T U M

I N S T I T U T F Ü R I N F O R M A T I K

Some Complexity Results for Polynomial Ideals

Ernst W. Mayr

TUM–I9704
Februar 97

T E C H N I S C H E U N I V E R S I T Ä T M Ü N C H E N

TUM-INFO-02-I9704-150/1.-FI
Alle Rechte vorbehalten
Nachdruck auch auszugsweise verboten

©1997

Druck: Institut für Informatik der
Technischen Universität München

Some Complexity Results for Polynomial Ideals

Ernst W. Mayr
Institut für Informatik
Technische Universität München
D-80290 München, GERMANY
e-mail: MAYR@INFORMATIK.TU-MUENCHEN.DE
WWW: HTTP://WWWMAYR.INFORMATIK.TU-MUENCHEN.DE/

January 11, 1997

Abstract

In this paper, we survey some of our new results on the complexity of a number of problems related to polynomial ideals. We consider multivariate polynomials over some ring, like the integers or the rationals. For instance, a polynomial ideal membership problem is a $(w+1)$-tuple $P = (f, g_1, g_2, \ldots, g_w)$ where f and the g_i are multivariate polynomials, and the problem is to determine whether f is in the ideal generated by the g_i. For polynomials over the integers or rationals, this problem is known to be exponential space complete. We discuss further complexity results for problems related to polynomial ideals, like the word and subword problems for commutative semigroups, a quantitative version of Hilbert's Nullstellensatz in a complexity theoretic version, and problems concerning the computation of reduced polynomials and Gröbner bases.

1 Introduction

Polynomial rings and their ideals are fundamental in many areas of mathematics, and they also have a surprising number of applications in various areas of computer science, like language generating and term rewriting systems, tiling problems, the complexity of algebraic manifolds, and the complexity of some models for parallel systems. They have also been used in some constraint logic programming software systems, like [1].

The decidability of the membership problem for polynomial ideals over a field or ring was established in [25], [52], and [50]. The computational complexity of the polynomial ideal membership problem was first discussed in [43] where the special case of the word problem for commutative semigroups was investigated and solved. The bounds derived there imply an exponential space lower bound for the membership problem in polynomial ideals over $\mathbb{Z}$ (the integers) or $\mathbb{Q}$ (the rationals), in fact over arbitrary infinite fields, as well as a doubly exponential lower bound for the time requirements for any Turing machine solving the polynomial ideal membership problem over the rationals or integers. Other, rather special cases of the polynomial ideal membership problem (given by restrictions on the form of the generators) and their complexity have been investigated in [26], and, for the case of special test polynomials, in *e.g.* [10], [4], [7], and [24]. Some other related complexity results, using, however, a different model (algebraic circuits) for parallel computation, can be found in [20].

In this paper, we give a survey on basic algorithmic problems involving polynomial ideals, on some new complexity bounds for these problems and algorithms for them, and on some applications of polynomial ideals in other areas of computer science. It should be emphasized, however, that this survey is not intended to be comprehensive and complete, a remark that just as well applies to the list of references cited at the end.

2 Notations and Some Fundamental Concepts

2.1 Polynomials and Ideals

Consider the finite set $\{x_1, \ldots, x_n\}$ of indeterminates and let $\mathbb{Q}[x]$ denote the (commutative) ring of polynomials in $x_1, \ldots, x_n$ with rational coefficients. An *ideal* in $\mathbb{Q}[x]$ is defined in the ordinary way to be any subset $\mathcal{I}$ of $\mathbb{Q}[x]$ satisfying

(i) $p, q \in \mathcal{I} \quad \Rightarrow \quad p - q \in \mathcal{I}$;

(ii) $p \in \mathcal{I},\ r \in \mathbb{Q}[x] \quad \Rightarrow \quad rp \in \mathcal{I}$.

For polynomials $g_1, \ldots, g_w \in \mathbb{Q}[x]$, let $(g_1, \ldots, g_w) \subseteq \mathbb{Q}[x]$ denote the ideal generated by $\{g_1, \ldots, g_w\}$, *i.e.*,

$$(g_1, \ldots, g_w) = \left\{ \sum_{1 \le i \le w} p_i g_i\ ;\ p_i \in \mathbb{Q}[x] \right\}.$$

If $\mathcal{I} = (g_1, \ldots, g_w)$, $\{g_1, \ldots, g_w\}$ is called a *basis* of $\mathcal{I}$.

A *term* τ in $x_1, \ldots, x_n$ is a product of the form

$$\tau = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}\,,$$

with $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ the *degree vector* of τ and $\deg(\tau) = \sum_{j=1}^{n} \alpha_j$ the *total degree* of τ. For succinctness, we also write $\tau = x^\alpha$.

Each *polynomial* $f(x_1, \ldots, x_n) \in \mathbb{Q}[x]$ is a finite sum

$$f(x_1, \ldots, x_n) = \sum_{1 \le i \le r} c_i \cdot x^{\alpha_i}\,,$$

with $c_i \in \mathbb{Q} - \{0\}$ the coefficient and $\alpha_i \in \mathbb{N}^n$ the degree vector of the ith term of f. The product $c_i \cdot x^{\alpha_i}$ is called the ith monomial of the polynomial f. The total degree of a polynomial is the maximum of the total degrees of its monomials.

Example: Consider $\mathbb{Q}[x_1, x_2, x_3]$, the ring of polynomials in x_1, x_2, x_3 with rational coefficients. Then the ideal $(x_1^3, x_2 x_3)$ consists of all polynomials $f \in \mathbb{Q}[x_1, x_2, x_3]$ such that each term of f is divisible by x_1^3 or by $x_2 x_3$.

An *admissible term ordering* in $\mathbb{Q}[x]$ is given by any total order $\prec$ on $\mathbb{N}^n$ satisfying the following two conditions:

1. $\alpha \succ (0, \ldots, 0)$ for all $\alpha \in \mathbb{N}^n - \{(0, \ldots, 0)\}$;

2. for all $\alpha, \beta, \gamma \in \mathbb{N}^n$,
$$\alpha \prec \beta \Rightarrow \alpha + \gamma \prec \beta + \gamma\,.$$

If $\alpha \succ \beta$, we say that the term x^α is greater in the term ordering than the term x^β, and, for a polynomial $f(x) = \sum_{i=1}^{r} c_i \cdot x^{\alpha_i}$, we always assume that $\alpha_1 \succ \alpha_2 \succ \ldots \succ \alpha_n$. We call $LT(f) = x^{\alpha_1}$ the *leading term* and $LM(f) = c_1 \cdot x^{\alpha_1}$ the *leading monomial* of f. Since we are dealing with polynomials with coefficients from the field $\mathbb{Q}$, we shall also usually assume that polynomials are normalized, *i.e.,* their leading coefficient c_1 is one. In an abuse of notation, we also write $\prec$ for the term ordering induced by the order $\prec$ on the degree vectors.

Example: Let $\prec$ be the lexicographic ordering on $\mathbb{N}^n$, *i.e.,* if $\alpha, \beta \in \mathbb{N}^n$, $\alpha \neq \beta$, $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$ then

$$\alpha \prec \beta \text{ iff there is an } i \text{ such that for all } j < i \ \alpha_j = \beta_j, \text{ and } \alpha_i < \beta_i\,.$$

Then, in the term ordering,

$$x_1 \succ x_2 \succ x_3 \succ 1\,,$$

and the leading monomial (and the leading term) of the polynomial

$$f(x_1, x_2, x_3) = x_1^5 + x_1^2 x_2^4 + x_1^2 x_3^5 + 3x_1 x_2^2 x_3^2 - 1$$

is x_1^5.

