Graph-coloring ideals

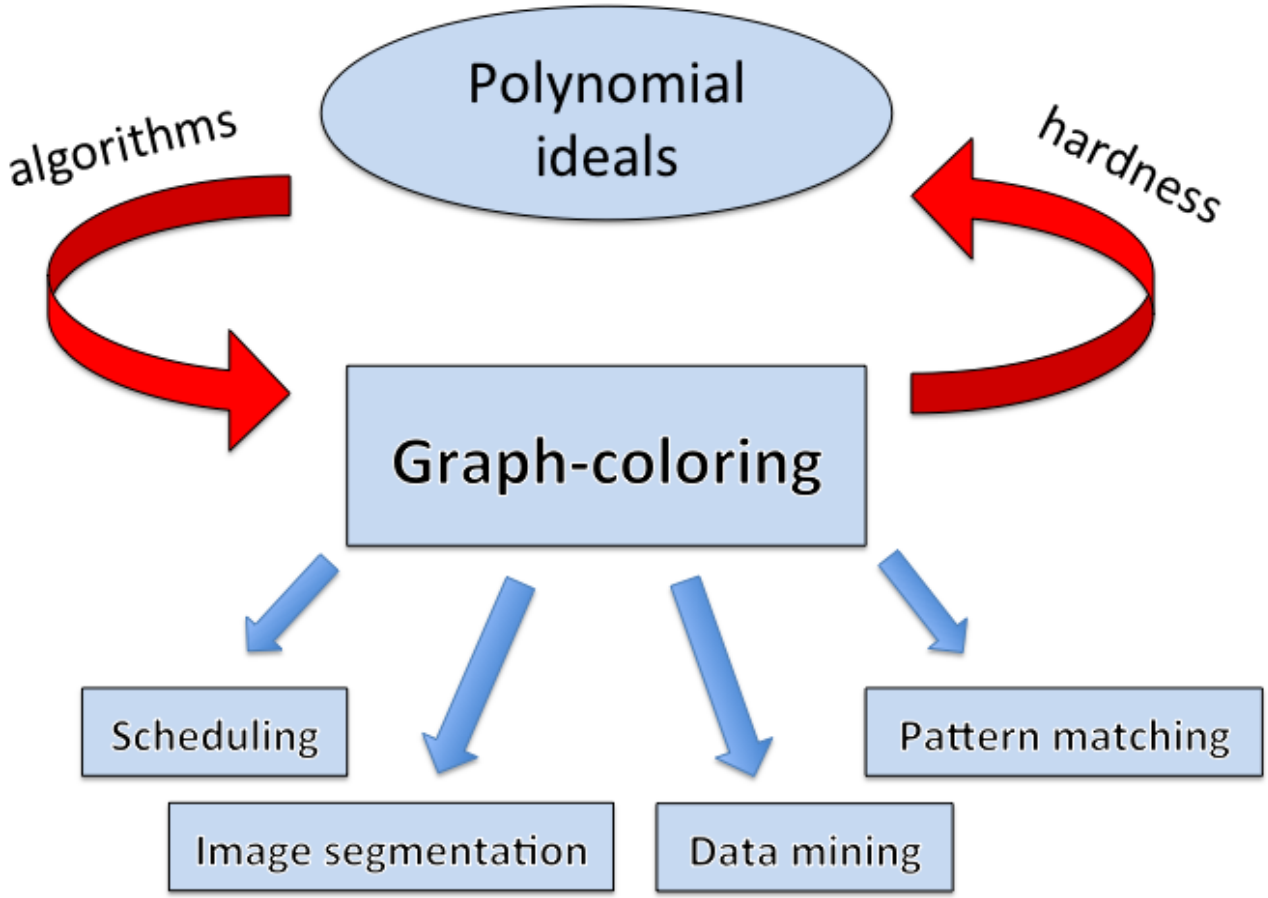
Nullstellensatz certificates, Gröbner bases for chordal graphs, and hardness of Gröbner bases

David Rolnick
Massachusetts Institute of Technology
drolnick@mit.edu

Joint work with Jesús De Loera, Susan Margulies, Michael Pernpeintner, Eric Riedl, Gwen Spencer, Despina Stasi, Jon Swenson

International Symposium on Symbolic and Algebraic Computation
Bath, July 2015

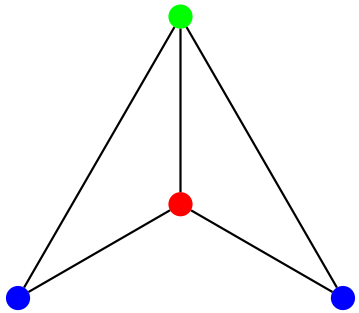
Overview


Polynomial ideals
algorithms
hardness
Graph-coloring
Scheduling
Image segmentation
Data mining
Pattern matching

Graph-coloring

Graph-coloring problem:

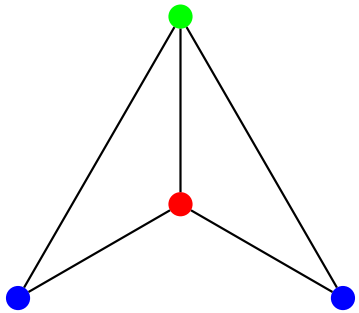
- Proper coloring: no two neighboring vertices the same color
- Is there a proper coloring with k colors?



Graph-coloring

Graph-coloring problem:

- Proper coloring: no two neighboring vertices the same color
- Is there a proper coloring with k colors?



Approach:

- k-coloring $\Leftrightarrow$ system of polynomial equations
- Solve the system or prove unsolvable

The coloring ideal

- Graph $G = (V, E)$
- Variable x_i for each vertex $i \in V$
- Coloring ideal $\mathcal{I}_k(G)$ generated by:

Vertex polynomials $$\nu_i(\mathbf{x}) := x_i^k - 1, \quad \forall i \in V$$

Edge polynomials $$\eta_{ij}(\mathbf{x}) := \frac{x_i^k - x_j^k}{x_i - x_j}, \quad \forall ij \in E$$

The coloring ideal

- Graph $G = (V, E)$
- Variable x_i for each vertex $i \in V$
- Coloring ideal $\mathcal{I}_k(G)$ generated by:

$$\text{Vertex polynomials} \quad \nu_i(\mathbf{x}) := x_i^k - 1, \quad \forall i \in V$$

$$\text{Edge polynomials} \quad \eta_{ij}(\mathbf{x}) := \frac{x_i^k - x_j^k}{x_i - x_j}, \quad \forall ij \in E$$

- Solutions $\mathbf{x} \Leftrightarrow$ proper k-colorings [Bayer 1982]

The coloring ideal

- Graph $G = (V, E)$
- Variable x_i for each vertex $i \in V$
- Coloring ideal $\mathcal{I}_k(G)$ generated by:

$$\text{Vertex polynomials} \quad \nu_i(\mathbf{x}) := x_i^k - 1, \quad \forall i \in V$$

$$\text{Edge polynomials} \quad \eta_{ij}(\mathbf{x}) := \frac{x_i^k - x_j^k}{x_i - x_j}, \quad \forall ij \in E$$

- Solutions $\mathbf{x} \Leftrightarrow$ proper k-colorings [Bayer 1982]
- Need tool for finding solutions to a polynomial system

Gröbner bases

- Polynomial ideal $\mathcal{I}$
- Leading terms of $f \in \mathcal{I}$ form leading term ideal $\mathcal{L}(\mathcal{I})$
- Gröbner basis: $g_1, g_2, \ldots, g_m \in \mathcal{I}$, leading terms generate $\mathcal{L}(\mathcal{I})$
- Implies that $\{g_i\}$ form basis for $\mathcal{I}$

