0 = \frac{\pi_1}{\pi_2}$ with $\pi_1, \pi_2 \in \mathcal{O}_S$ and

$$|\log N(\pi_k)| \leq d^3 h \log p \quad (k = 0, 1, 2). \tag{15}$$

It follows from (14) that

$$(x-1)^h = \varepsilon \pi_0 \kappa^q \tag{16}$$

for some S-unit ε. By virtue of Lemma 11 and Lemma 12 and (15) and (16) there are fundamental S-units $\eta_1, \ldots, \eta_{s-1}$ such that $h(\eta_i) \leq (2s)^{f_1 s}$ and that

$$(x-1)^h = \eta_1^{u_1} \cdots \eta_{s-1}^{u_{s-1}} \theta_0 w^q \tag{17}$$

where the u_i are rational integers with $0 \leq u_i < q$ for $i = 1, \ldots, s-1$, $0 \neq w \in \mathcal{O}_S$ and $0 \neq \theta_0 \in K$ with $\theta_0 = \frac{\theta_1}{\theta_2}$ such that $\theta_1, \theta_2 \in \mathcal{O}_S$ and

$$h(\theta_k) \leq \frac{1}{d} \log N(\pi_k) + c_2 R + \frac{h}{d} \log Q \leq d^2 h \log p + c_2 R + \frac{h}{d} \log Q \leq (2s)^{f_{27} s} R h P \log p \tag{18}$$

for $k = 1, 2$. By making f_{27} sufficiently large, (18) also holds for $k = 0$. Similarly, we can write

$$(1-y)^h = \eta_1^{v_1} \cdots \eta_{s-1}^{v_{s-1}} \tau_0 \sigma^p \tag{19}$$

with rational integers v_i such that $0 \leq v_i < p$ for $i = 1, \ldots, s-1$, and with $0 \neq \sigma \in \mathcal{O}_S$, $0 \neq \tau_0 \in K$ such that

$$h(\tau_0) \leq (2s)^{f_{27} s} R h P \log q. \tag{20}$$

D: first bounds for p and q

We show that

$$p \leq f_{28} d^{13} s P \log Y \log p. \tag{21}$$

Let $v \in S$ be such that $|x|_v \geq H(x)^{d/s}$. Put $X = H(x)$ and $Y = H(y)$. It follows from (1) that

$$\Lambda_1 := 1 - \frac{(-y)^q}{x^p} = \frac{1}{x^p}, \tag{22}$$

whence

$$|\Lambda_1|_v = \frac{1}{|x|_v^p} \leq X^{-pd/s}. \tag{23}$$

If v is infinite, embed K in $\mathbb{C}$ using an embedding σ corresponding to v. We use Lemma 15 with $n = 2$, $(\alpha_1, \alpha_2) = (-y, x)$ and $(b_1, b_2) = (q, -p)$, giving

$$\left| 1 - \frac{(-y)^q}{x^p} \right|_v > e^{-f_{29} d^5 \log X \log Y \log(3ep)}. \tag{24}$$

Assuming $p > 3e$, (23) and (24) imply

$$p \leq f_{29} d^4 s \log Y \log p, \tag{25}$$

hence (21).

If v is finite, we apply Lemma 16 with $n = 2$, $(\alpha_1, \alpha_2) = (-y, x)$ and $(b_1, b_2) = (q, p)$. So we can take $B = B_n = p$ and $\delta = \frac{1}{2}$. By assuming p and q sufficiently large, the necessary conditions are satisfied. Because we want to prove (21) in the case v finite, we may assume that

$$p > dP \log Y.$$

Hence

$$|\Lambda_1|_v > \exp\left(-f_{30} d^{14} P \log X \log Y \log p\right). \tag{26}$$

Now (23) and (26) imply

$$p \leq f_{30} d^{13} sP \log Y \log p. \tag{27}$$

So in all cases we have (21). By estimating $|\Lambda_2|_v$ with $\Lambda_2 := 1 - \frac{(-x)^p}{y^q} = \frac{1}{y^q}$ we can prove in a similar way that

$$q \leq f_{28} d^{13} sP \log X \log p. \tag{28}$$

E: a bound for q

We shall now prove that

$$q < c_{12} (\log p)^4 \tag{29}$$

with $c_{12} = (2s)^{f_{31} s} R^3 h^3 P^4 R_S^2$. To prove this we may assume that

$$q > \log p. \tag{30}$$

Further, we may assume that

$$\min(X, Y) > p^{c_{13}} \tag{31}$$

with $c_{13} := 4s/d$. Now if $Y \leq p^{c_{13}}$ then $q < p \leq f_{28} d^{13} sPc_{13} (\log p)^2$ follows from (21), whence (29). Further, in case $X \leq p^{c_{13}}$, (29) immediately follows from (28). Let $v \in S$ be such that $|x|_v \geq X^{d/s}$. From (1) we obtain

$$\left| \frac{(-y)^q}{x^p} - 1 \right|_v = \frac{1}{|x|_v^p}. \tag{32}$$

We combine the cases v real, v complex and v finite. Note that in all cases $| \cdot |_v^{1/2}$ satisfies the triangle inequality. Because $c_{13} = 4s/d$, we get $|x|_v \geq 12$. Hence

$$|x - 1|_v^{1/2} \geq |x|_v^{1/2} - |1|_v^{1/2} = |x|_v^{1/2} - 1 \geq \frac{1}{2}\sqrt{2}|x|_v^{1/2}$$

and

$$|x - 1|_v \geq \frac{1}{2}|x|_v \geq p^2 \tag{33}$$

again because $c_{13} = 4s/d$. It follows that

$$\left|\frac{x^p}{(x-1)^p} - 1\right|_v^{1/2} = \left|\frac{((x-1)+1)^p - (x-1)^p}{(x-1)^p}\right|_v^{1/2} \leq \sum_{i=1}^{p}\left(\frac{p^i}{|x-1|_v^i}\right)^{1/2} \leq p\left(\frac{p}{|x-1|_v}\right)^{1/2}$$

and after squaring

$$\left|\frac{x^p}{(x-1)^p} - 1\right|_v \leq \frac{p^3}{|x-1|_v} \leq \frac{2p^3}{|x|_v}. \tag{34}$$

Furthermore, by (1), $p > q$ and $|x|_v \geq 12$

$$\frac{|y|_v^{q/2}}{|x|_v^{q/2}} \geq \frac{|x|_v^{p/2} - 1}{|x|_v^{q/2}} \geq \frac{|x|_v^{p/2} - 1}{|x|_v^{p/2}} \geq \frac{1}{2} > \left(\frac{1}{2}\right)^{q/2}.$$

