HAL open science

Height Bounds, Nullstellensatz and Primality

Haydar Göral

▶ To cite this version:

Haydar Göral. Height Bounds, Nullstellensatz and Primality. 2012. hal-00738713v4

HAL Id: hal-00738713
https://hal.science/hal-00738713v4

Preprint submitted on 22 Oct 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

HEIGHT BOUNDS, NULLSTELLENSATZ AND PRIMALITY

HAYDAR GÖRAL

Abstract. In this study, we find height bounds in the polynomial ring over the field of algebraic numbers to test the primality of an ideal. We also obtain height bounds in the arithmetic Nullstellensatz. We apply nonstandard analysis and hence our constants will be ineffective.

1. Introduction

In this paper, our goal is to augment a result of van den Dries and Schmidt [8] by obtaining height bounds in the polynomial ring over the field of algebraic numbers to test the primality of an ideal. We also find height bounds in the arithmetic Nullstellensatz and a version of it.

Factorization is a difficult problem in integers and also in polynomial rings over fields. A primality test is an algorithm to decide whether an input number or polynomial is prime or not. Such tests have wide applications, for example in cryptography. There are many explicit methods to check the primality of an ideal over polynomial rings. On the other hand, nonstandard analysis can be useful to give noneffective criteria for the primality of an ideal. Nonstandard analysis originated in the 1960's in the work of Robinson, as a rigorous and exhaustive way of studying infinitesimal calculus. Now let K be a field and I be an ideal of $K[X_1, ..., X_n]$. It is well-known that $K[X_1, ..., X_n]$ is Noetherian, which means that every ideal of $K[X_1, ..., X_n]$ is finitely generated. We say that I is a *D-type ideal* if I is generated by polynomials of degree at most D. In [8, Theorem 2.10], using nonstandard analysis van den Dries and Schmidt proved that there is a bound $P(n, D)$ depending only on n and D such that if I is a D-type ideal then I is prime if and only if $1 \notin I$, and for all f, g in $K[X_1, ..., X_n]$ of degree less than $P(n, D)$, $fg \in I$ implies that f is in I or g is in I. In other words, to test the primality of an ideal in $K[X_1, ..., X_n]$, it is enough to check all products of

Partially supported by ValCoMo (ANR-13-BS01-0006) and MALOA (PITN-GA-2009-238381).
2010 *Mathematics subject classification.* 11G50, 03C98, 13L05.
Key words and phrases: model theory, nonstandard analysis, height, primality.

polynomials up to a certain degree bound. This result has algebraic-geometric consequences when K is algebraically closed. An explicit version of the bound $P(n, D)$ is not known. However, a partial result was given by Schmidt [25].

The ideal membership problem has been studied extensively. The following result was launched by Hentzelt and Noether [13] and then established in a paper by Hermann [14] using algorithmic tools: If $f_0, f_1, ..., f_s$ in $K[X_1, ..., X_n]$ all have degrees less than D and f_0 in $(f_1, ..., f_s)$, then

$$f_0 = \sum_{i=1}^{s} f_i h_i$$

for certain h_i whose degrees are bounded by a constant $C = C(n, D)$ depending only on n and D. This result was clarified by Seidenberg [26], and moreover it was obtained that we may take $C(n, D) = (2D)^{2^n}$. Applying nonstandard analysis, the same result was reproved by van den Dries and Schmidt [8], but the result is ineffective. Later on, Aschenbrenner [4] generalized Hermann's result to Prüfer domains but again the method is ineffective. One can improve the doubly exponential bound $C(n, D)$ drastically, if we consider the case of Nullstellensatz and take $f_0 = 1$. By the seminal work of Kollár [17], if $f_0 = 1$ then one can choose $C(n, D) = D^n$ for $D \geq 3$. Moreover, by the work of Sombra [28], we can take $C(n, 2) = 2^{n+1}$.

The ideal membership problem over the ring of integers $\mathbb{Z}$ and effective results were studied by Aschenbrenner [1, 2] and Krick, Pardo and Sombra [18]. Contrary to the field case, there is no uniform degree bound for $h_1, ..., h_s$ in the ideal membership problem which depends only on n and D. In [2], it was shown that there is a uniform degree bound which depends on n and D as well as the coefficients of the polynomials $f_1, ..., f_s$ in question. Estimates for the height of polynomials $h_1, ..., h_s$ were obtained in [18] for the arithmetic Nullstellensatz, and there the number of generators also plays a significant role.

