## Gröbner Bases

## Quick Updates and Extended Snapshots

David A. Cox<br>Department of Mathematics and Computer Science<br>Amherst College<br>dac@cs.amherst.edu<br>EACA 2012, Alcalá

## Outline

## Four Quick Updates:

- The F5 Algorithm
- One-Point Algebraic Geometry Codes
- Cost Minimization of Series-Parallel System
- May 2012


## Four Extended Snapshots:

- Graph Colorings
- The Join-Meet Ideal of a Finite Lattice
- The Nullstellensatz
- Geometric Theorem Discovery


## Outline

## Four Quick Updates:

- The F5 Algorithm
- One-Point Algebraic Geometry Codes
- Cost Minimization of Series-Parallel System
- May 2012


## Four Extended Snapshots:

- Graph Colorings
- The Join-Meet Ideal of a Finite Lattice
- The Nullstellensatz
- Geometric Theorem Discovery


## Outline

## Four Quick Updates:

- The F5 Algorithm
- One-Point Algebraic Geometry Codes
- Cost Minimization of Series-Parallel System
- May 2012


## Four Extended Snapshots:

- Graph Colorings
- The Join-Meet Ideal of a Finite Lattice
- The Nullstellensatz
- Geometric Theorem Discovery


## Outline

## Four Quick Updates:

- The F5 Algorithm
- One-Point Algebraic Geometry Codes
- Cost Minimization of Series-Parallel System
- May 2012


## Four Extended Snapshots:

- Graph Colorings
- The Join-Meet Ideal of a Finite Lattice
- The Nullstellensatz
- Geometric Theorem Discovery


## Update \#1: The F5 Algorithm

In 2002, Faugére proposed his F5 algorithm for computing Gröbner bases. Its termination was proved just recently!
S. Pan, Y. Hu and B. Wang, The Termination of Algorithms for Computing Gröbner Bases, arXiv:math.AC/1202.3524.

The F5 algorithm is generally believed as one of the fastest algorithms for computing Gröbner bases. However, its termination problem is still unclear. Recently, an algorithm GVW and its variant GVWHS have been proposed, and their efficiency are comparable to the F5 algorithm. ... Taking into account this situation, we prove the termination and correctness of the F5B algorithm. And we notice that the original F5 algorithm slightly differs from the F5B algorithm in the insertion strategy on which the F5-rewritten criterion is based. ...
Therefore, we have a positive answer to the long standing problem of proving the termination of the original F5 algorithm.

## Update \#1, Continued

V. Galkin, Termination of Original F5, arXiv:math.AC/1203.2402.

The original F5 algorithm described in Faugére's paper is formulated for any homogeneous polynomial set input. The correctness of output is shown for any input that terminates the algorithm, but the termination itself is proved only for the case of input being regular polynomial sequence. This article shows that algorithm correctly terminates for any homogeneous input without any reference to regularity.
C. Eder, Sweetening the sour taste of inhomogeneous signature-based Groebner basis computations, arXiv:math.AC/1203.6186.

In this paper we want to give an insight into the rather unknown behaviour of signature-based Groebner basis algorithms, like F5, G2V, or GVW, for inhomogeneous input.

## Update \#2: One-Point Algebraic Geometry Codes

O. Geil, R. Matsumoto and D. Ruano, List decoding algorithms based on Gröbner bases for general one-point AG codes, arXiv:cs.IT/1201.6248.

We generalize the list decoding algorithm for Hermitian codes proposed by Lee and O'Sullivan based on Gröbner bases to general one-point AG codes, under an assumption weaker than one used by Beelen and Brander. By using the same principle, we also generalize the unique decoding algorithm for one-point AG codes over the Miura-Kamiya $C_{a b}$ curves proposed by Lee, Bras-Amorós and O'Sullivan to general one-point AG codes, without any assumption.

## Update \#3: Cost Minimization

F. Castro, J. Gago, I. Hartillo, J. Puerto and J. M. Ucha, Exact cost minimization of a series-parallel system, arXiv:math.OC/1203.3307.

The redundancy allocation problem is formulated minimizing the design cost for a series-parallel system with multiple component choices whereas ensuring a given system reliability level. The obtained model is a nonlinear integer programming problem with a non linear, non separable constraint. We propose an algebraic method, based on Gröbner bases, to obtain the exact solution of the problem. In addition, we provide a closed form for the required Gröbner bases, avoiding the bottleneck associated with the computation, and promising computational results.

## Update \#4: May 2012

D. R. Grayson, A. Seceleanu and M. E. Stillman, Computations in intersection rings of flag bundles, arXiv:math.AG/1205.4190.

Intersection rings of flag varieties are generated by Chern classes of the tautological bundles modulo relations coming from multiplicativity of total Chern classes. We describe the Groebner bases of the ideals of relations.
V. Galkin, Simple signature-based Groebner basis algorithm, arXiv:math.AC/1205.6050

This paper presents an algorithm for computing Groebner bases based upon labeled polynomials and ideas from the algorithm F5.
D. J. Wilson, R. J. Bradford and J. H. Davenport, Speeding up Cylindrical Algebraic Decomposition by Gröbner bases, arXiv:cs.SC/1205.6285.

Gröbner Bases and Cylindrical Algebraic Decomposition are generally thought of as two, rather different, methods of looking at systems of equations and, in the case of Cylindrical Algebraic Decomposition, inequalities.

## Update Summary

The papers cited on the three updates were all posted on the arXiv in January, February, March and May of 2012.

However, they appeared in very different places in the arXiv:

- The F5 papers: math.AC - Commutative Algebra
- The coding theory paper: cs.IT - Information Theory
- The cost minimization paper: math.OC - Optimization and Control
- May 2012: math.AG - Algebraic Geometry cs.SC - Symbolic Computation


## This shows:

## Update Summary

The papers cited on the three updates were all posted on the arXiv in January, February, March and May of 2012.

However, they appeared in very different places in the arXiv:

- The F5 papers: math.AC - Commutative Algebra
- The coding theory paper: cs.IT - Information Theory
- The cost minimization paper: math.OC - Optimization and Control
- May 2012: math.AG - Algebraic Geometry
cs.SC - Symbolic Computation


## This shows:

## Update Summary

The papers cited on the three updates were all posted on the arXiv in January, February, March and May of 2012.

However, they appeared in very different places in the arXiv:

- The F5 papers: math.AC - Commutative Algebra
- The coding theory paper: cs.IT - Information Theory
- The cost minimization paper: math.OC - Optimization and Control
- May 2012: math.AG - Algebraic Geometry
cs.SC - Symbolic Computation


## This shows:

## Update Summary

The papers cited on the three updates were all posted on the arXiv in January, February, March and May of 2012.

However, they appeared in very different places in the arXiv:

- The F5 papers: math.AC - Commutative Algebra
- The coding theory paper: cs.IT - Information Theory
- The cost minimization paper: math.OC - Optimization and Control
- May 2012: math.AG - Algebraic Geometry cs.SC - Symbolic Computation


## This shows:

## Update Summary

The papers cited on the three updates were all posted on the arXiv in January, February, March and May of 2012.

However, they appeared in very different places in the arXiv:

- The F5 papers: math.AC - Commutative Algebra
- The coding theory paper: cs.IT - Information Theory
- The cost minimization paper: math.OC - Optimization and Control
- May 2012: math.AG - Algebraic Geometry cs.SC - Symbolic Computation


## This shows:

## Update Summary

The papers cited on the three updates were all posted on the arXiv in January, February, March and May of 2012.

However, they appeared in very different places in the arXiv:

- The F5 papers: math.AC - Commutative Algebra
- The coding theory paper: cs.IT - Information Theory
- The cost minimization paper: math.OC - Optimization and Control
- May 2012: math.AG - Algebraic Geometry cs.SC - Symbolic Computation


## This shows:

- The continued activity in Gröbner bases.
- The wide range of areas of mathematics and computer science


## Update Summary

The papers cited on the three updates were all posted on the arXiv in January, February, March and May of 2012.

However, they appeared in very different places in the arXiv:

- The F5 papers: math.AC - Commutative Algebra
- The coding theory paper: cs.IT - Information Theory
- The cost minimization paper: math.OC - Optimization and Control
- May 2012: math.AG - Algebraic Geometry cs.SC - Symbolic Computation


## This shows:

- The continued activity in Gröbner bases.
- The wide range of areas of mathematics and computer science


## Update Summary

The papers cited on the three updates were all posted on the arXiv in January, February, March and May of 2012.

However, they appeared in very different places in the arXiv:

- The F5 papers: math.AC - Commutative Algebra
- The coding theory paper: cs.IT - Information Theory
- The cost minimization paper: math.OC - Optimization and Control
- May 2012: math.AG - Algebraic Geometry cs.SC - Symbolic Computation


## This shows:

- The continued activity in Gröbner bases.
- The wide range of areas of mathematics and computer science involved.


## Snapshot \#1: Graph Colorings

Let $G=(V, E)$ be a graph with vertices $V=\{1, \ldots, n\}$.

## Definition

A $k$-coloring of $G$ is a function from $V$ to a set of $k$ colors such that adjacent vertices have distinct colors.

## Example

vertices $=81$ squares edges $=$ links between:

- squares in same column
- squares in same row
- squares in same $3 \times 3$

Colors $=\{1,2, \ldots, 9\}$
Goal: Extend the partial coloring to a full coloring.

|  |  |  |  | 3 | 5 |  |  |  |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
|  | 1 |  | 2 |  |  | 9 |  |  |
| 7 |  | 6 |  |  |  | 2 |  |  |
| 6 |  |  | 5 |  |  |  | 3 |  |
| 2 |  |  |  | 4 |  |  |  | 9 |
|  | 3 |  |  |  | 1 |  |  | 5 |
|  |  | 3 |  |  |  | 4 |  | 8 |
|  |  | 4 |  |  | 6 |  | 7 |  |
|  |  |  | 3 | 1 |  |  |  |  |

## Graph Ideal

## Definition

The $k$-coloring ideal of $G$ is the ideal $I_{G, k} \subseteq \mathbb{C}\left[x_{i} \mid i \in V\right]$ generated by:

$$
\text { for all } i \in V: \quad x_{i}^{k}-1
$$

$$
\text { for all } i j \in E: \quad x_{i}^{k-1}+x_{i}^{k-2} x_{j}+\cdots+x_{i} x_{j}^{k-2}+x_{j}^{k-1} .
$$

## Lemma

$\mathbf{V}\left(I_{G, k}\right) \subseteq \mathbb{C}^{n}$ consists of all $k$-colorings of $G$ for the set of colors consisting of the $k^{\text {th }}$ roots of unity


## Graph Ideal

## Definition

The $k$-coloring ideal of $G$ is the ideal $I_{G, k} \subseteq \mathbb{C}\left[x_{i} \mid i \in V\right]$ generated by:

$$
\begin{array}{ll}
\text { for all } i \in V: \quad x_{i}^{k}-1 \\
\text { for all } i j \in E: & x_{i}^{k-1}+x_{i}^{k-2} x_{j}+\cdots+x_{i} x_{j}^{k-2}+x_{j}^{k-1} .
\end{array}
$$

## Lemma

$\mathbf{V}\left(I_{G, k}\right) \subseteq \mathbb{C}^{n}$ consists of all $k$-colorings of $G$ for the set of colors consisting of the $k^{\text {th }}$ roots of unity

$$
\mu_{n}=\left\{1, \zeta_{k}, \zeta_{k}^{2}, \ldots, \zeta_{k}^{k-1}\right\}, \quad \zeta_{k}=e^{2 \pi i / k} .
$$

## Graph Ideal

## Definition

The $k$-coloring ideal of $G$ is the ideal $I_{G, k} \subseteq \mathbb{C}\left[x_{i} \mid i \in V\right]$ generated by:

$$
\begin{array}{ll}
\text { for all } i \in V: \quad x_{i}^{k}-1 \\
\text { for all } i j \in E: & x_{i}^{k-1}+x_{i}^{k-2} x_{j}+\cdots+x_{i} x_{j}^{k-2}+x_{j}^{k-1} .
\end{array}
$$

## Lemma

$\mathbf{V}\left(I_{G, k}\right) \subseteq \mathbb{C}^{n}$ consists of all $k$-colorings of $G$ for the set of colors consisting of the $k^{\text {th }}$ roots of unity

$$
\mu_{n}=\left\{1, \zeta_{k}, \zeta_{k}^{2}, \ldots, \zeta_{k}^{k-1}\right\}, \quad \zeta_{k}=e^{2 \pi i / k} .
$$

Proof. $\frac{\left(x_{i}^{k}-1\right)-\left(x_{j}^{k}-1\right)}{x_{i}-x_{j}}=x_{i}^{k-1}+x_{i}^{k-2} x_{j}+\cdots+x_{j}^{k-1}$.

