Chordal structure and polynomial systems

Diego Cifuentes

Laboratory for Information and Decision Systems
Electrical Engineering and Computer Science
Massachusetts Institute of Technology

Joint work with **Pablo A. Parrilo** (MIT)

UC Davis - November 2014

Polynomial ideals

Consider a system of m polynomial equations in n variables:

$$f_i(x_0, \ldots, x_{n-1}) = 0, \qquad i = 1, \ldots, m$$

The objective is to "solve" these equations.

Polynomial ideals

Consider a system of m polynomial equations in n variables:

$$f_i(x_0, \ldots, x_{n-1}) = 0, \qquad i = 1, \ldots, m$$

The objective is to "solve" these equations.

What it is solving?

- Decide if it is consistent.
- Find a solution.
- Describe all solutions.
- Find a Gröbner basis.

Polynomial ideals

Example:

$$I = \langle x_0^2 x_1 x_2 + 2x_1 + 1,\ x_1^2 + x_2,\ x_1 + x_2,\ x_2 x_3 \rangle$$

Polynomial ideals

Example:

$$I = \langle x_0^2 x_1 x_2 + 2x_1 + 1,\ x_1^2 + x_2,\ x_1 + x_2,\ x_2 x_3 \rangle$$

$$I = \{(x_0^2 x_1 x_2 + 2x_1 + 1)\, g_1 + (x_1^2 + x_2)\, g_2 + (x_1 + x_2) g_3 + (x_2 x_3) g_4 : g_1, g_2, g_3, g_3\}$$

Polynomial ideals

Example:

$$I = \langle x_0^2 x_1 x_2 + 2x_1 + 1,\ x_1^2 + x_2,\ x_1 + x_2,\ x_2 x_3 \rangle$$

$$I = \{(x_0^2 x_1 x_2 + 2x_1 + 1)\, g_1 + (x_1^2 + x_2)\, g_2 + (x_1 + x_2) g_3 + (x_2 x_3) g_4 : g_1, g_2, g_3, g_3\}$$

$$I = \{(x_0^2 - 3)\, g_1 + (x_1 - 1)\, g_2 + (x_2 + 1) g_3 + (x_3) g_4 : g_1, g_2, g_3, g_3\}$$

Polynomial ideals

Example:

$$I = \langle x_0^2 x_1 x_2 + 2x_1 + 1,\ x_1^2 + x_2,\ x_1 + x_2,\ x_2 x_3 \rangle$$

$$I = \{(x_0^2 x_1 x_2 + 2x_1 + 1)\, g_1 + (x_1^2 + x_2)\, g_2 + (x_1 + x_2) g_3 + (x_2 x_3) g_4 : g_1, g_2, g_3, g_3\}$$

$$I = \{(x_0^2 - 3)\, g_1 + (x_1 - 1)\, g_2 + (x_2 + 1) g_3 + (x_3) g_4 : g_1, g_2, g_3, g_3\}$$

Gröbner basis:

$$I = \langle x_0^2 - 3,\ x_1 - 1,\ x_2 + 1,\ x_3 \rangle$$

There are two solutions:

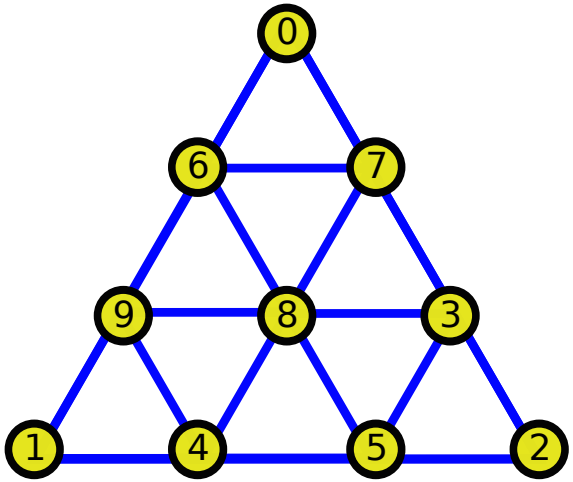
$$\mathbf{V}(I) = (\sqrt{3}, 1, -1, 0),\ \ (-\sqrt{3}, 1, -1, 0)$$