Example: Let $\prec$ be the so-called *graded reverse lexicographic (grevlex)* ordering on $\mathbb{N}^n$, *i.e.,* if $\alpha, \beta \in \mathbb{N}^n$, $\alpha \neq \beta$, $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$ then

$$\alpha \prec \beta \text{ iff } \textstyle\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i, \text{ or } \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i, \text{ and there is an } i \text{ such that } \alpha_j = \beta_j \text{ for all } j > i \text{ and } \alpha_i > \beta_i.$$

Then, in the term ordering,

$$x_1 \succ x_2 \succ x_3 \succ 1\,,$$

the polynomial of the previous example is written

$$f(x_1, x_2, x_3) = x_1^2 x_3^5 + x_1^2 x_2^4 + x_1^5 + 3x_1 x_2^2 x_3^2 - 1\,,$$

and its leading term is $x_1^2 x_3^5$.

Let $\mathcal{I}$ be an ideal in $\mathbb{Q}[x]$, and let some admissible term order $\prec$ on $\mathbb{Q}[x]$ be given. A finite set $\{g_1, \ldots, g_r\}$ of polynomials from $\mathbb{Q}[x]$ is called a *Gröbner* basis of $\mathcal{I}$ (wrt. $\prec$), if

(i) $\{g_1, \ldots, g_r\}$ is a basis of $\mathcal{I}$;

(ii) $\{LT(g_1), \ldots, LT(g_r)\}$ is a basis of the *leading term ideal* of $\mathcal{I}$, which is the smallest ideal containing the leading terms of all $f \in \mathcal{I}$; or, equivalently: if $f \in \mathcal{I}$, then

$$LT(f) \in (LT(g_1), \ldots, LT(g_r))\,.$$

Gröbner bases have been introduced in [8]. For an excellent exposition of their numerous useful properties, see e.g. [9]. A basis is called *minimal* if it does not strictly contain some other basis of the same ideal. A Gröbner basis is called *reduced* if no term in any one of its polynomials is divisible by the leading term of some other polynomial in the basis.

A polynomial $f \in \mathbb{Q}[x]$ is called *homogeneous* (of degree d) if all of its monomials have the same total degree d. Let $f \in \mathbb{Q}[x]$ be some arbitrary polynomial. Then f can uniquely be written as $f = \sum f_i$, where each f_i is homogeneous and $\deg(f_i) \neq \deg(f_j)$ for $i \neq j$. The f_i are called the *homogeneous components* of f. An ideal $\mathcal{I} \subseteq \mathbb{Q}[x]$ is called *homogeneous*, if, whenever $\mathcal{I}$ contains some polynomial f, it also contains the homogeneous components of f. It can be shown that this is equivalent to the following definition: An ideal $\mathcal{I} \subseteq \mathbb{Q}[x]$ is homogeneous if it has a basis consisting of homogeneous polynomials.

2.2 Commutative Semigroups

A *commutative semigroup* $(H, \circ)$ is a set H with a binary operation $\circ$ which is associative and commutative. Usually we shall write ab for $a \circ b$.

A commutative semigroup H is said to be *finitely generated* by a finite subset $S = \{s_1, \ldots, s_n\} \subseteq H$ if

$$H = \{s_1^{\alpha_1} s_2^{\alpha_2} \cdots s_n^{\alpha_n};\ \alpha_i \in \mathbb{N} \text{ for } i = 1, \ldots, n\}.$$

(Note: $s_i^{\alpha_i}$ is short for $\underbrace{s_i \cdots s_i}_{\alpha_i}$.) There is a canonical homomorphism from $\mathbb{N}^n$ to H, mapping $\alpha \in \mathbb{N}^n$ to $s^\alpha \in H$. If this homomorphism actually is a bijection, then H is the free commutative semigroup generated by $\{s_1, \ldots, s_n\}$, which is also denoted by S^*. For a word $m = s_1^{\alpha_1} s_2^{\alpha_2} \cdots s_n^{\alpha_n} \in S^*$, the sum $\alpha_1 + \alpha_2 + \ldots + \alpha_n$ is called the *length* of m.

Note that a term $x^\alpha \in \mathbb{Q}[x]$ can also be looked at as an element of the commutative semigroup generated by $x_1, \ldots, x_k$.

A *finitely presented commutative semigroup* over S is given by a finite set $\mathcal{P}$ of congruences $l_i \equiv r_i$, where l_i, $r_i \in S^*$. A word $m' \in S^*$ *is derived in one step* from $m \in S^*$ (written $m \leftrightarrow m'(\mathcal{P})$) via the congruence $(l_i \equiv r_i) \in \mathcal{P}$ iff, for some $\tilde{m} \in S^*$, we have $m = \tilde{m} l_i$ and $m' = \tilde{m} r_i$, or $m = \tilde{m} r_i$ and $m' = \tilde{m} l_i$. The word m *derives* m' iff $m \overset{*}{\leftrightarrow} m'(\mathcal{P})$, where $\overset{*}{\leftrightarrow}$ is the reflexive transitive closure of $\leftrightarrow$. A sequence $(m_0, \ldots, m_r)$ of words $m_i \in S^*$ with $m_i \leftrightarrow m_{i+1}(\mathcal{P})$ for $i = 0, \ldots, r-1$ is called a *derivation* (of length r) of m_r from m_0 in $\mathcal{P}$. Derivability establishes a congruence $\equiv_{\mathcal{P}}$ on S^* by the rule

$$m \equiv_{\mathcal{P}} m' \Leftrightarrow_{\text{def}} m \overset{*}{\leftrightarrow} m'(\mathcal{P}).$$

Clearly, commutative semigroups are a concept equivalent to commutative Thue systems.

If it is understood that $\mathcal{P}$ is a commutative Thue system then the commutativity productions are not explicitly mentioned in $\mathcal{P}$, nor is their application within a derivation in $\mathcal{P}$ counted as a step.

A commutative Thue system $\mathcal{P}$ is also called a *presentation of the quotient semigroup* $S^*/\equiv_{\mathcal{P}}$. For $m \in S^*$, we use $[m]$ to denote the congruence class of m wrt. $\equiv_{\mathcal{P}}$.

2.3 Semilinear Sets

A *linear* subset L of $\mathbb{N}^n$ is a set of the form

$$L = \left\{ a + \sum_{i=1}^{t} n_i b^{(i)};\ n_i \in \mathbb{N} \text{ for } i = 1, \ldots, t \right\}$$

for some vectors $a, b^{(1)}, \ldots, b^{(t)} \in \mathbb{N}^n$.

A *semilinear* set SL is a finite union of linear sets:

$$SL = \bigcup_{j=1}^{k} \left\{ a_j + \sum_{i=1}^{t_j} n_i b_j^{(i)};\ n_i \in \mathbb{N} \text{ for } i = 1, \ldots, t_j \right\}$$

for some vectors $a_j, b_j^{(1)}, \ldots, b_j^{(t_j)} \in \mathbb{N}^n$, $j = 1, \ldots, k$.

A *uniformly semilinear* subset UL of $\mathbb{N}^n$ is a set of the form

$$UL = \bigcup_{j=1}^{k} \left\{ a_j + \sum_{i=1}^{t} n_i b^{(i)};\ n_i \in \mathbb{N} \text{ for } i = 1, \ldots, t \right\}$$

for some vectors $a_j, b^{(1)}, \ldots, b^{(t)} \in \mathbb{N}^n$, $j = 1, \ldots, k$.