We conclude that

$$|y|_v \geq \frac{1}{2}|x|_v \geq p^2 > q. \tag{35}$$

Hence we have

$$\left|\frac{(1-y)^q}{(-y)^q} - 1\right|_v^{1/2} = \left|\frac{(1-y)^q + y^q}{(-y)^q}\right|_v^{1/2} \leq \sum_{i=1}^{q}\left(\frac{q^i}{|y|_v^i}\right)^{1/2} \leq q\left(\frac{q}{|y|_v}\right)^{1/2}$$

and after squaring

$$\left|\frac{(1-y)^q}{(-y)^q} - 1\right|_v \leq \frac{q^3}{|y|_v} \leq \frac{2p^3}{|x|_v}. \tag{36}$$

From (32), (34), (36) and the identity

$$z_1z_2z_3 - 1 = \prod_{i=1}^{3}(z_i - 1) + \sum_{1\leq i<j\leq 3}(z_i - 1)(z_j - 1) + \sum_{i=1}^{3}(z_i - 1),$$

we infer

$$\left|\frac{(1-y)^q}{(x-1)^p} - 1\right|_v \leq \frac{26p^6}{|x|_v} =: \frac{f_{32}p^6}{|x|_v}. \tag{37}$$

Further we have, by (1), (33) and (35),

$$\begin{aligned}\left|\frac{(1-y)^q}{(x-1)^p}\right|_v^{1/2} &= \left|\frac{(1-y)^q}{y^q}\right|_v^{1/2} \cdot \left|\frac{1-x^p}{(x-1)^p}\right|_v^{1/2} \leq 2\left(1 + \frac{1}{|y|_v^{1/2}}\right)^q\left(1 + \frac{1}{|x-1|_v^{1/2}}\right)^p \\ &\leq 2\left(1 + \frac{\sqrt{2}}{|x|_v^{1/2}}\right)^{p+q} \leq 2\left(1 + \frac{2}{p}\right)^{2p} \leq 2e^4 =: f_{33}.\end{aligned} \tag{38}$$

For

$$\Lambda_3 := \frac{(1-y)^{qh}}{(x-1)^{ph}} - 1 \tag{39}$$

we obtain, from (37) and (38),

$$|\Lambda_3|_v < \frac{f_{32}\left(1+f_{33}+\cdots+f_{33}^{h-1}\right)^2 p^6}{|x|_v} \leq \frac{f_{32}f_{33}^{2h}p^6}{|x|_v}. \tag{40}$$

Suppose now that $\Lambda_3 \neq 0$, i.e. that $(x-1)^{ph} \neq (1-y)^{qh}$. Using (39), (17) and (19), we obtain

$$\Lambda_3 = \eta_1^{e_1}\cdots\eta_{s-1}^{e_{s-1}}\tau_0^q\theta_0^{-p}\left(\frac{\sigma}{w}\right)^{pq} - 1$$

where $e_i \in \mathbb{Z}$ with $|e_i| \leq pq$ for $i = 1, \ldots, s-1$. Put $H_1 = H(\sigma)$, $H_2 = H(w)$ and $H_0 = \max(H_1, H_2)$. Then

$$H\left(\frac{\sigma}{w}\right) \leq H(\sigma)H(w) \leq H_0^2. \tag{41}$$

First suppose that v is infinite. By applying Lemma 15 to Λ_3 and using (18), (20), (41) and $p > q$ we obtain

$$|\Lambda_3|_v > \exp(-(2s)^{f_{34}s}R^2h^2P^2R_S(\log p)^3\log^* H_0)$$

if $pq > e(s+3)$. Next suppose that v is finite. By applying Lemma 16 to Λ_3 and using (18), (20), (41) and $p > q$ we obtain

$$|\Lambda_3|_v > \exp(-(2s)^{f_{35}s}R^2h^2P^3R_S(\log p)^3\log^* H_0)$$

if $pq > sRhPR_S\log p\log q$. This together with (40) gives in all cases

$$d/s\log X \leq \log|x|_v \leq (2s)^{f_{36}s}R^2h^2P^3R_S(\log p)^3\log^* H_0. \tag{42}$$

If $H_0 \leq c_{14} := e^{(2s)^{f_{37}s}RhPR_S}$, then (28) and (42) give (29). We therefore assume that $H_0 > c_{14}$.

First suppose that $H_2 > c_{14}$. Then, by (18) and (30), we have

$$\left|\frac{1}{\theta_0}\right|_v \leq H\left(\frac{1}{\theta_0}\right) = H(\theta_0) \leq e^{(2s)^{f_{27}s}RhP\log p} < e^{(2s)^{f_{27}s}RhPq} \leq H_2^{\frac{q}{4s}}$$

for all $v \in S$ by taking f_{37} sufficiently large. Hence we obtain from (17)

$$|w|_v^q \leq |x-1|_v^h\left|\frac{1}{\theta_0}\right|_v \cdot \prod_{i=1}^{s-1}\left|\frac{1}{\eta_i}\right|_v^{u_i} \leq |x-1|_v^h H_2^{\frac{q}{4s}} e^{(s-1)(2s)^{f_1 s}R_S q} < 4^{dh}X^h H_2^{\frac{q}{3s}}$$

again by taking f_{37} sufficiently large. Choosing $v \in S$ such that $|w|_v \geq H_2^{d/s}$, we obtain

$$4^{dh}X^hH_2^{\frac{q}{3s}} > |w|_v^q \geq H_2^{qd/s}.$$

Consequently, we have

$$h\log X > \frac{qd}{s}\log H_2 - \log(4^{dh}H_2^{\frac{q}{3s}}) \geq \left(\frac{d}{s}-\frac{2}{3s}\right)q\log H_2 \geq \frac{d}{3s}q\log H_2 \tag{43}$$

if $H_2^{\frac{q}{3s}} \geq c_{14}^{\frac{q}{3s}} \geq 4^{dh}$. By using (19) and (20) one can prove in a similar manner that

$$\log Y > \frac{d}{3hs} p \log H_1 \tag{44}$$

if $H_1 > c_{14}$. If $H_0 = H_2$, then (42) and (43) imply

$$q < (2s)^{f_{38}s} R^2 h^3 P^3 R_S (\log p)^3,$$

hence (29). Next suppose $H_0 = H_1$. From (1) we obtain

$$qh(y) = h(y^q) = h(x^p - 1) \leq \log 2 + h(x^p) + h(1) = \log 2 + ph(x),$$

so

$$q \log Y < \left(1 + \frac{d}{c_1} \log 2\right) p \log X. \tag{45}$$

Now (42), (44) and (45) imply

$$\frac{d}{3hs} pq \log H_0 < q \log Y < \left(1 + \frac{d}{c_1} \log 2\right) p \log X < (2s)^{f_{39}s} R^2 h^2 P^3 R_S p (\log p)^3 \log^* H_0,$$

whence (29).