Polynomial ideals

Example 2:

Let I be given by the equations:

$$x_i^3 - 1 = 0, \qquad 0 \leq i \leq 9$$
$$x_i^2 + x_i x_j + x_j^2 = 0, \qquad (i,j) \text{ edge}$$

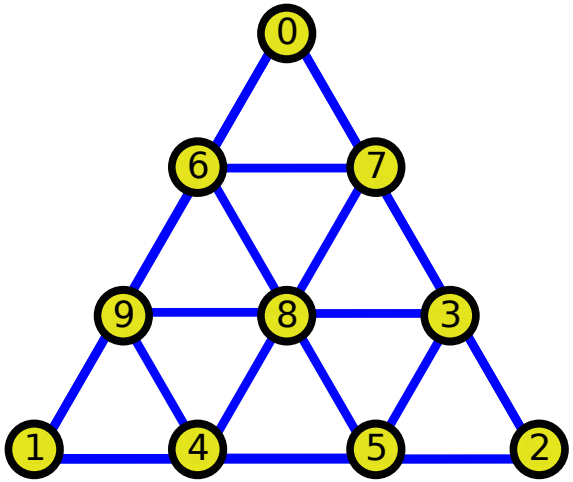


Polynomial ideals

Example 2:

Let I be given by the equations:

$$x_i^3 - 1 = 0, \qquad 0 \leq i \leq 9$$
$$x_i^2 + x_i x_j + x_j^2 = 0, \qquad (i,j) \text{ edge}$$



Gröbner basis:

$$I = \langle x_0 - x_8,\ x_1 - x_8,\ x_2 - x_8,\ x_3 + x_8 + x_9,\ x_4 + x_8 + x_9,$$
$$x_5 - x_9,\ x_6 + x_8 + x_9,\ x_7 - x_9,\ x_8^2 + x_8 x_9 + x_9^2,\ x_9^3 - 1 \rangle$$

There are six solutions: three choices for x_9, two choices for x_8.

Gröbner bases

- Given an ordering of the variables $x_0 > x_1 > \ldots > x_{n-1}$ there is a unique reduced *lex Gröbner basis*.
- The system is inconsistent iff the reduced Gröbner basis is $\langle 1 \rangle$.
- If the system has finite solutions, we can find them recursively: solve a univariate polynomial in x_{n-1}, for each solution $\hat{x}_{n-1}$, solve a univariate polynomial in x_{n-2}, etc.
- For an arbitrary ideal I, we can get the *elimination ideals*

$$\text{elim}_l(I) = I \cap \mathbb{K}[x_l, x_{l+1}, \ldots, x_{n-1}]$$

Gröbner bases

- Given an ordering of the variables $x_0 > x_1 > \ldots > x_{n-1}$ there is a unique reduced *lex Gröbner basis*.
- The system is inconsistent iff the reduced Gröbner basis is $\langle 1 \rangle$.
- If the system has finite solutions, we can find them recursively: solve a univariate polynomial in x_{n-1}, for each solution $\hat{x}_{n-1}$, solve a univariate polynomial in x_{n-2}, etc.
- For an arbitrary ideal I, we can get the *elimination ideals*

$$\text{elim}_l(I) = I \cap \mathbb{K}[x_l, x_{l+1}, \ldots, x_{n-1}]$$

Finding a solution to a system of quadratic equations is NP-hard.
Computing Gröbner bases may require (doubly) exponential time.

Polynomial systems and graphs

A polynomial system defined by m equations in n variables:

$$f_i(x_0, \ldots, x_{n-1}) = 0, \qquad i = 1, \ldots, m$$

Construct a graph G ("primal graph") with n nodes, as:

- Nodes are variables $\{x_0, \ldots, x_{n-1}\}$.
- For each equation, add a clique connecting the variables appearing in that equation

Polynomial systems and graphs

A polynomial system defined by m equations in n variables:

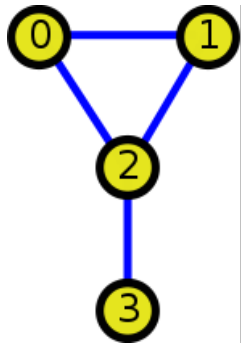
$$f_i(x_0, \ldots, x_{n-1}) = 0, \qquad i = 1, \ldots, m$$

Construct a graph G ("primal graph") with n nodes, as:

- Nodes are variables $\{x_0, \ldots, x_{n-1}\}$.
- For each equation, add a clique connecting the variables appearing in that equation

Example:

$$I = \langle x_0^2 x_1 x_2 + 2x_1 + 1, x_1^2 + x_2, x_1 + x_2, x_2 x_3 \rangle$$



Questions

"Abstracted" the polynomial system to a graph.

