

LENGTH OF POLYNOMIAL ASCENDING CHAINS AND PRIMITIVE RECURSIVENESS

Author(s): GUILLERMO MORENO SOCÍAS

Source: *Mathematica Scandinavica*, Vol. 71, No. 2 (1992), pp. 181-205

Published by: Mathematica Scandinavica

Stable URL: <https://www.jstor.org/stable/24492715>

Accessed: 08-10-2021 11:00 UTC

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at <https://about.jstor.org/terms>



JSTOR

Mathematica Scandinavica is collaborating with JSTOR to digitize, preserve and extend access to *Mathematica Scandinavica*

LENGTH OF POLYNOMIAL ASCENDING CHAINS AND PRIMITIVE RECURSIVENESS

GUILLERMO MORENO SOCÍAS

Abstract.

In a polynomial ring $K[X_1, \dots, X_n]$ over a field, let

$$I_0 \subset I_1 \subset \dots \subset I_s$$

be a strictly ascending chain of ideals, with the condition that every I_i can be generated by elements of degree not greater than $f(i)$. A. Seidenberg showed that there is a bound on the length s of such a chain depending only on n and f , which is recursive in f for every n and primitive recursive in f for $n = 2$. In this paper we give a better bound, expressed in a rather simple way in terms of f , which is attained when f is an increasing function. We prove that it is primitive recursive in f for all n . We also show that, on the contrary, there is no bound which is primitive recursive in n in general.

0. Introduction.

Let $R = K[X_1, \dots, X_n]$ be a polynomial ring over a field K . By definition of noetherianity, the length of any strictly ascending chain

$$I_0 \subset I_1 \subset \dots \subset I_i \dots$$

of ideals of R is finite, but to bound it we need some information about the ideals themselves. In [Seidenberg71], A. Seidenberg studied the case where I_i can be generated in degree not greater than $f(i)$, where $f: \mathbb{N} \longrightarrow \mathbb{N}$ is a given function (i.e., one can write $I_i = (p_{i1}, \dots, p_{ir_i})$ with $\deg p_{ij} \leq f(i)$). He showed that a bound $g_n(f)$ can be found which depends only on n and f , saying that “one could explicitly write down a formula for g_n in terms of f and n ”; in fact, the derivation he gives is rather complicated, so he adds that “it would be desirable to bring to a more satisfactory expression the nature of the dependent of g_n on f ”. About recursivity, he says: “This argument gives $g_n(f)$ as general recursive in f . For $n = 2$, following our argument, one can find a $g_n(f)$ primitive recursive in f . Even for $n \geq 3$, where primitive recursiveness looks doubtful, we still think we have more than general recursiveness.”

Here we show that if one looks for it, an optimal bound can be obtained which

Received August 2, 1991.

not only is easily expressible in terms of f and n , but also is primitive recursive in f for every n . The monomial ideal used to construct the bound permits it to be attained when f is increasing. On the other hand, while one has the recursivity in n , by taking simple linear functions we show that no general bound can exist which is primitive recursive in n .

We hope our methods in answering Seidenberg's questions will also fulfill his aspirations for constructive proofs, as stated in [Seidenberg72].

This paper is organized as follows, Sections 1 and 2 contain some preliminaries. In section 3, a series of reductions allows us to restrict ourselves to what we call simple monomial chains. The longest, as shown in section 4, are the compressed ones, and their Hilbert-Samuel functions are studied in section 5. The questions about primitive recursiveness in f and non primitive recursiveness in n are considered in sections 6 and 7, respectively, while in section 8 an example is given. Some of the results presented here have been partially given in [Moreno91], where a simpler problem was solved.

A question of notation: in the rest of the paper, superscripts will be used to number ideals, to avoid confusion which the graduation (thus I_v^i will refer to the set of elements of degree v belonging to the i th ideal of a chain).

1. Preliminaries: The Hilbert-Samuel function.

Here we make some definitions and recall some well known results we shall need. They are essentially due to F. S. Macaulay ([Macaulay27]; see also, e.g., [Sperner30], [Clements&Lindström69], [Stanley78], [Demazure84], [Robbiano90]).

Let $R = K[X_1, \dots, X_n]$ be our polynomial ring. In \mathcal{M} , the set of its monomials, we introduce the degree-lexicographic order: $X_1^{a_1} \dots X_n^{a_n} < X_1^{b_1} \dots X_n^{b_n}$ if and only if either (1) $a_1 + \dots + a_n < b_1 + \dots + b_n$ or (2) $a_1 + \dots + a_n = b_1 + \dots + b_n$ and $a_1 = b_1, \dots, a_{i-1} = b_{i-1}, a_i > b_i$ for some $i \in \{1, \dots, n\}$. This will be the order used, unless we state explicitly that we apply the degree-anti-lexicographic order: $m_1 \prec m_2$ if $\deg m_1 < \deg m_2$, or $\deg m_1 = \deg m_2$ and $m_1 > m_2$. Both are total orderings compatible with the natural graduation of R by total degree, indicated by subscripts:

$$R = R_0 \oplus R_1 \oplus \dots \oplus R_v \oplus \dots$$

A set of monomials $\{m_1, \dots, m_r\} \subseteq \mathcal{M}$ will be called *irredundant* if no m_i divides m_j for $i \neq j$.

For a monomial ideal $J \subseteq R$ we define $J_{[v]} = J \cap \mathcal{M}_v$, the set of its monomials of degree v .

Initial ideal. To every $p \in R$ we associate its leading monomial [for $<$] $m(p) \in \mathcal{M}$, which is the largest monomial having a non zero coefficient in p . The *initial ideal*

of an ideal $I \subseteq R$ is the monomial ideal $m(I) = (\{m(p) \mid p \in I\})$; it has the property that $R/I \simeq R/m(I)$ (isomorphism of K -modules induced by m). The set

$$s(I) = \{(a_1, \dots, a_n) \in \mathbb{N}^n \mid X_1^{a_1} \dots X_n^{a_n} \notin m(I)\}$$

is called the *stairs* of I , and its cardinal is the *volume* of the stairs.

Compressed sets. A set of monomials $M \subseteq \mathcal{M}$ will be called *compressed* [for $<$] if = downward closed

$$m, m' \in \mathcal{M}_v, \quad m' < m, \quad m \in M \Rightarrow m' \in M$$

for all v (i.e., the monomials of degree v of M are the first ones in the lexicographic order). For a monomial ideal J , we shall say that it is *compressed* if $J \cap \mathcal{M}$ (the set of its monomials) is compressed.

There is the following well known and easy to prove criterion of compression: A monomial ideal $J = (m_1, \dots, m_r)$, with $\{m_1, \dots, m_r\}$ irredundant and $m_1 < \dots < m_r$, is compressed if and only if for all $i = 1, \dots, r$

$$m_i = \min \{m \in J \mid m \notin (m_1, \dots, m_{i-1})\}$$

(or, equivalently, $m_i = \min \{m \in \mathcal{M}_{d_i} \mid m \notin (m_1, \dots, m_{i-1})\}$, where $d_i = \deg m_i$).

Binomial radices. For $v > 0$ and $a_0 \geq \dots \geq a_k \geq 0$ we define

$$\langle a_0, \dots, a_k \rangle_v = \binom{a_0 + v}{v} + \dots + \binom{a_k + v - k}{v - k},$$

where $\binom{m}{n} = m(m-1) \dots (m-n+1)/n!$ (in particular, $\langle \rangle_v = 0$).

For every $v > 0$, the application $(a_0, \dots, a_k) \mapsto \langle a_0, \dots, a_k \rangle_v$ is an order-preserving bijection between the decreasing sequences of length at most v (with the lexicographic order) and \mathbb{N} (with the usual order) (this is a consequence of lemma (6.3)). Thus the inverse of this bijection gives a unique decreasing sequence for every nonnegative integer, which we shall call its *v -binomial representation*.

If $a = \langle a_0, \dots, a_k \rangle_v$, we define

$$a^{<v>} = \langle a_0, \dots, a_k \rangle_{v+1}$$

(in particular, $0^{<v>} = 0$).

The theorem of Macaulay. Recall that the *Hilbert-Samuel function* of R/I is the function $H_{R/I}: \mathbb{N} \longrightarrow \mathbb{N}$ defined by

$$H_{R/I}(v) = \dim_K R_v/I_v,$$

and that one has $H_{R/I} = H_{R/m(I)}$ (by the isomorphism between the two quotients).

Now, by a theorem of Macaulay, $H: \mathbb{N} \longrightarrow \mathbb{N}$ is the Hilbert-Samuel function of some R/I if and only if

$$H(0) = 1$$

$$H(v+1) \leq H(v)^{<v>} \quad \forall v \geq 1.$$

Moreover, if $J = (m_1, \dots, m_r)$ is a monomial ideal with $\deg m_i \leq d$ for all i and $J_{[d]}$ is compressed, then one has $H_{R/J}(d+1) = H_{R/J}(d)^{<d>}$.

2. Preliminaries: Recursivity.

In this section, some more definitions and well known results are given. They are due to several people ([Ackermann28], [Gödel31], [Gödel34], [Kleene36]); we have used [Hermes69] as a general reference.

The functions considered here are those going from \mathbb{N}^r to \mathbb{N} (“total functions”, i.e., defined for every r -tuple of natural numbers), with $r \in \mathbb{N}$ (r is the number of arguments; for $r = 0$, one has the “constant functions”). Some basic functions are:

- the 0-ary constant function 0;
- the successor function $S: \mathbb{N} \longrightarrow \mathbb{N}$, $S(x) = x + 1$;
- the projection functions $\pi_{r,i}: \mathbb{N}^r \longrightarrow \mathbb{N}$, $\pi_{r,i}(x_1, \dots, x_r) = x_i$ ($r \in \mathbb{N}$, $i = 1, \dots, r$).

