Hilbert's Nullstellensatz and an Algorithm for proving Combinatorial Infeasibility

Peter Malkin*, UC Davis

joint work with J. De Loera, J. Lee and S. Margulies

MIP 2008

August 4th, 2008

*Research partly funded by an IBM OCR grant and the NSF.

Modeling combinatorial optimization problems

- Traditional approach: Model combinatorial optimization problems by **linear equalities and inequalities**, and integrality constraints.
- Solve model using branch-and-cut approach is the basis of modern discrete optimization.
- Very successful, *but ... we are looking for alternatives.*

Modeling combinatorial optimization problems

- Traditional approach: Model combinatorial optimization problems by **linear equalities and inequalities**, and integrality constraints.
- Solve model using branch-and-cut approach is the basis of modern discrete optimization.
- Very successful, *but ... we are looking for alternatives.*
- Another paradigm: Model combinatorial optimization problems by **non-linear polynomial equalities and inequalities**.
- Solve model using other tools (e.g SDP, algebraic geometry, number theory, etc).

Modeling combinatorial optimization problems...

- From work by Shor (87), Nesterov, Lasserre, Laurent and Parrilo (2000-), we can solve a polynomial optimization problem by a growing sequence of semi-definite relaxations.
- Applied to 0/1-problems, or any **finite varieties**. We know that this sequence converges in a finite number of steps.

Modeling combinatorial optimization problems...

- From work by Shor (87), Nesterov, Lasserre, Laurent and Parrilo (2000-), we can solve a polynomial optimization problem by a growing sequence of semi-definite relaxations.
- Applied to 0/1-problems, or any **finite varieties**. We know that this sequence converges in a finite number of steps.

What are we going to talk about today?

Modeling combinatorial optimization problems...

- From work by Shor (87), Nesterov, Lasserre, Laurent and Parrilo (2000-), we can solve a polynomial optimization problem by a growing sequence of semi-definite relaxations.
- Applied to 0/1-problems, or any **finite varieties**. We know that this sequence converges in a finite number of steps.

What are we going to talk about today?

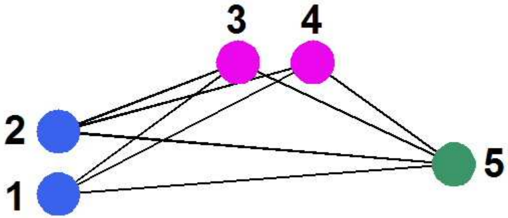
- We can solve a polynomial feasibility problem with only equality constraints by a growing sequence of linear algebra relaxations.
- We will talk about the complexity and practicality of this approach.

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 written $\alpha(G)$.

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 written $\alpha(G)$.
- The **Turán Graph** $T(5,3)$ has no independent set of size 3.



Independent set modeled by a polynomial system

Given a graph G and an integer k:

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

$$\sum_{i=1}^{n} x_i - k = 0.$$

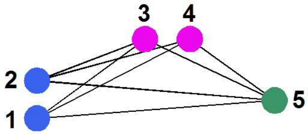
Independent set modeled by a polynomial system

Given a graph G and an integer k:

- One **variable** x_i per **vertex** $i \in \{1, ..., n\}$.
- For every vertex $i = 1, \ldots, n$, let $x_i^2 - x_i = 0$
- For every edge $(i, j) \in E$, let $x_i x_j = 0$
- Finally, let
$$\sum_{i=1}^{n} x_i - k = 0.$$

- **Theorem:** (Lovász) Let k be an integer and let G be a graph encoded as the above system of equations. 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

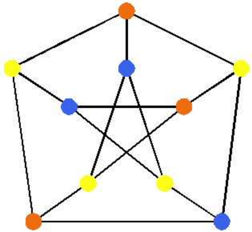


- The following system of equations has a solution if and only if $T(5,3)$ has an independent set of size 3.

$$x_1^2 - x_1 = 0, x_2^2 - x_2 = 0, x_3^2 - x_3 = 0, x_4^2 - x_4 = 0, x_5^2 - x_5 = 0,$$
$$x_1x_3 = 0, x_1x_4 = 0, x_1x_5 = 0, x_2x_3 = 0,$$
$$x_2x_4 = 0, x_2x_5 = 0, x_3x_5 = 0, x_4x_5 = 0,$$
$$x_1 + x_3 + x_5 + x_2 + x_4 - 3 = 0.$$

Another typical combinatorial feasibility problem

- **Graph vertex 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?
- E.g. the **Petersen Graph** is 3-colorable.