F: completing the proof of E)

To prove (29) we are left with the case

$$(x-1)^{ph} = (1-y)^{qh}. \tag{46}$$

We can now repeat the argument of part E) above with

$$\Lambda_4 := \frac{(1-y)^q}{(x-1)^p} - 1$$

instead of Λ_3. So we need to derive a lower bound for $|\Lambda_4|_v$. Note that

$$\frac{(1-y)^q}{(x-1)^p}$$

is a h-th root of unity, hence

$$\frac{1}{d} \log |\Lambda_4|_v \geq -h(\Lambda_4) = -h\left(\frac{(1-y)^q}{(x-1)^p} - 1\right) \geq -\log 2 - h\left(\frac{(1-y)^q}{(x-1)^p}\right) - h(-1) = -\log 2.$$

We conclude that

$$|\Lambda_4|_v \geq 2^{-d}.$$

Now inequality (29) follows.

G: finishing the proof

We shall now prove that p is bounded from above by using (21) and (29). By (21) we may assume that $Y > 4^{s/d}$. Let $v \in S$ be such that $|y|_v \geq Y^{d/s} \geq 4$. Then, by (1),

$$\left|\frac{x^p}{(1-y)^q}\right|_v^{1/2} = \left|\frac{1-y^q}{(1-y)^q}\right|_v^{1/2} \leq \frac{2|y|_v^{q/2}}{(|y|_v^{1/2}/2)^q} \leq 4^q. \tag{47}$$

Hence, using again (1),

$$\left|\frac{x^p}{(1-y)^q} - 1\right|_v^{1/2} = \left|\frac{x^p + (y-1)^q}{(1-y)^q}\right|_v^{1/2} \leq \frac{q2^{q/2}|y|_v^{(q-1)/2}}{(|y|_v^{1/2}/2)^q} \leq \frac{4^q}{|y|_v^{1/2}}. \tag{48}$$

Putting

$$\Lambda_5 := \frac{x^{ph}}{(1-y)^{qh}} - 1,$$

it follows from (47) and (48) that

$$|\Lambda_5|_v < \frac{16^q\left(1 + 4^q + \cdots + 4^{q(h-1)}\right)^2}{|y|_v} \leq \frac{16^{q(h+1)}}{|y|_v}. \tag{49}$$

Suppose that $|\Lambda_5| \neq 0$, i.e. that $x^{ph} \neq (1-y)^{qh}$. We are going to derive a lower bound for $|\Lambda_5|$. By (19) we have

$$\frac{x^{ph}}{(1-y)^{qh}} = \eta_1^{d_1} \cdots \eta_{s-1}^{d_{s-1}} \tau_0^{-q} \left(\frac{x^h}{\sigma^q}\right)^p$$

with rational integers d_i such that $|d_i| < pq$ for $i = 1, \ldots, s-1$. We claim that

$$|x|_v \geq \frac{1}{2} H(x)^{d/s}.$$

To prove our claim, we note that

$$|y^q|_v = |1 - x^p|_v \leq 4\max(1, |x^p|_v)$$

and

$$H(x^p) = H(1 - y^q) \leq 2H(y^q).$$

Combining gives

$$|x|_v^p = |x^p|_v \geq \frac{1}{4}|y^q|_v - 1 \geq \frac{1}{4}H(y)^{qd/s} - 1 \geq \frac{1}{8}H(x)^{pd/s} - 1 \geq \left(\frac{1}{2}\right)^p H(x)^{pd/s}$$

if $p \geq 4$ and $p \geq s/d$, proving the claim. Hence, by (47) and (20),

$$\left|\frac{x^h}{\sigma^q}\right|_v \leq 4^h \left(\prod_{i=1}^{s-1} |\eta_i|_w^{-d_i}\right)^{1/p} |\tau_0|_w^{q/p} \leq 4^h e^{(s-1)(2s)^{f_1 s} R_S q} q^{(2s)^{f_{27} s} RhP}.$$

So

$$\left(\frac{1}{2}\right)^h H(x^h)^{d/s} \leq |x^h|_v \leq |\sigma^q|_v 4^h e^{(s-1)(2s)^{f_1 s} R_S q} q^{(2s)^{f_{27} s} RhP}.$$

Put $H_3 = H(\sigma)$. Then

$$H\left(\frac{x^h}{\sigma^q}\right) \le H(x^h)H(\sigma)^q \le \left(8^h e^{(s-1)(2s)^{f_1 s} R_S q} q^{(2s)^{f_{27} s} RhP}\right)^{s/d} H_3^{q(1+s/d)}. \tag{50}$$

First suppose that v is infinite. By applying Lemma 15 to

$$\Lambda_5 = \eta_1^{d_1} \cdots \eta_{s-1}^{d_{s-1}} \tau_0^{-q} \left(\frac{x^h}{\sigma^q}\right)^p - 1$$

and using (20) and (50), we obtain

$$|\Lambda_5|_v > \exp(-(2s)^{f_{40} s} R^2 h^2 P^2 R_S^2 q (\log p)^2 \log^* H_3). \tag{51}$$

Next suppose that v is finite. By applying Lemma 16 to Λ_5 and using (20), we obtain

$$|\Lambda_5|_v > \exp(-(2s)^{f_{41} s} R^2 h^2 P^3 R_S^2 q (\log p)^2 \log^* H_3) \tag{52}$$

if $pq > sRhPR_S \log p$. So in all cases

$$|\Lambda_5|_v > \exp(-(2s)^{f_{42} s} R^2 h^2 P^3 R_S^2 q (\log p)^2 \log^* H_3). \tag{53}$$

Comparing (49) and (53) we obtain

$$\log Y \le s/d \log |y|_v \le (2s)^{f_{43} s} R^2 h^2 P^3 R_S^2 q (\log p)^2 \log^* H_3. \tag{54}$$

If $H_3 \le c_{15} := e^{(2s)^{f_{44} s} RhPR_S}$ then (54) together with (21) and (29) yields

$$p \le (2s)^{f_{45} s} R^6 h^6 P^9 R_S^5 (\log p)^7.$$

Suppose now that $H_3 > c_{15}$. Then we have, analogously to (44),

$$\log Y > \frac{d}{3hs} p \log H_3. \tag{55}$$

From (29), (54) and (55) it follows now again that

$$p \le (2s)^{f_{46} s} R^5 h^6 P^7 R_S^4 (\log p)^6.$$

So in all cases

$$p \le (2s)^{f_{47} s} R^6 h^6 P^9 R_S^5 (\log p)^7,$$

whence

$$p \le (2s)^{f_{48} s} R^{12} h^{12} P^{18} R_S^{10}. \tag{56}$$

Using the well-known inequalities

$$Rh \le |D_K|^{1/2} (\log^* |D_K|)^{d-1}$$

and

$$R_S \le Rh \prod_{i=1}^{t} \log N(\mathfrak{p}_i) \le |D_K|^{1/2} (\log^* |D_K|)^{d-1} (\log P)^t,$$

we get from (56)

$$p \leq (2s)^{f_{48}s} |D_K|^{11} (\log^* |D_K|)^{22(d-1)} P^{18} (\log P)^{10t}, \tag{57}$$

completing the proof. Recall that in A) we assumed that $q > c_{10} := P \geq 2$. If $q \leq c_{10}$, we derived (2). But observe that (2) gives a significantly larger bound for p than (57). So our final bound for p is (2).