Recursive functions. (We only give an informal description.) Suppose we are given a finite system Σ of functional equations formed with numbers (i.e., 0 , $1 = S(0)$, $2 = S(S(0))$, ...), the function S , number variables X_0, X_1, \dots, X_r and function variables F, F_0, F_1, \dots, F_s (for an example, see the Ackermann function below). We are allowed to add other equations constructed by using those we already have and two rules:

- substitution of numbers for variables (e.g., from $F_8(X_5, X_0) \equiv S(F_7(X_0, F_9(X_5)))$ one can build $F_8(3, X_0) \equiv S(F_7(X_0, F_9(3)))$ by making $X_5 \leftarrow 3$);
- replacement of an expression by its numerical value (e.g., if one has $7 \equiv F_1(4, F_2(6))$ and $F(F_1(4, F_2(6))) \equiv F_3(F_1(4, F_2(6)), S(F_1(4, F_2(6))))$, one can build for instance $F(F_1(4, F_2(6))) \equiv F_3(F_1(4, F_2(6)), S(7))$).

All these equations, new and old, are said to be derivable from Σ .

Now, a function f is said to be recursive (or general recursive for emphasis) if there exists a system Σ as above such that for all $x_1, \dots, x_n, y \in \mathbb{N}$ one has: the equation $F(x_1, \dots, x_n) \equiv y$ is derivable from Σ if and only if $y = f(x_1, \dots, x_n)$. Recursive functions are computable in the intuitive sense (the set of valid derived equations being enumerable, for given arguments x_1, \dots, x_n one “just” needs to apply the two rules to the corresponding system until finding an equation of the form $F(x_1, \dots, x_n) \equiv y$).

Primitive recursiveness. Two basic processes used to define new functions are:

- *substitution*: from $f: \mathbb{N}^r \longrightarrow \mathbb{N}$ and $g_1, \dots, g_r: \mathbb{N}^s \longrightarrow \mathbb{N}$ one obtains $h: \mathbb{N}^s \longrightarrow \mathbb{N}$ with

$$h(x_1, \dots, x_s) = f(g_1(x_1, \dots, x_s), \dots, g_r(x_1, \dots, x_s)).$$

- *induction*: from $f: \mathbb{N}^r \longrightarrow \mathbb{N}$ and $g: \mathbb{N}^{r+2} \longrightarrow \mathbb{N}$ one obtains $h: \mathbb{N}^{r+1} \longrightarrow \mathbb{N}$ defined by

$$h(x_1, \dots, x_r, 0) = f(x_1, \dots, x_r)$$

$$h(x_1, \dots, x_r, y + 1) = g(x_1, \dots, x_r, y, h(x_1, \dots, x_r, y)).$$

A function is said to be *primitive recursive in* f_1, \dots, f_t if it can be obtained from the basic functions 0, successor and projections, together with f_1, \dots, f_t , by finitely many applications of substitution and induction (if $t = 0$, then one has the plain primitive recursive functions). Since usual recursive functions encountered in mathematics are primitive recursive, one could ask if the two concepts are equivalent. Wilhelm Ackermann gave a negative answer by providing an example.

Ackermann's function. We define the *Ackermann generalized exponential* $\varphi: \mathbb{N}^3 \rightarrow \mathbb{N}$ by the recursion

$$\varphi(i + 1, x, y + 1) = \varphi(i, x, \varphi(i + 1, x, y))$$

with (for $i, x, y \geq 0$)

$$\varphi(0, x, y) = y + 1$$

$$\varphi(1, x, 0) = x$$

$$\varphi(2, x, 0) = 0$$

$$\varphi(i + 3, x, 0) = 1.$$

This definition is slightly different from the original one in [Ackermann28] (Ackermann makes $\varphi(3, x, 0) = 1$ but $\varphi(i + 4, x, 0) = x$), we choose it because we think it easier to grasp, as one has

$$\varphi(1, x, y) = x + 1 + \dots + 1 = x + y \quad (\text{iteration of successor})$$

$$\varphi(2, x, y) = x + x + \dots + x = xy \quad (\text{iteration of sum})$$

$$\varphi(3, x, y) = xx \dots x = x^y = x \uparrow y \quad (\text{iteration of product})$$

$$\varphi(4, x, y) = x^{x^{\dots^x}} = x \uparrow \uparrow y \quad (\text{iteration of power})$$

$$\varphi(i, x, y) = x \uparrow^{i-2} y.$$

What is usually known as “the” *Ackermann function* $A: \mathbb{N}^2 \longrightarrow \mathbb{N}$ is the simpler one given by

$$A(m, n) = \varphi(m, 2, n + 3) - 3.$$

Its traditional recursive definition is:

$$A(0, n) = n + 1$$

$$A(m + 1, 0) = A(m, 1)$$

$$A(m + 1, n + 1) = A(m, A(m + 1, n))$$

for $m, n \geq 0$. In fact, it can be defined over \mathbb{Z}^2 , here we only extend it a little by making

$$A(0, -1) = 0$$

$$A(m + 1, -1) = 1.$$

It has the property of bounding all primitive recursive functions (i.e., for every $f: \mathbb{N}^n \longrightarrow \mathbb{N}$ primitive recursive there exists m such that $f(x_1, \dots, x_n) \leq A(m, \max\{x_1, \dots, x_n\})$); this means in particular that $m \mapsto A(m, 0)$ is not primitive recursive (thus A itself and φ are not, either).

3. Reduction to the simple monomial case.

For a finite set $E = \{p_1, \dots, p_r\} \subset R$, we define $\deg E = \max\{\deg p_1, \dots, \deg p_r\}$, and for a non zero ideal $I \subseteq R$, we define

$$\text{gdeg } I = \min\{\deg\{p_1, \dots, p_r\} \mid I = (p_1, \dots, p_r)\}$$

(so that I can be generated by elements of degree not greater than $\text{gdeg } I$ and this is the best possible). By convention, $\text{gdeg}(0) = 0$.

We shall say that $\Xi = (I^0, \dots, I^s)$ is an *ascending chain* if I^0, \dots, I^s are ideals of R and

$$I^0 \subset I^1 \subset \dots \subset I^s.$$

An ascending chain will be called *monomial* if its ideals are so. We shall note $l(\Xi)$ the *length* s of the chain.

Let $f: \mathbb{N} \longrightarrow \mathbb{N}$ be any function. We shall say that the ascending chain Ξ is an ascending chain for f if

$$\text{gdeg } I^i \leq f(i) \quad \forall i = 0, \dots, s.$$

We want to bound the length s of such a chain in terms of the only data we have, namely n and f . To do this, we shall boil down our problem to a combinatorial one by means of the following successive reductions: 1) increasing f ; 2) monomial

chains; 3) “simple” chains (to be defined). We are looking for an optimal bound, and this is easier to do when f is increasing (note that we can suppose $f(0) = 0$, as we can always replace I^0 by (0) in our chains), so we begin by defining

$$F(0) = 0$$

$$F(x) = \max \{f(1), \dots, f(x)\} \quad (x > 0)$$

(it might be amusing for the reader to prove F is primitive recursive in f ; this fact will be used later). The optimal bounds we are looking for are:

$$g(n, f) = \max \{l(\mathcal{E}) \mid \mathcal{E} \text{ is an \u00a0ascending chain for } f\}$$

$$\gamma(n, f) = \max \{l(\mathcal{E}) \mid \mathcal{E} \text{ is a \u00a0monomial ascending chain for } f\},$$

for which we have

$$\gamma(n, f) \leq g(n, f).$$

First reduction. As $f(x) \leq F(x)$, every ascending chain for f is an ascending chain for F , and we obviously have

$$g(n, f) \leq g(n, F)$$

$$\gamma(n, f) \leq \gamma(n, F).$$

So we only need to consider increasing functions.

Second reduction. Monomial chains suffice:

3.1. LEMMA. $g(n, F) = \gamma(n, F)$.

PROOF. We shall see that the first is not greater than the second. Let $I^0 \subset \dots \subset I^s$ be an ascending chain for F , so that we have $I^i = (p_{i1}, \dots, p_{ir_i})$ with $\deg p_{ij} \leq F(i)$. For $i = 1, \dots, s$, as $I^{i-1} \subset I^i$, there exists a p_{ij} not belonging to I^{i-1} , let us call it q_i . Furthermore, we can suppose that $m(q_i)$ is not a multiple of $m(q_1), \dots, m(q_{i-1})$ (if $m(q_i) \in m(q_1), \dots, m(q_{i-1})$, replace q_i by the non-zero rest q'_i of the ordered division of q_i by q_j ; as $m(q'_i) < m(q_i)$, these replacements will be done only finitely many times). Now letting $J^0 = (0)$ and $J^i = (m(q_1), \dots, m(q_i))$ we obtain $J^0 \subset \dots \subset J^s$, a monomial ascending chain for F of the same length.

Third reduction. Let $\mathcal{E} = (J^0, \dots, J^s)$ be a monomial ascending chain for F . We can write $J^i = (m_1, \dots, m_{r_i})$, and we suppose it is done in as irredundant a way as possible; that is, we take $\{m_1, \dots, m_{r_0}\}$ to be irredundant (if $r_0 = 0$, as likely, we are asking for nothing here), and for $i = 1, \dots, s$ we take $\{m_{r_{i-1}+1}, \dots, m_{r_i}\}$ to be irredundant with $m_j \notin J^{i-1}$ for $r_{i-1} < j \leq r_i$.

