

# On ascending chains of ideals in the polynomial ring

Grzegorz Pastuszak (Toruń)

## Abstract

Assume that  $K$  is a field and  $I_1 \subsetneq \dots \subsetneq I_t$  is an ascending chain (of length  $t$ ) of ideals in the polynomial ring  $K[x_1, \dots, x_m]$ , for some  $m \geq 1$ . Suppose that  $I_j$  is generated by polynomials of degrees less or equal to some natural number  $f(j) \geq 1$ , for any  $j = 1, \dots, t$ . In the paper we construct, in an elementary way, a natural number  $\mathcal{B}(m, f)$  (depending on  $m$  and the function  $f$ ) such that  $t \leq \mathcal{B}(m, f)$ . We also discuss some possible applications of this result.

## 1 Introduction

Assume that  $K$  is a field and  $K[x_1, \dots, x_m]$  is the polynomial ring over  $K$  in  $m \geq 1$  variables. Denote by  $\mathbb{N}_1$  the set of all natural numbers greater or equal to 1 and let  $f : \mathbb{N}_1 \rightarrow \mathbb{N}_1$  be an arbitrary function. Assume that

$$I_1 \subsetneq \dots \subsetneq I_t \subseteq K[x_1, \dots, x_m]$$

is an ascending chain (of length  $t$ ) of ideals such that  $I_j$  is generated by polynomials of degrees less or equal to  $f(j)$ , for any  $j = 1, \dots, t$ .

In [17] A. Seidenberg shows that there exists a natural number  $g_m(f)$ , for an increasing  $f$ , such that  $t \leq g_m(f)$ . He proposes rather complicated, but an explicit formula for  $g_m(f)$  in terms of  $m$  and  $f$ . In [12] [G. Moreno Socías](#) finds a better bound for the number  $t$  and expresses it, in terms of  $m$  and  $f$ , in a quite optimal way. He also shows, among other things, that the number [g<sub>m</sub>\(f\) is primitive recursive in f, for any m ≥ 1](#). Another approach to the problem is given in [3] where the authors obtain more general facts in somewhat extended context. For example, Proposition 3.22 from [3] implies some of the main results of [17] and [12]. Note that both [12] and [3] widely use the *Hilbert-Samuel polynomials* and related concepts, see for example [6, Chapter 4] and [7, Section 19.5].

This paper is devoted to construct the number  $g_m(f)$ , denoted here by  $\mathcal{B}(m, f)$ , in an elementary way. We apply only some basic facts from the theory of Gröbner bases.

The paper is organized as follows. In Section 2 we fix the notation and recall some information about Gröbner bases, e.g. the renowned algorithm for constructing a Gröbner basis of a given ideal, due to B. Buchberger.

Section 3 is the core of the paper. In Theorem 3.5 (concluding all the preceding results) we define a function  $\mathcal{B}$  with the *bounding property* which sets a bound on the length of antichains in  $\mathbb{N}^m$ , see Sections 2 and 3 for all the definitions. Our arguments are combinatorial and rather elementary. Theorem 3.5 is further applied in the next section.

In Section 4 we present the main results of the paper. We show how to reduce the general problem studied in the paper to the situation considered in Section 3. The main result on ascending chains of ideals in  $K[x_1, \dots, x_m]$  is given in Theorem 4.2. Furthermore, we derive some interesting consequences of Theorem 4.2 in Corollaries 4.4 and 4.5.

In the last section of the paper we describe our motivation to study bounds of ascending chains of ideals in the polynomial ring. As we write in detail in Section 5, the motivation comes from the first order logic and elimination of quantifiers. Namely, in the subsequent paper [13] we apply Corollary 4.5 to give a constructive proof of Tarski's theorem on quantifier elimination in the theory of algebraically closed fields. In a sense, the present paper rediscovers some of the main results of [12] and [3] in order to prove Tarski's theorem in a constructive way.

The results presented in the paper are part of the author's master's thesis, supervised by Stanisław Kasjan in 2007. The author is grateful to the supervisor for all discussions and support during the work on the thesis.

## 2 Gröbner bases and Buchberger's algorithm

We denote by  $\mathbb{N}$  the set of all natural numbers and by  $\mathbb{N}_1$  the set  $\mathbb{N} \setminus \{0\}$ . Assume that  $K$  is a field and  $m \in \mathbb{N}_1$ . Then  $K[x_1, \dots, x_m]$  is the polynomial ring over  $K$  in  $m$  variables  $x_1, \dots, x_m$ . The set of all monomials in  $K[x_1, \dots, x_m]$  is denoted by  $\mathbb{T}_m$ . If  $\alpha = (a_1, \dots, a_m) \in \mathbb{N}^m$ , then the monomial  $x_1^{a_1} \dots x_m^{a_m} \in \mathbb{T}_m$  is denoted by  $\underline{x}^\alpha$ . The *degree* of  $\underline{x}^\alpha = x_1^{a_1} \dots x_m^{a_m}$  is the sum  $a_1 + \dots + a_m$ . A polynomial  $f \in K[x_1, \dots, x_m]$  is denoted by  $\sum_{\alpha} a_{\alpha} \underline{x}^{\alpha}$  where  $a_{\alpha} \in K$  and  $a_{\alpha} = 0$  for almost all  $\alpha \in \mathbb{N}^m$ . If  $f = \sum_{\alpha} a_{\alpha} \underline{x}^{\alpha}$ , then the set  $\{\underline{x}^{\alpha}; a_{\alpha} \neq 0\}$  is the *support* of  $f$ . The *degree* of  $f$ , denoted by  $\deg(f)$ , is the maximum of degrees of monomials from the support of  $f$ .

Assume that  $m \in \mathbb{N}_1$ . We view the set  $\mathbb{N}^m$  as a monoid with respect to the pointwise addition, denoted by  $+$ . We denote by  $\underline{0}$  the neutral element  $(0, \dots, 0) \in \mathbb{N}^m$  of  $+$ . If  $\alpha, \beta \in \mathbb{N}^m$  and  $\alpha + \gamma = \beta$  for some  $\gamma \in \mathbb{N}^m$ , then we write  $\alpha \parallel \beta$ . Note that  $\parallel$  defines an order on  $\mathbb{N}^m$  and  $\mathbb{N}^m$  is an ordered monoid with respect to  $+$  and  $\parallel$ . Obviously,  $\alpha \parallel \beta$  if and only if  $\underline{x}^{\alpha}$  divides  $\underline{x}^{\beta}$ . If  $\alpha \in \mathbb{N}^m$  and  $\alpha = (a_1, \dots, a_m)$ , then we

set  $|\alpha| = a_1 + \dots + a_m$  and hence  $\deg(\underline{x}^\alpha) = |\alpha|$ . Recall that a binary relation  $\preccurlyeq$  on  $\mathbb{N}^m$  is an *admissible relation* (or an *admissible ordering*) if and only if the following three conditions are satisfied:  $\preccurlyeq$  is a linear ordering,  $\underline{0} \preccurlyeq \alpha$  for any  $\alpha \in \mathbb{N}^m$  and  $\alpha \preccurlyeq \beta$  yields  $\alpha + \gamma \preccurlyeq \beta + \gamma$  for any  $\alpha, \beta, \gamma \in \mathbb{N}^m$ . Note that  $\alpha \parallel \beta$  implies  $\alpha \preccurlyeq \beta$  and any admissible relation is a well-order, see Chapter 1 of [1]. We call an admissible relation  $\preccurlyeq$  on  $\mathbb{N}^m$  *graded* if and only if  $\alpha \preccurlyeq \beta$  implies  $|\alpha| \leq |\beta|$  for any  $\alpha, \beta \in \mathbb{N}^m$ . A basic example of an admissible relation is the *lexicographical order*. Its graded version is called the *degree lexicographical order*. We send to [1] for definitions of these orders, as well as for other examples.