H: the remaining case

We are left with the case $x^{ph} = (1-y)^{qh}$. We can now repeat the argument of part G) above with

$$\Lambda_6 := \frac{x^p}{(1-y)^q} - 1$$

instead of Λ_5. So we need to derive a lower bound for $|\Lambda_6|_v$. Note that

$$\frac{x^p}{(1-y)^q}$$

is a h-th root of unity, hence

$$\frac{1}{d} \log |\Lambda_6|_v \geq -h(\Lambda_6) = -h\left(\frac{x^p}{(1-y)^q} - 1\right) \geq -\log 2 - h\left(\frac{x^p}{(1-y)^q}\right) - h(-1) = -\log 2.$$

We conclude that

$$|\Lambda_6|_v \geq 2^{-d}.$$

Now inequality (57) follows.

6 Specialization

In this section we will bound p and q for the Catalan equation over finitely generated domains. We will follow [5].

Notation
Let $A = \mathbb{Z}[z_1, \dots, z_r]$ be an integral domain finitely generated over $\mathbb{Z}$ with $r > 0$ of characteristic 0 and denote by K the quotient field of A. 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 $f(z_1, \dots, z_r) = 0$. Then I is prime and $I \cap \mathbb{Z} = (0)$. Furthermore, I is finitely generated. Let $d \geq 1$, $h \geq 1$ and assume that

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

with $\deg f_i \leq d$, $h(f_i) \leq h$ for $i = 1, \dots, m$. Here deg means the total degree of the polynomial f_i and $h(f_i)$ is the logarithmic height of f_i. Now we are ready to state and prove our main theorem.

Theorem 28. *All solutions of the equation*

$$x^p - y^q = 1$$

in positive integers p and q, $x, y \in A$ and x, y not roots of unity must satisfy

$$\max\{p, q\} < (2d)^{C_1^r} \tag{1}$$

if x, y are transcendental and

$$\max\{p, q\} < \exp\left(\exp\left(\exp\left((2d)^{C_2^r}(h+1)\right)\right)\right) \tag{2}$$

if x, y are algebraic, where C_1 and C_2 are effectively computable absolute constants.

Proof. We use the notation $O(\cdot)$ as an abbreviation for c times the expression between the parentheses, where c is an effectively computable absolute constant. At each occurrence of $O(\cdot)$, the value of c may be different.

Let x, y, p, q be an arbitrary solution. Without loss of generality we may assume that $z_1, \dots, z_k$ forms a transcendence basis of $K/\mathbb{Q}$. We write $t := r - k$ and rename $z_{k+1}, \dots, z_r$ as $y_1, \dots, y_t$ respectively. Define

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

Then

$$A = A_0[y_1, \dots, y_t], K = K_0(y_1, \dots, y_t).$$

By Corollary 3.4 in [9] we have $K = K_0(u)$, $u \in A$, u is integral over A_0, and u has minimal polynomial

$$F(X) = X^D + F_1 X^{D-1} + \dots + F_D$$

over K_0 with $F_i \in A_0$, $\deg F_i \leq (2d)^{\exp O(r)}$ and $h(F_i) \leq (2d)^{\exp O(r)}(h+1)$. Furthermore, Lemma 3.2(i) in [9] tells us that $D \leq d^t$.

By Lemma 3.6 in [9] there exists non-zero $f \in A_0$ such that

$$A \subseteq B := A_0[u, f^{-1}]$$

and moreover $\deg f \leq (2d)^{\exp O(r)}$ and $h(f) \leq (2d)^{\exp O(r)}(h+1)$. From now on, we will work in the larger ring B to bound p and q. So we will assume that $x, y \in B$ and bound p and q.

We distinguish two cases. First, we consider the case $k = 0$. In this case we have $A_0 = \mathbb{Z}$, $K_0 = \mathbb{Q}$ and $t = r$. Then K is a number field of degree $D \leq d^t$ and

$$|D_K| \leq D^{2D-1} \exp\left((2d)^{\exp O(r)}(h+1)\right) \leq \exp\left((2d)^{\exp O(r)}(h+1)\right)$$

by using the result on the bottom of page 335 in [12]. Let S contain all infinite valuations and all prime ideal divisors of f. Write $s = |S|$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the prime ideals in S. Put

$$P := \max\{2, N(\mathfrak{p}_1), \ldots, N(\mathfrak{p}_n)\}$$

and

$$Q := N(\mathfrak{p}_1 \cdots \mathfrak{p}_n) \text{ if } n > 0, Q := 1 \text{ if } n = 0.$$

By $h(f) \leq (2d)^{\exp O(r)}(h+1)$, it follows that

$$s \leq (2d)^{\exp O(r)}(h+1)$$

and

$$P \leq \exp\left((2d)^{\exp O(r)}(h+1)\right).$$

We conclude that

$$Q \leq |f|^D \leq \exp\left((2d)^{\exp O(r)}(h+1)\right)$$

and we can apply Theorem 22 to get (2).

Now consider the case $k > 0$. Fix an algebraic closure $\overline{K_0}$ of K_0. Put

$$T_i = \{z_1, \ldots, z_k\} \setminus \{z_i\}.$$

Let k_i be an algebraic closure of $\mathbb{Q}(T_i)$ contained in $\overline{K_0}$. Thus, A_0 is contained in $k_i[z_i]$. Define

$$M_i := k_i(z_i, u^{(1)}, \ldots, u^{(D)}),$$

where $u^{(1)}, \ldots, u^{(D)}$ are the conjugates of u over K_0. Now we need a lemma.

Lemma 29. *We have that*

$$\bigcap_{i=1}^{k} k_i = \overline{\mathbb{Q}}.$$

Proof. To prove our lemma, we need the following simple observation. If $F_1 \subseteq F_2$ are fields and $\mu, \nu \in F_2$ are algebraically independent over F_1, then

$$\overline{F_1(\mu)} \cap \overline{F_1(\nu)} = \overline{F_1}.$$

It is clear that

$$\overline{F_1(\mu)} \cap \overline{F_1(\nu)} \supseteq \overline{F_1}.$$

We will now prove the reverse inclusion. Assume the contrary and let τ be an element of $\overline{F_1(\mu)} \cap \overline{F_1(\nu)}$ with $\tau \notin \overline{F_1}$. Then τ satisfies a polynomial relation

$$f_s\tau^s + \cdots + f_1\tau + f_0 = 0$$

with $f_i \in F_1[\mu]$, $i = 0, \ldots, s$ and at least one f_i, $i \geq 0$, is not a constant in μ. Hence μ satisfies a similar non-trivial relation with coefficients from $F_1[\tau]$, that is $\mu \in \overline{F_1(\tau)}$ and the same argument gives $\nu \in \overline{F_1(\tau)}$. This is a contradiction, since μ and ν are algebraically independent over F_1.

