Hilbert's Nullstellensatz and Combinatorial Infeasibility

Jesús De Loera, UC Davis

based on joint work with J. Lee, S. Margulies, P. Malkin, and S. Onn

September 30, 2008

In today's lecture...

- **Combinatorial feasibility or existence problems** regard deciding whether a certain combinatorial property or structure exist or not (e.g., is there a hamiltonian cycle on a graph?, is a graph 3-colorable?).

In today's lecture...

- **Combinatorial feasibility or existence problems** regard deciding whether a certain combinatorial property or structure exist or not (e.g., is there a hamiltonian cycle on a graph?, is a graph 3-colorable?).
  Suppose your life depends on deciding it, What would you?

In today's lecture...

- **Combinatorial feasibility or existence problems** regard deciding whether a certain combinatorial property or structure exist or not (e.g., is there a hamiltonian cycle on a graph?, is a graph 3-colorable?).
  Suppose your life depends on deciding it, What would you?
  Probably you would do branch-and-bound and enumeration, perhaps even help yourself with integer programming...

In today's lecture...

- **Combinatorial feasibility or existence problems** regard deciding whether a certain combinatorial property or structure exist or not (e.g., is there a hamiltonian cycle on a graph?, is a graph 3-colorable?).
  Suppose your life depends on deciding it, What would you?
  Probably you would do branch-and-bound and enumeration, perhaps even help yourself with integer programming... Often those combinatorial feasibility
- What are we doing today?

In today's lecture...

- **Combinatorial feasibility or existence problems** regard deciding whether a certain combinatorial property or structure exist or not (e.g., is there a hamiltonian cycle on a graph?, is a graph 3-colorable?).
  Suppose your life depends on deciding it, What would you?
  Probably you would do branch-and-bound and enumeration, perhaps even help yourself with integer programming... Often those combinatorial feasibility
- What are we doing today?

  We transfer the Combinatorial feasibility problem to the solvability of a system of polynomials

In today's lecture...

- **Combinatorial feasibility or existence problems** regard deciding whether a certain combinatorial property or structure exist or not (e.g., is there a hamiltonian cycle on a graph?, is a graph 3-colorable?).
  Suppose your life depends on deciding it, What would you?
  Probably you would do branch-and-bound and enumeration, perhaps even help yourself with integer programming... Often those combinatorial feasibility
- What are we doing today?

  We transfer the Combinatorial feasibility problem to the solvability of a system of polynomials
  We then solve a Polynomial Feasibility Problem by a sequence of growing-size linear algebra problem!.

A Typical Combinatorial Feasibility Problem

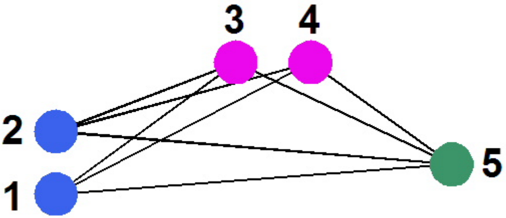
- **Independent Set:** Given a graph G and an integer k, does there exist a subset of the vertices of size k such that no two vertices in the subset are adjacent?

A Typical Combinatorial Feasibility Problem

- **Independent Set:** Given a graph G and an integer k, does there exist a subset of the vertices of size k such that no two vertices in the subset are adjacent?
- Recall, the *independence* number of a graph is the size of the largest independent set in the graph, and is denoted by $\alpha(G)$.

A Typical Combinatorial Feasibility Problem

- **Independent Set:** Given a graph G and an integer k, does there exist a subset of the vertices of size k such that no two vertices in the subset are adjacent?
- Recall, the *independence* number of a graph is the size of the largest independent set in the graph, and is denoted by $\alpha(G)$.
- **Turán Graph $T(5,3)$:** no stable set of size bigger than 2.



Independent Set as a System of Polynomial Equations (L. Lovász)

Given a graph G and an integer k:

- one **variable** per **vertex**
- For every vertex $i = 1, \ldots, n$, let $x_i^2 - x_i = 0$
- For every edge $(i, j) \in E(G)$, let $x_i x_j = 0$
- Finally, let

$$\left(-k + \sum_{i=1}^{n} x_i \right) = 0$$

Independent Set as a System of Polynomial Equations (L. Lovász)

Given a graph G and an integer k:

- one **variable** per **vertex**
- For every vertex $i = 1, \ldots, n$, let $x_i^2 - x_i = 0$
- For every edge $(i, j) \in E(G)$, let $x_i x_j = 0$
- Finally, let

$$\left(-k + \sum_{i=1}^{n} x_i \right) = 0$$

- **Theorem:** Let G be a graph, k an integer, encoded as the above $(n + m + 1)$ system of equations. Then this system has a solution if and only if G has an independent set of size k.

Turán Graph $T(5,3)$: $\Longrightarrow$ System of Polynomial Equations

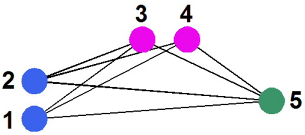


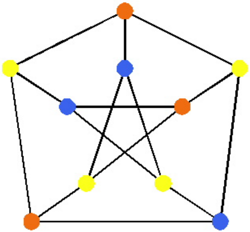
Figure: Does $T(5,3)$ have an independent set of size 3?

$$x_1x_3 = 0,\; x_1x_4 = 0,\; x_1x_5 = 0,\; x_2x_3 = 0, \qquad x_1^2 - x_1 = 0,\; x_2^2 - x_2 = 0$$

$$x_2x_4 = 0,\; x_2x_5 = 0,\; x_3x_5 = 0,\; x_4x_5 = 0, \qquad x_3^2 - x_3 = 0,\; x_4^2 - x_4 = 0$$

$$x_1 + x_3 + x_5 + x_2 + x_4 - 3 = 0, \qquad x_5^2 - x_5 = 0$$

- **Graph coloring:** Given a graph G, and an integer k, can the vertices be colored with k colors in such a way that no two adjacent vertices are the same color?
- **Is the Petersen Graph 3-colorable?**