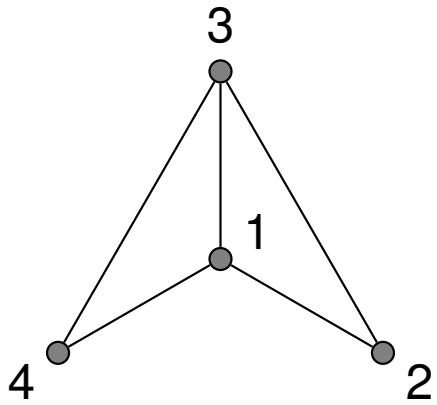
Gröbner bases

- Polynomial ideal $\mathcal{I}$
- Leading terms of $f \in \mathcal{I}$ form leading term ideal $\mathcal{L}(\mathcal{I})$
- Gröbner basis: $g_1, g_2, \ldots, g_m \in \mathcal{I}$, leading terms generate $\mathcal{L}(\mathcal{I})$
- Implies that $\{g_i\}$ form basis for $\mathcal{I}$
- Example:
  - $\mathcal{I} = \langle x + z, x + y \rangle$ with lexicographic monomial order $x > y > z$
  - $\{x + z, y - z\}$ is a Groebner basis for I
  - Check: $\langle x, y \rangle = \mathcal{L}(\mathcal{I})$

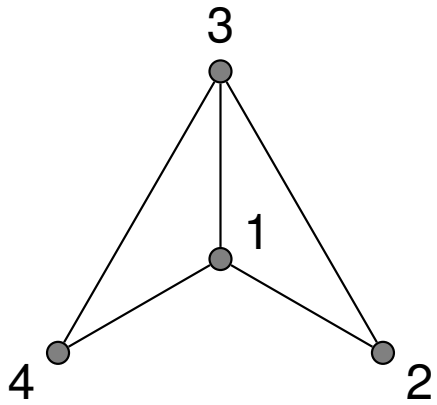
Gröbner bases

- Polynomial ideal $\mathcal{I}$
- Leading terms of $f \in \mathcal{I}$ form leading term ideal $\mathcal{L}(\mathcal{I})$
- Gröbner basis: $g_1, g_2, \ldots, g_m \in \mathcal{I}$, leading terms generate $\mathcal{L}(\mathcal{I})$
- Implies that $\{g_i\}$ form basis for $\mathcal{I}$
- Example:
  - $\mathcal{I} = \langle x + z, x + y \rangle$ with lexicographic monomial order $x > y > z$
  - $\{x + z, y - z\}$ is a Groebner basis for I
  - Check: $\langle x, y \rangle = \mathcal{L}(\mathcal{I})$
- Gröbner basis $\Rightarrow$ solutions to ideal

Gröbner basis of coloring ideal



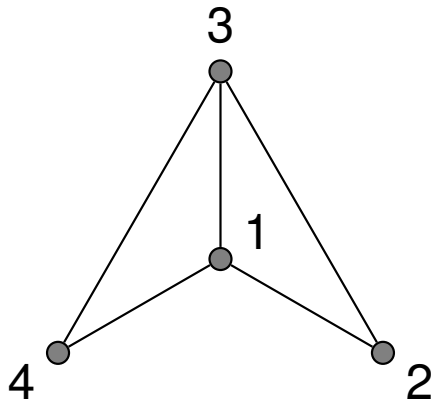
Gröbner basis of coloring ideal



- Coloring ideal for $k = 3$:

$$\langle x_1^3 - 1, x_2^3 - 1, x_3^3 - 1, x_4^3 - 1, x_1^2 + x_1x_2 + x_2^2, x_1^2 + x_1x_3 + x_3^2,$$
$$x_1^2 + x_1x_4 + x_4^2, x_2^2 + x_2x_3 + x_3^2, x_3^2 + x_3x_4 + x_4^2\rangle$$

Gröbner basis of coloring ideal

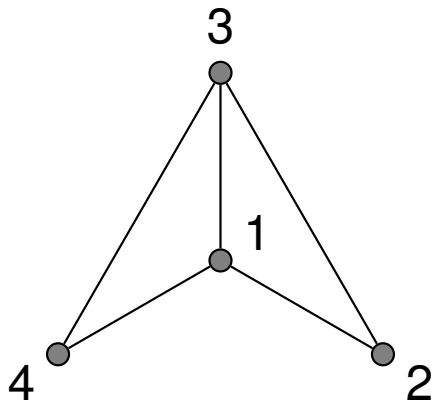


- Coloring ideal for $k = 3$:

$$\langle x_1^3 - 1, x_2^3 - 1, x_3^3 - 1, x_4^3 - 1, x_1^2 + x_1x_2 + x_2^2, x_1^2 + x_1x_3 + x_3^2,$$
$$x_1^2 + x_1x_4 + x_4^2, x_2^2 + x_2x_3 + x_3^2, x_3^2 + x_3x_4 + x_4^2\rangle$$

- Gröbner basis:

Gröbner basis of coloring ideal



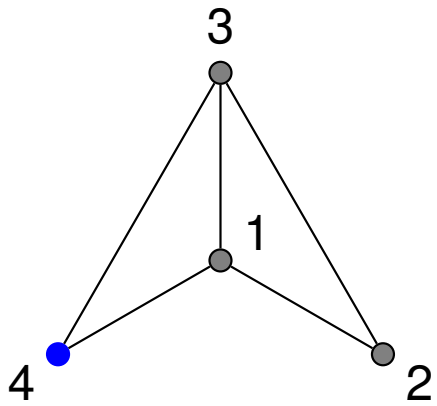
- Coloring ideal for $k = 3$:

$$\langle x_1^3 - 1, x_2^3 - 1, x_3^3 - 1, x_4^3 - 1, x_1^2 + x_1x_2 + x_2^2, x_1^2 + x_1x_3 + x_3^2,$$
$$x_1^2 + x_1x_4 + x_4^2, x_2^2 + x_2x_3 + x_3^2, x_3^2 + x_3x_4 + x_4^2\rangle$$

- Gröbner basis:

$$\{x_1 + x_3 + x_4, x_2 - x_4, {x_3}^2 + x_3x_4 + {x_4}^2, {x_4}^3 - 1\}$$

Gröbner basis of coloring ideal



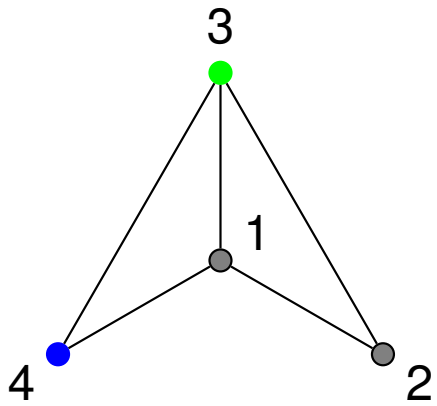
- Coloring ideal for $k = 3$:

$$\langle x_1^3 - 1, x_2^3 - 1, x_3^3 - 1, x_4^3 - 1, x_1^2 + x_1x_2 + x_2^2, x_1^2 + x_1x_3 + x_3^2,$$
$$x_1^2 + x_1x_4 + x_4^2, x_2^2 + x_2x_3 + x_3^2, x_3^2 + x_3x_4 + x_4^2\rangle$$

- Gröbner basis:

$$\{x_1 + x_3 + x_4, x_2 - x_4, {x_3}^2 + x_3x_4 + {x_4}^2, {x_4}^3 - 1\}$$

Gröbner basis of coloring ideal



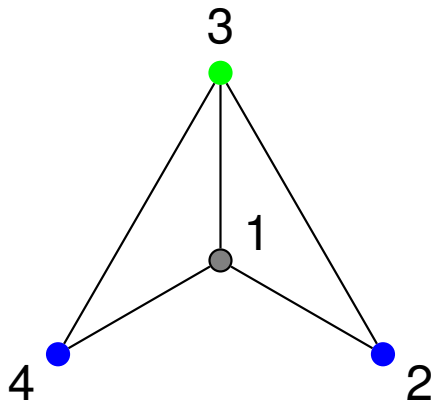
- Coloring ideal for $k = 3$:

$$\langle x_1^3 - 1, x_2^3 - 1, x_3^3 - 1, x_4^3 - 1, x_1^2 + x_1x_2 + x_2^2, x_1^2 + x_1x_3 + x_3^2,$$
$$x_1^2 + x_1x_4 + x_4^2, x_2^2 + x_2x_3 + x_3^2, x_3^2 + x_3x_4 + x_4^2\rangle$$