Using the observation we find that

$$\bigcap_{i=1}^{k} k_i = \bigcap_{i=2}^{k} (k_i \cap k_1) = \bigcap_{i=2}^{k} \overline{\mathbb{Q}(T_i \setminus \{z_1\})}.$$

The lemma now follows by induction on the transcendence degree. □

We may assume that there exists an $i \in \{1, \ldots, k\}$ such that $x \notin k_i$, for otherwise $x \in k_i$ and $y \in k_i$, $i = 1, \ldots, q$; hence x, y belong to the algebraic number field $\overline{\mathbb{Q}} \cap K$ and our goal will be to apply Theorem 22. For this, we will use a so called specialization argument.

Recall that $K = K_0(u)$, $u \in A$, u is integral over A_0, and u has minimal polynomial

$$F(X) = X^D + F_1X^{D-1} + \cdots + F_D$$

over K_0 with $F_i \in A_0$, $\deg F_i \leq (2d)^{\exp O(r)}$ and $h(F_i) \leq (2d)^{\exp O(r)}(h+1)$. In the case $D = 1$, we take $u = 1$, $F(X) = X - 1$.

Let $\mathbf{y} = (y_1, \ldots, y_k) \in \mathbb{Z}^k$. We put

$$|\mathbf{y}| := \max(|y_1|, \ldots, |y_k|).$$

The substitution $z_1 \mapsto y_1, \ldots, z_k \mapsto y_k$ defines a ring homomorphism (specialization)

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

We want to extend this to a ring homomorphism from B to $\overline{\mathbb{Q}}$ and for this, we have to impose some restrictions on $\mathbf{y}$. Denote by Δ_F the discriminant of F, and let

$$H := \Delta_F F_D f.$$

It follows that $H \in A_0$. Using that Δ_F is a polynomial of degree $2D - 2$ with integer coefficients in $F_1, \ldots, F_D$, it follows easily that

$$\deg H \leq (2d)^{\exp O(r)}.$$

Let N be an integer with $N \geq (2d)^{\exp O(r)}$. Lemma 5.4 in [9] implies that if $N \geq \deg H$ then

$$T := \{\mathbf{y} \in \mathbb{Z}^k : |\mathbf{y}| \leq N, H(y) \neq 0\}$$

is non-empty. Take $\mathbf{y} \in T$ and consider the polynomial

$$F_{\mathbf{y}} := X^D + F_1(\mathbf{y})X^{D-1} + \cdots + F_D(\mathbf{y}),$$

which has D distinct zeros which are all different from 0, say $u_1(\mathbf{y}), \dots, u_D(\mathbf{y})$. Thus, for $j = 1, \dots, D$ the assignment

$$z_1 \mapsto y_1, \dots, z_k \mapsto y_k, u \mapsto u_j(\mathbf{y})$$

defines a ring homomorphism $\varphi_{\mathbf{y},j}$ from B to $\overline{\mathbb{Q}}$. It is obvious that $\varphi_{\mathbf{y},j}$ is the identity on $B \cap \mathbb{Q}$. Thus, if $\alpha \in B \cap \overline{\mathbb{Q}}$, then $\varphi_{\mathbf{y},j}(\alpha)$ has the same minimal polynomial as α and so it is conjugate to α.

Define the algebraic number fields $K_{\mathbf{y},j} := \mathbb{Q}(u_j(\mathbf{y}))$ $(j = 1, \dots, D)$. Denote by Δ_L the discriminant of an algebraic number field L. Then for $j = 1, \dots, D$ we have by Lemma 5.5 in [9] that $[K_{\mathbf{y},j} : \mathbb{Q}] \leq D$ and

$$|\Delta_{K_{\mathbf{y},j}}| \leq D^{2D-1} \left(d_0^k \cdot e^{h_0} \cdot \max(1, |\mathbf{y}|)^{d_0} \right)^{2D-2},$$

where

$$d_0 \geq \max(\deg F_1, \dots, \deg F_D), \quad h_0 \geq \max(h(F_1), \dots, h(F_D)).$$

So we can take $d_0 = (2d)^{\exp O(r)}$ and $h_0 = (2d)^{\exp O(r)}(h+1)$ giving

$$\begin{aligned} |\Delta_{K_{\mathbf{y},j}}| &\leq D^{2D-1} \left((2d)^{k \exp O(r)} \cdot \exp\left((2d)^{\exp O(r)}(h+1) \right) \cdot (2d)^{(2d)^{\exp O(r)}} \right)^{2D-2} \\ &\leq \exp\left((2d)^{\exp O(r)}(h+1) \right). \end{aligned}$$

Now pick any $j = 1, \dots, D$. Let S contain all infinite valuations and all prime ideal divisors of $f(\mathbf{y})$. Then $\varphi_{\mathbf{y},j}$ maps B to the ring of S-integers of $K_{\mathbf{y},j}$. In order to apply Theorem 22 in our previous work, we still need to bound s, P and Q.

It is easy to verify that for any $g \in A_0$, $\mathbf{y} \in \mathbb{Z}^k$,

$$\log |g(\mathbf{y})| \leq k \log \deg g + h(g) + \deg g \log \max(1, |\mathbf{y}|).$$

Applying this with f and $\mathbf{y}$ we get

$$|f(\mathbf{y})| \leq (2d)^{k \exp O(r)} \cdot \exp\left((2d)^{\exp O(r)}(h+1) \right) \cdot (2d)^{(2d)^{\exp O(r)}} \leq \exp\left((2d)^{\exp O(r)}(h+1) \right).$$

Hence

$$s \leq (2d)^{\exp O(r)}(h+1)$$

and

$$P \leq \exp\left((2d)^{\exp O(r)}(h+1) \right).$$

We conclude that

$$Q \leq |f(\mathbf{y})|^D \leq \exp\left((2d)^{\exp O(r)}(h+1) \right)$$

and we can apply Theorem 22 to get (2).

If $x \notin k_i$ for some i, then also $y \notin k_i$. Let S denote the subset of valuations v of M_i/k_i such that $v(z_i) < 0$, $v(f) > 0$, $v(x) > 0$ or $v(y) > 0$. Now let v be any valuation such that $v \notin S$. We claim that

$$v(x) = v(y) = v(1) = 0.$$

Because $v \notin S$, it follows that $v(z_i) \geq 0$. Recall that u is integral over $k[z_i]$. Together this implies that $v(u) \geq 0$. We also have that $v(f) \leq 0$, hence $v(f^{-1}) \geq 0$. But $x, y \in B$, so we get $v(x), v(y) \geq 0$. But then

$$v(x) = v(y) = v(1) = 0$$

as claimed.