The results in [8] influenced us to apply nonstandard analysis in the current paper. Here we show that it is also enough to check the primality up to a certain height

bound, and we provide uniform height bounds for the case of Nullstellensatz. More precisely, let $\overline{\mathbb{Q}}$ be the field of algebraic numbers and H be the *height function* on $\overline{\mathbb{Q}}$. For a polynomial f in several variables over the field of algebraic numbers, define the height of f as the maximum of the heights of its coefficients. We say that an ideal I of $\overline{\mathbb{Q}}[X_1, ..., X_n]$ is a (D, H)*-type ideal*, if I can be generated by elements of degree at most D and height at most H. We prove the existence of the constants C in the following three results. An explicit bound C below is not known in general. The main observation that makes the machinery of the paper is **Lemma 2.4**, which may be seen as the model-theoretic analog of the properties of the height function and Gelfond's lemma (see Fact 2.1 and Theorem 2.2). More precisely, we prove the following results:

Theorem A. *There are bounds $P(n, D)$ and $C(n, D, H)$ such that if I is a (D, H)-type ideal of $\overline{\mathbb{Q}}[X_1, ..., X_n]$ then I is prime if and only if $1 \notin I$, and for all f, g in $\overline{\mathbb{Q}}[X_1, ..., X_n]$ of degree less than $P(n, D)$ and height less than $C(n, D, H)$, if $fg \in I$, then f or g is in I.*

Theorem B. *There are bounds $N = N(n, D)$, $r = r(n, D)$ and $C = C(n, D, H)$ such that for all polynomials $f_1, ..., f_m, g$ in $\overline{\mathbb{Q}}[X_1, ..., X_n]$ of degree at most D and height at most H, if g vanishes for all joint zeros of $f_1, ..., f_m$, then there are $h_1, ..., h_m$ in $\overline{\mathbb{Q}}[X_1, ..., X_n]$ of degree at most N and height at most C such that $g^r = f_1h_1 + \cdots + f_mh_m$.*

Theorem C. *There exists $C(n, D, H)$ such that for all polynomials $f_1, ..., f_m, g$ in $\overline{\mathbb{Q}}[X_1, ..., X_n]$ of degree at most D and height at most H, if there is some $x \in \overline{\mathbb{Q}}^n$ such that $f_1(x) = \cdots = f_m(x) = 0$, $g(x) \neq 0$, then there is some x with this property of height at most C.*

2. Preliminaries

2.1. **The Height Function.** For the details of this subsection we refer the reader to [5, Chapter 1] and [15, Part B, B.7].

Before defining the height function, we first define the *Mahler measure* of a polynomial over $\mathbb{C}$. For a non-zero polynomial $f(x) = a_d(X - \alpha_1) \cdots (X - \alpha_d)$ with complex

coefficients, its *Mahler measure* is defined as the product

$$m(f) = |a_d| \prod_{|\alpha_j| \geq 1} |\alpha_j|.$$

By convention $m(0)$ is defined to be 1. For a non-zero α in $\overline{\mathbb{Q}}$ with minimal (irreducible) polynomial $f(x) \in \mathbb{Z}[X]$ of degree d, we define its *Mahler measure* as $m(\alpha) = m(f)$. The *height* of α is defined by

$$H(\alpha) = m(\alpha)^{1/d}.$$

Sometimes one also considers the logarithm of the height function and it is called the logarithmic height function. Note that $H(0) = 1$ and for a non-zero integer a we have $H(a) = |a|$. It is not known whether there exists an absolute constant $c > 1$ such that if $m(\alpha) > 1$ then $m(\alpha) \geq c$; see [19, 27]. The height function measures the arithmetic complexity of an algebraic number and it behaves well under arithmetic operations. More precisely, the height function satisfies the following properties:

Fact 2.1.

- $H(0) = H(1) = 1$,
- For a non-zero rational number a/b where a and b are coprime,

$$H(a/b) = \max\{|a|, |b|\},$$

- For all α in $\overline{\mathbb{Q}}$ and $n \in \mathbb{N}$, we have $H(\alpha^n) = H(\alpha)^n$,
- For all α and β in $\overline{\mathbb{Q}}$, we have $H(\alpha + \beta) \leq 2H(\alpha)H(\beta)$,
- For all α and β in $\overline{\mathbb{Q}}$, we have $H(\alpha\beta) \leq H(\alpha)H(\beta)$,
- For all non-zero α in $\overline{\mathbb{Q}}$, we have $H(1/\alpha) = H(\alpha)$.

Now we give the *height inequality* which is also called Gelfond's lemma. There is a relation between the height of a polynomial and the height of its roots. For a polynomial

$$f = a_0 + a_1 X + \cdots + a_d X^d$$

over the field of algebraic numbers, define

$$H(f) = \max_i H(a_i).$$

Similarly we can define the height of a polynomial in several variables, as we already mentioned in the introduction. The following lemma is the height inequality and it states that the height function translates geometric properties into arithmetic ones.