Questions

"Abstracted" the polynomial system to a graph.

- Can the graph structure help *solve* this system?
- For instance, to compute Groebner bases?
- Or, perhaps we can do something *better*?
- Preserve graph (sparsity) structure?
- Complexity aspects?

Graphical modelling

Pervasive idea in many areas, in particular: numerical linear algebra, graphical models, constraint satisfaction, database theory, ...

Key notions: chordality and treewidth.

Many names: Arnborg, Beeri/Fagin/Maier/Yannakakis, Blair/Peyton, Bodlaender, Courcelle, Dechter, Lauritzen/Spiegelhalter, Pearl, Robertson/Seymour, ...

Graphical modelling

Pervasive idea in many areas, in particular: numerical linear algebra, graphical models, constraint satisfaction, database theory, ...

Key notions: chordality and treewidth.

Many names: Arnborg, Beeri/Fagin/Maier/Yannakakis, Blair/Peyton, Bodlaender, Courcelle, Dechter, Lauritzen/Spiegelhalter, Pearl, Robertson/Seymour, ...

Remarkably (AFAIK) almost no work in computational algebraic geometry exploits this structure.

Graphical modelling

Pervasive idea in many areas, in particular: numerical linear algebra, graphical models, constraint satisfaction, database theory, ...

Key notions: chordality and treewidth.

Many names: Arnborg, Beeri/Fagin/Maier/Yannakakis, Blair/Peyton, Bodlaender, Courcelle, Dechter, Lauritzen/Spiegelhalter, Pearl, Robertson/Seymour, ...

Remarkably (AFAIK) almost no work in computational algebraic geometry exploits this structure.

We hope to change this... ;)

Chordality and treewidth

Let G be a graph with vertices $x_0, \ldots, x_{n-1}$.
A vertex ordering $x_0 > x_1 > \cdots > x_{n-1}$ is a *perfect elimination ordering* if for each x_l, the set

$$X_l := \{x_l\} \cup \{x_m : x_m \text{ is adjacent to } x_l, \;\; x_l > x_m\}$$

is such that the restriction $G|_{X_l}$ is a clique.
A graph is chordal if it has a perfect elimination ordering.

Chordality and treewidth

Let G be a graph with vertices $x_0, \ldots, x_{n-1}$.
A vertex ordering $x_0 > x_1 > \cdots > x_{n-1}$ is a *perfect elimination ordering* if for each x_l, the set

$$X_l := \{x_l\} \cup \{x_m : x_m \text{ is adjacent to } x_l, \ \ x_l > x_m\}$$

is such that the restriction $G|_{X_l}$ is a clique.
A graph is chordal if it has a perfect elimination ordering.

A *chordal completion* of G is a chordal graph with the same vertex set as G, and which contains all edges of G.
The treewidth of a graph is the clique number (minus one) of its smallest chordal completion.

Chordality and treewidth

Let G be a graph with vertices $x_0, \ldots, x_{n-1}$.
A vertex ordering $x_0 > x_1 > \cdots > x_{n-1}$ is a *perfect elimination ordering* if for each x_l, the set

$$X_l := \{x_l\} \cup \{x_m : x_m \text{ is adjacent to } x_l, \;\; x_l > x_m\}$$

is such that the restriction $G|_{X_l}$ is a clique.
A graph is chordal if it has a perfect elimination ordering.

A *chordal completion* of G is a chordal graph with the same vertex set as G, and which contains all edges of G.
The treewidth of a graph is the clique number (minus one) of its smallest chordal completion.

Meta-theorem: NP-complete problems are "easy" on graphs of small treewidth.

