FACTORING BIVARIATE SPARSE (LACUNARY) POLYNOMIALS

MARTÍN AVENDAÑO, TERESA KRICK, AND MARTÍN SOMBRA

ABSTRACT. We present a deterministic algorithm for computing all irreducible factors of degree $\leq d$ of a given bivariate polynomial $f \in K[x,y]$ over an algebraic number field K and their multiplicities, whose running time is polynomial in the bit length of the sparse encoding of the input and in d. Moreover, we show that the factors over $\overline{\mathbb{Q}}$ of degree $\leq d$ which are not binomials can also be computed in time polynomial in the sparse length of the input and in d.

INTRODUCTION

Effective factorization of polynomials, when possible, is an important task in computational algebra and number theory. This problem has a long history, going back to I. Newton in 1707, and to the astronomer F. von Schubert who in 1793 presented an algorithm for factoring a univariate polynomial, later rediscovered and generalized by L. Kronecker in 1882. Many other more efficient algorithms were designed since then: we cite [Zas69], based on [Ber70], among the most famous ones.

In 1982, A.K. Lenstra, H.W. Lenstra Jr. and L. Lovász made a fundamental advance by obtaining the first deterministic polynomial-time algorithm for factoring a univariate polynomial over the rationals. Based on [LLL82] and the technique of lattice basis reduction introduced for its proof, several new factorization algorithms were obtained [CG82, Len84, Kal85, Lan85, Len87, Lec05, BHKS05]. These algorithms succeeded in bringing to polynomial time the problem of factoring univariate and multivariate polynomials over algebraic number fields when given by their *dense* encoding, that is the input f is given by the list of all its terms of degree $\leq \deg(f)$ including the zero ones.

For practical purposes, it is worth considering the *sparse* (or lacunary) encoding of a polynomial. In this paper we consider the problem of factoring a bivariate polynomial

$$f = \sum_{i=1}^{t} a_i x^{\alpha_i} y^{\beta_i} \in \mathbb{Q}[x,y]$$

given in sparse encoding, i.e. by the list $(a_i, \alpha_i, \beta_i)_{1 \leq i \leq t}$ of its non-zero coefficients and corresponding exponents. Let $\ell(f)$ denote the *bit length* of the sparse encoding of f; informally speaking this is the number of bits needed to spell out the data. We obtain a deterministic algorithm for computing the low degree factors of f in time polynomial in $\ell(f)$:

Theorem 1. *There is a deterministic algorithm that, given $f \in \mathbb{Z}[x,y]$ and $d \geq 1$, computes all irreducible factors of f in $\mathbb{Q}[x,y]$ of degree $\leq d$ together with their multiplicities, in $(d \cdot \ell(f))^{O(1)}$ bit operations.*

2000 *Mathematics Subject Classification.* Primary 11Y05; Secondary 11Y16, 11G50.

Key words and phrases. Polynomial factorization, lacunary (sparse) polynomials, height of points, Lehmer's problem.

M. Avendaño was supported by a CONICET fellowship, Argentina.

T. Krick was partially supported by research grants UBACYT X-112 and CONICET PIP 2461/01, Argentina.

M. Sombra was supported by the Ramón y Cajal program of the Ministerio de Educación y Ciencia, Spain.

Actually, this algorithm applies for factoring bivariate polynomials over number fields (see Subsection 3.2).

Let us observe that the degree of a polynomial can be exponentially big in its sparse length: we have $\deg(f) \leq 2^{\ell(f)}$ and this upper bound is attainable. A direct application of the algorithms for factoring dense polynomials would give an exponential complexity. The restriction to bounded degree factors is unavoidable: the polynomial $f = x^p - 1$ (p prime) is of sparse length $\log_2(p) + O(1)$ but has the dense irreducible factor $x^{p-1} + \cdots + 1$.

The first result in this direction appeared in 1998, when F. Cucker, P. Koiran and S. Smale showed how to find all the integer roots of a univariate polynomial with integer coefficients in polynomial time in its sparse encoding, and asked whether one can find in the same time the rational roots as well [CKS99]. This question (and more!) was affirmatively answered by H.W. Lenstra Jr. who presented an algorithm that —given a number field K and a univariate polynomial $f \in K[x]$— computes all its irreducible factors of degree $\leq d$ together with their multiplicities, in $(d+\ell(f))^{O(1)}$ bit operations [Len99b, Thm]. The first and inspiring result in the multivariate setting was obtained by E. Kaltofen and P. Koiran [KK05, Thm 3] last year, who showed how to compute the *linear* factors of a bivariate polynomial $f \in \mathbb{Q}[x, y]$ in polynomial time in $\ell(f)$. Our result is then an extension of Kaltofen-Koiran's, and a full generalization of Lenstra's to the case of bivariate polynomials.

All these algorithms (including ours) are based on a *gap* principle first applied by Cucker, Koiran and Smale. The idea is so strikingly simple and natural that it deserves to be explained. Let $f \in \mathbb{Z}[x]$ and $\xi \in \mathbb{Z}$ be given, how can we test if $f(\xi) = 0$? Direct evaluation is not feasible, as the size of $f(\xi)$ can be exponentially big in the input size; an important exception to this are the easy cases $\xi = 0, \pm 1$. For the other cases, assume that $f = \sum_{i=1}^{t} a_i x^{\alpha_i}$ can be split as

$$f = r + x^u q$$

for non-zero polynomials r of degree $\deg(r) = k$ and q, where there is a gap between the exponents of r and those of $x^u q$ of length

$$u - k \geq \log_2 ||f||_1$$

(here $||f||_1 := \sum_{i=1}^{t} |a_i|$ denotes as usual the ℓ^1 *-norm* of f). Then, except for the cases $\xi = 0, \pm 1$, this implies that $f(\xi) = 0$ if and only $q(\xi) = r(\xi) = 0$: if this were not the case, namely $f(\xi) = 0$ but $q(\xi) \neq 0$, then

$$|r(\xi)| \leq ||r||_1 \cdot |\xi|^k < ||f||_1 \cdot |\xi|^k \quad \text{and} \quad |r(\xi)| = |\xi|^u \cdot |q(\xi)| \geq |\xi|^u$$

so that $||f||_1 > |\xi|^{u-k} \geq 2^{u-k}$, which contradicts the gap assumption! Therefore, to test if f vanishes at $\xi \neq 0, \pm 1$, one decomposes f into widely spaced short pieces

$$f = \sum_i x^i f_i$$

and tests if $f_i(\xi) = 0$ for all i.

One crucial fact here is that the decomposition is independent of the point ξ; therefore to find integer roots it is enough to find the common roots of a set of low degree polynomials.
The other key ingredient that makes the above argument work is that any integer $\xi \neq 0, \pm 1$ satisfies a uniform lower bound $|\xi| \geq 2$! In order to apply the same idea to $\xi \in \mathbb{Q}$, the correct generalization of the absolute value is the *height*, defined as the maximum between relatively prime expressions for the numerator and denominator. By imitating the argument above, but this time for the usual absolute value *and* all the p-adic ones, we arrive at the same conclusion as a consequence that all rational numbers except $0, \pm 1$ have height at least 2. This is essentially what Lenstra applied in [Len99b]; more generally, he was able to handle in this way other factors besides the

linear ones by considering the height of their roots after applying a suitable lower bound for them, namely Dobrowolski's theorem [Dob79] in the version of P. Voutier [Vou96]. In [KK05], the authors succeeded to present the first generalization of this gap principle for non-univariate polynomials, more precisely for linear factors of bivariate polynomials.

As in these previous works, the key of our algorithm is a suitable gap theorem. We obtain it as a consequence of a lower bound for the height of Zariski dense points lying on a curve due to F. Amoroso and S. David [AD00], as explained in detail in Section 2. This result allows to decompose the given polynomial $f \in \mathbb{Q}[x,y]$ into short pieces; the factors of f are then computed as the common factors of these low degree pieces. This strategy works for all factors except the trivial x and y and the cyclotomic ones, that is, factors which are a product of binomials (including monomials) whose coefficients are roots of the unity. As in the univariate and linear bivariate cases, these factors have to be handled separately, see Section 3.
Since our algorithm operates by reducing to the cases of dense bivariate and sparse univariate polynomials, our concern is only to prove that this reduction can be done in polynomial time in the sparse encoding. We have not attempted to compute the exponent in the complexity estimate, which in principle can be quite big. It is certainly possible to improve it in view of practical implementation: in Subsection 3.4 we present one idea in this direction, which consists on adapting the decomposition of f to the size of the candidate factor.

As a consequence of the algorithm, we derive that the number of irreducible factors of degree $\leq d$ of $f \in \mathbb{Q}[x,y]$ counted with multiplicities (different from the trivial factors x or y) is bounded by $(d \cdot \ell(f))^{O(1)}$. This is not trivial, as the degree of f can be exponential in $\ell(f)$, but in fact much better can be said:

Proposition 2. *Let $f \in \mathbb{Z}[x_1, \ldots, x_n]$ and consider the factorization*

$$f = q \cdot \prod_p p^{e_p}$$

where q is a cyclotomic polynomial, $p \in \mathbb{Q}[x_1, \ldots, x_n]$ runs over all non-cyclotomic irreducible factors of f, and e_p is the corresponding multiplicity. Then

$$\sum_p e_p \leq 5^6 \cdot n^3 \cdot \log ||f||_1 \cdot \log^3(8n \deg(f)).$$

In particular the total number of non-cyclotomic irreducible factors of any degree of f is polynomially bounded in terms of the sparse length of f. This fairly unexpected property generalizes [Dob79, Thm 2] and is a further consequence of the connection with Diophantine Geometry *via* the theory of heights: the Amoroso-David lower bound together with the theorem of successive algebraic minima of S.-W. Zhang [Zha95] imply a lower bound for the Mahler measure of a non-cyclotomic polynomial, and from this the statement follows easily.
Moreover, a positive answer to Lehmer's problem would imply in the univariate case, see Subsection 1.2 for details, the stronger estimate

$$\sum_p e_p \leq c \cdot \log ||f||_1.$$

for some absolute constant $c > 0$. This is even more surprising, since the right-hand side depends on the coefficients of f but not on its degree. It would be interesting to determine if it is possible to obtain such a bound without assuming Lehmer's conjecture.
Proposition 2 should be compared with another result of H.J. Lenstra Jr.: the total number of irreducible factors of degree $\leq d$ of $f \in \mathbb{Q}[x]$ counted with multiplicities (different from x) is

bounded by

$$c \cdot t^2 \cdot 2^d \cdot d \cdot \log(2dt)$$

where t is the number of non zero terms of f [Len99a, Thm 1]. This bound is exponential, but independent of the degree and coefficients of f. Based on these two results, it seems natural to consider the following generalization of Descartes' rule of signs: is the number of all irreducible (and non-cyclotomic maybe?) factors different from x of a t-nomial in $\mathbb{Q}[x]$ uniformly bounded by some function $B(t)$ depending only on t, and maybe even by $t^{O(1)}$?