Graph Coloring modeled by a Polynomial System

- one **variable** per **vertex**

Graph Coloring modeled by a Polynomial System

- one **variable** per **vertex**
- **vertex polynomials:** For every vertex $i = 1, \ldots, n$,

$$x_i^k - 1 = 0$$

Graph Coloring modeled by a Polynomial System

- one **variable** per **vertex**
- **vertex polynomials:** For every vertex $i = 1, \ldots, n$,

$$x_i^k - 1 = 0$$

- **edge polynomials:** For every edge $(i, j) \in E(G)$,

$$x_i^{k-1} + x_i^{k-2} x_j + \cdots + x_i x_j^{k-2} + x_j^{k-1} = 0$$

Graph Coloring modeled by a Polynomial System

- one **variable** per **vertex**
- **vertex polynomials:** For every vertex $i = 1, \ldots, n$,

$$x_i^k - 1 = 0$$

- **edge polynomials:** For every edge $(i, j) \in E(G)$,

$$x_i^{k-1} + x_i^{k-2} x_j + \cdots + x_i x_j^{k-2} + x_j^{k-1} = 0$$

- **Theorem:**(1988 D. Bayer) Let G be a graph, k an integer, then the system of equations has a solution if and only if G is k-colorable.

Graph Coloring modeled by a Polynomial System

- one **variable** per **vertex**
- **vertex polynomials:** For every vertex $i = 1, \ldots, n$,

$$x_i^k - 1 = 0$$

- **edge polynomials:** For every edge $(i, j) \in E(G)$,

$$x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_i x_j^{k-2} + x_j^{k-1} = 0$$

- **Theorem:**(1988 D. Bayer) Let G be a graph, k an integer, then the system of equations has a solution if and only if G is k-colorable. Moreover, the number of k-colorings is equal to the number of solutions divided by $k!$.

Graph Coloring modeled by a Polynomial System

- one **variable** per **vertex**
- **vertex polynomials:** For every vertex $i = 1, \dots, n$,

$$x_i^k - 1 = 0$$

- **edge polynomials:** For every edge $(i, j) \in E(G)$,

$$x_i^{k-1} + x_i^{k-2} x_j + \cdots + x_i x_j^{k-2} + x_j^{k-1} = 0$$

- **Theorem:**(1988 D. Bayer) Let G be a graph, k an integer, then the system of equations has a solution if and only if G is k-colorable. Moreover, the number of k-colorings is equal to the number of solutions divided by $k!$.
- **Theorem:** (2008 Hillar-Windfeldt) Gröbner bases characterization for when the graph is uniquely k-colorable.

Example: Petersen Graph Polynomial System of Equations

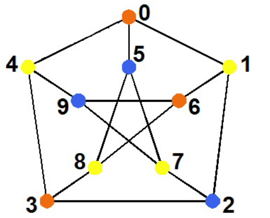


Figure: Decision Question: Is the Petersen graph 3-colorable?

$$x_1^3 - 1 = 0, x_2^3 - 1 = 0, \quad x_1^2 + x_1x_2 + x_2^2 = 0, x_1^2 + x_1x_5 + x_5^2 = 0$$
$$x_3^3 - 1 = 0, x_4^3 - 1 = 0, \quad x_1^2 + x_1x_6 + x_6^2 = 0, x_2^2 + x_2x_3 + x_3^2 = 0$$
$$x_5^3 - 1 = 0, x_6^3 - 1 = 0, \quad x_2^2 + x_2x_7 + x_7^2 = 0, x_3^2 + x_3x_8 + x_8^2 = 0$$
$$x_7^3 - 1 = 0, x_8^3 - 1 = 0, \quad \cdots\cdots \quad \cdots\cdots$$
$$x_9^3 - 1 = 0, x_{10}^3 - 1 = 0, \quad x_7^2 + x_7x_9 + x_9^2 = 0, x_8^2 + x_8x_{10} + x_{10}^2 = 0$$

Other algebraic ways to think about colorability

Definition: Let G be a graph with vertices $V = \{1, \ldots, n\}$ and edges E. The *graph polynomial* of G is

$$f_G = \prod_{\{i,j\} \in E,\ i<j} (x_i - x_j).$$

Other algebraic ways to think about colorability

Definition: Let G be a graph with vertices $V = \{1, \ldots, n\}$ and edges E. The *graph polynomial* of G is

$$f_G = \prod_{\{i,j\} \in E,\ i<j} (x_i - x_j).$$

Theorem: (1990 Kleitman Lovász) Let $\mathcal{H}$ be the set of all graphs with n vertices consisting of a clique of size $k+1$ and all other $n-k$ vertices isolated. The graph G on n vertices is not k-colorable if and only if f_G belongs to the ideal $J_{n,k} = \langle f_H : H \in \mathcal{H} \rangle$.

Other algebraic ways to think about colorability

Definition: Let G be a graph with vertices $V = \{1, \ldots, n\}$ and edges E. The *graph polynomial* of G is

$$f_G = \prod_{\{i,j\} \in E,\ i<j} (x_i - x_j).$$

Theorem: (1990 Kleitman Lovász) Let $\mathcal{H}$ be the set of all graphs with n vertices consisting of a clique of size $k+1$ and all other $n-k$ vertices isolated. The graph G on n vertices is not k-colorable if and only if f_G belongs to the ideal $J_{n,k} = \langle f_H : H \in \mathcal{H} \rangle$.

Theorem: (1995 JDL) The set of polynomials f_H for $H \in \mathcal{H}$ is a universal Gröbner basis for the ideal $J_{n,k}$.