Theorem 2.2. [5, Theorem 1.6.13] *and* [15, Proposition B.7.2]
For a polynomial

$$f(x) = (X - \alpha_1) \cdots (X - \alpha_d) = a_0 + a_1 X + \cdots + X^d \in \overline{\mathbb{Q}}[X],$$

we have that

$$\prod_{i \leq d} H(\alpha_i) \leq 2^{2d+1} H(f).$$

2.2. **Nonstandard Analysis.** Next, we define nonstandard extension which we will need in the proof of our results.

Definition 2.3. (Nonstandard Extension of a Structure) Let $\mathbb{M}$ be a nonempty structure in a countable language L. A *nonstandard extension* ${}^*\mathbb{M}$ of $\mathbb{M}$ is an ultrapower of $\mathbb{M}$ with respect to a non-principal ultrafilter on $\mathbb{N}$.

Now let ${}^*\mathbb{M}$ be a nonstandard extension of $\mathbb{M}$ with respect to a non-principal ultrafilter D on $\mathbb{N}$. The elements of ${}^*\mathbb{M}$ are of the form $(x_n)_n/D$ where $(x_n)_n$ is a sequence in $\mathbb{M}$. We identify each element x of $\mathbb{M}$ with the class of the constant sequence $(x)_n/D$ of ${}^*\mathbb{M}$. Viewing $\mathbb{M}$ as a subset of ${}^*\mathbb{M}$ in this way, the structure $\mathbb{M}$ becomes an elementary substructure of ${}^*\mathbb{M}$. For a subset A of $\mathbb{M}$, the set ${}^*A$ is defined to be the set

$$\{(a_n)_n/D : \{n : a_n \in A\} \in D\}.$$

Note that ${}^*A$ contains A. Every function on a subset A of $\mathbb{M}$ extends to ${}^*A$ coordinatewise and this is well-defined. Subsets of ${}^*\mathbb{M}$ of the form ${}^*A$ for some subset A of $\mathbb{M}$ are called internal. Not every subset of ${}^*\mathbb{M}$ is internal. The following sets ${}^*\mathbb{N}$, ${}^*\mathbb{Z}$, ${}^*\mathbb{Q}$, ${}^*\mathbb{R}$ are called hypernatural numbers, hyperintegers, hyperrational numbers and hyperreals respectively. The elements ${}^*\mathbb{R} \setminus \mathbb{R}$ are called *nonstandard real numbers.* Let

$$\mathbb{R}_{fin} = \{x \in {}^*\mathbb{R} : |x| < n \text{ for some } n \in \mathbb{N}\}$$

be the set of finite numbers. The elements in ${}^*\mathbb{R} \setminus \mathbb{R}_{fin}$ are called infinite. Note that $\mathbb{R}_{fin}$ is a subring of ${}^*\mathbb{R}$ containing $\mathbb{R}$.

The notion of a nonstandard extension and its properties can be generalized to many-sorted structures. This will be significant for the concept of the height function which takes values in $\mathbb{R}$. For more detailed information about nonstandard analysis and model theory, the reader might consult [10, 12] and [20].

Let ${}^*\overline{\mathbb{Q}}$ be a nonstandard extension of $\overline{\mathbb{Q}}$ with respect to a non-principal ultrafilter D on $\mathbb{N}$. Note that ${}^*\overline{\mathbb{Q}}$ is also algebraically closed. For an element $x = (x_n)_n/D$ in ${}^*\overline{\mathbb{Q}}$, its height is defined to be

$$(H(x_n))_n/D.$$

Set

$$\overline{\mathbb{Q}}_{fin} = \{x \in {}^*\overline{\mathbb{Q}} : H(x) \in \mathbb{R}_{fin}\}.$$

As the height function is unbounded, the extension

$$\overline{\mathbb{Q}}_{fin} \subsetneq {}^*\overline{\mathbb{Q}}$$

is proper. The element $(2^{1/n})_n/D$ is in $\overline{\mathbb{Q}}_{fin}$ and it is not in $\overline{\mathbb{Q}}$. Hence the extension $\overline{\mathbb{Q}} \subsetneq \overline{\mathbb{Q}}_{fin}$ is also proper. The following lemma plays a central role in proving all the results of the paper, and it is the model-theoretic analog of the properties of the height function and Gelfond's lemma.

Lemma 2.4. *The set $\overline{\mathbb{Q}}_{fin}$ is an algebraically closed subfield of ${}^*\overline{\mathbb{Q}}$.*

Proof. Since the height function behaves well under addition, multiplication and inverse as given in Fact 2.1, we obtain that $\overline{\mathbb{Q}}_{fin}$ is a field. By the height inequality Theorem 2.2, we see that $\overline{\mathbb{Q}}_{fin}$ is also algebraically closed. □

2.3. **Degree Bound.** In this subsection, we provide some facts from commutative algebra and give the result in [8].