Trying to get further, one might ask if it is possible to compute in polynomial time the *absolute* factorization of a polynomial given in sparse encoding, that is, its irreducible factors over $\overline{\mathbb{Q}}$. For the univariate case the answer is clearly "no": a univariate polynomial splits completely as a product of linear factors, and this cannot be done in sparse polynomial time. For the bivariate case, it can be shown that the computation of binomial factors is equivalent to the factorization of a univariate polynomial, so that binomials factors over $\overline{\mathbb{Q}}$ cannot be computed either.
Here, we show that except for these, we can compute all other irreducible factors over $\overline{\mathbb{Q}}$ of low degree, in sparse polynomial time. To give sense to such a statement, we have to specify the way algebraic coefficients are handled: a number field K is described by an irreducible monic polynomial $g = \sum_{j=0}^{\delta-1} g_j z^j \in \mathbb{Z}[z]$ such that $K = \mathbb{Q}(\theta)$ for one of its roots, and this g is given in dense representation by the list of all coefficients g_j in some specified order, including the zero ones. Each irreducible factor p in the output of the algorithm is encoded by giving a number field K such that $p \in K[x, y]$ and by the dense list of its coefficients, each coefficient $b \in K$ being represented by its vector of rational components $b := (b_0, \dots, b_{\delta-1})$ with respect to the basis $(\theta^j)_{0 \le j \le \delta-1}$.

Theorem 3. *There is a deterministic algorithm that, given $f \in \mathbb{Q}[x, y]$ and $d \ge 1$, computes all irreducible factors of f in $\overline{\mathbb{Q}}[x, y]$ of degree $\le d$, together with their multiplicities, except for the binomial ones, in $(d \cdot \ell(f))^{O(1)}$ bit operations.*

This algorithm follows from another suitable gap theorem that we obtain as a consequence of a further result of Amoroso and David, a quantitative version of the Bomogolov problem over the torus [AD03]. Furthermore, we deduce from their result an estimate for the number of non-binomial factors of a given $f \in \overline{\mathbb{Q}}[x_1, \dots, x_n]$ (Proposition 1.4).

Several interesting questions arose during our work. The most obvious is the extension of these algorithms to multivariate polynomials; this seems quite feasible as the necessary lower bounds for the height of points in a hypersurface already appeared in the literature [AD00, AD03, Pon01, Pon05b].
An interesting open problem is the following: the restriction to computing bounded degree factors keeps their length under control, giving the possibility of computing them in sparse polynomial time. But, what if we look for factors with a fixed number of monomials, can we still find all of them in sparse polynomial time? For instance, can we compute all trinomial factors

$$p = a_1 x^{\alpha_1} + a_2 x^{\alpha_2} + a_3 x^{\alpha_3} \in \mathbb{Q}[x]$$

of a given $f \in \mathbb{Q}[x]$ in polynomial time?

The outline of the paper is as follows. In Section 1 we explain the basics of the height theory for points, polynomials and curves, and we prove the upper bounds for the number of factors of a sparse polynomial. In Section 2 we obtain the gap theorems, as a consequence of the lower bounds for the height of points on curves. In Section 3 we present the algorithms for rational and absolute factorization and estimate their theoretical complexity.

Note. Theorem 1 was independently achieved in [KK06] by Kaltofen and Koiran. This article also relies on the method in [CKS99], [Len99b] and [KK05], although it differs from ours in all other aspects: the corresponding gap theorem is obtained as a consequence of a lower bound for the height of numbers in abelian extensions due to Amoroso and F. Zannier, and the binomial factors are handled differently. As observed by the authors, their algorithm requires the a priori knowledge of a universal but non-explicit constant c [KK06, Thm 1]. In the present paper this problem is avoided by using the more explicit results in [AD00] and [Pon01]. Our approach also allows to compute not only the rational factors but also the absolute ones.

Acknowledgements. We thank Corentin Pontreau for helpful discussions on lower bounds for the height. The core of this paper was written during October–December 2005 while M. Sombra was visiting the University of Buenos Aires, Argentina; he particularly thanks Ricardo Durán for his invitation. He also thanks the Mathematical Sciences Research Institute at Berkeley, USA, where he stayed during January 2006.

1. Heights

Throughout this paper $\mathbb{Q}$ denotes the field of rational numbers, K a number field, L a finite extension of K, $\overline{\mathbb{Q}}$ an algebraic closure of $\mathbb{Q}$ and G_∞ the subset of $\overline{\mathbb{Q}}$ of all roots of the unity. We denote by $\mathbb{A}^n$ the affine space of n dimensions over $\overline{\mathbb{Q}}$. For a polynomial $p \in \overline{\mathbb{Q}}[x_1, \ldots, x_n]$ we denote by $Z(p) \subset \mathbb{A}^n$ the affine hypersurface defined by p. A curve or a variety is assumed to be equidimensional; by irreducibility of a variety we understand its geometric irreducibility, that is with respect to $\overline{\mathbb{Q}}$.

For every rational prime p we denote by $|\cdot|_p$ the p-adic absolute value over $\mathbb{Q}$ such that $|p|_p = p^{-1}$. We also denote the ordinary absolute value over $\mathbb{Q}$ by $|\cdot|_\infty$ or simply by $|\cdot|$. These form a complete set of independent absolute values over $\mathbb{Q}$: we identify the set $M_\mathbb{Q}$ of these absolute values with the set $\{\infty, p\,;\ p \text{ prime}\}$. More generally, we write M_K for the set of absolute values over K extending the absolute values in $M_\mathbb{Q}$, and we note by M_K^∞ the subset of Archimedean absolute values of M_K.

For $v_0 \in M_\mathbb{Q}$ we denote by $\mathbb{Q}_{v_0}$ the completion of $\mathbb{Q}$ with respect to the absolute value v_0. In case $v_0 = \infty$ we have $\mathbb{Q}_\infty = \mathbb{R}$, while in case $v_0 = p$ is a prime, $\mathbb{Q}_p$ is the p-adic field. There exists a unique extension of v_0 to an absolute value over the algebraic closure $\overline{\mathbb{Q}}_{v_0}$. For $v \in M_K$ we also denote by K_v the completion of K with respect to v. If v extends an absolute value $v_0 \in M_\mathbb{Q}$, then K_v is a finite extension of $\mathbb{Q}_{v_0}$. We denote $\sigma_v : K \hookrightarrow \overline{\mathbb{Q}}_v$ a (not necessarily unique) embedding corresponding to v, that is such that $|a|_v = |\sigma_v(a)|_{v_0}$ for every $a \in K$.

1.1. Height of points and polynomials.

In this subsection we introduce the basic definitions and properties of the height of points and polynomials that we will use in the sequel. We refer for instance to [HS00] for a complete treatment.

The *(logarithmic) height* $h(\xi)$ of an algebraic number $\xi \in \overline{\mathbb{Q}}$ can be defined in terms of its primitive integer minimal polynomial

$$p_\xi(x) = c \cdot \prod_{\sigma : K \hookrightarrow \overline{\mathbb{Q}}} (x - \sigma(\xi)) \quad \in \mathbb{Z}[x]$$

where σ runs over all $\mathbb{Q}$-embeddings of $K := \mathbb{Q}(\xi)$ in $\overline{\mathbb{Q}}$, by the formula

$$h(\xi) = \frac{1}{[K : \mathbb{Q}]} \left(\log|c| + \sum_{\sigma : K \hookrightarrow \overline{\mathbb{Q}}} \max\{0, \log|\sigma(\xi)|\} \right). \tag{1}$$

We have $h(\xi) \geq 0$, and $h(\xi) = 0$ if and only if either $\xi = 0$ or $\xi \in G_\infty$, the subset of $\overline{\mathbb{Q}}$ of all roots of 1 (Kronecker's theorem). Besides, for a rational $\xi = m/n \in \mathbb{Q}^\times$ in reduced expression, we easily check that $h(\xi) = \log \max\{|m|, n\}$. Alternatively, the height can be defined *via* the Mahler measure of the minimal polynomial as

$$m(p_\xi) := \int_0^1 \log |p_\xi(e^{2\pi i u})|\, du = [K : \mathbb{Q}] \cdot h(\xi);$$

this identity is a consequence of Jensen's formula.

More generally, the *height* of a point $\xi := (\xi_1, \ldots, \xi_n) \in \mathbb{A}^n$ is defined *via* the Weil formula

$$h(\xi) := \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} [K_v : \mathbb{Q}_v] \log \max\{1, |\xi_1|_v, \ldots, |\xi_n|_v\}$$

for any number field K containing the coordinates ξ_i. For $n = 1$ this gives

$$h(\xi) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} [K_v : \mathbb{Q}_v] \log \max\{1, |\xi|_v\}$$

and it can be shown that this coincides with the previous definition. With this expression we readily verify that for $\xi, \eta \in \overline{\mathbb{Q}}$ we have that $h(\xi \cdot \eta) \leq h(\xi) + h(\eta)$ and

$$h(\xi^n) = |n|\, h(\xi) \quad \text{for } n \in \mathbb{Z};$$

in particular $h(\xi^{-1}) = h(\xi)$ and $h(\omega \cdot \xi) = h(\xi)$ for any root of unity $\omega \in G_\infty$. We will be mostly interested on points in the plane $\xi = (\xi_1, \xi_2) \in \mathbb{A}^2$, in that case the formula reduces to

$$h(\xi) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} [K_v : \mathbb{Q}_v] \log \max\{1, |\xi_1|_v, |\xi_2|_v\}.$$

Now we introduce a few notions for the height of a polynomial that will prove useful in the sequel. We will restrict to bivariate polynomials, although it is clear that all this extends to the multivariate case.