Application: Largest k-colorable subgraph

A graph G has a k-colorable subgraph with R edges if and only if the following system of equations has a solution:

- $$\sum_{\{i,j\}\in E(G)} y_{ij} - R = 0,$$

Application: Largest k-colorable subgraph

A graph G has a k-colorable subgraph with R edges if and only if the following system of equations has a solution:

- $$\sum_{\{i,j\}\in E(G)} y_{ij} - R = 0,$$
- For each vertex $i \in V(G)$:
$$x_i^k = 1,$$

Application: Largest k-colorable subgraph

A graph G has a k-colorable subgraph with R edges if and only if the following system of equations has a solution:

- $$\sum_{\{i,j\}\in E(G)} y_{ij} - R = 0,$$
- For each vertex $i \in V(G)$:
$$x_i^k = 1,$$
- For each edge $\{i,j\} \in E(G)$:
$$y_{ij}^2 - y_{ij} = 0, \quad y_{ij}\left(x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_j^{k-1}\right) = 0.$$

Many other interesting encodings: e.g., existence of length k cycle in a graph, largest planar subgraph, others...

Hilbert's Nullstellensatz

- **Theorem:** Let $\mathbb{K}$ be a field and $\bar{\mathbb{K}}$ its algebraic closure field. Let $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. The system of equations $f_1 = f_2 = \cdots = f_s = 0$ has **no** solution over $\bar{\mathbb{K}}$ if and only if there exist polynomials $\alpha_1, \ldots, \alpha_s \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$1 = \sum_{i=1}^{s} \alpha_i f_i$$

This polynomial identity is a *Nullstellensatz certificate*.

Hilbert's Nullstellensatz

- **Theorem:** Let $\mathbb{K}$ be a field and $\bar{\mathbb{K}}$ its algebraic closure field. Let $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. The system of equations $f_1 = f_2 = \cdots = f_s = 0$ has **no** solution over $\bar{\mathbb{K}}$ if and only if there exist polynomials $\alpha_1, \ldots, \alpha_s \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$1 = \sum_{i=1}^{s} \alpha_i f_i$$

  This polynomial identity is a *Nullstellensatz certificate*.
- Let $d = \max\{\deg(\alpha_1), \deg(\alpha_2), \ldots, \deg(\alpha_s)\}$. Then d is the degree of the Nullstellensatz certificate.

Hilbert's Nullstellensatz

- **Theorem:** Let $\mathbb{K}$ be a field and $\bar{\mathbb{K}}$ its algebraic closure field. Let $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. The system of equations $f_1 = f_2 = \cdots = f_s = 0$ has **no** solution over $\bar{\mathbb{K}}$ if and only if there exist polynomials $\alpha_1, \ldots, \alpha_s \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$1 = \sum_{i=1}^{s} \alpha_i f_i$$

  This polynomial identity is a *Nullstellensatz certificate*.
- Let $d = \max\{\deg(\alpha_1), \deg(\alpha_2), \ldots, \deg(\alpha_s)\}$. Then d is the degree of the Nullstellensatz certificate.
- **Remark:** Nullstellensatz certificates are certificates for the *infeasibility* of a given system of polynomial equations.

Key Point: For fixed degree this is a linear algebra Problem!!

- **Example:** Consider system of polynomial equations

$$x_1^2 - 1 = 0, \qquad x_1 + x_3 = 0, \qquad x_1 + x_2 = 0, \qquad x_2 + x_3 = 0$$

Key Point: For fixed degree this is a linear algebra Problem!!

- **Example:** Consider system of polynomial equations

$$x_1^2 - 1 = 0, \qquad x_1 + x_3 = 0, \qquad x_1 + x_2 = 0, \qquad x_2 + x_3 = 0$$

1. Assume Nullstellensatz certificate has degree 1

$$1 = (c_0x_1 + c_1x_2 + c_2x_3 + c_3)(x_1^2 - 1) + (c_4x_1 + c_5x_2 + c_6x_3 + c_7)(x_1 + x_2)$$
$$+ (c_8x_1 + c_9x_2 + c_{10}x_3 + c_{11})(x_1 + x_3) + (c_{12}x_1 + c_{13}x_2 + c_{14}x_3 + c_{15})(x_2 + x_3)$$

Key Point: For fixed degree this is a linear algebra Problem!!

- **Example:** Consider system of polynomial equations

$$x_1^2 - 1 = 0, \qquad x_1 + x_3 = 0, \qquad x_1 + x_2 = 0, \qquad x_2 + x_3 = 0$$

1. Assume Nullstellensatz certificate has degree 1

$$1 = (c_0x_1 + c_1x_2 + c_2x_3 + c_3)(x_1^2 - 1) + (c_4x_1 + c_5x_2 + c_6x_3 + c_7)(x_1 + x_2) + (c_8x_1 + c_9x_2 + c_{10}x_3 + c_{11})(x_1 + x_3) + (c_{12}x_1 + c_{13}x_2 + c_{14}x_3 + c_{15})(x_2 + x_3)$$

2. Expand the Nullstellensatz certificate, group by monomials

$$c_0x_1^3 + c_1x_1^2x_2 + c_2x_1^2x_3 + (c_3 + c_4 + c_8)x_1^2 + (c_5 + c_{13})x_2^2 + (c_{10} + c_{14})x_3^2 + (c_4 + c_5 + c_9 + c_{12})x_1x_2 + (c_6 + c_8 + c_{10} + c_{12})x_1x_3 + (c_6 + c_9 + c_{13} + c_{14})x_2x_3 + (c_7 + c_{11} - c_0)x_1 + (c_7 + c_{15} - c_1)x_2 + (c_{11} + c_{15} - c_2)x_3 - c_3$$

3. We extract a *linear* system of equations from expanded certificate

$$c_0 = 0, \qquad \dots, \qquad c_3 + c_4 + c_8 = 0, \qquad c_{11} + c_{15} - c_2 = 0, \qquad -c_3 = 1$$

3. We extract a *linear* system of equations from expanded certificate

$$c_0 = 0, \qquad \dots, \qquad c_3 + c_4 + c_8 = 0, \qquad c_{11} + c_{15} - c_2 = 0, \qquad -c_3 = 1$$

4. Solve the linear system, and reconstitute the certificate

$$1 = -(x_1^2 - 1) + \frac{1}{2}x_1(x_1 + x_2) - \frac{1}{2}x_1(x_2 + x_3) + \frac{1}{2}x_1(x_1 + x_3)$$

Bounds for the Nullstellensatz degree

- Question: How big can the degree of the coefficients α_i be?