- Gröbner basis:

$$\{x_1 + x_3 + x_4, x_2 - x_4, {x_3}^2 + x_3x_4 + {x_4}^2, {x_4}^3 - 1\}$$

Gröbner basis of coloring ideal



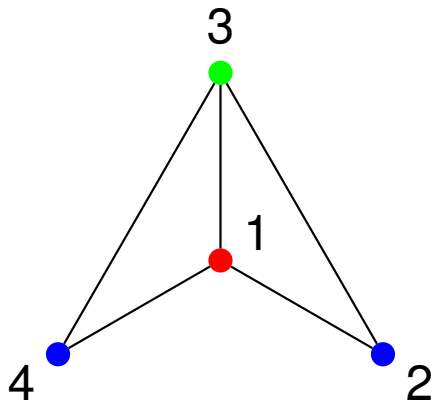
- Coloring ideal for $k = 3$:

$$\langle x_1^3 - 1, x_2^3 - 1, x_3^3 - 1, x_4^3 - 1, x_1^2 + x_1x_2 + x_2^2, x_1^2 + x_1x_3 + x_3^2,$$
$$x_1^2 + x_1x_4 + x_4^2, x_2^2 + x_2x_3 + x_3^2, x_3^2 + x_3x_4 + x_4^2\rangle$$

- Gröbner basis:

$$\{x_1 + x_3 + x_4, x_2 - x_4, {x_3}^2 + x_3x_4 + {x_4}^2, {x_4}^3 - 1\}$$

Gröbner basis of coloring ideal



- Coloring ideal for $k = 3$:

$$\langle x_1^3 - 1, x_2^3 - 1, x_3^3 - 1, x_4^3 - 1, x_1^2 + x_1x_2 + x_2^2, x_1^2 + x_1x_3 + x_3^2,$$
$$x_1^2 + x_1x_4 + x_4^2, x_2^2 + x_2x_3 + x_3^2, x_3^2 + x_3x_4 + x_4^2\rangle$$

- Gröbner basis:

$$\{x_1 + x_3 + x_4, x_2 - x_4, {x_3}^2 + x_3x_4 + {x_4}^2, {x_4}^3 - 1\}$$

Computing Gröbner bases

- Buchberger's algorithm works but is slow
- Computation of Gröbner bases is EXPSPACE-complete [Kühnle and Mayr 1996]
- Even hard to write down: maximum degree can be large
- Mayr, Ritscher (2010): upper bound on maximum degree for r-dimensional ideal, n generators of degree d:

$$2\left(\frac{1}{2}d^{n-r}+d\right)^{2^r}$$

- Ritscher (2009): example attaining maximum degree d^n
- In practice, special cases often tractable

Chordal graph algorithm

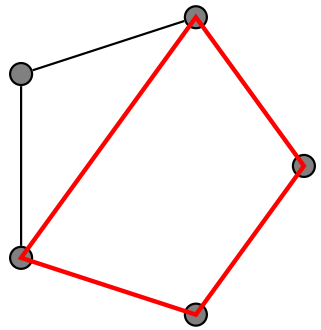
Definition

A graph is chordal if it has no induced cycle of length ≥ 4.

Chordal graph algorithm

Definition

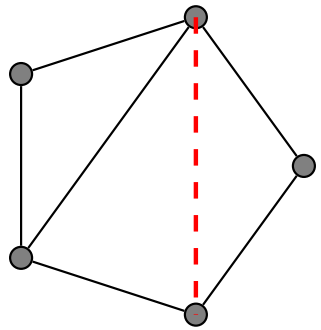
A graph is chordal if it has no induced cycle of length ≥ 4.



Chordal graph algorithm

Definition

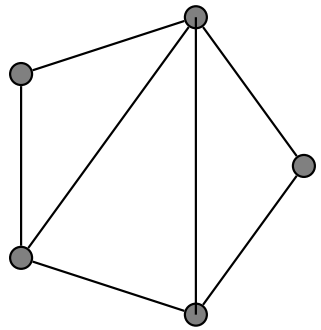
A graph is chordal if it has no induced cycle of length ≥ 4.



Chordal graph algorithm

Definition

A graph is chordal if it has no induced cycle of length ≥ 4.

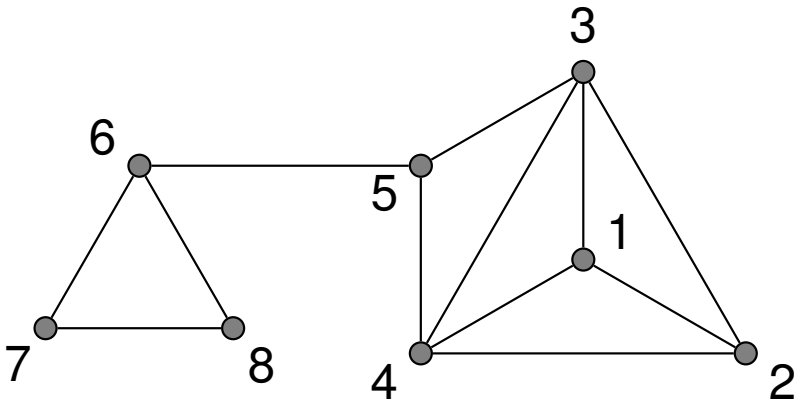


Chordal graph algorithm

Definition

A graph is chordal if it has no induced cycle of length ≥ 4.

- Chordal graphs admit a perfect elimination ordering:
  When a vertex is added, its neighborhood forms a clique



Chordal graph algorithm

Definition

A graph is chordal if it has no induced cycle of length ≥ 4.

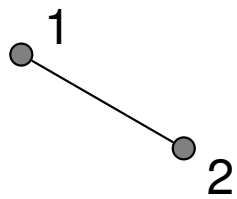
- Chordal graphs admit a perfect elimination ordering:
  When a vertex is added, its neighborhood forms a clique

Chordal graph algorithm

Definition

A graph is chordal if it has no induced cycle of length ≥ 4.

- Chordal graphs admit a perfect elimination ordering:
  When a vertex is added, its neighborhood forms a clique

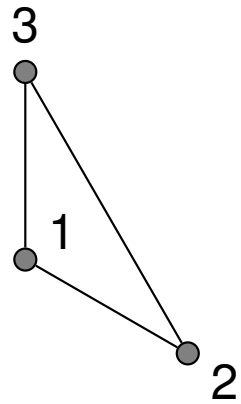


Chordal graph algorithm

Definition

A graph is chordal if it has no induced cycle of length ≥ 4.

- Chordal graphs admit a perfect elimination ordering:
  When a vertex is added, its neighborhood forms a clique

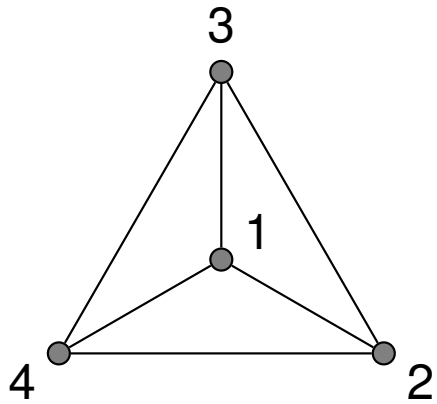


Chordal graph algorithm

Definition

A graph is chordal if it has no induced cycle of length ≥ 4.