For a polynomial $f = \sum_{i=1}^t a_i\, x^{\alpha_i} y^{\beta_i} \in K[x, y]$, its *absolute value* with respect to $v \in M_K$ is

$$|f|_v := \max\{|a_1|_v, \ldots, |a_t|_v\}.$$

The *height* of f is then defined as

$$h(f) := \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} [K_v : \mathbb{Q}_v] \log(|f|_v),$$

which is invariant by scalar multiplication because of the product formula

$$\sum_{v \in M_K} [K_v : \mathbb{Q}_v] \log(|a|_v) = 0, \quad \forall\, a \in K^\times.$$

Therefore $h(f)$ is the Weil height of the projective point $(a_1 : \cdots : a_t)$. This is independent of the chosen field K as long as it contains all of the a_i's.

For a bivariate polynomial with complex coefficients $f \in \mathbb{C}[x, y]$ we consider the *Mahler measure*

$$m(f) := \int_0^1 \int_0^1 \log |f(e^{2\pi i u}, e^{2\pi i v})|\, du\, dv,$$

and for a polynomial $f \in K[x,y]$ with *algebraic* coefficients we define its *(global) Mahler measure* by the adelic formula

$$m_{\overline{\mathbb{Q}}}(f) := \frac{1}{[K:\mathbb{Q}]} \left(\sum_{v \in M_K^\infty} [K_v : \mathbb{Q}_v]\, m(\sigma_v(f)) + \sum_{v \notin M_K^\infty} [K_v : \mathbb{Q}_v] \log |f|_v \right).$$

We also consider the height associated to the ℓ^1-norm:

$$h_1(f) := \frac{1}{[K:\mathbb{Q}]} \left(\sum_{v \in M_K^\infty} [K_v : \mathbb{Q}_v]\, \log ||\sigma_v(f)||_1 + \sum_{v \notin M_K^\infty} [K_v : \mathbb{Q}_v] \log |f|_v \right),$$

where for $v \in M_K^\infty$, the usual definition $||\sigma_v(f)||_1 := \sum_i |\sigma_v(a_i)|$ holds.

For a *primitive* $f \in \mathbb{Z}[x,y]$, these notions give

$$h(f) = \log |f| = \log \max\{|a_1|, \dots, |a_t|\},\ h_1(f) = \log ||f||_1 = \log(|a_1| + \cdots + |a_t|),\ m_{\overline{\mathbb{Q}}}(f) = m(f).$$

All these are invariant by scalar multiplication. In general for any $f \in \mathbb{Q}[x,y]$ write $f = c \cdot \widetilde{f}$ for some $c \in \mathbb{Q}^\times$ and $\widetilde{f} \in \mathbb{Z}[x,y]$ the primitive polynomial with integer coefficients associated to f, then $h(f) = \log |\widetilde{f}|$, $h_1(f) = \log ||\widetilde{f}||_1$ and $m_{\overline{\mathbb{Q}}}(f) = m(\widetilde{f})$.

We will use the following comparison between the heights of a given $f \in K[x,y]$, which can be directly proven from the definitions:

$$h(f), m_{\overline{\mathbb{Q}}}(f) \le h_1(f) \le h(f) + \log(t). \tag{2}$$

1.2. **Height** *of* **and** *on* **plane curves.** A plane curve $C \subset \mathbb{A}^2$ can have some isolated points of small height. For instance the line

$$Z(x+y-1) \subset \mathbb{A}^2$$

has the points $(1,0), (0,1), \big((1 \pm \sqrt{3})/2, (1 \mp \sqrt{3})/2\big)$ all of whose coordinates are roots of 1 and so their height is 0. D. Zagier [Zag93] showed that the height of any other point $\xi \in Z(x+y-1)$ is bounded from below by a positive constant

$$h(\xi) \ge h(\xi_0) = 0.1911$$

where ξ_0 denotes the largest real root of the polynomial $x^6 - x^4 - 1$. Somehow the fact that a curve has some torsion points on it does not reflect its general behavior. A more interesting parameter is the height of a Zariski dense set of points. This is measured by the *essential minimum*, which for a plane curve $C \subset \mathbb{A}^2$ is defined as

$$\mu^{\text{ess}}(C) := \inf \big\{ \eta \ge 0 : \{\xi \in C : h(\xi) \le \eta\} \text{ is an infinite set } \big\}.$$

For instance, thanks to Zagier's result,

$$\mu^{\text{ess}}(Z(x+y-1)) \ge 0.1911.$$

This is a particular case of the Bogomolov problem over the torus proved by Zhang [Zha95] which asserts that for a subvariety of $\mathbb{T}^n := (\overline{\mathbb{Q}}^\times)^n$, the vanishing of the essential minimum is equivalent to being *torsion*. This result, and others we are going to use, are stated for the torus, but $\mathbb{T}^n$ is naturally embedded as an open subset of $\mathbb{A}^n$, and since these results depend on Zariski dense sets, they can all be translated to $\mathbb{A}^n$.

For an irreducible plane curve $C \subset \mathbb{A}^2$, being *torsion* is equivalent to say that there exist $\alpha, \beta \ge 0$ not both zero, and $\omega \in G_\infty \cup \{0\}$ such that

$$\text{either} \quad C = Z(x^\alpha - \omega y^\beta) \quad \text{or} \quad C = Z(x^\alpha y^\beta - \omega).$$

The irreducible curve C is (we should rather say "corresponds to") a *translate of a subgroup* whenever there exists $\xi \in \overline{\mathbb{Q}}$ such that

$$\text{either} \quad C = Z(x^\alpha - \xi y^\beta) \quad \text{or} \quad C = Z(x^\alpha y^\beta - \xi).$$

By definition, a general affine plane curve is torsion (resp. translate of a subgroup) if and only if all its irreducible components are so. The statement of the Bogomolov problem (now a theorem) is that $\mu^{\mathrm{ess}}(C) = 0$ if and only if C is torsion. In other words, if C is not of this form, there exists a positive constant $c(C) > 0$ such that

$$h(\xi) \geq c(C) \quad \text{for all but a finite number of } \xi \in C.$$

There is an extension of the notion of Weil height of points to higher-dimensional varieties. This notion was first introduced by P. Philippon [Phi91]; for an irreducible hypersurface $V \subset \mathbb{A}^n$ defined by a polynomial $p \in K[x_1, \ldots, x_n]$, it coincides with the global Mahler measure of p [DP99, Pon01]:

$$h(V) = m_{\overline{\mathbb{Q}}}(p). \tag{3}$$

The distribution of the height of algebraic points in a curve is in close connection with the height of the curve itself. The relation is given by the *theorem of algebraic successive minima* of Zhang [Zha95, Thm 5.2 and Lem. 6.5(3)]:

$$\mu^{\mathrm{ess}}(C) \leq \frac{h(C)}{\deg(C)} \leq 2\mu^{\mathrm{ess}}(C).$$

Actually, Zhang's result is more precise (all successive minima appear, not only the first one which is the essential minimum) and more general, as it works for varieties of any dimension and for any "reasonable" height function.
The stated version is sufficient for our application; for a more elementary proof we refer to [DP99, § 6]. It is an open problem to determine if this estimate is optimal for the case of plane curves or more generally for hypersurfaces (it has been shown to be optimal if we allow varieties of higher codimension [PS04, Thm 5.1]). Thanks to this result, the Bomogolov problem for plane curves can be rephrased as $h(C) = 0$ if and only if C is torsion. Under this form, the conjecture was already proven by W. Lawton in 1977 [Law77].

For $\xi \in \overline{\mathbb{Q}}^\times$ we have that $h(\xi) = 0$ if and only if $\xi \in G_\infty$; this is the 0-dimensional (easy) case of the Bogomolov problem. Lehmer's conjecture gives a lower bound for the height of non-torsion points, its statement being that there exists a positive constant $c > 0$ such that

$$h(\xi) \geq \frac{c}{[\mathbb{Q}(\xi) : \mathbb{Q}]} \quad \text{for } \xi \notin G_\infty.$$

This conjecture has been widely generalized. Here we are only interested in the case of curves:

Conjecture 1.1.

(i) Lehmer's problem for plane curves: *Let $C \subset \mathbb{A}^2$ be an irreducible curve defined over a number field K which is not torsion. Then there exists a universal $c > 0$ such that*

$$\mu^{\mathrm{ess}}(C) \geq \frac{c}{[K : \mathbb{Q}] \deg(C)}.$$

(ii) Effective Bogomolov problem for plane curves: *Let $C \subset \mathbb{A}^2$ be an irreducible curve which is not a translate of a subgroup. Then there exists a universal $c > 0$ such that*

$$\mu^{\mathrm{ess}}(C) \geq \frac{c}{\deg(C)}.$$

These two conjecture look similar but they are not. The generalization of Lehmer's problem is of arithmetic nature since the degree of the number field plays a role, while the quantitative Bogomolov problem is of geometric nature since it makes no reference to the field of definition. It has been shown that conjecture 1.1(i) is implied by the classical Lehmer's problem [Law77]. Conjecture 1.1(ii) is [DP99, Conj. 1.1].
Because of the theorem of successive minima, it is equivalent to have lower bounds for the essential minimum or for the height, that is the (global) Mahler measure of the defining polynomial of C.

