FROM PETRI NETS TO POLYNOMIALS: MODELING, ALGORITHMS, AND COMPLEXITY

Ernst W. Mayr
Fakultät für Informatik
TU München
http://www.in.tum.de/~mayr/

OUTLINE OF TALK

- some basics of polynomial ideals
- Petri nets and binomial ideals, and
- complexity theoretic consequences of this relationship
- Gröbner bases and their complexity
- modeling power of polynomial ideals
- recent trends and results

OUTLINE OF TALK

- some basics of polynomial ideals
- Petri nets and binomial ideals, and
- complexity theoretic consequences of this relationship
- Gröbner bases and their complexity
- modeling power of polynomial ideals
- recent trends and results

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

Examples

- The ideal generated in $\mathbb{Q}[x, y]$ by the two polynomials

$$p_1 = x^2 \quad \text{and} \quad p_2 = y$$

is the set of all those polynomials all of whose monomials are divisible by x^2 or y.

Examples

- The ideal generated in $\mathbb{Q}[x, y]$ by the two polynomials

$$p_1 = x^2 \quad \text{and} \quad p_2 = y$$

  is the set of all those polynomials all of whose monomials are divisible by x^2 or y.

- We have:

$$\begin{aligned} y^2 - xz &= (y + x^2)(y - x^2) - x(z - x^3) \\ &= (y + x^2) \cdot p_1 - x \cdot p_2 \\ &\in \langle p_1, p_2 \rangle \end{aligned}$$

  Thus

$$y^2 - xz \in \langle y - x^2, z - x^3 \rangle \ .$$

A Graphical Example

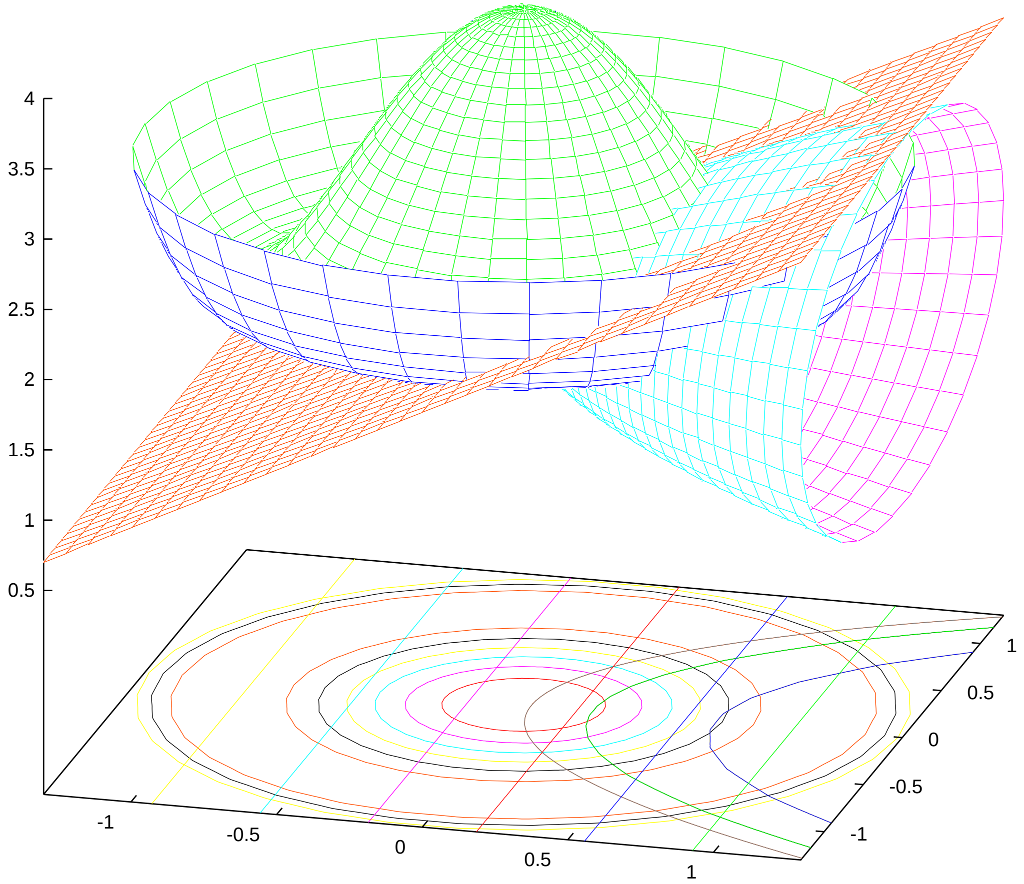
We consider the ideal in $\mathbb{R}^3$ generated by the polynomials

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: $z - x - 3$.

