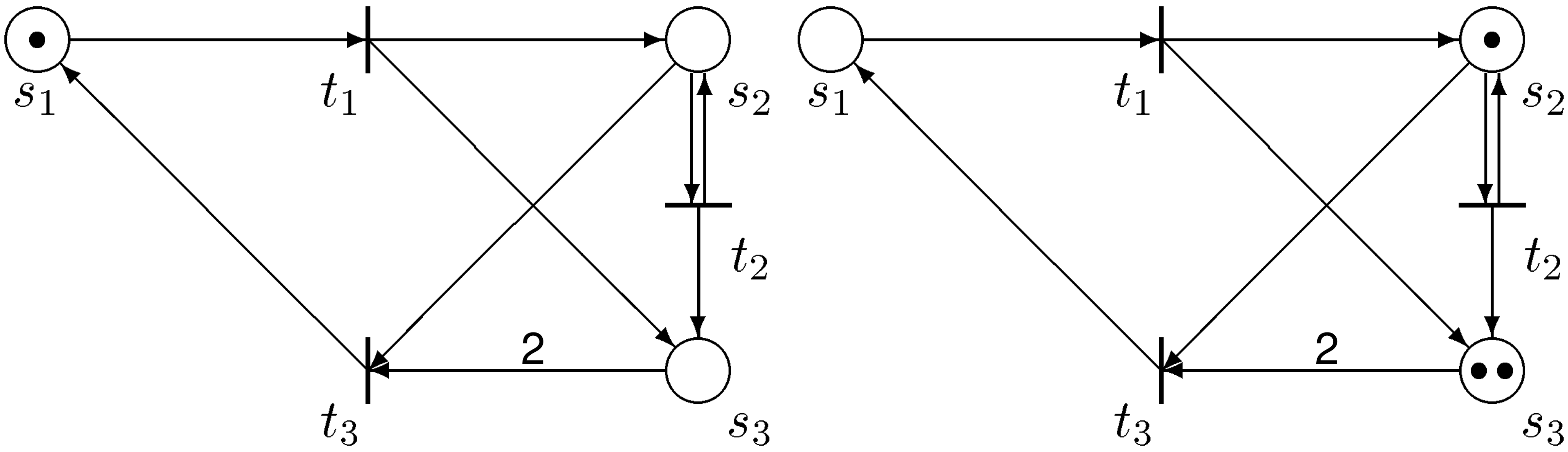
Algebraic Analysis of Parallel Process Models

Ernst W. Mayr

Technical University Munich

- Petri nets
- reversible PN's and commutative semigroups
- binomial polynomial ideals
- Gröbner bases and properties
- state space representation

Petri Nets and Vector Addition Systems



Petri Nets

marking: number of tokens on places

firing of transition: change of marking

reachability set: set of reachable markings

Petri nets and VAS (VRS) are widely used models for parallel processes.

Basic facts:

1. The reachability problem is decidable [Mayr/80].

2. The equality/containment problem is undecidable [Hack/76].

3. Bisimulation is undecidable [Jančar/94].

Finitely Presented CSG's

Given:

1. finite set Σ of symbols, commutative
2. finite set Γ of congruences:

$$l_i \equiv r_i; \;\; i = 1, \ldots, w; \; l_i, r_i \in \Sigma^*$$

3. two words $u, v \in \Sigma^*$.

Problem:

Is $u \equiv v \; (\Gamma)$?

Example:

$$\begin{aligned} a^2 &\equiv b \\ b^2 c &\equiv c \end{aligned}$$

Then we have:

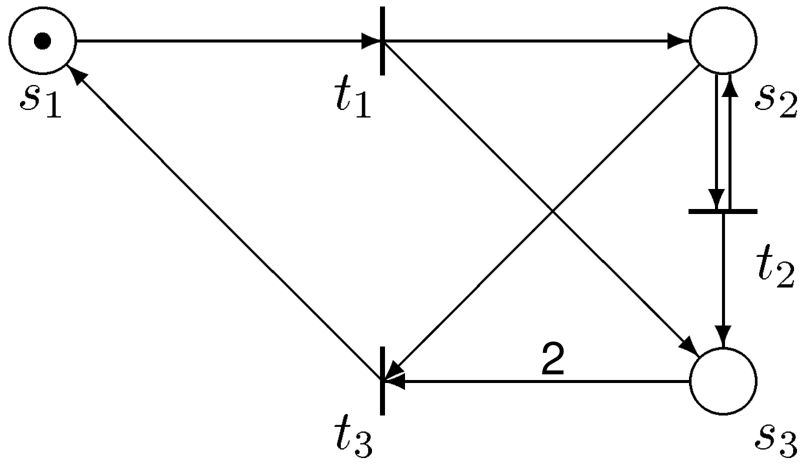
$$\begin{aligned} a^4 c &\equiv c \\ a^4 &\not\equiv \lambda \end{aligned}$$