Now we notice that if s is to be maximum, then we should have $r_i = i$ (i.e., we

begin with $J^0 = (0)$, and we add only one monomial at each step); otherwise, we could lengthen our chain by replacing (m_1, \dots, m_{r_0}) by

$$(0) \subset (m_1) \subset (m_1, m_2) \subset \dots \subset (m_1, \dots, m_{r_0}),$$

or $(m_1, \dots, m_{r_{i-1}}) \subset (m_1, \dots, m_{r_i})$ by

$$(m_1, \dots, m_{r_{i-1}}) \subset (m_1, \dots, m_{r_{i-1}}, m_{r_{i-1}+1}) \subset \dots \subset (m_1, \dots, m_{r_i}).$$

We shall say that \mathcal{E} is simple if it has this property (i.e., if one can write $J^i = (m_1, \dots, m_i)$ for $i = 0, \dots, s$).

We have thus shown:

3.2. PROPOSITION.

$$g(n, f) \leq g(n, F) = \gamma(n, F) = \gamma_{\text{simple}}(n, F).$$

Therefore, we can restrain ourselves to the study of simple monomial chains.

4. The simple monomial case.

We let

$$\Gamma(n, f) = \gamma_{\text{simple}}(n, F).$$

And from now on, in order to minimize notations, we shall often drop n and f , considered to be fixed unless otherwise explicitly stated.

Now we are going to construct a special “compressed” simple chain $\tilde{\mathcal{E}}(n, f)$, and we shall show that it has maximum length. Our strategy is the following: every new monomial to be added will be chosen among those of maximum possible degree, by taking the least available one for the lexicographic order (so as to get compressed ideals). Thus starting with $\bar{J}^0 = (0)$, we add $\bar{J}^1 = (\mu_1)$ where $\mu_1 = \max^* \{m \in \mathcal{M} \mid \deg m \leq F(1)\}$ (this is the maximum for the degree-anti-lexicographic order), and we go on in this way while possible, letting $\bar{J}^i = (\mu_1, \dots, \mu_i)$ where

$$\mu_i = \max^* \{m \in \mathcal{M} \mid \deg m \leq F(i), m \notin (\mu_1, \dots, \mu_{i-1})\}$$

(“while possible” means thus “while $\bar{J}^{i-1} \neq (1)$ ”). Let $\tilde{\mathcal{E}}(n, f) = (\bar{J}^0, \dots, \bar{J}^L)$ be the chain obtained. We are going to see that $L = \Gamma$.

Before proceeding, we wish to make a remark we think important to understand what follows. Note that in this process there are two different stages: while $\dim \bar{J}^{i-1} > 0$ (i.e., the corresponding projective variety is not empty), we can (and do) always add a monomial of degree $F(i)$; but eventually our Hilbert-Samuel function will become zero at a large degree, and then $F(i)$ will be of no importance, as the available monomials will have small degree. The frontier, which will play an important rôle in our proofs, is given by

$$\Omega = \Omega(n, f) = \max \{i \mid \deg \mu_i = F(i)\}.$$

(In stairs language: μ_Ω closes the stairs, i.e., its volume becomes finite, and after that the monomials of the stairs will be removed one by one, in descending degree, till none is left.) The maximum of the degrees of the generators in our chain is thus

$$\mathcal{D} = \mathcal{D}(n, f) = F(\Omega(n, f)) = \text{gdeg } \bar{J}^\Omega.$$

Now, for the sake of completeness, we justify our claim about compression (this is easy and surely well known):

4.1. LEMMA. \bar{J}^i is compressed for $i = 0, \dots, L$.

PROOF. We suppose $i > 0$, as \bar{J}^0 is obviously compressed. If $i \leq \Omega$, then $\mu_1 < \dots < \mu_i$ and $\{\mu_1, \dots, \mu_i\}$ is irredundant, so that \bar{J}^i is compressed by the criterion indicated in section 1.

Suppose now $i > \Omega$, and note that in this case $\{\mu_1, \dots, \mu_i\}$ need not be irredundant (in fact, it will not be). We proceed by induction. Let us suppose \bar{J}^{i-1} is compressed, and let $d = \deg \mu_i$. For $v < d$ one has $\bar{J}_v^i = \bar{J}_v^{i-1}$ which is compressed. For $v = d$, the set $\bar{J}_{[d]}^i = \bar{J}_{[d]}^{i-1} \sqcup \{\mu_i\}$ is compressed by definition of μ_i . If $v > d$, then $d < F(i)$ means $\bar{J}_{[v]}^{i-1} = \mathcal{M}_v$, so that $\bar{J}_{[v]}^i = \mathcal{M}_v$ which is obviously compressed. ■

To show that compressed simple monomial chains have maximum length, we shall need to compare the Hilbert-Samuel functions of their ideals. This will be done using the lexicographic order (for $h_1, h_2: \mathbf{N} \longrightarrow \mathbf{N}$, one has $h_1 < h_2$ if and only if there exists $i \in \mathbf{N}$ such that $h_1(j) = h_2(j)$ for $j < i$ and $h_1(i) < h_2(i)$). The Hilbert-Samuel function of \bar{J}^i will be noted \bar{H}^i .

We shall make implicit use of the next easily verified fact:

4.2. LEMMA. Let $I \subset R$ be an ideal and $\Gamma = I' = I + (p)$, where $p \in R_d \setminus I$; then

$$H_{R/I'}(v) = H_{R/I}(v) \quad \forall v < d$$

$$H_{R/I'}(d) = H_{R/I}(d) - 1$$

$$H_{R/I'}(v) \leq H_{R/I}(v) \quad \forall v > d.$$

Now we have:

4.3. PROPOSITION. (Compressed monomial simple chains have maximum length)

$$\Gamma(n, f) = l(\bar{\Xi}(n, f)).$$

PROOF. Let $\Xi = (J^0, \dots, J^l)$ be any simple monomial chain with $J^i = (m_1, \dots, m_i)$, and suppose $l \geq L$. We must show that our choice of the monomials μ_i is the best possible, i.e., that $l = L$.

Let H^i be the Hilbert-Samuel function of J^i . We have $\bar{J}^L = (1)$, so that $\bar{H}^L \equiv 0$; if we show that $H^L \leq \bar{H}^L$, then $H^L \equiv 0$ and $J^L = (1)$, and we shall be done.

One could expect to show that $H^i \leq \bar{H}^i$ by recursion on i , but this need not be true for all i . However, it is so for some i , and that will be enough to conclude (see remarks below on non-uniqueness of simple monomial chains of maximum length). Let $i_0 = 0$, $i_r = L$ and

$$\{i_1, \dots, i_{r-1}\} = \{i \mid 0 < i < L, \deg \mu_i \neq \deg \mu_{i+1}\},$$

with $i_1 < \dots < i_{r-1}$. Let us see that $H^{i_j} \leq \bar{H}^{i_j}$ by recursion on j . Clearly $H^0 = \bar{H}^0$, so suppose $0 < j < r$ and $H^{i_{j-1}} \leq \bar{H}^{i_{j-1}}$. Let $\alpha = i_{j-1}$ and $\beta = i_j$, and let

$$\begin{aligned}\delta &= \deg \mu_{\alpha+1} = \dots = \deg \mu_\beta \\ d &= \min \{\deg m_{\alpha+1}, \dots, \deg m_\beta\} \\ v_0 &= \min \{v \mid H^\alpha(v) < \bar{H}^\alpha(v)\} \cup \{\infty\}\end{aligned}$$

(v_0 is thus the first place where the two Hilbert-Samuel functions differ). Note that $d \leq \deg m_k \leq \delta$ for $\alpha < k \leq \beta$, by definition of μ_k .

We consider four cases (we recall that (4.2) is used all the time):

– If $d > v_0$, then

$$\begin{aligned}H^\beta(v) &= H^\alpha(v) = \bar{H}^\alpha(v) = \bar{H}^\beta(v) \quad \forall v < v_0 \\ H^\beta(v_0) &= H^\alpha(v_0) < \bar{H}^\alpha(v_0) = \bar{H}^\beta(v_0),\end{aligned}$$

which implies $H^\beta < \bar{H}^\beta$.

– If $d \leq v_0$ and $d < \delta$, then

$$\begin{aligned}H^\beta(v) &= H^\alpha(v) = \bar{H}^\alpha(v) = \bar{H}^\beta(v) \quad \forall v < d \\ H^\beta(d) &< H^\alpha(d) \leq \bar{H}^\alpha(d) = \bar{H}^\beta(d),\end{aligned}$$

which implies $H^\beta < \bar{H}^\beta$.

– If $d = \delta = v_0$, we have

$$\begin{aligned}H^\beta(v) &= H^\alpha(v) = \bar{H}^\alpha(v) = \bar{H}^\beta(v) \quad \forall v < d \\ H^\beta(d) &= H^\alpha(d) - (\beta - \alpha) < \bar{H}^\alpha(d) - (\beta - \alpha) = \bar{H}^\beta(d),\end{aligned}$$

which implies $H^\beta < \bar{H}^\beta$.

– If $d = \delta < v_0$ (this is the interesting case), we have

$$\begin{aligned}H^\beta(v) &= H^\alpha(v) = \bar{H}^\alpha(v) = \bar{H}^\beta(v) \quad \forall v < \delta \\ H^\beta(\delta) &= H^\alpha(\delta) - (\beta - \alpha) = \bar{H}^\alpha(\delta) - (\beta - \alpha) = \bar{H}^\beta(\delta).\end{aligned}$$

Now if $\beta \leq \Omega$, the theorem of Macaulay says, for $v \geq \delta$, that

$$H^\beta(v+1) \leq H^\beta(v)^{\langle v \rangle}$$

$$\bar{H}^\beta(v+1) = \bar{H}^\beta(v)^{\langle v \rangle}$$

(where we have equality because \bar{J}^β is compressed and $\text{gdeg } \bar{J}^\beta = \delta$); as $a \leq b$ implies $a^{\langle v \rangle} \leq b^{\langle v \rangle}$ (remember, e.g., the order-preserving bijection), we conclude that $H^\beta \leq \bar{H}^\beta$.