- Chordal graphs admit a perfect elimination ordering:
  When a vertex is added, its neighborhood forms a clique

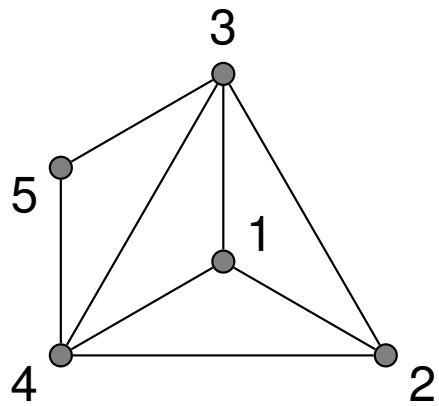


Chordal graph algorithm

Definition

A graph is chordal if it has no induced cycle of length ≥ 4.

- Chordal graphs admit a perfect elimination ordering:
  When a vertex is added, its neighborhood forms a clique

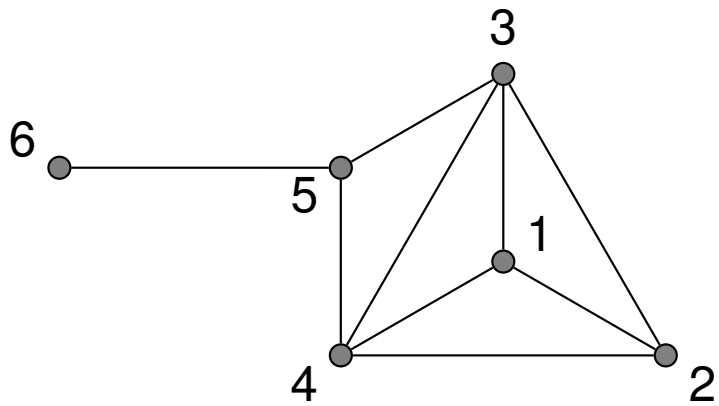


Chordal graph algorithm

Definition

A graph is chordal if it has no induced cycle of length ≥ 4.

- Chordal graphs admit a perfect elimination ordering:
  When a vertex is added, its neighborhood forms a clique

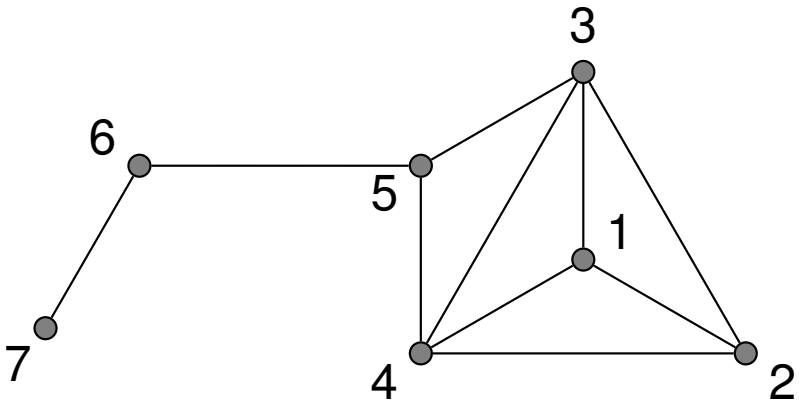


Chordal graph algorithm

Definition

A graph is chordal if it has no induced cycle of length ≥ 4.

- Chordal graphs admit a perfect elimination ordering:
  When a vertex is added, its neighborhood forms a clique

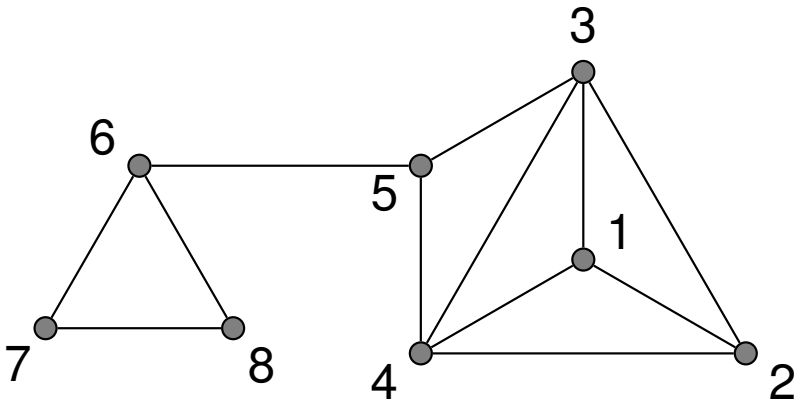


Chordal graph algorithm

Definition

A graph is chordal if it has no induced cycle of length ≥ 4.

- Chordal graphs admit a perfect elimination ordering:
  When a vertex is added, its neighborhood forms a clique



Chordal graph algorithm

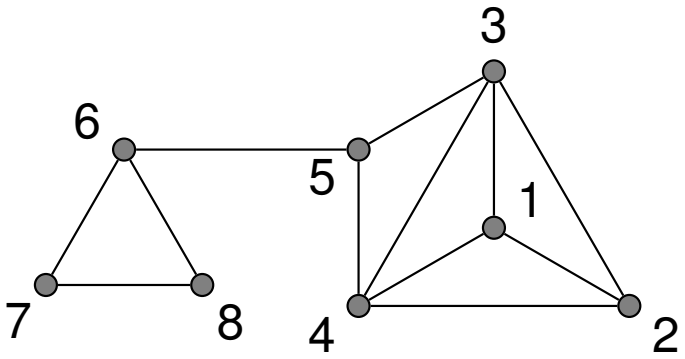
Theorem (DMPRRSSS)

Let G be a chordal graph on n vertices. Then there exists a Gröbner basis of size n for $\mathcal{I}_k(G)$, and it can be found efficiently.

Chordal graph algorithm

Theorem (DMPRRSSS)

Let G be a chordal graph on n vertices. Then there exists a Gröbner basis of size n for $\mathcal{I}_k(G)$, and it can be found efficiently.



Chordal graph algorithm

Theorem (DMPRRSSS)

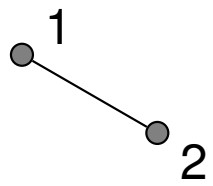
Let G be a chordal graph on n vertices. Then there exists a Gröbner basis of size n for $\mathcal{I}_k(G)$, and it can be found efficiently.

Gröbner basis $(k = 4)$: $\{\nu_1(x_1),$

Chordal graph algorithm

Theorem (DMPRRSSS)

Let G be a chordal graph on n vertices. Then there exists a Gröbner basis of size n for $\mathcal{I}_k(G)$, and it can be found efficiently.

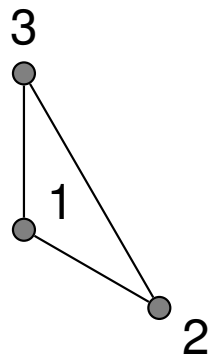


Gröbner basis $(k = 4)$: $\{\nu_1(x_1), S_3(x_1, x_2),$

Chordal graph algorithm

Theorem (DMPRRSSS)

Let G be a chordal graph on n vertices. Then there exists a Gröbner basis of size n for $\mathcal{I}_k(G)$, and it can be found efficiently.

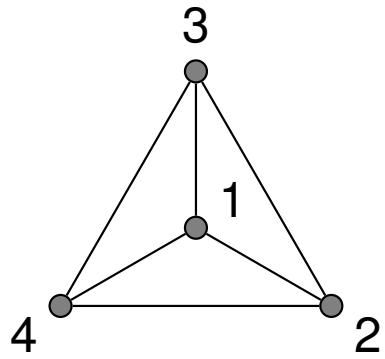


Gröbner basis $(k = 4)$: $\{\nu_1(x_1), S_3(x_1, x_2), S_2(x_1, x_2, x_3),$

Chordal graph algorithm

Theorem (DMPRRSSS)

Let G be a chordal graph on n vertices. Then there exists a Gröbner basis of size n for $\mathcal{I}_k(G)$, and it can be found efficiently.