We have (see [17]) the following

Theorem 1 *Let $\equiv$ be any congruence relation on $\mathbb{N}^n$. Then the congruence class $[u]$ of any element $u \in \mathbb{N}^n$ with respect to $\equiv$ is a uniformly semilinear set in $\mathbb{N}^n$.*

2.4 Some Complexity Issues

Since we are mainly concerned with the computational complexity of problems, it is necessary to speak about how we measure complexity. We consider the standard multi-tape Turing machine model (see, e.g., [2]). For space bounds, we only count, as is usual, the space used on the work tapes, and we do not take into account the space used on the write-only output tape (which may be exponentially larger). We state complexity bounds as worst-case bounds in terms of the input size, which is the number of bits used to encode the input. For encoding, we can, unless stated otherwise, use any standard encoding, *i.e.,* write numbers in binary, write vectors as delimited lists of numbers, etc..

We should also remark here that our results really do not depend much on the chosen encoding. In fact, all our upper bounds hold if we encode numbers in binary (*i.e.,* use a *succinct* encoding), while all our lower bounds hold even if we encode numbers in unary notation (*i.e.,* are very generous with the space required to write down the input; the reason is that the numbers occuring in the input of the problem instances for our lower bounds are all very small). Note that this independence from the details of the encoding of the input makes our results (upper as well as lower bounds) even stronger!

Occasionally, we also mention the Parallel Random Access Machine or PRAM as a machine model for parallel computation. Such a machine consists of an unbounded number of processors (each with the basic capabilities of a Random Access Machine, a model quite similar to actual microprocessors) and a global shared memory of unbounded size and consisting of memory cells, each of which can store an arbitrary integer. Each processor can access any cell of the global memory cell in one step, and appropriate measures are taken to resolve (or forbid a priori) memory access conflicts. For more details on this model, see [21].

We use the abbreviation PSPACE to refer to the class of problems that can be decided by (multi-tape) Turing machines using an amount of work space that is polynomial in the size of the input. PSPACE is a very fundamental and (with respect to variations of the machine model) very robust complexity class. For more details, see [2].

3 Basic Results

In this section, we are going to review several very basic and fundamental complexity results for the structures we have presented in the previous section. Arguably one of the most central problems for almost all of these structures turns out to be the *uniform word problem for commutative semigroups* which is defined as follows:

Definition 3.1 *Let S be a finite set of generators, and $\mathcal{P}$ a finite set of congruences on S^*. Let $m, m' \in S^*$.*

(i) **Decision Problem:** *Given $S, \mathcal{P}, m$, and m' as input, decide whether*

$$m \equiv_{\mathcal{P}} m' ;$$

(ii) **Representation Problem:** *Given $S, \mathcal{P}, m$, and m' as input, decide whether*

$$m \equiv_{\mathcal{P}} m' ,$$

and if so, find a derivation of m' from m in $\mathcal{P}$.

Another problem, just as central, is the *polynomial ideal membership problem (PIMP)*. It is

Definition 3.2 *Let $f, g_1, \ldots, g_w$ be polynomials in $\mathbb{Q}[x] = \mathbb{Q}[x_1, \ldots, x_n]$, and let $\mathcal{I} = (g_1, \ldots, g_w)$.*

(i) **Decision Problem:** *Given $f, g_1, \ldots, g_w$, decide whether*

$$f \in \mathcal{I};$$

(ii) **Representation Problem:** *Given $f, g_1, \ldots, g_w$, decide whether $f \in \mathcal{I}$, and if so, find $p_i \in \mathbb{Q}[x]$ such that*

$$f(x) = \sum_{i=1}^{w} p_i g_i \, .$$

It is well known (see, e.g., [12]) that the word problem for commutative semigroups can be reduced to PIMP, simply by interpreting each word $m \in S^*$ as a monomial in the indeterminates $s_1, \ldots, s_n$ and observing that

$$m \equiv_{\mathcal{P}} m' \iff m' - m \in (r_1 - l_1, \ldots, r_w - l_w) \subseteq \mathbb{Q}[s_1, \ldots, s_n] \, ,$$

where $l_i \equiv r_i$, $i = 1, \ldots, w$ are the congruences in $\mathcal{P}$.

In the fundamental paper [25], G. Hermann gave a doubly exponential degree bound for PIMP:

Theorem 2 *Let $f, g_1, \ldots, g_w$ be polynomials $\in \mathbb{Q}[x]$, and let $d = \max\{\deg(g_i);\ i = 1, \ldots, w\}$. If $f \in (g_1, \ldots, g_w)$, then there exist $p_1, \ldots, p_w \in \mathbb{Q}[x]$ such that*

1. *$f = \sum_{i=1}^{w} p_i g_i$; and*
2. *$\deg(p_i) \leq \deg(f) + (wd)^{2^n}$, for all i, $i = 1, \ldots, w$.*

For improved proofs of this theorem, see [52] and [43].

In [11] and [43] it was shown how to transform this degree bound for PIMP into a space bound for the special case of PIMP, the uniform word problem for commutative semigroups:

Theorem 3 *The uniform word problem for finitely presented commutative semigroups can be decided in exponential space (*i.e.*, space $2^{O(n)}$, with n here the size of the input).*

In [41, 42], this exponential space upper bound (for the Turing machine model) was generalized to PIMP:

Theorem 4 *Let P be a polynomial ideal membership problem over $\mathbb{Q}$, and let s be the size of the input for P. Then there is a PRAM algorithm which solves P in parallel time $2^{O(s)}$ using $2^{2^{O(s)}}$ processors.*

Using the Parallel Computation Thesis ([21]) and techniques from [47], one obtains

Theorem 5 *The polynomial ideal membership problem is solvable in sequential space exponential in the size of the problem instance.*

for the decision problem, and also, for the representation problem,

Theorem 6 *Let f and $g_1, \ldots, g_w$ be multivariate polynomials over the rationals. If f is an element of the ideal generated by the g_i then a representation*

$$f = \sum_{1 \leq i \leq w} p_i g_i$$

can be found in exponential space.

As is customary, the space bound for the representation problem bounds the work space, not the space on the output tape needed to write down the p_is. This distinction is crucial, since, as we shall see below, the total length needed for writing down the p_is can be double exponential in the size of the input. For a detailed proof of these two theorems, see [41].

As we have already mentioned, Gröbner bases play an important role in the algorithmic treatment of problems in polynomial ideals. The complexity of algorithms for generating a Gröbner basis from a given set of generators for an ideal has been the subject of intensive study (see e.g. [18] for a rather comprehensive survey). From the numerous complexity results, we would like to mention the following:

Theorem 7 *Let $\mathcal{I} = (g_1, \ldots, g_w) \subseteq \mathbb{Q}[x_1, \ldots, x_n]$ be an ideal, let d be the maximal total degree of the g_i, $i = 1, \ldots, w$, and let $\prec$ be any admissible ordering on $\mathbb{Q}[x]$. Then the reduced Gröbner basis for $\mathcal{I}$ consists of polynomials whose total degree is bounded by*

$$2(\frac{d^2}{2} + d)^{2^{n-1}}.$$

An elegant, elementary proof of this doubly exponential degree bound is given in [15]. For earlier, somewhat weaker doubly exponential degree bounds, also see [23] and [35]. Similar results, but for more restricted subproblems, can also be found in *e.g.* [3], [40], or [45].

Let $g_1, \ldots, g_w \in \mathbb{Q}[x_1, \ldots, x_n]$ be given. A *syzygy* for the g_i is any vector $(p_1, \ldots, p_w) \in (\mathbb{Q}[x])^w$ such that $\sum_{i=1}^{w} p_i g_i = 0$. The set of syzygies forms a (finite dimensional) $\mathbb{Q}[x]$-module ([25]).