Bad news? (I)

Subset sum problem, with data $A = \{a_1, \ldots, a_n\} \subset \mathbb{Z}$.
Is there a subset of A that adds up to S?

Letting s_i be the partial sums, we can write a polynomial system:

$$\begin{aligned} 0 &= s_0 \\ 0 &= (s_i - s_{i-1})(s_i - s_{i-1} - a_i) \\ S &= s_n \end{aligned}$$

The graph associated with these equations is a path

But, subset sum is NP-complete...

Bad news? (II)

For *linear* equations, "good" elimination preserves graph structure (perfect!)

Bad news? (II)

For *linear* equations, "good" elimination preserves graph structure (perfect!)

For polynomials, however, Groebner bases can destroy chordality.

Ex: Consider

$$I = \langle x_0 x_2 - 1, x_1 x_2 - 1 \rangle,$$

whose associated graph is the path 

.

Bad news? (II)

For *linear* equations, "good" elimination preserves graph structure (perfect!)

For polynomials, however, Groebner bases can destroy chordality.

Ex: Consider

$$I = \langle x_0 x_2 - 1, x_1 x_2 - 1 \rangle,$$

whose associated graph is the path 

.

Every Groebner basis must contain the polynomial $x_0 - x_1$, breaking the sparsity structure.

Our results

- A *chordal elimination* algorithm, to exploit graphical structure.
- Conditions under which chordal elimination succeeds.
- Recursive method for computing elimination ideals of *maximal cliques*
- For a certain class, complexity is *linear* in number of variables! (exponential in treewidth)
- Implementation and experimental results

Chordal elimination (sketch)

Given equations, construct graph G, a chordal completion, and a perfect elimination ordering.

Will produce a decreasing sequence of ideals $I = I_0 \supseteq I_1 \supseteq \cdots \supseteq I_{n-1}$.

Given current ideal I_l, split the generators

$$I_l = \underbrace{J_l}_{\in \mathbb{K}[x_l]} + \underbrace{K_{l+1}}_{\notin \mathbb{K}[x_l]}$$

and eliminate variable x_l

$$I_{l+1} = \mathrm{elim}_{l+1}(J_l) + K_{l+1}$$

"Ideally" (!), I_l should be the l-th elimination ideal $\mathrm{elim}_l(I)$...

Notice that by chordality, graph structure is always preserved!

When does chordal elimination succeed?

We need conditions for this to work, i.e., for $\mathbf{V}(I_l) = \mathbf{V}(\mathrm{elim}_l(I))$.

Thm 1: Let I be an ideal and assume that for each l such that X_l is a maximal clique of G, the ideal $J_l \subseteq \mathbb{K}[X_l]$ is zero dimensional. Then, chordal elimination succeeds.

In particular, finite fields $\mathbb{F}_q$, and $0/1$ problems.

When does chordal elimination succeed?

We need conditions for this to work, i.e., for $\mathbf{V}(I_l) = \mathbf{V}(\mathrm{elim}_l(I))$.

Thm 1: Let I be an ideal and assume that for each l such that X_l is a maximal clique of G, the ideal $J_l \subseteq \mathbb{K}[X_l]$ is zero dimensional. Then, chordal elimination succeeds.

In particular, finite fields $\mathbb{F}_q$, and $0/1$ problems.

Def: A polynomial f is *simplicial* if for each variable x_l, the monomial m_l of largest degree in x_l is unique and has the form $m_l = x^{d_l}$.

Thm 2: Let $I = \langle f_1, \ldots, f_s \rangle$ be an ideal such that for each $1 \leq i \leq s$, f_i is generic simplicial. Then, chordal elimination succeeds.

When does chordal elimination succeed?

We need conditions for this to work, i.e., for $\mathbf{V}(I_l) = \mathbf{V}(\mathrm{elim}_l(I))$.

Thm 1: Let I be an ideal and assume that for each l such that X_l is a maximal clique of G, the ideal $J_l \subseteq \mathbb{K}[X_l]$ is zero dimensional. Then, chordal elimination succeeds.

In particular, finite fields $\mathbb{F}_q$, and 0/1 problems.