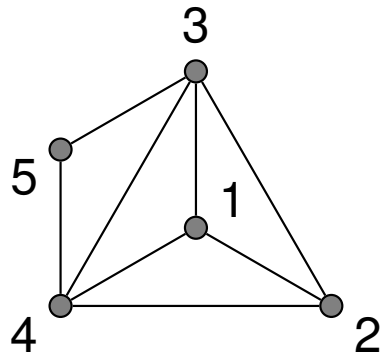


Gröbner basis $(k = 4)$: $\{\nu_1(x_1), S_3(x_1, x_2), S_2(x_1, x_2, x_3), S_1(x_1, x_2, x_3, x_4),$

Chordal graph algorithm

Theorem (DMPRRSSS)

Let G be a chordal graph on n vertices. Then there exists a Gröbner basis of size n for $\mathcal{I}_k(G)$, and it can be found efficiently.

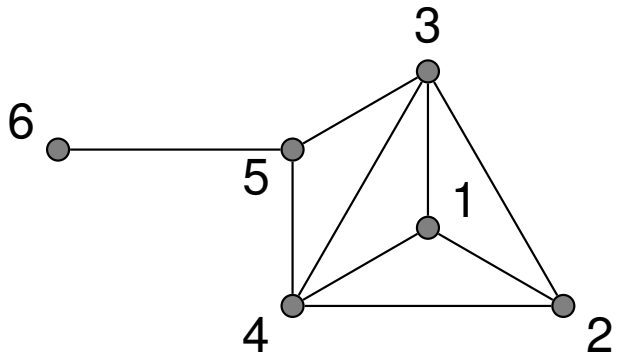


Gröbner basis $(k = 4)$: $\{\nu_1(x_1), S_3(x_1, x_2), S_2(x_1, x_2, x_3),$
$S_1(x_1, x_2, x_3, x_4), S_2(x_3, x_4, x_5),$

Chordal graph algorithm

Theorem (DMPRRSSS)

Let G be a chordal graph on n vertices. Then there exists a Gröbner basis of size n for $\mathcal{I}_k(G)$, and it can be found efficiently.

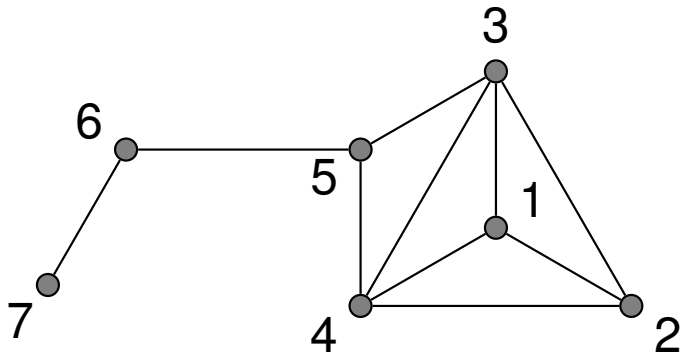


Gröbner basis $(k = 4)$: $\{\nu_1(x_1), S_3(x_1, x_2), S_2(x_1, x_2, x_3),$
$S_1(x_1, x_2, x_3, x_4), S_2(x_3, x_4, x_5), S_3(x_5, x_6),$

Chordal graph algorithm

Theorem (DMPRRSSS)

Let G be a chordal graph on n vertices. Then there exists a Gröbner basis of size n for $\mathcal{I}_k(G)$, and it can be found efficiently.

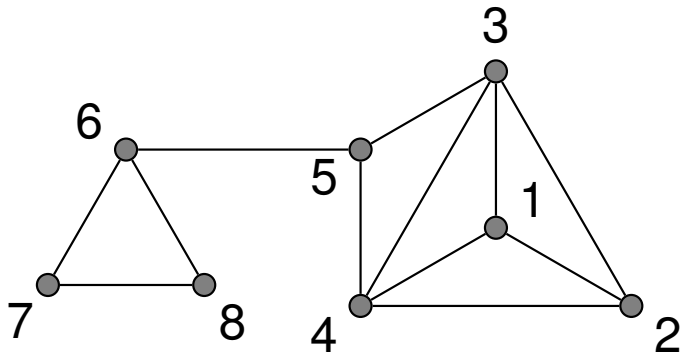


Gröbner basis $(k = 4)$: $\{\nu_1(x_1), S_3(x_1, x_2), S_2(x_1, x_2, x_3),$
$S_1(x_1, x_2, x_3, x_4), S_2(x_3, x_4, x_5), S_3(x_5, x_6), S_3(x_6, x_7),$

Chordal graph algorithm

Theorem (DMPRRSSS)

Let G be a chordal graph on n vertices. Then there exists a Gröbner basis of size n for $\mathcal{I}_k(G)$, and it can be found efficiently.



Gröbner basis $(k = 4)$: $\{\nu_1(x_1), S_3(x_1, x_2), S_2(x_1, x_2, x_3),$
$S_1(x_1, x_2, x_3, x_4), S_2(x_3, x_4, x_5), S_3(x_5, x_6), S_3(x_6, x_7), S_2(x_6, x_7, x_8)\}$

Chordal graph algorithm

Theorem (DMPRRSSS)

Let G be a chordal graph on n vertices. Then there exists a Gröbner basis of size n for $\mathcal{I}_k(G)$, and it can be found efficiently.

Gröbner basis $(k = 4)$: $\{\nu_1(x_1), S_3(x_1, x_2), S_2(x_1, x_2, x_3),$
$S_1(x_1, x_2, x_3, x_4), S_2(x_3, x_4, x_5), S_3(x_5, x_6), S_3(x_6, x_7), S_2(x_6, x_7, x_8)\}$

$$S_m(y_1, \ldots, y_t) := \sum_{1 \le j_1 \le \cdots \le j_m \le t} y_{j_1} \cdots y_{j_m} \quad .$$

Chordal graph algorithm

Theorem (DMPRRSSS)

Let G be a chordal graph on n vertices. Then there exists a Gröbner basis of size n for $\mathcal{I}_k(G)$, and it can be found efficiently.

Complete homogeneous symmetric polynomials:

$$S_m(y_1, \ldots, y_t) := \sum_{1 \le j_1 \le \cdots \le j_m \le t} y_{j_1} \cdots y_{j_m} \quad .$$

Chordal graph algorithm

Theorem (DMPRRSSS)

Let G be a chordal graph on n vertices. Then there exists a Gröbner basis of size n for $\mathcal{I}_k(G)$, and it can be found efficiently.

Complete homogeneous symmetric polynomials:

$$S_m(y_1, \ldots, y_t) := \sum_{1 \le j_1 \le \cdots \le j_m \le t} y_{j_1} \cdots y_{j_m} \quad .$$

Lemma

For a positive integer k, let $\zeta_1, \zeta_2, \ldots, \zeta_k$ be the kth roots of unity in some order. Then, for every $k > r$,
$S_m(\zeta_1, \zeta_2, \ldots, \zeta_{k-m}, x) = (x - \zeta_{k-m+1})(x - \zeta_{k-m+2}) \cdots (x - \zeta_k)$.

Chordal graph algorithm

$$S_m(y_1, \ldots, y_t) := \sum_{1 \le j_1 \le \cdots \le j_m \le t} y_{j_1} \cdots y_{j_m} \quad .$$

Lemma

For a positive integer k, let $\zeta_1, \zeta_2, \ldots, \zeta_k$ be the kth roots of unity in some order. Then, for every $k > r$,
$S_m(\zeta_1, \zeta_2, \ldots, \zeta_{k-m}, x) = (x - \zeta_{k-m+1})(x - \zeta_{k-m+2}) \cdots (x - \zeta_k)$.