It is easy to see that an admissible relation on  $\mathbb{N}^m$  induces a relation on the set  $\mathbb{T}_m$  of all monomials in  $K[x_1, \dots, x_m]$  via the natural identification  $(a_1, \dots, a_m) \leftrightarrow x_1^{a_1} \dots x_m^{a_m}$ . We call such a relation a *monomial ordering*.

Assume that  $\preccurlyeq$  is an admissible relation on  $\mathbb{N}^m$ . If  $f = \sum_{\alpha} a_{\alpha} \underline{x}^{\alpha}$  and  $\eta$  is the greatest element of the set  $\{\alpha \in \mathbb{N}^m; a_{\alpha} \neq 0\}$  with respect to  $\preccurlyeq$ , then  $\underline{x}^{\eta}$  is the *leading monomial* of  $f$  (denoted by  $\text{lm}(f)$ ) and  $a_{\eta} \underline{x}^{\eta}$  is the *leading term* of  $f$  (denoted by  $\text{lt}(f)$ ). If  $I$  is an ideal in  $K[x_1, \dots, x_m]$ , then we set  $\text{LM}(I) = \{\text{lm}(f); f \in I\}$  and  $\text{LT}(I) = \{\text{lt}(f); f \in I\}$ .

Assume that  $f, f_1, \dots, f_s \in K[x_1, \dots, x_m]$  and set  $F = \{f_1, \dots, f_s\}$ . Then there are  $a_1, \dots, a_s, r \in K[x_1, \dots, x_m]$  such that  $f = a_1 f_1 + \dots + a_s f_s + r$ ,  $\text{lm}(f)$  is the greatest element of the set  $\{\text{lm}(a_1 f_1), \dots, \text{lm}(a_s f_s), \text{lm}(r)\}$  and  $r$  is *reduced* modulo  $F$ , that is,  $\text{lm}(f_i)$  does not divide any element of support of  $r$ , for any  $i = 1, \dots, s$ . In this case we say that  $r$  is a *reduction* of  $f$  modulo  $F$  and we write  $f \xrightarrow{F} r$  or  $r = f_F$ . A reduction  $r$  of  $f$  modulo  $F$  is the result of the *Multivariable Division Algorithm*, see for example [1, I.5].

Assume that  $I$  is an ideal in  $K[x_1, \dots, x_m]$  and  $\preccurlyeq$  is an admissible relation on  $\mathbb{N}^m$ . A set  $G = \{g_1, \dots, g_t\} \subseteq I$  is a *Gröbner basis* of  $I$  (with respect to  $\preccurlyeq$ ) if and only if, for any  $f \in I$ , there is  $i = 1, \dots, t$  such that  $\text{lm}(g_i)$  divides  $\text{lm}(f)$ .

For the rest of the section  $\preccurlyeq$  denotes a fixed admissible relation on  $\mathbb{N}^m$ . The following theorem is a basic result in the theory of Gröbner bases.

**Theorem 2.1.** *Assume that  $I$  is a non-zero ideal in  $K[x_1, \dots, x_m]$  and  $G = \{g_1, \dots, g_t\}$ ,  $G \subseteq I$ , is a set of non-zero polynomials. The following conditions are equivalent.*

- (1) *The set  $G$  is a Gröbner basis of  $I$ .*
- (2)  *$f \in I$  if and only if  $f \xrightarrow{G} 0$ .*
- (3)  *$f \in I$  if and only if there are polynomials  $h_1, \dots, h_t$  such that  $f = \sum_{i=1}^t h_i g_i$  and  $\text{lm}(f) = \max\{\text{lm}(h_1 g_1), \dots, \text{lm}(h_t g_t)\}$ .*
- (4)  *$\langle \text{LM}(G) \rangle = \langle \text{LM}(I) \rangle$ .*

**Proof.** See the proof of [1, Theorem 1.6.2].  $\square$

The above theorem yields that if  $G$  is a Gröbner basis of  $I$ , then  $\langle G \rangle = I$ . Hence we say that a finite set of polynomials  $G$  is a *Gröbner basis* if and only if  $G$  is a Gröbner basis of  $\langle G \rangle$ . Theorem 2.1 also implies that any non-zero ideal in  $K[x_1, \dots, x_m]$  has a Gröbner basis.

The definition of Gröbner basis was introduced by B. Buchberger in [4]. Now we present a fundamental method for constructing a Gröbner basis of a given ideal, known as the *Buchberger's algorithm*, which is also given in [4]. We start with the following crucial notion of  $S$ -polynomial.

Assume that  $f, g \in K[x_1, \dots, x_m]$ ,  $f, g \neq 0$  and  $\underline{x}^\alpha$  is the greatest common multiple of  $\text{lm}(f)$  and  $\text{lm}(g)$ . Then the polynomial

$$S(f, g) = \frac{\underline{x}^\alpha}{\text{lt}(f)}f - \frac{\underline{x}^\alpha}{\text{lt}(g)}g$$

is the  $S$ -polynomial of  $f$  and  $g$ . If  $B = \{b_1, \dots, b_s\}$  is a finite set of polynomials in  $K[x_1, \dots, x_m]$ , then we define  $S_B$  to be the set of all non-trivial reductions of  $S$ -polynomials of  $b_i$  and  $b_j$  modulo  $B$ , that is,

$$S_B = \{S(b_i, b_j)_B; b_i, b_j \in B\} \setminus \{0\}.$$

The following fact from [4] (see also [5]) sets the ground for the succeeding Buchberger's algorithm.

**Theorem 2.2.** *Assume that  $G = \{g_1, \dots, g_t\}$  is a set of non-zero polynomials in  $K[x_1, \dots, x_m]$ . Then  $G$  is a Gröbner basis if and only if  $S(g_i, g_j) \xrightarrow{G} 0$  for any  $i, j$ .*

**Proof.** See the proof of [1, Theorem 1.7.4].  $\square$

**Algorithm (B. Buchberger).** Input: a set  $F = \{f_1, \dots, f_s\} \subseteq K[x_1, \dots, x_n]$  of non-zero polynomials. Output: a set  $G = \{g_1, \dots, g_t\} \subseteq K[x_1, \dots, x_n]$  such that  $F \subseteq G$  and  $G$  is a Gröbner basis of  $\langle F \rangle$ .

- (1) Set  $B_0 := F$  and  $i := 0$ .
- (2) Put  $B_{i+1} := B_i \cup S_{B_i}$ . If  $B_{i+1} \neq B_i$ , then put  $i := i + 1$  and return to (2). Otherwise put  $G := B_i$  and finish.

Theorem 2.2 yields that the Buchberger's algorithm is correct. Note that this algorithm halts, because  $\langle \text{LT}(B_i) \rangle \subsetneq \langle \text{LT}(B_{i+1}) \rangle$  for any  $i \geq 0$  and, in a noetherian ring, any ascending chain of ideals is finite.

### 3 Antichains in $\mathbb{N}^m$

A sequence  $\alpha_1, \dots, \alpha_t \in \mathbb{N}^m$  is an *antichain* if and only if  $\alpha_i \not\leq \alpha_j$  for any  $i < j$ . Denote by  $\mathbb{F}$  the set of all non-decreasing functions  $\mathbb{N}_1 \rightarrow \mathbb{N}_1$  and let  $f \in \mathbb{F}$ . We say that an antichain  $\alpha_1, \dots, \alpha_t \in \mathbb{N}^m$  is *f-bounded* if and only if  $|\alpha_i| \leq f(i)$  for any  $i = 1, \dots, t$ .

In this section we give a bound on the length of *f*-bounded antichains in  $\mathbb{N}^m$  depending on  $m \in \mathbb{N}_1$  and  $f \in \mathbb{F}$ . Let us start with some notation and terminology.