The Zeroes of p_1, p_2, and p_3



Algebraic Varieties

Definition: The common zeroes $\in \mathbb{C}^n$ of a (finite) set of polynomials $\in \mathbb{C}[x_1, \ldots, x_n$ is called an (algebraic) variety.

Algebraic Varieties

Definition: The common zeroes $\in \mathbb{C}^n$ of a (finite) set of polynomials $\in \mathbb{C}[x_1, \ldots, x_n$ is called an (algebraic) variety.

Definition: The radical $\sqrt{\mathcal{I}}$ of an ideal $\mathcal{I} \subseteq \mathcal{K}[\mathbf{x}]$ is the ideal

$$\{p \in K[\mathbf{x}];\ p^k \in \mathcal{I} \text{ for some } k \in \mathbb{N}\}\ .$$

Algebraic Varieties

Definition: The common zeroes $\in \mathbb{C}^n$ of a (finite) set of polynomials $\in \mathbb{C}[x_1, \ldots, x_n$ is called an (algebraic) variety.

Definition: The radical $\sqrt{\mathcal{I}}$ of an ideal $\mathcal{I} \subseteq \mathcal{K}[\mathbf{x}]$ is the ideal

$$\{p \in K[\mathbf{x}];\ p^k \in \mathcal{I} \text{ for some } k \in \mathbb{N}\} \ .$$

Let K be some algebraically closed field. Then, by the strong version of Hilbert's Nullstellensatz, there is a one-to-one correspondence between the radical ideals in $K[x_1, \ldots, x_n]$ and the algebraic varieties in $\mathbb{C}^n$.

Polynomial Ideal Membership Problem

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

- Decision problem:

Is $p \in \langle p_1, \ldots, p_w \rangle$?

Polynomial Ideal Membership Problem

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

- Decision problem:

Is $p \in \langle p_1, \ldots, p_w \rangle$?

- Representation problem:

