T U M

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

On Polynomial Ideals, Their Complexity, and Applications

Ernst W. Mayr

TUM-I9520
Mai 1995

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-05-1995-I9520-350/1.-FI

Typescript: ---

Druck: Mathematisches Institut und
Institut für Informatik der
Technischen Universität München

On Polynomial Ideals, Their Complexity, and Applications

Ernst W. Mayr
Institut für Informatik
Technische Universität München
D-80290 München, GERMANY
e-mail: mayr@informatik.tu-muenchen.de

May 15, 1995

Abstract

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 over some ring, and the problem is to determine whether f is in the ideal generated by the g_i. For polynomials over the integers or rationals, it is known that this problem is exponential space complete. We discuss complexity results known for a number of problems related to polynomial ideals, like the word problem for commutative semigroups, a quantitative version of Hilbert's Nullstellensatz, and the reachability and other problems for (reversible) Petri nets.

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 constrained logic programming software systems, like [1].

The decidability of the membership problem for polynomial ideals over a field or ring can, in a sense, be traced back to ideas in Hilbert's work, and was established in [16], [34], and [33]. The computational complexity of the polynomial ideal membership problem was first discussed in [28] where the special case of the word problem for commutative semigroups was investigated. 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 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. 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 [19], and, for the case of special p, in *e.g.* [6], [2], [3], and [15].

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

2 Notation, 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 any subset I of $\mathbb{Q}[x]$ satisfying

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

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

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

A *monomial* m in $x_1, \ldots, x_n$ is a product of the form

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

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

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 monomial of f. The product $c_i \cdot x^{\alpha_i}$ is called the ith term of the polynomial f. The total degree of a polynomial is the maximum of the total degrees of its monomials.

Example: Consider $\mathbb{Q}[x_1, x_2]$, the ring of polynomials in x_1 and x_2 with rational coefficients. Then the ideal (x_1^2, x_2) consists of all polynomials $f \in \mathbb{Q}[x_1, x_2]$ such that each monomial of f is divisible by x_1^2 or by x_2.

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

1. $\alpha > (0, \ldots, 0)$ for all $\alpha \in \mathbb{N}^n - \{(0, \ldots, 0)\}$;
2. for all $\alpha, \beta, \gamma \in \mathbb{N}^n$,
$$\alpha < \beta \Rightarrow \alpha + \gamma < \beta + \gamma \,.$$

If $\alpha > \beta$, we say that any term $c \cdot x^\alpha$ is greater in the term ordering than any term $c' \cdot x^\beta$, and, for a polynomial $f(x) = \sum_{i=1}^{r} c_i \cdot x^{\alpha_i}$, we always assume that $\alpha_1 > \alpha_2 > \ldots > \alpha_n$. We call $LM(f) = x^{\alpha_1}$ the *leading monomial* and $LT(f) = c_1 \cdot x^{\alpha_1}$ the *leading term* 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 $<$ for the term ordering induced by the order $<$ on the degree vectors.

Example: Let $<$ 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

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

Then, in the term ordering,
$$x_1 > x_2 > x_3 > 1 \,,$$
and the leading term (and the leading monomial) of the polynomial

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

is x_1^5.

Example: Let $<$ 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

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

Then, in the term ordering,
$$x_1 > x_2 > x_3 > 1 \,,$$
the polynomial in the previous example is written

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

and its leading term is $x_1^2 x_2^4$.

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

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

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

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

Standard and Gröbner bases have been introduced in [17, 18] and [4]. For an excellent exposition of their numerous useful properties, also see [5]. 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 monomial 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 $I \subseteq \mathbb{Q}[x]$ is called *homogeneous*, if, whenever 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 $I \subseteq \mathbb{Q}[x]$ 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 power a monomial $x^\alpha \in \mathbb{Q}[x]$ can also be looked at as an element of $\{x_1, \ldots, x_k\}^*$.

A *commutative semi-Thue system* over S is given by a finite set $\mathcal{P}$ of productions $l_i \to r_i$, where l_i, $r_i \in S^*$. A word $m' \in S^*$ *is derived in one step* from $m \in S^*$ (written $m \to m'(\mathcal{P})$) applying the production $(l_i \to r_i) \in \mathcal{P}$ iff, for some $\tilde{m} \in S^*$, we have $m = \tilde{m} l_i$ and $m' = \tilde{m} r_i$. The word m *derives* m' iff $m \xrightarrow{*} m'(\mathcal{P})$, where $\xrightarrow{*}$ is the reflexive transitive closure of $\to$. A sequence $(m_0, \ldots, m_r)$ of words $m_i \in S^*$ with $m_i \to m_{i+1}(\mathcal{P})$ for $i = 0, \ldots, r-1$ is called a *derivation* (of length r) of m_r from m_0 in $\mathcal{P}$.