We write  $f \leq f'$  if and only if  $f(n) \leq f'(n)$  for any  $n \in \mathbb{N}_1$  and  $f, f' \in \mathbb{F}$ . Assume that  $m \geq 1$  is a natural number. We say that a function  $\mathcal{B}_m : \mathbb{F} \rightarrow \mathbb{N}$  has the *bounding property for m* if and only if the following conditions are satisfied:

- (1)  $t \leq \mathcal{B}_m(f)$  for any  $f \in \mathbb{F}$  and *f*-bounded antichain  $\alpha_1, \dots, \alpha_t \in \mathbb{N}^m$  of length  $t$ ,
- (2)  $\mathcal{B}_m(f) \leq \mathcal{B}_m(f')$  for any  $f, f' \in \mathbb{F}$  such that  $f \leq f'$ .

We say that a function  $\mathcal{B} : \mathbb{N}_1 \times \mathbb{F} \rightarrow \mathbb{N}$  has the *bounding property* if and only if, for any  $m \in \mathbb{N}_1$ , the function  $\mathcal{B}_m : \mathbb{F} \rightarrow \mathbb{N}$  defined by  $\mathcal{B}_m(f) = \mathcal{B}(m, f)$ , for any  $f \in \mathbb{F}$ , has the bounding property for  $m$ .

This section is devoted to construct a function with the bounding property in the above sense. As an equivalent, we construct a sequence  $(\mathcal{B}_m)_{m \in \mathbb{N}_1}$  of functions such that  $\mathcal{B}_m$  has the bounding property for  $m$ . Our construction is inductive with respect to the number  $m$ .

The existence of a function with the bounding property is rather straightforward consequence of the Compactness Theorem of first order logic, see [8] and [3, Proposition 3.25] for more details. However, this approach does not provide the explicit form of a function with the bounding property.

In the following proposition we construct a function  $\mathcal{B}_1 : \mathbb{F} \rightarrow \mathbb{N}$  with the bounding property for  $m = 1$ . This is the first step of our induction.

**Proposition 3.1.** *The function  $\mathcal{B}_1 : \mathbb{F} \rightarrow \mathbb{N}$  such that  $\mathcal{B}_1(f) = f(1) + 1$ , for any  $f \in \mathbb{F}$ , has the bounding property for  $m = 1$ .*

**Proof.** Assume that  $f \in \mathbb{F}$  and  $\alpha_1, \dots, \alpha_t \in \mathbb{N}$  is an *f*-bounded antichain. Then  $f(1) \geq \alpha_1 > \alpha_2 > \dots > \alpha_t$  and so  $t \leq f(1) + 1 = \mathcal{B}_1(f)$ . Moreover, if  $f, g \in \mathbb{N}_1$  and  $f \leq g$ , then  $\mathcal{B}_1(f) = f(1) + 1 \leq g(1) + 1 = \mathcal{B}_1(g)$ . This yields  $\mathcal{B}_1 : \mathbb{F} \rightarrow \mathbb{N}$  has the bounding property for  $m = 1$ .  $\square$

Before the second step of the induction, we introduce the following terminology which generalizes, in some sense, the one given before.

Assume that  $m \geq 1$ ,  $\alpha_1 = (a_{11}, a_{12}, \dots, a_{1m}), \dots, \alpha_t = (a_{t1}, a_{t2}, \dots, a_{tm}) \in \mathbb{N}^m$  is an antichain,  $\beta = (b_1, \dots, b_k) \in \mathbb{N}^k$ , for some  $k \in \{1, \dots, m\}$  (we treat  $\beta$  as the sequence  $b_1, \dots, b_k$ ), and  $f \in \mathbb{F}$ . We say that the chain  $\alpha_1, \dots, \alpha_t$  is *(f,  $\beta$ )-bounded* (or

$(f, b_1, \dots, b_k)$ -bounded) if and only if it is  $f$ -bounded and

$$\begin{aligned} a_{11}, a_{21}, \dots, a_{t1} &\leq b_1, \\ a_{12}, a_{22}, \dots, a_{t2} &\leq b_2, \\ &\vdots \\ a_{1k}, a_{2k}, \dots, a_{tk} &\leq b_k. \end{aligned}$$

We say that a function  $\mathcal{B}_m^k : \mathbb{F} \times \mathbb{N}^k \rightarrow \mathbb{N}$  has the  $k$ -bounding property for  $m$  if and only if the following conditions are satisfied:

- (1)  $t \leq \mathcal{B}_m^k(f, \beta)$  for any  $f \in \mathbb{F}$ ,  $\beta \in \mathbb{N}^k$  and  $(f, \beta)$ -bounded antichain  $\alpha_1, \dots, \alpha_t \in \mathbb{N}^m$  of length  $t$ ,
- (2)  $\mathcal{B}_m^k(f, \beta) \leq \mathcal{B}_m^k(f', \beta')$  for any  $f, f' \in \mathbb{F}$  and  $\beta, \beta' \in \mathbb{N}^k$  such that  $f \leq f'$  and  $\beta \parallel \beta'$ .

Recall that if  $\beta = (b_1, \dots, b_k)$  and  $\beta' = (b'_1, \dots, b'_k)$ , then the condition  $\beta \parallel \beta'$  means  $b_i \leq b'_i$  for any  $i = 1, \dots, k$ .

We agree that a function  $\mathcal{B}_m : \mathbb{F} \rightarrow \mathbb{N}$  with the bounding property for  $m$  has the 0-bounding property for  $m$  (and vice versa).

Assume that the function  $\mathcal{B}_{m-1} : \mathbb{F} \rightarrow \mathbb{N}$ ,  $m \geq 2$ , has the bounding property for  $m-1$ . Our aim is to construct a function  $\mathcal{B}_m : \mathbb{F} \rightarrow \mathbb{N}$  with the bounding property for  $m$ . In order to do this, we construct functions  $\mathcal{B}_m^k : \mathbb{F} \times \mathbb{N}^k \rightarrow \mathbb{N}$  having  $k$ -bounding properties for  $m$  by the backward induction with respect to  $k$ . To be more precise, we first construct the function  $\mathcal{B}_m^m : \mathbb{F} \times \mathbb{N}^m \rightarrow \mathbb{N}$  having the  $m$ -bounding property for  $m$  (this construction is general and does not depend on  $\mathcal{B}_{m-1} : \mathbb{F} \rightarrow \mathbb{N}$ , see Proposition 3.2). Then we show how to obtain  $\mathcal{B}_m^k : \mathbb{F} \times \mathbb{N}^k \rightarrow \mathbb{N}$  from  $\mathcal{B}_m^{k+1} : \mathbb{F} \times \mathbb{N}^{k+1} \rightarrow \mathbb{N}$ . This process provides a function with the 0-bounding property for  $m$ , that is, a function with the bounding property for  $m$ .

The first step of the backward induction is given in the following fact.