Graph coloring modeled by a polynomial system

- One **variable** x_i per **vertex** $i \in \{1, ..., n\}$.
- **Vertex polynomials:** For every vertex $i = 1, \ldots, n$,

$$x_i^k - 1 = 0.$$

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

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

Note that

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

Graph coloring modeled by a polynomial system

- One **variable** x_i per **vertex** $i \in \{1, ..., n\}$.
- **Vertex polynomials:** For every vertex $i = 1, \ldots, n$,

$$x_i^k - 1 = 0.$$

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

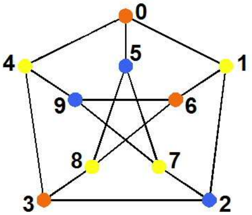
$$x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_i x_j^{k-2} + x_j^{k-1} = 0.$$

Note that

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

- **Theorem:** (D. Bayer) Let k be an integer and let G be a graph encoded as vertex and edge polynomials as above. This system of polynomial equations has a solution if and only if G is k-colorable.

E.g. Petersen graph polynomial system of equations



This system has a solution iff the Petersen graph is 3-colorable.

$$
\begin{array}{ll}
x_0^3 - 1 = 0,\ x_1^3 - 1 = 0, & x_0^2 + x_0x_1 + x_1^2 = 0,\ x_0^2 + x_0x_4 + x_4^2 = 0,\\
x_2^3 - 1 = 0,\ x_3^3 - 1 = 0, & x_0^2 + x_0x_5 + x_5^2 = 0,\ x_1^2 + x_1x_2 + x_2^2 = 0,\\
x_4^3 - 1 = 0,\ x_5^3 - 1 = 0, & x_1^2 + x_1x_6 + x_6^2 = 0,\ x_2^2 + x_2x_7 + x_7^2 = 0,\\
x_6^3 - 1 = 0,\ x_7^3 - 1 = 0, & \cdots\cdots \qquad\qquad \cdots\cdots\\
x_8^3 - 1 = 0,\ x_9^3 - 1 = 0, & x_6^2 + x_6x_8 + x_8^2 = 0,\ x_7^2 + x_7x_9 + x_9^2 = 0.
\end{array}
$$

Hilbert's Nullstellensatz

- **Theorem:** Let $\mathbb{K}$ be a field and $\overline{\mathbb{K}}$ 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 $\overline{\mathbb{K}}$ if and only if there exist $\alpha_1, \ldots, \alpha_s \in \mathbb{K}[x_1, \ldots, x_n]$ 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 $\overline{\mathbb{K}}$ 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 $\overline{\mathbb{K}}$ if and only if there exist $\alpha_1, \ldots, \alpha_s \in \mathbb{K}[x_1, \ldots, x_n]$ such that

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

  This polynomial identity is a *Nullstellensatz certificate*.
- If $x \in \overline{\mathbb{K}}^n$ was a solution, then $\sum_{i=1}^{s} \alpha_i(x) f_i(x) = 0 \neq 1$.
- Nullstellensatz certificates are certificates of *infeasibility*.
- Let $d = \max\{\deg(\alpha_1), \deg(\alpha_2), \ldots, \deg(\alpha_s)\}$. Then, we say that d is the degree of the Nullstellensatz certificate.

How do we find a Nullstellensatz certificate

Key point:

For fixed degree, this is a linear algebra problem!!

How do we find a Nullstellensatz certificate

Key point:

For fixed degree, this is a linear algebra problem!!

E.g. Consider the system of polynomial equations

$$f_1 = x_1^2 - 1 = 0,\ f_2 = x_1 + x_2 = 0,\ f_3 = x_1 + x_3 = 0,\ f_4 = x_2 + x_3 = 0$$

- This system has no solution over $\mathbb{C}$.

How do we find a Nullstellensatz certificate

Key point:

For fixed degree, this is a linear algebra problem!!