Theorem 8 *Let $g_1, \ldots, g_w \in \mathbb{Q}[x_1, \ldots, x_n]$ be given, and let d be a bound on the total degree of the g_i. Then there is a basis for the module of syzygies whose polynomials have a total degree bounded by*

$$2(\frac{d^2}{2} + d)^{2^{n-1}}.$$

For a proof, see [25] (for corrections to this paper, see *e.g.,* [39], [52], and [43]) and [15].

In the remainder of this section, we turn to lower bounds for the algorithmic problems considered so far. The central result here is the lower bound for the uniform word problem for finitely presented commutative semigroups shown in [43]:

Theorem 9 *There is an infinite family of instances $(m^{(i)}, m'^{(i)}, \mathcal{P}^{(i)})$ of the uniform word problem for finitely presented commutative semigroups and a constant $c > 0$ such that each derivation of $m'^{(i)}$ from $m^{(i)}$ in $\mathcal{P}^{(i)}$ contains a word of length $\geq 2^{2^{c \cdot s}}$, where s denotes the input size.*

Using commutative semigroups to simulate *counter* or *Minsky automata* ([44]), this result implies (cf. [43]):

Theorem 10 *The uniform word problem for finitely presented commutative semigroups requires exponential space, and is therefore, together with the matching upper bound, exponential space complete.*

Since the word problem for commutative semigroups is a special case of PIMP (the corresponding ideals are also called *(pure difference) binomial ideals*, see [19]), we also obtain an exponential space lower bound (and thus completeness for exponential space) for PIMP. The construction in [43] has been sharpened in [53] (which greatly improves the constant in the exponent from 1/14 to basically 1/2) to yield the following lower bounds:

Theorem 11 *Let n be the number of indeterminates and d the maximal total degree of the generating polynomials in $\mathbb{Q}[x] = \mathbb{Q}[x_1, \ldots, x_n]$. Then there is an infinite family of instances of PIMP, including infinitely many n, such that, for each of these instances, say with generators $g_1, \ldots, g_w$,*

(i) there is a polynomial $f \in \mathbb{Q}[x_1, \ldots, x_n]$ with total degree $\leq d$, such that $f \in (g_1, \ldots, g_w)$ and, whenever

$$f(x) = \sum_{i=1}^{w} p_i g_i \,,$$

then the maximal total degree of the p_i is $\geq 2^{2^{n/2-O(\sqrt{n})}}$;

(ii) any syzygy basis for the $g_1, \ldots, g_w$ contains polynomials of degree

$$\geq 2^{2^{n/2-O(\sqrt{n})}} \,.$$

4 Complexity Results for Commutative Semigroups

As shown in [30], we get the following exponential space complexity bounds from the results in [43] and [41].

Definition 4.1 *Let $\mathcal{P}$ be a finite set of congruences on S^*, $S = \{s_1, \ldots, s_n\}$, and let $m, m' \in S^*$.*

1. *The* **Boundedness Problem** *is: Given $S, \mathcal{P}$, and m, decide whether $[m]$ is finite.*
2. *The* **Coverability Problem** *is: Given $S, \mathcal{P}, m$, and m', decide whether there is an $m'' \in [m]$ such that m' is a subword of m''.*
3. *The* **Selfcoverability Problem** *is: Given $S, \mathcal{P}$, and m, decide whether there is an $m'' \in [m]$ such that m is a proper subword of m''.*

In [30] we show that, in terms of upper bounds, the boundedness, coverability and selfcoverability problems can all be reduced to instances of PIMP for binomial ideals, and hence are in exponential space. An exponential space lower bound can be obtained by observing that the construction in [43] actually proves the following, slightly stronger statement:

Theorem 12 *There is an infinite family of instances $(m, m', \mathcal{P})$ of the commutative semigroup word problem such that for each of them*

(i) $[m]$ is finite,

(ii) m' is not a proper subword of any word in $[m]$, and

(iii) any Turing machine requires exponential space on an infinite number of these instances.

Furthermore, the uniform word problem for finitely generated commutative semigroups with the above restrictions is still complete for exponential space under log-lin reductions.

Using this version, we can reduce exponential space to any of the boundedness, coverability, or selfcoverability problem for commutative semigroups, establishing an exponential space lower bound and thus exponential space completeness for these three problems.

Next, we consider the *generalized subword problem for commutative semigroups*, unifying several of the problems above.

Let $V \subseteq S$ be a subset of $S = \{s_1, \ldots, s_n\}$, wlog $V = \{s_1, \ldots, s_l\}$, and let $\bar{V} = S - V$. Further, let Y be the subset $\{s_{l_1}, \ldots, s_{l_2}\}$ of X with $l_2 \geq l$ (if $l_1 > l_2$ then $Y = \emptyset$). Similarly, let $Z = \{s_{l_3}, \ldots, s_n\}$ be another subset of S, with $l_2 < l_3$, and $Z = \emptyset$ if $l_3 > n$.

Then, for the case $l_1 < l < l_2 < l_3 < n$, we get the following picture:

$$\overbrace{s_1, \ldots, s_{l_1-1},\ \rlap{$\underbrace{\phantom{s_{l_1}, \ldots, s_l,\ s_{l+1}, \ldots, s_{l_2}}}_{Y}$}s_{l_1}, \ldots, s_l,}^{V}\ \overbrace{s_{l+1}, \ldots, s_{l_2},\ s_{l_2+1}, \ldots, s_{l_3-1},\ \underbrace{s_{l_3}, \ldots, s_n}_{Z}}^{\bar{V}}$$

With this notation, we define the *generalized subword problem* as follows.

Definition 4.2 *Given S, $\mathcal{P}$, $V \subseteq S$, $u \in S^*$, $v \in V^*$, Y and Z as above, and with $y = s_{l_1} \cdots s_{l_2}$, decide whether there is a $u' \in [u]$ such that $u' = v \cdot y \cdot w$ for some $w \in (Y \cup Z)^*$.*

We see that the word problem and the coverability problem are special cases of the generalized subword problem. If Y and Z are both empty, then the generalized subword problem is equivalent to the word problem. If Y is the empty set and $Z = X$, then the subword problem is equivalent to the coverability problem.

Theorem 13 *The generalized subword problem is decidable in space exponential in the size of the input.*

Proof: [Sketch] In addition to $s_1, \ldots, s_n$ we introduce three new variables s, $\bar{s}$, and t. Let $S_t = S \cup \{s, \bar{s}, t\}$. Given $\mathcal{P}$ and the two words $u, v \in S^*$, we construct a new commutative semigroup presentation $\mathcal{P}_t$ over S_t as follows: For every congruence $l_i \equiv r_i$ in $\mathcal{P}$, $\mathcal{P}_t$ contains the congruence $t \cdot l_i \equiv t \cdot r_i$.

Then we add to $\mathcal{P}_t$ the congruences $s \equiv t \cdot u$,

and $t \cdot v_1 \cdot v \equiv \bar{s}$.

Let $\prec$ be any lexicographic term ordering satisfying

$$s \succ t \succ s' \succ s'' \succ \bar{s} \succ s_y \succ s_z\ ,$$

for all $s' \in V - (Y \cup Z)$, $s'' \in \bar{V} - (Y \cup Z)$, $s_y \in Y$ and $s_z \in Z$.

Let m_s be the minimal element wrt $\prec$ of the congruence class $[s]_{\mathcal{P}_t}$ of s in $\mathcal{P}_t$. As shown in [34], the binomial $s - m_s$ is an element of the reduced Gröbner basis of $I(\mathcal{P}_t)$, the ideal generated by the congruences in $\mathcal{P}_t$ considered as binomials. It is also shown that, because of the particular term ordering, there is a $u' \in [u]_{\mathcal{P}}$ such that $u' = v \cdot y \cdot w'$ for some $w' \in (Y \cup Z)^*$ iff $m_s = \bar{s} \cdot w$ for some $w \in (Y \cup Z)^*$.