Otherwise $\alpha \geq \Omega$ (the case $\alpha < \Omega < \beta$ is impossible), and then we know that $H^\alpha(\delta+1) \leq \bar{H}^\alpha(\delta+1) = 0$, so that

$$H^\beta(v) = \bar{H}^\beta(v) = 0 \quad \forall v > \delta$$

and $H^\beta = \bar{H}^\beta$.

The proof just given shows that compressed monomial simple chains are not the only monomial chains having maximum length. If F is not strictly increasing in the range $\{1, \dots, \Omega\}$, then there are consecutive monomials of the same degree among the μ_i , which can be permuted. And beyond Ω , where the value of F is no more considered, the monomials are added so as to fill every degree, and this can be done in any order. All these permutations of monomials of the same degree do not seem to be very relevant, so we can perhaps say that the monomial simple chain of maximum length is essentially unique. And because of the properties of initial ideals, the same could be said of general chains.

5. Hilbert-Samuel function.

Using the theorem of Macaulay, we shall give in this section the expression of the Hilbert-Samuel functions occurring in our chain. First we define

$$a^{0\langle v \rangle} = a$$

$$a^{(k+1)\langle v \rangle} = (a^{\langle v \rangle})^{k\langle v+1 \rangle}$$

(so that $a^{(k+1)\langle v \rangle} = a^{\langle v \rangle \langle v+1 \rangle \dots \langle v+k \rangle}$); and for a non zero Hilbert-Samuel function H and $a \geq 0$ we define a new function $H \div a$ as follows:

$$(H \div a)(v) = \begin{cases} H(v) & \text{for } v < \alpha \\ \min \{ (H(\alpha) - 1)^{(v-\alpha)\langle \alpha \rangle}, H(v) \} & \text{for } v \geq \alpha \end{cases}$$

where $\alpha = \max \{ v \leq a \mid H(v) > 0 \}$.

In the previous section we have built a chain $\bar{\mathcal{E}} = (\bar{J}^0, \dots, \bar{J}^\Omega)$, with $\bar{J}^1 = (\mu_1, \dots, \mu_i)$ of Hilbert-Samuel function \bar{H}^i . Now we can state:

5.1. LEMMA. For $i = 1, \dots, \Gamma$ one has

$$\bar{H}^i = \bar{H}^{i-1} \div F(i).$$

PROOF. Remember that $\bar{J}^i = \bar{J}^{i-1} + (\mu_i)$, where

$$\mu_i = \max^* \{m \in \mathcal{M} \mid \deg m \leq F(i), m \notin (\mu_1, \dots, \mu_{i-1})\}.$$

We consider two cases, as usual. If $i \leq \Omega$, then $\bar{H}^{i-1}(v) > 0$ for all v and $\deg \mu_i = F(i)$, so that $\text{gdeg } \bar{J}^i = F(i)$, and then, \bar{J}^i being compressed, we have

$$\bar{H}^i(v) = \begin{cases} \bar{H}^{i-1}(v) & (v < F(i)) \\ \bar{H}^{i-1}(v) - 1 & (v = F(i)) \\ \bar{H}^i(v-1)^{\langle v-1 \rangle} & (v > F(i)). \end{cases}$$

Thus $\bar{H}^i = \bar{H}^{i-1} \div F(i)$ (the corresponding α equals $F(i)$). If $i > \Omega$, then $\deg \mu_i < F(i)$ and we know that $\bar{H}^{i-1}(v) = 0$ if and only if $v > \deg \mu_i$, so that $\text{gdeg } \bar{J}^i = \deg \mu_i$ and we have

$$\bar{H}^i(v) = \begin{cases} \bar{H}^{i-1}(v) & (v < \deg \mu_i) \\ \bar{H}^{i-1}(v) - 1 & (v = \deg \mu_i) \\ 0 = \bar{H}^{i-1}(v) & (v > \deg \mu_i). \end{cases}$$

Thus once again $\bar{H}^i = \bar{H}^{i-1} \div F(i)$ (now the corresponding α equals $\deg \mu_i$).

6. Primitive recursiveness.

In order to find a primitive recursive expression for Γ , we shall write it as $\Omega + \mathcal{V}$. The second term $\mathcal{V} = \Gamma - \Omega$ is just the volume of the stairs of \bar{J}^Ω :

6.1. LEMMA.

$$\mathcal{V} = \#_s(\bar{J}^\Omega) = \bar{H}^\Omega(0) + \dots + \bar{H}^\Omega(\mathcal{D} - 1).$$

PROOF. This is a corollary of (5.1): for $i > \Omega$ we have

$$\sum_{v \in \mathbb{N}} \bar{H}^i(v) = \sum_{v \in \mathbb{N}} \bar{H}^{i-1}(v) - 1,$$

so that, as $\bar{J}^\Gamma = (1)$,

$$0 = \sum_{v \in \mathbb{N}} \bar{H}^\Gamma(v) = \sum_{v \in \mathbb{N}} \bar{H}^\Omega(v) - (\Gamma - \Omega)$$

as claimed (we recall that $\bar{H}^\Omega(v) = 0$ for $v \geq \mathcal{D}$).

To compute the first term Ω , we shall make use of the v -binomial representations. The following “exponential” notation for them will be very useful:

$$[e_r, \dots, e_{s+1}, e_s]_{s,t} = \langle \underbrace{r, \dots, r}_{e_r}, \underbrace{s+1, \dots, s+1}_{e_{s+1}}, \underbrace{s, \dots, s}_{e_s} \rangle_v$$

where $v = e_r + \dots + e_{s+1} + e_s + t$ (in particular, $[\]_{s,t} = 0$). This will be called the v -expbin representation, where the number t is the number of *free places* in the binomial representation. (It is unique if we demand that $s \geq 0$, $e_s > 0$, as $[e_r, \dots, e_{s+1}, 0]_{s,t} = [e_r, \dots, e_{s+1}]_{s+1,t}$. Note that one could admit $s = -1$, so that $[e_r, \dots, e_0]_{0,t} = [e_r, \dots, e_0, t]_{-1,0}$ (this is admissible because $(-1)! = \infty$), the number of free places being then e_{-1} .)

ΔF will denote the derivative of F :

$$\Delta F(0) = F(0)$$

$$\Delta F(i) = F(i) - F(i-1) \quad (i > 0).$$

We shall focus on $\bar{J} = \bar{J}^\Omega$, the most important ideal of our chain (the entire chain can be deduced from it), and on $\bar{H} = \bar{H}^\Omega$, its Hilbert-Samuel function. For simplicity, in the proofs we shall implicitly suppose henceforth that $n \neq 1$ (one has $\Omega(1, f) = 1$, $\Gamma(1, f) = 1 + f(1)$), and that $\bar{J} \neq (1)$ (i.e., $F(1) > 0$), but the reader will have no pains in seeing everything works for $n = 1$ or the trivial chain $(0) \subset (1)$.

6.2. LEMMA. Let $i \leq \Omega$.

(1) If $\bar{H}(F(i-1)) = \langle a_0, \dots, a_k \rangle_{F(i-1)}$, then

$$\bar{H}(v) = \langle a_0, \dots, a_k \rangle_v \quad (F(i-1) \leq v < F(i))$$

$$\bar{H}(F(i)) = \langle a_0, \dots, a_k \rangle_{F(i)} - 1,$$

(2) If $\bar{H}(F(i-1)) = [e_r, \dots, e_s]_{s,t}$ in $F(i-1)$ -expbin representation (i.e., $e_r + \dots + e_s + t = F(i-1)$), then

$$\bar{H}(F(i)) = [e_r, \dots, e_s]_{s,t+\Delta F(i)} - 1.$$

PROOF. (1) is an immediate consequence of the theorem of Macaulay and (4.1): as our ideal is compressed, we have

$$\bar{H}(v) = (\langle a_0, \dots, a_k \rangle_{F(i-1)})^{\langle F(i-1) \rangle} \dots^{\langle v-1 \rangle} = \langle a_0, \dots, a_k \rangle_v \quad (F(i-1) \leq v < F(i))$$

$$\bar{H}(F(i)) = \bar{H}(F(i-1))^{F(i)-1} - 1 = \langle a_0, \dots, a_k \rangle_{F(i)} - 1.$$

Expressing $\bar{H}(F(i))$ in exponential notation we obtain (2).

Let us see how to find the expbin representation of $[e_r, \dots, e_s]_{s,t} - 1$:

6.3. LEMMA. If $e_0 > 0$, then

$$[e_r, \dots, e_1, e_0]_{0,t} - 1 = [e_r, \dots, e_1, e_0 - 1]_{0,t+1}.$$

If $s > 0$ and $e_s > 0$, then

$$[e_r, \dots, e_{s+1}, e_s]_{s,t} - 1 = [e_r, \dots, e_{s+1}, e_s - 1, t + 1]_{s-1,0}.$$

PROOF. For $s \geq 0$ and $e_s > 0$ we have by definition

$$[e_r, \dots, e_{s+1}, e_s]_{s,t} = [e_r, \dots, e_{s+1}, e_s - 1]_{s,t+1} + \binom{s+t+1}{t+1}.$$

If $s = 0$ we are done, else using $\binom{m}{n+1} + \binom{m}{n} = \binom{m+1}{n+1}$ we can write

$$\begin{aligned} \binom{s+t+1}{t+1} - 1 &= \binom{(s-1)+t+1}{t+1} + \binom{(s-1)+t}{t} + \dots + \binom{(s-1)+1}{1} \\ &= \underbrace{\langle s-1, \dots, s-1 \rangle}_{t+1}_{t+1}, \end{aligned}$$

and we are done too.