Let $F \subseteq E$ be a field extension. The following fact is well-known and completely standard, as a consequence of the faithful flatness of $E[X_1, ..., X_n]$ over $F[X_1, ..., X_n]$.

Fact 2.5. Let $F \subseteq E$ be a field extension and $I \subset F[X_1, ..., X_n]$ be a proper ideal. Then the ideal $IE[X_1, ..., X_n] \subset E[X_1, ..., X_n]$ is also proper. Moreover, we have the following equality

$$(IE[X_1, ..., X_n]) \cap F[X_1, ..., X_n] = I.$$

Recall that a field extension $F \subseteq E$ is called *regular*, if E and F^{ac} are linearly disjoint over F. For the following fact, we refer the reader to [6, Chapter 5, Section 15, Proposition 15] and [6, Chapter 5, Section 17, Corollary to Proposition 1].

Fact 2.6. Let $F \subseteq E$ be a regular field extension and $I \subseteq F[X_1, ..., X_n]$. Then I is a prime ideal in $F[X_1, ..., X_n]$ if and only if $IE[X_1, ..., X_n]$ is a prime ideal in $E[X_1, ..., X_n]$.

Now let K be a field and take a nonstandard extension ${}^*\mathbb{K}$ of the 2-sorted structure

$$\mathbb{K} = (K[X_1, ..., X_n], +, -, \cdot, 0, 1, \deg, \mathbb{N}),$$

where deg is the degree function on $K[X_1, ..., X_n]$ assuming values in $\mathbb{N}$. Note that

$${}^*K[X_1, ..., X_n] \subsetneq {}^*(K[X_1, ..., X_n])$$

and ${}^*K[X_1, ..., X_n] = \{f \in {}^*(K[X_1, ..., X_n]) : \deg f \in \mathbb{N}\}$. The following Theorem is from [8, 2.5] and it yields the existence of the constant P in Theorem A.

Theorem 2.7. [8, 2.5] *Let K be a field. The ideal I of ${}^*K[X_1, ..., X_n]$ is a prime ideal in ${}^*K[X_1, ..., X_n]$ if and only if $I^*(K[X_1, ..., X_n])$ is a prime ideal in the nonstandard extension ${}^*(K[X_1, ..., X_n])$.*

3. Results

3.1. **Proof of Theorem A.**

Proof. Note that

$$V(n, D) = \{f \in \overline{\mathbb{Q}}[X_1, ..., X_n] : \deg(f) \leq D\}$$

is a finite dimensional vector space over $\overline{\mathbb{Q}}$. In fact, the dimension is

$$q(n,D)=\binom{n+D}{n}.$$

Thus if $J=(f_1,...,f_s)$ is an ideal of D-type, then the number of generators of J can be taken less than q. So we can always assume that $s\leq q$. We know the existence of the bound $P=P(n,D)$ by [8]. Now we prove the existence of the bound $C(n,D,H)$. Suppose there is no such bound. This means that for all $m>0$ there is an ideal I_m of (D,H)-type of $\overline{\mathbb{Q}}[X_1,...,X_n]$ which is not prime such that for all f,g with $\deg f$ and $\deg g$ less than P, and $H(f)$, $H(g)$ less than m, if $fg\in I_m$ then f or g is in I_m. Let ${}^*\mathbb{M}$ be a nonstandard extension of the many-sorted structure

$$\mathbb{M}=(\overline{\mathbb{Q}}[X_1,...,X_n],+,-,\cdot,0,1,H,\deg,\mathbb{R}_{\geq 1},\mathbb{N}),$$

where H is the height function from $\overline{\mathbb{Q}}[X_1,...,X_n]$ to $\mathbb{R}_{\geq 1}$, and deg is the degree function on $\overline{\mathbb{Q}}[X_1,...,X_n]$ which takes values in $\mathbb{N}$. Then the functions H and deg extend to ${}^*(\overline{\mathbb{Q}}[X_1,...,X_n])$ and they take values in the positive hyperreals ≥ 1 and hypernaturals respectively. Then by saturation, there is an ideal I of (D,H)-type of ${}^*(\overline{\mathbb{Q}}[X_1,...,X_n])$ which is not prime but for all $m>0$, if f,g are of degree less than P and are of height less than m, if $fg\in I$ then f or g is in I. Now, we see that the ideal I is prime in $\overline{\mathbb{Q}}_{fin}[X_1,...,X_n]$. However, it is not prime in ${}^*\overline{\mathbb{Q}}[X_1,...,X_n]$ by Theorem 2.7. This contradicts Fact 2.6 since $\overline{\mathbb{Q}}_{fin}$ is algebraically closed by Lemma 2.4, and the field extension $\overline{\mathbb{Q}}_{fin}\subseteq {}^*\overline{\mathbb{Q}}$ is regular. □