CSG's

Basic (complexity) facts about CSG's:

1. The (uniform) word problem is EXPSPACE-complete [Mayr-Meyer/82].
2. The equivalence problem is decidable in space $O(2^{c \cdot n \cdot \log n})$ [Huynh/85].
3. Finitely presented commutative semigroups correspond to *reversible* Petri nets.

CSG's and Reversible PN's



Symbols: s_1, s_2, s_3

congruences:

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

polynomials:

$$\begin{aligned} p_1 &= s_2 s_3 - s_1 \\ p_2 &= s_2 s_3 - s_2 \\ p_3 &= s_1 - s_2 s_3^2 \end{aligned}$$

Polynomial Ideals

Given: A finite set of polynomials

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

and a test polynomial p.

The ideal

$$\langle p_1, \ldots, p_w \rangle$$

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

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

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

Decision problem:

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

Representation problem:

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

A small example

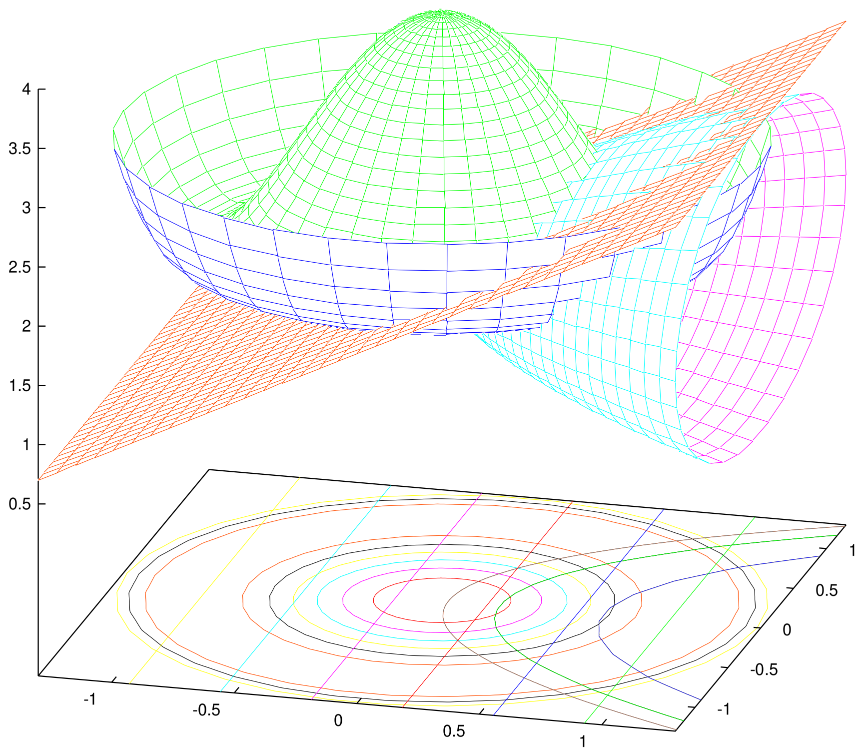
Consider the ideal generated in $\mathbb{R}^3$ by the polynomials