Define $\Delta_i = [M_i : k_i(z_i)]$. Each valuation of $k_i(z_i)$ can be extended to at most Δ_i valuations of M_i. Hence M_i has at most Δ_i valuations with $v(z_i) < 0$ and at most $\Delta_i \deg_{z_i} f$ valuations with $v(f) > 0$. So

$$|S| \leq \Delta_i + \Delta_i \deg_{z_i} f + H_{M_i/k_i}(x) + H_{M_i/k_i}(y) \leq \Delta_i(1 + \deg f) + H_{M_i/k_i}(x) + H_{M_i/k_i}(y)$$

Now we consider

$$x^p - y^q = 1$$

as an S-unit equation. Because $x^p \notin k_i$ and $y^q \notin k_i$, we can apply Theorem 3 resulting in

$$H_{M_i/k_i}(x^p) \leq |S| + 2g_{M_i/k_i} - 2 \leq \Delta_i(1 + \deg f) + H_{M_i/k_i}(x) + H_{M_i/k_i}(y) + 2g_{M_i/k_i} - 2$$

and

$$H_{M_i/k_i}(y^q) \leq |S| + 2g_{M_i/k_i} - 2 \leq \Delta_i(1 + \deg f) + H_{M_i/k_i}(x) + H_{M_i/k_i}(y) + 2g_{M_i/k_i} - 2.$$

Define $K_i = k_i(z_i, u)$. Then we have that $[K_i : k_i(z_i)] \leq D$. Hence

$$H_{M_i/k_i}(x) = [M_i : K_i] H_{K_i/k_i}(x) \geq [M_i : K_i] = \Delta_i / [K_i : k_i(z_i)] \geq \Delta_i / D$$

and similarly for y. This gives

$$\frac{\Delta_i}{D}(p - 2 + q - 2) \leq (p-2) H_{M_i/k_i}(x) + (q-2) H_{M_i/k_i}(y) \leq 2\Delta_i(1 + \deg f) + 4g_{M_i/k_i} - 4,$$

hence

$$p + q - 4 \leq \frac{D}{\Delta_i}(2\Delta_i(1 + \deg f) + 4g_{M_i/k_i} - 4) \leq 2D(1 + \deg f) + \frac{D}{\Delta_i} 4g_{M_i/k_i}.$$

Recall that $\Delta_i = [M_i : k_i(z_i)]$ and that M_i is the splitting field of F over $k(z_i)$. So Lemma 4 gives

$$g_{M_i/k_i} \leq (\Delta_i - 1) D \max_j \deg_{z_i}(F_j) \leq \Delta_i \cdot D \cdot (2d)^{\exp O(r)}.$$

Combining gives

$$p + q - 4 \leq 2d^t(1 + (2d)^{\exp O(r)}) + 4(d^t)^2 (2d)^{\exp O(r)} \leq (2d)^{\exp O(r)}$$

and hence (1). □

7 Catalan's equation in positive characteristic

In this section we will bound p and q for the Catalan equation in characteristic $l > 0$.

Notation
Let $A = \mathbb{F}_l[z_1, \ldots, z_r]$ with $r > 0$ be an integral domain finitely generated over $\mathbb{F}_l$ and denote by K the quotient field of A. We have

$$A \cong \mathbb{F}_l[X_1, \ldots, X_r]/I$$

where I is the ideal of polynomials $f \in \mathbb{F}_l[X_1, \ldots, X_r]$ such that $f(z_1, \ldots, z_r) = 0$. Then I is finitely generated. Let $d \geq 1$ and assume that

$$I = (f_1, \ldots, f_m)$$

with $\deg f_i \leq d$. Here deg means the total degree of the polynomial f_i. Our main result in this section is as follows.

Theorem 30. *All solutions of the equation*

$$x^p - y^q = 1$$

in positive integers p and q coprime with l and $x, y \in A$, $x, y \notin \overline{\mathbb{F}_l}$ must satisfy

$$\max\{p, q\} < (2d)^{C_3^r}, \tag{1}$$

where C_3 is an effectively computable absolute constant.

Proof. Before we start with the proof, we state a key result due to Aschenbrenner. It is based on earlier work of Hermann and Seidenberg.

Lemma 31. *Let F be a field, $N \geq 1$, and $R := F[X_1, \ldots, X_N]$. Further, let A be an $n \times m$-matrix and $\mathbf{b}$ an m-dimensional column vector, both consisting of polynomials from R of degree $\leq d$ where $d \geq 1$.*

(i) The R-module of $\mathbf{x} \in R^n$ with $A\mathbf{x} = \mathbf{0}$ is generated by vectors $\mathbf{x}$ whose coordinates are polynomials of degree at most $(2md)^{2^N}$.

(ii) Suppose that $A\mathbf{x} = \mathbf{b}$ is solvable in $\mathbf{x} \in R^n$. Then it has a solution $\mathbf{x}$ whose coordinates are polynomials of degree at most $(2md)^{2^N}$.

Proof. See Theorem 3.2 and Theorem 3.4 in Aschenbrenner [2]. □

We use again the notation $O(\cdot)$ as an abbreviation for c times the expression between the parentheses, where c is an effectively computable absolute constant. At each occurrence of $O(\cdot)$, the value of c may be different.

Let x, y, p, q be an arbitrary solution. Without loss of generality we may assume that $z_1, \ldots, z_k$ forms a transcendence basis of $K/\mathbb{F}_l$. We may assume that $k > 0$, for otherwise there are no solutions by our assumption $x, y \notin \overline{\mathbb{F}_l}$.

We write $t := r - k$ and rename $z_{k+1}, \ldots, z_r$ as $y_1, \ldots, y_t$ respectively. Define

$$A_0 := \mathbb{F}_l[z_1, \ldots, z_k], \quad K_0 := \mathbb{F}_l(z_1, \ldots, z_k).$$

Then

$$A = A_0[y_1, \ldots, y_t], \quad K = K_0(y_1, \ldots, y_t).$$

Fix an algebraic closure $\overline{K_0}$ of K_0. Put

$$T_i := \{z_1, \ldots, z_k\} \setminus \{z_i\}$$

for $i = 1, \ldots, k$. Let k_i be the algebraic closure of $\mathbb{F}_l(T_i)$ in $\overline{K_0}$. Then A_0 is contained in $k_i[z_i]$. Define

$$M_i := k_i(z_i, y_1, \ldots, y_t).$$

In analogy to Lemma 29, we have

$$\bigcap_{i=1}^{k} k_i = \overline{\mathbb{F}_l}. \tag{2}$$

The proof is similar. We first show that if $F_1 \subseteq F_2$ are fields and $\mu, \nu \in F_2$ are algebraically independent over F_1, then

$$\overline{F_1(\mu)} \cap \overline{F_1(\nu)} = \overline{F_1}.$$

It is clear that

$$\overline{F_1(\mu)} \cap \overline{F_1(\nu)} \supseteq \overline{F_1}.$$

We will now prove the reverse inclusion. Assume the contrary and let τ be an element of $\overline{F_1(\mu)} \cap \overline{F_1(\nu)}$ with $\tau \notin \overline{F_1}$. Then τ satisfies a polynomial relation

$$f_s\tau^s + \ldots + f_1\tau + f_0 = 0$$

with $f_i \in F_1[\mu]$, $i = 0, \ldots, s$ and at least one f_i is not a constant in μ. Hence μ satisfies a similar non-trivial relation with coefficients from $F_1[\tau]$, that is $\mu \in \overline{F_1(\tau)}$ and the same argument gives $\nu \in \overline{F_1(\tau)}$. This is a contradiction, since μ and ν are algebraically independent over F_1.