E.g. Consider the system of polynomial equations

$$f_1 = x_1^2 - 1 = 0,\ f_2 = x_1 + x_2 = 0,\ f_3 = x_1 + x_3 = 0,\ f_4 = x_2 + x_3 = 0$$

- This system has no solution over $\mathbb{C}$.
- Does this system have a Nullstellensatz certificate of degree 1?

$$1 = \underbrace{(c_0x_1 + c_1x_2 + c_2x_3 + c_3)}_{\alpha_1}\underbrace{(x_1^2 - 1)}_{f_1} + \underbrace{(c_4x_1 + c_5x_2 + c_6x_3 + c_7)}_{\alpha_2}\underbrace{(x_1 + x_2)}_{f_2}$$
$$+ \underbrace{(c_8x_1 + c_9x_2 + c_{10}x_3 + c_{11})}_{\alpha_3}\underbrace{(x_1 + x_3)}_{f_3} + \underbrace{(c_{12}x_1 + c_{13}x_2 + c_{14}x_3 + c_{15})}_{\alpha_4}\underbrace{(x_2 + x_3)}_{f_4}$$

- Expand the Nullstellensatz certificate grouping by monomials.

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

- Extract a *linear* system of equations from expanded certificate.

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

- Expand the Nullstellensatz certificate grouping by monomials.

$$1 = c_0x_1^3 + c_1x_1^2x_2 + c_2x_1^2x_3 + (c_3 + c_4 + c_8)x_1^2 + (c_5 + c_{13})x_2^2 + (c_{10} + c_{14})x_3^2$$
$$+(c_4 + c_5 + c_9 + c_{12})x_1x_2 + (c_6 + c_8 + c_{10} + c_{12})x_1x_3 + (c_6 + c_9 + c_{13} + c_{14})x_2x_3$$
$$+(c_7 + c_{11} - c_0)x_1 + (c_7 + c_{15} - c_1)x_2 + (c_{11} + c_{15} - c_2)x_3 - c_3$$

- Extract a *linear* system of equations from expanded certificate.

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

- Solve the linear system. This linear system is feasible, so we have found a certificate and proven the polynomial system is infeasible. **Note:** the linear system is over $\mathbb{R}$ and not $\mathbb{C}$.

- Expand the Nullstellensatz certificate grouping by monomials.

$$1 = c_0x_1^3 + c_1x_1^2x_2 + c_2x_1^2x_3 + (c_3 + c_4 + c_8)x_1^2 + (c_5 + c_{13})x_2^2 + (c_{10} + c_{14})x_3^2$$
$$+(c_4 + c_5 + c_9 + c_{12})x_1x_2 + (c_6 + c_8 + c_{10} + c_{12})x_1x_3 + (c_6 + c_9 + c_{13} + c_{14})x_2x_3$$
$$+(c_7 + c_{11} - c_0)x_1 + (c_7 + c_{15} - c_1)x_2 + (c_{11} + c_{15} - c_2)x_3 - c_3$$

- Extract a *linear* system of equations from expanded certificate.

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

- Solve the linear system. This linear system is feasible, so we have found a certificate and proven the polynomial system is infeasible. **Note:** the linear system is over $\mathbb{R}$ and not $\mathbb{C}$.
- Reconstruct the Nullstellensatz certificate from a solution of the linear system.

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

- Expand the Nullstellensatz certificate grouping by monomials.

$$1 = c_0x_1^3 + c_1x_1^2x_2 + c_2x_1^2x_3 + (c_3 + c_4 + c_8)x_1^2 + (c_5 + c_{13})x_2^2 + (c_{10} + c_{14})x_3^2$$
$$+(c_4 + c_5 + c_9 + c_{12})x_1x_2 + (c_6 + c_8 + c_{10} + c_{12})x_1x_3 + (c_6 + c_9 + c_{13} + c_{14})x_2x_3$$
$$+(c_7 + c_{11} - c_0)x_1 + (c_7 + c_{15} - c_1)x_2 + (c_{11} + c_{15} - c_2)x_3 - c_3$$

- Extract a *linear* system of equations from expanded certificate.