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

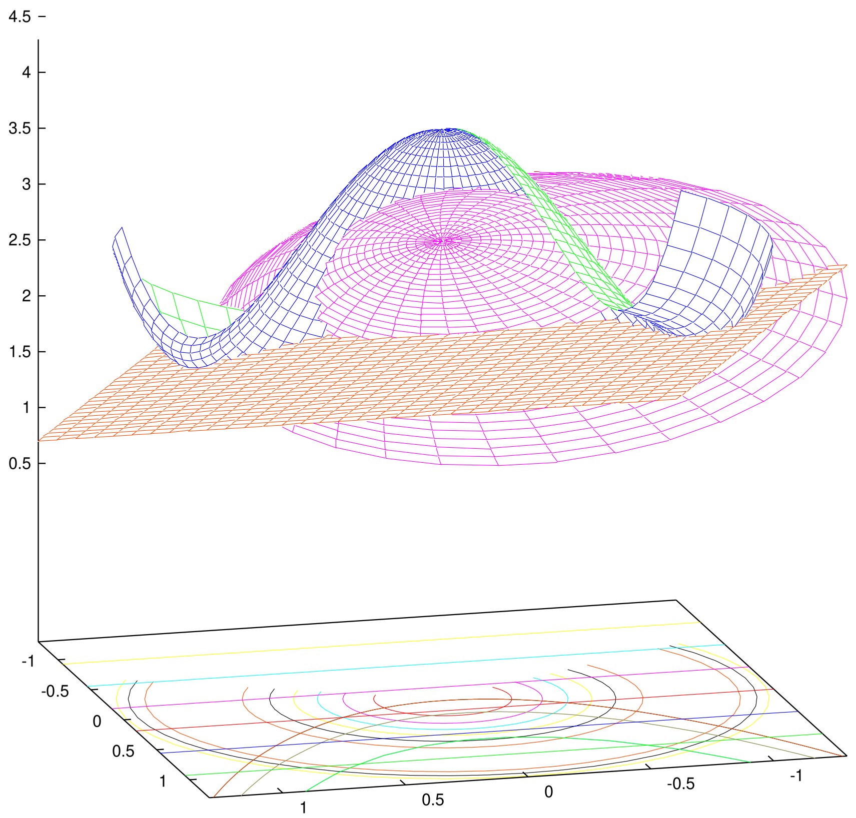
$$p_2: \quad z - 2x^4 - 4y^2x^2 + 4x^2 - 2y^4 + 4y^2 - 5, \text{ and}$$

$$p_3: \quad z - x - 3\,.$$

Graph of functions in example



. . . and another view



Hilbert's Nullstellensatz

Theorem: *Let k be an algebraically closed field, and let $p, p_1, \ldots, p_w \in k[x_1, \ldots, x_n]$. If p vanishes on all the common zeroes of the p_i, then there is an $e \in \mathbb{N}$ such that*

$$p^e \in \langle p_1, \ldots, p_w \rangle.$$

Standard (Gröbner) Bases

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 monomials 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 $x_1 x_2 x_3 \succ x_1 x_3^2$

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 $\mathbb{Q}[x]$ is a Standard or Gröbner basis for I (wrt. $\prec$) if the following hold:

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

Example

Consider the basis

$$\{x^5 + y^4 + z^3 - 1, x^3 + y^2 + z^2 - 1\} \ ,$$

with the lex term ordering.

Mathematica computes the following Gröbner basis:

$$y^{12} - y^{10} + 3z^3y^8 - 5z^2y^8 + 2y^8 - 10z^4y^6 + 20z^2y^6 - 10y^6 - 7z^6y^4 + 30z^4y^4 - 6z^3y^4 - 30z^2y^4 + 13y^4 - 5z^8y^2 + 20z^6y^2 - 30z^4y^2 + 20z^2y^2 - 5y^2 - z^{10} + z^9 + 5z^8 - 13z^6 + 10z^4 + 3z^3 - 5z^2$$

$$z^{11}x + 4z^{10}x + z^9x - 10z^8x - 4z^7x + 8z^6x - 3z^3y^{10} - 2z^2y^{10} + 4zy^{10} + 4y^{10} + z^5y^8 - 2z^4y^8 - 2z^3y^8 - 6z^6y^6 + 10z^5y^6 + 20z^4y^6 - 16z^3y^6 - 24z^2y^6 + 8zy^6 + 8y^6 + 2z^8y^4 + 21z^7y^4 + 17z^6y^4 - 78z^5y^4 - 64z^4y^4 + 90z^3y^4 + 76z^2y^4 - 32zy^4 - 32y^4 + 17z^9y^2 + 24z^8y^2 - 68z^7y^2 - 80z^6y^2 + 106z^5y^2 + 108z^4y^2 - 77z^3y^2 - 70z^2y^2 + 20zy^2 + 20y^2 + 7z^{11} + 7z^{10} - 31z^9 - 42z^8 + 55z^7 + 77z^6 - 39z^5 - 62z^4 + 8z^3 + 20z^2$$