Proof of algorithm

- Perfect elimination order $\Rightarrow$ polynomial $S_m(\mathbf{x})$ for each vertex

Chordal graph algorithm

$$S_m(y_1, \ldots, y_t) := \sum_{1 \le j_1 \le \cdots \le j_m \le t} y_{j_1} \cdots y_{j_m} \quad .$$

Lemma

For a positive integer k, let $\zeta_1, \zeta_2, \ldots, \zeta_k$ be the kth roots of unity in some order. Then, for every $k > r$,
$S_m(\zeta_1, \zeta_2, \ldots, \zeta_{k-m}, x) = (x - \zeta_{k-m+1})(x - \zeta_{k-m+2}) \cdots (x - \zeta_k)$.

Proof of algorithm

- Perfect elimination order $\Rightarrow$ polynomial $S_m(\mathbf{x})$ for each vertex
- These polynomials generate graph coloring ideal by induction

Chordal graph algorithm

$$S_m(y_1, \ldots, y_t) := \sum_{1 \le j_1 \le \cdots \le j_m \le t} y_{j_1} \cdots y_{j_m} \quad .$$

Lemma

For a positive integer k, let $\zeta_1, \zeta_2, \ldots, \zeta_k$ be the kth roots of unity in some order. Then, for every $k > r$,
$S_m(\zeta_1, \zeta_2, \ldots, \zeta_{k-m}, x) = (x - \zeta_{k-m+1})(x - \zeta_{k-m+2}) \cdots (x - \zeta_k)$.

Proof of algorithm

- Perfect elimination order $\Rightarrow$ polynomial $S_m(\mathbf{x})$ for each vertex
- These polynomials generate graph coloring ideal by induction
- Form Gröbner basis, by considering *S-pairs*

Hilbert's Nullstellensatz

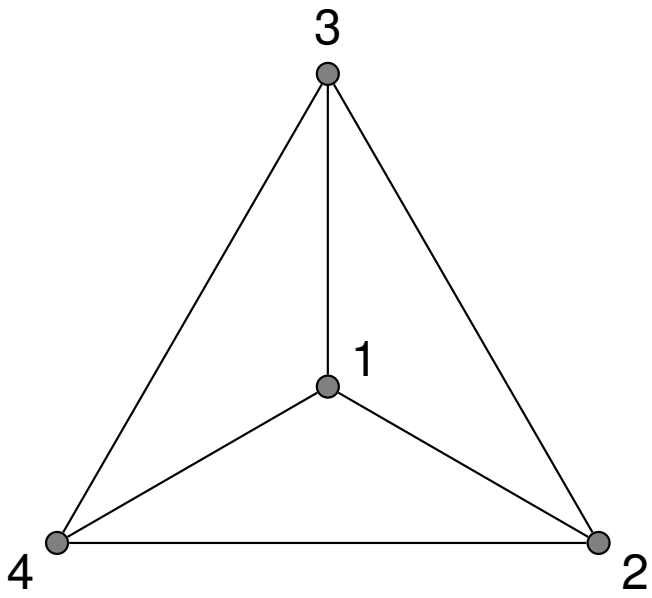
Theorem (Hilbert)

Given a field $\mathbb{K}$ *and* $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$*, the system* $f_1 = f_2 = \cdots = f_s = 0$ *has no solutions in the algebraic closure of* $\mathbb{K}$ *iff there exist polynomials* $\beta_1, \ldots, \beta_s \in \mathbb{K}[x_1, \ldots, x_n]$ *such that*

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

The set $\{\beta_i\}$ *is a Nullstellensatz certificate.*

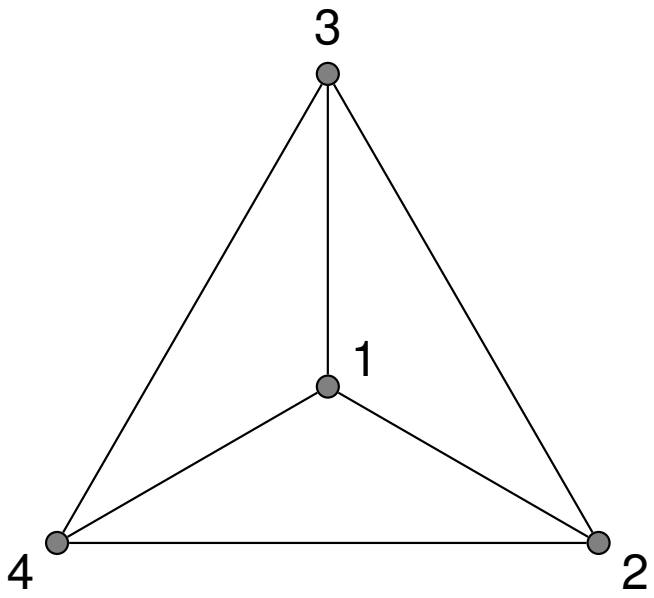
Hilbert's Nullstellensatz



Certificate of infeasibility for 3-coloring ideal:

$$1 = \nu_4(\mathbf{x}) + (-x_1) \cdot \eta_{12}(\mathbf{x}) + (-x_2 - x_4) \cdot \eta_{13}(\mathbf{x}) + (-x_1) \cdot \eta_{14}(\mathbf{x})$$
$$+ (-x_1 - x_4) \cdot \eta_{23}(\mathbf{x}) + (-x_2) \cdot \eta_{24}(\mathbf{x}) + (-x_1 - x_2) \cdot \eta_{34}(\mathbf{x})$$

Hilbert's Nullstellensatz



Gröbner basis for coloring ideal:

$$\{1\}$$

Certificate of infeasibility for 3-coloring ideal:

$$1 = \nu_4(\mathbf{x}) + (-x_1) \cdot \eta_{12}(\mathbf{x}) + (-x_2 - x_4) \cdot \eta_{13}(\mathbf{x}) + (-x_1) \cdot \eta_{14}(\mathbf{x}) + (-x_1 - x_4) \cdot \eta_{23}(\mathbf{x}) + (-x_2) \cdot \eta_{24}(\mathbf{x}) + (-x_1 - x_2) \cdot \eta_{34}(\mathbf{x})$$

Hilbert's Nullstellensatz

Theorem (Hilbert)

Given a field $\mathbb{K}$ *and* $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$*, the system* $f_1 = f_2 = \cdots = f_s = 0$ *has no solutions in the algebraic closure of* $\mathbb{K}$ *iff there exist polynomials* $\beta_1, \ldots, \beta_s \in \mathbb{K}[x_1, \ldots, x_n]$ *such that*

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

The set $\{\beta_i\}$ *is a Nullstellensatz certificate.*

- Degree of the certificate is minimum degree of the β_i

Hilbert's Nullstellensatz

Theorem (Hilbert)

Given a field $\mathbb{K}$ and $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, the system $f_1 = f_2 = \cdots = f_s = 0$ has no solutions in the algebraic closure of $\mathbb{K}$ iff there exist polynomials $\beta_1, \ldots, \beta_s \in \mathbb{K}[x_1, \ldots, x_n]$ such that

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

The set $\{\beta_i\}$ is a Nullstellensatz certificate.

- Degree of the certificate is minimum degree of the β_i
- If degree small, find certificate by brute force over finite field $\mathbb{K}$

Certificates for $\mathcal{I}_k(G)$

Theorem (DMPRRSSS)

Given a non-k-colorable graph G, let d be the minimum degree of a Nullstellensatz certificate.

- $d \equiv 1 \mod k$
- $d \geq k+1$ *if* $k > 3$.

Certificates for $\mathcal{I}_k(G)$

Theorem (DMPRRSSS)

Given a non-k-colorable graph G, let d be the minimum degree of a Nullstellensatz certificate.

- $d \equiv 1 \mod k$
- $d \geq k+1$ *if* $k > 3$.