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

- Solve the linear system. This linear system is feasible, so we have found a certificate and proven the polynomial system is infeasible. **Note:** the linear system is over $\mathbb{R}$ and not $\mathbb{C}$.
- Reconstruct the Nullstellensatz certificate from a solution of the linear system.

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

- If the linear system was not feasible, we would have had to try a higher degree.

Bounds for the Nullstellensatz degree

Question:

How big can the degree of a Nullstellensatz certificate be?

Bounds for the Nullstellensatz degree

Question:

How big can the degree of a Nullstellensatz certificate be?

The most general bound...

Theorem: (Kollár)

The degree 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 a Nullstellensatz certificate be?

The most general bound...

Theorem: (Kollár)

The degree 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 k-coloring and independent sets, we have a better bound:

Theorem: (Lazard)

The degree is bounded by $n(D-1)$.

NulLA: Nullstellensatz linear algebra algorithm

- **Input:** A system of polynomial equations $F = \{f_1 = 0, f_2 = 0, \ldots, f_s = 0\}$.
- Set $d = 0$.
- **While** $d \leq$ HNBound and no solution found for L_d:
  - Construct a tentative Nullstellensatz certificate of degree d.
  - Extract a linear system of equations L_d.
  - Solve the linear system L_d.
  - **If** there is a solution, **then** reconstruct the certificate and **Output**: F is INFEASIBLE.
  - **Else** Set $d = d + 1$.
- **If** $d =$ HNBound and no solution found for L_d, **then** **Output**: F is FEASIBLE.

What is the performance of the NulLA algorithm for combinatorial problems??

Nullstellensatz certificates for independents sets

Lemma: (De Loera, Lee, Margulies, Onn) If P $\neq$ NP, then there must exist an infinite family of graphs without independent sets of size k for whom the degree of a Nullstellensatz certificate grows with respect to $|V|$ and $|E|$.

Nullstellensatz certificates for independents sets

Lemma: (De Loera, Lee, Margulies, Onn) If P $\neq$ NP, then there must exist an infinite family of graphs without independent sets of size k for whom the degree of a Nullstellensatz certificate grows with respect to $|V|$ and $|E|$.

Question (L. Lovász): Can we explicitly describe such graphs?

Nullstellensatz certificates for independents sets

Lemma: (De Loera, Lee, Margulies, Onn) If P $\neq$ NP, then there must exist an infinite family of graphs without independent sets of size k for whom the degree of a Nullstellensatz certificate grows with respect to $|V|$ and $|E|$.

Question (L. Lovász): Can we explicitly describe such graphs?

Theorem: (DLMO) A graph G with no independent set of size k has a minimum-degree Nullstellensatz certificate of degree $\alpha(G)$ that contains at least one term for every independent set in G.

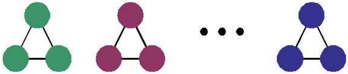
Nullstellensatz certificates for independents sets

Lemma: (De Loera, Lee, Margulies, Onn) If P $\neq$ NP, then there must exist an infinite family of graphs without independent sets of size k for whom the degree of a Nullstellensatz certificate grows with respect to $|V|$ and $|E|$.

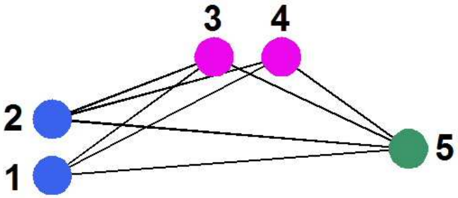
Question (L. Lovász): Can we explicitly describe such graphs?

Theorem: (DLMO) A graph G with no independent set of size k has a minimum-degree Nullstellensatz certificate of degree $\alpha(G)$ that contains at least one term for every independent set in G.

- E.g. The disjoint union of triangles has a Nullstellensatz certificate of degree at least $n/3$ and at least $4^{n/3}$ terms.



Turán graph $T(5,3)$: reduced certificate example



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

Nullstellensatz certificates for non-3-colorability

Theorem: (DLMO) Every Nullstellensatz certificate over $\mathbb{R}$ for non-3-colorability of a graph has degree at least four.

- A graph with a 4-clique subgraph has a Nullstellensatz certificate over $\mathbb{R}$ of minimal-degree exactly 4.

