Some Complexity Results for Polynomial Ideals

Ernst W. Mayr
Technical University Munich
http://wwwmayr.informatik.tu-muenchen.de/

Outline:

1. Basic concepts
2. Statement of results
3. Computing normal forms in exponential space
4. Application to Gröbner basis computation
5. Further results, applications
6. Conclusion and open problems

Polynomial Ideals

Given: A finite set of polynomials

$$p_1, \ldots, p_h \in \mathbb{Q}[x_1, \ldots, x_n]$$

and a test polynomial p.

The ideal

$$\langle p_1, \ldots, p_h \rangle$$

generated by the p_i is the set of all polynomials q which can be written

$$q = \sum_{i=1}^{h} g_i p_i$$

with polynomials $g_i \in \mathbb{Q}[x_1, \ldots, x_n]$.

Binomial polynomials are polynomials which are the difference of two *monomials*.

The Polynomial Ideal Membership Problem — PIMP

Let polynomials $p, p_1, \ldots, p_h \in \mathbb{Q}[x_1, \ldots, x_n]$ be given.

Decision problem:

$$\boxed{\text{Is } p \in \langle p_1, \ldots, p_h \rangle\text{?}}$$

Representation problem:

$$\boxed{\text{Determine } g_i \in \mathbb{Q}[x_1, \ldots, x_n] \text{ such that } p = \sum_{i=1}^{h} g_i p_i.}$$

A Small Example

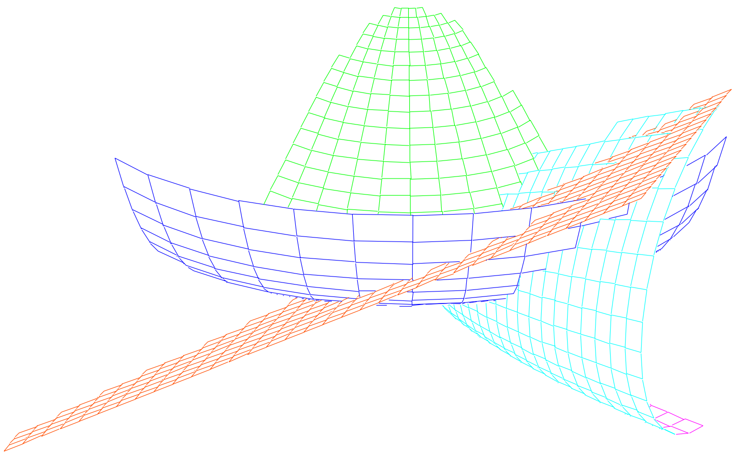
Consider the ideal generated in $\mathbb{R}^3$ by the polynomials

p_1: $z^2 - 8z - 13/10x + y^2 + 16$,

p_2: $z - 2x^4 - 4y^2x^2 + 4x^2 - 2y^4 + 4y^2 - 5$, and

p_3: $z - x - 3$.

Graph of functions in example



Term Orderings

Admissible term ordering:

(i) $x_{\pi(1)} \succ x_{\pi(2)} \succ \ldots \succ x_{\pi(n)} \succ 1$

(ii) Let m, m_1, m_2 be terms with $m_1 \prec m_2$. Then

$$mm_1 \prec mm_2 \, .$$

Examples:

1. lex: $x_1^2 \succ x_1 x_2^3 x_3^5$
2. grevlex: $x_2^3 \succ x_1$ und $x_1 x_2 x_3 \succ x_1 x_3^2$

Gröbner Basis Definition

Definition: Let I be an ideal in $\mathbb{Q}[x] = \mathbb{Q}[x_1, \ldots, x_n]$, and $\prec$ an admissible term ordering. A set $\{g_1, \ldots, g_r\}$ of polynomials in I is a Gröbner basis for I (wrt. $\prec$) if

> $\{LT(g_1), \ldots, LT(g_r)\}$ is a basis of the leading term ideal of I, *i.e.,* the smallest ideal containing the leading term $LT(f)$ of every $f \in I$.

Another Small Example

Using the basis

$$\{-x^3 + y, x^2y - z, 1 - v(xy^3 - z^2 + y^5 - z^3)\} \ ,$$

with any term ordering,

our favorite symbolic algebra package computes the following Gröbner basis:

$$1$$

This example highlights the so-called Rabinovich trick, establishing that some power of $xy^3 - z^2 + y^5 - z^3$ is in $\langle -x^3 + y, x^2y - z\rangle$.

Why Gröbner Bases?