Using this we find that

$$\bigcap_{i=1}^{k} k_i = \bigcap_{i=2}^{k} (k_i \cap k_1) = \bigcap_{i=2}^{k} \overline{\mathbb{F}_l(T_i \setminus \{z_1\})}.$$

Now (2) follows by induction on the transcendence degree.

We may assume that there exists an $i \in \{1, \ldots, k\}$ such that $x \notin k_i$. Otherwise it would follow that $x \in \overline{\mathbb{F}_l}$ by (2), contrary to our assumptions. From now on fix any i such that $x \notin k_i$, then also $y \notin k_i$.

By assumption $x, y \notin k_i$ and hence

$$H_{M_i/k_i}(x), H_{M_i/k_i}(y) \neq 0.$$

So we can write

$$x = \alpha^{l^a}, y = \beta^{l^b}$$

with $a, b \in \mathbb{Z}_{\geq 0}$ and $\alpha, \beta \notin M_i^l$. We claim that $a = b$. Suppose for the sake of contradiction that $a > b$, the other case can be dealt with similarly. Then

$$\alpha^{pl^a} - \beta^{ql^b} = 1$$

implies

$$\alpha^{pl^{a-b}} - \beta^q = 1.$$

But this implies that $\beta^q \in M_i^l$. By assumption q is coprime with l and hence $\beta \in M_i^l$, giving a contradiction. So we conclude that $a = b$ and we get

$$\alpha^p - \beta^q = 1$$

with $\alpha, \beta \notin M_i^l$.

Let S denote the subset of valuations v of M_i/k_i such that $v(z_i) < 0$, $v(y_j) < 0$ for some $j = 1, \ldots, t$, $v(\alpha) > 0$ or $v(\beta) > 0$. Now let v be any valuation such that $v \notin S$. We claim that

$$v(\alpha) = v(\beta) = v(1) = 0.$$

Because $v \notin S$, it follows that $v(z_i) \geq 0$ and $v(y_j) \geq 0$ for all $j = 1, \ldots, t$. Now $x, y \in A$ gives $v(x), v(y) \geq 0$. Therefore $v(\alpha), v(\beta) \geq 0$ and hence

$$v(\alpha) = v(\beta) = v(1) = 0$$

as claimed.

Define $\Delta_i = [M_i : k_i(z_i)]$. Before proceeding with the argument, we will bound Δ_i. It suffices to bound the degree of y_1 over $k_i(z_i)$. Write $\mathbf{X} = (X_1, \ldots, X_{k+1})$ and $\mathbf{Y} = (X_{k+2}, \ldots, X_r)$. Throughout $\mathbf{i} = (i_{k+2}, \ldots, i_r)$ will be an element of $\mathbb{Z}_{\geq 0}^{t-1}$ and we define

$$\mathbf{Y}^{\mathbf{i}} := X_{k+2}^{i_{k+2}} \cdots X_r^{i_r}.$$

Furthermore, we define

$$|\mathbf{i}| = i_{k+2} + \cdots + i_r.$$

Our goal is to make a non-zero polynomial $m(\mathbf{X}) \in \mathbb{F}_l[\mathbf{X}]$ such that

$$m(z_1, \ldots, z_k, y_1) = 0$$

with $\deg_{\mathbf{X}} m$ bounded.

Let $h(\mathbf{X}) \in K_0[Y]$ be the minimal polynomial of y_1 over K_0. By clearing denominators we may assume that $h(\mathbf{X}) \in A_0[Y]$, although h no longer needs to be monic. We find that

$$h(z_1, \ldots, z_k, y_1) = 0$$

and hence $h \in I$. So we can write

$$h(\mathbf{X}) = \sum_{j=1}^{m} g_j(\mathbf{X}, \mathbf{Y}) f_j(\mathbf{X}, \mathbf{Y})$$

with $g_1, \ldots, g_m \in \mathbb{F}_l[\mathbf{X}, \mathbf{Y}]$ to be determined. We need to find $g_1, \ldots, g_m$ satisfying the above with bounded total degree. Write for $j = 1, \ldots, m$

$$f_j(\mathbf{X}, \mathbf{Y}) = \sum_{\mathbf{i}} p_{\mathbf{i}j}(\mathbf{X}) \mathbf{Y}^{\mathbf{i}}$$

with $p_{\mathbf{i}j}(\mathbf{X}) \in \mathbb{F}_l[\mathbf{X}]$. Furthermore, write for $j = 1, \dots, m$

$$g_j(\mathbf{X}, \mathbf{Y}) = \sum_{\mathbf{i}} q_{\mathbf{i}j}(\mathbf{X})\mathbf{Y}^{\mathbf{i}},$$

where we view $g_j(\mathbf{X}, \mathbf{Y})$ as unknown polynomials in $\mathbf{Y}$ over $\mathbb{F}_l(\mathbf{X})$. So for now we only require that $q_{\mathbf{i}j}(\mathbf{X}) \in \mathbb{F}_l(\mathbf{X})$. Consider the linear equation

$$h(\mathbf{X}) = \sum_{j=1}^{m} g_j(\mathbf{X}, \mathbf{Y}) f_j(\mathbf{X}, \mathbf{Y})$$

in $\mathbb{F}_l(\mathbf{X})[\mathbf{Y}]$ with unknowns $g_j(\mathbf{X}, \mathbf{Y})$. Because $h \in I$, this equation has a solution. Hence Lemma 31 tells us that there is a solution such that $\deg_{\mathbf{Y}} g_j \leq (2d)^{\exp O(r)}$ for $j = 1, \dots, m$. Note that a priori we have $q_{\mathbf{i}j}(\mathbf{X}) \in \mathbb{F}_l(\mathbf{X})$, but by clearing denominators we may assume that in fact $q_{\mathbf{i}j}(\mathbf{X}) \in \mathbb{F}_l[\mathbf{X}]$. This amounts to multiplying $h(\mathbf{X})$ by a non-zero polynomial in $\mathbf{X}$, but for simplicity we will keep writing $h(\mathbf{X})$.