**Proposition 3.2.** *Assume that  $m \geq 1$ . The function  $\mathcal{B}_m^m : \mathbb{F} \times \mathbb{N}^m \rightarrow \mathbb{N}$  such that  $\mathcal{B}_m^m(f, b_1, \dots, b_m) = (b_1 + 1) \cdot \dots \cdot (b_m + 1)$  has the  $m$ -bounding property for  $m$ .*

**Proof.** Assume that  $f \in \mathbb{F}$  and  $b_1, \dots, b_m \in \mathbb{N}$ . The set of all  $m$ -tuples  $(a_1, \dots, a_m)$  of natural numbers such that  $a_i \leq b_i$ , for  $i = 1, \dots, m$ , has  $(b_1 + 1) \cdot \dots \cdot (b_m + 1)$  elements. This shows that if  $\alpha_1, \dots, \alpha_t \in \mathbb{N}$  is an  $(f, b_1, \dots, b_m)$ -bounded antichain, then

$$t \leq (b_1 + 1) \cdot \dots \cdot (b_m + 1) = \mathcal{B}_m^m(f, b_1, \dots, b_m).$$

Moreover, if  $b_i \leq b'_i$  for  $i = 1, \dots, m$ , then  $\mathcal{B}_m^m(f, b_1, \dots, b_m) \leq \mathcal{B}_m^m(g, b'_1, \dots, b'_m)$  for any  $f, g \in \mathbb{F}$ . Hence  $\mathcal{B}_m^m : \mathbb{F} \times \mathbb{N}^m \rightarrow \mathbb{N}$  has the  $m$ -bounding property for  $m$ .  $\square$

Now we introduce some notation. If  $\alpha = (a_1, \dots, a_m) \in \mathbb{N}^m$  and  $s \in \{1, \dots, m\}$ , then we set  $\hat{\alpha}^s = (a_1, \dots, a_{s-1}, a_{s+1}, \dots, a_m) \in \mathbb{N}^{m-1}$ .

If  $f \in \mathbb{F}$  and  $s \in \mathbb{N}$ , then  ${}^s f : \mathbb{N}_1 \rightarrow \mathbb{N}_1$  is a function such that  ${}^s f(n) = f(s+n)$  for any  $n \in \mathbb{N}_1$ . Observe that  ${}^s f \in \mathbb{F}$ .

Assume that  $m \geq 2$ ,  $k \in \{0, \dots, m-1\}$  and the function  $\mathcal{B}_m^{k+1} : \mathbb{F} \times \mathbb{N}^{k+1} \rightarrow \mathbb{N}$  has the  $(k+1)$ -bounding property for  $m$ . Suppose  $f \in \mathbb{F}$ ,  $\beta \in \mathbb{N}^k$  and define recursively a function  $g : \mathbb{N}_1 \rightarrow \mathbb{N}_1$  in the following way:

- (1)  $g(1) = 1$ ,
- (2)  $g(n+1) = 1 + g(n) + \mathcal{B}_m^{k+1}(g(n)f, \beta, f(g(n)))$  for any  $n \geq 1$ .

Obviously  $g \in \mathbb{F}$  and hence we get a function  $\mathcal{F}_m^k : \mathbb{F} \times \mathbb{N}^k \rightarrow \mathbb{F}$  such that  $(f, \beta) \mapsto g$ . We use this function in the following lemma which is the key ingredient of the second step of the backward induction.

**Lemma 3.3.** *Assume that  $m \geq 2$ ,  $k \in \{0, \dots, m-1\}$  and  $\mathcal{B}_m^{k+1} : \mathbb{F} \times \mathbb{N}^{k+1} \rightarrow \mathbb{N}$  has the  $(k+1)$ -bounding property for  $m$ . Assume that  $f \in \mathbb{F}$ ,  $\beta \in \mathbb{N}^k$  and  $\alpha_1, \dots, \alpha_t$  is an  $(f, \beta)$ -bounded antichain in  $\mathbb{N}^m$  of length  $t$ .*

- (1) *Assume that  $\alpha_{s_1}, \dots, \alpha_{s_r}$  is a subsequence of  $\alpha_1, \dots, \alpha_t$  such that the sequence  $\hat{\alpha}_{s_1}^{k+1}, \dots, \hat{\alpha}_{s_r}^{k+1} \in \mathbb{N}^{m-1}$  is an antichain. Set  $\mu = s_r + \mathcal{B}_m^{k+1}(s_r f, \beta, f(s_r))$ . If we have  $\mu + 1 \leq t$ , then there is a natural number  $c \in \{s_r + 1, \dots, \mu + 1\}$  such that the sequence  $\hat{\alpha}_{s_1}^{k+1}, \dots, \hat{\alpha}_{s_r}^{k+1}, \hat{\alpha}_c^{k+1}$  is an antichain in  $\mathbb{N}^{m-1}$ .*
- (2) *Set  $g = \mathcal{F}_m^k(f, \beta)$ , fix a natural number  $n \geq 1$  and suppose that  $g(n) \leq t$ . Then there is a subsequence  $\alpha_{p_1}, \dots, \alpha_{p_n}$  of length  $n$  of the sequence  $\alpha_1, \dots, \alpha_t$  such that the sequence  $\hat{\alpha}_{p_1}^{k+1}, \dots, \hat{\alpha}_{p_n}^{k+1}$  is an  $(f \circ g)$ -bounded antichain in  $\mathbb{N}^{m-1}$ .*

**Proof.** (1) Set  $\alpha_1 = (a_{11}, a_{12}, \dots, a_{1m}), \dots, \alpha_t = (a_{t1}, a_{t2}, \dots, a_{tm})$  and assume  $\mu + 1 \leq t$ ,  $d \geq s_r + 1$ . Suppose that, for any  $n \in \{s_r + 1, \dots, d\}$ , the sequence  $\hat{\alpha}_{s_1}^{k+1}, \dots, \hat{\alpha}_{s_r}^{k+1}, \hat{\alpha}_n^{k+1}$  is not an antichain in  $\mathbb{N}^{m-1}$ . We show that  $d \leq \mu$ . Indeed, for a fixed  $n$  we have  $\hat{\alpha}_{s_i}^{k+1} \parallel \hat{\alpha}_n^{k+1}$  for some  $i$ , because  $\hat{\alpha}_{s_1}^{k+1}, \dots, \hat{\alpha}_{s_r}^{k+1}$  is an antichain in  $\mathbb{N}^{m-1}$ . Note that  $\alpha_{s_1}, \dots, \alpha_{s_r}, \alpha_n$  is an antichain in  $\mathbb{N}^m$ , so  $\alpha_{s_i} \not\parallel \alpha_n$ . Hence we get  $a_{s_i(k+1)} > a_{n(k+1)}$  and  $f(s_r) \geq f(s_i) \geq a_{s_i(k+1)} > a_{n(k+1)}$ .

Consequently,  $a_{n(k+1)} \leq f(s_r)$  for any  $n \in \{s_r + 1, \dots, d\}$  and thus the sequence  $\alpha_{s_r+1}, \alpha_{s_r+2}, \dots, \alpha_d \in \mathbb{N}^m$  is  $(s_r f, \beta, f(s_r))$ -bounded. This implies that  $d - s_r \leq \mathcal{B}_m^{k+1}(s_r f, \beta, f(s_r))$ , so  $d \leq \mu$  and (1) follows.

(2) We use induction with respect to  $n$ . Assume that  $n = 1$  and set  $p_1 = 1$ . Then  $\hat{\alpha}_1^{k+1}$  is an  $(f \circ g)$ -bounded antichain in  $\mathbb{N}^{m-1}$ , because  $|\hat{\alpha}_1^{k+1}| \leq f(1) = f(g(1))$ .



Assume that the thesis holds for some  $n \geq 1$ . Moreover, assume a technical condition  $p_1 \leq g(1), \dots, p_n \leq g(n)$ . We show that the thesis holds for  $n+1$  and  $p_1 \leq g(1), \dots, p_{n+1} \leq g(n+1)$ . Indeed, if  $g(n+1) \leq t$ , then  $g(n) \leq t$  and hence there is an antichain in  $\mathbb{N}^{m-1}$  of the form  $\hat{\alpha}_{p_1}^{k+1}, \dots, \hat{\alpha}_{p_n}^{k+1}$ . Observe that

$$g(n+1) = 1 + g(n) + \mathcal{B}_m^{k+1}(g(n)f, \beta, f(g(n))) \leq t$$

and thus, applying (1) for  $s_r = g(n)$ , we get  $c \in \{g(n) + 1, \dots, g(n+1)\}$  such that the sequence  $\hat{\alpha}_{p_1}^{k+1}, \dots, \hat{\alpha}_{p_n}^{k+1}, \hat{\alpha}_c^{k+1}$  is an antichain in  $\mathbb{N}^{m-1}$ . Set  $p(n+1) = c$ . Since  $p_{n+1} \leq g(n+1)$ , we get  $|\hat{\alpha}_{p_{n+1}}^{k+1}| \leq f(p_{n+1}) \leq f(g(n+1))$  and thus this antichain is  $(f \circ g)$ -bounded. This finishes the proof.  $\square$

Given the above lemma we are able to prove the second step of the backward induction with respect to  $k$  and hence the second step of the main induction (with respect to  $m$ ).