  The most general bound...

Bounds for the Nullstellensatz degree

- Question: How big can the degree of the coefficients α_i be?

  The most general bound...

- **Theorem:** (Kollár) The $\deg(\alpha_i)$ is bounded by $\max\{3, D\}^n$, where n is the number of variables and $D = \max\{\deg(f_1), \deg(f_2), \ldots, \deg(f_s)\}$.

Bounds for the Nullstellensatz degree

- Question: How big can the degree of the coefficients α_i be?

  The most general bound...

- **Theorem:** (Kollár) The $\deg(\alpha_i)$ is bounded by $\max\{3, D\}^n$, where n is the number of variables and $D = \max\{\deg(f_1), \deg(f_2), \ldots, \deg(f_s)\}$.

  But for the ideals in question we have a better bound:

- **Theorem:** (Brownawell-Lazard) The $\deg(\alpha_i)$ is bounded by $n(D-1)$.

NulLA: Nullstellensatz Linear Algebra Algorithm for checking infeasibility:

- **INPUT:** A system of polynomial equations $F = \{f_1 = 0, f_2 = 0, \dots, f_s = 0\}$.
- While $d \leq$ HBound and no solution found for L_d
  - Construct a tentative Nullstellensatz certificate of degree d
  - Extract a *linear* system of equations from tentative Nullstellensatz certificate
  - Solve the linear system L_d.
  - If there is a solution, construct the certificate, **OUTPUT: F is Infeasible**.
  - Else, $d = d + 1$,
- If $d =$ HBound and no solution found for L_d, then **OUTPUT: F is Feasible**

We can't expect miracles...

Lemma: The Kollár bound is known to be tight for some exotic polynomial systems.

We can't expect miracles...

Lemma: The Kollár bound is known to be tight for some exotic polynomial systems.
Lemma: If P $\neq$ NP, then there must exist an infinite family of graphs such that the degree of a Nullstellensatz certificates for the non-existence of an independent set of size k grows with respect to the number of vertices and edges in the graph.

We can't expect miracles...

Lemma: The Kollár bound is known to be tight for some exotic polynomial systems.
Lemma: If P $\neq$ NP, then there must exist an infinite family of graphs such that the degree of a Nullstellensatz certificates for the non-existence of an independent set of size k grows with respect to the number of vertices and edges in the graph.

Question (L. Lovász, 1994)

Can we explicitly describe such families of graphs?

We can't expect miracles...

Lemma: The Kollár bound is known to be tight for some exotic polynomial systems.

Lemma: If P $\neq$ NP, then there must exist an infinite family of graphs such that the degree of a Nullstellensatz certificates for the non-existence of an independent set of size k grows with respect to the number of vertices and edges in the graph.

Question (L. Lovász, 1994)

Can we explicitly describe such families of graphs?

Lemma: (Razborov, Beam, Impagliazzo et al) Propositional logic statements encoded via "boolean" polynomials. Nullstellensatz degree grows linear on number of logical variables for the Pigeonhole principle.

So, what is the performance of NulLA algorithm for Combinatorial Problems??

So, what is the performance of NulLA algorithm for Combinatorial Problems??

NEXT THE RESULTS...

But first a commercial break...

- From work by Parrilo, Nesterov, Lasserre, Laurent and others developed We can solve a Polynomial Optimization Program by a sequence of growing-size semidefinite programming relaxations

But first a commercial break...

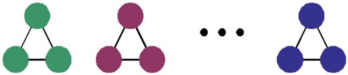
- From work by Parrilo, Nesterov, Lasserre, Laurent and others developed We can solve a Polynomial Optimization Program by a sequence of growing-size semidefinite programming relaxations
- Applied to 0/1-problems, or any **finite varieties**. We know that there is finite converge for this sequence of semidefinite programs.

But first a commercial break...

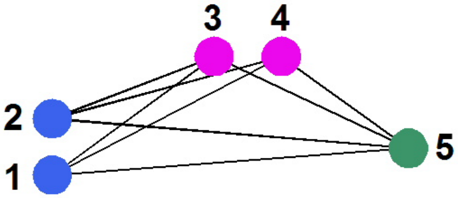
- From work by Parrilo, Nesterov, Lasserre, Laurent and others developed We can solve a Polynomial Optimization Program by a sequence of growing-size semidefinite programming relaxations
- Applied to 0/1-problems, or any **finite varieties**. We know that there is finite converge for this sequence of semidefinite programs.
- They aim to work over the reals, but for our purposes we can work over field. Semidefinite programming is replaced by large-scale linear algebra.

- **Theorem:** For a graph G, a minimum-degree Nullstellensatz certificate for the non-existence of a independent set of size greater than $\alpha(G)$ has degree equal to $\alpha(G)$ and contains at least one term for every independent set in G.

- **Theorem:** For a graph G, a minimum-degree Nullstellensatz certificate for the non-existence of a independent set of size greater than $\alpha(G)$ has degree equal to $\alpha(G)$ and contains at least one term for every independent set in G.
- **Example:** The disjoint union of triangles has a minimum-degree Nullstellensatz of degree $n/3$ and at least $4^{n/3-1}$ terms.