Nowadays all these results are proved "up to an ε": for the Lehmer's problem we will be mainly applying the following lower bound due to Amoroso and David [AD00], in the version of C. Pontreau [Pon05a, Prop. IV.1] who simplified the proof and made all constants explicit: if $C \subset \mathbb{A}^2$ is a non-torsion curve defined by an irreducible polynomial $p \in \mathbb{Z}[x,y]$ of degree d, then

$$\mu^{\text{ess}}(C) \geq \frac{1}{5^6 d} \times \left(\frac{\log\log(16d)}{\log(16d)} \right)^3 . \tag{4}$$

In the reference this result is stated in terms of $h(C)$; you have to look into the proof for the version up here. In fact we will be using the version over a number field:

Corollary 1.2. *Let $C \in \mathbb{A}^2$ be a curve defined by an irreducible polynomial $p \in K[x,y]$ which is not of the form $p = \prod_i (x^\alpha - \omega_i y^\beta)$ nor $p = \prod_i (x^\alpha y^\beta - \omega_i)$ for some $\alpha, \beta \geq 0$ not both zero and $\omega_i \in G_\infty \cup \{0\}$ and set $d := \deg(C) = \deg(p)$. Then*

$$\mu^{\text{ess}}(C) \geq \frac{1}{5^6 [K:\mathbb{Q}] d} \times \left(\frac{\log\log(16[K:\mathbb{Q}]d)}{\log(16[K:\mathbb{Q}]d)} \right)^3 .$$

This follows immediately from (4) by considering the norm $N(p) := \prod_{\sigma : K \hookrightarrow \overline{\mathbb{Q}}} \sigma(p) \in \mathbb{Q}[x,y]$.

For the effective Bogomolov problem we use another result of Amoroso and David: if $C \subset \mathbb{A}^2$ is a curve which is not a translate of a subgroup and $d := \deg(C) = \deg(p)$, then [AD03, Thm 1.5]:

$$\mu^{\text{ess}}(C) \geq \frac{1}{2^{70} d} \times \frac{(\log\log(d+2))^4}{(\log(d+2))^5}. \tag{5}$$

1.3. **On the number of factors of a sparse polynomial.** General lower bounds for the Mahler measure immediately yield upper bounds for the number of factors of a given polynomial. To the best of our knowledge, this observation appears for the first time in the work of E. Dobrowolski [Dob79]. Here we treat the general n-dimensional case. The notions and results of the previous subsection extend to hypersurfaces. We will state them but instead refer the interested reader to the literature for $n \geq 3$.
We recall that a polynomial is cyclotomic if it is a product of binomials (including monomials) whose coefficients are roots of the unity.

Proposition 1.3. *Let $f \in K[x_1, \ldots, x_n]$ and consider the factorization*

$$f = q \cdot \prod_p p^{e_p}$$

where q is cyclotomic, $p \in K[x_1, \ldots, x_n]$ runs over all non-cyclotomic irreducible factors of f, and e_p is the corresponding multiplicity. Then

$$\sum_p e_p \leq 5^6 \cdot n^3 \cdot [K:\mathbb{Q}] \cdot h_1(f) \cdot \log^3(8n[K:\mathbb{Q}]\deg(f)).$$

Proof. We have that $m_{\overline{\mathbb{Q}}}(q) = 0$ as q is cyclotomic an so

$$\sum_p e_p m_{\overline{\mathbb{Q}}}(p) = m_{\overline{\mathbb{Q}}}(f) \leq h_1(f).$$

For each non-cyclotomic factor $p \in \mathbb{Q}[x_1, \ldots, x_n]$ we minorate the Mahler measure by the Amoroso-David's lower bound in the version of Pontreau [Pon01, Thm 1.6] (see the estimate (4) above for the case $n = 2$), from which we derive that if $V \subset \mathbb{A}^n$ is an hypersurface defined by an irreducible polynomial over K, then

$$[K : \mathbb{Q}] \cdot h(V) \geq \frac{1}{5^6 \cdot n^3} \cdot \left(\frac{\log(n \log(8n[K : \mathbb{Q}] \deg(V))}{\log(8n[K : \mathbb{Q}] \deg(V))} \right)^3.$$

Therefore, by Identity (3), we have

$$[K : \mathbb{Q}] \cdot m_{\overline{\mathbb{Q}}}(p) \geq \frac{1}{5^6 \cdot n^3 \cdot \log^3(8n[K : \mathbb{Q}] \deg(p))} \geq \frac{1}{5^6 \cdot n^3 \cdot \log^3(8n[K : \mathbb{Q}] \deg(f))},$$

which implies

$$[K : \mathbb{Q}] \cdot h_1(f) \geq \frac{1}{5^6 \cdot n^3 \cdot \log^3(8n[K : \mathbb{Q}] \deg(f))} \sum_p e_p$$

from where we deduce our result. □

This is a generalization to $n \geq 2$ of [Dob79, Thm 2]. As said, a positive answer to the classical Lehmer's problem would imply a positive lower bound for the Mahler measure of an arbitrary non-cyclotomic polynomial $p \in K[x_1, \ldots, x_n]$, of the form

$$m_{\overline{\mathbb{Q}}}(p) \geq \frac{c}{[K : \mathbb{Q}]}$$

for some universal constant $c > 0$, namely Conjecture 1.1(i). Applying this to the argument above, the previous proposition would improve to

$$\sum_p e_p \leq c^{-1} \cdot [K : \mathbb{Q}] \cdot h_1(f). \tag{6}$$

In a similar way, we can produce an upper bound for the number of non-binomial irreducible factors over $\overline{\mathbb{Q}}$:

Proposition 1.4. *Let $f \in \overline{\mathbb{Q}}[x_1, \ldots, x_n]$ and consider the factorization*

$$f = q \cdot \prod_p p^{e_p}$$

were q is a product of binomials, $p \in \overline{\mathbb{Q}}[x_1, \ldots, x_n]$ runs over all non-binomial irreducible factors of f, and e_p is the corresponding multiplicity. Then

$$\sum_p e_p \leq 10^{14} \cdot n^8 \cdot h_1(f) \cdot \log^5(\max\{16, n \deg(f)\}).$$

Proof. We have that

$$\sum_p e_p m_{\overline{\mathbb{Q}}}(p) = m_{\overline{\mathbb{Q}}}(f) \leq h_1(f);$$

apply the Amoroso-David quantitative Bogomolov problem in the version of Pontreau [Pon05b, Thm 1.5] (or (5) above for the case $n = 2$). □

Similarly, a positive answer to the effective Bogomolov problem (Conjecture 1.1(ii)) would imply that

$$\sum_p e_p \leq c^{-1} \cdot h_1(f) \quad \text{for a universal constant } c > 0.$$

2. Gap theorems

By a *gap theorem*, following [CKS99, Len99b, KK05], we understand a statement asserting that for a polynomial f decomposed as

$$f = r + s$$

for non-zero polynomials r and s, then f has a given property if and only r and s have it, provided that r and s are sufficiently separated. We introduce some notation:

Definition 2.1. For $p \in \overline{\mathbb{Q}}[x,y]$ such that $\deg_y(p) \geq 1$ we set

$$\lambda(p) := \inf\left\{\eta \geq 0 : \{(\omega,\nu) \in G_\infty \times \overline{\mathbb{Q}} : p(\omega,\nu) = 0,\ h(\nu) \leq \eta\} \text{ is an infinite set }\right\}.$$

Since $\deg_y(p) \geq 1$, for all but a finite number of $\omega \in G_\infty$ there exists some $\nu \in \overline{\mathbb{Q}}$ such that $p(\omega,\nu) = 0$ and so $\lambda(p)$ is well-defined and non-negative.
In what follows we deal with irreducible polynomials, that are defined up to a scalar factor. For simplicity we always refer to one (obvious) representant in each class of associate irreducible polynomials.
The following is the main result of this section:

Theorem 2.2. *Let $f,r,q \in \overline{\mathbb{Q}}[x,y]$ be such that $f = r + y^u \cdot q$. Let also be given an irreducible polynomial $p \in \overline{\mathbb{Q}}[x,y]$, $p \neq y$, such that $\deg_y(p) \geq 1$, and suppose that*

$$(u - \deg_y(r)) \cdot \lambda(p) \geq h_1(f).$$

Then p divides f if and only if it divides r and q.

For its proof we need the following lemma:

Lemma 2.3. *Let $f,r,q \in \overline{\mathbb{Q}}[x,y]$ be such that $f = r + y^u \cdot q$. Let also be given $\omega \in G_\infty$ and $\nu \in \overline{\mathbb{Q}}^\times$ be such that $f(\omega,\nu) = 0$ but $q(\omega,\nu) \neq 0$. Then there exists a constant $\delta(f) > 0$ not depending on (ω,ν) such that*

$$(u - \deg_y(r)) \cdot h(\nu) \leq h_1(f) - \delta(f).$$

Proof. Let K be a number field containing the coefficients of f, ω and ν, and set $k := \deg_y(r)$. For each absolute value $v \in M_K$ we have two cases:

- $|\nu|_v \leq 1$: since $|\omega|_v = 1$ we have that
$$|q(\omega,\nu)|_v \leq \begin{cases} ||\sigma_v(q)||_1 & \text{for } v \in M_K^\infty, \\ |q|_v & \text{for } v \notin M_K^\infty. \end{cases}$$
- $|\nu|_v > 1$: using that $f(\omega,\nu) = r(\omega,\nu) + \nu^u q(\omega,\nu) = 0$ we infer that
$$|\nu|_v^u \cdot |q(\omega,\nu)|_v = |r(\omega,\nu)|_v \leq \begin{cases} |\nu|_v^k \cdot ||\sigma_v(r)||_1 & \text{for } v \in M_K^\infty, \\ |\nu|_v^k \cdot |r|_v & \text{for } v \notin M_K^\infty. \end{cases}$$

As both r and q are non-zero, $||\sigma_v(q)||_1, ||\sigma_v(r)||_1 < ||\sigma_v(f)||_1$ and so

$$\log||\sigma_v(q)||_1,\ \log||\sigma_v(r)||_1 \leq \log||\sigma_v(f)||_1 - \delta(f)$$

for some $\delta(f) > 0$ depending only on f. The previous inequalities imply that

$$(u-k)\log\max\{1,|\nu|_v\} + \log|q(\omega,\nu)|_v \leq \begin{cases} \log||\sigma_v(f)||_1 - \delta(f) & \text{for } v \in M_K^\infty, \\ \log|f|_v & \text{for } v \notin M_K^\infty. \end{cases}$$