## The Existence of Colorings

## Two Observations <br> - $G$ has a $k$-coloring $\Longleftrightarrow V\left(I_{G, k}\right) \neq \emptyset$. <br> - Hence there is a Gröbner basis criterion for the existence of a $k$-coloring.

```
3-Colorings
For 3-colorings, the ideal I}\mp@subsup{I}{G,3}{}\mathrm{ is generated by
for all i}\inV:\quad\mp@subsup{x}{i}{3}-
for all ij }\inE:\quad\mp@subsup{x}{i}{2}+\mp@subsup{x}{i}{}\mp@subsup{x}{j}{}+\mp@subsup{x}{j}{2}
```

These equations can be hard to solve!

```
Theorem
3-colorability is NP-complete.
```


## The Existence of Colorings

## Two Observations <br> - $G$ has a $k$-coloring $\Longleftrightarrow \mathbf{V}\left(I_{G, k}\right) \neq \emptyset$. <br> - Hence there is a Gröbner basis criterion for the existence of a $k$-coloring.

```
3-Colorings
For 3-colorings, the ideal I}\mp@subsup{I}{G,3}{}\mathrm{ is generated by
for all i\inV : }\quad\mp@subsup{x}{}{3}-
for all ij }\inE:\quad\mp@subsup{x}{i}{2}+\mp@subsup{x}{i}{}\mp@subsup{x}{j}{}+\mp@subsup{x}{j}{2
```


## These equations can be hard to solve!

## Theorem <br> 3-colorability is NP-complete.

## The Existence of Colorings

## Two Observations

- $G$ has a $k$-coloring $\Longleftrightarrow \mathbf{V}\left(I_{G, k}\right) \neq \emptyset$.
- Hence there is a Gröbner basis criterion for the existence of a $k$-coloring.

```
3-Colorings
For 3-colorings, the ideal I}\mp@subsup{I}{G,3}{}\mathrm{ is generated by
for all i\inV: }\quad\mp@subsup{x}{i}{3}-
for all ij }\inE:\quad\mp@subsup{x}{i}{2}+\mp@subsup{x}{i}{}\mp@subsup{x}{j}{}+\mp@subsup{x}{j}{2
```


## These equations can be hard to solve!

## Theorem <br> 3-colorability is NP-complete.

## The Existence of Colorings

## Two Observations

- $G$ has a $k$-coloring $\Longleftrightarrow \mathbf{V}\left(I_{G, k}\right) \neq \emptyset$.
- Hence there is a Gröbner basis criterion for the existence of a $k$-coloring.


## 3-Colorings

For 3-colorings, the ideal $I_{G, 3}$ is generated by

$$
\begin{array}{ll}
\text { for all } i \in V: & x_{i}^{3}-1 \\
\text { for all } i j \in E: & x_{i}^{2}+x_{i} x_{j}+x_{j}^{2} .
\end{array}
$$

These equations can be hard to solve!

## Theorem <br> 3 -colorability is NP-complete.

## The Existence of Colorings

## Two Observations

- $G$ has a $k$-coloring $\Longleftrightarrow \mathbf{V}\left(I_{G, k}\right) \neq \emptyset$.
- Hence there is a Gröbner basis criterion for the existence of a $k$-coloring.


## 3-Colorings

For 3-colorings, the ideal $I_{G, 3}$ is generated by

$$
\begin{array}{ll}
\text { for all } i \in V: & x_{i}^{3}-1 \\
\text { for all } i j \in E: & x_{i}^{2}+x_{i} x_{j}+x_{j}^{2} .
\end{array}
$$

These equations can be hard to solve!

## Theorem <br> 3-colorability is NP-complete.

## Example

This example of a graph with a 3 -coloring is due to Chao and Chen (1993).
Hillar and Windfeldt (2008)
compute the reduced Gröbner basis of the graph ideal $I_{G, 3}$ for lex with $x_{1}>\cdots>x_{12}$.

The reduced Gröbner basis is:


$$
\begin{aligned}
& \left\{x_{12}^{3}-1, x_{7}-x_{12}, x_{4}-x_{12}, x_{3}-x_{12}\right. \\
& x_{11}^{2}+x_{11} x_{12}+x_{12}^{2}, x_{9}-x_{11}, x_{6}-x_{11}, x_{2}-x_{11} \\
& x_{10}+x_{11}+x_{12}, \quad x_{8}+x_{11}+x_{12}, x_{5}+x_{11}+x_{12}
\end{aligned}
$$

$$
\left.x_{1}+x_{11}+x_{12}\right\}
$$

$\square$

## Example

This example of a graph with a 3 -coloring is due to Chao and Chen (1993). Hillar and Windfeldt (2008) compute the reduced Gröbner basis of the graph ideal $I_{G, 3}$ for lex with $x_{1}>\cdots>x_{12}$.

The reduced Gröbner basis is:


$$
\begin{aligned}
& \left\{x_{12}^{3}-1, x_{7}-x_{12}, x_{4}-x_{12}, x_{3}-x_{12}\right. \\
& \\
& x_{11}^{2}+x_{11} x_{12}+x_{12}^{2}, x_{9}-x_{11}, x_{6}-x_{11}, x_{2}-x_{11} \\
& \\
& x_{10}+x_{11}+x_{12}, x_{8}+x_{11}+x_{12}, x_{5}+x_{11}+x_{12} \\
& \\
& \left.x_{1}+x_{11}+x_{12}\right\}
\end{aligned}
$$

Note $x_{8}-x_{10}, x_{5}-x_{10}, x_{1}-x_{10} \in I_{G, 3}$.

## Uniquely k-Colorable Graphs

The Chao/Chen graph has essentially only one 3-coloring.

## Definition

A graph $G$ is uniquely $k$-colorable if it has a unique $k$-coloring up the permutation of the colors.

Hillar and Windfeldt show that unique $k$-colorability is easy to detect using Gröbner bases.
We start with a $k$-coloring of $G$ that uses all $k$ colors. Assume the $k$ colors occur among the last $k$ vertices. Then:

- Use variables $x_{1}, \ldots, x_{n-k}, y_{1}, \ldots, y_{k}$ with lex order
- Use these variables to label the vertices of $G$.


## Uniquely k-Colorable Graphs

The Chao/Chen graph has essentially only one 3-coloring.

## Definition

A graph $G$ is uniquely $k$-colorable if it has a unique $k$-coloring up the permutation of the colors.

Hillar and Windfeldt show that unique $k$-colorability is easy to detect using Gröbner bases.
We start with a $k$-coloring of $G$ that uses all $k$ colors. Assume the $k$ colors occur among the last $k$ vertices. Then:

- Use variables $x_{1}, \ldots, x_{n-k}, y_{1}, \ldots, y_{k}$ with lex order

$$
x_{1}>\cdots>x_{n-k}>y_{1}>\cdots>y_{k}
$$

- Use these variables to label the vertices of $G$.


## Uniquely k-Colorable Graphs

The Chao/Chen graph has essentially only one 3-coloring.

## Definition

A graph $G$ is uniquely $k$-colorable if it has a unique $k$-coloring up the permutation of the colors.

Hillar and Windfeldt show that unique $k$-colorability is easy to detect using Gröbner bases.
We start with a $k$-coloring of $G$ that uses all $k$ colors. Assume the $k$ colors occur among the last $k$ vertices. Then:

- Use variables $x_{1}, \ldots, x_{n-k}, y_{1}, \ldots, y_{k}$ with lex order

$$
x_{1}>\cdots>x_{n-k}>y_{1}>\cdots>y_{k}
$$

- Use these variables to label the vertices of $G$.


## Some Interesting Polynomials

Consider the following polynomials:

$$
\begin{aligned}
& y_{k}^{k}-1 \\
& h_{j}\left(y_{j}, \ldots, y_{k}\right)=\sum_{\alpha_{j}+\cdots+\alpha_{k}=j} y_{j}^{\alpha_{j}} \cdots y_{k}^{\alpha_{k}}, \quad j=1, \ldots, k-1 \\
& x_{i}-y_{j}, \quad \operatorname{color}\left(x_{i}\right)=\operatorname{color}\left(y_{j}\right), j \geq 2 \\
& x_{i}+y_{2}+\cdots+y_{k}, \quad \operatorname{color}\left(x_{i}\right)=\operatorname{color}\left(y_{1}\right) .
\end{aligned}
$$

In this notation, the Gröbner basis given earlier is:

$$
\begin{aligned}
& \left\{y_{3}^{3}-1,\right. \\
& \\
& h_{2}\left(y_{2}, y_{3}\right)=y_{2}^{2}+y_{2} y_{3}+y_{3}^{2}, h_{1}\left(y_{1}, y_{2}, y_{3}\right)=y_{1}+y_{2}+y_{3}, \\
& x_{7}-y_{3}, x_{4}-y_{3}, x_{3}-y_{3}, x_{9}-y_{2}, x_{6}-y_{2}, x_{2}-y_{2}, \\
& \left.x_{8}+y_{2}+y_{3}, x_{5}+y_{2}+y_{3}, x_{1}+y_{2}+y_{3}\right\} .
\end{aligned}
$$

## Some Interesting Polynomials

Consider the following polynomials:

$$
\begin{aligned}
& y_{k}^{k}-1 \\
& h_{j}\left(y_{j}, \ldots, y_{k}\right)=\sum_{\alpha_{j}+\cdots+\alpha_{k}=j} y_{j}^{\alpha_{j}} \cdots y_{k}^{\alpha_{k}}, \quad j=1, \ldots, k-1 \\
& x_{i}-y_{j}, \quad \operatorname{color}\left(x_{i}\right)=\operatorname{color}\left(y_{j}\right), j \geq 2 \\
& x_{i}+y_{2}+\cdots+y_{k}, \quad \operatorname{color}\left(x_{i}\right)=\operatorname{color}\left(y_{1}\right) .
\end{aligned}
$$

In this notation, the Gröbner basis given earlier is:

$$
\begin{aligned}
& \left\{y_{3}^{3}-1,\right. \\
& h_{2}\left(y_{2}, y_{3}\right)=y_{2}^{2}+y_{2} y_{3}+y_{3}^{2}, h_{1}\left(y_{1}, y_{2}, y_{3}\right)=y_{1}+y_{2}+y_{3}, \\
& x_{7}-y_{3}, x_{4}-y_{3}, x_{3}-y_{3}, x_{9}-y_{2}, x_{6}-y_{2}, x_{2}-y_{2}, \\
& \left.x_{8}+y_{2}+y_{3}, x_{5}+y_{2}+y_{3}, x_{1}+y_{2}+y_{3}\right\} .
\end{aligned}
$$

## A Theorem

Summary:

- $G$ has vertices $x_{1}, \ldots, x_{n-k}, y_{1}, \ldots, y_{k}$.
- $G$ has a $k$-coloring where $y_{1}, \ldots, y_{k}$ get all the colors.
- $\mathbb{C}[\mathbf{x}, \mathbf{y}]$ has lex with $x_{1}>\cdots>x_{n-k}>y_{1}>\cdots>y_{k}$.

Using this data, we create:

- The coloring ideal $I_{G, k} \subseteq \mathbb{C}[\mathbf{x}, \mathbf{y}]$.
- The $n$ polynomials $g_{1}, \ldots, g_{n}$ given by

Theorem (Fillar and Windfeldt)
The following are equivalent:

## A Theorem

Summary:

- $G$ has vertices $x_{1}, \ldots, x_{n-k}, y_{1}, \ldots, y_{k}$.
- $G$ has a $k$-coloring where $y_{1}, \ldots, y_{k}$ get all the colors.
- $\mathbb{C}[\mathbf{x}, \mathbf{y}]$ has lex with $x_{1}>\cdots>x_{n-k}>y_{1}>\cdots>y_{k}$.