Nullstellensatz certificates for non-3-colorability

Theorem: (DLMO) Every Nullstellensatz certificate over $\mathbb{R}$ for non-3-colorability of a graph has degree at least four.

- A graph with a 4-clique subgraph has a Nullstellensatz certificate over $\mathbb{R}$ of minimal-degree exactly 4.

What about certificates over finite fields? What about $\mathbb{F}_2$?

Nullstellensatz certificates for non-3-colorability

Theorem: (DLMO) Every Nullstellensatz certificate over $\mathbb{R}$ for non-3-colorability of a graph has degree at least four.

- A graph with a 4-clique subgraph has a Nullstellensatz certificate over $\mathbb{R}$ of minimal-degree exactly 4.

What about certificates over finite fields? What about $\mathbb{F}_2$?

Theorem: For a graph G, the following system of polynomial equations has a solution over $\overline{\mathbb{F}}_2$ iff G is 3-colorable.

$$x_i^3 + 1 = 0 \ \forall i \in V, \quad x_i^2 + x_i x_j + x_j^2 = 0 \ \forall (i,j) \in E.$$

Nullstellensatz certificates for non-3-colorability

Theorem: (DLMO) Every Nullstellensatz certificate over $\mathbb{R}$ for non-3-colorability of a graph has degree at least four.

- A graph with a 4-clique subgraph has a Nullstellensatz certificate over $\mathbb{R}$ of minimal-degree exactly 4.

What about certificates over finite fields? What about $\mathbb{F}_2$?

Theorem: For a graph G, the following system of polynomial equations has a solution over $\overline{\mathbb{F}}_2$ iff G is 3-colorable.

$$x_i^3 + 1 = 0 \ \forall i \in V, \quad x_i^2 + x_i x_j + x_j^2 = 0 \ \forall (i,j) \in E.$$

- A graph with 4-clique subgraph has a Nullstellensatz certificate over $\mathbb{F}_2$ of minimal-degree exactly 1.
- **Note:** the linear system we need to solve is over $\mathbb{F}_2$, so there are no numerical stability problems!!

Experimental results for NulLA 3-colorability

Graph	$\|V\|$	$\|E\|$	#rows	#cols	d	sec
Mycielski 7	95	755	64,281	71,726	1	1
Mycielski 9	383	7,271	2,477,931	2,784,794	1	269
Mycielski 10	767	22,196	15,270,943	17,024,333	1	14835
$(8,3)$-Kneser	56	280	15,737	15,681	1	0
$(10,4)$-Kneser	210	1,575	349,651	330,751	1	4
$(12,5)$-Kneser	792	8,316	7,030,585	6,586,273	1	467
$(13,5)$-Kneser	1,287	36,036	45,980,650	46,378,333	1	216105
1-Insertions_5	202	1,227	268,049	247,855	1	2
2-Insertions_5	597	3,936	2,628,805	2,349,793	1	18
3-Insertions_5	1,406	9,695	15,392,209	13,631,171	1	83
ash331GPIA	662	4,185	3,147,007	2,770,471	1	14
ash608GPIA	1,216	7,844	10,904,642	9,538,305	1	35
ash958GPIA	1,916	12,506	27,450,965	23,961,497	1	90

Table: DIMACS graphs without 4-cliques.

Comparison with other graph coloring algorithms

- *DSATUR* a sequential coloring heuristic by Brelaz, 1979.
- *A Branch-and-Cut algorithm for graph coloring* (B&C) by Isabel Méndez-Díaz and Paula Zabala (2006)

Comparison with other graph coloring algorithms

- *DSATUR* a sequential coloring heuristic by Brelaz, 1979.
- *A Branch-and-Cut algorithm for graph coloring* (B&C) by Isabel Méndez-Díaz and Paula Zabala (2006)

			B&C		DSATUR		NulLA		
Graph	$\|V\|$	$\|E\|$	lb	up	lb	up	lb	deg	sec
4-Insertions_3.col	79	156	3	4	2	4	4	1	0
3-Insertions_4.col	281	1046	3	5	2	5	4	1	2
4-Insertions_4.col	475	1795	3	5	2	5	4	1	6
2-Insertions_5.col	597	3936	3	6	2	6	4	1	19
3-Insertions_5.col	1,406	9695	3	6	2	6	4	1	169

"This shouldn't work ...

but it does!"