3.2. **Proof of Theorem B.**

Proof. Suppose that n,D and H are fixed. The existence of $N=N(n,D)$ and $r=r(n,D)$ is well-known and was already proved in [23, Chapter 8] and [24, Section 4]. For the sake of completeness, we give its proof briefly here. As in the proof of Theorem A, we can assume that

$$m\leq q(n,D)=\binom{n+D}{n}.$$

It is enough to show that there exists $N'(n,D)$ such that for all algebraically closed fields K and polynomials $f_1,...,f_m$ in $K[X_1,...,X_n]$ of degree at most D without common zeros in K^n, there are $h_1,...,h_m$ in $K[X_1,...,X_n]$ of degree at most N' such that

$1 = f_1h_1 + \cdots + f_mh_m$. The existence of N' implies the existence of N, r by the Rabinovich trick: introduce a new variable Y and the additional polynomial $f_0 = 1 - gY$; then we see that $f_0, f_1, ..., f_m$ have no common zeros. Now suppose that there is no such bound N'. Then we obtain a non-standard extension ${}^*K$ of K and polynomials $f_1, ..., f_m \in {}^*K[X_1, ..., X_n]$ of degree at most D without common zeros in $({}^*K)^n$. However, $1 \notin (f_1, ..., f_m)$, contradicting Hilbert's Nullstellensatz applied to the algebraically closed field ${}^*K$. Thus we proved the existence of N and r. Now we show the existence of $C = C(n, D, H)$. Suppose that there is no such bound $C = C(n, D, H)$. Then we obtain a non-standard extension ${}^*\overline{\mathbb{Q}}$ and polynomials $f_1, ..., f_m, g \in \overline{\mathbb{Q}}_{fin}[X_1, ..., X_n]$ of degree at most D and height at most H such that g vanishes for all joint zeros of $f_1, ..., f_m$ in $({}^*\overline{\mathbb{Q}})^n$ but there are no $h_1, ..., h_m \in \overline{\mathbb{Q}}_{fin}[X_1, ..., X_n]$ of degree at most N such that $g^r = f_1h_1 + \cdots + f_mh_m$. However, by Lemma 2.4, the field $\overline{\mathbb{Q}}_{fin}$ is algebraically closed. This contradicts the choice of N and r. □

3.3. **Proof of Theorem C.**

Proof. Suppose there is no such bound $C(n, D, H)$. Then, we obtain a non-standard extension ${}^*\overline{\mathbb{Q}}$ and polynomials $f_1, ..., f_m, g \in \overline{\mathbb{Q}}_{fin}[X_1, ..., X_n]$ (of degree at most D and height at most H) such that for some x in $({}^*\overline{\mathbb{Q}})^n$ we have $f_1(x) = \cdots = f_m(x) = 0$ and $g(x) \neq 0$, but there is no such x in $(\overline{\mathbb{Q}}_{fin})^n$. This contradicts Lemma 2.4 as $\overline{\mathbb{Q}}_{fin}$ is an elementary substructure of ${}^*\overline{\mathbb{Q}}$ by model-completeness of the theory of algebraically closed fields. □

3.4. **Some Corollaries.** Next, we prove the existence of a height bound similar to the height bound in Theorem A. For the details of this subsection, we direct the reader to [9, 21]. Let R be a commutative Noetherian ring with 1 and M be an R-module. For a prime ideal p of R, we say that p is an associated prime of M, if p is the annihilator of some x in M. For an ideal J of R, the associated prime ideals containing J coincide with $Ass_R(R/J)$, which in fact is the set of prime ideals that are the radicals of the primary ideals occurring in the primary decomposition of J. First, we recall the following facts from commutative algebra.

Remark 3.1.

- An ideal J is a primary ideal if and only if

$$Ass_R(R/J)$$

has exactly one element.

- Every ideal J (through primary decomposition) is expressible as a finite intersection of primary ideals. The radical of each of these ideals is a prime ideal and these primes are exactly the elements of $Ass_R(R/J)$.
- Any prime ideal that is minimal with respect to containing an ideal J is in $Ass_R(R/J)$. These primes are precisely the isolated primes.