A *commutative Thue system* is a symmetric commutative semi-Thue system $\mathcal{P}$, *i.e.*,

$$(l \to r) \in \mathcal{P} \Rightarrow (r \to l) \in \mathcal{P}.$$

Clearly, commutative Thue systems and commutative semigroups are equivalent concepts.

Derivability in a (commutative) semigroup establishes a congruence $\equiv_{\mathcal{P}}$ on S^* by the rule

$$m \equiv m' \bmod \mathcal{P} \Leftrightarrow_{\text{def}} m \xrightarrow{*} m'(\mathcal{P}).$$

For semigroups, we also use the notation $l \equiv r \bmod \mathcal{P}$ to denote the pair of productions $(l \to r)$ and $(r \to l)$ in $\mathcal{P}$.

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 mod $\mathcal{P}$.

We remark that commutative semi-Thue systems appear in the literature in two additional equivalent formulations: *vector addition systems* (see next section) and *Petri nets*. Finitely presented commutative semigroups are equivalent to *reversible* vector addition systems or Petri nets. A reader more familiar with Petri nets may want to think of a vector in $\mathbb{N}^k$ as a marking.

2.3 Vector Addition Systems, Petri Nets, and Semilinear Sets

A *vector addition system (VAS)* is a pair (m, V), with $m \in \mathbb{N}^n$ and V a finite set $\{v_1, \ldots, v_r\}$ of vectors in $\mathbb{Z}^n$. The vector m is called the *start vector*, n is the dimension of the VAS, and the v_i are the *transitions*. A VAS is called *reversible*, if, whenever it contains a transition v, it also contains $-v$.

The *reachability set* of a VAS (m, V) is the smallest set $R(m, V)$ satisfying the following two properties:

(i) $m \in R(m, V)$;

(ii) whenever $z \in R(m, V)$, $v \in V$, and $z + v \in \mathbb{N}^n$ then $z + v \in R(m, V)$.

Thus, $R(m, V)$ is the smallest subset of $\mathbb{N}^n$ containing m which is closed under addition of transitions as long as the sum has only nonnegative components.

A *transition sequence* $\left(v^{(i)}\right)_{1 \le i \le t}$ of transitions $v^{(i)}$ is *applicable* to some vector $m' \in \mathbb{N}^n$ if $m' + \sum_{j=1}^{i} v^{(j)} \in \mathbb{N}^n$ for all $i = 1, \ldots, t$. In this case, the vector $m'' = m' + \sum_{j=1}^{t} v^{(j)}$ is called *reachable from y in (x, V)*, and the transition sequence is called a *derivation* (of length t) of m'' from m'. For this property, we also use the notation $m' \xrightarrow{*} m''\ (V)$.

Clearly, reversible VASs can be simulated by commutative semigroups (the other direction is also possible, though not directly; the probably simplest way is to replace vector addition systems by *vector replacement systems (VRS)*). For an n-dimensional reversible VAS (m, V) we use a commutative semigroup with n generators $s_1, \ldots, s_n$, and a congruence $l \equiv r$ for every pair $\{v, -v\} \subseteq V$, with

$$\begin{aligned} l &= s_1^{\max\{0, v_1\}} \cdots s_n^{\max\{0, v_n\}} \\ r &= s_1^{\max\{0, -v_1\}} \cdots s_n^{\max\{0, -v_n\}}, \end{aligned}$$

where $v = (v_1, \ldots, v_n) \in \mathbb{Z}^n$.

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 [11]) 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 $\mathbb{N}^n$.*

For a reversible VAS (m, V) this theorem says that the reachability set $R(n, V)$ is a uniformly semilinear set.

Petri nets [31] are a graphical representation of VASs and VRSs, equivalent to VRSs. A marked Petri net P consists of

(i) a finite bipartite multi-digraph (S, T, F), with

  (a) $S = \{s_1, \ldots, s_n\}$ the set of *places*,

  (b) $T = \{t_1, \ldots, t_r\}$ the set of *transitions*, and

  (c) $F : S \times T \cup T \times S \to \mathbb{N}$ giving the multiplicity of the arcs;

(ii) and an *initial marking* $m \in \mathbb{N}^n$.