Using this data, we create:

- The coloring ideal $I_{G, k} \subseteq \mathbb{C}[\mathbf{x}, \mathbf{y}]$.
- The $n$ polynomials $g_{1}, \ldots, g_{n}$ given by

$$
y_{k}^{k}-1, \quad h_{j}\left(y_{j}, \ldots, y_{k}\right), \quad x_{i}-y_{j}, \quad x_{i}+y_{2}+\cdots+y_{k}
$$

## Theorem (-filar and Windieldt)

The following are equivalent:

## A Theorem

Summary:

- $G$ has vertices $x_{1}, \ldots, x_{n-k}, y_{1}, \ldots, y_{k}$.
- $G$ has a $k$-coloring where $y_{1}, \ldots, y_{k}$ get all the colors.
- $\mathbb{C}[\mathbf{x}, \mathbf{y}]$ has lex with $x_{1}>\cdots>x_{n-k}>y_{1}>\cdots>y_{k}$.

Using this data, we create:

- The coloring ideal $I_{G, k} \subseteq \mathbb{C}[\mathbf{x}, \mathbf{y}]$.
- The $n$ polynomials $g_{1}, \ldots, g_{n}$ given by

$$
y_{k}^{k}-1, \quad h_{j}\left(y_{j}, \ldots, y_{k}\right), x_{i}-y_{j}, \quad x_{i}+y_{2}+\cdots+y_{k}
$$

## Theorem (Hillar and Windfeldt)

The following are equivalent:

- $G$ is uniquely $k$-colorable.
- $g_{1}, \ldots, g_{n} \in I_{G, k}$.
- $\left\{g_{1}, \ldots, g_{n}\right\}$ is the reduced Gröbner basis for $I_{G, k}$.


## A Final Amusement

To solve this sudoku, use:

- 81 variables $x_{i j}, 1 \leq i, j \leq 9$.
- Relabel the 9 variables for red squares as $y_{1}, \ldots, y_{9}$.
- The graph ideal $I_{G, 9}$.
- The 9 polynomials $y_{9}{ }^{9}-1$, $h_{8}\left(y_{8}, y_{9}\right), h_{7}\left(y_{7}, y_{8}, y_{9}\right)$, $h_{6}\left(y_{6}, y_{7}, y_{8}, y_{9}\right), \ldots$, $h_{1}\left(y_{1}, \ldots, y_{9}\right)=y_{1}+\cdots+y_{9}$.
- The 16 polynomials $x_{31}-y_{7}$,

|  |  |  |  | 3 | 5 |  |  |  |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
|  | 1 |  | 2 |  |  | 9 |  |  |
| 7 |  | 6 |  |  |  | 2 |  |  |
| 6 |  |  | 5 |  |  |  | 3 |  |
| 2 |  |  |  | 4 |  |  |  | 9 |
|  | 3 |  |  |  | 1 |  |  | 5 |
|  |  | 3 |  |  |  | 4 |  | 8 |
|  |  | 4 |  |  | 6 |  | 7 |  |
|  |  |  | 3 | 1 |  |  |  |  | $x_{33}-y_{6}, x_{37}-y_{2}, \ldots$

Assuming a unique solution, the Gröbner basis of the ideal generated by these polynomials will contain $x_{11}-y_{i}$, etc. This will tell us how to fill in the blank squares!

## Comments and References

- This is a terrible way to solve a $9 \times 9$ sudoku. Doug Leonard has been able to implement this in Magma, but only by working over the finite field $\mathbb{F}_{11}$ and limiting interreductions to generators of degree at most 4.
- On the other hand, doing the $4 \times 4$ sudoku this way makes an excellent student project.


## Reference

## Comments and References

- This is a terrible way to solve a $9 \times 9$ sudoku. Doug Leonard has been able to implement this in Magma, but only by working over the finite field $\mathbb{F}_{11}$ and limiting interreductions to generators of degree at most 4.
- On the other hand, doing the $4 \times 4$ sudoku this way makes an excellent student project.


## Reference

## Comments and References

- This is a terrible way to solve a $9 \times 9$ sudoku. Doug Leonard has been able to implement this in Magma, but only by working over the finite field $\mathbb{F}_{11}$ and limiting interreductions to generators of degree at most 4.
- On the other hand, doing the $4 \times 4$ sudoku this way makes an excellent student project.


## Reference

- C. Hillar, T. Windfeldt, Algebraic characterization of uniquely vertex colorable graphs, J. Comb. Th., Ser. B 98 (2008), 400-414.


## Snapshot \#2: Join-Meet Ideals

Graphs are not the only combinatorial objects that give interesting ideals. Here we explore ideals associated to finite lattices.

## Definition

A lattice is a partially ordered set $L$ such that every $a, b \in L$ have a $\sup a \vee b$ and an inf $a \wedge b$.

All lattices in this talk will be assumed to be finite.
Definition
A lattice $L$ is:

Every distributive lattice is modular; the converse is not true.

## Snapshot \#2: Join-Meet Ideals

Graphs are not the only combinatorial objects that give interesting ideals. Here we explore ideals associated to finite lattices.

## Definition

A lattice is a partially ordered set $L$ such that every $a, b \in L$ have a $\sup a \vee b$ and an inf $a \wedge b$.

All lattices in this talk will be assumed to be finite.

## Definition

A lattice $L$ is:


[^0]
## Snapshot \#2: Join-Meet Ideals

Graphs are not the only combinatorial objects that give interesting ideals. Here we explore ideals associated to finite lattices.

## Definition

A lattice is a partially ordered set $L$ such that every $a, b \in L$ have a $\sup a \vee b$ and an inf $a \wedge b$.

All lattices in this talk will be assumed to be finite.

## Definition

A lattice $L$ is:

- distributive if $a \wedge(b \vee c)=(a \wedge b) \vee(a \wedge c)$ for all $a, b, c \in L$.

[^1]
## Snapshot \#2: Join-Meet Ideals

Graphs are not the only combinatorial objects that give interesting ideals. Here we explore ideals associated to finite lattices.

## Definition

A lattice is a partially ordered set $L$ such that every $a, b \in L$ have a $\sup a \vee b$ and an inf $a \wedge b$.

All lattices in this talk will be assumed to be finite.

## Definition

A lattice $L$ is:

- distributive if $a \wedge(b \vee c)=(a \wedge b) \vee(a \wedge c)$ for all $a, b, c \in L$.
- modular if $a \leq b$ implies $a \vee(c \wedge b)=(a \vee c) \wedge b$ for all $c \in L$.

Every distributive lattice is modular; the converse is not true.

## Snapshot \#2: Join-Meet Ideals

Graphs are not the only combinatorial objects that give interesting ideals. Here we explore ideals associated to finite lattices.

## Definition

A lattice is a partially ordered set $L$ such that every $a, b \in L$ have a $\sup a \vee b$ and an inf $a \wedge b$.

All lattices in this talk will be assumed to be finite.

## Definition

A lattice $L$ is:

- distributive if $a \wedge(b \vee c)=(a \wedge b) \vee(a \wedge c)$ for all $a, b, c \in L$.
- modular if $a \leq b$ implies $a \vee(c \wedge b)=(a \vee c) \wedge b$ for all $c \in L$.

Every distributive lattice is modular; the converse is not true.

## Join-Meet Ideals

## Definition

Let $L$ be a finite lattice and let $k[L]$ be the polynomial rings whose variables are the elements of $L$. Then the join-meet ideal of $L$ is

$$
I_{L}=\langle a b-(a \vee b)(a \wedge b) \mid a, b \in L\rangle \subseteq k[L] .
$$

A natural question concerns how properties of the lattice $L$ relate to properties of the ideal $I_{L}$. Here is a nice example.

## Theorem (Hibi)

The join-meet ideal $l_{L}$ is prime if and only if the lattice $L$ is distributive.

We now discuss some of the interesting relations between Gröbner bases and join-meet ideals.

## Join-Meet Ideals

## Definition

Let $L$ be a finite lattice and let $k[L]$ be the polynomial rings whose variables are the elements of $L$. Then the join-meet ideal of $L$ is

$$
I_{L}=\langle a b-(a \vee b)(a \wedge b) \mid a, b \in L\rangle \subseteq k[L]
$$

A natural question concerns how properties of the lattice $L$ relate to properties of the ideal $I_{L}$. Here is a nice example.

Theorem (-fibi)
The join-meet ideal $I_{L}$ is prime if and only if the lattice $L$ is distributive.

We now discuss some of the interesting relations between Gröbner bases and join-meet ideals.

## Join-Meet Ideals

## Definition

Let $L$ be a finite lattice and let $k[L]$ be the polynomial rings whose variables are the elements of $L$. Then the join-meet ideal of $L$ is

$$
I_{L}=\langle a b-(a \vee b)(a \wedge b) \mid a, b \in L\rangle \subseteq k[L]
$$

A natural question concerns how properties of the lattice $L$ relate to properties of the ideal $I_{L}$. Here is a nice example.

## Theorem (Hibi)

The join-meet ideal $I_{L}$ is prime if and only if the lattice $L$ is distributive.
We now discuss some of the interesting relations between Gröbner bases and join-meet ideals.

## Join-Meet Ideals

## Definition

Let $L$ be a finite lattice and let $k[L]$ be the polynomial rings whose variables are the elements of $L$. Then the join-meet ideal of $L$ is

$$
I_{L}=\langle a b-(a \vee b)(a \wedge b) \mid a, b \in L\rangle \subseteq k[L]
$$

A natural question concerns how properties of the lattice $L$ relate to properties of the ideal $I_{L}$. Here is a nice example.

## Theorem (Hibi)

The join-meet ideal $I_{L}$ is prime if and only if the lattice $L$ is distributive.

We now discuss some of the interesting relations between Gröbner bases and join-meet ideals.

## Gröbner Bases and Distributive Lattices

We first give a Gröbner basis criterion for a lattice to be distributive.

## Theorem

Let $L$ be a lattice. The following are equivalent:
(1) $L$ is distributive.
(2) $I_{L}$ is prime.
(3) $\{a b-(a \vee b)(a \wedge b) \mid a, b \in L$ incomparable $\}$ is a

Gröbner basis for $I_{L}$ for any monomial order satisfying
$a b>(a \vee b)(a \wedge b)$ when $a, b$ are incomparable.
$(1) \Leftrightarrow(2) \Rightarrow(3)$ was proved by Hibi in 1987
$(3) \Rightarrow(1)$ was noted by Qureshi in 2012.

## Gröbner Bases and Distributive Lattices

We first give a Gröbner basis criterion for a lattice to be distributive.

## Theorem

Let $L$ be a lattice. The following are equivalent:
(1) $L$ is distributive.
(2) IL is prime.
3) $\{a b-(a \vee b)(a \wedge b) \mid a, b \in L$ incomparable $\}$ is a Gröbner basis for $I_{L}$ for any monomial order satisfying $a b>(a \vee b)(a \wedge b)$ when $a, b$ are incomparable.
$\square$
$(1) \Leftrightarrow(2) \Rightarrow(3)$ was proved by Hibi in 1987 $(3) \Rightarrow(1)$ was noted by Qureshi in 2012.

## Gröbner Bases and Distributive Lattices

We first give a Gröbner basis criterion for a lattice to be distributive.

## Theorem

Let $L$ be a lattice. The following are equivalent:
(1) $L$ is distributive.
(2) $I_{L}$ is prime.

$(1) \Leftrightarrow(2) \Rightarrow(3)$ was proved by Hibi in 1987
$(3) \Rightarrow(1)$ was noted by Qureshi in 2012.

## Gröbner Bases and Distributive Lattices

We first give a Gröbner basis criterion for a lattice to be distributive.

## Theorem

Let $L$ be a lattice. The following are equivalent:
(1) $L$ is distributive.
(2) $I_{L}$ is prime.
(3) $\{a b-(a \vee b)(a \wedge b) \mid a, b \in L$ incomparable $\}$ is $a$ Gröbner basis for $I_{L}$ for any monomial order satisfying $a b>(a \vee b)(a \wedge b)$ when $a, b$ are incomparable.
$(1) \Leftrightarrow(2) \Rightarrow(3)$ was proved by Hibi in 1987
$(3) \Rightarrow(1)$ was noted by Qureshi in 2012.