Turán Graph $T(5,3)$: Reduced Certificate Example



$$1 = \left(\frac{x_1x_2 + x_3x_4}{12} - \frac{x_1 + x_3 + x_5 + x_2 + x_4}{12} - \frac{1}{4}\right)(x_1 + x_3 + x_5 + x_2 + x_4 - 4) +$$
$$\left(\frac{x_4}{12} + \frac{x_2}{12} + \frac{1}{6}\right)x_1x_3 + \left(\frac{x_2}{12} + \frac{1}{6}\right)x_1x_4 + \left(\frac{x_2}{12} + \frac{1}{6}\right)x_1x_5 + \left(\frac{x_4}{12} + \frac{1}{6}\right)x_2x_3 +$$
$$\frac{x_2x_4}{6} + \frac{x_2x_5}{6} + \left(\frac{x_4}{12} + \frac{1}{6}\right)x_3x_5 + \frac{x_4x_5}{6} + \left(\frac{x_2}{12} + \frac{1}{12}\right)(x_1^2 - x_1) +$$
$$\left(\frac{x_1}{12} + \frac{1}{12}\right)(x_2^2 - x_2) + \left(\frac{x_4}{12} + \frac{1}{12}\right)(x_3^2 - x_3) + \left(\frac{x_3}{12} + \frac{1}{12}\right)(x_4^2 - x_4) + \frac{x_5^2 - x_5}{12}$$

Nullstellensatz certificates for non-3-colorability

Theorem Every Nullstellensatz certificate for non-3-colorability of a graph has degree at least four. Moreover, in the case of a graph containing an odd-wheel or a clique as a subgraph, a minimum-degree Nullstellensatz certificate for non-3-colorability has degree exactly four.

So far all has used fields of characteristic zero...

We tried it with finite fields...

Graph 3-Coloring as a System of Polynomial Equations over $\overline{\mathbb{F}_2}$ (inspired by Bayer)

- one **variable** per **vertex**
- **vertex polynomials:** For every vertex $i = 1, \ldots, n$,

$$x_i^3 + 1 = 0$$

- **edge polynomials:** For every edge $(i, j) \in E(G)$,

$$x_i^2 + x_i x_j + x_j^2 = 0$$

Graph 3-Coloring as a System of Polynomial Equations over $\overline{\mathbb{F}_2}$ (inspired by Bayer)

- one **variable** per **vertex**
- **vertex polynomials:** For every vertex $i = 1, \ldots, n$,

$$x_i^3 + 1 = 0$$

- **edge polynomials:** For every edge $(i, j) \in E(G)$,

$$x_i^2 + x_i x_j + x_j^2 = 0$$

- **Theorem:** Let G be a graph encoded as the above $(n+m)$ system of equations. Then this system has a solution if and only if G is 3-colorable.

Experimental results for NulLA 3-colorability

Graph	*vertices*	*edges*	*rows*	*cols*	*deg*	*sec*
Mycielski 7	95	755	64,281	71,726	1	.46
Mycielski 9	383	7,271	2,477,931	2,784,794	1	268.78
Mycielski 10	767	22,196	15,270,943	17,024,333	1	14835
$(8, 3)$-Kneser	56	280	15,737	15,681	1	.07
$(10, 4)$-Kneser	210	1,575	349,651	330,751	1	3.92
$(12, 5)$-Kneser	792	8,316	7,030,585	6,586,273	1	466.47
$(13, 5)$-Kneser	1,287	36,036	45,980,650	46,378,333	1	216105
1-Insertions_5	202	1,227	268,049	247,855	1	1.69
2-Insertions_5	597	3,936	2,628,805	2,349,793	1	18.23
3-Insertions_5	1,406	9,695	15,392,209	13,631,171	1	83.45
ash331GPIA	662	4,185	3,147,007	2,770,471	1	13.71
ash608GPIA	1,216	7,844	10,904,642	9,538,305	1	34.65
ash958GPIA	1,916	12,506	27,450,965	23,961,497	1	90.41

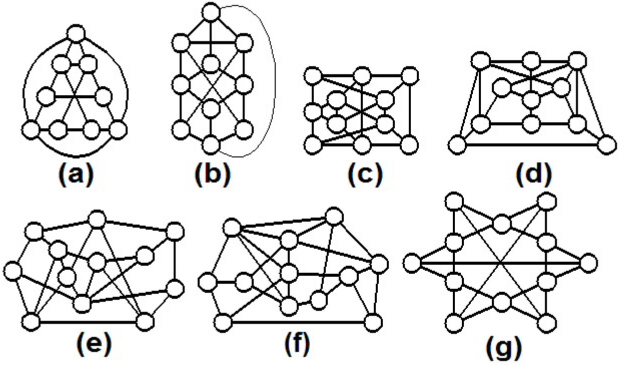
Table: Graphs without 4-cliques.

Comparison with graph coloring heuristics

- *A Branch-and-Cut algorithm for graph coloring* by Isabel Méndez-Díaz and Paula Zabala (2006)

			B&C		DSATUR		NULL-LA	
Graph	*n*	*m*	*lb*	*up*	*lb*	*up*	deg	*sec*
4-Insertions_3.col	79	156	3	4	2	4	1	0
3-Insertions_4.col	281	1046	3	5	2	5	1	2
4-Insertions_4.col	475	1795	3	5	2	5	1	6
2-Insertions_5.col	597	3936	3	6	2	6	1	19
3-Insertions_5.col	1,406	9695	3	6	2	6	1	169

What are the ugliest examples?



near-4-clique free 4-critical graphs by Nishihara-Mizuno

Growth in Nullstellensatz degree

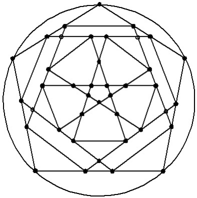
G_i	n	m	*row*	*col*	deg	*sec*	*max terms*
G_0	10	18	336	319	1	0	3
G_1	20	37	401,699	626,934	4	5	563
G_2	30	55	3,073,952	4,081,088	4	58	1961
G_3	39	72	11,703,170	14,192,150	4	287	2272
G_4	49	90	–	–	≥ 6	–	–

Comparison with Gröbner bases

Wheels	*n*	*m*	*GB*	*NulLA*
17	18	34	0	0
151	152	302	2.21	.21
501	502	1,002	126.83	15.58
1001	1,002	2,002	1706.69	622.73
2001	2,002	4,002	–	12905.6

NOTE: Lower bounds for the Nullstellensatz translate in lower bounds for Gröbner!!!!

Appending auxiliary equations helps!!