A transition $t \in T$ is said to be *enabled* at some marking $m' \in \mathbb{N}^n$ if

$$m'_i \geq F(s_i, t) \text{ for all } i,\ i = 1, \ldots, n\,.$$

If t is enabled at m', it can (but does not have to) fire, producing the new marking m'' with

$$m''_i = m'_i - F(s_i, t) + F(t, s_i) \text{ for all } i,\ i = 1, \ldots, n\,.$$

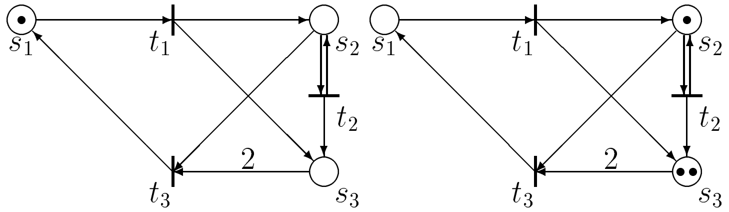
We also write $m' \xrightarrow{t} m''$. Note that $m'' \in \mathbb{N}^n$.

The *reachability set* $R(P)$ with initial marking m is the smallest subset of $\mathbb{N}^n$ containing m which is closed under $\xrightarrow{t}$ for all $t \in T$.

A Petri net is called *reversible* if, for every transition t, it contains a transition t^{rev} with

$$F(s, t) = F(t^{rev}, s) \text{ and } F(t, s) = F(s, t^{rev}) \text{ for all } s \in S\,.$$

The following figure shows a simple example of a Petri net. The places are depicted by circles, the transitions by bars, the marking of each place by a corresponding number of dots.



The marking shown on the right is obtained from that on the left by firing t_1 and then t_2. If we make this Petri net reversible by adding transitions t_i^{rev}, for $i = 1, 2, 3$, we obtain a reversible Petri net which is equivalent, as can easily be seen, to a commutative semigroup with generators s_1, s_2, s_3 and the following congruences:

$$\begin{aligned} s_1 &\equiv s_2 s_3 \\ s_2 &\equiv s_2 s_3 \\ s_2 s_3^2 &\equiv s_1 \end{aligned}$$

3 Basic Problems and Their Complexity

In this section, we are going to consider some of the very basic and fundamental algorithmic problems 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*

$$m \equiv m' \bmod \mathcal{P}\,;$$

(ii) **Representation Problem:** *Given $S, \mathcal{P}, m$, and m' as input, decide whether $m \equiv m' \bmod \mathcal{P}$, 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 $I = (g_1, \ldots, g_w)$.*

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

$$f \in I\,;$$

(ii) **Representation Problem:** *Given $f, g_1, \ldots, g_w$, decide whether $f \in I$, 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., [8]) 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

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

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

In the fundamental paper [16], 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 [34] and [28].

In [7] and [28] 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 [26, 27], this exponential space upper bound 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 ([14]) and techniques from [30], 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 g_i. This is crucial, since, as we shall see below, their total length can be double exponential in the size of the input. For a detailed proof of these two theorems, see [26].

While the exponential space bound in [26] is based on the classical construction in [16], 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 7 *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 $\deg(p_i) \leq \mu n d^{\mu} + \mu d$, with $\mu = \min\{n, w\}$.

Using the so-called "Rabinowitsch trick", Brownawell also obtained

Theorem 8 *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 [2], [3], and [21]. The method of [26] immediately yields

Corollary 8.1 *Whether*

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

can be tested in PSPACE.

Corollary 8.2 *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., [36]), one variant of which is

Theorem 9 (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 $I = (g_1, \ldots, g_w) \subseteq \mathbb{Q}[x]$ 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. [9]). For zero-dimensional ideals, an exponential degree upper bound is known for the presentation problem [6]. 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 [2].

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 [26] again yields a PSPACE algorithm.

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. [12] for a rather comprehensive survey). From the numerous complexity result, we would like to mention the following:

Theorem 10 *Let $I = (g_1, \ldots, g_w) \subseteq \mathbb{Q}[x_1, \ldots, x_n]$ be an ideal, let d be the maximal total degree of the g_i, $i = 1, \ldots, w$, and let $<$ be any admissible ordering on $\mathbb{Q}[x]$. Then the reduced Gröbner basis for 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 [10].

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 [16].

Theorem 11 *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 [16] and [10].

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 [28]:

Theorem 12 *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 [29], this result implies [26]:

Theorem 13 *The uniform word problem for finitely presented commutative semigroups requires exponential space, and, together with the matching upper bound, is therefore exponential space complete.*

Since the word problem for commutative semigroups is a special case of PIMP (the corresponding ideals are also called *binomial ideals*, see [13]), we also obtain an exponential space lower bound (and thus completeness for exponential space) for PIMP. The construction in [28] has been sharpened in [35] (which greatly improves the constant in the exponent from 1/14 to basically 1/2) to yield the following lower bounds:

Theorem 14 *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

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

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. Using the relationship of such ideals to (finitely presented) commutative semigroups, we immediately obtain the following lower bounds for Gröbner bases.

Theorem 15 *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, $\deg(g_i) \leq d$, 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 [20].

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

Finally, we present a PSPACE lower bound for PIMP restricted to homogeneous ideals.