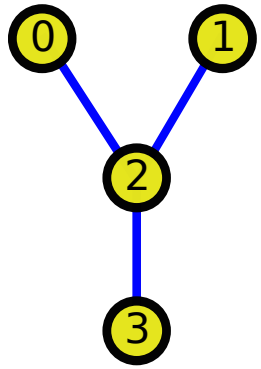
Def: A polynomial f is *simplicial* if for each variable x_l, the monomial m_l of largest degree in x_l is unique and has the form $m_l = x^{d_l}$.

Thm 2: Let $I = \langle f_1, \ldots, f_s \rangle$ be an ideal such that for each $1 \leq i \leq s$, f_i is generic simplicial. Then, chordal elimination succeeds.

[Intuition: interaction of (iterated) "closure/extension thm" + chordality]

Naive chordal elimination can fail

$I = \langle x_0x_2 + 1, x_1^2 + x_2, x_1 + x_2, x_2x_3 \rangle$



Groebner basis:

$$\{x_0 - 1, x_1 - 1, x_2 + 1, x_3\}$$

Elimination:

$$\left.\begin{array}{l} x_0x_2 + 1 \\ x_1^2 + x_2 \\ x_1 + x_2 \\ x_2x_3 \end{array}\right\} \quad \left.\begin{array}{l} x_1^2 + x_2 \\ x_1 + x_2 \\ x_2x_3 \end{array}\right\} \rightarrow \left.\begin{array}{l} x_2^2 + x_2 \\ x_2x_3 \end{array}\right\} \rightarrow 0$$

We got $I_3 = \langle 0 \rangle$, but really $\mathrm{elim}_3(I) = \langle x_3 \rangle$.

Elimination ideals of maximal cliques

In general, Groebner bases can be very large, and destroy chordality.

Can we do something nearly as good, *preserving* graph structure?

Idea: Compute elimination ideals $H_l := I \cap \mathbb{K}[X_l]$ for the *maximal cliques*. (A chordal graph has at most n maximal cliques)

Elimination ideals of maximal cliques

In general, Groebner bases can be very large, and destroy chordality.

Can we do something nearly as good, *preserving* graph structure?

Idea: Compute elimination ideals $H_l := I \cap \mathbb{K}[X_l]$ for the *maximal cliques*. (A chordal graph has at most n maximal cliques)

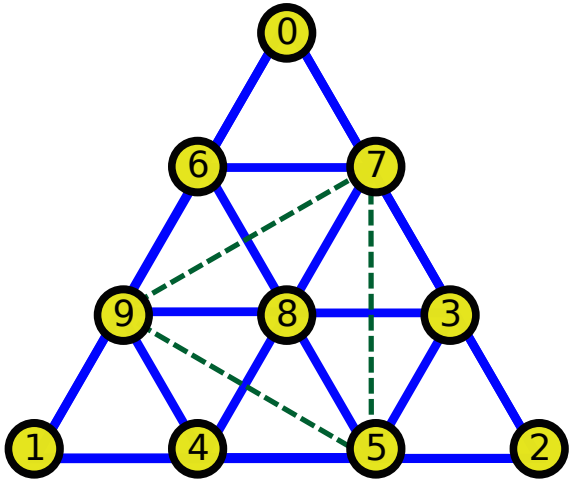
- For some purposes, $\cup_l gb(H_l)$ has same information as $gb(I)$, and is much smaller/sparser.
- Compute the maximal clique ideals $\mathbb{K}[X_l]$ from the output of the chordal elimination algorithm, in a structure-preserving way.

[Intuition: variety has "small" coordinate projections, can compute those, and glue them]

Example: graph colorings

Let I be given by the equations:

$$x_i^3 - 1 = 0, \qquad 0 \leq i \leq 8$$
$$x_9 - 1 = 0$$
$$x_i^2 + x_i x_j + x_j^2 = 0, \qquad (i,j) \text{ blue edge}$$