**Corollary 3.4.** *Assume  $m \geq 2$ ,  $k \in \{0, \dots, m-1\}$ ,  $\mathcal{B}_m^{k+1} : \mathbb{F} \times \mathbb{N}^{k+1} \rightarrow \mathbb{N}$  has the  $(k+1)$ -bounding property for  $m$  and  $\mathcal{B}_{m-1} : \mathbb{F} \rightarrow \mathbb{N}$  has the bounding property for  $m-1$ .*

(1) *The function  $\mathcal{B}_m^k : \mathbb{F} \times \mathbb{N}^k \rightarrow \mathbb{N}$  such that*

$$\mathcal{B}_m^k(f, \beta) = g(\mathcal{B}_{m-1}(f \circ g) + 1),$$

*for any  $f \in \mathbb{F}$ ,  $\beta \in \mathbb{N}^k$  and  $g = \mathcal{F}_m^k(f, \beta)$ , has the  $k$ -bounding property for  $m$ .*

(2) *The function  $\mathcal{B}_m^0 : \mathbb{F} \rightarrow \mathbb{N}$  has the bounding property for  $m$ .*

**Proof.** (1) Assume that the antichain  $\alpha_1, \dots, \alpha_t \in \mathbb{N}^m$  of length  $t$  is  $(f, \beta)$ -bounded. If  $g(\mathcal{B}_{m-1}(f \circ g) + 1) \leq t$ , then Lemma 3.3 (2) implies there is an  $(f \circ g)$ -bounded antichain in  $\mathbb{N}^{m-1}$  of length  $\mathcal{B}_{m-1}(f \circ g) + 1$ , a contradiction. Hence  $t < g(\mathcal{B}_{m-1}(f \circ g) + 1)$  and it is enough to prove that  $\mathcal{B}_m^k(f, \beta) \leq \mathcal{B}_m^k(f', \beta')$  for any  $f, f' \in \mathbb{F}$  and  $\beta, \beta' \in \mathbb{N}^k$  such that  $f \leq f'$  and  $\beta || \beta'$ . Set  $g = \mathcal{F}_m^k(f, \beta)$  and  $g' = \mathcal{F}_m^k(f', \beta')$ . It follows easily from the construction of  $g, g'$  that  $g \leq g'$ . Thus  $f \circ g \leq f' \circ g'$ ,  $\mathcal{B}_{m-1}(f \circ g) \leq \mathcal{B}_{m-1}(f' \circ g')$  and finally  $g(\mathcal{B}_{m-1}(f \circ g) + 1) \leq g(\mathcal{B}_{m-1}(f' \circ g') + 1)$ .

(2) Proposition 3.2 shows that the function  $\mathcal{B}_m^m : \mathbb{F} \times \mathbb{N}^m \rightarrow \mathbb{N}$  given by the formula  $\mathcal{B}_m^m(f, b_1, \dots, b_m) = (b_1 + 1) \cdot \dots \cdot (b_m + 1)$  has the  $m$ -bounding property for  $m$ . Then (1) yields a construction of the function  $\mathcal{B}_m^k : \mathbb{F} \times \mathbb{N}^k \rightarrow \mathbb{N}$  having the  $k$ -bounding property for  $m$  given  $\mathcal{B}_{m-1} : \mathbb{F} \rightarrow \mathbb{N}$  (with the bounding property for  $m-1$ ) and  $\mathcal{B}_m^{k+1} : \mathbb{F} \times \mathbb{N}^{k+1} \rightarrow \mathbb{N}$  (with the  $(k+1)$ -bounding property for  $m$ ), for any  $k \in \{0, \dots, m-1\}$ . This shows that the function  $\mathcal{B}_m^0 : \mathbb{F} \rightarrow \mathbb{N}$  has the bounding property for  $m$ .  $\square$

Recall that Proposition 3.1 is the first step of the induction with respect to  $m$ .



The second step of this induction is given in Corollary 3.4 (2). Hence we get the following main result of the section.

**Theorem 3.5.** *The function  $\mathcal{B} : \mathbb{N}_1 \times \mathbb{F} \rightarrow \mathbb{N}$  defined recursively in the following way:*

- (1)  $\mathcal{B}(1, f) = \mathcal{B}_1(f)$  for any  $f \in \mathbb{F}$ ,
- (2)  $\mathcal{B}(m, f) = \mathcal{B}_m^0(f)$  for any  $m \geq 2$  and  $f \in \mathbb{F}$

*has the bounding property.*

**Proof.** It follows from Proposition 3.1 that the function  $\mathcal{B}_1 : \mathbb{F} \rightarrow \mathbb{N}$  such that  $\mathcal{B}_1(f) = f(1) + 1$  has the bounding property for  $m = 1$ . It follows from Corollary 3.4 (2) that the function  $\mathcal{B}_m^0 : \mathbb{F} \rightarrow \mathbb{N}$  has the bounding property for  $m$ , for any  $m \geq 2$ . This shows that the construction given in the thesis is correct.  $\square$

## 4 The main results

In this section we prove the main results of the paper. Throughout we assume that our admissible ordering  $\preccurlyeq$  is graded, e.g.  $\preccurlyeq$  is the degree lexicographical order.

Assume  $m \geq 1$  and  $f : \mathbb{N}_1 \rightarrow \mathbb{N}_1$  is a function (we do not assume here that  $f \in \mathbb{F}$ ). An ascending chain  $I_1 \subsetneq \dots \subsetneq I_t$  of ideals in  $K[x_1, \dots, x_m]$  is *f-bounded* if and only if  $I_j$  is generated by polynomials of degrees less or equal to  $f(j)$ , for any  $j = 1, \dots, t$ .

Our first goal is to give a bound on the length of *f*-bounded ascending chains of ideals in  $K[x_1, \dots, x_m]$  depending on  $m$  and  $f$ . The following proposition shows that this problem reduces to the situation studied in Section 3.

**Proposition 4.1.** *Assume that  $m \geq 1$ ,  $f : \mathbb{N}_1 \rightarrow \mathbb{N}_1$  is a function and  $I_1 \subsetneq \dots \subsetneq I_t$  is an *f*-bounded ascending chain of ideals in  $K[x_1, \dots, x_m]$ . Then there exist monomials  $\underline{x}^{\alpha_1}, \dots, \underline{x}^{\alpha_t} \in \mathbb{T}_m$  such that  $\deg(\underline{x}^{\alpha_i}) \leq f(i)$  for  $i = 1, \dots, t$  and  $\underline{x}^{\alpha_{i+1}} \notin \langle \underline{x}^{\alpha_1}, \dots, \underline{x}^{\alpha_i} \rangle$  for  $i = 1, \dots, t-1$ . If  $f : \mathbb{N}_1 \rightarrow \mathbb{N}_1$  is non-decreasing, this condition is equivalent to the fact that the sequence  $\alpha_1, \dots, \alpha_t$  is an *f*-bounded antichain.*