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

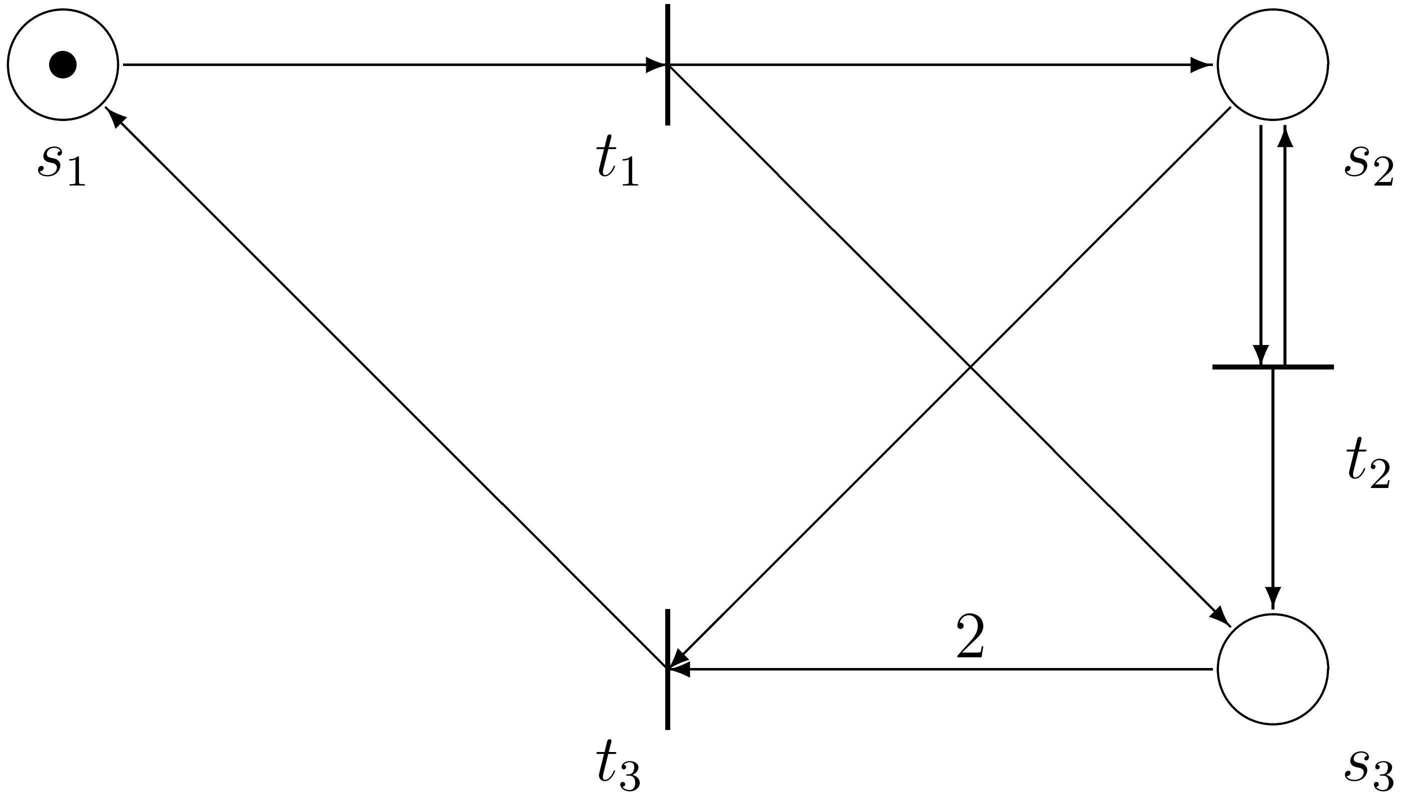
OUTLINE OF TALK

- some basics of polynomial ideals
- Petri nets and binomial ideals
- complexity theoretic consequences of this relationship
- Gröbner bases and their complexity
- modeling power of polynomial ideals
- recent trends and results