- Brute force is inefficient for **every** G

Certificates for $\mathcal{I}_k(G)$

Example: degree-4 certificate over $\mathbb{F}_2$:

$$
\begin{aligned}
1 = {} & (1 + x_0x_2x_4 + x_0x_2x_6 + x_0x_3x_4 + x_0x_3x_5 + x_0x_4x_5 + x_0x_4x_6 + x_1^2x_4 + x_1^2x_6 \\
& + x_1x_3x_4 + x_1x_3x_5 + x_1x_5x_6 + x_2x_3x_4 + x_2x_3x_6 + x_3x_5x_6 + x_4x_5x_6)(\mathbf{x_0^3 + 1}) \\
& + (x_1 + x_3 + x_4 + x_0^2x_1x_4 + x_0^2x_1x_6 + x_0^2x_2x_4 + x_0^2x_2x_6 + x_0^2x_3x_4 + x_0^2x_3x_5 \\
& + x_0^2x_5x_6 + x_0x_1x_3x_4 + x_0x_1x_3x_6 + x_0x_2x_3x_4 + x_0x_2x_3x_6 + x_0x_2x_4x_5 + x_0x_2x_4x_6 \\
& + x_0x_2x_5x_6 + x_0x_3x_4x_5 + x_0x_3x_4x_6 + x_0x_3x_5x_6 + x_0x_4x_5x_6 + \\
& + x_1x_3x_4x_5 + x_1x_3x_4x_6 + x_1x_4x_5x_6 + x_2x_3x_4x_5 + x_2x_3x_4x_6)(\mathbf{x_0^2 + x_0x_1 + x_1^2}) \\
& + (x_1 + x_3 + x_4 + x_6 + x_0^2x_1x_4 + x_0^2x_1x_6 + x_0^2x_4x_5 + x_0^2x_4x_6 + x_0^2x_5x_6 \\
& + x_0x_1x_3x_4 + x_0x_1x_3x_6 + x_0x_3x_4x_5 + x_0x_3x_4x_6 + x_1x_3x_4x_5 + x_1x_3x_4x_6 \\
& + x_1x_4x_5x_6 + x_3x_4x_5x_6)(\mathbf{x_0^2 + x_0x_2 + x_2^2}) + \cdots
\end{aligned}
$$

Certificates for $\mathcal{I}_k(G)$

Example: degree-4 certificate over $\mathbb{F}_2$:

$$
\begin{aligned}
1 = {} & (1 + x_0x_2x_4 + x_0x_2x_6 + x_0x_3x_4 + x_0x_3x_5 + x_0x_4x_5 + x_0x_4x_6 + x_1^2x_4 + x_1^2x_6 \\
& + x_1x_3x_4 + x_1x_3x_5 + x_1x_5x_6 + x_2x_3x_4 + x_2x_3x_6 + x_3x_5x_6 + x_4x_5x_6)(\mathbf{x_0^3 + 1}) \\
& + (x_1 + x_3 + x_4 + x_0^2x_1x_4 + x_0^2x_1x_6 + x_0^2x_2x_4 + x_0^2x_2x_6 + x_0^2x_3x_4 + x_0^2x_3x_5 \\
& + x_0^2x_5x_6 + x_0x_1x_3x_4 + x_0x_1x_3x_6 + x_0x_2x_3x_4 + x_0x_2x_3x_6 + x_0x_2x_4x_5 + x_0x_2x_4x_6 \\
& + x_0x_2x_5x_6 + x_0x_3x_4x_5 + x_0x_3x_4x_6 + x_0x_3x_5x_6 + x_0x_4x_5x_6 + \\
& + x_1x_3x_4x_5 + x_1x_3x_4x_6 + x_1x_4x_5x_6 + x_2x_3x_4x_5 + x_2x_3x_4x_6)(\mathbf{x_0^2 + x_0x_1 + x_1^2}) \\
& + (x_1 + x_3 + x_4 + x_6 + x_0^2x_1x_4 + x_0^2x_1x_6 + x_0^2x_4x_5 + x_0^2x_4x_6 + x_0^2x_5x_6 \\
& + x_0x_1x_3x_4 + x_0x_1x_3x_6 + x_0x_3x_4x_5 + x_0x_3x_4x_6 + x_1x_3x_4x_5 + x_1x_3x_4x_6 \\
& + x_1x_4x_5x_6 + x_3x_4x_5x_6)(\mathbf{x_0^2 + x_0x_2 + x_2^2}) + \cdots
\end{aligned}
$$

Certificates for $\mathcal{I}_k(G)$

Example: degree-4 certificate over $\mathbb{F}_2$:

$$
\begin{aligned}
1 = {} & (1 + x_0x_2x_4 + x_0x_2x_6 + x_0x_3x_4 + x_0x_3x_5 + x_0x_4x_5 + x_0x_4x_6 + x_1^2x_4 + x_1^2x_6 \\
& + x_1x_3x_4 + x_1x_3x_5 + x_1x_5x_6 + x_2x_3x_4 + x_2x_3x_6 + x_3x_5x_6 + x_4x_5x_6)(\mathbf{x_0^3 + 1}) \\
& + (x_1 + x_3 + x_4 + x_0^2x_1x_4 + x_0^2x_1x_6 + x_0^2x_2x_4 + x_0^2x_2x_6 + x_0^2x_3x_4 + x_0^2x_3x_5 \\
& + x_0^2x_5x_6 + x_0x_1x_3x_4 + x_0x_1x_3x_6 + x_0x_2x_3x_4 + x_0x_2x_3x_6 + x_0x_2x_4x_5 + x_0x_2x_4x_6 \\
& + x_0x_2x_5x_6 + x_0x_3x_4x_5 + x_0x_3x_4x_6 + x_0x_3x_5x_6 + x_0x_4x_5x_6 + \\
& + x_1x_3x_4x_5 + x_1x_3x_4x_6 + x_1x_4x_5x_6 + x_2x_3x_4x_5 + x_2x_3x_4x_6)(\mathbf{x_0^2 + x_0x_1 + x_1^2}) \\
& + (x_1 + x_3 + x_4 + x_6 + x_0^2x_1x_4 + x_0^2x_1x_6 + x_0^2x_4x_5 + x_0^2x_4x_6 + x_0^2x_5x_6 \\
& + x_0x_1x_3x_4 + x_0x_1x_3x_6 + x_0x_3x_4x_5 + x_0x_3x_4x_6 + x_1x_3x_4x_5 + x_1x_3x_4x_6 \\
& + x_1x_4x_5x_6 + x_3x_4x_5x_6)(\mathbf{x_0^2 + x_0x_2 + x_2^2}) + \cdots
\end{aligned}
$$

Certificates for $\mathcal{I}_k(G)$

Example: degree-4 certificate over $\mathbb{F}_2$:

$$
\begin{aligned}
1 = {} & (1 + x_0x_2x_4 + x_0x_2x_6 + x_0x_3x_4 + x_0x_3x_5 + x_0x_4x_5 + x_0x_4x_6 + x_1^2x_4 + x_1^2x_6 \\
& + x_1x_3x_4 + x_1x_3x_5 + x_1x_5x_6 + x_2x_3x_4 + x_2x_3x_6 + x_3x_5x_6 + x_4x_5x_6)(\mathbf{x_0^3 + 1}) \\
& + (x_1 + x_3 + x_4 + x_0^2x_1x_4 + x_0^2x_1x_6 + x_0^2x_2x_4 + x_0^2x_2x_6 + x_0^2x_3x_4 + x_0^2x_3x_5 \\
& + x_0^2x_5x_6 + x_0x_1x_3x_4 + x_0x_1x_3x_6 + x_0x_2x_3x_4 + x_0x_2x_3x_6 + x_0x_2x_4x_5 + x_0x_2x_4x_6 \\
& + x_0x_2x_5x_6 + x_0x_3x_4x_5 + x_0x_3x_4x_6 + x_0x_3x_5x_6 + x_0x_4x_5x_6 + \\
& + x_1x_3x_4x_5 + x_1x_3x_4x_6 + x_1x_4x_5x_6 + x_2x_3x_4x_5 + x_2x_3x_4x_6)(\mathbf{x_0^2 + x_0x_1 + x_1^2}) \\
& + (x_1 + x_3 + x_4 + x_6 + x_0^2x_1x_4 + x_0^2x_1x_6 + x_0^2x_4x_5 + x_0^2x_4x_6 + x_0^2x_5x_6 \\
& + x_0x_1x_3x_4 + x_0x_1x_3x_6 + x_0x_3x_4x_5 + x_0x_3x_4x_6 + x_1x_3x_4x_5 + x_1x_3x_4x_6 \\
& + x_1x_4x_5x_6 + x_3x_4x_5x_6)(\mathbf{x_0^2 + x_0x_2 + x_2^2}) + \cdots
\end{aligned}
$$