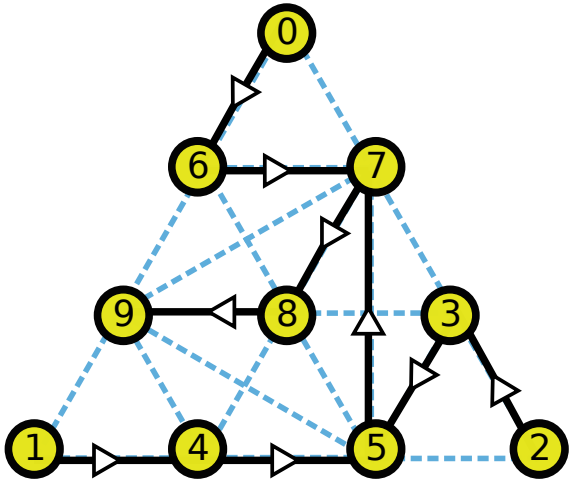


Graph G (blue) and its chordal completion $\bar{G}$ (green).

There are 7 maximal cliques:

$$X_0 = \{x_0, x_6, x_7\},\ X_1 = \{x_1, x_4, x_9\},\ X_2 = \{x_2, x_3, x_5\},\ X_3 = \{x_3, x_5, x_7, x_8\},$$
$$X_4 = \{x_4, x_5, x_8, x_9\},\ X_5 = \{x_5, x_7, x_8, x_9\},\ X_6 = \{x_6, x_7, x_8, x_9\}$$

Elimination tree of the graph $\bar{G}$.
The root/sink is 9.



Some of the clique elimination ideals:

$$H_0 = \langle x_0 + x_6 + 1, x_6^2 + x_6 + 1, x_7 - 1 \rangle$$
$$H_5 = \langle x_5 - 1, x_7 - 1, x_8^2 + x_8 + 1, x_9 - 1 \rangle$$
$$H_6 = \langle x_6 + x_8 + 1, x_7 - 1, x_8^2 + x_8 + 1, x_9 - 1 \rangle$$

The corresponding varieties are:

$$H_0 : \{x_0, x_6, x_7\} \quad \to \left\{\zeta, \zeta^2, 1\right\}, \ \left\{\zeta^2, \zeta, 1\right\}$$
$$H_5 : \{x_5, x_7, x_8, x_9\} \to \{1, 1, \zeta, 1\}, \ \left\{1, 1, \zeta^2, 1\right\}$$
$$H_6 : \{x_6, x_7, x_8, x_9\} \to \left\{\zeta^2, 1, \zeta, 1\right\}, \left\{\zeta, 1, \zeta^2, 1\right\}$$

Complexity

For "nice" cases, complexity is *linear* in number of variables n, number of equations s, and exponential in treewidth κ.

Thm: Let I be such that each (maximal) $\tilde{H}^j$ is q-dominated. The complexity of computing I_l is $\tilde{O}(s + lq^{\alpha\kappa})$. We can find all elimination ideals in $\tilde{O}(nq^{\alpha\kappa})$.

E.g., we recover known results on linear-time colorability for bounded treewidth:
Cor: Let G be a graph and $\bar{G}$ a chordal completion with largest clique of size κ. We can describe all q-colorings of G in $\tilde{O}(nq^{\alpha\kappa})$.

Implementation and examples

Implemented in Sage, using Singular and PolyBoRi (for $\mathbb{F}_2$).

- Graph colorings (counting q-colorings)
- Cryptography ("baby" AES, Cid *et al.*)
- Sensor Network localization
- Discretization of polynomial equations

Results: Crypto - AES variant (Cid et al.) - $\mathbb{F}_2[x]$

Performance on $SR(n, 1, 2, 4)$ for chordal elimination, and computing (lex/degrevlex) Gröbner bases (PolyBoRi).

n	Variables	Equations	Seed	ChordElim	LexGB	DegrevlexGB
6	176	320	0	575.516	402.255	256.253
			1	609.529	284.216	144.316
			2	649.408	258.965	133.367
10	288	528	0	941.068	$>$ 1100, aborted	1279.879
			1	784.709	$>$ 1400, aborted	1150.332
			2	1124.942	$>$ 3600, aborted	$>$ 2500, aborted

- For small problems standard Gröbner bases outperform chordal elimination, particularly using degrevlex order.
- Nevertheless, chordal elimination scales better, being faster than both methods for $n = 10$.
- In addition, standard Gröbner bases have higher memory requirements, which is reflected in the many experiments that aborted for this reason.