1. Given some ideal I together with an admissible term ordering $\prec$, the reduced Gröbner basis for $(I, \prec)$ is uniquely determined and hence represents a normal form for I.

2. Given I and $\prec$ as before, and some polynomial $p \in \mathbb{Q}[x_1, \ldots, x_n]$, we can use the polynomials in a Gröbner basis for $(I, \prec)$ and the polynomial division algorithm to determine the normal form of p modulo I, i.e., the wrt. $\prec$ minimal polynomial in $p + I$.

Some Previous Work

— Decidability: Hilbert [1890], G. Hermann [1926]

for rings: Seidenberg [1974], Richman [1974]

— doubly exponential degree bound with coefficients in $\mathbb{Q}$: Hermann [1926]

— exponential degree bound for special p: Brownawell[1987], Heintz et al.[1988], Berenstein/Yger [1988]

— doubly exponential degree lower bound for PIMP: Mayr/Meyer [1982]

— doubly exponential degree lower bound for Gröbner bases: Huynh[1986]

— exponential space upper bound for the general word problem, with coefficients in $\mathbb{Q}$: Mayr [1988]

— doubly exponential upper degree bound for Gröbner bases: Giusti [1984], Dubé [1990]

Thus:

— Gröbner bases can be doubly exponentially large.

— Coefficients therein may become triply exponentially large (in value).

— The space requirement for computing normal forms of polynomials using Gröbner bases is doubly exponential.

— Upper bounds are known only for special cases (0 or 1-dimensional, unmixed ideals: Lazard [1983], Caniglia/Galligo/Heintz [1989], Krick/Logar [1991], . . .

— Many known upper bounds are in terms of the arithmetic model.

Our Main Results

Theorem: *Let I be some ideal in $\mathbb{Q}[x_1, \ldots, x_n]$, given via some basis $p_1, \ldots, p_w$, and let $\prec$ be some given admissible term order. Then*

1. *for any given $p \in \mathbb{Q}[x_1, \ldots, x_n]$, the normal form of p wrt $(I, \prec)$ can be computed within exponential space*

2. *the uniquely determined reduced Gröbner basis of I wrt $\prec$ can be computed within exponential space.*

Note: Our machine model is the multitape Turing machine.

Representation of Term Orderings

Any term order can be represented by a collection of n weight functions $W_1, \ldots, W_n$ assigning a real number to every term such that

$$u \prec v \Leftrightarrow \exists k : W_k(u) < W_k(v) \wedge \forall i < k : W_i(u) = W_i(v)$$

where the weight functions are defined by

$$W_i(\prod_{j=1}^{n} {x_j}^{e_j}) := \sum_{j=1}^{n} w_{ij} e_j$$

with w_{ij} nonnegative real numbers [Robbiano 1985].

An Example

In the polynomial ring $\mathbb{Q}[x, y, z]$, the term order $\prec$ given by the 9 rational weights

$$\begin{pmatrix} w_{1,x} & w_{1,y} & w_{1,z} \\ w_{2,x} & w_{2,y} & w_{2,z} \\ w_{3,x} & w_{3,y} & w_{3,z} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 3 & 1 \\ 1 & 2 & 2 \end{pmatrix}$$

implies for example $xyz \prec x^2y^2 \prec x^3y \prec z^3 \prec x^2yz$.

A Degree Bound for the Normal Form

By combining the weight functions to a valuation of polynomials that decreases in every step of the Gröbner basis reduction one can bound the number of these steps [Dubé/Mishra/Yap 1986].

In our case, the length of a reduction is doubly exponential.

In every reduction step the degree will increase by at most the degree of the polynomial in the Gröbner basis used in this step.

The degrees of the polynomials in the reduced Gröbner basis are doubly exponential [Dubé 1990].

$$\Downarrow$$

The degree of the normal form is at most doubly exponential in the input size.

Finding the Normal Form

Find the smallest (wrt the term order) $\bar{p}$ in the coset of p, i.e., the smallest solution to

$$p - \bar{p} = \sum_{i=1}^{w} c_i p_i \ .$$

Any such representation can be chosen such that the degrees of the c_i are doubly exponentially bounded [Hermann 1926].

Therefore we can write out all polynomials as sums of their monomials (with unknown coefficients in the case of $\bar{p}$ and the c_i), expand and compare coefficients.

We thus get at most doubly exponentially many linear equations in at most doubly exponentially many unknowns in the field $\mathbb{Q}$, i.e., a matrix equation of doubly exponential format.