**Proof.** Assume that  $I_j = \langle h_{j1}, h_{j2}, \dots, h_{js_j} \rangle$  and  $\deg(h_{ji}) \leq f(j)$  for any  $j = 1, \dots, t$  and  $i = 1, \dots, s_j$ . It is easy to see that there are polynomials  $h_1, \dots, h_t$  such that  $h_j \in \{h_{j1}, h_{j2}, \dots, h_{js_j}\}$  and  $h_j \notin \langle h_1, h_2, \dots, h_{j-1} \rangle$ . Thus we get an ascending chain of ideals of the form

$$\langle h_1 \rangle \subsetneq \langle h_1, h_2 \rangle \subsetneq \dots \subsetneq \langle h_1, h_2, \dots, h_t \rangle$$

of length  $t$  with the property that  $h_{j+1} \notin \langle h_1, h_2, \dots, h_j \rangle$  and  $\deg(h_j) \leq f(j)$  for any  $j$ . We set  $H_1 = \{h_1\}$ ,  $H_2 = \{h_1, (h_2)_{H_1}\}$ ,  $H_3 = \{h_1, (h_2)_{H_1}, (h_3)_{H_2}\}$  and so on. We show that  $\langle H_t \rangle = \langle h_1, h_2, \dots, h_t \rangle$  and the sequence

$$\text{lm}(h_1), \text{lm}((h_2)_{H_1}), \dots, \text{lm}((h_t)_{H_{t-1}})$$

of monomials satisfies the required condition. Indeed, since the admissible ordering  $\preccurlyeq$  is graded, we get  $\deg(\text{lm}(h_1)) = \deg(h_1) \leq f(1)$  and thus the assertion holds for  $t = 1$ . Assume that the assertion holds for some  $t \geq 1$  and there is an ascending chain of ideals

$$\langle h_1 \rangle \subsetneq \langle h_1, h_2 \rangle \subsetneq \dots \subsetneq \langle h_1, h_2, \dots, h_t \rangle \subsetneq \langle h_1, h_2, \dots, h_t, h_{t+1} \rangle$$

of length  $t + 1$  such that  $h_{j+1} \notin \langle h_1, h_2, \dots, h_j \rangle$  and  $\deg(h_j) \leq f(j)$  for any  $j$ . There are polynomials  $a_1, \dots, a_t$  such that

$$h_{t+1} = a_1 h_1 + a_2 (h_2)_{H_1} + \dots + a_t (h_t)_{H_{t-1}} + (h_{t+1})_{H_t}$$

and  $\text{lm}(h_{t+1}) = \max\{\text{lm}(a_1 h_1), \text{lm}(a_2 (h_2)_{H_1}), \dots, \text{lm}(a_t (h_t)_{H_{t-1}}), \text{lm}((h_{t+1})_{H_t})\}$ . This yields  $h_{t+1} \in \langle H_{t+1} \rangle$  and since  $\langle h_1, h_2, \dots, h_t \rangle = \langle H_t \rangle \subseteq \langle H_{t+1} \rangle$ , we get that  $\langle h_1, h_2, \dots, h_t, h_{t+1} \rangle \subseteq H_{t+1}$ . Moreover,  $h_1, (h_2)_{H_1}, \dots, (h_{t+1})_{H_t} \in \langle h_1, h_2, \dots, h_t, h_{t+1} \rangle$  and so  $\langle H_{t+1} \rangle = \langle h_1, h_2, \dots, h_t, h_{t+1} \rangle$ . Observe that  $(h_{t+1})_{H_t} \neq 0$ , because otherwise  $h_{t+1} \in \langle H_t \rangle = \langle h_1, \dots, h_t \rangle$ , a contradiction. Since  $\text{lm}((h_{t+1})_{H_t}) \preccurlyeq \text{lm}(h_{t+1})$  and the ordering  $\preccurlyeq$  is graded, we get  $\deg(\text{lm}(h_{t+1})_{H_t}) \leq \deg(\text{lm}(h_{t+1})) \leq f(t + 1)$ . Finally, the elements of  $\text{LM}(H_t)$  do not divide  $\text{lm}((h_{t+1})_{H_t})$ , because  $(h_{t+1})_{H_t}$  is reduced modulo  $H_t$ . This implies  $\text{lm}((h_{t+1})_{H_t}) \notin \langle \text{LM}(H_t) \rangle$  which finishes the induction.

To prove the second assertion, assume that  $\alpha_i = (a_{i1}, a_{i2}, \dots, a_{im}) \in \mathbb{N}^m$  for  $i = 1, \dots, t$ . Then  $\alpha_1, \dots, \alpha_t$  is an antichain if and only if for any  $i < j$  there is  $k$  such that  $a_{ik} > a_{jk}$ . This implies that the sequence  $\underline{x}^{\alpha_1}, \dots, \underline{x}^{\alpha_t}$  of monomials in  $K[x_1, \dots, x_m]$  satisfies the conditions  $\underline{x}^{\alpha_{i+1}} \notin \langle \underline{x}^{\alpha_1}, \dots, \underline{x}^{\alpha_i} \rangle$  (for  $i = 1, \dots, t - 1$ ) and  $\deg(\underline{x}^{\alpha_i}) \leq f(i)$  (for  $i = 1, \dots, t$ ) if and only if the sequence  $\alpha_1, \dots, \alpha_t$  is an  $f$ -bounded antichain.  $\square$

The above proposition shows that one can associate an  $f$ -bounded antichain of length  $t$  to an  $f$ -bounded ascending chain of ideals of the same length  $t$  (if  $f$  is non-decreasing). Therefore we get the following theorem on the length of ascending chains of ideals as a direct consequence of Theorem 3.5 and Proposition 4.1.

**Theorem 4.2.** *Assume that  $m \geq 1$  and  $f : \mathbb{N}_1 \rightarrow \mathbb{N}_1$  is a function. Suppose that  $I_1 \subsetneq \dots \subsetneq I_t$  is an  $f$ -bounded ascending chain of ideals in  $K[x_1, \dots, x_m]$  of length  $t$ . Let  $g : \mathbb{N}_1 \rightarrow \mathbb{N}_1$  be a non-decreasing function such that  $g(n)$  is the greatest number of the set  $\{f(1), f(2), \dots, f(n)\}$ , for any  $n \in \mathbb{N}$ . Then  $t \leq \mathcal{B}(m, g)$ . In particular, we have  $t \leq \mathcal{B}(m, f)$ , if  $f$  is non-decreasing.*

**Proof.** The chain  $I_1 \subsetneq \dots \subsetneq I_t$  is  $g$ -bounded, so the assertion follows from Theorem 3.5 and Proposition 4.1. Note that if  $f$  is non-decreasing, then  $f = g$ .  $\square$

Now we deduce some consequences of Theorem 4.2 (and hence of Theorem 3.5) in the context of Gröbner bases. We start with the following preparatory fact.

**Proposition 4.3.** *Assume that  $F = \{f_1, \dots, f_s\} \subseteq K[x_1, \dots, x_m]$  is a set of non-zero polynomials and  $d \geq 1$  is a natural number such that  $\deg(f_i) \leq d$  for  $i = 1, \dots, s$ . Let*

$$\langle \text{LT}(B_0) \rangle \subsetneq \langle \text{LT}(B_1) \rangle \subsetneq \dots$$

*be the associated ascending chain of monomial ideals arising from the Buchberger's algorithm. Assume that  $n \geq 0$  and  $b \in B_n$ .*

- (1) *There exist polynomials  $a_1, \dots, a_s \in K[x_1, \dots, x_m]$  such that  $b = a_1 f_1 + \dots + a_s f_s$  and  $\deg(a_1), \dots, \deg(a_s) \leq (3^n - 1)d$ .*
- (2) *We have  $\deg(\text{lt}(b)) \leq 3^n d$ .*

**Proof.** Set  $\chi(n) = (3^n - 1)d$  for any  $n \in \mathbb{N}$ . Observe that (1) implies (2). Indeed, if  $b = a_1 f_1 + \dots + a_s f_s$  for some  $a_1, \dots, a_s$  such that  $\deg(a_1), \dots, \deg(a_s) \leq \chi(n)$ , then  $\deg(a_1 f_1), \dots, \deg(a_s f_s) \leq \chi(n) + d = 3^n d$ . This implies  $\deg(\text{lt}(b)) \leq 3^n d$ , because the ordering  $\preccurlyeq$  is graded.