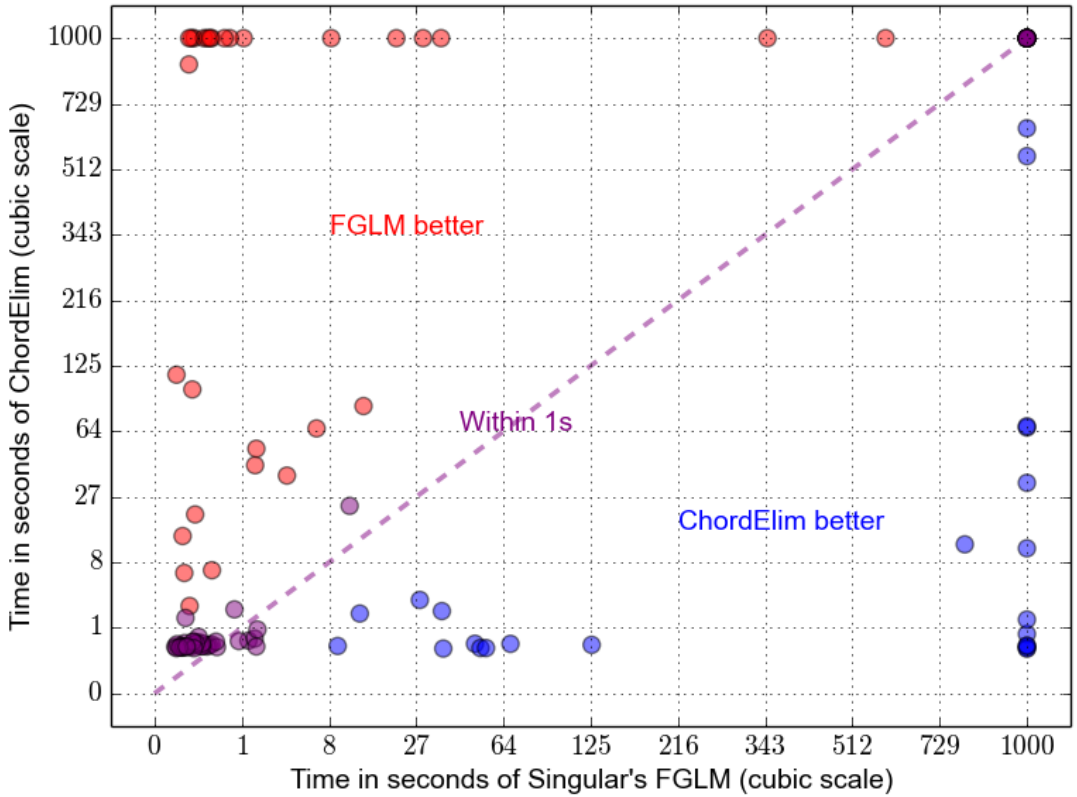
Results: Sensor network localization - $\mathbb{Q}[x]$

Find positions, given a few known fixed anchors and pairwise distances.
Comparison with Singular: DegrevlexGB, LexFGLM

- Natural graph structure

$$\|x_i - x_j\|^2 = d_{ij}^2 \quad ij \in \mathcal{A}$$
$$\|x_i - a_k\|^2 = e_{ij}^2 \quad ik \in \mathcal{B}$$

- Simplicial, therefore exact elimination
- Underconstrained regime: chordal is much better
- Overconstrained regime: competitive (plot)



Summary

- Chordal structure can notably simplify polynomial system solving
- Under assumptions (treewidth + algebraic structure), tractable!
- Yields practical, competitive, implementable algorithms

Summary

- Chordal structure can notably simplify polynomial system solving
- Under assumptions (treewidth + algebraic structure), tractable!
- Yields practical, competitive, implementable algorithms

If you want to know more:

- D. Cifuentes, P.A. Parrilo, Exploiting chordal structure in polynomial ideals: a Groebner basis approach. `arXiv:1411.1745`.
- D. Cifuentes, Exploiting chordal structure in systems of polynomial equations, S.M. thesis, MIT, 2014.

Thanks for your attention!