We can now give the expbin representation of $\bar{H}(F(i))$:

6.4. PROPOSITION. For $i \leq \Omega$, if one has the $F(i-1)$ -expbin representation

$$\bar{H}(F(i-1)) = [e_r, \dots, e_s]_{s,t}$$

with $e_s > 0$, then one has the $F(i)$ -expbin representation

$$\bar{H}(F(i)) = \begin{cases} [e_r, \dots, e_1, e_0 - 1]_{0,t+\Delta F(i)+1} & \text{if } s = 0 \\ [e_r, \dots, e_{s+1}, e_s - 1, t + \Delta F(i) + 1]_{s-1,0} & \text{if } s > 0. \end{cases}$$

PROOF. It is enough to put together (6.2) and (6.3).

We are now ready to give a primitive recursive expression for $\Gamma = \Omega + \mathcal{V}$. Let us define $\Psi = \Psi_{n,g}: \mathbb{N} \times \mathbb{N}^{n-1} \times \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, where $g: \mathbb{N} \longrightarrow \mathbb{N}$, by

$$\Psi(i, (0, \dots, 0), t, v) = i + v,$$

with

$$\Psi(i-1, (e_{n-2}, \dots, e_{r+1}, e_r, 0, 0, \dots, 0), t, v) = \Psi(i, (e_{n-2}, \dots, e_{r+1}, e_r - 1, t', 0, \dots, 0), 0, v)$$

if $r > 0$ and $e_r > 0$ and

$$\Psi(i-1, (e_{n-2}, \dots, e_1, e_0), t, v) = \Psi(i, (e_{n-2}, \dots, e_1, e_0 - 1), t', v + t')$$

if $e_0 > 0$, where $t' = t + g(i) + 1$. Replacing “=” by “ \rightarrow ” we orient these two equations to obtain two rewriting rules for Ψ .

6.5. THEOREM.

$$\Gamma(n, f) = \Psi_{n,\Delta F}(1, (F(1), 0, \dots, 0), 0, 0).$$

(Perhaps $\Gamma(n, f) = \Psi_{n,\Delta F}(0, (1, 0, \dots, 0), -1, 0)$ with $\Psi: \mathbb{N} \times \mathbb{N}^n \times \mathbb{N}' \times \mathbb{N} \longrightarrow \mathbb{N}$ could be more aesthetic.)

6.6 COROLLARY. $\Gamma(n, f)$ is primitive recursive in f for every n .

PROOFS. It is easy to see that $\Psi_{n, \Delta F}$ is primitive recursive in ΔF , hence in F , hence in f , so the corollary is clear. Let us prove the theorem.

Our function $\Psi(i, (e_{n-2}, \dots, e_0), t, v)$ codes the information about the chain $\bar{\mathcal{E}}$ in the way suggested by the notation: i for the index going from 1 to Ω ; $[e_{n-2}, \dots, e_0]_{0,t}$ for the value of $\bar{H}(F(i))$, t being the number of free places; and v for counting the volume of the stairs, to become \mathcal{V} at the end.

This is not difficult to show. At the beginning we have

$$\bar{H}^1(v) = \langle n-1 \rangle_v \quad \forall v < F(1),$$

thus (using (6.3))

$$\begin{aligned} \bar{H}^1(F(1)) &= \langle n-1 \rangle_{F(1)} - 1 = [1]_{n-1, F(1)-1} - 1 = [F(1)]_{n-2, 0} \\ &= [F(1), \underbrace{0, \dots, 0}_{n-2}]_{0, 0}, \end{aligned}$$

$F(1)$ -expbin representation which corresponds to $\Psi(1, (F(1), 0, \dots, 0), 0, 0)$, the starting point. And the recursive definition of Ψ corresponds to the obtaining of the $F(i)$ -expbin representation for $\bar{H}^i(F(i))$ from the $F(i-1)$ -expbin representation $\bar{H}^{i-1}(F(i-1)) = [e_{n-2}, \dots, e_0]_{0,t}$ by using (6.3) (we think unnecessary to detail the two cases to be considered).

So starting with $\Psi(1, (F(1), 0, \dots, 0), 0, 0)$ and applying the recursion rules we obtain successively $\Psi(i, (e_{i, n-2}, \dots, e_{i, 0}), t_i, v_i)$ for $i = 1, 2, \dots$, with the property that $[e_{i, n-2}, \dots, e_{i, 0}]_{0, t_i} = \bar{H}^i(F(i))$. The rules can no more be applied when $e_{i, n-2} = \dots = e_{i, 0} = 0$, i.e., when $\bar{H}^i(F(i)) = 0$, which happens for $i = \Omega$. So we have

$$\Psi(1, (F(1), 0, \dots, 0), 0, 0) \rightarrow \dots \rightarrow \Psi(\Omega, (0, \dots, 0), t_\Omega, v_\Omega) = \Omega + v_\Omega,$$

where $t_\Omega = F(\Omega) = \mathcal{D} = \text{gdeg } \bar{J}$, the maximum of the degrees of the generators appearing in our chain.

If we prove that $v_\Omega = \mathcal{V}$, then we shall be done. For that we need two results, so we make now a paranthesis to show them (they are perhaps well known; our proofs are given for the convenience of the reader).

6.7. LEMMA. (Correspondence between generators and Hilbert-Samuel function for compressed monomial ideals)

Let $J = (m_1, \dots, m_r)$ be a compressed monomial ideal, with $\{m_1, \dots, m_r\}$ irredundant and $m_1 < \dots < m_r$, and let $d_i = \deg m_i$. If $d_i < d_{i+1}$ or $i = r$, then

$$m_i = X_1^{a_1} \dots X_{n-1}^{a_{n-1}} X_n^{a_n} \iff H(d_i) = [a_1, \dots, a_{n-1}]_{0, a_n},$$

where H is the Hilbert-Samuel function of J .

PROOF. (As usual, we shall identify $X_1^{a_1} \dots X_n^{a_n} \in \mathcal{M}$ with $(a_1, \dots, a_n) \in \mathbb{N}^n$.) First we show that the application

$$(a_1, \dots, a_{n-1}, a_n) \mapsto [a_1, \dots, a_{n-1}]_{0, a_n}$$

is an order-preserving bijection between (\mathcal{M}_v, \prec) , the monomials of degree v with the degree-anti-lexicographic order, and $\left(\left\{0, \dots, \binom{v+n-1}{n-1} - 1\right\}, <\right)$, the first natural numbers. To begin with, we have

$$(0, \dots, 0, v) \mapsto [0, \dots, 0]_{0, v} = 0.$$

Let $m = (e_{n-2}, \dots, e_{s+1}, e_s, e_{s-1}, 0, \dots, 0) \in \mathcal{M}_v$ with $e_{s-1} > 0$; the successor of this monomial for \prec , if it is not the last (i.e., if $s-1 < n-2$) is $m' = (e_{n-2}, \dots, e_{s+1}, e_s + 1, 0, \dots, 0, e_{s-1} - 1)$; suppose $m \mapsto i$, $m' \mapsto i'$; using (6.3), if $s = 0$ then

$$i' - 1 = [e_{n-2}, \dots, e_1, e_0 + 1]_{0, e_{-1}-1} - 1 = [e_{n-2}, \dots, e_1, e_0]_{0, e_{-1}} = i,$$

else

$$i' - 1 = [e_{n-2}, \dots, e_{s+1}, e_s + 1]_{s, e_{s-1}-1} - 1 = [e_{n-2}, \dots, e_{s+1}, e_s, e_{s-1}]_{s-1, 0} = i.$$

The order-preserving bijection is thus established by induction.

Now let $d = d_i$, $h = H(d_i)$. As $J_{[d]} = (m_1, \dots, m_i) \cap \mathcal{M}_d$ is compressed, the set $\{m \in \mathcal{M}_d \mid m \notin J_{[d]}\}$, of cardinality equal to h , contains all degree d monomials less than m_i (for \prec), so by the above bijection they map to $0, \dots, h-1$. This means that m_i maps to h , as claimed.

6.8. PROPOSITION (*Volume of the stairs of a compressed monomial ideal*).

Let $J = (m_1, \dots, m_r) \subseteq K[X_1, \dots, X_n]$ be a 0-dimensional compressed monomial ideal, $m_i = X_1^{a_{i,1}} \dots X_n^{a_{i,n}}$, with $\{m_1, \dots, m_r\}$ irredundant, and let H be its Hilbert-Samuel function. Then

$$\#s(J) = \sum_{v \in \mathbb{N}} H(v) = a_{1,n} + \dots + a_{r,n}.$$

PROOF. Here we use induction on n . The result is obvious for $n = 1$ (one has $r = 1$, $s(J) = \{0, \dots, a_{1,1} - 1\}$). Let $n > 1$. We can suppose $m_1 < \dots < m_r$, so that $a_{1,1} \geq \dots \geq a_{r,1}$; more precisely, letting $\alpha = a_{1,1}$, we take $i_{\alpha+1} = 0$, $i_j = \max\{i \mid a_{i,1} = j\}$, so that

$$a_{i_{\alpha+1}+1,1} = \dots = a_{i_{\alpha},1} > a_{i_{\alpha}+1,1} = \dots = a_{i_{\alpha-1},n} > \dots > a_{i_1+1,1} = \dots = a_{i_0,1}.$$

Notice that the criterion of compression given in section 1 implies that $a_{i_j+1,1} = a_{i_j,1} + 1$: there are no “holes” between the values of $a_{i,1}$; the same is true for the $a_{i,2}$ corresponding to a fixed $a_{i,1}$; the same is true for the $a_{i,2}$

corresponding to a fixed $a_{i,1}$, and so on (“the steps of a compressed stairs are of depth 1”).