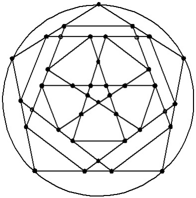


degree 4 certificate

$7,585,826 \times 9,887,481$

over 4 hours

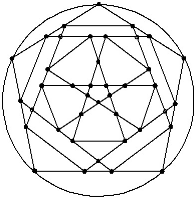
Appending auxiliary equations helps!!



degree 4 certificate
$7,585,826 \times 9,887,481$
over 4 hours

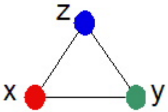
$\Longrightarrow$ 25 triangles

Appending auxiliary equations helps!!

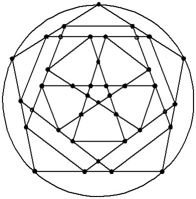


degree 4 certificate
$7,585,826 \times 9,887,481$
over 4 hours

$\Longrightarrow$ 25 triangles

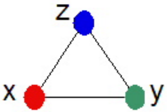


Appending auxiliary equations helps!!



degree 4 certificate
$7,585,826 \times 9,887,481$
over 4 hours

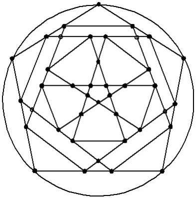
$\Longrightarrow$ 25 triangles



"Triangle" equation:

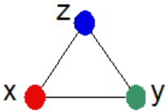
$$0 = x + y + z$$

Appending auxiliary equations helps!!



degree 4 certificate
$7,585,826 \times 9,887,481$
over 4 hours

$\Longrightarrow$ 25 triangles



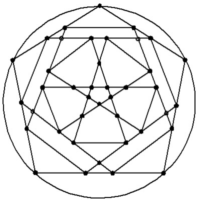
"Triangle" equation:

$$0 = x + y + z$$

Degree two triangle equation:

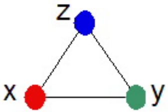
$$0 = x^2 + y^2 + z^2$$

Appending auxiliary equations helps!!



degree 4 certificate
$7,585,826 \times 9,887,481$
over 4 hours
$\Downarrow$
degree 1 certificate

$\Longrightarrow$ 25 triangles



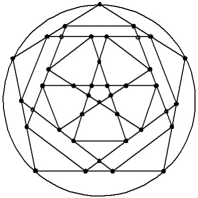
"Triangle" equation:

$$0 = x + y + z$$

Degree two triangle equation:

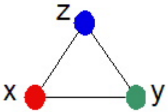
$$0 = x^2 + y^2 + z^2$$

Appending auxiliary equations helps!!



degree 4 certificate
$7,585,826 \times 9,887,481$
over 4 hours
$\Downarrow$
degree 1 certificate
$4,626 \times 4,3464$

$\Longrightarrow$ 25 triangles



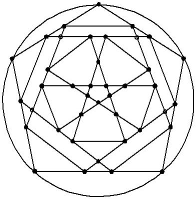
“Triangle” equation:

$$0 = x + y + z$$

Degree two triangle equation:

$$0 = x^2 + y^2 + z^2$$

Appending auxiliary equations helps!!



degree 4 certificate

$7,585,826 \times 9,887,481$

over 4 hours

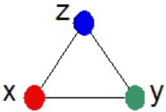
$\Downarrow$

degree 1 certificate

$4,626 \times 4,3464$

.2 seconds

$\Longrightarrow$ 25 triangles



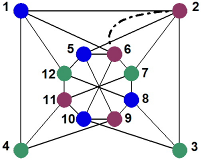
“Triangle” equation:

$$0 = x + y + z$$

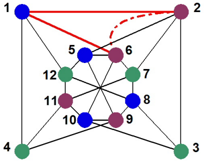
Degree two triangle equation:

$$0 = x^2 + y^2 + z^2$$

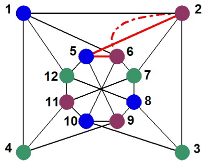
Alternative Nullstellensätze



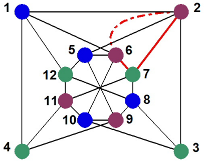
Alternative Nullstellensätze



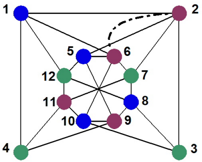
Alternative Nullstellensätze



Alternative Nullstellensätze



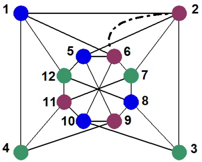
Alternative Nullstellensätze



Alternative Nullstellensätze

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} = \sum_{i=1}^{s} \beta_i f_i$$

Alternative Nullstellensätze

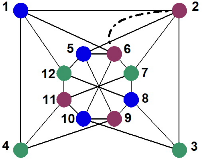


Alternative Nullstellensätze

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} = \sum_{i=1}^{s} \beta_i f_i$$

non-zero $\neq 0$

Alternative Nullstellensätze



Alternative Nullstellensätze

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} = \sum_{i=1}^{s} \beta_i f_i$$

non-zero $\neq 0$

$$\begin{aligned} x_1 x_8 x_9 = & (x_1 + x_2)(x_1^2 + x_1 x_2 + x_2^2) + (x_4 + x_9 + x_{12})(x_1^2 + x_1 x_4 + x_4^2) + \cdots + \\ & + (x_1 + x_4 + x_8)(x_1^2 + x_1 x_{12} + x_{12}^2) + (x_2 + x_7 + x_8)(x_2^2 + x_2 x_3 + x_3^2) \\ & + (x_8 + x_9) \underbrace{(x_1^2 + x_2^2 + x_6^2)}_{\text{degree-cutter}} + (x_9) \underbrace{(x_2^2 + x_5^2 + x_6^2)}_{\text{degree-cutter}} + (x_8) \underbrace{(x_2^2 + x_6^2 + x_7^2)}_{\text{degree-cutter}} . \end{aligned}$$