An Example

Let the ideal $I = \langle x^2 + 3xy, \quad xy - 1 \rangle \trianglelefteq \mathbb{Q}[x, y]$, the lexicographic term order with $x \succ y$ and the polynomial $p = x$ be given.

We want to calculate $\bar{p} = \mathrm{NF}(p)$. To this end, we solve $p = \bar{p} + b(x^2 + 3xy) + c(xy - 1)$ for $\bar{p}$.

Instead of something like 10^9, we assume a bound of 1 on the degrees of $\bar{p}$, b and c, and thus write

$$\begin{aligned} x = & \quad r_1 + r_y y + r_x x \\ & + \quad (b_1 + b_y y + b_x x)(x^2 + 3xy) \\ & + \quad (c_1 + c_y y + c_x x)(xy - 1) \end{aligned}$$

Expanding and comparing coefficients yields the following system of equations:

$$x = r_1 + r_y y + r_x x \; + (b_1 + b_y y + b_x x)(x^2 + 3xy) \; + (c_1 + c_y y + c_x x)(xy - 1)$$

$$\begin{array}{rrllllll}
(1) & 0 = & r_1 & & & & -c_1 & & \\
(y) & 0 = & & r_y & & & & -c_y & \\
(x) & 1 = & & & r_x & & & & -c_x \\
(xy) & 0 = & & & 3b_1 & & +c_1 & & \\
(xy^2) & 0 = & & & & 3b_y & & +c_y & \\
(x^2) & 0 = & & & b_1 & & & & \\
(x^2y) & 0 = & & & & b_y \;\; +3b_x & & & +c_x \\
(x^3) & 0 = & & & & \;\;\;\;\; b_x & & &
\end{array}$$

After simplification, we are left with the system

$$\begin{aligned}
0 &= r_y \quad && - c_y \\
1 &= r_x && - c_x \\
0 &= 3b_y && + c_y \\
0 &= b_y && + c_x
\end{aligned}$$

whose solution is not unique.

Since we are interested in the minimal (wrt the term order) solution, we set the coefficient of the largest term of the solution to zero, i.e., $r_x = 0$.

Now we obtain a unique solution with $c_x = -1$, $b_y = 1$, $c_y = -3$ and $r_y = -3$.

Hence, $\bar{p} = \mathrm{NF}(x) = -3y$.

What about the Space Complexity?

Why not just solve this matrix equation with appropriate choice of pivots to get the minimal solution?

The format of our matrix is doubly exponential. We cannot afford to write it down if we want to use only exponential (work) space.

But we can compute each entry of the matrix in exponential space.

So, we just recompute every entry each time it is needed during the matrix calculation, instead of reading it from store.

Note that this still does not allow extensive storage of intermediate results as e.g. in Gaussian elimination.

How to Solve the Matrix Equation?

We specify a maximal regular minor of our matrix by giving a method to decide for any given row or column whether it is in the minor.

- This is done by comparing the ranks of a certain submatrix with and without that row or column.
- The proper choice of the submatrices ensures that the resulting regular minor will yield the minimal solution wrt the term order.

Then we solve the matrix equation corresponding to this regular minor by Cramer's rule (except that, again, we cannot write down the minor, but have to recompute it over and over).

Characterization of Gröbner Bases

We will call a term minimally reducible, if it is not in normal form but all its divisors are.

Note that all divisors are in normal form if and only if the at most n maximal divisors (those where the exponent vectors are smaller by one in exactly one place and equal in all others) are.

The reduced Gröbner basis wrt an ideal and a term order is unique and consists of all polynomials which are the difference of a minimally reducible term and its normal form.

Computation of the Gröbner Basis

Enumerate all terms up to the degree bound for Gröbner bases (exponential space) and proceed with all these terms, one at a time, as follows:

- Check whether the term is minimally reducible.
- If so, calculate the normal form of the term and output the difference of the term and its normal form.
  (All normal form calculations take exponential space that can be reused)

The entire Gröbner basis computation can be done in exponential space.

Further Results

1. Exponential space bounds also result for many operations on ideals.
2. We obtain PSPACE algorithms for cases where exponential degree bounds hold for Gröbner bases.
3. The exponential space lower bound already holds for pure difference binomial ideals.
4. All bounds also hold for nonzero characteristic (infinite fields).
5. The subword reachability problem for commutative semigroups is in EXPSPACE.
6. The equivalence problem for finitely generated commutative semigroups can be solved in exponential space.