The claim of the theorem now follows from the degree bound given in Theorem 7. □

As an example, consider the finite commutative semigroup presentation $\mathcal{P} = \{s_1 \equiv s_2s_3\,,\ s_1 \equiv s_2s_3^3\,,\ s_2s_3^4 \equiv s_2\}$ over $S = \{s_1, s_2, s_3\}$, the words $u = s_1$, $v = s_1$ and the sets $Y = \{s_3\}$ and $Z = \emptyset$. In this special case, the subword problem is to decide whether there is a $u' \in [s_1]_{\mathcal{P}}$ such that $u' = s_1s_3 \cdot w'$ for some $w' \in \{s_3\}^*$.

Using the construction in the proof of Theorem 13 we compute the reduced Gröbner basis G of the ideal

$$\mathcal{I} := (\ ts_1 - ts_2s_3\,,\ ts_1 - ts_2s_3^3\,,\ ts_2s_3^4 - ts_2\,,\ s - ts_1\,,\ ts_1s_3 - \bar{s}\ )$$

wrt the lexicographic term ordering $\succ$ satisfying

$$s \succ t \succ s_1 \succ s_2 \succ \bar{s} \succ s_3\ .$$

We obtain

$$G = \{\bar{s}s_3^2 - \bar{s}\,,\ \bar{s}s_1 - \bar{s}s_2s_3\,,\ ts_2 - \bar{s}\,,\ ts_1 - \bar{s}s_3\,,\ s - \bar{s}s_3\}\ .$$

The binomial $s - \bar{s}s_3$ provides the solution $w = s_3$ and $u' = s_1s_3^2$, resp., which can be verified by the following derivation in $\mathcal{P}$:

$$u = s_1 \leftrightarrow s_2s_3 \leftrightarrow s_2s_3^5 \leftrightarrow s_1s_3^2 = u'\,(\mathcal{P})\ .$$

In further constructions in [34], the algorithm for the generalized subword problem is then used to obtain explicit semilinear representations of congruence classes in finitely presented commutative semigroups, and, using these, to solve the equivalence problem, *i.e.,* to decide, given two commutative semigroup presentations $\mathcal{P}$ and $\mathcal{P}'$ over the same alphabet S, and two words $u, u' \in S^*$, whether the two respective congruence classes are equal, *i.e.,* whether

$$[u]_{\mathcal{P}} = [u']_{\mathcal{P}'}$$

Since this new algorithm for the equivalence problem also requires only exponential space, it closes the gap left by the earlier algorithm given in [26].

5 Results for the Membership Problem for Polynomial Ideals

In this section, we are going to summarize some results (upper and lower bounds) on the complexity of PIMP, the polynomial ideal membership problem. We have already mentioned (see Theorem 5) the exponential space upper bound for $\mathbb{Q}[x_1, \ldots, x_n]$ obtained in [41], [42], and also the matching lower bound coming from the lower bound for the special case, the uniform word problem for commutative semigroups, in [43].

While the exponential space bound in [41] is based on the classical construction in [25], more recently exciting improvements have been obtained for the degree bound for a number of special cases of PIMP. Among them, maybe the most prominent are the following:

Theorem 14 *Let g_i, $i = 1, \ldots, w$, be polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$, let d be the maximal degree of the g_i, and assume that the g_i have no common zero in $\mathbb{C}^n$. Then*

$$1 = \sum_{i=1}^{w} p_i g_i$$

for p_i with $\deg(p_i) \le \mu n d^\mu + \mu d$, with $\mu = \min\{n, w\}$.

For a proof, see [7].

Using the so-called "Rabinovich trick", Brownawell [7] also obtained

Theorem 15 *Let $f, g_i \in \mathbb{Q}[x_1, \ldots, x_n]$ for $i = 1, \ldots, w$, let d and μ be as above, and assume that $f(x) = 0$ for all common zeros x (in $\mathbb{C}^n$) of the g_i. Then there are*

$$e \in \mathbb{N}, \ e \leq (\mu+1)(n+2)(d+1)^{\mu+1},$$

$$p_i \in \mathbb{Q}[x_1, \ldots, x_n], \ \textit{with} \ \deg(p_i) \leq (\mu+1)(n+2)(d+1)^{\mu+2}$$

such that

$$f^e = \sum_{i=1}^{w} p_i g_i.$$

For proofs of these and similar exponential degree bounds, see [7], [4], and [29]. The method of [41] immediately yields

Corollary 15.1 *Whether*

$$1 \in (g_1, \ldots, g_w)$$

can be tested in PSPACE.

Corollary 15.2 *Whether there is an $e \in \mathbb{N}$ such that*

$$g^e \in (g_1, \ldots, g_w)$$

can be tested in PSPACE.

These two corollaries could be termed *quantitative versions* of Hilbert's Nullstellensatz (see, e.g., [54]), one variant of which is

Theorem 16 (Hilbert's Nullstellensatz) *Let k be some algebraically closed field, let $f, g_i \in k[x_1, \ldots, x_n]$, for $i = 1, \ldots, w$, and assume that $f(x) = 0$ for all common zeros x of the g_i. Then (and only then) there is an integer $e \geq 1$ such that*

$$f^e \in (g_1, \ldots, g_w).$$

There are a few more special cases of PIMP, where we get a PSPACE upper bound. An ideal $\mathcal{I} = (g_1, \ldots, g_w) \subseteq \mathbb{Q}[x]$ is called *zero-dimensional* if the common zeros (in $\mathbb{C}^n$) of the g_i are a finite set (for an exact definition of the dimension of an algebraic variety or an ideal we refer the reader to e.g. [13]). For zero-dimensional ideals, an exponential degree upper bound is known for the presentation problem [10]; also see [38]. Such an exponential degree upper bound also holds for complete intersections (the dimension of the algebraic variety defined by the g_i (in $\mathbb{C}^n$) is $n - w$), as shown in [4].

Another "easy" case is when the generators $g_1, \ldots, g_w \in \mathbb{Q}[x]$ are homogeneous. Then the question whether a general $f \in \mathbb{Q}[x]$ is an element of the ideal $(g_1, \ldots, g_w)$ can be solved by treating each homogeneous component of f separately. Hence, we may assume that f is homogeneous. In this case, $f \in (g_1, \ldots, g_w)$ iff $f(x) = \sum_{i=1}^{w} p_i g_i$ for homogeneous polynomials p_i with $\deg(p_i) = \deg(f) - \deg(g_i)$. Since a homogeneous polynomial in n variables and of degree d can consist of at most $\binom{n+d-1}{n-1}$ distinct monomials, the method of [41] again yields a PSPACE algorithm.

Finally, we present another lower bound, concerning PIMP restricted to homogeneous ideals.