Corollary 3.2. *Let $n \in \mathbb{N}$, $X = (X_1, ..., X_n)$ and I be an ideal of $\overline{\mathbb{Q}}_{fin}[X]$.*

(1) *If $p_k, ..., p_m$ are the distinct minimal primes of I then*

$$p_1{}^*\overline{\mathbb{Q}}[X], ..., p_m{}^*\overline{\mathbb{Q}}[X]$$

are the distinct minimal primes of $I^*\overline{\mathbb{Q}}[X_1, ..., X_n]$.

(2) $\sqrt{I^*\overline{\mathbb{Q}}[X]} = \sqrt{I}^*\overline{\mathbb{Q}}[X]$.

(3) *If M is a $\overline{\mathbb{Q}}_{fin}[X]$-module, then*

$$Ass_{*\overline{\mathbb{Q}}[X]}(M \otimes_{\overline{\mathbb{Q}}_{fin}[X]} {}^*\overline{\mathbb{Q}}[X]) = \{p^*\overline{\mathbb{Q}}[X] : p \in Ass_{\overline{\mathbb{Q}}_{fin}[X]}(M)\}.$$

(4) *The ideal I is a primary ideal if and only if $I^*\overline{\mathbb{Q}}[X]$ is a primary ideal of ${}^*\overline{\mathbb{Q}}[X]$.*

(5) *Let $I = I_1 \cap ... \cap I_m$ be a reduced primary decomposition, I_k being a p_k-primary ideal. Then*

$$I^*\overline{\mathbb{Q}}[X] = I_1{}^*\overline{\mathbb{Q}}[X] \cap ... \cap I_m{}^*\overline{\mathbb{Q}}[X]$$

is a reduced primary decomposition of $I^*\overline{\mathbb{Q}}[X]$, and $I_k{}^*\overline{\mathbb{Q}}[X]$ is a $p_k{}^*\overline{\mathbb{Q}}[X]$-primary ideal.

Proof. (1) is an immediate consequence of Fact 2.6 and Lemma 2.4. (2) follows from (1), since the radical of an ideal is the intersection of minimal prime ideals which contain the ideal. Since $\overline{\mathbb{Q}}_{fin}[X]$ is Noetherian, (3) follows from [7, Chapter 4, 2.6, Theorem 2] and Fact 2.5. To prove (4), suppose that I is a p-primary ideal. So we get $Ass_{\overline{\mathbb{Q}}_{fin}[X]}(\overline{\mathbb{Q}}_{fin}[X]/I) = \{p\}$. Applying (3) with $M = \overline{\mathbb{Q}}_{fin}[X]/I$, we obtain that

$Ass_{*\overline{\mathbb{Q}}[X]}(^*\overline{\mathbb{Q}}[X]/I) = \{p^*\overline{\mathbb{Q}}[X]\}$ and this yields (4) with the help of Remark 3.1. The converse of (4) can be seen by Fact 2.5. (5) follows from (4). □

Now we give the standard corollaries with no proof, since the proofs are similar to that of Theorem A. For the following corollary, the existence of the constant $E(n, D, H)$ is new and the other constants are due to [8].

Corollary 3.3. *There are constants $B(n, D)$, $M(n, D)$ and $E(n, D, H)$ such that if I is an ideal of (D, H)-type, then*

(1) *$\sqrt{I}$ is generated by polynomials of degree less than B and height less than E, if $f \in \sqrt{I}$ then $f^M \in I$.*
(2) *There are at most B associated primes of I and each is generated by polynomials of degree less than B and height less than E.*
(3) *I is primary if and only if $1 \notin I$, and for all f, g of degree less than B and height less than E, if $fg \in I$ then $f \in I$ or $g^M \in I$.*
(4) *There is a reduced primary decomposition of I consisting of at most B primary ideals, each of which is generated by polynomials of degree at most B and height at most E.*

4. Generalized Height Function

In this section we define a generalized version of the height function, and we state a generalized version of Theorem A for fields. For this purpose, we let R be a commutative ring with unity, and $\theta : \mathbb{N} \to \mathbb{N}$ be a function. We say that

$$h : R \to [0, \infty)$$

is a *height function* of θ-type if for any x and y in R with $h(x) \leq n$ and $h(y) \leq n$, then both $h(x + y) \leq \theta(n)$ and $h(xy) \leq \theta(n)$. We say that h is a height function on R if h is a height function of θ-type for some $\theta : \mathbb{N} \to \mathbb{N}$.

We can extend the height function h to the polynomial ring $R[X_1, ..., X_n]$ by setting

$$h\left(\sum_{\alpha} a_\alpha X^\alpha\right) = \max_{\alpha} h(a_\alpha).$$

Note that this extension does not have to be a height function, it is just an extension of functions. Now we give some examples of height functions.