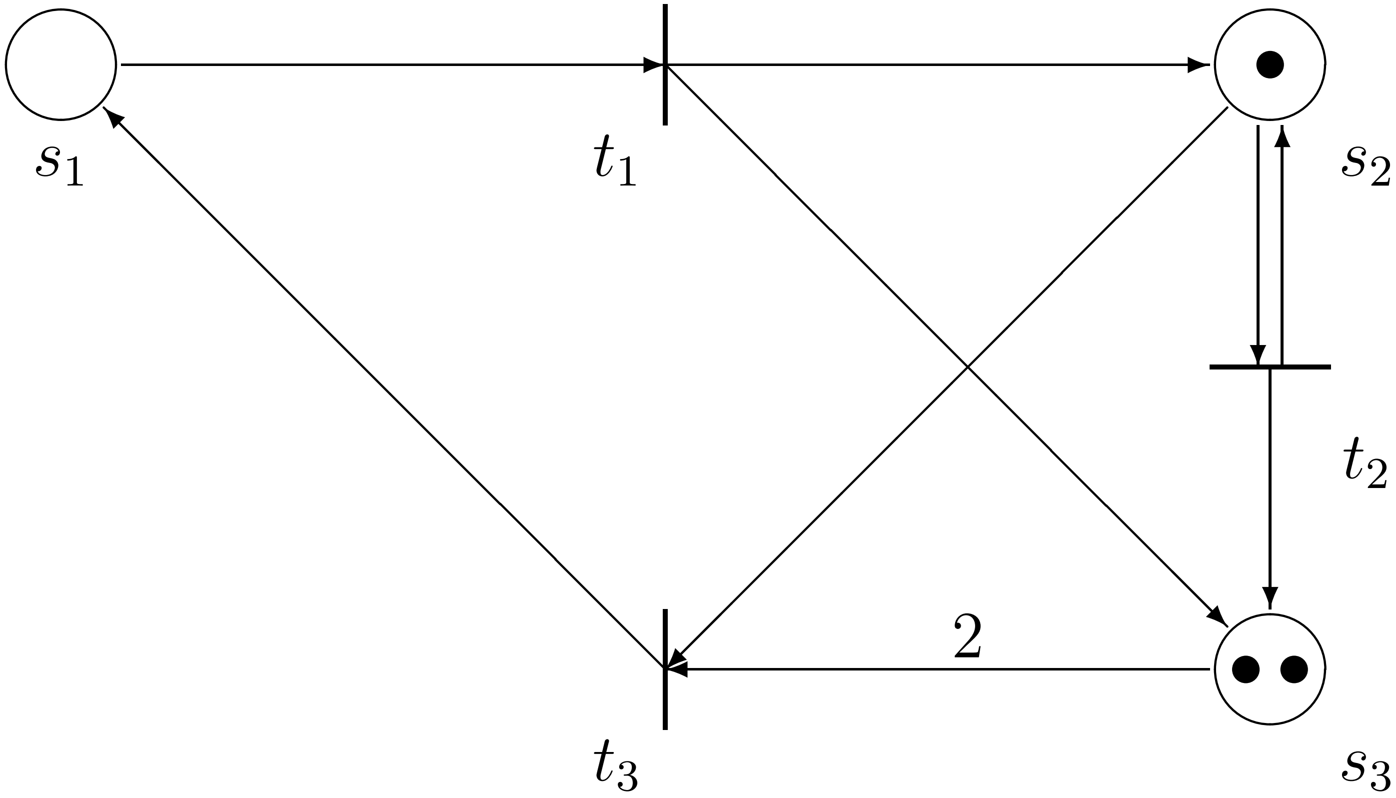
BINOMIAL IDEALS

- Binomial polynomials are polynomials which are the difference of two monomials
- Binomial ideals are ideals generated by binomial polynomials
- Binomials can be thought of as specifying (symmetric, i.e., Thue) commutative replacement systems
- Every polynomial can be represented by (a system of) trinomials

Petri Nets and VAS



Petri Nets and VAS



Petri Nets and VAS

marking: number of tokens on places

firing of transition: marking change

reachability set: set of reachable markings

Reversible PNs correspond to systems of binomials:

Symbols: s_1, s_2, s_3

congruences: binomials:

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

SOME FACTS ABOUT PETRI NETS

- invented by Carl Adam Petri in 1962
- greatly advanced by the MIT Project MAC
- numerous applications and uses, like
  - modeling program synchronization
  - modeling a Berlin beer brewery
  - modeling the Murmansk economic region
  - modeling enzyme action and metabolism of cells
- also see

  http://www.informatik.uni-hamburg.de/TGI/pnbib/

OUTLINE OF TALK

- some basics of polynomial ideals
- Petri nets and binomial ideals
- complexity theoretic consequences of this relationship
- Gröbner bases and their complexity
- modeling power of polynomial ideals
- recent trends and results

SOME FACTS ABOUT PETRI-NET COMPLEXITY

- The reachability problem for PNs is decidable: M [1980]
- simple generalizations of the model make the reachability problem undecidable
- The containment and equivalence problems for PNs are undecidable: Hack [1976]
- These problems are non-primitive recursive even for finite reachability sets: M [1981]

SOME RESULTS

- upper bounds for PIMP:
  - decidability: G. Hermann [1926]
  - doubly exponential degree bound with coefficients in Q: Hermann [1926]
  - exponential degree bound for special *p* : Brownawell[1987], Heintz et al. [1988], Berenstein/Yger [1988]
  - exponential space upper bound with coefficients in Q, polynomial for special *p* : M [1988]
- upper bound for PN reachability:
  - decidability: M [1980]
  - exponential space for reversible PN: M/Meyer [1982]