Put $N := d + (2d)^{\exp O(r)}$. By expanding

$$h(\mathbf{X}) = \sum_{j=1}^{m} g_j(\mathbf{X}, \mathbf{Y}) f_j(\mathbf{X}, \mathbf{Y}),$$

we get the following system of linear equations in $\mathbb{F}_l[\mathbf{X}]$

$$\sum_{j=1}^{m} \sum_{\substack{\mathbf{i}_1 + \mathbf{i}_2 = \mathbf{i} \\ |\mathbf{i}| \leq N \\ \mathbf{i} \neq \mathbf{0}}} r_{\mathbf{i_1}j}(\mathbf{X}) p_{\mathbf{i_2}j}(\mathbf{X}) = 0$$

with unknowns $r_{\mathbf{i_1}j}(\mathbf{X})$. Lemma 31 tells us that the solution module is generated by vectors $\mathbf{r} = (r_{\mathbf{i_1}j}(\mathbf{X}))_{\mathbf{i_1}j}$ with components satisfying

$$\deg_{\mathbf{X}} r_{\mathbf{i_1}j}(\mathbf{X}) \leq (2(2d)^{\exp O(r)} d)^{\exp O(r)} \leq (2d)^{\exp O(r)}.$$

Recall that $\mathbf{q} = (q_{\mathbf{i}j}(\mathbf{X}))_{\mathbf{i}j}$ is inside the solution module. Furthermore,

$$\sum_{j=1}^{m} q_{\mathbf{0}j}(\mathbf{X}) p_{\mathbf{0}j}(\mathbf{X}) \neq 0.$$

So there must be a generator $\mathbf{r} = (r_{\mathbf{i_1}j}(\mathbf{X}))_{\mathbf{i_1}j}$ such that

$$\sum_{j=1}^{m} r_{\mathbf{0}j}(\mathbf{X}) p_{\mathbf{0}j}(\mathbf{X}) \neq 0.$$

Now define

$$m_1(\mathbf{X}) = \sum_{j=1}^{m} r_{\mathbf{0}j}(\mathbf{X}) p_{\mathbf{0}j}(\mathbf{X}).$$

Then it follows that

$$[K_0(y_1) : K_0] \leq \deg_{\mathbf{X}} m_1(\mathbf{X}) \leq (2d)^{\exp O(r)}.$$

By following the same argument we get polynomials $m_j(\mathbf{X}) \in \mathbb{F}_l[\mathbf{X}]$ for $j = 1, \dots, t$ such that

$$[K_0(y_j) : K_0] \le \deg_{\mathbf{X}} m_j(\mathbf{X}) \le (2d)^{\exp O(r)}$$

and hence

$$\Delta_i \le (2d)^{\exp O(r)}.$$

Each valuation of $k_i(z_i)$ can be extended to at most Δ_i valuations of M_i. Hence M_i has at most Δ_i valuations with $v(z_i) < 0$ and at most $\Delta_i(1+\deg_{\mathbf{X}} m_i(\mathbf{X}))$ valuations with $v(y_j) < 0$. So

$$|S| \le (2d)^{\exp O(r)} + H_{M_i/k_i}(\alpha) + H_{M_i/k_i}(\beta).$$

Now we consider

$$\alpha^p - \beta^q = 1$$

as an S-unit equation.

Recall that $\alpha, \beta \notin M_i^l$, so we can apply Theorem 5 resulting in

$$H_{M_i/k_i}(\alpha^p) \le |S| + 2g_{M_i/k_i} - 2 \le (2d)^{\exp O(r)} + H_{M_i/k_i}(\alpha) + H_{M_i/k_i}(\beta) + 2g_{M_i/k_i} - 2$$

and

$$H_{M_i/k_i}(\beta^q) \le |S| + 2g_{M_i/k_i} - 2 \le (2d)^{\exp O(r)} + H_{M_i/k_i}(\alpha) + H_{M_i/k_i}(\beta) + 2g_{M_i/k_i} - 2.$$

This gives

$$p - 2 + q - 2 \le (p-2)H_{M_i/k_i}(\alpha) + (q-2)H_{M_i/k_i}(\beta) \le (2d)^{\exp O(r)} + 4g_{M_i/k_i} - 4.$$

We still need to bound g_{M_i/k_i}. Let L be any function field over k_i and write g_L for the genus of L over k_i. Then we need to bound g_{M_i}. Fix any $j = 1, \dots, t$ and define

$$L_j = k_i(z_i, y_j).$$

Then L_j is a function field over k_i and

$$g_{L_j} \le (2d)^{\exp O(r)}$$

by Lemma 6. By repeatedly applying Lemma 7 we get

$$g_{M_i} \le (2d)^{\exp O(r)}.$$

This proves (1). □

References

[1] E. Artin, *Algebraic Numbers and Algebraic Functions,* Notes on mathematics and its applications (1967), AMS Chelsea Publishing.

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

[3] A. Bérczes, J.H. Evertse, K. Győry, *Effective results for hyper- and superelliptic equations over number fields,* Acta Arith. 163 (2014), 71-100.

[4] B. Brindza, *On S-integral solutions of the Catalan equation,* Acta Arith. 48 (1987), 397-412.

[5] B. Brindza, *The Catalan equation over finitely generated integral domains,* Publ. Math. Debrecen 42 (1993), 193-198.

[6] B. Brindza, K. Győry, R. Tijdeman, *On the Catalan equation over algebraic number fields,* Journal für die reine und angewandte Mathematic 367 (1986), 90-102.

[7] Y. Bugeaud, K. Győry, *Bounds for the solutions of unit equations,* Acta Arith. 74 (1996), 67-80.

[8] J.W.S. Cassels, *On the equation $a^x - b^y = 1$,* Amer. J. Math. 75 (1953), 159-162.

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

[10] J.H. Evertse, K. Győry, *Unit Equations in Diophantine Number Theory,* Cambridge University Press, To appear in Fall 2015.

[11] V.A. Lebesgue, *Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$,* Nonv. Ann. Math. 9 (1850), 178-181.

[12] D.J. Lewis, K. Mahler, *On the representation of integers by binary forms,* Acta Arith. 6 (1961), 333-363.

[13] R.C. Mason, *Diophantine Equations over Function Fields,* London Mathematical Society Lecture Note Series 96 (1984), Cambridge University Press.

[14] E.M. Matveev, *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers,* Izv. Math. 62 (1998), 81-136.

[15] P. Mihăilescu, *Catalan's Conjecture: Another old Diophantine problem solved,* Bull. Amer. Math. Soc. 41 (2013), 43-57.

[16] W.M. Schmidt, *Thue's equation over function fields,* J. Austral. Math. Soc. Ser. A 25 (1978), 385-422.

[17] T.N. Shorey, R. Tijdeman, *Exponential Diophantine Equations,* Cambridge Tracts in Mathematics 87 (1986), Cambridge University Press.

[18] H. Stichtenoth, *Algebraic Function Fields and Codes,* Graduate Texts in Mathematics 254 (2009), Springer.

[19] R. Tijdeman, *On the equation of Catalan,* Acta Arith. 29 (1976), 197-209.

[20] P.M. Voutier, *An effective lower bound for the height of algebraic numbers,* Acta Arith. 74 (1996), 81-95.

[21] M. Waldschmidt, *Diophantine Approximation on Linear Algebraic Groups,* Springer-Verlag (2000), Berlin Heidelberg.

[22] Kunrui Yu, *P-adic logarithmic forms and group varieties III,* Forum Mathematicum 19 (2007), 187-280.