Now we decompose the stairs $s(J)$ in slices along the X_1 -axis:

$$s(J) = s_0(J) \sqcup s_1(J) \sqcup \cdots \sqcup s_\alpha(J),$$

where

$$s_j(J) = \{(e_1, \dots, e_n) \in s(J) \mid e_1 = j\}.$$

By the previous remark, the only generators m_i which have an effect on the j th slice are those with $a_{i,1} = j$, so that

$$s_j(J) = \{(e_1, \dots, e_n) \mid e_1 = j, X_1^{e_1} \cdots X_n^{e_n} \notin (m_{i_{j+1}+1}, \dots, m_{i_j})\}.$$

Through the projection $(e_1, e_2, \dots, e_n) \mapsto (e_2, \dots, e_n)$, we obtain a stairs of the same volume corresponding to the monomial ideal

$$J'_j = (m'_{i_{j+1}+1}, \dots, m'_{i_j}) \subseteq k[X_2, \dots, X_n],$$

where $m'_i = X_2^{a_{i,2}} \cdots X_n^{a_{i,n}}$.

This monomial ideal is 0-dimensional and compressed (the compression follows from the recursive definition of the degree-lexicographic ordering), so that by the hypothesis of induction we have

$$\#s(J'_j) = a_{i_{j+1}+1,n} + \cdots + a_{i_j,n}.$$

Putting all the volumes together we obtain

$$\#s(j) = \#s_0(J) + \cdots + \#s_\alpha(J) = a_{1,n} + \cdots + a_{r,n},$$

the desired result.

We can now finish the proof of (6.5): v_Ω is equal to the sum for $i \leq \Omega$ of the free places of the binomial representation of $\bar{H}(F(i))$, which by (6.7) corresponds to the sum of the last coordinate of the μ_i , and this by (6.8) is the volume of the stairs, so that $v_\Omega = \mathcal{V}$.

7. Non primitive recursiveness.

This section is devoted to showing that $\Omega(n, f)$ is not primitive recursive in n if the function f increases at least linearly. As $\Gamma(n, f) \geq \Omega(n, f)$ is the maximum length, attained by $\bar{\Xi}(n, f)$, this will imply that no bound can be primitive recursive in n in general. Of course, for some special classes of functions f (e.g., constant functions), $\Gamma(n, f)$ can be primitive recursive in n too.

So from now on n will no more be fixed. On the other hand, throughout this section f will be a linear function

$$f(i) = ai + b,$$

with $a, b \in \mathbb{Z}$, $a \geq -b \geq 0$, and we let

$$\Gamma(n, a, b) = \Gamma(n, f)$$

$$\Omega(n, a, b) = \Omega(n, f)$$

$$\mathcal{D}(n, a, b) = \mathcal{D}(n, f)$$

(a and b will not always be written, as they can be considered fixed).

We want to show that $\Gamma(n, a, b)$ is an Ackermann-like function, using $\Psi_{n,a}$ (we identify ΔF with a), and for that we turn once again to free places. As a consequence of, e.g., (6.7), we have by applying the rewritten rules to Ψ that

$$\Psi(i, (e_{n-2}, \dots, e_{r+1}, e_r, 0, \dots, 0), t, v) \rightarrow \dots \rightarrow \Psi(i', (e_{n-2}, \dots, e_{r+1}, 0, 0, \dots, 0), t', v')$$

(i.e., e_r becomes 0; note that e_{n-2}, \dots, e_{r+1} remain unchanged). Let

$$\tau(r, e_r, t) = t'$$

(the number of free places after eliminating e_r), which is well defined (see the rewriting rules). It can be characterized as follows:

7.1. LEMMA. For $k, r \geq 1$ and $t \geq 0$, one has

$$\tau(r, 0, t) = t$$

$$\tau(0, k, t) = \tau(0, k-1, t+a+1)$$

$$\tau(r, k, t) = \tau(r, k-1, \tau(r-1, t+a+1, 0)).$$

PROOF. Replace $g(i) = \Delta F(i) = a$ in the rules for Ψ .

Our rewriting sequence is (see the proof of (6.5))

$$\Gamma = \Psi(1, (f(1), 0, \dots, 0), 0, 0) \rightarrow \dots \rightarrow \Psi(\Omega, (0, 0, \dots, 0), \mathcal{D}, \mathcal{V}) = \Omega + \mathcal{V},$$

so that

$$a\Omega + b = \mathcal{D} = \tau(n-2, f(1), 0) = \tau(n-2, a+b, 0).$$

We are going to write $\tau(r, k, 0)$ in terms of the following ackermannian function:

$$\Phi(i+1, x, y+1) = \Phi(i, x, \Phi(i+1, x, y))$$

with (for $i, x, y \geq 0$)

$$\Phi(0, x, y) = y + 1$$

$$\Phi(1, x, 0) = x$$

$$\Phi(i+2, x, 0) = 1.$$

Note that the “only” difference with the Ackermann generalized exponential φ is in the initial condition for $i = 2$. This is a slight difference (one has $\Phi(i, x, y) \sim \varphi(i, x, y + 1)$), but it makes Φ more difficult to write:

$$\begin{aligned}\Phi(0, x, y) &= 1 + y \\ \Phi(1, x, y) &= x + y \\ \Phi(2, x, y) &= 1 + xy \\ \Phi(3, x, y) &= x \uparrow y = 1 + x + x^2 + \dots + x^y \\ \Phi(4, x, y) &= x \uparrow \uparrow y = 1 + x + x^2 + \dots + x^{1 + \dots + x^{1 + \dots + x^{1 + \dots + x^1}}}_y \\ \Phi(i, x, y) &= x \uparrow^{i-2} y.\end{aligned}$$

(We could say that Φ is in a way the “integral” of φ , which explains our “ \uparrow ” notation.)

7.2. LEMMA.

$$\tau(r, k, 0) = \Phi(r + 2, a + 1, k + 1) - a - 2 = (a + 1) \uparrow^r (k + 1) - a - 2.$$

PROOF. (By induction on r , using (7.1).) For $r = 0$, we have

$$\begin{aligned}\tau(0, k, 0) &= \tau(0, k - 1, a + 1) = \dots \\ &= \tau(0, 0, (a + 1)k) = (a + 1)k = \Phi(2, a + 1, k + 1) - a - 2.\end{aligned}$$

Suppose $r > 0$. For the sake of readability let us make

$$\begin{aligned}\alpha_r(k) &= \tau(r, k + a + 1, 0) \\ \beta_i(y) &= \Phi(i, a + 1, y).\end{aligned}$$

To write τ in terms of Φ , first we roll up α :

$$\tau(r, k, 0) = \tau(r, k - 1, \alpha_{r-1}(0)) = \tau(r, k - 2, \alpha_{r-1}^2(0)) = \dots = \tau(r, 0, \alpha_{r-1}^k(0)) = \alpha_{r-1}^k(0).$$

Then using the induction hypothesis, namely

$$\begin{aligned}\alpha_{r-1}(u) &= \tau(r - 1, u + a + 1, 0) = \Phi(r + 1, a + 1, u + a + 2) - a - 2 \\ &= \beta_{r+1}(u + a + 2) - a - 2,\end{aligned}$$

we exchange α and β :

$$\begin{aligned}\alpha_{r-1}^{k-1}(\alpha_{r-1}(0)) &= \alpha_{r-1}^{k-1}(\beta_{r+1}(a + 2) - a - 2) = \alpha_{r-1}^{k-2}(\beta_{r+1}^2(a + 2) - a - 2) = \dots \\ &= \beta_{r+1}^k(a + 2) - a - 2.\end{aligned}$$

One sees by induction that $\beta_{i+1}(1) = a + 2$ for $i \geq 0$:

$$\beta_1(1) = a + 1 + 1 = a + 2$$

$$\beta_{i+2}(1) = \beta_{i+1}(\beta_{i+2}(0)) = \beta_{i+1}(1) = a + 2,$$

which allows us to unroll β :

$$\beta_{r+1}^k(a + 2) = \beta_{r+1}^k(\beta_{r+2}(1)) = \beta_{r+1}^{k-1}(\beta_{r+2}(2)) = \cdots = \beta_{r+1}(\beta_{r+2}(k)) = \beta_{r+2}(k + 1).$$

Thus $\tau(r, k, 0) = \Phi(r + 2, a + 1, k + 1) - a - 2$ as wanted.

From this we obtain:

7.3. PROPOSITION. For $a > 0$,

$$\Omega(n, a, b) = \frac{1}{a} ((a + 1) \uparrow^{n-2} (a + b + 1) - a - b - 2),$$

while

$$\Omega(n, 0, b) = \binom{n - 1 + b}{b}.$$

PROOF. For $a > 0$ we have

$$a\Omega + b = \tau(n - 2, a + b, 0) = (a + 1) \uparrow^{n-2} (a + b + 1) - a - 2.$$

If $a = 0$, then Ω is the number of monomials of degree b in n variables.