## Gröbner Bases and Distributive Lattices

We first give a Gröbner basis criterion for a lattice to be distributive.

## Theorem

Let $L$ be a lattice. The following are equivalent:
(1) $L$ is distributive.
(2) $I_{L}$ is prime.
(3) $\{a b-(a \vee b)(a \wedge b) \mid a, b \in L$ incomparable $\}$ is a Gröbner basis for $I_{L}$ for any monomial order satisfying $a b>(a \vee b)(a \wedge b)$ when $a, b$ are incomparable.
$(1) \Leftrightarrow(2) \Rightarrow(3)$ was proved by Hibi in 1987.
$(3) \Rightarrow(1)$ was noted by Qureshi in 2012.

## Modular Non-Distributive Lattices

We next study $I_{L}$ for some modular non-distributive lattices $L$. Here, Gröbner bases play a key role in the proof.

We begin with two closely related lattices. The one on the left is distributive; the one on the right is modular but not distributive.


The lattice on the right will be denoted $L_{k}$.

## Some Radical Modular Lattices

Theorem (Ene and Hibi)
The ideal $I_{L_{k}}$ is radical.


## Proof.

## Some Radical Modular Lattices

Theorem (Ene and Hibi)
The ideal $I_{L_{k}}$ is radical.


## Proof.

- Step 1: Write down a Gröbner basis of $I=I_{L_{k}}$. The basis includes $y_{k}^{2} z-y_{k} z^{2}$ and $x_{k+1} z-y_{k} z$.
- Step 2: Prove that $I=\left\langle I, x_{k+1}-y_{k}\right\rangle \cap\langle I, z\rangle$ using Gröbner bases.
- Step 3: Prove that $\left\langle I, x_{k+1}-y_{k}\right\rangle$ and $\langle I, z\rangle$ have squarefree initial ideals.

Since ideals with squarefree initial ideals are radical, the theorem follows from Steps 2 and 3.

Note that the initial ideal of $I_{L_{k}}$ is not squarefree.

## Some Radical Modular Lattices

Theorem (Ene and Hibi)
The ideal $I_{L_{k}}$ is radical.


## Proof.

- Step 1: Write down a Gröbner basis of $I=I_{L_{k}}$. The basis includes $y_{k}^{2} z-y_{k} z^{2}$ and $x_{k+1} z-y_{k} z$.
- Step 2: Prove that $I=\left\langle I, x_{k+1}-y_{k}\right\rangle \cap\langle I, z\rangle$ using Gröbner bases.
- Step 3: Prove that $\left\langle I, x_{k+1}-y_{k}\right\rangle$ and $\langle I, z\rangle$ have squarefree initial ideals.

Since ideals with squarefree initial ideals are radical, the theorem follows from Steps 2 and 3.

Note that the initial ideal of $I_{L_{k}}$ is not squarefree.

## Some Radical Modular Lattices

## Theorem (Ene and Hibi)

The ideal $I_{L_{k}}$ is radical.


## Proof.

- Step 1: Write down a Gröbner basis of $I=I_{L_{k}}$. The basis includes $y_{k}^{2} z-y_{k} z^{2}$ and $x_{k+1} z-y_{k} z$.
- Step 2: Prove that $I=\left\langle I, x_{k+1}-y_{k}\right\rangle \cap\langle I, z\rangle$ using Gröbner bases.
- Step 3: Prove that $\left\langle I, x_{k+1}-y_{k}\right\rangle$ and $\langle I, z\rangle$ have squarefree initial ideals.

Since 'd'ea's with squarefree initial ideals are radical, the theorem follows from Steps 2 and 3.

Note that the initial ideal of $I_{L_{k}}$ is not squarefree.

## Some Radical Modular Lattices

## Theorem (Ene and Hibi)

The ideal $I_{L_{k}}$ is radical.


## Proof.

- Step 1: Write down a Gröbner basis of $I=I_{L_{k}}$. The basis includes $y_{k}^{2} z-y_{k} z^{2}$ and $x_{k+1} z-y_{k} z$.
- Step 2: Prove that $I=\left\langle I, x_{k+1}-y_{k}\right\rangle \cap\langle I, z\rangle$ using Gröbner bases.
- Step 3: Prove that $\left\langle I, x_{k+1}-y_{k}\right\rangle$ and $\langle I, z\rangle$ have squarefree initial ideals.

Since ideals with squarefree initial ideals are radical, the theorem follows from Steps 2 and 3.

Note that the initial ideal of $I_{L_{k}}$ is not squarefree.

## Some Radical Modular Lattices

## Theorem (Ene and Hibi)

The ideal $I_{L_{k}}$ is radical.


## Proof.

- Step 1: Write down a Gröbner basis of $I=I_{L_{k}}$. The basis includes $y_{k}^{2} z-y_{k} z^{2}$ and $x_{k+1} z-y_{k} z$.
- Step 2: Prove that $I=\left\langle I, x_{k+1}-y_{k}\right\rangle \cap\langle I, z\rangle$ using Gröbner bases.
- Step 3: Prove that $\left\langle I, x_{k+1}-y_{k}\right\rangle$ and $\langle I, z\rangle$ have squarefree initial ideals.

Since ideals with squarefree initial ideals are radical, the theorem follows from Steps 2 and 3.

Note that the initial ideal of $I_{L_{k}}$ is not squarefree.

## Some Radical Modular Lattices

## Theorem (Ene and Hibi)

The ideal $I_{L_{k}}$ is radical.


## Proof.

- Step 1: Write down a Gröbner basis of $I=I_{L_{k}}$. The basis includes $y_{k}^{2} z-y_{k} z^{2}$ and $x_{k+1} z-y_{k} z$.
- Step 2: Prove that $I=\left\langle I, x_{k+1}-y_{k}\right\rangle \cap\langle I, z\rangle$ using Gröbner bases.
- Step 3: Prove that $\left\langle I, x_{k+1}-y_{k}\right\rangle$ and $\langle I, z\rangle$ have squarefree initial ideals.

Since ideals with squarefree initial ideals are radical, the theorem follows from Steps 2 and 3.

Note that the initial ideal of $I_{L_{k}}$ is not squarefree.

## References

## References

- T. Hibi, Distributive lattices, affine semigroup rings and algebras with straightening laws, in Commutative Algebra and Combinatorics (Kyoto, 1985), North-Holland, Amsterdam, 1987, 93-109,
- A. Qureshi, Indespensible Hibi relations and Gröbner bases, arXiv:math.CA/1203.0438.
- V. Ene and T. Hibi, The join-meet ideal of a finite lattice, arXiv:math.AC/1203.6794.


## Snapshot \#3: The Nullstellensatz

There are many proofs of the Nullstellensatz. Here we present a proof due to Lev Glebsky that uses Gröbner bases.

## Notation

- $k[u, \boldsymbol{x}], \boldsymbol{x}=\left(x_{1}, \ldots, x_{n-1}\right)$, is a polynomial ring in $n$ variables.
- $a \in k$ gives the evaluation map $\mathrm{ev}_{a}: k[u, \boldsymbol{x}] \rightarrow k[\boldsymbol{x}]$ defined by $\mathrm{ev}_{a}(p)=p(a, \boldsymbol{x})$.


## Theorem

Let $k$ be an algebraically closed field and let $I \subsetneq k[u, x]$ be an ideal. Then there is $a \in k$ such that $\mathrm{ev}_{a}(I) \subsetneq k[\boldsymbol{x}]$

Applying this theorem repeatedly, we can find $a_{1}, \ldots, a_{n} \in k$ with $\mathrm{ev}_{a_{1}, \ldots, a_{n}}(I) \subsetneq k$, hence $\mathrm{ev}_{a_{1}, \ldots, a_{n}}(I)=\{0\}$. It follows that $\mathbf{V}(I) \neq \emptyset$. This in turn implies the Nullstellensatz.

## Snapshot \#3: The Nullstellensatz

There are many proofs of the Nullstellensatz. Here we present a proof due to Lev Glebsky that uses Gröbner bases.

## Notation

- $k[u, \boldsymbol{x}], \boldsymbol{x}=\left(x_{1}, \ldots, x_{n-1}\right)$, is a polynomial ring in $n$ variables.
- $a \in k$ gives the evaluation map $\mathrm{ev}_{\mathrm{a}}: k[u, \boldsymbol{x}] \rightarrow k[\boldsymbol{x}]$ defined by $\mathrm{ev}_{\mathrm{a}}(p)=p(a, \boldsymbol{x})$.


## Theorem

Let $k$ be an algebraically closed field and let $I \subsetneq k[u, x]$ be an ideal. Then there is $a \in k$ such that $\mathrm{ev}_{a}(I) \subsetneq k[\boldsymbol{x}]$.


## Snapshot \#3: The Nullstellensatz

There are many proofs of the Nullstellensatz. Here we present a proof due to Lev Glebsky that uses Gröbner bases.

## Notation

- $k[u, \boldsymbol{x}], \boldsymbol{x}=\left(x_{1}, \ldots, x_{n-1}\right)$, is a polynomial ring in $n$ variables.
- $a \in k$ gives the evaluation map $\mathrm{ev}_{\mathrm{a}}: k[u, \boldsymbol{x}] \rightarrow k[\boldsymbol{x}]$ defined by $\mathrm{ev}_{\mathrm{a}}(p)=p(a, \boldsymbol{x})$.


## Theorem

Let $k$ be an algebraically closed field and let $I \subsetneq k[u, \boldsymbol{x}]$ be an ideal. Then there is $a \in k$ such that $\mathrm{ev}_{a}(I) \subsetneq k[\boldsymbol{x}]$.

Applying this theorem repeatedly, we can find $a_{1}, \ldots, a_{n} \in k$ with $\mathrm{ev}_{a_{1}, \ldots, a_{n}}(I) \subsetneq k$, hence $\mathrm{ev}_{a_{1}, \ldots, a_{n}}(I)=\{0\}$. It follows that $\mathbf{V}(I) \neq \emptyset$. This in turn implies the Nullstellensatz.

## Case I

- Assume $I \cap k[u]=\langle p\rangle, p \neq 0$. Then $p$ is nonconstant since $I$ is a proper ideal.
- Write $p=\prod_{i=1}^{r}\left(u-a_{i}\right)^{m_{i}}$. Then

$$
I=\langle p\rangle+I=\bigcap_{i=1}^{r}\left(\left\langle u-a_{i}\right)^{m_{i}}+I\right),
$$

so that $\left\langle u-a_{i}\right\rangle^{m_{i}}+l$ is proper for some index $i$.

- Observe that

$$
\left\langle u-a_{i}\right\rangle^{m_{i}}+I \subseteq\left\langle u-a_{i}\right\rangle+I \subseteq \sqrt{\left\langle u-a_{i}\right\rangle^{m_{i}}+l} .
$$

Hence $\left\langle u-a_{i}\right\rangle+l$ is also a proper ideal.

- It follows easily that $\mathrm{ev}_{a_{i}}(I) \subsetneq k[\boldsymbol{x}]$.


## Case I

- Assume $I \cap k[u]=\langle p\rangle, p \neq 0$. Then $p$ is nonconstant since $I$ is a proper ideal.
- Write $p=\prod_{i=1}^{r}\left(u-a_{i}\right)^{m_{i}}$. Then

$$
I=\langle p\rangle+I=\bigcap_{i=1}^{r}\left(\left\langle u-a_{i}\right\rangle^{m_{i}}+I\right)
$$

so that $\left\langle u-a_{i}\right\rangle^{m_{i}}+l$ is proper for some index $i$.

- Observe that

$$
\left\langle u-a_{i}\right\rangle^{m_{i}}+I \subseteq\left\langle u-a_{i}\right\rangle+I \subseteq \sqrt{\left\langle u-a_{i}\right\rangle^{m_{i}}+l} .
$$

Hence $\left\langle u-a_{i}\right\rangle+I$ is also a proper ideal.

- It follows easily that $\mathrm{ev}_{a_{i}}(I) \subsetneq k[\boldsymbol{x}]$.