Thus it is enough to show (1). We use induction with respect to  $n$ . In the case  $n = 0$ , we have  $B_0 = F$  and  $\chi(0) = 0$ , so the assertion holds. Assume that the assertion holds for some  $n \geq 0$ , that is, set  $B_n = \{b_1, \dots, b_r\}$  and  $b_i = a_{i1} f_1 + \dots + a_{is} f_s$  for some  $a_{i1}, \dots, a_{is} \in K[x_1, \dots, x_m]$  such that  $\deg(a_{i1}), \dots, \deg(a_{is}) \leq \chi(n)$ , for any  $i = 1, \dots, r$ . We show that the assertion holds for  $n + 1$ .

Assume that  $b_i, b_j \in B_n$  and  $b_i \neq b_j$ . Recall that  $B_{n+1} = B_n \cup S_{B_n}$  and thus it is enough to show the assertion for  $S(b_i, b_j)_{B_n}$ . Observe that

$$\begin{aligned} S(b_i, b_j) &= \frac{\underline{x}^\alpha}{\text{lt}(b_i)} b_i - \frac{\underline{x}^\alpha}{\text{lt}(b_j)} b_j = \\ &= \left( \frac{\underline{x}^\alpha}{\text{lt}(b_i)} a_{i1} - \frac{\underline{x}^\alpha}{\text{lt}(b_j)} a_{j1} \right) f_1 + \dots + \left( \frac{\underline{x}^\alpha}{\text{lt}(b_i)} a_{is} - \frac{\underline{x}^\alpha}{\text{lt}(b_j)} a_{js} \right) f_s \end{aligned}$$

where  $\underline{x}^\alpha$  denotes the greatest common multiple of  $\text{lm}(b_i)$  and  $\text{lm}(b_j)$ . Since (1) implies (2), we get

$$\deg\left(\frac{\underline{x}^\alpha}{\text{lt}(b)}\right) \leq \deg(\text{lt}(b')) \leq \chi(n) + d$$

where  $b = b_i$ ,  $b' = b_j$  or vice versa. This yields

$$(*) \quad \deg\left(\frac{\underline{x}^\alpha}{\text{lt}(b_i)} a_{ik} - \frac{\underline{x}^\alpha}{\text{lt}(b_j)} a_{jk}\right) \leq 2\chi(n) + d,$$

for any  $k = 1, \dots, s$ , and consequently  $\deg(S(b_i, b_j)) \leq 2\chi(n) + 2d$ . Moreover, there are polynomials  $c_1, \dots, c_r$  such that

$$\begin{aligned} S(b_i, b_j)_{B_n} &= S(b_i, b_j) - c_1 b_1 - \dots - c_r b_r = \\ &= S(b_i, b_j) - c_1(a_{11}f_1 + \dots + a_{1s}f_s) - \dots - c_r(a_{r1}f_1 + \dots + a_{rs}f_s) \end{aligned}$$

and  $\text{lm}(c_t b_t) \preccurlyeq \text{lm}(S(b_i, b_j))$  for any  $t = 1, \dots, r$ . Because  $\preccurlyeq$  is graded, we get

$$\deg(c_t) \leq \deg(c_t b_t) \leq \deg(S(b_i, b_j)) \leq 2\chi(n) + 2d$$

and thus  $(**)$   $\deg(c_t a_{tk}) \leq 3\chi(n) + 2d$  for any  $t = 1, \dots, r$  and  $k = 1, \dots, s$ .

It follows by  $(*)$  and  $(**)$  that the polynomial  $S(b_i, b_j)_{B_n}$  can be written in the form  $a'_1 f_1 + \dots + a'_s f_s$  where  $\deg(a'_i) \leq 3\chi(n) + 2d$ . Since  $3\chi(n) + 2d = \chi(n+1)$ , this shows the assertion for  $n+1$ .  $\square$

By a string  $3^nd$  we mean the function  $f : \mathbb{N}_1 \rightarrow \mathbb{N}_1$  such that  $f(n) = 3^nd$  ( $d \geq 1$  is a fixed natural number).

**Corollary 4.4.** *Assume that  $F = \{f_1, \dots, f_s\} \subseteq K[x_1, \dots, x_m]$  is a set of non-zero polynomials and  $d$  is a natural number such that  $\deg(f_i) \leq d$  for  $i = 1, \dots, s$ . Let*

$$\langle \text{LT}(B_0) \rangle \subsetneq \langle \text{LT}(B_1) \rangle \subsetneq \dots \subsetneq \langle \text{LT}(B_r) \rangle$$

*be the associated ascending chain of monomial ideals arising from the Buchberger's algorithm such that  $B_r$  is the Gröbner basis of  $\langle F \rangle$ . Then  $r+1 \leq \mathcal{B}(m, 3^nd)$ .*

**Proof.** It follows from Proposition 4.3 (2) that the ascending chain  $\langle \text{LT}(B_0) \rangle \subsetneq \langle \text{LT}(B_1) \rangle \subsetneq \dots \subsetneq \langle \text{LT}(B_r) \rangle$  is  $3^nd$ -bounded. Hence Theorem 4.2 yields the condition  $r+1 \leq \mathcal{B}(m, 3^nd)$ .  $\square$

Set  $m \geq 1$ ,  $d \geq 1$  and define the function  $\gamma_{m,d} : \mathbb{N} \rightarrow \mathbb{N}$  in the following way

$$\gamma_{m,d}(i) = (3^{\mathcal{B}(m, 3^nd)-1} - 1)d + i$$

for any  $i \in \mathbb{N}$ . The function  $\gamma_{m,d}$  has the following property.

**Corollary 4.5.** *Assume that  $m \geq 1$  and  $d \geq 1$ . Then for any  $g \in K[x_1, \dots, x_m]$  and  $f_1, \dots, f_s \in K[x_1, \dots, x_m]$  such that  $\deg(f_i) \leq d$  for  $i = 1, \dots, s$  the following condition is satisfied:  $g \in \langle f_1, \dots, f_s \rangle$  if and only if there exist  $h_1, \dots, h_s \in K[x_1, \dots, x_m]$  such that  $g = h_1 f_1 + \dots + h_s f_s$  and  $\deg(h_i) \leq \gamma_{m,d}(\deg(g))$  for  $i = 1, \dots, s$ .*

**Proof.** Assume that  $g, f_1, \dots, f_s \in K[x_1, \dots, x_m]$  and  $\deg(f_i) \leq d$  for  $i = 1, \dots, s$ . Set  $F = \{f_1, \dots, f_s\}$  and let  $\langle \text{LT}(B_0) \rangle \subsetneq \langle \text{LT}(B_1) \rangle \subsetneq \dots \subsetneq \langle \text{LT}(B_r) \rangle$  be the ascending chain of monomial ideals arising from the Buchberger's algorithm such that  $B_r = G = \{g_1, \dots, g_t\}$  is the Gröbner basis of  $\langle F \rangle$ .

Assume that  $g \in \langle f_1, \dots, f_s \rangle$ . Since  $G$  is a Gröbner basis of  $\langle F \rangle$ , there are polynomials  $p_1, \dots, p_t$  such that  $g = p_1 g_1 + \dots + p_t g_t$  and  $\text{lm}(g)$  is the maximal element of  $\{\text{lm}(p_1 g_1), \dots, \text{lm}(p_t g_t)\}$ . Hence  $\text{lm}(p_i g_i) \preceq \text{lm}(g)$  so  $\deg(p_i g_i) \leq \deg(g)$  and consequently  $\deg(p_i) \leq \deg(g)$ , for any  $i = 1, \dots, t$ .