SOME MORE RESULTS

- lower bounds for PIMP:
  - doubly exponential degree lower bound in pure difference binomial ideals: M/Meyer [1982]
  - exponential space lower bound: M/Meyer [1982]
- lower bounds for PN reachability:
  - exponential space lower bound for general PN: Lipton [1974]
  - Exponential space lower bound for reversible PN: M/Meyer [1982]

FURTHER RESULTS FOR POLYNOMIAL IDEAL MEMBERSHIP

- PIMP is in PSPACE for:
  - homogeneous ideals (and complete): M [1988]
  - ideals of constant dimension: Berenstein/Yger [1990]
  - special cases, like $p = 1$: Brownawell [1987]
- The PI triviality problem is in the second level of the polynomial hierarchy: Koiran [1996]

OUTLINE OF TALK

- some basics of polynomial ideals
- Petri nets and binomial ideals
- complexity theoretic consequences of this relationship
- Gröbner bases and their complexity
- modeling power of polynomial ideals
- recent trends and results

Gröbner Bases I

Admissible term ordering:

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

Gröbner Bases I

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

$$mm_1 \prec mm_2 \ .$$

Gröbner Bases I

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:

Gröbner Bases I

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: $x_1^2 \succ x_1 x_2^3 x_3^{1023}$

Gröbner Bases I

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: $x_1^2 \succ x_1 x_2^3 x_3^{1023}$
2. grevlex: $x_2^3 \succ x_1$ and $x_1 x_2 x_3 \succ x_1 x_3^2$

Gröbner Bases I

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: $x_1^2 \succ x_1 x_2^3 x_3^{1023}$
2. grevlex: $x_2^3 \succ x_1$ and $x_1 x_2 x_3 \succ x_1 x_3^2$

Arrange the monomials in polynomials according to $\prec$ in decreasing order.

Polynomial Reduction

Definition:

1. A polynomial f is reducible by some other polynomial g if the leading term $lt(g)$ divides one of the momomials m of f. The reduct is

$$\tilde{f} = f - \frac{m}{lt(g)} \cdot g \ .$$

Polynomial Reduction

Definition:

1. A polynomial f is reducible by some other polynomial g if the leading term $lt(g)$ divides one of the momomials m of f. The reduct is
$$\tilde{f} = f - \frac{m}{lt(g)} \cdot g \; .$$
2. A polynomial f is reducible by a set G of polynomials if there is a sequence $g = g^{(0)}, g^{(1)}, \ldots, g^{(r)}$, $r \geq 1$, such that each $g^{(i)}$ is the reduct of $g^{(i-1)}$ by one of the polynomials in G.

Polynomial Reduction

Definition:

1. A polynomial f is reducible by some other polynomial g if the leading term $lt(g)$ divides one of the momomials m of f. The reduct is
$$\tilde{f} = f - \frac{m}{lt(g)} \cdot g \ .$$
2. A polynomial f is reducible by a set G of polynomials if there is a sequence $g = g^{(0)}, g^{(1)}, \ldots, g^{(r)}$, $r \geq 1$, such that each $g^{(i)}$ is the reduct of $g^{(i-1)}$ by one of the polynomials in G.
3. A polynomial f is in normal form wrt a set G of polynomials if it cannot be reduced by G.

Gröbner Bases II

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 $G = \{g_1, \ldots, g_r\}$ of polynomials in I is called a Gröbner basis of I (wrt $\prec$) if for all $f \in \mathbb{Q}[x]$ the normal form of f wrt G is uniquely determined.

Gröbner Bases II

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 $G = \{g_1, \ldots, g_r\}$ of polynomials in I is called a Gröbner basis of I (wrt $\prec$) if for all $f \in \mathbb{Q}[x]$ the normal form of f wrt G is uniquely determined.

Remark:

Thus, in particular, the normal form does not depend on the order of the reductions by the $g \in G$.

Further Results

- exponential space algorithm for the computation of Gröbner bases: Kühnle/M [1996],
- exponential space bounds also result for a number of ideal operations, like intersection, union, quotient, etc.
- PSPACE algorithms for those cases where exponential degree bounds hold,
- the bounds also hold for characteristic $\neq 0$ (but infinite fields).