## Case I

- Assume $I \cap k[u]=\langle p\rangle, p \neq 0$. Then $p$ is nonconstant since $l$ is a proper ideal.
- Write $p=\prod_{i=1}^{r}\left(u-a_{i}\right)^{m_{i}}$. Then

$$
I=\langle p\rangle+I=\bigcap_{i=1}^{r}\left(\left\langle u-a_{i}\right\rangle^{m_{i}}+I\right)
$$

so that $\left\langle u-a_{i}\right\rangle^{m_{i}}+I$ is proper for some index $i$.

- Observe that

$$
\left\langle u-a_{i}\right\rangle^{m_{i}}+l \subseteq\left\langle u-a_{i}\right\rangle+I \subseteq \sqrt{\left\langle u-a_{i}\right\rangle^{m_{i}}+l} .
$$

Hence $\left\langle u-a_{i}\right\rangle+l$ is also a proper ideal.

- It follows easily that $\mathrm{ev}_{a_{i}}(I) \subsetneq k[x]$.


## Case I

- Assume $I \cap k[u]=\langle p\rangle, p \neq 0$. Then $p$ is nonconstant since $l$ is a proper ideal.
- Write $p=\prod_{i=1}^{r}\left(u-a_{i}\right)^{m_{i}}$. Then

$$
I=\langle p\rangle+I=\bigcap_{i=1}^{r}\left(\left\langle u-a_{i}\right\rangle^{m_{i}}+I\right)
$$

so that $\left\langle u-a_{i}\right\rangle^{m_{i}}+I$ is proper for some index $i$.

- Observe that

$$
\left\langle u-a_{i}\right\rangle^{m_{i}}+I \subseteq\left\langle u-a_{i}\right\rangle+I \subseteq \sqrt{\left\langle u-a_{i}\right\rangle^{m_{i}}+I}
$$

Hence $\left\langle u-a_{i}\right\rangle+I$ is also a proper ideal.

- It follows easily that $\mathrm{ev}_{\mathrm{a}_{i}}(I) \subsetneq k[\boldsymbol{x}]$.


## Case II

This is where we use Gröbner bases.

- Assume $I \cap k[u]=\{0\}$. This easily implies that

$$
J:=\text { ideal of } k(u)[\boldsymbol{x}] \text { generated by } I
$$

is a proper ideal of $k(u)[\boldsymbol{x}]$.

- Let $G$ be a reduced Gröbner basis of $J$. Elements of $G$ are polynomials in $\boldsymbol{x}$ with coefficients in $k(u)$. Let $h \in k[u]$ be the LCM of all denominators of the coefficients of elements of $G$.
- Since $k$ is infinite, we can pick $a \in k$ such that $h(a) \neq 0$.
- Let $R_{a}=\{f / g \in k(u) \mid f, g \in k[u], g(a) \neq 0\}$. Then the evaluation map $\mathrm{ev}_{a}: k[u, \boldsymbol{x}]=k[u][\boldsymbol{x}] \rightarrow k[\boldsymbol{x}]$ extends to an evaluation map

$$
\mathrm{ev}_{a}: R_{a}[\boldsymbol{x}] \longrightarrow k[\boldsymbol{x}]
$$

## Case II

This is where we use Gröbner bases.

- Assume $I \cap k[u]=\{0\}$. This easily implies that

$$
J:=\text { ideal of } k(u)[\boldsymbol{x}] \text { generated by } I
$$

is a proper ideal of $k(u)[\boldsymbol{x}]$.

- Let $G$ be a reduced Gröbner basis of $J$. Elements of $G$ are polynomials in $\boldsymbol{x}$ with coefficients in $k(u)$. Let $h \in k[u]$ be the LCM of all denominators of the coefficients of elements of $G$.
- Since $k$ is infinite, we can pick $a \in k$ such that $h(a) \neq 0$.
- Let $R_{a}=\{f / g \in k(u) \mid f, g \in k[u], g(a) \neq 0\}$. Then the evaluation
map eva $: k[u, \boldsymbol{x}]=k[u][\boldsymbol{x}] \rightarrow k[\boldsymbol{x}]$ extends to an evaluation map
$\mathrm{ev}_{\mathrm{a}}: R_{\mathrm{a}}[\mathrm{x}] \longrightarrow \mathrm{k}[\mathrm{x}]$


## Case II

This is where we use Gröbner bases.

- Assume $I \cap k[u]=\{0\}$. This easily implies that

$$
J:=\text { ideal of } k(u)[\boldsymbol{x}] \text { generated by } I
$$

is a proper ideal of $k(u)[\boldsymbol{x}]$.

- Let $G$ be a reduced Gröbner basis of $J$. Elements of $G$ are polynomials in $\boldsymbol{x}$ with coefficients in $k(u)$. Let $h \in k[u]$ be the LCM of all denominators of the coefficients of elements of $G$.
- Since $k$ is infinite, we can pick $a \in k$ such that $h(a) \neq 0$.



## Case II

This is where we use Gröbner bases.

- Assume $I \cap k[u]=\{0\}$. This easily implies that

$$
J:=\text { ideal of } k(u)[\boldsymbol{x}] \text { generated by } I
$$

is a proper ideal of $k(u)[\boldsymbol{x}]$.

- Let $G$ be a reduced Gröbner basis of $J$. Elements of $G$ are polynomials in $\boldsymbol{x}$ with coefficients in $k(u)$. Let $h \in k[u]$ be the LCM of all denominators of the coefficients of elements of $G$.
- Since $k$ is infinite, we can pick $a \in k$ such that $h(a) \neq 0$.
- Let $R_{a}=\{f / g \in k(u) \mid f, g \in k[u], g(a) \neq 0\}$. Then the evaluation map ev ${ }_{a}: k[u, \boldsymbol{x}]=k[u][\boldsymbol{x}] \rightarrow k[\boldsymbol{x}]$ extends to an evaluation map

$$
\mathrm{ev}_{a}: R_{a}[\boldsymbol{x}] \longrightarrow k[\boldsymbol{x}]
$$

## Case II, Continued

## Lemma

$\mathrm{ev}_{\mathrm{a}}(G)$ is a Gröbner basis in $k[\boldsymbol{x}]$.
Proof.
Exercise!

- Since $G$ is a Gröbner basis of a proper ideal $J \subseteq k(x)[x]$, none of its elements lie in $k(u)$. Hence no elements of $\mathrm{ev}_{a}(G)$ lie in $k$.
- Then $\left\langle\mathrm{ev}_{a}(G)\right\rangle$ is proper in $k[x]$ since $\mathrm{ev}_{a}(G)$ is a Gröbner basis.
- Applying the division algorithm to $I \subseteq J=\langle G\rangle$ shows that $\mathrm{ev}_{a}(I) \subseteq\left\langle\mathrm{ev}_{a}(G)\right\rangle$. Hence $\mathrm{ev}_{a}(I)$ is a proper ideal of $k[\boldsymbol{x}]$. QED


## Reference

## Case II, Continued

## Lemma

$\mathrm{ev}_{a}(G)$ is a Gröbner basis in $k[\boldsymbol{x}]$.

## Proof.

Exercise!

- Since $G$ is a Gröbner basis of a proper ideal $J \subseteq k(x)[x]$, none of its elements lie in $k(u)$. Hence no elements of $\mathrm{ev}_{a}(G)$ lie in $k$.
- Then $\left\langle\mathrm{ev}_{a}(G)\right\rangle$ is proper in $k[\boldsymbol{x}]$ since $\mathrm{ev}_{a}(G)$ is a Gröbner basis.
- Applying the division algorithm to $I \subseteq J=\langle G\rangle$ shows that $\mathrm{ev}_{\mathrm{a}}(I) \subseteq\left\langle\mathrm{ev}_{\mathrm{a}}(G)\right\rangle$. Hence $\mathrm{ev}_{\mathrm{a}}(I)$ is a proper ideal of $k[\boldsymbol{x}]$. QED


## Reference

## Case II, Continued

## Lemma

$\mathrm{ev}_{a}(G)$ is a Gröbner basis in $k[x]$.

## Proof.

## Exercise!

- Since $G$ is a Gröbner basis of a proper ideal $J \subseteq k(x)[\boldsymbol{x}]$, none of its elements lie in $k(u)$. Hence no elements of $\mathrm{ev}_{a}(G)$ lie in $k$.
- Then $\left\langle\mathrm{ev}_{a}(G)\right\rangle$ is proper in $k[x]$ since $\mathrm{ev}_{a}(G)$ is a Gröbner basis.
- Applying the division algorithm to $I \subseteq J=\langle G\rangle$ shows that $\mathrm{ev}_{\mathrm{a}}(I) \subseteq\left\langle\mathrm{ev}_{a}(G)\right\rangle$. Hence $\mathrm{ev}_{\mathrm{a}}(I)$ is a proper ideal of $k[\boldsymbol{x}]$. QED


## Reference

## Case II, Continued

## Lemma

$\mathrm{ev}_{a}(G)$ is a Gröbner basis in $k[\boldsymbol{x}]$.

## Proof.

## Exercise!

- Since $G$ is a Gröbner basis of a proper ideal $J \subseteq k(x)[\boldsymbol{x}]$, none of its elements lie in $k(u)$. Hence no elements of $\mathrm{ev}_{a}(G)$ lie in $k$.
- Then $\left\langle\mathrm{ev}_{a}(G)\right\rangle$ is proper in $k[x]$ since $\mathrm{ev}_{a}(G)$ is a Gröbner basis.



## Case II, Continued

## Lemma

$\mathrm{ev}_{a}(G)$ is a Gröbner basis in $k[\boldsymbol{x}]$.

## Proof.

## Exercise!

- Since $G$ is a Gröbner basis of a proper ideal $J \subseteq k(x)[\boldsymbol{x}]$, none of its elements lie in $k(u)$. Hence no elements of $\mathrm{ev}_{a}(G)$ lie in $k$.
- Then $\left\langle\mathrm{ev}_{a}(G)\right\rangle$ is proper in $k[x]$ since $\mathrm{ev}_{a}(G)$ is a Gröbner basis.
- Applying the division algorithm to $I \subseteq J=\langle G\rangle$ shows that $\mathrm{ev}_{a}(I) \subseteq\left\langle\mathrm{ev}_{a}(G)\right\rangle$. Hence $\mathrm{ev}_{a}(I)$ is a proper ideal of $k[\boldsymbol{x}]$.


## Case II, Continued

## Lemma

$\mathrm{ev}_{a}(G)$ is a Gröbner basis in $k[\boldsymbol{x}]$.

## Proof.

## Exercise!

- Since $G$ is a Gröbner basis of a proper ideal $J \subseteq k(x)[\boldsymbol{x}]$, none of its elements lie in $k(u)$. Hence no elements of $\mathrm{ev}_{a}(G)$ lie in $k$.
- Then $\left\langle\mathrm{ev}_{a}(G)\right\rangle$ is proper in $k[x]$ since $\mathrm{ev}_{a}(G)$ is a Gröbner basis.
- Applying the division algorithm to $I \subseteq J=\langle G\rangle$ shows that $\mathrm{ev}_{a}(I) \subseteq\left\langle\mathrm{ev}_{a}(G)\right\rangle$. Hence $\mathrm{ev}_{a}(I)$ is a proper ideal of $k[\boldsymbol{x}]$.


## Reference

- L. Glebsky, A proof of Hilbert's Nullstellensatz based on Groebner bases, arXiv:math.AC/1204.3128.


## Snapshot \#4: Geometric Theorem Discovery

Our final topic involves an application of comprehensive Gröbner systems to the problem of discovering the correct hypotheses that give an interesting theorem in geometry.

Our discussion was inspired by a 2007 paper of Montes and Recio.
We begin with a 2006 example of Sato and Suzuki that illustrates specialization of Gröbner bases.