Example

Consider the complete graph K_4. A degree-one Hilbert Nullstellensatz certificate for non-3-colorability, over $\overline{\mathbb{F}}_2$ is

$$
\begin{aligned}
1 &= c_0(x_1^3+1) \\
&+ (c_{12}^1x_1+c_{12}^2x_2+c_{12}^3x_3+c_{12}^4x_4)(x_1^2+x_1x_2+x_2^2)+(c_{13}^1x_1+c_{13}^2x_2+c_{13}^3x_3+c_{13}^4x_4)(x_1^2+x_1x_3+x_3^2) \\
&+ (c_{14}^1x_1+c_{14}^2x_2+c_{14}^3x_3+c_{14}^4x_4)(x_1^2+x_1x_4+x_4^2)+(c_{23}^1x_1+c_{23}^2x_2+c_{23}^3x_3+c_{23}^4x_4)(x_2^2+x_2x_3+x_3^2) \\
&+ (c_{24}^1x_1+c_{24}^2x_2+c_{24}^3x_3+c_{24}^4x_4)(x_2^2+x_2x_4+x_4^2)+(c_{34}^1x_1+c_{34}^2x_2+c_{34}^3x_3+c_{34}^4x_4)(x_3^2+x_3x_4+x_4^2)
\end{aligned}
$$

Matrix $M_{F,1}$

	c_0	c_{12}^1	c_{12}^2	c_{12}^3	c_{12}^4	c_{13}^1	c_{13}^2	c_{13}^3	c_{13}^4	c_{14}^1	c_{14}^2	c_{14}^3	c_{14}^4	c_{23}^1	c_{23}^2	c_{23}^3	c_{23}^4	c_{24}^1	c_{24}^2	c_{24}^3	c_{24}^4	c_{34}^1	c_{34}^2	c_{34}^3	c_{34}^4
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
x_1^3	1	1	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$x_1^2x_2$	0	1	1	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$x_1^2x_3$	0	0	0	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
$x_1^2x_4$	0	0	0	0	1	0	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
$x_1x_2^2$	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0
$x_1x_2x_3$	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
$x_1x_2x_4$	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0
$x_1x_3^2$	0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0
$x_1x_3x_4$	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0
$x_1x_4^2$	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	1	0	0	0	1	0	0	0
x_2^3	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0
$x_2^2x_3$	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0	0	0	0	0
$x_2^2x_4$	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0
$x_2x_3^2$	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	0	0
$x_2x_3x_4$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	1	0	0
$x_2x_4^2$	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	1	0	1	0	0
x_3^3	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0
$x_3^2x_4$	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1
$x_3x_4^2$	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	1	1
x_4^3	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	1

Suppose we have a group acting...

Suppose a finite permutation group G acts on the variables $x_1, \ldots, x_n$. Assume that the set F of polynomials is invariant under the action of G, i.e., $g(f_i) \in F$ for each $f_i \in F$.

We wish to shrink the matrix using the group!!!

Example, Part 2, action of Z_3 by (2,3,4)

	c_0	c_{12}^1	c_{13}^1	c_{14}^1	c_{12}^2	c_{13}^3	c_{14}^4	c_{12}^3	c_{13}^4	c_{14}^2	c_{12}^4	c_{13}^2	c_{14}^3	c_{23}^1	c_{34}^1	c_{24}^1	c_{23}^2	c_{34}^3	c_{24}^4	c_{24}^2	c_{23}^3	c_{34}^4	c_{34}^2	c_{24}^3	c_{23}^4
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
x_1^3	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$x_1^2x_2$	0	1	0	0	1	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
$x_1^2x_3$	0	0	1	0	0	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
$x_1^2x_4$	0	0	0	1	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$x_1x_2^2$	0	1	0	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0
$x_1x_3^2$	0	0	1	0	0	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0
$x_1x_4^2$	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
$x_1x_2x_3$	0	0	0	0	0	0	0	1	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0
$x_1x_2x_4$	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0
$x_1x_3x_4$	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0
x_2^3	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0
x_3^3	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0
x_4^3	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0
$x_2^2x_3$	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	1	0
$x_3^2x_4$	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	1
$x_2x_4^2$	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1	0	0	1	0	0
$x_2^2x_4$	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	1	0	0	0	0	1
$x_2x_3^2$	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	1	0	1	0	0
$x_3x_4^2$	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	1	0	1	0
$x_2x_3x_4$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1

The Matrix $M_{F,1,G}$

	$\bar{c}_0$	$\bar{c}^1_{12}$	$\bar{c}^2_{12}$	$\bar{c}^3_{12}$	$\bar{c}^4_{12}$	$\bar{c}^1_{23}$	$\bar{c}^2_{23}$	$\bar{c}^2_{24}$	$\bar{c}^2_{34}$
$Orb(1)$	1	0	0	0	0	0	0	0	0
$Orb(x_1^3)$	1	3	0	0	0	0	0	0	0
$Orb(x_1^2 x_2)$	0	1	1	1	1	0	0	0	0
$Orb(x_1 x_2^2)$	0	1	1	0	0	2	0	0	0
$Orb(x_1 x_2 x_3)$	0	0	0	1	1	1	0	0	0
$Orb(x_2^3)$	0	0	1	0	0	0	1	1	0
$Orb(x_2^2 x_3)$	0	0	0	1	0	0	1	1	1
$Orb(x_2^2 x_4)$	0	0	0	0	1	0	1	1	1
$Orb(x_2 x_3 x_4)$	0	0	0	0	0	0	0	0	3

$\overset{(\mathrm{mod}\ 2)}{\equiv}$

	$\bar{c}_0$	$\bar{c}^1_{12}$	$\bar{c}^2_{12}$	$\bar{c}^3_{12}$	$\bar{c}^4_{12}$	$\bar{c}^1_{23}$	$\bar{c}^2_{23}$	$\bar{c}^2_{24}$	$\bar{c}^2_{34}$
$Orb(1)$	1	0	0	0	0	0	0	0	0
$Orb(x_1^3)$	1	1	0	0	0	0	0	0	0
$Orb(x_1^2 x_2)$	0	1	1	1	1	0	0	0	0
$Orb(x_1 x_2^2)$	0	1	1	0	0	0	0	0	0
$Orb(x_1 x_2 x_3)$	0	0	0	1	1	1	0	0	0
$Orb(x_2^3)$	0	0	1	0	0	0	1	1	0
$Orb(x_2^2 x_3)$	0	0	0	1	0	0	1	1	1
$Orb(x_2^2 x_4)$	0	0	0	0	1	0	1	1	1
$Orb(x_2 x_3 x_4)$	0	0	0	0	0	0	0	0	1

Theorem

Let $\mathbb{K}$ be an algebraically-closed field. Let $F = \{f_1, \ldots, f_s\}$ $\subset \mathbb{K}[x_1, \ldots, x_n]$ polynomials and suppose F is closed under the action of the group G on the variable. Suppose that the order of the group $|G|$ and the characteristic of the field $\mathbb{K}$ are relatively prime.