Theorem 16 *The polynomial ideal membership problem, when restricted to homogeneous ideals, requires space $n^{\Omega(1)}$, and hence is PSPACE-complete.*

Proof: We merely sketch a proof here. Let M be any deterministic LBA. Wlog we assume that the tape alphabet of M is $\{0, 1\}$, and that M has a unique accepting and rejecting final configuration. 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 monomial $\tilde{m}$ over these indeterminates, and the unique final accepting configuration by some monomial $\tilde{m}'$. 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 monomials. 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 $\tilde{m}' - \tilde{m}$ and the polynomials g_j are homogeneous, the g_j of degree say 4 and $\tilde{m}' - \tilde{m}$ of degree roughly n. Now,

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

As already noted by [32], 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.

4 Commutative Semigroups and Petri Nets

As we have seen in the previous section, many lower bounds for problems in polynomial ideals arise from lower bounds for the word problem for commutative semigroups. In this section, we would like to present some upper bounds for commutative semigroup problems which are derived from the double exponential upper bound for the degree of Gröbner bases [10].

An immediate consequence of the Gröbner bases degree bound is

Theorem 17 *Let $\mathcal{P}$ be a finite set of congruences on S^*, $S = \{s_1, \ldots, s_n\}$, let $m \in S^*$ and assume that $b \in [m]$, b minimal wrt the subword ordering (or, equivalently, when interpreted as element of $\mathbb{N}^n$, minimal wrt the standard partial ordering of $\mathbb{N}^n$). Then there is a double exponential upper bound for the length of b.*

With this bound, we can sharpen the upper bound given in [19] for the equivalence problem for commutative semigroups:

Theorem 18 *The equivalence problem for commutative semigroups can be decided in exponential space. It is also exponential space complete.*

As shown in [22], we also get the following exponential space complexity bounds from the results in [28] and [26].

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 [22] 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 [28] actually proves the following, slightly stronger statement:

Theorem 19 *There is an infinite family of commutative semigroup word problems $(m, m', \mathcal{P})$ 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.

As we have already seen, finitely generated commutative semigroups are equivalent to reversible Petri nets. Therefore, the exponential space lower bound given in [28] improves upon Lipton's original lower bound of $2^{\Omega(\sqrt{n})}$ for the Petri net (or VAS, or VRS) reachability problem [23]. Decidability of this problem has first been established in [24, 25], by means of an algorithm whose complexity is non-primitive recursive, and since then no improvements have been obtained.

From our earlier discussion, it should be clear that the general Petri net reachability problem is equivalent to a version of a (binomial) ideal membership problem where we require that the coefficient polynomials p_i are from the semiring $\mathbb{N}[x]$ (or $\mathbb{Q}^+[x]$, for that matter). However, so far and to the knowledge of this author, this interpretation has not provided any essential insights.

5 Open Problems, 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, the very fundamental commutative semigroups, and models used in computer science for representing parallel and concurrent processes, like vector addition systems or Petri nets. 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 basically string rewriting techniques while matching upper bounds can be 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 instead of $\mathbb{Z}$). So far, we just have the doubly exponential lower bounds from the word problem for commutative semigroups, and no explicit upper bounds. Another is the complexity of the reachability problem for (general) Petri nets. While this complexity has been characterized for many subclasses of Petri nets, these are all so restricted as of being 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, 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. Constrained 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] Carlos Berenstein and Alain Yger. Bounds for the degrees in the division problem. *Michigan Math. J.*, 37(1):25–43, 1990.

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

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

[5] 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.

[6] 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.

[7] 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.

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

[9] 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.

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

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

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

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

[14] 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.

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

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

[17] Heisuke Hironaka. Resolution of singularities of an algebraic variety over a field of characteristic zero: I. *Ann. of Math.*, 79(1):109–203, 1964.

[18] Heisuke Hironaka. Resolution of singularities of an algebraic variety over a field of characteristic zero: II. *Ann. of Math.*, 79(2):205–326, 1964.

[19] 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.

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

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

[22] 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.

[23] Richard Lipton. The reachability problem requires exponential space. Research Report 62, Computer Science Dept., Yale University, January 1976.

[24] Ernst W. Mayr. An algorithm for the general Petri net reachability problem. In *Proceedings of the 13th Ann. ACM Symposium on Theory of Computing (Milwaukee, WI)*, pages 238–246, New York, 1981. ACM, ACM Press.

[25] Ernst W. Mayr. An algorithm for the general Petri net reachability problem. *SIAM J. Comput.*, 13(3):441–460, August 1984.

[26] 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.

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

[28] 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.

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

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

[31] C.A. Petri. Kommunikation mit Automaten. Technical Report 2, Institut für Instrumentelle Mathematik, Bonn, 1962.

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

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

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

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

[36] 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.