In the special case $a = 1$ we come upon the Ackermann function:

7.4. COROLLARY.

$$\Omega(n, 1, b) = A(n, b) - b - 1.$$

PROOF. (All recursions are on i for $i \geq 0$). We begin by seeing that $\varphi(i + 2, 2, 1) = 2$:

$$\varphi(2, 2, 1) = \varphi(1, 2, \varphi(2, 2, 0)) = \varphi(1, 2, 0) = 2$$

$$\varphi(i + 3, 2, 1) = \varphi(i + 2, 2, \varphi(i + 3, 2, 0)) = \varphi(i + 2, 2, 1) = 2.$$

Next, we show that $\Phi(i, 2, y) = \varphi(i, 2, y + 1) - 1$; first for the initial conditions:

$$\Phi(0, 2, y) = y + 1 = \varphi(0, 2, y + 1) - 1$$

$$\Phi(1, 2, 0) = 2 = \varphi(1, 2, 1) - 1$$

$$\Phi(i + 2, 2, 0) = 1 = \varphi(i + 2, 2, 1) - 1$$

and second for the recursion formula:

$$\begin{aligned}\Phi(i+1, 2, y+1) &= \Phi(i, 2, \Phi(i+1, 2, y)) = \Phi(i, 2, \varphi(i+1, 2, y+1) - 1) \\ &= \varphi(i, 2, \varphi(i+1, 2, y+1)) - 1 = \varphi(i+1, 2, y+1) - 1.\end{aligned}$$

We then conclude that

$$\Omega(n, 1, b) = \Phi(n, 2, b+2) - b - 3 = \varphi(n, 2, b+3) - b - 4 = A(n, b) - b - 1,$$

as wanted.

7.5. COROLLARY. *The length of the ascending chains in $K[X_1, \dots, X_n]$ for the identity function $f(i) = i$ cannot be bound by a function which is primitive recursive in n .*

PROOF. We have $l(\tilde{E}(n, 1, 0)) = \Gamma(n, 1, 0) \geq \Omega(n, 1, 0) = A(n, 0) - 1$ which is not primitive recursive.

REMARK. It is easy to see that the same holds for the classes of functions f verifying $f(i) \geq \alpha i + \beta$ with $\alpha, \beta \in \mathbb{R}$, $\alpha > -\beta \geq 0$.

We have the following expression for the volume $\mathcal{V}(n, a, b)$:

7.6. PROPOSITION.

$$\mathcal{V}(n, a, b) = \sum_{k=-a}^{b-1} \mathcal{V}(n-1, a, \mathcal{D}(n, a, k) + 1),$$

where $\mathcal{V}(0, a, b) = 1$ by convention.

PROOF. Let $\Gamma_b = \Gamma(n, a, b)$, $\Gamma'_b = \Gamma(n-1, a, b)$, and analogously for Ω and \mathcal{D} , and let $d = F(1) = a + b$. Values which are uninteresting will be replaced by “ \star ”.

We are going to split the rewriting of Γ_b , namely,

$$\begin{aligned}\Gamma_b &= \Psi_n(1, (d, 0, 0, \dots, 0), 0, 0) \rightarrow \dots \rightarrow \Psi_n(i, (1, 0, 0, \dots, 0), t, v) \rightarrow \\ &\rightarrow \Psi_n(i+1, (0, t+a+1, 0, \dots, 0), 0, v) \rightarrow \dots \rightarrow \Psi_n(\star, (0, 0, 0, \dots, 0), \star, \mathcal{V}_b).\end{aligned}$$

First, from the parallel rewritings

$$\begin{aligned}\Gamma_{b-1} &= \Psi_n(1, (d-1, 0, 0, \dots, 0), 0, 0) \rightarrow \Psi_n(2, (d-2, a+1, 0, \dots, 0), 0, 0) \rightarrow \dots \\ &\dots \rightarrow \Psi_n(\star, (0, 0, 0, \dots, 0), \mathcal{D}_{b-1}, \mathcal{V}_{b-1})\end{aligned}$$

and

$$\begin{aligned}\Psi_n(1, (d, 0, 0, \dots, 0), 0, 0) &\rightarrow \Psi_n(2, (d-1, a+1, 0, \dots, 0), 0, 0) \rightarrow \dots \\ &\dots \rightarrow \Psi_n(i, (1, 0, 0, \dots, 0), t, v),\end{aligned}$$

we see that $t = \mathcal{D}_{b-1}$, $v = \mathcal{V}_{b-1}$. Then, from the parallel rewritings

$$\begin{aligned} \Gamma'_{\mathcal{D}_{b-1}+1} &= \Psi_{n-1}(1, (\mathcal{D}_{b-1} + a + 1, 0, \dots, 0), 0, 0) \rightarrow \dots \\ &\dots \rightarrow \Psi_{n-1}(\star, (0, 0, \dots, 0), \star, \mathcal{V}'_{\mathcal{D}_{b-1}+1}) \end{aligned}$$

and

$$\begin{aligned} \Psi_n(i + 1, (0, \mathcal{D}_{b-1} + a + 1, 0, \dots, 0), 0, \mathcal{V}_{b-1}) &\rightarrow \dots \\ &\dots \rightarrow \Psi_n(\star, (0, 0, 0, \dots, 0), \star, \mathcal{V}_b) \end{aligned}$$

we see that $\mathcal{V}_b = \mathcal{V}_{b-1} + \mathcal{V}'_{\mathcal{D}_{b-1}+1}$, i.e.,

$$\mathcal{V}(n, a, b) = \mathcal{V}(n, a, b - 1) + \mathcal{V}(n - 1, a, \mathcal{D}(n, a, b - 1) + 1).$$

As $\mathcal{V}(n, a, -a) = 0$, the result follows by induction.

(What we have done here is to cut the stairs in slices along the X_1 -axis; cf. the proof of (6.8).)

In the special case $a = 1$, the Ackermann function appears once again:

7.7. COROLLARY. $\mathcal{V}(n, 1, b) = v(n, b)$, where

$$\begin{aligned} v(n, b) &= \sum_{k=-1}^{b-1} v(n - 1, A(n, k)) \quad (n > 0) \\ v(0, b) &= 1. \end{aligned}$$

PROOF. $\mathcal{D}(n, 1, k) = A(n, k) - 1$ by (7.4).

It is interesting to note that though in general $\mathcal{V}(n, f)$ grows much faster than $\Omega(n, f)$, the latter increases rapidly enough for our results about non primitive recursiveness in n to hold true; in fact, \mathcal{V} is obtained through Ψ as a “by-product” of the computation of Ω , making it no more difficult to calculate (up to coefficient growth).

8. An example.

Let us take

$$f = (0 \ 4 \ 4 \ 5 \ 5 \ 5 \ 5 \ 7 \ 7 \ 8 \ 9 \ 10 \ 11 \ 11 \ 12 \ 12 \ 16 \ 17 \ 19 \ 20 \ 20 \ 20 \ 21 \ 22 \ 24 \ 25 \ 26 \ 29 \ \dots)$$

(i.e., $f(0) = 0$, $f(1) = 4$, and so on), so that $F = f$. Then for $n = 3$ we have:

$F(1) = 4$	$\Psi(1, (4, 0), 0, 0)$	$\mu_1 = x^4$	$\bar{H}^1(4) = [4, 0]_{0,0} = \langle 1, 1, 1, 1 \rangle_4 = 14$
$F(2) = 4$	$\Psi(2, (3, 1), 0, 0)$	$\mu_2 = x^3 y$	$\bar{H}^2(4) = [3, 1]_{0,0} = \langle 1, 1, 1, 0 \rangle_4 = 13$
$F(3) = 5$	$\Psi(3, (3, 0), 2, 2)$	$\mu_3 = x^3 z^2$	$\bar{H}^3(5) = [3, 0]_{0,2} = \langle 1, 1, 1 \rangle_5 = 15$
$F(4) = 5$	$\Psi(4, (2, 3), 0, 2)$	$\mu_4 = x^2 y^3$	$\bar{H}^4(5) = [2, 3]_{0,0} = \langle 1, 1, 0, 0, 0 \rangle_5 = 14$
$F(5) = 5$	$\Psi(5, (2, 2), 1, 3)$	$\mu_5 = x^2 y^2 z$	$\bar{H}^5(5) = [2, 2]_{0,1} = \langle 1, 1, 0, 0 \rangle_5 = 13$
$F(6) = 5$	$\Psi(6, (2, 1), 2, 5)$	$\mu_6 = x^2 y z^2$	$\bar{H}^6(5) = [2, 1]_{0,2} = \langle 1, 1, 0 \rangle_5 = 12$