Anonymous.

Growth in Nullstellensatz degree

Lemma: (DLMO) If P $\neq$ NP, then there must exist an infinite family of graphs without k-colorings for whom the degree of a Nullstellensatz certificate grows with respect to $|V|$ and $|E|$.

Growth in Nullstellensatz degree

Lemma: (DLMO) If P $\neq$ NP, then there must exist an infinite family of graphs without k-colorings for whom the degree of a Nullstellensatz certificate grows with respect to $|V|$ and $|E|$.

- 4-critical graphs by Mizuno-Nishihara are the ugliest non-3-colorable graphs for NulLA that we found.

G_i	n	m	#*row*	#*col*	deg	*sec*
G_0	10	18	336	319	1	0
G_1	20	37	350,040	65,527	3	1
G_2	30	55	1,844,857	2,643,432	4	52
G_3	39	72	7,316,382	9,008,930	4	246
G_4	49	90	–	–	≥ 5	–

What if NulLA cannot determine infeasibility?

What if NulLA cannot determine infeasibility?

- Some *simple preprocessing* can help, but this is often not enough.

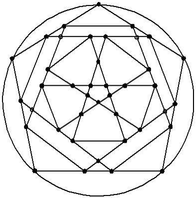
What if NulLA cannot determine infeasibility?

- Some *simple preprocessing* can help, but this is often not enough.

Four *key mathematical ideas* are as follows:

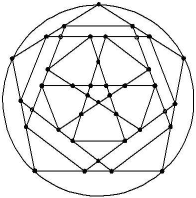
- use finite fields,
- append redundant equations,
- use Alternative Nullstellensätze, and
- use symmetry.

Appending redundant valid equations



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

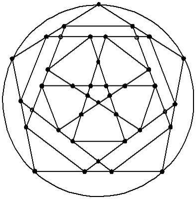
Appending redundant valid equations



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

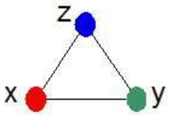
There are 25 triangles

Appending redundant valid equations



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

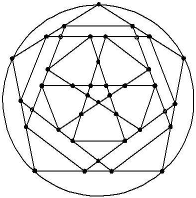
There are 25 triangles



"Triangle" equation:

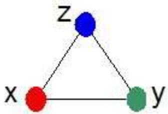
$$0 = x + y + z$$

Appending redundant valid equations



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

There are 25 triangles



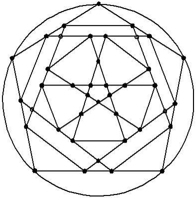
"Triangle" equation:

$$0 = x + y + z$$

Degree two triangle equation:

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

Appending redundant valid equations



degree 4 certificate

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

over 4 hours

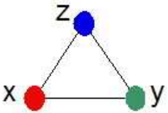
$\Downarrow$

degree 1 certificate

$4,626 \times 4,3464$

0.2 seconds

There are 25 triangles



"Triangle" equation:

$$0 = x + y + z$$

Degree two triangle equation:

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

Alternative Nullstellensätze

Theorem: The system of equations $f_1 = f_2 = \cdots = f_s = 0$ has **no** solution if and only if there exist polynomials $\alpha_1, \ldots, \alpha_s$ and g where $f_1 = f_2 = \cdots = f_s = 0$ and $g = 0$ has **no** solution such that

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

- Note that $g = 1$ is Hilbert's Nullstellensatz.

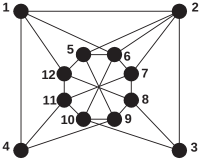
Alternative Nullstellensätze

Theorem: The system of equations $f_1 = f_2 = \cdots = f_s = 0$ has **no** solution if and only if there exist polynomials $\alpha_1, \ldots, \alpha_s$ and g where $f_1 = f_2 = \cdots = f_s = 0$ and $g = 0$ has **no** solution such that

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

- Note that $g = 1$ is Hilbert's Nullstellensatz.

E.g. This graph has a degree 4 certificate for non-3-colorability.