Finitely Presented Commutative Semigroups

Given:

1. finite set X of symbols, commutative
2. finite set $\mathcal{P}$ of congruences $l_i \equiv r_i;\ 1 \leq i \leq h;\ l_i, r_i \in X^*$
3. two words $u, v \in X^*$.

The (Uniform) Word Problem:

$$\boxed{\text{Is} \quad u \equiv v \bmod \mathcal{P} \quad ?}$$

I.e., is there a derivation $u = w_0 \Rightarrow w_1 \Rightarrow \ldots \Rightarrow w_n = v$, where each $w_i = w_i' l_{j_i}$ and $w_{i+1} = w_i' r_{j_i}$ (resp., $w_i = w_i' r_{j_i}$ and $w_{i+1} = w_i' l_{j_i}$).

A Small Example

Given:

$$
\begin{aligned}
X &= \{x, y, z\} \\
\mathcal{P} &= \{x^2 \equiv y, \quad y^2 z \equiv z\}
\end{aligned}
$$

Then we have:

$$x^4 z \equiv x^2 yz \equiv y^2 z \equiv z \ ,$$

$$x^7 y^3 z \equiv x^7 yz \equiv x^5 y^2 z \equiv x^5 z \equiv xz \ ,$$

but

$$x^4 \not\equiv \lambda \ .$$

Semilinear Sets

Definition:

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

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

3. 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 [Eilenberg-Schuetzenberger/69] the following

Theorem: *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 (finitely presented) commutative semigroup $\mathcal{P}$ this theorem says that each congruence class $[u]_{\mathcal{P}}$ is a uniformly semilinear set.

A Few More Known Facts about CSG's and the Equivalence Problem

1. The (uniform) word problem is EXPSPACE-complete [Mayr-Meyer/82], where

$$\text{EXPSPACE} = \bigcup_{c>0} \text{SPACE}(2^{c \cdot n}) \; .$$

2. The equivalence problem is decidable in space $O(2^{c \cdot n \cdot \log n})$ [Huynh/85].
3. The equivalence problem is EXPSPACE-hard.
4. Finitely presented commutative semigroups correspond to reversible Petri nets in a straightforward manner.

The Subword Reachability Problem for CSG's

Let $X = \{x_1, \ldots, x_k\}$, $X_{v_1} = \{x_1, \ldots, x_l\}$ with $l \leq k$, $v_1 \in X_{v_1}^*$, and $X_{\overline{v_1}} = X - X_{v_1}$. Let also Y and Z be defined as follows:

$$\overbrace{x_1, \ldots, x_{l_1-1}, \; x_{l_1}, \ldots, x_l,}^{X_{v_1}} \; \overbrace{x_{l+1}, \ldots, x_{l_2}, \; x_{l_2+1}, \ldots, x_{l_3-1}, \; x_{l_3}, \ldots, x_k}^{X_{\overline{v_1}}}$$

$$Y = \underbrace{x_{l_1}, \ldots, x_l, \; x_{l+1}, \ldots, x_{l_2}}_{Y}, \qquad Z = \underbrace{x_{l_3}, \ldots, x_k}_{Z}$$

Definition: The subword reachability problem is: Given $X, \mathcal{P}, u, v_1, Y,$ and Z, decide whether there is some $v_2 \in [u]_{\mathcal{P}}$ such that

$$v_2 = v_1 \cdot x_{l_1} \cdots x_{l_2} \cdot w \text{ for some } w \in (Y \cup Z)^* \; .$$

Theorem: *Let $X = \{x_1, \ldots, x_k\}$, and $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$ be a commutative semigroup presentation over X. Then there is an algorithm which decides for any two words u, $v_1 \in X^*$, and sets Y, $Z \subseteq X$ defined as above whether there is a $v_2 \in [u]_{\mathcal{P}}$ such that $v_2 = v_1 \cdot v \cdot w$, where $v = x_{l_1} \cdots x_{l_2}$ if $Y = \{x_{l_1}, \ldots, x_{l_2}\}$ (resp., $v = \varepsilon$ if $Y = \emptyset$), using at most space $(\mathrm{size}(u, v_1, \mathcal{P}))^2 \cdot 2^{\bar{c} \cdot k} \leq 2^{c \cdot \mathrm{size}(u, v_1, \mathcal{P})}$ for some constants $\bar{c}$, $c > 0$ independent of u, v_1 and $\mathcal{P}$.*

Corollary: *The subword problem for commutative semigroups is exponential space complete with respect to log-lin reducibility.*

The proof of the theorem is based on a reduction to a Gröbner basis construction problem, selecting an appropriate term ordering depending on the subdivision of X.