$$zy^2x - y^2x - 1/8z^{10}x - 7/24z^9x + 1/2z^8x + 7/8z^7x - 23/24z^6x + 1/2z^4x - 1/2z^3x - zx + x + 3/8z^2y^{10} - 3/8zy^{10} - 7/24y^{10} - 1/8z^4y^8 + 11/24z^3y^8 - 3/8z^2y^8 + 1/4zy^8 - 1/4y^8 + 3/4z^5y^6 - 5/2z^4y^6 + 5/6z^3y^6 + 31/12z^2y^6 - zy^6 - 1/3y^6 - 1/4z^7y^4 - 53/24z^6y^4 + 11/6z^5y^4 + 113/12z^4y^4 - 55/8z^3y^4 - 29/4z^2y^4 + 15/4zy^4 + 19/12y^4 - 17/8z^8y^2 + 13/24z^7y^2 + 239/24z^6y^2 - 59/12z^5y^2 - 151/12z^4y^2 + 85/12z^3y^2 + 43/8z^2y^2 - 29/8zy^2 + 7/24y^2 - 7/8z^{10} + 7/12z^9 +$$

$$31/8z^8 - 11/12z^7 - 103/12z^6 + 17/6z^5 + 127/24z^4 - 3/2z^3 - 17/24z^2 + z - 1$$

$$y^4x + z^3x - x + y^4 + 2z^2y^2 - 2y^2 + z^4 - 2z^2 + 1$$

$$z^4x^2 + z^3x^2 - 2z^2x^2 - 1/6z^{10}x - 2/3z^9x - 1/4z^8x + 7/6z^7x - 1/12z^6x - z^5x + z^4x + 1/2z^2y^{10} + 1/3zy^{10} - 5/12y^{10} - 1/6z^4y^8 + 1/3z^3y^8 + 1/4z^2y^8 + 1/2y^8 + z^5y^6 - 5/3z^4y^6 - 17/6z^3y^6 + 17/6z^2y^6 + 2/3zy^6 - 1/3y^6 - 1/3z^7y^4 - 7/2z^6y^4 - 3z^5y^4 + 131/12z^4y^4 + 23/4z^3y^4 - 13z^2y^4 - 8/3zy^4 + 29/6y^4 - 17/6z^8y^2 - 4z^7y^2 + 119/12z^6y^2 + 17/2z^5y^2 - 16z^4y^2 - 14/3z^3y^2 + 12z^2y^2 + 5/3zy^2 - 55/12y^2 - 7/6z^{10} - 7/6z^9 + 55/12z^8 + 21/4z^7 - 31/4z^6 - 15/2z^5 + 83/12z^4 + 41/12z^3 - 31/12z^2$$

$$y^2x^2 + z^2x^2 - x^2 - y^4 - z^3 + 1$$

$$x^3 + y^2 + z^2 - 1$$

Another Example

Using the basis

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

with any term ordering,

our favorite symbolic algebra package computes the following Gröbner basis:

$$1$$

This example highlights the so-called Rabinovich trick, showing

$$xy^3 - z^2 + y^5 - z^3 \in \sqrt{\langle y - x^3, x^2 y - z\rangle} .$$

Gröbner Bases

A few facts about Gröbner bases:

1. *Reduced* Gröbner bases are uniquely determined.
2. Gröbner bases for binomial ideals are again binomial [Eisenbud-Sturmfels/94].
3. Reduced Gröbner bases have degree bounded by $2(\frac{d^2}{2} + d)^{2^{n-1}}$ [Dubé/90].
4. The reduced Gröbner basis of a binomial ideal can be computed in EXPSPACE [Koppenhagen-Mayr/95].

CSG's and Binomial Ideals

Theorem: *The (uniform) word problem for finitely generated commutative semigroups and the membership problem for binomial ideals are polynomially equivalent.*

Proof: Consider u, v and the l_i and r_i as monomials. It is not hard to see that

$$u \equiv v\ (\Gamma) \Longleftrightarrow u - v \in \langle r_1 - l_1, \ldots, r_w - l_w \rangle\ .$$

∎

Definition: Let $[u]$ denote the equivalence class of u, *i.e.,*

$$[u] = \{v;\ u \equiv v\ (\Gamma)\}\ .$$

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

Representation of the Reachability Set

1. We show that the minimal elements of the uniformly semilinear reachability set have norm bounded by $2^{2^{c \cdot n}}$.
2. We show an analogous bound for the periods of the reachability set.