## Example 1

Consider the ideal

$$
I:=\left\langle(u-1) x_{1}+x_{2}^{2}, u x_{2}+u\right\rangle \subseteq k[u, \boldsymbol{x}]=k\left[u, x_{1}, x_{2}\right] .
$$

As in our discussion of the Nullstellensatz, I generates the ideal

$$
J=\left\langle x_{1}+\frac{x_{2}^{2}}{u-1}, x_{2}+1\right\rangle \subset k(u)[\boldsymbol{x}]=k(u)\left[x_{1}, x_{2}\right] .
$$

The generators $G$ of $J$ are a lex Gröbner basis for $x_{1}>x_{2}$.
We will write $\bar{g}_{a}=\mathrm{ev}_{a}(g)=g(a, \boldsymbol{x})$ for $a \in k$ and $g \in k[u, \boldsymbol{x}]$. The previous lemma implies that when $a \neq 1, \bar{G}_{a}$ is a Gröbner basis in $k[\boldsymbol{x}]$. This is a simple example of specialization of Gröbner bases.

To make things more interesting, we go back to $I$, whose lex Gröbner basis for $x_{1}>x_{2}>u$ is

$$
\left\{u x_{1}-x_{1}+x_{2}^{2}, u x_{2}+u, x_{1} x_{2}+x_{1}-x_{2}^{3}-x_{2}^{2}\right\}
$$

There are two questions to ask about this situation.

## First Question

We will think of $u$ as a parameter in $\mathbb{A}^{1}$.
Does $G=\left\{u x_{1}-x_{1}+x_{2}^{2}, u x_{2}+u, x_{1} x_{2}+x_{1}-x_{2}^{3}-x_{2}^{2}\right\}$ remain a Gröbner basis (for lex with $x_{1}>x_{2}$ ) when the parameter $u$ is given a specific numerical value $a \in \mathbb{A}^{1}$ ?

Two observations:

- If $u=1$, then $\bar{G}_{1}=\left\{x_{2}^{2}, x_{2}+1, x_{1} x_{2}+x_{1}-x_{2}^{3}-x_{2}^{2}\right\}$, which generates $\langle 1\rangle$. Since $1 \notin\left\langle x_{2}^{2}, x_{2}, x_{1} x_{2}\right\rangle, \bar{G}_{1}$ is not a Gröbner basis.
- If $u=a \neq 0,1$, then one can show that $\bar{G}_{a}$ is a reduced Gröbner basis (up to constants)

General Question: How do Gröbner bases specialize?

## First Question

We will think of $u$ as a parameter in $\mathbb{A}^{1}$.
Does $G=\left\{u x_{1}-x_{1}+x_{2}^{2}, u x_{2}+u, x_{1} x_{2}+x_{1}-x_{2}^{3}-x_{2}^{2}\right\}$ remain a Gröbner basis (for lex with $x_{1}>x_{2}$ ) when the parameter $u$ is given a specific numerical value $a \in \mathbb{A}^{1}$ ?

Two observations:

- If $u=1$, then $\bar{G}_{1}=\left\{x_{2}^{2}, x_{2}+1, x_{1} x_{2}+x_{1}-x_{2}^{3}-x_{2}^{2}\right\}$, which generates $\langle 1\rangle$. Since $1 \notin\left\langle x_{2}^{2}, x_{2}, x_{1} x_{2}\right\rangle, \bar{G}_{1}$ is not a Gröbner basis.
- If $u=a \neq 0,1$, then one can show that $\bar{G}_{a}$ is a reduced Gröbner basis (up to constants).

General Question: How do Gröbner bases specialize?

## First Question

We will think of $u$ as a parameter in $\mathbb{A}^{1}$.
Does $G=\left\{u x_{1}-x_{1}+x_{2}^{2}, u x_{2}+u, x_{1} x_{2}+x_{1}-x_{2}^{3}-x_{2}^{2}\right\}$ remain a Gröbner basis (for lex with $x_{1}>x_{2}$ ) when the parameter $u$ is given a specific numerical value $a \in \mathbb{A}^{1}$ ?

Two observations:

- If $u=1$, then $\bar{G}_{1}=\left\{x_{2}^{2}, x_{2}+1, x_{1} x_{2}+x_{1}-x_{2}^{3}-x_{2}^{2}\right\}$, which generates $\langle 1\rangle$. Since $1 \notin\left\langle x_{2}^{2}, x_{2}, x_{1} x_{2}\right\rangle, \bar{G}_{1}$ is not a Gröbner basis.
- If $u=a \neq 0,1$, then one can show that $\bar{G}_{a}$ is a reduced Gröbner basis (up to constants).

General Question: How do Gröbner bases specialize?

## Second Question

Consider the systems of equations:

$$
(u-1) x_{1}+x_{2}^{2}=u x_{2}+u=0
$$

How does the number of solutions change as we vary $u \in \mathbb{A}^{1}$ ?

- $u=a \neq 0,1 \Rightarrow(a-1) x_{1}+x_{2}^{2}=x_{2}+1=0$ has a unique solution.
- $u=0 \Rightarrow-x_{1}+x_{2}^{2}=0$ has infinitely many solutions.
- $u=1 \Rightarrow x_{2}^{2}=x_{2}+1=0$ has no solutions.

General Question: How do we describe the number of solutions?

## Second Question

Consider the systems of equations:

$$
(u-1) x_{1}+x_{2}^{2}=u x_{2}+u=0
$$

How does the number of solutions change as we vary $u \in \mathbb{A}^{1}$ ?

- $u=a \neq 0,1 \Rightarrow(a-1) x_{1}+x_{2}^{2}=x_{2}+1=0$ has a unique solution.
- $u=0 \Rightarrow-x_{1}+x_{2}^{2}=0$ has infinitely many solutions.
- $u=1 \Rightarrow x_{2}^{2}=x_{2}+1=0$ has no solutions.

General Question: How do we describe the number of solutions?

## Second Question

Consider the systems of equations:

$$
(u-1) x_{1}+x_{2}^{2}=u x_{2}+u=0
$$

How does the number of solutions change as we vary $u \in \mathbb{A}^{1}$ ?

- $u=a \neq 0,1 \Rightarrow(a-1) x_{1}+x_{2}^{2}=x_{2}+1=0$ has a unique solution.
- $u=0 \Rightarrow-x_{1}+x_{2}^{2}=0$ has infinitely many solutions.
- $u=1 \Rightarrow x_{2}^{2}=x_{2}+1=0$ has no solutions.

General Question: How do we describe the number of solutions?

## Second Question

Consider the systems of equations:

$$
(u-1) x_{1}+x_{2}^{2}=u x_{2}+u=0
$$

How does the number of solutions change as we vary $u \in \mathbb{A}^{1}$ ?

- $u=a \neq 0,1 \Rightarrow(a-1) x_{1}+x_{2}^{2}=x_{2}+1=0$ has a unique solution.
- $u=0 \Rightarrow-x_{1}+x_{2}^{2}=0$ has infinitely many solutions.
- $u=1 \Rightarrow x_{2}^{2}=x_{2}+1=0$ has no solutions.

General Question: How do we describe the number of solutions?

## Second Question

Consider the systems of equations:

$$
(u-1) x_{1}+x_{2}^{2}=u x_{2}+u=0
$$

How does the number of solutions change as we vary $u \in \mathbb{A}^{1}$ ?

- $u=a \neq 0,1 \Rightarrow(a-1) x_{1}+x_{2}^{2}=x_{2}+1=0$ has a unique solution.
- $u=0 \Rightarrow-x_{1}+x_{2}^{2}=0$ has infinitely many solutions.
- $u=1 \Rightarrow x_{2}^{2}=x_{2}+1=0$ has no solutions.

General Question: How do we describe the number of solutions?

## Answers for the Example

Consider the following pairs:

$$
\begin{aligned}
& \left(S_{1}, G_{1}\right):=\left(\mathbb{A}^{1} \backslash\{0,1\},\left\{(u-1) x_{1}+x_{2}^{2}, u x_{2}+x\right\}\right) \\
& \left(S_{2}, G_{2}\right):=\left(\{0\},\left\{x_{1}-x_{2}^{2}\right\}\right) \\
& \left(S_{3}, G_{3}\right):=(\{1\},\{1\}) .
\end{aligned}
$$

The $S_{i}$ are called segments. Note that:

- $S_{i}$ is constructible, $S_{1} \cup S_{2} \cup S_{3}=\mathbb{A}^{1}$ is a partition.
- For $a \in S_{i}, \bar{G}_{i a}$ is a reduced Gröbner basis (up to constants).
- For $a \in S_{i},\left\langle\operatorname{Lt}\left(\bar{G}_{i a}\right)\right\rangle$ is independent of a.
- $\left\langle\operatorname{LT}\left(\bar{G}_{1}\right)\right\rangle=\left\langle x_{1}, x_{2}\right\rangle,\left\langle\operatorname{LT}\left({\overline{G_{2}}}_{2}\right)\right\rangle=\left\langle x_{1}\right\rangle,\left\langle\operatorname{LT}\left(\bar{G}_{3 a}\right)\right\rangle=\langle 1\rangle$ gives the number of solutions.

This is a minimal canonical comprehensive Gröbner system.

## Answers for the Example

Consider the following pairs:

$$
\begin{aligned}
& \left(S_{1}, G_{1}\right):=\left(\mathbb{A}^{1} \backslash\{0,1\},\left\{(u-1) x_{1}+x_{2}^{2}, u x_{2}+x\right\}\right) \\
& \left(S_{2}, G_{2}\right):=\left(\{0\},\left\{x_{1}-x_{2}^{2}\right\}\right) \\
& \left(S_{3}, G_{3}\right):=(\{1\},\{1\}) .
\end{aligned}
$$

The $S_{i}$ are called segments. Note that:

- $S_{i}$ is constructible, $S_{1} \cup S_{2} \cup S_{3}=\mathbb{A}^{1}$ is a partition.
- For $a \in S_{i}, \bar{G}_{i a}$ is a reduced Gröbner basis (up to constants).
- For $a \in S_{i},\left\langle L T\left(G_{i a}\right)\right\rangle$ is independent of a.
- $\left\langle\operatorname{Lt}\left(\overline{G_{1}}\right)\right\rangle=\left\langle x_{1}, x_{2}\right\rangle,\left\langle\operatorname{Lt}\left(\overline{G_{2 a}}\right)\right\rangle=\left\langle x_{1}\right\rangle,\left\langle\operatorname{LT}\left(\overline{G_{3 a}}\right)\right\rangle=\langle 1\rangle$ gives the
number of solutions.
This is a minimal canonical comprehensive Gröbner system.


## Answers for the Example

Consider the following pairs:

$$
\begin{aligned}
& \left(S_{1}, G_{1}\right):=\left(\mathbb{A}^{1} \backslash\{0,1\},\left\{(u-1) x_{1}+x_{2}^{2}, u x_{2}+x\right\}\right) \\
& \left(S_{2}, G_{2}\right):=\left(\{0\},\left\{x_{1}-x_{2}^{2}\right\}\right) \\
& \left(S_{3}, G_{3}\right):=(\{1\},\{1\}) .
\end{aligned}
$$

The $S_{i}$ are called segments. Note that:

- $S_{i}$ is constructible, $S_{1} \cup S_{2} \cup S_{3}=\mathbb{A}^{1}$ is a partition.
- For $a \in S_{i}, \bar{G}_{i a}$ is a reduced Gröbner basis (up to constants).
- For $a \in S_{i},\left\langle\operatorname{Lt}\left(\overline{G_{i a}}\right)\right\rangle$ is independent of $a$.
$\left\langle\operatorname{Lt}\left(\overline{G_{1}}\right)\right\rangle=\left\langle x_{1}, x_{2}\right\rangle,\left\langle\operatorname{LT}\left(\overline{G_{2}}\right)\right\rangle=\left\langle x_{1}\right\rangle,\left\langle\operatorname{LT}\left(\overline{G_{3 a}}\right)\right\rangle=\langle 1\rangle$ gives the
number of solutions.
This is a minimal canonical comprehensive Gröbner system.