By summing up over all absolute values, using the product formula and the definition of the height, one obtains that

$$\begin{aligned}(u-k)\cdot h(\nu) &= \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K}[K_v:\mathbb{Q}_v]\left((u-k)\log\max\{1,|\nu|_v\}+\log|q(\omega,\nu)|_v\right)\\ &\le \frac{1}{[K:\mathbb{Q}]}\left(\sum_{v\in M_K^\infty}[K_v:\mathbb{Q}_v]\big(\log||\sigma_v(f)||_1-\delta(f)\big)\quad+\sum_{v\notin M_K^\infty}[K_v:\mathbb{Q}_v]\log|f|_v\right)\\ &= h_1(f)-\delta(f).\end{aligned}$$

□

Proof of Theorem 2.2. The "$\Leftarrow$" is trivial, so we show the other implication.
Suppose that $p\,|\,f$ but $p\nmid q$. From the fact that p is irreducible we have that the set of common roots of p and q is finite. Also, since $\deg_y(p)\ge 1$ and $p\ne y$, the set $\{(\omega,\nu)\in G_\infty\times\overline{\mathbb{Q}}^\times : p(\omega,\nu)=0\}$ is infinite. Given $\varepsilon>0$, it follows from the definition of $\lambda(p)$ that the set $\{(\omega,\nu)\in G_\infty\times\overline{\mathbb{Q}} : p(\omega,\nu)=0,\ h(\nu)\le\lambda(p)-\varepsilon\}$ is finite. Therefore there exist an infinite number of $(\omega,\nu)\in G_\infty\times\overline{\mathbb{Q}}^\times$ such that $p(\omega,\nu)=0$ and $h(\nu)>\lambda(p)-\varepsilon$, and there still exist some $\omega\in G_\infty$ and $\nu\in\overline{\mathbb{Q}}^\times$ such that

$$p(\omega,\nu)=0,\quad q(\omega,\nu)\ne 0\quad\text{and } h(\nu)>\lambda(p)-\varepsilon.$$

Applying Lemma 2.3

$$(u-k)\,(\lambda(p)-\varepsilon)\le(u-k)\,h(\nu)\le h_1(f)-\delta(f).$$

Since this holds for all $\varepsilon>0$, we infer

$$(u-k)\,\lambda(p)\le h_1(f)-\delta(f)<h_1(f)$$

because $\delta(f)$ does not depend on (ω,ν) and so does not depend on ε either. This contradicts the hypothesis: $(u-k)\,\lambda(p)\ge h_1(f)$. Therefore $p\,|\,q$ and $p\,|\,-y^u\cdot q=r$ as wanted. □

Corollary 2.4. *Let $f,r,q\in\overline{\mathbb{Q}}[x,y]$ be such that $f=r+y^u\cdot q$. Let also be given $n\ge 1$ and an irreducible polynomial $p\in\overline{\mathbb{Q}}[x,y]$, $p\ne y$, such that $\deg_x(p)\ge 1$, $\deg_y(p)\ge 1$, and suppose that*

$$(u-\deg_y(r))\cdot\lambda(p)\ge h_1(f)+(n-1)\log(\deg_x(f)).$$

Then p^n divides f if and only if it divides r and q.

Proof. Since $\deg_x(p)\ge 1$, we have that $p^n\,|\,f$ if and only if

$$p\,|\,\frac{\partial^j f}{\partial x^j}\quad\text{for } j=0,\dots,n-1.$$

The result follows by applying the Gap Theorem 2.2 to $\partial^j f/\partial x^j$: We have

$$\frac{\partial^j f}{\partial x^j}=\frac{\partial^j r}{\partial x^j}+y^u\frac{\partial^j q}{\partial x^j}.$$

If $\partial^j r/\partial x^j$ or $\partial^j q/\partial x^j$ vanish, there is nothing to prove. Otherwise, $u-\deg_y(\partial^j r/\partial x^j)\ge u-\deg_y(r)$ since $\deg_y(\partial^j r/\partial x^j)\le\deg_y r$. Furthermore, from the definition of h_1 we infer that

$$h_1(\frac{\partial^j f}{\partial x^j})\le h_1(f)+(n-1)\log(\deg_x(f)),$$

since for a coefficient a_i of f in K and $d\in\mathbb{N}$, for $v\in M_K^\infty$, $||\sigma_v(\partial f/\partial x)||_1\le\deg_x f\,||\sigma_v(f)||_1$ holds, while for $v\notin M_K^\infty$, $|\partial f/\partial x|_v\le|f|_v$ since $|k|_v=1$ for $k\in\mathbb{N}$. □

We observe that for instance by [Len99b, Prop. 3.2], we know the *a priori* bound $n \leq t-1$.

Of course this result is only useful whenever $\lambda(p) > 0$. What happens is that this parameter is bounded from below by the essential minimum, and so all existing estimations for the essential minimum will give us a corresponding gap theorem.

Lemma 2.5. *Let p be an irreducible polynomial in $K[x,y]$ such that $\deg_y(p) \geq 1$. Then*

$$\lambda(p) \geq \mu^{\mathrm{ess}}(Z(p)).$$

Proof. Observe that $h(\nu) = h(\omega, \nu)$; we can then rephrase the definition of $\lambda(p)$ as

$$\lambda(p) = \inf\big\{\eta \geq 0 : \{\xi \in Z(p) \cap (G_\infty \times \overline{\mathbb{Q}}) : h(\xi) \leq \eta\} \text{ is an infinite set }\big\}.$$

Compare with the definition of the essential minimum:

$$\mu^{\mathrm{ess}}(Z(p)) = \inf\big\{\eta \geq 0 : \{\xi \in Z(p) : h(\xi) \leq \eta\} \text{ is an infinite set }\big\},$$

so that $\lambda(p)$ is the infimum over a subset of the set used to define $\mu^{\mathrm{ess}}(Z(p))$ and the inequality is clear. □

Equality in Lemma 2.5 above does not necessarily hold: consider $p := x^\alpha - \xi y^\beta$, then for any $(\omega, \nu) \in G_\infty \times \overline{\mathbb{Q}}$ we have that $p(\omega, \nu) = 0 \iff \nu^\beta = \omega^\alpha/\xi$ and so

$$h(\nu) = \frac{h(\nu^\beta)}{\beta} = \frac{h(\omega^\alpha/\xi)}{\beta} = \frac{h(\xi)}{\beta}.$$

Hence

$$\lambda(p(x,y)) = h(\xi)/\beta \quad \text{ while } \quad \lambda(p(y,x)) = h(\xi)/\alpha.$$

In particular, λ depends on the order of the variables, while of course the essential minimum does not, so there cannot coincide in general. One can prove, however, that $\mu^{\mathrm{ess}}(p) = h(\xi)/\max\{\alpha, \beta\}$ [PS04, Prop. 5.4].

From Corollary 1.2 we deduce:

Corollary 2.6. *Let $f, r, q \in K[x,y]$ be such that $f = r + y^u \cdot q$. Let also be given $n \leq t-1$ and an irreducible polynomial $p \in K[x,y]$, $\deg_x p \geq 1$, that is non-cyclotomic, that is, not of the form $p = \prod_i (x^\alpha - \omega_i y^\beta)$ nor $p = \prod_i (x^\alpha y^\beta - \omega_i)$ for some $\alpha, \beta \geq 0$ not both zero and $\omega_i \in G_\infty \cup \{0\}$, and set $d := \deg(p)$. Suppose that*

$$u - \deg_y(r) \geq 5^6 \cdot [K:\mathbb{Q}] \cdot d \cdot \log^3(16[K:\mathbb{Q}]d) \cdot (h_1(f) + (t-2)\log(\deg_x(f))).$$

Then p^n divides f if and only if it divides r and q.

Similarly we obtain the following gap theorem from the lower bound (5):

Corollary 2.7. *Let $f, r, q \in \overline{\mathbb{Q}}[x,y]$ be such that $f = r + y^u \cdot q$. Let also be given $n \leq t-1$ and an irreducible polynomial $p \in \overline{\mathbb{Q}}[x,y]$ which is not a binomial, and set $d := \deg(p)$. Suppose that*

$$u - \deg_y(r) \geq 2^{70} \cdot d \cdot \log^5(d+2) \cdot (h_1(f) + (t-2)\log(\deg_x(f))).$$

Then p^n divides f if and only if it divides r and q.

3. Computing the low degree factors of sparse polynomials

The goal of this section is to present the rational and absolute factorization algorithms for sparse bivariate polynomials. Our conventions about encoding are the usual ones, the same as in for instance [Len99b]. The number of bits needed to write down a non-zero integer $a \in \mathbb{Z}$ is $\lfloor \log_2(a) \rfloor + 1$ for the digits and 1 more for the sign. For a rational $a = m/n \in \mathbb{Q}$ in reduced expression, we define its bit length as

$$\ell(a) = \ell(m) + \ell(n) - 2 = \lfloor \log_2 |m| \rfloor + \lfloor \log_2(n) \rfloor + 2;$$

the somewhat artificial "-2" is there just to make this coincide with the previous notation for an integer a. The sparse encoding of $f = \sum_{i=1}^{t} a_i x^{\alpha_i} y^{\beta_i} \in \mathbb{Q}[x,y]$ is the list $(a_i, \alpha_i, \beta_i)_{1 \le i \le t}$ of its (non-zero) coefficients and corresponding exponents, and so its bit length is

$$\ell(f) := \sum_{i=1}^{t} \Big(\ell(a_i) + \lfloor \log_2(\alpha_i) \rfloor + \lfloor \log_2(\beta_i) \rfloor + 2 \Big); \tag{7}$$

observe that $\ell(f)$ is an upper bound for t, $\log_2(\deg f)$ and $h(f)$, and in fact is polynomially equivalent to these quantities: $\ell(f) = (t \cdot \log_2(\deg f) \cdot h(f))^{O(1)}$.