Theorem 17 *The polynomial ideal membership problem, when restricted to homogeneous ideals, requires space $n^{\Omega(1)}$, and hence is PSPACE-complete.*

Proof: [Sketch] We merely sketch a proof here. Let M be any deterministic Turing machine with just one tape (functioning as input, work, and output tape), with the additional restriction that the tape head must never move outside the section of the tape initially occupied by the input (this variant is also called a (deterministic) linear bounded automaton (LBA)). Wlog we assume that the tape alphabet of M is $\{0,1\}$, and that M has unique accepting and rejecting final configurations. Let m be some input for M of length n. Construct a homogeneous instance of PIMP as follows. Let the set of indeterminates be $\{x_i, y_i, z_i;\ i = 1, \ldots, n\} \cup Q$, where Q is the set of states of the finite control of M. We use x_i and y_i to denote that the contents of the ith cell of M's tape contains a 0 (resp., a 1), and z_i to denote the fact that M's head is positioned over the ith tape cell. Then the initial configuration of M can be represented by a term τ over these indeterminates, and the unique final accepting configuration by some term τ'. Also, if we allow that each transition of M can also be reversed (*i.e.,* if we turn M from a semi-Thue system into a Thue system), the transition relation of this "symmetric" machine can be represented by a linear (in n) number of polynomials g_j in the above indeterminates, each of which is a difference of two terms. Each of these polynomials simply expresses the local change that occurs when M, with its head at some position i, executes one step (in forward or backward direction). Also, the polynomial $\tau' - \tau$ and the polynomials g_j are homogeneous, the g_j of degree say 3 and $\tau' - \tau$ of degree roughly n. Now,

$$M \text{ accepts } m \text{ iff } \tau' - \tau \text{ is in the ideal generated by the } g_j\,.$$

As already noted in [48], the fact that we have replaced the semi-Thue system underlying M by a Thue system does not hurt us since M was assumed to be deterministic. □

We also remark that the exponential space lower bound for PIMP also holds if we replace $\mathbb{Q}$ by an infinite field of finite characteristic, say 2. The reason is that the lower bound proof in [43] uses commutative semigroups or, equivalently, pure difference binomial ideals. Closer inspection also shows that even $+1$ and -1 need not be distinguishable, since the exponential space lower bound is actually obtained for the question whether, in a commutative semigroup, there is a derivation between some two given words. This setting also works in the case of finite characteristic. Note, however, that for the exponential space lower bound to hold, we must not add the Fermat polynomials $x_i^2 - x_i$ to the generators.

Even this restriction can be dropped in the homogeneous case discussed above. Based on the same reasoning, the PSPACE lower bound also holds for $\mathbb{Z}[x_1, \ldots, x_n]$.

6 Gröbner Bases and Reductions

It is not hard to see that binomial ideals have binomial reduced Gröbner bases, *i.e.,* each polynomial in such a basis is the difference of two terms (one of them possibly 1, corresponding to the empty word). Using the relationship of such ideals to (finitely presented) commutative semigroups, we immediately obtain the following lower bounds for Gröbner bases.

Theorem 18 *There are infinitely many $n > 0$ and a $d > 0$ ($d = 5$ suffices) such that for every such n, there is a generating set $g_1, \ldots, g_w$ (with w depending linearly on n), such that each g_i is a difference of two monomials, $\deg(g_i) \le d$, and there is a constant $c > 0$ (c is roughly $\frac{1}{2}$) such that* *(i) every Gröbner basis for* $(g_1, \ldots, g_w)$ *contains a polynomial of total degree* $\geq 2^{2^{c \cdot n}}$*; and*

(ii) every Gröbner basis for $(g_1, \ldots, g_w)$ *contains at least* $2^{2^{c \cdot n}}$ *elements.*

For a proof, also see [27].

Since we can always homogenize the generators of some ideal in $\mathbb{Q}[x_1, \ldots, x_n]$ introducing an additional indeterminate x_0, this double exponential lower bound for Gröbner bases also holds for homogeneous ideals.

Note that the exponential space lower bound implied by Theorem 18 already holds for pure difference binomial ideals (homogeneous or not), and hence of course also for general ideals. The bound also holds for finite characteristic, with the same provisions as mentioned above.

In terms of upper bounds, we now present two exponential space algorithms, one for binomial ideals, and one for the general case. We give a separate algorithm for the case of binomials since, even though both algorithms are exponential space, this one is much simpler and could be termed "combinatorial".

6.1 Computing Gröbner Bases for Binomial Ideals

We first consider pure difference ideals in $\mathbb{Q}[x_1, \ldots, x_n]$, *i.e.,* ideals with a basis in which each polynomial is a difference of two terms. Let $\mathcal{B}$ be such a binomial ideal in $\mathbb{Q}[x_1, \ldots, x_n]$. Given an admissible term ordering $\prec$, the reduced Gröbner basis is uniquely determined. We call a term $\tau \in \{x_1, \ldots, x_n\}^*$ *minimal reducible* iff its normal form $N(\tau)$, *i.e.,* the minimal (wrt $\prec$) term in $\tau + \mathcal{B}$, is strictly smaller (wrt $\prec$) than τ itself, and the term τ is minimal (wrt divisibility) with this property.

In [33], we show the

Theorem 19 *The reduced Gröbner basis of* $\mathcal{B}$ *with the term ordering* $\prec$ *consists exactly of all the binomials* $h - N(h)$*, where* h *is minimal reducible.*

Based on the degree bound from Theorem 7, we can, in exponential space, enumerate all binomials below this degree bound and check which ones satisfy the condition stated in the theorem.

For general binomial ideals, *i.e.,* ideals generated wlog by a finite set of polynomials each of which is the difference of a term and a monomial (with a coefficient from $\mathbb{Q}$, including 0), the situation becomes slightly more difficult since now cancellation of terms can occur, and since the coefficients can become extremely large (up to triple exponential in the input size). Nonetheless, as shown in [31] (also see [32]), there is still a very close relationship to the corresponding pure difference binomial ideal (where the coefficients in the basis binomials are replaced by 1 and -1, as appropriate). Once the terms in the binomials of the reduced Gröbner basis (of the general binomial ideal) are known, their coefficients can be determined in exponential space using the Chinese Remainder Theorem.

Theorem 20 *The reduced Gröbner basis of a binomial ideal can be computed in exponential space.*

6.2 Computing Reduced Forms and Gröbner Bases in General Polynomial Ideals

We now consider general polynomial ideals in $\mathbb{Q}[x_1, \ldots, x_n]$, together with some admissible term ordering $\prec$. As before, the term ordering is assumed to be represented by n linear forms with integer coefficients [51]. Let $\mathcal{I}$ be such an ideal, generated by the polynomials $g_1, \ldots, g_w \in \mathbb{Q}[x_1, \ldots, x_n]$, let d be an upper bound on the total degree of the g_i, and let $\prec$ be some given term ordering, with A an upper bound on the absolute value of the integer coefficients in the linear forms representing $\prec$.

In [36] (also see [37]), we show, based on an estimate originally given in [16], the following

Proposition 1 *Let $\mathcal{I}$, d, $\prec$ and A be as stated. Then the degree of the unique normal form of a given polynomial p wrt the given ideal $\mathcal{I}$ and the term order $\prec$ is bounded by $((2A(\frac{d^2}{2} + d)^{2^{n-1}} + 1)^n \deg(p))^{n+1}$.*

Based on this degree bound, we can use the construction given in [41] and [42] to reduce the question, whether a given term or polynomial is reducible modulo $\mathcal{I}$, to solving a linear system of equations with coefficients in $\mathbb{Q}$: The columns of the matrix correspond to the terms less than (wrt $\prec$) the given term (respectively, the leading term of the given polynomial) and, in terms of their degree, bounded by the quantity stated in the above Proposition. The rows of the matrix are determined by the Fundamental Theorem of Algebra stating that a (multivariate) polynomial over $\mathbb{Q}$ is identically zero iff all of its coefficients are zero. The dimensions of the resulting matrix are double exponential in the size of the input, hence we cannot afford to write this matrix down in storage. Computing its entries whenever they are needed, and using fast parallel algorithms for parallel rank computation ([28],[46]) and the relationship between parallel time and sequential space as expressed in the Parallel Computation Thesis [21], we can determine within exponential space whether a given term τ is minimal reducible, and, of course, also whether it is irreducible.