## Answers for the Example

Consider the following pairs:

$$
\begin{aligned}
& \left(S_{1}, G_{1}\right):=\left(\mathbb{A}^{1} \backslash\{0,1\},\left\{(u-1) x_{1}+x_{2}^{2}, u x_{2}+x\right\}\right) \\
& \left(S_{2}, G_{2}\right):=\left(\{0\},\left\{x_{1}-x_{2}^{2}\right\}\right) \\
& \left(S_{3}, G_{3}\right):=(\{1\},\{1\}) .
\end{aligned}
$$

The $S_{i}$ are called segments. Note that:

- $S_{i}$ is constructible, $S_{1} \cup S_{2} \cup S_{3}=\mathbb{A}^{1}$ is a partition.
- For $a \in S_{i}, \bar{G}_{i a}$ is a reduced Gröbner basis (up to constants).
- For $a \in S_{i},\left\langle L \tau\left(\bar{G}_{i a}\right)\right\rangle$ is independent of $a$.
- $\left\langle\operatorname{LT}\left(\overline{G_{12}}\right)\right\rangle=\left\langle x_{1}, x_{2}\right\rangle,\left\langle\operatorname{LT}\left(\overline{G_{2}} a\right)\right\rangle=\left\langle x_{1}\right\rangle,\left\langle\operatorname{L\tau }\left(\overline{G_{3 a}}\right)\right\rangle=\langle 1\rangle$ gives the number of solutions.


## Answers for the Example

Consider the following pairs:

$$
\begin{aligned}
& \left(S_{1}, G_{1}\right):=\left(\mathbb{A}^{1} \backslash\{0,1\},\left\{(u-1) x_{1}+x_{2}^{2}, u x_{2}+x\right\}\right) \\
& \left(S_{2}, G_{2}\right):=\left(\{0\},\left\{x_{1}-x_{2}^{2}\right\}\right) \\
& \left(S_{3}, G_{3}\right):=(\{1\},\{1\}) .
\end{aligned}
$$

The $S_{i}$ are called segments. Note that:

- $S_{i}$ is constructible, $S_{1} \cup S_{2} \cup S_{3}=\mathbb{A}^{1}$ is a partition.
- For $a \in S_{i}, \bar{G}_{i a}$ is a reduced Gröbner basis (up to constants).
- For $a \in S_{i},\left\langle L \tau\left(\bar{G}_{i a}\right)\right\rangle$ is independent of $a$.
- $\left\langle\operatorname{LT}\left(\overline{G_{12}}\right)\right\rangle=\left\langle x_{1}, x_{2}\right\rangle,\left\langle\operatorname{LT}\left(\overline{G_{2}} a\right)\right\rangle=\left\langle x_{1}\right\rangle,\left\langle\operatorname{L\tau }\left(\overline{G_{3 a}}\right)\right\rangle=\langle 1\rangle$ gives the number of solutions.
This is a minimal canonical comprehensive Gröbner system.


## MCCGS

Let $I \subseteq k[\boldsymbol{u}, \boldsymbol{x}]$ be an ideal with variables $\boldsymbol{x}=\left(x_{1}, \ldots, x_{n}\right)$ and parameters $\boldsymbol{u}=\left(u_{1}, \ldots, u_{m}\right)$. Fix an order $>$ on $k[\boldsymbol{x}]$.

## Definition

A minimal canonical comprehensive Gröbner system for I and > consists of pairs $\left(S_{i}, G_{i}\right)$ satisfying:

> The segments $S_{i}$ give a constructible partition of $\mathbb{A}^{m}$.
> For $\boldsymbol{a} \in S_{i}$, setting $\boldsymbol{u}=\boldsymbol{a}$ gives a reduced Gröbner basis $\overline{G_{i}} \boldsymbol{a}$ (up to constants).
> For $\boldsymbol{a} \in S_{i},\left\langle\operatorname{LT}\left(\overline{G_{i}} \boldsymbol{a}\right)\right\rangle$ is independent of $\boldsymbol{a}$.
> No smaller partition exists with these properties.

This definition is due to Manubens and Montes in 2009.

## MCCGS

Let $I \subseteq k[\boldsymbol{u}, \boldsymbol{x}]$ be an ideal with variables $\boldsymbol{x}=\left(x_{1}, \ldots, x_{n}\right)$ and parameters $\boldsymbol{u}=\left(u_{1}, \ldots, u_{m}\right)$. Fix an order $>$ on $k[\boldsymbol{x}]$.

## Definition

A minimal canonical comprehensive Gröbner system for I and > consists of pairs $\left(S_{i}, G_{i}\right)$ satisfying:

- The segments $S_{i}$ give a constructible partition of $\mathbb{A}^{m}$.
- For $\mathbf{a} \in S_{i}$, setting $u=a$ gives a reduced Gröbner basis $\bar{G}_{i}$ (up to constants).
- For $\boldsymbol{a} \in S_{i},\left\langle\operatorname{LT}\left(\overline{\mathcal{C}}_{i}\right)\right)$ is independent of $a$.
- No smaller partition exists with these properties.

$$
\text { This definition is due to Manubens and Montes in } 2009 .
$$

## MCCGS

Let $I \subseteq k[\boldsymbol{u}, \boldsymbol{x}]$ be an ideal with variables $\boldsymbol{x}=\left(x_{1}, \ldots, x_{n}\right)$ and parameters $\boldsymbol{u}=\left(u_{1}, \ldots, u_{m}\right)$. Fix an order $>$ on $k[\boldsymbol{x}]$.

## Definition

A minimal canonical comprehensive Gröbner system for I and > consists of pairs $\left(S_{i}, G_{i}\right)$ satisfying:

- The segments $S_{i}$ give a constructible partition of $\mathbb{A}^{m}$.
- For $\boldsymbol{a} \in S_{i}$, setting $\boldsymbol{u}=\boldsymbol{a}$ gives a reduced Gröbner basis $\overline{G_{i}} \boldsymbol{a}$ (up to constants).
- For $\boldsymbol{a} \in S_{i},\left\langle\operatorname{Lt}\left(\bar{G}_{i} a\right)\right\rangle$ is independent of $\boldsymbol{a}$.
- No smaller partition exists with these properties.

$$
\text { This definition is due to Manubens and Montes in } 2009 .
$$

## MCCGS

Let $I \subseteq k[\boldsymbol{u}, \boldsymbol{x}]$ be an ideal with variables $\boldsymbol{x}=\left(x_{1}, \ldots, x_{n}\right)$ and parameters $\boldsymbol{u}=\left(u_{1}, \ldots, u_{m}\right)$. Fix an order $>$ on $k[\boldsymbol{x}]$.

## Definition

A minimal canonical comprehensive Gröbner system for I and > consists of pairs $\left(S_{i}, G_{i}\right)$ satisfying:

- The segments $S_{i}$ give a constructible partition of $\mathbb{A}^{m}$.
- For $\boldsymbol{a} \in S_{i}$, setting $\boldsymbol{u}=\boldsymbol{a}$ gives a reduced Gröbner basis $\overline{G_{i}} \boldsymbol{a}$ (up to constants).
- For $\boldsymbol{a} \in S_{i},\left\langle\operatorname{Lt}\left(\overline{G_{i}} \boldsymbol{a}\right)\right\rangle$ is independent of $\boldsymbol{a}$.
- No smaller partition exists with these properties.

$$
\text { This definition is due to Manubens and Montes in } 2009 .
$$

## MCCGS

Let $I \subseteq k[\boldsymbol{u}, \boldsymbol{x}]$ be an ideal with variables $\boldsymbol{x}=\left(x_{1}, \ldots, x_{n}\right)$ and parameters $\boldsymbol{u}=\left(u_{1}, \ldots, u_{m}\right)$. Fix an order $>$ on $k[\boldsymbol{x}]$.

## Definition

A minimal canonical comprehensive Gröbner system for I and > consists of pairs $\left(S_{i}, G_{i}\right)$ satisfying:

- The segments $S_{i}$ give a constructible partition of $\mathbb{A}^{m}$.
- For $\boldsymbol{a} \in S_{i}$, setting $\boldsymbol{u}=\boldsymbol{a}$ gives a reduced Gröbner basis $\overline{G_{i}} \boldsymbol{a}$ (up to constants).
- For $\boldsymbol{a} \in S_{i},\left\langle\operatorname{LT}\left(\bar{G}_{i} \boldsymbol{a}\right)\right\rangle$ is independent of $\boldsymbol{a}$.
- No smaller partition exists with these properties.

$$
\text { This definition is due to Manubens and Montes in } 2009 .
$$

## MCCGS

Let $I \subseteq k[\boldsymbol{u}, \boldsymbol{x}]$ be an ideal with variables $\boldsymbol{x}=\left(x_{1}, \ldots, x_{n}\right)$ and parameters $\boldsymbol{u}=\left(u_{1}, \ldots, u_{m}\right)$. Fix an order $>$ on $k[\boldsymbol{x}]$.

## Definition

A minimal canonical comprehensive Gröbner system for I and > consists of pairs $\left(S_{i}, G_{i}\right)$ satisfying:

- The segments $S_{i}$ give a constructible partition of $\mathbb{A}^{m}$.
- For $\boldsymbol{a} \in S_{i}$, setting $\boldsymbol{u}=\boldsymbol{a}$ gives a reduced Gröbner basis $\overline{G_{i}} \boldsymbol{a}$ (up to constants).
- For $\boldsymbol{a} \in S_{i},\left\langle\operatorname{Lt}\left({\overline{G_{i}}}_{\boldsymbol{a}}\right)\right\rangle$ is independent of $\boldsymbol{a}$.
- No smaller partition exists with these properties.

This definition is due to Manubens and Montes in 2009.

## A False Theorem

Let $C D$ be the diameter of a circle of radius 1 . Fix $A$. Then:

- The line $\overleftrightarrow{A E}$ is tangent to the circle at $E$.
- The lines $\overleftarrow{A C}$ and $\overleftarrow{E D}$ meet at $F$.


## Challenge: Discover reasonable

 hypotheses on A to make the theorem true.

## A False Theorem

Let $C D$ be the diameter of a circle of radius 1. Fix $A$. Then:

- The line $\overleftrightarrow{A E}$ is tangent to the circle at $E$.
- The lines $\overleftrightarrow{A C}$ and $\overleftrightarrow{E D}$ meet at $F$.


## False Theorem

$$
A E=A F .
$$

## Challenge: Discover reasonable

 hypotheses on $A$ to make the theorem true.

## A False Theorem

Let $C D$ be the diameter of a circle of radius 1. Fix $A$. Then:

- The line $\overleftrightarrow{A E}$ is tangent to the circle at $E$.
- The lines $\overleftrightarrow{A C}$ and $\overleftrightarrow{E D}$ meet at $F$.

$$
\begin{aligned}
& \text { False Theorem } \\
& A E=A F \text {. }
\end{aligned}
$$

Challenge: Discover reasonable hypotheses on $A$ to make the theorem true.


## Hypotheses

Set $A=\left(u_{1}, u_{2}\right)$

$$
\begin{aligned}
& E=\left(x_{1}, x_{2}\right) \\
& F=\left(x_{3}, x_{4}\right) .
\end{aligned}
$$

Then:

- $\overleftrightarrow{A E} \perp \overleftrightarrow{O E}$ gives $h_{1}:=\left(x_{1}-u_{1}\right)\left(x_{1}-1\right)+\left(x_{2}-u_{2}\right) x_{2}$.
- $O E=1$ gives
$h_{2}:=\left(x_{1}-1\right)^{2}+x_{2}^{2}-1$.
- $F=\overleftrightarrow{A C} \cap \overleftrightarrow{E D}$ gives
$h_{3}:=u_{1} x_{4}-u_{2} x_{3}$.

$h_{4}:=x_{4}\left(x_{1}-2\right)-x_{2}\left(x_{3}-2\right)$.


## More Hypotheses

We also need to assume:

- $A \neq C$, so

$$
u_{1} \neq 0 \text { or } u_{2} \neq 0
$$

- $E \neq D$, so
$x_{2} \neq 2$.
Conclusion: The ideal that describes this problem is the saturation
$I:=\left\langle h_{1}, h_{2}, h_{3}, h_{4}\right\rangle:\left\langle\left(x_{2}-2\right) u_{1},\left(x_{2}-2\right) u_{2}\right\rangle^{\infty}$ in the ring $k\left[u_{1}, u_{2}, x_{1}, x_{2}, x_{3}, x_{4}\right]$.