Corollary 4.4 yields  $r + 1 \leq \mathcal{B}(m, 3^n d)$ . Furthermore, Proposition 4.3 (1) implies that  $g_i = a_{i1} f_1 + \dots + a_{is} f_s$  for some polynomials  $a_{i1}, \dots, a_{is}$  with

$$\deg(a_{i1}), \dots, \deg(a_{is}) \leq (3^r - 1)d \leq (3^{\mathcal{B}(m, 3^n d) - 1} - 1)d,$$

for  $i = 1, \dots, t$ . It follows that

$$\deg(p_i a_{ik}) \leq (3^{\mathcal{B}(m, 3^n d) - 1} - 1)d + \deg(g) = \gamma_{m,d}(\deg(g))$$

for  $i = 1, \dots, t$  and  $k = 1, \dots, s$ . This shows the assertion.  $\square$

Let us note that the main results of this section (Theorem 4.2 and Corollaries 4.4 and 4.5) do not depend on the choice of the base field  $K$  of the polynomial ring  $K[x_1, \dots, x_m]$ .

## 5 Remarks

Our motivation to study problems concerning ascending chains of ideals in the polynomial ring arises from the first order logic. The goal is to give a constructive proof of the renowned Tarski's theorem on quantifier elimination in the theory of algebraically closed fields. This theorem was proved by A. Tarski in 1948 in an unpublished paper, see [16] for the details.

Roughly, Tarski's theorem states that if  $\varphi(x_1, \dots, x_n)$  is a formula in the first order language of the theory of fields with  $n$  free variables  $x_1, \dots, x_n$ , then there exists a quantifier-free formula  $\varphi'(x_1, \dots, x_n)$  (a formula in which quantifiers do not occur), with the same free variables, such that  $\varphi(x_1, \dots, x_n)$  is equivalent with  $\varphi'(x_1, \dots, x_n)$ . This means that for any algebraically closed field  $K$  and any elements  $a_1, \dots, a_n \in K$  we have  $\varphi(a_1, \dots, a_n) \leftrightarrow \varphi'(a_1, \dots, a_n)$ . We refer to [11] for the necessary details.

As an example, consider the formula  $\varphi(A) = \exists B \ AB = BA = I_n$  where  $A, B$  are  $n \times n$  complex matrices and  $I_n$  is the  $n \times n$  identity matrix ( $\varphi(A)$  can be suitably written in the first order language of the theory of fields). This formula states that  $A$  is non-singular and thus  $\varphi(A)$  holds if and only if  $\det(A) \neq 0$ . The latter formula is quantifier-free and very easy to verify. Generally, this is the case for any quantifier-free formula.

Standard proofs of Tarski's theorem are existential, that is, they do not provide the form of the quantifier-free formula equivalent with the given one. A constructive proof aims to provide that form. In the subsequent paper [13] we apply Corollary 4.5 to give a constructive proof of Tarski's theorem. Moreover, we show some interesting

applications of this constructive version. For example, a formula stating the existence of a common invariant subspace of  $n \times n$  complex matrices  $A_1, \dots, A_s$  is a first order formula  $\psi$  of the theory of fields. By the constructive Tarski's theorem we are able to give a quantifier-free formula  $\psi'$  which is equivalent to  $\psi$ . The formula  $\psi'$  may be considered as an algorithm for verifying the existence of a common invariant subspace of  $A_1, \dots, A_s$ . We emphasize that until [2], published in 2004, it was not known if such an algorithm exists in the general case (for special cases see [18], [19] and [10]).

In the series of papers [9], [10], [14] and [15] we consider algorithms (called there *computable conditions*) for the existence of various common invariant subspaces of complex linear operators. We further apply these algorithms in some problems of quantum information theory. All the problems we consider can be expressed in the first order language of the theory of fields, and hence the constructive Tarski's theorem is applicable. This gives a new general context for this research and opens the possibility for other applications. Note that some impact of quantifier elimination technique on quantum information theory has been recently noticed in [20].

## Acknowledgements

This research has been supported by grant No. DEC-2011/02/A/ST1/00208 of National Science Center of Poland.

## References

- [1] W. W. Adams and P. Loustau, *An Introduction to Gröbner Bases*, American Mathematical Society, 1994.
- [2] D. Arapura, Ch. Peterson, *The common invariant subspace problem: an approach via Gröbner bases*, Linear Algebra and its Applications 384 (2004), 1–7.
- [3] M. Aschenbrenner and W.Y. Pong, *Orderings of Monomial Ideals*, Fundam. Math. 181, 2004.
- [4] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Ph.D. Thesis, Inst. University of Innsbruck, Innsbruck, Austria, 1965.
- [5] B. Buchberger, *Gröbner Bases: An algorithmic method in polynomial ideal theory*, Multidimensional Systems Theory (N.K Bose ed.), Reidel, Dordrecht, 1985, 184–232.
- [6] W. Bruns and J. Herzog, *Cohen-Macaulay Rings*, Cambridge Stud. Adv. Math. 39, Cambridge Univ. Press, Cambridge, 1993.

- [7] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Grad. Texts in Math. 150, Springer, New York, 1995.
- [8] H. Friedman, *The Ackermann function in elementary algebraic geometry*, manuscript, 1999.
- [9] A. Jamiołkowski, T. Kamizawa and G. Pastuszak, *On Invariant Subspace In Quantum Control Systems and Some Concepts of Integrable Quantum Systems*, Int. J. Theor. Phys. Volume 54, Issue 8 (2015), 2662–2674.
- [10] A. Jamiołkowski and G. Pastuszak, *Generalized Shemesh Criterion, Common Invariant Subspaces and Irreducible Completely Positive Superoperators*, Linear and Multilinear Algebra 63(2) (2015), 314–325.
- [11] D. Marker, *Model Theory: An Introduction*, Springer, Berkeley, 2002.
- [12] G. Moreno Socías, *Length of polynomial ascending chains and primitive recursiveness*, Math. Scand. 71 (1992), 181–205.
- [13] G. Pastuszak, *A constructive proof of Tarski’s theorem on quantifier elimination in ACF*, preprint.
- [14] G. Pastuszak and A. Jamiołkowski, *Common reducing unitary subspaces and decoherence in quantum systems*, Electron. J. Linear Algebra, Vol. 30 (2015) 253–270.
- [15] G. Pastuszak, T. Kamizawa and A. Jamiołkowski, *On a Criterion for Simultaneous Block-Diagonalization of Normal Matrices*, Open Syst. Inf. Dyn. 23, 1650003 (2016).
- [16] A. Robinsom, *Introduction to Model Theory and to the Metamathematics of Algebra*, Studies in Logic and the Foundations of Mathematics 66, North-Holland, Amsterdam, 1965.
- [17] A. Seidenberg, *On the length of a Hilbert ascending chain*, Proc. Amer. Math. Soc. 29 (1971), 443–450.
- [18] D. Shemesh, *Common eigenvectors of two matrices*, Linear Algebra and its Applications 62 (1984), 11–18.
- [19] M. Tsatsomeros, *A criterion for the existence of common invariant subspaces of matrices*, Linear Algebra and its Applications 322 (2001), 51–59.
- [20] M.M. Wolf, T.S. Cubitt, D. Perez-Garcia, *Are problems in Quantum Information Theory (un)decidable?*, arXiv:1111.5425v1 [quant-ph], 2011.



Grzegorz Pastuszak  
Faculty of Mathematics and Computer Science  
Nicholaus Copernicus University  
Chopina 12/18  
87-100 Toruń, Poland  
past@mat.uni.torun.pl