Theorem

Let $\mathbb{K}$ be an algebraically-closed field. Let $F = \{f_1, \ldots, f_s\} \subset \mathbb{K}[x_1, \ldots, x_n]$ polynomials and suppose F is closed under the action of the group G on the variable. Suppose that the order of the group $|G|$ and the characteristic of the field $\mathbb{K}$ are relatively prime.
Then, the degree d Nullstellensatz linear system of equations $M_{F,d}\, y = b_{F,d}$ has a solution over $\mathbb{K}$ if and only if the system of linear equations $\bar{M}_{F,d,G}\, \bar{y} = \bar{b}_{F,d,G}$ has a solution over $\mathbb{K}$.

THANK YOU!

Poset Dimension

- For an n element poset P, a *linear extension* is an order preserving bijection $\sigma : P \longrightarrow \{1, 2, \ldots, n\}$.

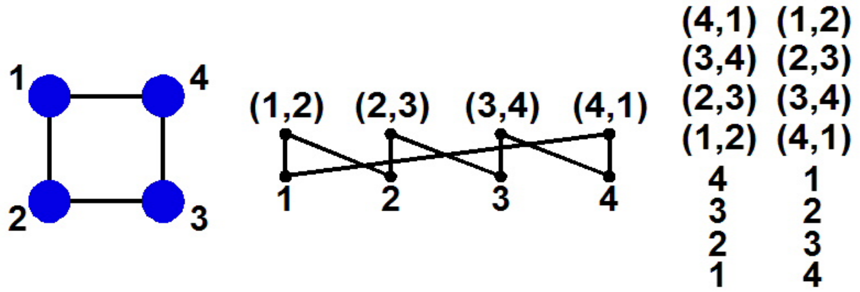
Poset Dimension

- For an n element poset P, a *linear extension* is an order preserving bijection $\sigma : P \rightarrow \{1, 2, \ldots, n\}$.
- The *poset dimension* of P is the smallest integer t for which there exists a family of t linear extensions $\sigma_1, \ldots, \sigma_t$ of P such that $x < y$ in P if and only if $\sigma_i(x) < \sigma_i(y)$ for all σ_i.

Poset Dimension

- For an n element poset P, a *linear extension* is an order preserving bijection $\sigma : P \rightarrow \{1, 2, \ldots, n\}$.
- The *poset dimension* of P is the smallest integer t for which there exists a family of t linear extensions $\sigma_1, \ldots, \sigma_t$ of P such that $x < y$ in P if and only if $\sigma_i(x) < \sigma_i(y)$ for all σ_i.
- The *incidence poset* $P(G)$ of a graph G with node set V and edge set E is the partially ordered set of height two on the union of nodes and edges, where we say $x < y$ if x is a node and y is an edge, and y is incident to x.

Example



Schnyder's theorem

- **Theorem** A graph G is planar if and only if the poset dimension of $P(G)$ is no more than three.
- Our goal is to encode the linear extensions and the poset dimension of a poset P in terms of polynomials equations.
- **Lemma** The poset $P = (E, >)$ has poset dimension at most p if and only if the following system of equations has a solution: For $k = 1, \ldots, p$:

$$\prod_{s=1}^{|E|} (x_i(k) - s) = 0, \text{ for each } i \in \{1, \ldots, |E|\},$$

$$s_k \left(\prod_{\substack{\{i,j\} \in \{1,\ldots,|E|\}, \\ i<j}} x_i(k) - x_j(k) \right) = 1.$$

For $k = 1, \ldots, p$, and each ordered pair of comparable elements $e_i > e_j$ in P:

$$\big(x_i(k) - x_j(k) - \Delta_{ij}(k)\big) = 0. \tag{1}$$

For $k = 1, \ldots, p$, and each ordered pair of comparable elements $e_i > e_j$ in P:

$$\left(x_i(k) - x_j(k) - \Delta_{ij}(k)\right) = 0. \tag{1}$$

For each ordered pair of incomparable elements of P (i.e., $e_i \not> e_j$ and $e_j \not> e_i$):

$$\prod_{k=1}^{p} \left(x_i(k) - x_j(k) - \Delta_{ij}(k)\right) = 0, \qquad \prod_{k=1}^{p} \left(x_j(k) - x_i(k) - \Delta_{ji}(k)\right) = 0, \tag{2}$$

For $k = 1, \ldots, p$, and each ordered pair of comparable elements $e_i > e_j$ in P:

$$\left(x_i(k) - x_j(k) - \Delta_{ij}(k)\right) = 0. \qquad (1)$$

For each ordered pair of incomparable elements of P (i.e., $e_i \not> e_j$ and $e_j \not> e_i$):

$$\prod_{k=1}^{p} \left(x_i(k) - x_j(k) - \Delta_{ij}(k)\right) = 0, \qquad \prod_{k=1}^{p} \left(x_j(k) - x_i(k) - \Delta_{ji}(k)\right) = 0, \qquad (2)$$

For $k = 1, \ldots, p$, and for each pair $\{i, j\} \in \{1, \ldots, |E|\}$:

$$\prod_{d=1}^{|E|-1} (\Delta_{ij}(k) - d) = 0, \qquad \prod_{d=1}^{|E|-1} (\Delta_{ji}(k) - d) = 0. \qquad (3)$$