## Strategy

Our false theorem asserts $A E=A F$. This gives

$$
g:=\left(u_{1}-x_{1}\right)^{2}+\left(u_{2}-x_{2}\right)^{2}-\left(u_{1}-x_{3}\right)^{2}-\left(u_{2}-x_{4}\right)^{2}
$$

## Strategy

Compute a MCCGS for the ideal

$$
I+\langle g\rangle \subseteq k\left[u_{1}, u_{2}, x_{1}, x_{2}, x_{3}, x_{4}\right], \quad u_{1}, u_{2} \text { parameters. }
$$

## Intuition

The false theorem is true for those $u=a \in \mathbb{A}^{2}$ for which

$$
\emptyset \neq \mathrm{V}\left(\bar{T}_{a}+\langle\bar{g} a\rangle\right) \subseteq \mathbb{A}^{4} .
$$

## Strategy

Our false theorem asserts $A E=A F$. This gives

$$
g:=\left(u_{1}-x_{1}\right)^{2}+\left(u_{2}-x_{2}\right)^{2}-\left(u_{1}-x_{3}\right)^{2}-\left(u_{2}-x_{4}\right)^{2}
$$

## Strategy

Compute a MCCGS for the ideal

$$
I+\langle g\rangle \subseteq k\left[u_{1}, u_{2}, x_{1}, x_{2}, x_{3}, x_{4}\right], \quad u_{1}, u_{2} \text { parameters. }
$$

## Intuition

The false theorem is true for those $\boldsymbol{u}=\mathbf{a} \in \mathbb{A}^{2}$ for which

$$
\emptyset \neq \mathbf{V}\left(\bar{l}_{\mathbf{a}}+\langle\bar{g} \mathbf{a}\rangle\right) \subseteq \mathbb{A}^{4}
$$

## The MCCGS

The MCCGS for $I+\langle g\rangle \subseteq k\left[u_{1}, u_{2}, x_{1}, x_{2}, x_{3}, x_{4}\right]$ under lex order with $x_{1}>x_{2}>x_{3}>x_{4}$ is

$$
\left(S_{1}, G_{1}\right) \cup \cdots \cup\left(S_{6}, G_{6}\right)
$$

## The MCCGS

The MCCGS for $I+\langle g\rangle \subseteq k\left[u_{1}, u_{2}, x_{1}, x_{2}, x_{3}, x_{4}\right]$ under lex order with $x_{1}>x_{2}>x_{3}>x_{4}$ is

$$
\left(S_{1}, G_{1}\right) \cup \cdots \cup\left(S_{6}, G_{6}\right)
$$

The $S_{i}$ and Leading Terms

| $i$ | $S_{i}$ | $\operatorname{LT}\left(\overline{G_{i}} \mathbf{a}\right)$ |
| :---: | :---: | :---: |
| 1 | $\mathbb{A}^{2} \backslash\left(\mathbf{V}\left(u_{1}^{2}+u_{2}^{2}-2 u_{1}\right) \cup \mathbf{V}\left(u_{1}\right)\right)$ | 1 |
| 2 | $\mathbf{V}\left(u_{1}^{2}+u_{2}^{2}-2 u_{1}\right) \backslash\{(0,0),(2,0)\}$ | $x_{1}, x_{2}, x_{3}, x_{4}^{2}$ |
| 3 | $\mathbf{V}\left(u_{1}\right) \backslash\{(0,0),(0, \pm i)\}$ | $x_{1}, x_{2}, x_{3}, x_{4}^{2}$ |
| 4 | $\{(0, \pm i)\}$ | $x_{1}, x_{2}, x_{3}, x_{4}$ |
| 5 | $\{(2,0)\}$ | $x_{1}, x_{2}^{2}, x_{3}, x_{4}^{2}$ |
| 6 | $\{(0,0)\}$ | $x_{1}, x_{2}, x_{3}^{2}, x_{4}^{2}$ |

## Consequences of the MCCGS

- We can ignore

$$
S_{4}=\{(0, \pm i)\}, \quad S_{5}=\{(2,0)\}, \quad S_{6}=\{(0,0)\}
$$

The first is not real, and the second and third are impossible since $E \neq D$ and $A \neq C$.

- $G_{1}=\{1\}$ on $S_{1}=\mathbb{A}^{2} \backslash\left(V\left(u_{1}^{2}+u_{2}^{2}-2 u_{1}\right) \cup V\left(u_{1}\right)\right)$ implies

- Hence the "false theorem" $A E=A F$ (i.e., $g=0$ ) cannot follow from our hypotheses (i.e., the ideal $I$ ) unless the point $A$ comes from $V\left(u_{1}^{2}+u_{2}^{2}-2 u_{1}\right) \cup V\left(u_{1}\right)$.
- This holds $\Leftrightarrow A$ is on the circle or the tangent at $C$.


## Consequences of the MCCGS

- We can ignore

$$
S_{4}=\{(0, \pm i)\}, \quad S_{5}=\{(2,0)\}, \quad S_{6}=\{(0,0)\}
$$

The first is not real, and the second and third are impossible since $E \neq D$ and $A \neq C$.

- $G_{1}=\{1\}$ on $S_{1}=\mathbb{A}^{2} \backslash\left(\mathbf{V}\left(u_{1}^{2}+u_{2}^{2}-2 u_{1}\right) \cup \mathbf{V}\left(u_{1}\right)\right)$ implies

$$
\mathbf{V}(I+\langle g\rangle)=\emptyset \text { if } \boldsymbol{u}=\mathbf{a} \notin \mathbf{V}\left(u_{1}^{2}+u_{2}^{2}-2 u_{1}\right) \cup \mathbf{V}\left(u_{1}\right)
$$

- Hence the "false theorem" $A E=A F$ (i.e., $g=0$ ) cannot follow from our hypotheses (i.e., the ideal $I$ ) unless the point $A$ comes from $\mathbf{V}\left(u_{1}^{2}+u_{2}^{2}-2 u_{1}\right) \cup \mathbf{V}\left(u_{1}\right)$.
- This holds $\Leftrightarrow A$ is on the circle or the tangent at $C$.


## Consequences of the MCCGS

- We can ignore

$$
S_{4}=\{(0, \pm i)\}, \quad S_{5}=\{(2,0)\}, \quad S_{6}=\{(0,0)\}
$$

The first is not real, and the second and third are impossible since $E \neq D$ and $A \neq C$.

- $G_{1}=\{1\}$ on $S_{1}=\mathbb{A}^{2} \backslash\left(\mathbf{V}\left(u_{1}^{2}+u_{2}^{2}-2 u_{1}\right) \cup \mathbf{V}\left(u_{1}\right)\right)$ implies

$$
\mathbf{V}(I+\langle g\rangle)=\emptyset \text { if } \boldsymbol{u}=\mathbf{a} \notin \mathbf{V}\left(u_{1}^{2}+u_{2}^{2}-2 u_{1}\right) \cup \mathbf{V}\left(u_{1}\right)
$$

- Hence the "false theorem" $A E=A F$ (i.e., $g=0$ ) cannot follow from our hypotheses (i.e., the ideal $I$ ) unless the point $A$ comes from $\mathbf{V}\left(u_{1}^{2}+u_{2}^{2}-2 u_{1}\right) \cup \mathbf{V}\left(u_{1}\right)$.


## Consequences of the MCCGS

- We can ignore

$$
S_{4}=\{(0, \pm i)\}, \quad S_{5}=\{(2,0)\}, \quad S_{6}=\{(0,0)\}
$$

The first is not real, and the second and third are impossible since $E \neq D$ and $A \neq C$.

- $G_{1}=\{1\}$ on $S_{1}=\mathbb{A}^{2} \backslash\left(\mathbf{V}\left(u_{1}^{2}+u_{2}^{2}-2 u_{1}\right) \cup \mathbf{V}\left(u_{1}\right)\right)$ implies

$$
\mathbf{V}(I+\langle g\rangle)=\emptyset \text { if } \boldsymbol{u}=\mathbf{a} \notin \mathbf{V}\left(u_{1}^{2}+u_{2}^{2}-2 u_{1}\right) \cup \mathbf{V}\left(u_{1}\right)
$$

- Hence the "false theorem" $A E=A F$ (i.e., $g=0$ ) cannot follow from our hypotheses (i.e., the ideal $I$ ) unless the point $A$ comes from $\mathbf{V}\left(u_{1}^{2}+u_{2}^{2}-2 u_{1}\right) \cup \mathbf{V}\left(u_{1}\right)$.
- This holds $\Leftrightarrow A$ is on the circle or the tangent at $C$.


## Conclusion



In order for $A E=A F$, we must have
" $A$ is on the circle or the tangent at $C$ "
This is detected by the remaining segments of the MCCGS:

## A on the circle: $S_{2}=$ $V\left(u_{1}^{2}+u_{2}^{2}-2 u_{1}\right) \backslash\{(0,0),(2,0)\}$

$A$ on the tangent: $S_{3}=$
$\mathbf{V}\left(u_{1}\right) \backslash\{(0,0),(0, \pm i)\}$

## Conclusion



In order for $A E=A F$, we must have " $A$ is on the circle or the tangent at $C$ "
This is detected by the remaining segments of the MCCGS:
$A$ on the circle: $S_{2}=$
$\mathbf{V}\left(u_{1}^{2}+u_{2}^{2}-2 u_{1}\right) \backslash\{(0,0),(2,0)\}$
$A$ on the tangent: $S_{3}=$
$\mathbf{V}\left(u_{1}\right) \backslash\{(0,0),(0, \pm i)\}$
A on the Circle
$A E=A F$ is true but boring.

## Conclusion



In order for $A E=A F$, we must have " $A$ is on the circle or the tangent at $C$ "
This is detected by the remaining segments of the MCCGS:
$A$ on the circle: $S_{2}=$
$\mathbf{V}\left(u_{1}^{2}+u_{2}^{2}-2 u_{1}\right) \backslash\{(0,0),(2,0)\}$
$A$ on the tangent: $S_{3}=$ $\mathbf{V}\left(u_{1}\right) \backslash\{(0,0),(0, \pm i)\}$

## $A$ on the Circle

$A E=A F$ is true but boring.

## Conclusion



In order for $A E=A F$, we must have
" $A$ is on the circle or the tangent at $C$ "
This is detected by the remaining segments of the MCCGS:
$A$ on the circle: $S_{2}=$
$\mathbf{V}\left(u_{1}^{2}+u_{2}^{2}-2 u_{1}\right) \backslash\{(0,0),(2,0)\}$
$A$ on the tangent: $S_{3}=$ $\mathbf{V}\left(u_{1}\right) \backslash\{(0,0),(0, \pm i)\}$

## $A$ on the Circle

$A E=A F$ is true but boring.


## A on the Tangent

When $A$ is on the tangent, we get the picture to the right.

There are two choices for $E$ :

- For $E_{1}$, we get
$F_{1}=E_{1}$, so $A E=A F$ is true but boring.
- For $E_{2}$, we get an interesting theorem!

This is automatic theorem discovery using MCCGS.


## References

## References

- M. Manubens, A. Montes, Minimal canonical comprehensive Groebner systems, J. of Symbolic Comput. 44 (2009) 463-478.
- A. Montes, T. Recio, Automatic discovery of geometric theorems using minimal canonical comprehensive Groebner systems, In: Automatic Deduction in Geometry, Proc. ADG 2006, Lect. Notes in AI 4869, Springer, 2007, pp. 113-138.


## Recent Development

## References

## References

- M. Manubens, A. Montes, Minimal canonical comprehensive Groebner systems, J. of Symbolic Comput. 44 (2009) 463-478.
- A. Montes, T. Recio, Automatic discovery of geometric theorems using minimal canonical comprehensive Groebner systems, In: Automatic Deduction in Geometry, Proc. ADG 2006, Lect. Notes in AI 4869, Springer, 2007, pp. 113-138.


## Recent Development

- A. Montes, M. Wibmer, Gröbner bases for polynomial systems with parameters, J. of Symbolic Comput. 45 (2010) 1391-1425.
- Introduces Gröbner covers.
- "Therefore the main focus of this article is not on the efficiency of the algorithm but on computing a Gröbner system that has as few segments as possible and satisfies some additional nice properties."


[^0]:    Every distributive lattice is modular; the converse is not true

[^1]:    Every distributive lattice is modular; the converse is not true