$F(7) = 7$	$\Psi(7, (2, 0), 5, 10)$	$\mu_7 = x^2 z^5$	$\bar{H}^7(7) = [2, 0]_{0,5} = \langle 1, 1 \rangle_7 = 15$
$F(8) = 7$	$\Psi(8, (1, 6), 0, 10)$	$\mu_8 = xy^6$	$\bar{H}^8(7) = [1, 6]_{0,0} = \langle 1, 0, 0, 0, 0, 0 \rangle_7 = 14$
$F(9) = 8$	$\Psi(9, (1, 5), 2, 12)$	$\mu_9 = xy^5 z^2$	$\bar{H}^9(8) = [1, 5]_{0,2} = \langle 1, 0, 0, 0, 0, 0 \rangle_8 = 14$
$F(10) = 9$	$\Psi(10, (1, 4), 4, 16)$	$\mu_{10} = xy^4 z^4$	$\bar{H}^{10}(9) = [1, 4]_{0,4} = \langle 1, 0, 0, 0, 0 \rangle_9 = 14$
$F(11) = 10$	$\Psi(11, (1, 3), 6, 22)$	$\mu_{11} = xy^3 z^6$	$\bar{H}^{11}(10) = [1, 3]_{0,6} = \langle 1, 0, 0, 0 \rangle_{10} = 14$
$F(12) = 11$	$\Psi(12, (1, 2), 8, 30)$	$\mu_{12} = xy^2 z^8$	$\bar{H}^{12}(11) = [1, 2]_{0,8} = \langle 1, 0, 0 \rangle_{11} = 14$
$F(13) = 11$	$\Psi(13, (1, 1), 9, 39)$	$\mu_{13} = xyz^9$	$\bar{H}^{13}(11) = [1, 1]_{0,9} = \langle 1, 0 \rangle_{11} = 13$
$F(14) = 12$	$\Psi(14, (1, 0), 11, 50)$	$\mu_{14} = xz^{11}$	$\bar{H}^{14}(12) = [1, 0]_{0,11} = \langle 1 \rangle_{12} = 13$
$F(15) = 12$	$\Psi(15, (0, 12), 0, 50)$	$\mu_{15} = y^{12}$	$\bar{H}^{15}(12) = [0, 12]_{0,0} = \langle 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 \rangle_{12} = 12$
$F(16) = 16$	$\Psi(16, (0, 11), 5, 55)$	$\mu_{16} = y^{11} z^5$	$\bar{H}^{16}(16) = [0, 11]_{0,5} = \langle 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 \rangle_{16} = 11$
$F(17) = 17$	$\Psi(17, (0, 10), 7, 62)$	$\mu_{17} = y^{10} z^7$	$\bar{H}^{17}(17) = [0, 10]_{0,7} = \langle 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 \rangle_{17} = 10$
$F(18) = 19$	$\Psi(18, (0, 9), 10, 72)$	$\mu_{18} = y^9 z^{10}$	$\bar{H}^{18}(19) = [0, 9]_{0,10} = \langle 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 \rangle_{19} = 9$
$F(19) = 20$	$\Psi(19, (0, 8), 12, 84)$	$\mu_{19} = y^8 z^{12}$	$\bar{H}^{19}(20) = [0, 8]_{0,12} = \langle 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 \rangle_{20} = 8$
$F(20) = 20$	$\Psi(20, (0, 7), 13, 97)$	$\mu_{20} = y^7 z^{13}$	$\bar{H}^{20}(20) = [0, 7]_{0,13} = \langle 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 \rangle_{20} = 7$
$F(21) = 20$	$\Psi(21, (0, 6), 14, 111)$	$\mu_{21} = y^6 z^{14}$	$\bar{H}^{21}(20) = [0, 6]_{0,14} = \langle 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 \rangle_{20} = 6$
$F(22) = 21$	$\Psi(22, (0, 5), 16, 127)$	$\mu_{22} = y^5 z^{16}$	$\bar{H}^{22}(21) = [0, 5]_{0,16} = \langle 0, 0, 0, 0, 0 \rangle_{21} = 5$
$F(23) = 22$	$\Psi(23, (0, 4), 18, 145)$	$\mu_{23} = y^4 z^{18}$	$\bar{H}^{23}(22) = [0, 4]_{0,18} = \langle 0, 0, 0, 0 \rangle_{22} = 4$
$F(24) = 24$	$\Psi(24, (0, 3), 21, 166)$	$\mu_{24} = y^3 z^{21}$	$\bar{H}^{24}(24) = [0, 3]_{0,21} = \langle 0, 0, 0 \rangle_{24} = 3$
$F(25) = 25$	$\Psi(25, (0, 2), 23, 189)$	$\mu_{25} = y^2 z^{23}$	$\bar{H}^{25}(25) = [0, 2]_{0,23} = \langle 0, 0 \rangle_{25} = 2$
$F(26) = 26$	$\Psi(26, (0, 1), 25, 214)$	$\mu_{26} = yz^{25}$	$\bar{H}^{26}(26) = [0, 1]_{0,25} = \langle 0 \rangle_{26} = 1$
$F(27) = 29$	$\Psi(27, (0, 0), 29, 243)$	$\mu_{27} = z^{29}$	$\bar{H}^{27}(29) = [0, 0]_{0,29} = \langle \rangle_{29} = 0$

Thus

$$\Gamma(3, f) = \Psi_{3, \Delta F}(1, (F(1), 0), 0, 0) \rightarrow \cdots \rightarrow \Psi_{3, \Delta F}(27, (0, 0), 29, 243) = 270,$$

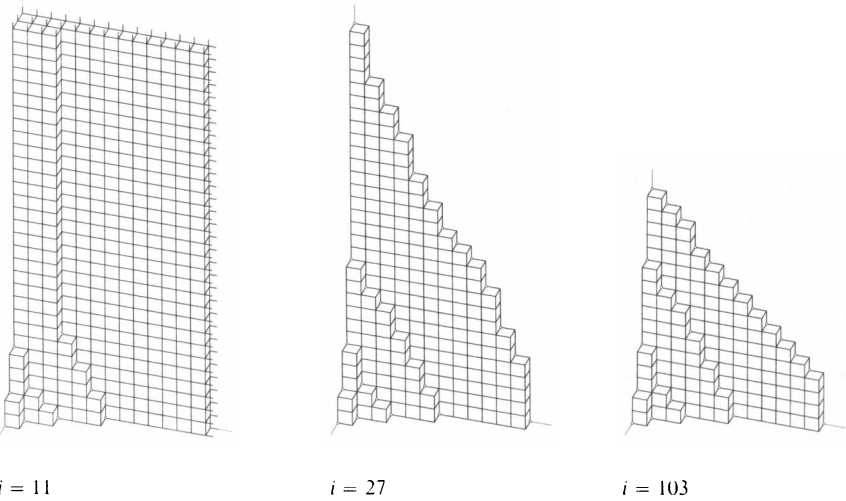
which means

$$\begin{aligned}\Omega(3, f) &= 27 \\ \mathcal{D}(3, f) &= 29 \\ \mathcal{V}(3, f) &= 243 \\ \Gamma(3, f) &= 270.\end{aligned}$$

And we have $\bar{J} = \bar{J}^\Omega = (\mu_1, \dots, \mu_\Omega)$, its Hilbert-Samuel function $\bar{H} = \bar{H}^\Omega$ being $\bar{H} = (1\ 3\ 6\ 10\ 13\ 12\ 14\ 14\ 14\ 14\ 14\ 13\ 12\ 12\ 12\ 12\ 11\ 10\ 10\ 9\ 6\ 5\ 4\ 4\ 3\ 2\ 1\ 1\ 1\ 0\ \dots)$ (notice by the way that it is not of the “increasing-constant-decreasing” type).

Next we show the stairs of three of the ideals $\bar{J}^i = (\mu_1, \dots, \mu_i)$ of our chain $\bar{\Xi}(3, f) = (\bar{J}^0, \dots, \bar{J}^I)$, namely for $i = 11 < \Omega$, $i = 27 = \Omega$ and $i = 103 > \Omega$. The last is irredundantly generated by:

$$\{\mu_1, \dots, \mu_{15}, y^{11}z^4, y^{10}z^5, y^9z^6, y^8z^7, y^7z^8, y^6z^9, y^5z^{10}, y^4z^{11}, y^3z^{12}, y^2z^{14}, yz^{15}, z^{16}\}.$$



ACKNOWLEDGEMENTS. This paper can be considered as a generalization and extension of a problem I solved in [Moreno91]. I am most grateful to the referee who told me about Seidenberg’s questions, which gave me the opportunity to answer them.

REFERENCES

- [Ackermann28] Wilhelm Ackermann, *Zum Hilbertschen Aufbau der reellen Zahlen*, Math. Ann. 99 (1928), 118–133.
- [Clements&Lindström69] G. F. Clements & B. Lindström, *A generalization of a combinatorial theorem of Macaulay*, J. Combin. Theory 7 (1969), 230–238.
- [Demazure84] Michel Demazure, *Fonctions de Hilbert-Samuel d'après Macaulay, Stanley et Bayer*, Notes informelles de Calcul Formel 1, preprint, Centre de Mathématiques de l'École Polytechnique, Palaiseau (1984).
- [Gödel31] Kurt Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I*, Mh. Math. Phys. 38 (1931), 173–198.
- [Gödel34] Kurt Gödel, *On Undecidable Propositions of Formal Mathematical Systems*, Institute for Advanced Study, Princeton, 1934.
- [Hermes69] Hans Hermes, *Enumerability, Decidability, Computability*, Die Grundlehren der mathematischen Wissenschaften 127, Springer, Berlin, 1969.
- [Kleene36] S. C. Kleene, *General recursive functions of natural numbers*, Math. Ann. 112 (1936), 727–742.
- [Macaulay27] F. S. Macaulay, *Some properties of enumeration in the theory of modular systems*, Proc. London Math. Soc. (2) 26 (1927), 531–555.
- [Moreno91] Guillermo Moreno Socías, *An ackermannian polynomial ideal*, in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Proceedings, 1991*, Lect. Notes in Comp. Sc. 539 (1991), 269–280.
- [Robbiano90] Lorenzo Robbiano, *Introduction to the theory of Hilbert functions*, Queen's Papers in Pure and Appl. Math. 85 (1990).
- [Seidenberg71] A. Seidenberg, *On the length of a Hilbert ascending chain*, Proc. Amer. Math. Soc. 29 (1971), 443–450.
- [Seidenberg72] A. Seidenberg, *Constructive proof of Hilbert's theorem on ascending chains*, Trans. Amer. Math. Soc. 174 (1972), 305–312.
- [Sperner30] E. Sperner, *Über einen kombinatorischen Satz von Macaulay und seine Anwendungen auf die Theorie der Polynomideale*, Abh. Math. Sem. Univ. Hamburg 7 (1930), 149–163.
- [Stanley78] Richard P. Stanley, *Hilbert functions of graded algebras*, Adv. in Math. 28 (1978), 57–83.

ÉQUIPE DE CALCUL FORMEL
 CENTRE DE MATHÉMATIQUES & LIX
 ÉCOLE POLYTECHNIQUE
 F-91128 PALAISEAU CEDEX
 FRANCE
 INTERNET: MORENO@POLY. POLYTECHNIQUE. FR