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

Determining the Minimal Elements

Let $\Gamma = \{l_i \equiv r_i;\ i = 1, \ldots, w\}$ be the given set of congruences, over $\Sigma = \{x_1, \ldots, x_n\}$.

Consider the semigroup presentation

$$\begin{array}{rcll}
sx_j & \equiv & sa_jb_j & \text{for } j = 1, \ldots, n \\
sb(l_i) & \equiv & sb(r_i) & i = 1, \ldots, w \\
sb(u) & \equiv & t & \\
ta(l_i) & \equiv & ta(r_i) & i = 1, \ldots, w \\
su & \equiv & m &
\end{array}$$

where s, t, m, and the a_j, b_j are new symbols, a (resp., b are the homomorphisms replacing x_j by a_j (resp., b_j), for $j = 1, \ldots, n$, and $u \in \{x_1, \ldots, x_n\}^*$ is the word corresponding to the initial marking of the reversible Petri net.

Also, let a term ordering be given such that, for all $j = 1, \ldots, n$,

$$t \succ a_j \succ b_j \succ s \succ x_j \succ m \,,$$

and consider the ideal $\mathcal{I}$ generated by the corresponding binomials.

Theorem: *The binomial $sv - m$ occurs in the reduced Gröbner basis of $\mathcal{I}$ iff $v \in [u]$. Hence, if $v \in [u]$, the monomial sv has at most doubly exponential degree.*

The Subword Reachability Problem

Definition: The subword reachability problem is: Given $u, v \in \Sigma^*$ and $k \in \{1, \ldots, n+1\}$, determine whether there is a $v' \in \{x_k, \ldots, x_n\}^*$ such that

$$vv' \in [u] \ .$$

Consider the semigroup presentation

$$\begin{array}{rcll} s' & \equiv & su & \\ sl_i & \equiv & sr_i & \text{for } i = 1, \ldots, w \\ sv & \equiv & t & \end{array}$$

where s, s', and t are new symbols.

Let a term order be given such that

$$s' \succ s \succ x_1 \succ \cdots \succ x_{k-1} \succ t \succ x_k \succ \ldots \succ x_n \ ,$$

and let $\mathcal{J}$ be the ideal generated by the corresponding binomials.

Theorem: *There exists $vv' \in [u]$, $v' \in \{x_k, \ldots, x_n\}^*$ iff the reduced Gröbner basis for $\mathcal{J}$ contains a binomial $s' - tv'$, $v' \in \{x_k, \ldots, x_n\}^*$.*

Results

Theorem: *The subword reachability problem for reversible Petri nets is complete for EXPSPACE.*

Theorem: *A closed representation (as a semilinear set) of the reachability set of a reversible Petri net can be computed in exponential space.*

Corollary: *The equivalence problem for finitely presented commutative semigroups is decidable in exponential space.*

More Results

Theorem: *Given a basis for an ideal and a term ordering, the corresponding uniquely determined reduced Gröbner basis can be computed in EXPSPACE.*

Proof: [Kühnle-Mayr/96] ∎

Theorem: *Given a basis for an ideal, a term ordering, and a polynomial $p \in \mathbb{Q}[x_1, \ldots, x_n]$, the uniquely determined normal form of p can be computed in EXPSPACE.*

Remark:

1. For all these problems, there are matching EXPSPACE lower bounds.
2. The Gröbner bases or normal forms computed above may contain numbers triply exponential in size.

Conclusion, Open Problems

There are very close connections between the complexities of various problems for commutative semigroups, Petri nets, and polynomial ideals. These sometimes produce interesting applications of results obtained in one of these areas.

Open problems:

1. Find “efficient” parallel algorithms for PIMP!
2. Determine the complexity of the Petri net reachability problem ($\equiv$ coefficients in $\mathbb{N}$ or $\mathbb{Q}^+$)!
3. Determine the complexity of bisimulation for reversible PN’s!
4. Determine the complexity of bisimulation for BPP’s!