OUTLINE OF TALK

- some basics of polynomial ideals
- Petri nets and binomial ideals
- complexity theoretic consequences of this relationship
- Gröbner bases and their complexity
- modeling power of polynomial ideals
- recent trends and results

Propositional Derivation/Proof Systems

One of the most fundamental questions in logic is:
Given a (propositional) tautology, what is a shortest proof for it (in a standard proof system)?

Propositional Derivation/Proof Systems

One of the most fundamental questions in logic is:
Given a (propositional) tautology, what is a shortest proof for it (in a standard proof system)?

What is a standard proof system?

Propositional Derivation/Proof Systems

One of the most fundamental questions in logic is:
Given a (propositional) tautology, what is a shortest proof for it (in a standard proof system)?

What is a standard proof system?

One example is resolution calculus, with just one derivation rule (resolution for a variable x):

$$\frac{x \vee A, \quad \neg x \vee B}{A \vee B}.$$

Propositional Derivation/Proof Systems

One of the most fundamental questions in logic is:
Given a (propositional) tautology, what is a shortest proof for it (in a standard proof system)?

What is a standard proof system?

One example is resolution calculus, with just one derivation rule (resolution for a variable x):

$$\frac{x \vee A, \quad \neg x \vee B}{A \vee B}.$$

The goal is to derive the contradiction consisting of the empty clause (resolution of clauses x and $\neg x$).

Translation to Polynomial Ideals

- $\phi(x) = 1 - x$,
- $\phi(\neg x) = 1 - \phi(x)$,
- $\phi(x \vee y) = \phi(x)\phi(y)$,
- and with DeMorgan:
  $\phi(x \wedge y) = \phi(\neg(\neg x \vee \neg y)) = \phi(x) + \phi(y) - \phi(x)\phi(y)$

Translation to Polynomial Ideals

- $\phi(x) = 1 - x$,
- $\phi(\neg x) = 1 - \phi(x)$,
- $\phi(x \vee y) = \phi(x)\phi(y)$,
- and with DeMorgan:
  $\phi(x \wedge y) = \phi(\neg(\neg x \vee \neg y)) = \phi(x) + \phi(y) - \phi(x)\phi(y)$

Question: Does the ideal generated by these polynomials contain false, i.e., the constant polynomial 1 ?

Algebraic Derivation Systems

We consider polynomial rings in several variables over GF(2), including the Fermat polynomials $x_i^2 - x_i = 0$.

Theorem: *Let polynomials* $p, p_1, \ldots, p_w \in GF(2)[x_1, \ldots, x_n]$ *be given. The word problem*

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

is co-NP-complete.

Algebraic Derivation Systems

We consider polynomial rings in several variables over GF(2), including the Fermat polynomials $x_i^2 - x_i = 0$.

Theorem: *Let polynomials* $p, p_1, \ldots, p_w \in GF(2)[x_1, \ldots, x_n]$ *be given. The word problem*

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

is co-NP-complete.

Theorem: *The radical word problem*

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

is co-NP-complete.

Properties of Algebraic Derivation Systems

Theorem: *For each ring R, Frege proofs (and extended Frege proofs) can be simulated efficiently by algebraic derivations of polynomial length.*

Properties of Algebraic Derivation Systems

Theorem: *For each ring R, Frege proofs (and extended Frege proofs) can be simulated efficiently by algebraic derivations of polynomial length.*

Observation: There exist examples, for which algebraic derivation systems (or Gröbner proof systems) are considerably more efficient (asymptotically) than resolution.

FURTHER APPLICATIONS

- Geometric design
- Computation of the possible movements of robots or multi-joint robot arms
- Modeling of the electrical behavior of integrated circuits
- Modeling of carbon rings and their degrees of freedom in chemistry

… CONT'D

- Application of involutive Gröbner bases for the solution of partial differential equations in nuclear physics
- Combinatorial optimization
- Coding theory
- Modeling of combinatorial graph properties

SOME OPEN PROBLEMS

- translate new degree bounds (for polynomials over rings not fields) into space efficient algorithms
- develop and analyze algorithms for ideal operations
- complexity of radical ideals
- complexity of toric ideals

THE END!

Thank you
for your
attention!