For encoding polynomials over number fields we have to say how number fields and algebraic numbers are handled: a number field K of degree $\delta = [K : \mathbb{Q}]$ is described by an irreducible monic polynomial $g = \sum_{j=0}^{\delta-1} g_j z^j \in \mathbb{Z}[z]$ such that $K = \mathbb{Q}(\theta)$ for one of its roots, and this g is given in dense representation by the (ordered) list of all its coefficients g_j including the zero ones. The length of this description is

$$\ell(K) := \sum_{j=0}^{\delta-1} \ell(g_j);$$

in particular $\ell(K) \ge [K : \mathbb{Q}], h(g)$. An element $b \in K$ is represented by its vector of rational components $(b_0, \dots, b_{\delta-1})$ with respect to the basis $(\theta^j)_{0 \le j \le \delta-1}$. It can be shown by (you need some estimate between the height of an algebraic integer and that of its minimal polynomial) that

$$h(b) \le \ell_K(b) + [K : \mathbb{Q}](h(g) + [K : \mathbb{Q}] \log(2)) = (\ell(K) + \ell_K(b))^{O(1)}.$$

A sparsely given polynomial $f = \sum_{i=1}^{t} a_i x^{\alpha_i} y^{\beta_i} \in K[x,y]$ is then encoded by the list of its (non-zero) coefficients and corresponding exponents, and its length relative to K is

$$\ell_K(f) := \sum_{i=1}^{t} (\ell_K(a_i) + \ell(\alpha_i) + \ell(\beta_i)).$$

Note that the input data is specified by *f and K*, and so the input length is $\ell(K) + \ell_K(f)$. We have that

$$t, \log_2(\deg f) \le \ell(f) \quad \text{and} \quad h(f) \le \ell_K(f) + [K : \mathbb{Q}](h(g) + [K : \mathbb{Q}] \log(2)) = (\ell(K) + \ell_K(f))^{O(1)}.$$

When the input of our algorithms comprises an inclusion $K \hookrightarrow L$ of number fields, L is described as an extension of K by a monic irreducible polynomial $k(z) \in \mathcal{O}_K[z]$ such that $L = K(\vartheta)$ for a root ϑ of k; this polynomial is represented in a dense way. A polynomial $p \in L[x,y]$ in the output is then encoded by the (dense) list of its coefficients with respect to the product basis $(\theta^j \vartheta^k)_{0 \le j \le \delta-1, 0 \le k \le \gamma-1}$ of L over $\mathbb{Q}$; here we set $\gamma := [L : K]$. Note that for an element $b \in K$ in the base field encoded as $b = b_0 + \cdots + b_{\delta-1} x^{\delta-1}$ with respect to the given basis of K over $\mathbb{Q}$, its encoding with respect to the product base will be the same and so

$$\ell_L(b) \le [L : K]\, \ell_K(b)$$

since we have to count the zero coefficients corresponding to the monomials $\theta^j \vartheta^k$ with $k \ge 1$. In particular $\ell_L(f) \le [L : K]\, \ell_K(f)$ for $f \in K[x,y]$.

For the absolute factorization algorithm for $f \in K[x,y]$, the output irreducible polynomials $p_i \in \overline{\mathbb{Q}}[x,y]$ are encoded by (L_i, p_i), where L_i consists in the minimal extension of K such that $p_i \in L_i[x,y]$ (we observe that this encodes a full set $(\sigma(p_i))_{\sigma:K\hookrightarrow\overline{\mathbb{Q}}}$ of $[L_i : K]$ conjugate factors of f). The couple (L_i, p_i) is encoded by a monic irreducible polynomial $k_i(z) \in \mathcal{O}_K[z]$ such that $L_i = K[z]/(k_i(z))$, and p_i is given by its coefficients.

3.1. **Binomial factors.** The computation of the irreducible factors of a bivariate polynomial that are binomials or, more generally, products of binomials can be reduced to the univariate case as we show in this section. We first observe that if an irreducible polynomial $p \in K[x,y]$ is a product of binomials then it has one of the following forms:

$$p(x,y) = \prod_{\sigma}(x^\alpha - \sigma(\xi)y^\beta) \quad \text{or} \quad p(x,y) = \prod_{\sigma}(x^\alpha y^\beta - \sigma(\xi)), \tag{8}$$

where $\alpha, \beta \geq 0$ are not 0 simultaneously, $\xi \in \overline{\mathbb{Q}}$ and where $\sigma : K(\xi) \hookrightarrow \overline{\mathbb{Q}}$ runs over all K-embeddings of $K(\xi)$ in $\overline{\mathbb{Q}}$.
We have the following results:

Lemma 3.1. *Let $\alpha, \beta, n \in \mathbb{N}$, $\xi \in \overline{\mathbb{Q}}^\times$ and $f \in \overline{\mathbb{Q}}[x,y]$ be given. Set z for a new variable and denote by $g \in \overline{\mathbb{Q}}[x,y,z]$ the remainder of the division with respect to the variable x of $f(x,y)$ by the monic polynomial $x^\alpha - zy^\beta$. Then*

$$(x^\alpha - \xi\, y^\beta)^n \mid f(x,y) \quad \iff \quad (z-\xi)^n \mid g(x,y,z).$$

Proof. Consider the ring

$$A := \overline{\mathbb{Q}}[x, y^{\pm 1}, z]/(x^\alpha - zy^\beta).$$

We have that $x^\alpha - \xi y^\beta = (z-\xi)y^\beta$ in A, and, since y is invertible, we have the following equality of ideals

$$((x^\alpha - \xi y^\beta)^n) \;=\; ((z-\xi)^n) \text{ in } A.$$

We call this ideal I. By definition $f = g$ in A and so $f \in I$ if and only if $g \in I$, that is

$$(x^\alpha - \xi\, y^\beta)^n \mid f(x,y) \quad \text{in } A \quad \iff \quad (z-\xi)^n \mid g(x,y,z) \quad \text{in } A.$$

We have to show that we can take out the words "in A" from the above statement.
We observe that there is a natural identification $A = \overline{\mathbb{Q}}[x, y^{\pm 1}]$. Therefore,

$$(x^\alpha - \xi\, y^\beta)^n \mid f \text{ in } A \iff (x^\alpha - \xi\, y^\beta)^n \mid f \text{ in } \overline{\mathbb{Q}}[x, y^{\pm 1}] \iff (x^\alpha - \xi\, y^\beta)^n \mid f \text{ in } \overline{\mathbb{Q}}[x,y]$$

since y is prime to $x^\alpha - \xi\, y^\beta$.
We have a second identification

$$A = \bigoplus_{j=0}^{\alpha-1} \overline{\mathbb{Q}}[y^{\pm 1}, z] \cdot x^j,$$

and therefore

$$(z-\xi)^n \mid g \text{ in } A \iff (z-\xi)^n \mid g \text{ in } \overline{\mathbb{Q}}[x, y^{\pm 1}, z] \iff (z-\xi)^n \mid g \text{ in } \overline{\mathbb{Q}}[x,y,z]$$

since y is prime to $z - \xi$. □

Corollary 3.2. *With the same notations than in the previous lemma, let K be a number field and suppose that $f \in K[x,y]$. Set*

$$p(x,y) := \prod_{\sigma}(x^\alpha - \sigma(\xi)y^\beta) \in K[x,y] \quad \text{and} \quad q(z) := \prod_{\sigma}(z - \sigma(\xi)) \in K[z]$$

where σ runs over all K-embeddings of $K(\xi)$ in $\overline{\mathbb{Q}}$. Then

$$p(x,y)^n \mid f(x,y) \quad \iff \quad q(z)^n \mid g(x,y,z).$$

Proof. The polynomials $x^\alpha - \sigma(\xi)y^\beta$ for different σ's are relatively prime, and the same is true for the polynomials $z - \sigma(\xi)$. Hence $p(x,y)^n \mid f(x,y)$ if and only if $(x^\alpha - \sigma(\xi)y^\beta)^n \mid f(x,y)$ for all σ if and only if $(z-\sigma(\xi))^n \mid g(x,y,z)$ for all σ if and only if $q(z)^n \mid g(x,y,z)$. □

The algorithm to compute the irreducible factors of $f \in K[x,y]$, of degree bounded by d, that are product of binomials is now clear:
We are looking for factors $p(x,y) \in K[x,y]$ of degree $\leq d$ of one of the forms in (8). The cases $\xi = 0$, $\alpha = 0$ or $\beta = 0$ reduce directly to the univariate case where we apply Lenstra's algorithm [Len99b, Thm] to the corresponding content of f.
So we can restrict ourselves to the cases when $\xi \in \overline{\mathbb{Q}}^\times$ and $\alpha, \beta \in \mathbb{N}$. We consider first the factors of the first form in (8).
We fix $1 \leq \alpha, \beta \leq d$, and we set $g := g_{\alpha,\beta} \in K[x,y,z]$ for the remainder of dividing f (with respect to x) by $x^\alpha - zy^\beta$ (g depends only on f and α, β). It is easy to compute g by Euclidean division:

$$g(x,y,z) = \sum_{i=1}^{t} a_i x^{\alpha_i \bmod \alpha} (z\, y^\beta)^{\lfloor \alpha_i/\alpha \rfloor} y^{\beta_i},$$

so that g is as sparse as f. We write

$$g(x,y,z) = \sum_{i,j} g_{i,j}(z) x^i y^j$$

and observe that an irreducible factor $q \in K[z]$ satisfies $q^n \mid g \iff q^n \mid g_{i,j}$ for all i,j, where there are at most t non-zero polynomials $g_{i,j}$, and each of them is as sparse as f, with coefficients obtained as the sum of at most t coefficients of f.
We compute all irreducible factors $q \in K[z]$ of g of degree bounded by $d/\max\{\alpha,\beta\}$ and their corresponding multiplicities, by examining the common irreducible factors (and their multiplicities) of all the $g_{i,j}$'s. This is done again applying Lenstra's univariate algorithm.
Since the irreducible polynomial q is of the form $q = \prod_\sigma (z - \sigma(\xi))$, the corresponding candidate factor p of f is then derived as

$$p(x,y) = (y^\beta)^{\deg(q)} q(x^\alpha y^{-\beta}),$$

where $\deg(p) = \max\{\alpha,\beta\} \cdot \deg(q) \leq d$. Before including p within the list of factor, we check if it is irreducible by applying a factorization algorithm like [Len87, Thm. 3.26] or the recent improvement in [Lec05]. Corollary 3.2 certifies that for given α, β, we obtain in this way all irreducible factors of f of degree $\leq d$ of the first form in (8), as well as their multiplicities.
For the factors in (8) of the second form, we proceed similarly, by considering the remainder $g \in K[x, y^{\pm 1}, z]$ of dividing f (with respect to x) by $x^\alpha y^\beta - z$. We observe that the corresponding extensions of Lemma 3.1 and Corollary 3.2 hold. In this case, p is derived from the factor $q \in K[z]$ of g as $p(x,y) = q(x^\alpha y^\beta)$.