- If we use $g = x_1x_8x_9$, the graph has a degree 1 certificate.

Using symmetry to shrink the linear system

Suppose that $F = \{f_1, ..., f_s\}$ is invariant under the action of a permutation group P acting on the variables $x_1, \ldots, x_n$.

- So, for every permutation $p \in P$, we have $p(F) = F$.
- For graph k-coloring, P is the automorphism group.

Using symmetry to shrink the linear system

Suppose that $F = \{f_1, ..., f_s\}$ is invariant under the action of a permutation group P acting on the variables $x_1, \ldots, x_n$.

- So, for every permutation $p \in P$, we have $p(F) = F$.
- For graph k-coloring, P is the automorphism group.
- **Note:** permuting a certificate gives another certificate!

$$1 = \sum_{i=1}^{s} \alpha_i f_i \Rightarrow 1 = \sum_{i=1}^{s} p(\alpha_i) p(f_i) \Rightarrow 1 = \sum_{i=1}^{s} \bar{\alpha}_i f_i.$$

Using symmetry to shrink the linear system

Suppose that $F = \{f_1, ..., f_s\}$ is invariant under the action of a permutation group P acting on the variables $x_1, \ldots, x_n$.

- So, for every permutation $p \in P$, we have $p(F) = F$.
- For graph k-coloring, P is the automorphism group.
- **Note:** permuting a certificate gives another certificate!

$$1 = \sum_{i=1}^{s} \alpha_i f_i \Rightarrow 1 = \sum_{i=1}^{s} p(\alpha_i)p(f_i) \Rightarrow 1 = \sum_{i=1}^{s} \bar{\alpha}_i f_i.$$

E.g. Consider K_4 and the cyclic group $P = \langle(2,3,4)\rangle$.

- A degree-one certificate for non-3-colorability of K_4 is

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

K_4 linear system matrix

	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

K_4 linear system matrix

	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

K_4 linear system orbit matrix

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

$\overset{\pmod 2}{\equiv}$

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

- This reduced matrix has a solution if and only if the original matrix has a solution.

Different encodings: the good, the bad, and the ugly

The good:

- Is a graph 3-colorable?
- Is a graph 2-colorable?

Different encodings: the good, the bad, and the ugly

The good:

- Is a graph 3-colorable?
- Is a graph 2-colorable?

The bad:

- Does a graph have an independent set of size k?

Different encodings: the good, the bad, and the ugly

The good:

- Is a graph 3-colorable?
- Is a graph 2-colorable?

The bad:

- Does a graph have an independent set of size k?

The ugly:

- Is a binary knapsack problem feasible? (Weismantel).
- Does a bipartite graph have a perfect matching?

Different encodings: the good, the bad, and the ugly

The good:

- Is a graph 3-colorable?
- Is a graph 2-colorable?

The bad:

- Does a graph have an independent set of size k?

The ugly:

- Is a binary knapsack problem feasible? (Weismantel).
- Does a bipartite graph have a perfect matching?

The promising:

- Does a graph have a cycle of length k (Hamiltonian cycle)?
- Does a graph have a k-colorable subgraph with r edges?
- Does a graph have a planar subgraph with k edges?

THANK YOU!

- J.A. De Loera, J. Lee, P.N. Malkin, S. Margulies, *Hilbert's Nullstellensatz and an Algorithm for Proving Combinatorial Infeasibility*, Proc. ISSAC'08, ACM, pages 197–206.
- NulLA: Software will be available soon under COIN-OR.

Comparison with Gröbner basis (dual) method

Gröbner basis (dual) method: A graph is k-colorable if and only if the Gröbner basis of the ideal generated by the vertex and edge polynomials is trivial, that is, the Gröbner basis is $\{1\}$.

Graphs	$\lvert V\rvert$	$\lvert E\rvert$	GB (CoCoA)	NulLA
Wheel 501	502	1,002	127	16
Wheel 1001	1,002	2,002	1,707	623
Mycielski 8	191	2,360	9,015	8
(10,4)-Kneser	210	1,575	9,772	4
4-Insertions 4	475	1,795	1,596	3

Note: Lower bounds for the Nullstellensatz translate into lower bounds for the Gröbner basis method!