Example 4.1. For the following examples of height functions, one can take $\theta(n) = (n+1)^2$.

- The height function on the set of algebraic numbers.
- Absolute values on R.
- The degree function on $R[X_1, ..., X_n]$.
- Let λ be a positive real number. On $\mathbb{Z}[X]$, define

$$h(a_0 + a_1X + ... + a_kX^k) = \sum_{i=0}^{k} |a_i|\lambda^i.$$

  Then this is a height function on $\mathbb{Z}[X]$.

Constructing height functions has been always crucial, as it has important arithmetic consequences. To illustrate, elliptic curves over number fields are finitely generated and the height function attached to them plays a crucial role in the proof. For more on the general frameworks for constructing height functions, the reader may consult [16, 22]. The work of Kani [16] was discussed by Aschenbrenner [3], and this has applications to the ideal membership problem over $\mathbb{Z}$.

For a function $h : R \to [0, \infty)$ and a nonstandard extension ${}^*R$ of R, we define

$$R_{hfin} = \{x \in {}^*R : h(x) < n \text{ for some } n \in \mathbb{N}\}.$$

In fact, h being a height function can be detected by the set R_{hfin}. The following proposition gives a nonstandard point of view on the concept of height functions. However, this characterization is ineffective, i.e. it does not provide the θ-type of the height function.

Proposition 4.2. *A function $h : R \to [0, \infty)$ is a height function on R if and only if R_{hfin} is a subring of ${}^*R$.*

Proof. We see that if h is a height function of θ-type, then R_{hfin} is a subring by the first-order properties of the generalized height function. Conversely, suppose R_{hfin}

is a subring and h is not a height function. This means there is some $N \in \mathbb{N}$ such that we have two sequences (r_n) and (s_n) in R with $h(r_n) \leq N$ and $h(s_n) \leq N$, but $\lim_{n\to\infty} h(r_n \star s_n) = \infty$, where the binary operation $\star$ means either addition or multiplication. By saturation, we get two elements r and s in ${}^*R$ such that $h(r) \leq N$, $h(s) \leq N$ but $h(r \star s)$ is infinite. This contradicts the fact that R_{hfin} is a subring. $\square$

The next remark shows when R_{hfin} is internal.

Remark 4.3. Let h be a height function on R. The set R_{hfin} is an internal subset of ${}^*R$ if and only if h is bounded.

Proof. Suppose $R_{hfin} = {}^*A$ for some subset A of R. First we show that the height function on A must be bounded. To see this, if there is a sequence $(a_n)_n$ in A such that $\lim_{n\to\infty} h(a_n) = \infty$, then there is an element in ${}^*A$ whose height is infinite. This contradicts the fact that all the elements in R_{hfin} have bounded height. So the height function on A is bounded. Therefore the height function on ${}^*A$ is also bounded. However since R_{hfin} contains R, the height function on R must be bounded. Conversely if the height function on R is bounded, then we have $R_{hfin} = {}^*R$ and so R_{hfin} is internal. $\square$

Definition 4.4. Let K be an algebraically closed field with a height function h. We say that h satisfies the height inequality, if for every d there is a bound $B(d)$ such that for each monic polynomial $f(x)$ in $K[X]$ of degree d and each zero α of f, we have

$$h(\alpha) \leq B(d)h(f).$$

We finish with a generalized version of Theorem A with no proof, as the proof is similar to that of Theorem A.

Theorem 4.5. *Let K be an algebraically closed field with a height function of θ-type. Suppose that for any non-zero x in K with $h(x) \leq n$, we have $h(1/x) \leq \theta(n)$. Moreover suppose that h satisfies the height inequality. Then there are bounds $P(n, D)$ and $C(n, D, H)$ such that if I is a (D, H)-type ideal of $K[X_1, ..., X_n]$ then I is prime if and only if $1 \notin I$, and for all f, g in $K[X_1, ..., X_n]$ of degree less than $P(n, D)$ and height less than $C(n, D, H)$, if $fg \in I$, then f or g is in I.*

In Theorem 4.5, there are cases where K does not have to be algebraically closed and we do not need h to satisfy the height inequality. If the height function on K is bounded, then we do not require K to be algebraically closed. By Northcott's theorem [5, Theorem 1.6.8], there are only finitely many elements of bounded height and degree in $\overline{\mathbb{Q}}$. This yields that the height bound C is trivial when K is a number field.