The algorithm described above yields the following result:

Theorem 3.3. *There is a deterministic algorithm that, given $f \in K[x,y]$ and $d \geq 1$, computes all irreducible factors of f in $K[x,y]$ of degree $\leq d$ which are products of binomials, together with their multiplicities, in $\big(d \cdot (\ell(K) + \ell_K(f))\big)^{O(1)}$ bit operations.*

Proof. We have already established that the previous algorithm gives these factors and their multiplicities. Its running time is estimated as follows: for each pair α, β, we are applying Lenstra's algorithm $\leq t$ times to the polynomials $g_{i,j}$ of sparse length $\ell(g_{i,j}) = O(\ell(f))$, in order to compute their irreducible factors of degree $\leq d/\max\{\alpha,\beta\}$ and their multiplicities. This task is done in $\big(d \cdot (\ell(K) + \ell_K(f))\big)^{O(1)}$ bit operations. Since there are at most d^2 pairs α, β, the total bit cost of the algorithm remains of order $\big(d \cdot (\ell(K) + \ell_K(f))\big)^{O(1)}$. □

3.2. **Rational factorization.** The search of all the low degree bivariate factors of a sparse $f \in K[x,y]$ is done by decomposing it as a sum of short pieces, as in the previous papers [CKS99, Len99b, KK05]. For given $\Delta_x, \Delta_y \geq 0$, these pieces have to be separated by a distance ("gap") of at least Δ_x in the x-direction or Δ_y in the y-direction. This is done here by decomposing f first with respect to the y-exponents, then with respect to the x-exponents.

Let $f = \sum_{i=1}^{t} a_i x^{\alpha_i} y^{\beta_i}$ and suppose that the monomials are already ordered so that $\beta_1 \leq \beta_2 \leq \cdots \leq \beta_t$. Then we determine

$$\ell_0 := 0 < \ell_1 < \cdots < \ell_s < \ell_{s+1} = t$$

subject to the conditions

$$\beta_{i+1} - \beta_i < \Delta_y \ \text{ for } \ell_j + 1 \leq i \leq \ell_{j+1}, 0 \leq j \leq s, \quad \text{and} \quad \beta_{\ell_j+1} - \beta_{\ell_j} \geq \Delta_y \ \text{ for } 1 \leq j \leq s,$$

namely we split the y-exponents $\beta_1, \ldots, \beta_t$ into subsets so that consecutive exponents in the same subset are at distance $< \Delta_y$ and between different subsets there is a gap of length $\geq \Delta_y$. Set

$$r_j := \sum_{i=\ell_j+1}^{\ell_{j+1}} a_i x^{\alpha_i} y^{\beta_i - \beta_{\ell_j+1}} \ \text{ for } 0 \leq j \leq s \quad \text{so that} \quad f = y^{\beta_{\ell_0+1}} r_0 + y^{\beta_{\ell_1+1}} r_1 + \cdots + y^{\beta_{\ell_s+1}} r_s.$$

Next we do the same procedure over each r_j with respect to Δ_x: first we reorder the monomials applying a permutation τ so that

$$r_j = \sum_{i=\ell_j+1}^{\ell_{j+1}} a_{\tau(i)} x^{\alpha_{\tau(i)}} y^{\beta_{\tau(i)} - \beta_{\ell_j+1}}$$

and $\alpha_{\tau(\ell_j+1)} \leq \alpha_{\tau(\ell_j+2)} \leq \cdots \leq \alpha_{\tau(\ell_{j+1})}$. Then for each $0 \leq j \leq s$ we sub-split this set of $\ell_{j+1} - \ell_j$ exponents into subsets such that the consecutive x-exponents in the same subset are at distance $< \Delta_x$, and between different subsets there is a gap of length $\geq \Delta_x$. Using this, we decompose r_j into pieces

$$r_j = x^{\zeta_{0,j}} r_{0,j} + \cdots + x^{\zeta_{t_j,j}} r_{t_j,j}$$

for some exponents $\{\zeta_{i,j} : 0 \leq j \leq s, 0 \leq i \leq t_j\} \subset \{\alpha_1, \ldots, \alpha_t\}$ that we do not explicit to avoid useless proliferation of indexes.

Each $r_{i,j}$ is (up to a monomial) some part of r_j, which in time is (up to a monomial) some part of f. We arrive in this way to a list of $k \leq t$ non-zero polynomials $f_1, \ldots, f_k$ (after rewriting the $r_{i,j}$'s into f_i's) such that

$$f = x^{\gamma_1} y^{\delta_1} f_1 + x^{\gamma_2} y^{\delta_2} f_2 + \cdots + x^{\gamma_k} y^{\delta_k} f_k; \tag{9}$$

and by construction for $1 \leq i \leq k$,

$$\ell_K(f_i) \leq \ell_K(f), \quad \deg_x(f_i) < (t-1)\,\Delta_x, \quad \deg_y(f_i) < (t-1)\,\Delta_y$$

and for $i \neq j$ we have that

$$\begin{aligned} \text{either} \quad & \gamma_j - \gamma_i - \deg_x(f_i) \geq \Delta_x \quad \text{or} \quad \gamma_i - \gamma_j - \deg_x(f_j) \geq \Delta_x \\ \text{or} \quad & \delta_j - \delta_i - \deg_y(f_i) \geq \Delta_y \quad \text{or} \quad \delta_i - \delta_j - \deg_x(f_j) \geq \Delta_y. \end{aligned}$$

We have decomposed f in $\leq t$ pieces of controlled degree and separated by a gap of length $\geq \Delta_x$ in the x-direction or $\geq \Delta_y$ in the y-direction.

The computation of the irreducible factors of f of degree $\leq d$ is then clear. Pure factors in x or y reduce to the univariate case [Len99b]. For the truly bivariate factors, we compute first a constant c such that $h_1(f) + (t-2)\log(\deg_x(f)) \leq c$ in time $(\ell(K) + \ell_K(f))^{O(1)}$, as in [Len99b, Prop.3.6]. We set

$$\Delta_x := \Delta_y := \Delta = 5^6 \cdot [K:\mathbb{Q}] \cdot d \cdot \log^3(16[K:\mathbb{Q}]d) \cdot c.$$

Applying Corollary 2.6 we infer that for $f = x^{\gamma_1} y^{\delta_1} f_1 + x^{\gamma_2} y^{\delta_2} f_2 + \cdots + x^{\gamma_k} y^{\delta_k} f_k$ as in (9), then for $p \in K[x,y]$, $\deg_x p \geq 1$, that is not a cyclotomic polynomial, we have

$$p^n \mid f \iff p^n \mid f_i \quad \text{for all } i.$$

The procedure consists on computing first the cyclotomic factors together with their multiplicity, by using the algorithm in Subsection 3.1. For the other factors, we compute them as the common factors of the f_i's, by using any polynomial-time algorithm for factoring dense bivariate polynomials over a number field, for instance [Len87, Thm 3.26] or [Lec05]. Therefore we obtain the following result:

Theorem 3.4. *There is a deterministic algorithm that, given $f \in K[x,y]$ and $d \geq 1$, computes all irreducible factors of f in $K[x,y]$ of degree $\leq d$, together with their multiplicities, in $\big(d \cdot (\ell(K) + \ell_K(f))\big)^{O(1)}$ bit operations.*

Proof. We have already established that the previous algorithm gives all these factors and their multiplicities. We estimate its running time. We show that the degree of f_i for all i, $1 \leq i \leq k$, in the decomposition (9) is polynomial in the input size. This is a consequence of our estimate for the gap length:

$$\ell(f_i) \leq \ell(f) \quad \text{and} \quad \deg_x(f_i), \deg_y(f_i) < (t-1)\,\Delta = O(t \cdot ([K:\mathbb{Q}] \cdot d)^{1+\varepsilon} \cdot c) = \big(d \cdot (\ell(K) + \ell_K(f))\big)^{O(1)}.$$

Then we apply to each f_i a polynomial-time algorithm for factoring dense bivariate polynomials over K, which would do the task in $\big(d \cdot (\ell(K) + \ell_K(f))\big)^{O(1)}$ bit operations. Since the number of f_i's is at most $t \leq \ell$, the total complexity remains of the same order. □

If for an input polynomial $f \in K[x,y]$ we are interested in its factors in an extension L, we can compute them by just including f into $L[x,y]$ and then applying the above algorithm over L; its cost would be of $\big(d \cdot (\ell(K) + \ell_K(f) + \ell_K(L)\big)^{O(1)}$ bit operations.

We note that here, for the factors which are products of binomials but not cyclotomic, we have the choice of computing them either by reduction to the univariate sparse case of Theorem 3.3 or by reduction to the dense bivariate case.