Using the above algorithm as a subroutine, we can determine the normal form $N(p)$ of a given polynomial p wrt the ideal $\mathcal{I}$ and the term ordering $\prec$ as follows: Using once again the degree bound from Proposition 1, we check whether there is a polynomial $p - \tilde{p}$ in $\mathcal{I}$, where $\tilde{p}$ contains just terms that are irreducible wrt $\mathcal{I}$. If such a $\tilde{p}$ exists, it is $N(p)$, and we can compute it using just exponential work space. For this, we again employ the Parallel Computation Thesis and efficient parallel algorithms for the solution of linear systems of equations ([14],[49],[6],[5],[47],[22]).

We thus obtain

Theorem 21 *Given the basis of an ideal $\mathcal{I}$, a term ordering $\prec$, and a polynomial p, the unique normal form of p wrt $(\mathcal{I}, \prec)$ can be computed in exponential space.*

Given a basis for some ideal $\mathcal{I}$ and an admissible term ordering, it is now quite straightforward to compute the uniquely determined reduced Gröbner basis of $\mathcal{I}$ wrt $\prec$: We just combine our algorithm for finding the minimal reducible terms τ with the normal form algorithm. The reduced Gröbner basis consists of the polynomials $\tau - N(\tau)$, with τ ranging over the minimal reducible terms.

Theorem 22 *Given the basis of an ideal $\mathcal{I} \subseteq \mathbb{Q}[x_1, \ldots, x_n]$ and a term ordering $\prec$, the unique reduced Gröbner basis of $\mathcal{I}$ wrt $\prec$ can be computed using exponential space.*

We have now presented several algorithms for computing (reduced) Gröbner bases of binomial resp. general polynomial ideals. While these algorithms are space optimal in the asymptotic sense, this does not mean, and we do not claim that they are practical. However, our algorithms are asymptotically space optimal (requiring workspace $2^{c \cdot n}$), whereas for instance Buchberger's algorithm, in the worst case, uses double exponential workspace.

7 Conclusion

In this survey, we have highlighted some of the connections between such different areas as the algebraic theory of multivariate polynomial ideals, elimination theory and complex function theory providing complexity bounds, algebraic geometry, and the very fundamental commutative semigroups. These interrelationships are quite intriguing since a large number of very basic complexity results for these structures has been obtained using these connections. And this maybe even more so, if one realizes that in several instances, a lower bound has been shown (how else?) using basical string rewriting techniques while matching upper bounds have been established using (sometimes quite elaborate and deep) techniques from analysis or complex function theory.

Another phenomenon that is quite indicative here and possibly typical for other practical areas (and computer algebra and Gröbner bases are being used in practice, even if quite often with some frustration and long waiting hours, as this author can attest to) could be the following: while the worst-case lower bounds for PIMP and Gröbner bases are terrible, seemingly precluding any application in practice, it turns out that much better (more "encouraging") bounds can be derived for the cases that really tend to occur in practical applications, like radical membership or regular intersections. And there are interesting developments to even characterize some *really* applicable cases (bounds better than PSPACE).

While such advances will be necessary in order to apply polynomial ideals in fields like robotics, motion planning, vision, modeling, constrained programming, and others, there also remain a few fundamental questions concerning complexity issues of polynomial ideals and related structures. One is to obtain explicit upper (and possibly better lower) bounds for ideals in $\mathbb{Z}[x]$ (or other nice and effective rings in place of $\mathbb{Z}$). So far, we just have the double exponential lower bounds from the word problem for commutative semigroups, and no explicit upper bounds. Another open problem is the complexity of the reachability problem for (general) Petri nets. While this complexity has been characterized for many subclasses of Petri nets, these subclasses are all so restricted that they are of little practical value. This means that we should try, on the one hand, to upper bound the complexity of the general Petri net reachability problem, but also to find characterizations of new subclasses of Petri nets which are of practical relevance and at the same time permit efficient solutions of basic problems like reachability, boundedness, or absence of deadlock. One might object that these goals are contradictory in themselves, since e.g. the reachability problem is already PSPACE-complete for 1-safe Petri nets, but this only says that *different* types of characterizations probably should be investigated, as the example of PIMP seems to indicate in a (slightly?) different area.

References

[1] Akira Aiba, Kô Sakai, Yosuke Sato, David J. Hawley, and Ryuzo Hasegawa. Con-

strained logic programming language CAL. In *Proceedings of the International Conference on Fifth Generation Computer Systems 1988 (Tokyo, Japan, November/December 1988)*, volume 1, pages 263–276. Institute for New Generation Computer Technology, ICOT, 1988.

[2] José Luis Balcázar, Josep Díaz, and Joaquim Gabarró. *Structural Complexity I*, volume 11 of *EATCS Monographs on Theoretical Computer Science*. Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong, 1988.

[3] David Allen Bayer. *The division algorithm and the Hilbert scheme.* Ph.d. thesis, Department of Mathematics, Harvard University, June 1982.

[4] Carlos Berenstein and Alain Yger. Bounds for the degrees in the division problem. *Michigan Math. J.*, 37(1):25–43, 1990.

[5] Stuart J. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Information Processing Letters*, 18(3):147–150, 1984.

[6] Allan Borodin, Joachim von zur Gathen, and John Hopcroft. Fast parallel matrix and GCD computations. *Information and Control*, 52:241–256, 1982.

[7] W. Dale Brownawell. Bounds for the degrees in the Nullstellensatz. *Ann. of Math.*, 126:577–591, 1987.

[8] Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal.* Ph.d. thesis, Department of Mathematics, University of Innsbruck, 1965.

[9] Bruno Buchberger. Gröbner bases: An algorithmic method in polynomial ideal theory. In N.K. Bose, editor, *Multidimensional systems theory*, pages 184–232. D. Reidel Publishing Company, Dordrecht-Boston-London, 1985.

[10] Léandro Caniglia, André Galligo, and Joos Heintz. Some new effectivity bounds in computational geometry. In *Proceedings of AAECC-6 (Roma, 1988)*, volume 357 of *LNCS*, pages 131–152, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1988. Springer-Verlag.

[11] E. Cardoza, R. Lipton, and A.R. Meyer. Exponential space complete problems for Petri nets and commutative semigroups. In *Proceedings of the 8th Ann. ACM Symposium on Theory of Computing (Hershey, PA)*, pages 50–54, New York, 1976. ACM, ACM Press.

[12] Edward W. Cardoza. Computational complexity of the word problem for commutative semigroups. Technical Memorandum TM 67, Project MAC, M.I.T., October 1975.

[13] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra.* Springer-Verlag, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1992.

[14] L. Csanky. Fast parallel matrix inversion algorithms. *SIAM Journal on Computing*, 5(4):618–623, 1976.

[15] Thomas W. Dubé. The structure of polynomial ideals and Gröbner bases. *SIAM J. Comput.*, 19:750–773, 1990.

[16] Thomas W. Dubé, B. Mishra, and C. K. Yap. Admissible orderings and bounds for Gröbner bases normal form algorithms. Technical Report 258, Department of Computer Science, Courant Institute of Mathematical Sciences, New York University, 1986.

[17] Samuel Eilenberg and M.P. Schützenberger. Rational sets in commutative monoids. *J. Algebra*, 13:173–191, 1969.

[18] David Eisenbud and Lorenzo Robbiano, editors. *Computational algebraic geometry and commutative algebra*, volume XXXIV of *Symposia Mathematica*. Cambridge University Press, Cambridge, 1993.

[19] David Eisenbud and Bernd Sturmfels. Binomial ideals, June 1994.