The Finite Enumeration Problem

Let $\mathcal{P}$ be a finite commutative semigroup presentation over some alphabet X, and $u \in X^*$ a word such that the congruence class of u is bounded. Then the finite enumeration problem is the problem of generating a complete list of all the elements in $[u]_{\mathcal{P}}$.

Theorem: *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$ be a finite commutative semigroup presentation over X, and $u \in X^*$ a word such that the congruence class of u is bounded. Then there is an algorithm which generates the elements of $[u]_{\mathcal{P}}$ using at most space $(\mathrm{size}(u, \mathcal{P}))^2 \cdot 2^{\bar{c} \cdot k} \le 2^{c \cdot \mathrm{size}(u, \mathcal{P})}$, where $\bar{c}$, $c > 0$ are some constants independent of u and $\mathcal{P}$.*

Proof Sketch

We introduce $2k+3$ new variables m, s, t, $y_1, \ldots, y_k$, and $z_1, \ldots, z_k$. Let $X' = X \cup \{m, s, t, y_1, \ldots, y_k, z_1, \ldots, z_k\}$. Given $\mathcal{P}$ and the word $u \in X^*$, we construct a new commutative semigroup presentation $\mathcal{P}'$ over X' as follows: $\mathcal{P}'$ contains the congruences

$$\begin{aligned} s \cdot x_j &\equiv s \cdot y_j \cdot z_j, \quad \text{for} \quad j = 1, \ldots, k, & (1) \\ s \cdot y(u) &\equiv t, & (2) \\ s \cdot u &\equiv m, & (3) \end{aligned}$$

and, for every congruence $l_i \equiv r_i$ in $\mathcal{P}$, the congruences

$$\begin{aligned} s \cdot y(l_i) &\equiv s \cdot y(r_i), \quad \text{and} & (4) \\ t \cdot z(l_i) &\equiv t \cdot z(r_i). & (5) \end{aligned}$$

Also, let $\prec$ be a term ordering satisfying

$$m \prec a \prec s \prec b$$

for all $a \in \{x_1, \ldots, x_k\},\ b \in \{t, y_1, \ldots, y_k, z_1, \ldots, z_k\}$.

Lemma:

$$v \in [u]_{\mathcal{P}} \text{ \textit{iff} } m - sv \in \text{ the reduced Gröbner basis}$$

The Equivalence Problem

Theorem: *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^*, i \in I_h\}$ be a finite commutative semigroup presentation over X, and let $u \in X^*$. Then there is an algorithm which generates a closed representation of $[u]_\mathcal{P}$ using at most space $2^{c \cdot \mathrm{size}(u,\mathcal{P})}$, where $c > 0$ is some constant independent of u and $\mathcal{P}$.*

Theorem:

Let $\mathcal{P}$, $\mathcal{Q}$ be two finite commutative semigroup presentations over $X = \{x_1, \ldots, x_k\}$, and let u, v be two words in X^*. Then there is an algorithm which decides whether $[u]_\mathcal{P}$ is equal to $[v]_\mathcal{Q}$ using at most space $2^{c \cdot \max\{\mathrm{size}(u,\mathcal{P}),\mathrm{size}(v,\mathcal{Q})\}} \leq 2^{c \cdot \mathrm{size}(u,v,\mathcal{P},\mathcal{Q})}$, where c is some constant independent of u, v, $\mathcal{P}$ and $\mathcal{Q}$.

Sketch of Proof

1. We show that the minimal elements of the uniformly semilinear congruence class have norm bounded by $2^{2^{c \cdot n}}$.

2. We show an analogous bound for the periods of the congruence class.

For determining the minimal elements, we first project the congruence class onto the bounded coordinates and then use the algorithm for the subword reachability problem in commutative semigroups [Koppenhagen-Mayr/96]. The bounded coordinates can be found using an exponential space algorithm for the coverability problem [Koppenhagen-Mayr/95].

Conclusion, Open Problems

Amazingly, for many problems, the richer structure of polynomial rings, as compared to commutative semigroups, does not cause any marked increase for the complexity of these problems.

Open problems:

1. Which properties of ideals make PIMP simpler?
2. Investigate the complexity of polynomial ideals with integer coefficients!
3. Investigate the complexity of polynomial ideals over finite fields!
4. Determine the complexity of the Petri net reachability problem ($\equiv$ coefficients in $\mathbb{N}$ or $\mathbb{Q}^+$)!