3.3. **Absolute factorization.** Given a polynomial $f \in K[x,y]$, we can apply Corollary 2.7 to extend the previous algorithm to the computation of all irreducible factors of f over $\overline{\mathbb{Q}}$, of degree bounded by d, except the binomial ones. We assume that the input f is encoded in $K[x,y]$ and as before we compute a constant c such that $h_1(f) + (t-2)\log(\deg_x(f)) \leq c$ in time $(\ell(K) + \ell_K(f))^{O(1)}$, then we set

$$\Delta_x := \Delta_y := \Delta = 2^{70} \cdot d \cdot \log^5(d+2) \cdot c.$$

Corollary 2.7 implies that for the associated decomposition $f = x^{\gamma_1} y^{\delta_1} f_1 + x^{\gamma_2} y^{\delta_2} f_2 + \cdots + x^{\gamma_k} y^{\delta_k} f_k$ as in (9), any irreducible $p \in \overline{\mathbb{Q}}[x,y]$ that is not of the form

$$p(x,y) = x^\alpha - \xi y^\beta \quad \text{or} \quad p(x,y) = x^\alpha y^\beta - \xi,$$

satisfies

$$p^n \mid f \iff p^n \mid f_i \quad \text{for all } i.$$

Now we need to determine the common factors of the f_i's over $\overline{\mathbb{Q}}[x,y]$ and their multiplicity. In order to do this, we first factor completely each of the f_i over $K[x,y]$ by applying any dense polynomial-time bivariate factorization algorithm over K. An irreducible factor $p \in \overline{\mathbb{Q}}[x,y]$ of f will necessarily divide a common irreducible factor $q \in K[x,y]$ of all the f_i's. Thus it is enough to keep all common irreducible factors $q \in K[x,y]$ of all the f_i's and their multiplicities, and then to factor them in $\overline{\mathbb{Q}}[x,y]$ by applying any polynomial-time algorithm for factoring dense bivariate polynomials over $\overline{\mathbb{Q}}$, for instance [Kal95, Theorem 11]. We only keep those factors in the output

which are of degree $\leq d$ and which are not binomials. We proceed in this way in order to avoid comparing irreducible factors in $\overline{\mathbb{Q}}[x,y]$ of different f_i's, that can, although equal, be described in different field extensions.

Theorem 3.5. *There is a deterministic algorithm that, given $f \in K[x,y]$ and $d \geq 1$, computes all irreducible factors of f in $\overline{\mathbb{Q}}[x,y]$ of degree $\leq d$, together with their multiplicities, except for the binomial ones, in $\big(d \cdot (\ell(K) + \ell_K(f))\big)^{O(1)}$ bit operations.*

Proof. As with the previous one, the complexity of this algorithm is estimated in $\big(d \cdot (\ell(K) + \ell_K(f))\big)^{O(1)}$ bit operations, because we have to factor $\leq t$ polynomials f_i of degree polynomially bounded in the input length to find all possible q, which are of input length $\ell_K(q) = \big(d \cdot (\ell(K) + \ell_K(f))\big)^{O(1)}$ and at most the same quantity, and then to factor them in $\overline{\mathbb{Q}}[x,y]$. □

3.4. **A practical improvement: adaptive gap methods.** The practical efficiency of the proposed algorithms depends essentially on the length Δ defining the gap in f: the degree of the pieces f_i depends on Δ, and if this degree is large, the dense factorization algorithm will be clearly slower. In other words, the smaller the gap length Δ is, the faster the algorithm works. Since the gap is proportional to the inverse of the essential minimum, the greatest the essential minimum, the faster the algorithm.

There are some special situations where we can get better bounds, for instance for linear factors $p(x,y) = ax + by + c$ with integer coefficients, as in [KK05].
The Mahler measure of a polynomial is bounded from below by the Mahler measure of any of its facet polynomials. Hence for $a, b, c \in \mathbb{Z}$ relatively prime numbers such that $a \cdot b \cdot c \neq 0$, we have that

$$m(ax + by + c) \geq \max\{m(ax + by), m(by + c), m(ax + c)\} = \log \max\{|a|, |b|, |c|\}$$

as it can be proved that the Mahler measure of a binomial coincides with its height. The theorem of successive minima then implies

$$\mu^{\text{ess}}(Z(ax + by + c)) \geq \frac{1}{2} \log \max\{|a|, |b|, |c|\} = \frac{1}{2} h(p).$$

The only case for which this lower bound is meaningless is when $a, b, c = 0, \pm 1$. (When a, b or c vanish, we reduce easily to the univariate case so we do not consider it here.) When $a, b, c = \pm 1$, Zagier's theorem [Zag93], see also Subsection 1.2, shows that $h(\xi) \geq 0.1911$. Hence

$$\mu^{\text{ess}}(Z(ax + by + c)) \geq \begin{cases} \log(\xi_0) = 0.1911 & \text{if } a, b, c = \pm 1 \\ h(p) \geq \frac{\log(2)}{2} = 0.3465 & \text{otherwise.} \end{cases}$$

which improves the bound $\log(1.045) \approx 0.0440$ proposed in [KK05].
Note that in this case the gap size associated with $p = ax + by + c$ gets smaller as the coefficients of p tend to infinity. Therefore, a good strategy to make the algorithm more efficient might be to exclude a finite number of candidates by testing them as factors of f (using a rough estimate for their gap length), and then use a much smaller gap length to find the rest of the factors by reduction to the dense case.

References

[AD00] F. Amoroso, S. David, *Minoration de la hauteur normalisée des hypersurfaces.* Acta Arith. **92** (2000) 339-366.

[AD03] F. Amoroso, S. David, *Minoration de la hauteur normalisée dans un tore.* J. Inst. Math. Jussieu **2** (2003) 335-381.

[BHKS05] K. Belabas, M. van Hoeij, J. Klüners, A. Steel, *Factoring polynomials over global fields.* Preprint (2005).

[Ber70] E.R. Berlekamp, *Factoring polynomials over large finite fields.* Math. Comp. **24** (1970) 713-735.

[CG82] A.L. Chistov, D.Y. Grigoriev, *Polynomial-time factoring of the multivariate polynomials over a global field.* LOMI preprint E-5-82, Leningrad, 1982.

[CKS99] F. Cucker, P. Koiran, S. Smale, *A polynomial time algorithm for Diophantine equations in one variable.* J. Symbolic Comput. **27** (1999) 21-29.

[DP99] S. David, P. Philippon, *Minoration des hauteurs normalisées des sous-variétés des tores.* Ann. Sci. Scuola Norm. Sup. Pisa **28** (1999) 489-543.

[Dob79] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial.* Acta Arith. **34** (1979) 391-401.

[HS00] M. Hindry, J.H. Silverman, *Diophantine geometry. An introduction.* Graduate Texts in Mathematics **201**, Springer-Verlag, 2000.

[Kal85] E. Kaltofen, *Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization.* SIAM J. Comput. **14** (1995) 469-489.

[Kal95] E. Kaltofen, *Effective Noether irreducibility forms and applications.* J. Comput. System Sci. **50** (1995) 274-295.

[KK05] E. Kaltofen, P. Koiran, *On the complexity of factoring bivariate supersparse (lacunary) polynomials.* ISSAC'05, Proc. 2005 Internat. Symp. Symbolic Algebraic Comput., ACM Press, 2005.

[KK06] E. Kaltofen, P. Koiran, *Finding small degree factors of multivariate supersparse (lacunary) polynomials over algebraic number fields.* To appear in ISSAC'06, Proc. 2006 Internat. Symp. Symbolic Algebraic Comput.

[Lan85] S. Landau, *Factoring polynomials over algebraic number fields.* SIAM J. Comput. **14** (1985) 184-195.

[Law77] W. Lawton, *A generalization of a theorem of Kronecker.* J. Sci. Fac. Chiangmai Univ. **4** (1977) 15-23.

[Lec05] G. Lecerf, *Improved dense multivariate polynomial factorization algorithms.* To appear in J. Symb. Comput..

[Len84] A.K. Lenstra, *Factoring multivariate integral polynomials.* Theoret. Comput. Sci. **34** (1984) 207-213.

[Len87] A.K. Lenstra, *Factoring multivariate polynomials over algebraic number fields.* SIAM J. Comput. **16** (1987) 591-598.

[LLL82] A.K. Lenstra, H.W. Lenstra Jr., L. Lovász, *Factoring polynomials with rational coefficients.* Math. Ann. **261** (1982) 515-534.

[Len99a] H.W. Lenstra Jr., *On the factorization of lacunary polynomials.* Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997) 277-291, de Gruyter, Berlin, 1999.

[Len99b] H.W. Lenstra Jr., *Finding small degree factors of lacunary polynomials.* Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997) 267-276, de Gruyter, Berlin, 1999.

[Phi91] P. Philippon, *Sur des hauteurs alternatives I.* Math. Ann. **289** (1991) 255-283.

[PS04] P. Philippon, M. Sombra, *Quelques aspects diophantiens des variétés toriques projectives.* E-print `math.NT/0411084`, 38 pp.

[Pon01] C. Pontreau, *Une généralisation du théorème de Dobrowolski pour les hypersurfaces algébriques.* Master thesis, Univ. Caen, 2001. Downloadable from `http://www.math.unicaen.fr/~pontreau/`.

[Pon05a] C. Pontreau, *Minoration effective de la hauteur des points d'une courbe de G_m^2 définie sur $\mathbb{Q}$.* Acta Arith. Vol. **120** Nr. 1 (2005) 1-26.

[Pon05b] C. Pontreau, *Geometric lower bounds for the normalized height of hypersurfaces.* To appear Int. J. of Number Theory (2006).

[Vou96] P. Voutier, *An effective lower bound for the height of algebraic numbers.* Acta Arith. 74 (1996) 81–95.

[Zag93] D. Zagier, *Algebraic numbers close to both 0 and 1.* Math. Comp. **61** (1993) 485-491.

[Zas69] H. Zassenhaus, *On Hensel factorization.* J. Number Theory **1** (1969) 291-311.

[Zha95] S. Zhang, *Small points and adelic metrics.* J. Alg. Geom. **4** (1995) 281-300.

Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires
E-mail address: mavendar@bigua.dm.uba.ar

Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires
E-mail address: krick@dm.uba.ar

Departament d'Àlgebra i Geometria, Universitat de Barcelona
E-mail address: sombra@ub.edu