[20] Noaï Fitchas, André Galligo, and Jacques Morgenstern. Precise sequential and parallel complexity bounds for quantifier elimination over algebraically closed fields. *J. Pure Appl. Algebra*, 67:1–14, 1990.

[21] S. Fortune and J. Wyllie. Parallelism in random access machines. In *Proceedings of the 10th Ann. ACM Symposium on Theory of Computing (San Diego, CA)*, pages 114–118, New York, 1978. ACM, ACM Press.

[22] Zvi Galil and Victor Pan. Parallel evaluation of the determinant and of the inverse of a matrix. *Information Processing Letters*, 30:41–45, 1989.

[23] M. Giusti. Some effectivity problems in polynomial ideal theory. In John Fitch, editor, *Proceedings of the 3rd International Symposium on Symbolic and Algebraic Computation EUROSAM 84 (Cambridge, England, July 9-11, 1984)*, volume LNCS 174, pages 159–171, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong, 1984. ACM SIGSAM, SAME, Springer-Verlag.

[24] Marc Giusti, Joos Heintz, and Juan Sabia. On the efficiency of effective Nullstellensätze. *Comput. Complexity*, 3:56–95, 1993.

[25] Grete Hermann. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. *Math. Ann.*, 95:736–788, 1926.

[26] D.T. Huynh. The complexity of the equivalence problem for commutative semigroups and symmetric vector addition systems. In *Proceedings of the 17th Ann. ACM Symposium on Theory of Computing (Providence, RI)*, pages 405–412, New York, 1985. ACM, ACM Press.

[27] D.T. Huynh. A superexponential lower bound for Gröbner bases and Church-Rosser commutative Thue systems. *Inf. Control*, 68(1-3):196–206, 1986.

[28] Oscar H. Ibarra, Shlomo Moran, and Louis E. Rosier. A note on the parallel complexity of computing the rank of order n matrices. *Information Processing Letters*, 11:162, 1980.

[29] J. Kollár. Sharp effective Nullstellensatz. *J. Amer. Math. Soc.*, 1:963–975, 1988.

[30] Ulla Koppenhagen and Ernst W. Mayr. The complexity of the boundedness, coverability, and selfcoverability problems for commutative semigroups. Technical Report TUM-I9518, Institut für Informatik, Technische Universität München, May 1995.

[31] Ulla Koppenhagen and Ernst W. Mayr. An optimal algorithm for constructing the reduced Grbner basis of binomial ideals. Technical Report TUM-I9605, Institut für Informatik, Technische Universität München, January 1996.

[32] Ulla Koppenhagen and Ernst W. Mayr. An optimal algorithm for constructing the reduced Grbner basis of binomial ideals. In *Proceedings of the 1996 Int. Symposium on Symbolic and Algebraic Computation, ISAAC'96 (Zürich, 24–26 July 1996)*, pages 55–62, New York, 1996. ACM, ACM PRESS.

[33] Ulla Koppenhagen and Ernst W. Mayr. Optimal Grbner base algorithms for binomial ideals. Technical Report TUM-I9604, Institut für Informatik, Technische Universität München, January 1996.

[34] Ulla Koppenhagen and Ernst W. Mayr. The complexity of the equivalence problem for commutative semigroups. Technical Report TUM-I9603, Institut für Informatik, Technische Universität München, January 1996.

[35] Teresa Krick and Alessandro Logar. Membership problem, representation problem and the computation of the radical for one-dimensional ideals. In *Proceedings of Effective Methods in Algebraic Geometry (MEGA'90)*, volume 94 of *Progress in Mathematics*, pages 203–216, Boston-Basel-Berlin-Stuttgart, 1991. Birkhäuser Verlag.

[36] Klaus Kühnle and Ernst W. Mayr. Exponential space computation of Grbner bases. Technical Report TUM-I9606, Institut für Informatik, Technische Universität München, January 1996.

[37] Klaus Kühnle and Ernst W. Mayr. Exponential space computation of Grbner bases. In *Proceedings of the 1996 Int. Symposium on Symbolic and Algebraic Computation, ISAAC'96 (Zürich, 24–26 July 1996)*, pages 63–71, New York, 1996. ACM, ACM PRESS.

[38] Y.N. Lakshman. On the complexity of computing a grbner basis for the radical of a zero dimensional ideal. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing (Baltimore, Maryland, May 14–16, 1990)*, pages 555–563, New York, 1990. ACM Press.

[39] Daniel Lazard. Algèbre linéaire sur $K[X_1, \ldots, X_n]$ et élimination. *Bull. Soc. Math. France*, 105:165–190, 1977.

[40] Daniel Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In J.A. van Hulzen, editor, *Proceedings of the European Computer Algebra Conference, Eurocal '83 (London, England, March 1983)*, volume LNCS 162, pages 146–156, New York-Berlin-Heidelberg-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1983. Springer-Verlag.

[41] Ernst W. Mayr. Membership in polynomial ideals over $\mathbb{Q}$ is exponential space complete. In B. Monien and R. Cori, editors, *Proceedings of the 6th Annual Symposium on Theoretical Aspects of Computer Science (Paderborn, FRG, February 1989)*, volume LNCS 349, pages 400–406, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong, 1989. GI, afcet, Springer-Verlag.

[42] Ernst W. Mayr. Polynomial Ideals and Applications. *Mitteilungen der Mathematischen Gesellschaft in Hamburg*, XII(4):1207–1215, 1992. Festschrift zum 300jährigen Bestehen der Gesellschaft.

[43] Ernst W. Mayr and Albert Meyer. The complexity of the word problems for commutative semigroups and polynomial ideals. *Adv. Math.*, 46(3):305–329, December 1982.

[44] Marvin L. Minsky. *Computation: Finite and infinite machines.* Prentice-Hall, Englewood Cliffs, 1967.

[45] H.M. Möller and F. Mora. Upper and lower bounds for the degree of Groebner bases. In John Fitch, editor, *Proceedings of the 3rd International Symposium on Symbolic and Algebraic Computation EUROSAM 84 (Cambridge, England, July 9-11, 1984)*, volume LNCS 174, pages 172–183, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong, 1984. ACM SIGSAM, SAME, Springer-Verlag.

[46] Ketan Mulmuley. A fast parallel algorithm to compute the rank of a matrix over an arbitrary field. In *Proceedings of the 18th Annual ACM Symposium on Theory of Computing*, pages 338–339. ACM Press, 1986.

[47] V. Pan. Complexity of parallel matrix computations. *Theor. Comput. Sci.*, 54(1):65–85, September 1987.

[48] E. Post. Recursive unsolvability of a problem of Thue. *J. Symbolic Logic*, 12:1–11, 1947.

[49] F. P. Preparata and D. V. Sarwate. An improved parallel processor bound in fast matrix inversion. *Information Processing Letters*, 7(2):148–150, 1978.

[50] Fred Richman. Constructive aspects of Noetherian rings. In *Proceedings of the American Math. Society*, volume 44, pages 436–441, June 1974.

[51] Lorenzo Robbiano. Term orderings on the polynomial ring. In *Proceedings of the 10th European Conference on Computer Algebra, EUROCAL'85. Vol. 2: Research Contributions*, volume LNCS 204, pages 513–517, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1985. Springer-Verlag.

[52] A. Seidenberg. Constructions in algebra. *Trans. Am. Math. Soc.*, 197:273–313, 1974.

[53] Chee K. Yap. A new lower bound construction for commutative Thue systems, with applications. *J. Symbolic Comput.*, 12:1–28, 1991.

[54] Oscar Zariski and Pierre Samuel. *Commutative algebra. Volume I.* Van Nostrand Reinhold Company, New York-Cincinnati-Toronto-London-Melbourne, 1958. The University Series in Higher Mathematics.