From the nonstandard point of view, for any ideal I of $K_{hfin}[X_1, ..., X_n]$ if we have that I is prime if and only if the ideal $I^*K[X_1, ..., X_n]$ is prime in ${}^*K[X_1, ..., X_n]$, then the conclusion of Theorem 4.5 holds without assuming that K is algebraically closed and h obeys the height inequality. In light of Fact 2.6, this means that Theorem 4.5 holds whenever the field extension $K_{hfin} \subseteq {}^*K$ is regular; to illustrate, if K_{hfin} is an elementary substructure of ${}^*K$. This will be the case if K is the field of real algebraic numbers with the height function H. If h is an absolute value function on a field, then the result 4.5 holds again. Finally, if K_{hfin} is an elementary substructure of ${}^*K$, then this leads to Theorem C as well.

Acknowledgements. This work is partially based on the author's Ph.D thesis [11]. The author thanks his Ph.D supervisors Amador Martin-Pizarro and Frank Wagner for many motivating discussions. The author also would like to thank the anonymous referee for the invaluable suggestions, which immensely improved the quality and presentation of the paper.

References

[1] M. Aschenbrenner, Ideal Membership in Polynomial Rings over the Integers, Ph.D. thesis, University of Illinois at Urbana-Champaign, 2001.

[2] M. Aschenbrenner, Ideal membership in polynomial rings over the integers, *J. Amer. Math. Soc.* **17** (2004), 407-441.

[3] M. Aschenbrenner, *An effective Weierstrass Division Theorem*, preprint.

[4] M. Aschenbrenner, *Bounds and definability in polynomial rings*, Quart. J. Math. **56** (2005), 263-300.

[5] E. Bombieri, W. Gubler, Heights in Diophantine Geometry, Cambridge University Press; 1st edition (September 24, 2007).

[6] N. Bourbaki, Elements of Mathematics, Algebra 2, Chapters 4-7.

[7] N. Bourbaki, Commutative Algebra, Paris: Hermann, 1972.

[8] L. van den Dries and K. Schmidt, *Bounds in the theory of polynomial rings over fields. A nonstandard approach*, Inventiones Math. **76** (1984), 77-91.

[9] D. Eisenbud, Commutative Algebra with a View toward Algebraic Geometry, Springer-Verlag, 2004.

[10] R. Goldblatt, Lectures on the Hyperreals, A Introduction to Nonstandard Analysis Springer-Verlag, New York, 1998.

[11] H. Göral, Model Theory of Fields and Heights, Ph.D thesis, Lyon, 2015.

[12] C. W. Henson, Foundation of Nonstandard Analysis, A Gentle Introduction to Nonstandard Extensions, Lecture Notes.

[13] K. Hentzelt, E. Noether, *Zur Theorie der Polynomideale und Resultanten.* Math. Ann. **88**, 1923, 53-79.

[14] G. Hermann *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. **95** (1926), 736-788.

[15] M. Hindry, J.H. Silverman, Diophantine Geometry, An Introduction, Springer-Verlag, 2000.

[16] E. Kani, Nonstandard Diophantische Geometrie, insbesondere Satz von Mordell-Weil, Ph.D thesis, Universität Heidelberg, 1978.

[17] J. Kollár, Sharp Effective Nullstellensatz, *Journal of the American Math. Soc.* Volume 1, Number 4, 1988.

[18] T. Krick, L.M. Pardo, M. Sombra, *Sharp estimates for the arithmetic Nullstellensatz*, Duke Math. J. 109 (2001), no. 3, 521-598.

[19] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. (2) **34** (1933), 461-479.

[20] D. Marker, Model Theory: An Introduction, Springer-Verlag, New York, 2002.

[21] H. Matsumura, Commutative Algebra, Second Edition, U.S.A, 1980.

[22] A. Moriwaki, *Arithmetic height functions over finitely generated fields*, Inventiones Math. (2000) 140, 101-142.

[23] A. Robinson, *Théorie métamathématiques des idéaux*, collection de logique mathématiques, Ser A, Paris-Louvain, 1955.

[24] A. Robinson, *Some problems of definability in the lower predicate calculus*, J. Symbolic Logic, Volume 25, Issue 2 (1960), 171.

[25] K. Schmidt, *Polynomial bounds in polynomial rings over fields*, J. Algebra **125**, 164-180 (1989).

[26] A. Seidenberg, *Constructions in algebra*, Trans. AMS 197, 273-313 (1974).

[27] C. Smyth, *The Mahler Measure of Algebraic Numbers: A survey* Number Theory and Polynomials, 322-349, London Math. Soc. Lecture Note Ser., 352, Cambridge Univ. Press, Cambridge, 2008.

[28] M. Sombra, *Sparse Effective Nullstellensatz*, Advances in Applied Mathematics, Volume 22, Issue 2, February 1999, Pages 271-295.

Department of Mathematics, Koç University, Rumelifeneri Yolu, 34450, Sariyer, Istanbul, TURKEY.

E-mail address: hgoral@gmail.com