Certificates for $\mathcal{I}_k(G)$

Example: degree-4 certificate over $\mathbb{F}_2$:

$$
\begin{aligned}
1 = {} & (1 + x_0x_2x_4 + x_0x_2x_6 + x_0x_3x_4 + x_0x_3x_5 + x_0x_4x_5 + x_0x_4x_6 + x_1^2x_4 + x_1^2x_6 \\
& + x_1x_3x_4 + x_1x_3x_5 + x_1x_5x_6 + x_2x_3x_4 + x_2x_3x_6 + x_3x_5x_6 + x_4x_5x_6)(\mathbf{x_0^3 + 1}) \\
& + (x_1 + x_3 + x_4 + x_0^2x_1x_4 + x_0^2x_1x_6 + x_0^2x_2x_4 + x_0^2x_2x_6 + x_0^2x_3x_4 + x_0^2x_3x_5 \\
& + x_0^2x_5x_6 + x_0x_1x_3x_4 + x_0x_1x_3x_6 + x_0x_2x_3x_4 + x_0x_2x_3x_6 + x_0x_2x_4x_5 + x_0x_2x_4x_6 \\
& + x_0x_2x_5x_6 + x_0x_3x_4x_5 + x_0x_3x_4x_6 + x_0x_3x_5x_6 + x_0x_4x_5x_6 + \\
& + x_1x_3x_4x_5 + x_1x_3x_4x_6 + x_1x_4x_5x_6 + x_2x_3x_4x_5 + x_2x_3x_4x_6)(\mathbf{x_0^2 + x_0x_1 + x_1^2}) \\
& + (x_1 + x_3 + x_4 + x_6 + x_0^2x_1x_4 + x_0^2x_1x_6 + x_0^2x_4x_5 + x_0^2x_4x_6 + x_0^2x_5x_6 \\
& + x_0x_1x_3x_4 + x_0x_1x_3x_6 + x_0x_3x_4x_5 + x_0x_3x_4x_6 + x_1x_3x_4x_5 + x_1x_3x_4x_6 \\
& + x_1x_4x_5x_6 + x_3x_4x_5x_6)(\mathbf{x_0^2 + x_0x_2 + x_2^2}) + \cdots
\end{aligned}
$$

Certificates for $\mathcal{I}_k(G)$

Theorem (DMPRRSSS)

Given a non-k-colorable graph G, let d be the minimum degree of a certificate.

- $d \equiv 1 \mod k$
- $d \geq k+1$ *if* $k > 3$.

Certificates for $\mathcal{I}_k(G)$

Theorem (DMPRRSSS)

Given a non-k-colorable graph G, let d be the minimum degree of a certificate.

- $d \equiv 1 \mod k$
- $d \geq k+1$ *if* $k > 3$.

Graph	k	Possible degrees	$\mathbb{F}_2$	$\mathbb{F}_3$	$\mathbb{F}_5$	$\mathbb{F}_7$
K_4	3	$1, 4, 7, 10, \ldots$	1	–	4	4
K_5	4	$5, 9, 13, \ldots$	–	5	5	5
K_6	5	$6, 11, 16, \ldots$	6	6	–	11
K_7	6	$7, 13, 19, \ldots$	–	–	13	13
K_8	7	$8, 15, 22, \ldots$	8	≥ 15	≥ 15	–
K_9	8	$9, 17, 25, \ldots$	–	≥ 17	≥ 17	≥ 17
K_{10}	9	$10, 19, 28, \ldots$	≥ 19	–	≥ 19	≥ 19
K_{11}	10	$11, 21, 31, \ldots$	–	≥ 21	–	≥ 21

Certificates for $\mathcal{I}_k(G)$

Theorem (DMPRRSSS)

Given a non-k-colorable graph G, let d be the minimum degree of a certificate.

- $d \equiv 1 \mod k$
- $d \geq k+1$ *if* $k > 3$.

Graph	k	Possible degrees	$\mathbb{F}_2$	$\mathbb{F}_3$	$\mathbb{F}_5$	$\mathbb{F}_7$
K_4	3	$1, 4, 7, 10, \ldots$	1	–	4	4
K_5	4	$5, 9, 13, \ldots$	–	5	5	5
K_6	5	$6, 11, 16, \ldots$	6	6	–	11
K_7	6	$7, 13, 19, \ldots$	–	–	13	13
K_8	7	$8, 15, 22, \ldots$	8	≥ 15	≥ 15	–
K_9	8	$9, 17, 25, \ldots$	–	≥ 17	≥ 17	≥ 17
K_{10}	9	$10, 19, 28, \ldots$	≥ 19	–	≥ 19	≥ 19
K_{11}	10	$11, 21, 31, \ldots$	–	≥ 21	–	≥ 21

- Computation over $\mathbb{F}_p$ possible only if p, k relatively prime

Certificates for $\mathcal{I}_k(G)$

Conjecture

For every field $\mathbb{K}$, the minimum degree of a k-coloring certificate grows superlinearly in k.

Graph	k	Possible degrees	$\mathbb{F}_2$	$\mathbb{F}_3$	$\mathbb{F}_5$	$\mathbb{F}_7$
K_4	3	$1, 4, 7, 10, \ldots$	1	–	4	4
K_5	4	$5, 9, 13, \ldots$	–	5	5	5
K_6	5	$6, 11, 16, \ldots$	6	6	–	11
K_7	6	$7, 13, 19, \ldots$	–	–	13	13
K_8	7	$8, 15, 22, \ldots$	8	≥ 15	≥ 15	–
K_9	8	$9, 17, 25, \ldots$	–	≥ 17	≥ 17	≥ 17
K_{10}	9	$10, 19, 28, \ldots$	≥ 19	–	≥ 19	≥ 19
K_{11}	10	$11, 21, 31, \ldots$	–	≥ 21	–	≥ 21

Inapproximability results

Definition

Given a set of polynomials f_i and an integer c.
An independent set of variables do not pairwise co-occur in any f_i.

- *Gröbner problem: Find a Gröbner basis.*

Inapproximability results

Definition

Given a set of polynomials f_i and an integer c.
An independent set of variables do not pairwise co-occur in any f_i.

- *Gröbner problem: Find a Gröbner basis.*
- *Weak c-partial Gröbner problem: Throw away c variables and the polynomials containing them, then find a Gröbner basis.*

Inapproximability results

Definition

Given a set of polynomials f_i and an integer c.
An independent set of variables do not pairwise co-occur in any f_i.

- *Gröbner problem: Find a Gröbner basis.*
- *Weak c-partial Gröbner problem: Throw away c variables and the polynomials containing them, then find a Gröbner basis.*
- *Strong c-partial Gröbner problem: Throw away c independent sets of variables and the polynomials containing them, then find a Gröbner basis.*

Inapproximability results

Definition

Given a set of polynomials f_i and an integer c.
An independent set of variables do not pairwise co-occur in any f_i.

- *Gröbner problem: Find a Gröbner basis.*
- *Weak c-partial Gröbner problem: Throw away c variables and the polynomials containing them, then find a Gröbner basis.*
- *Strong c-partial Gröbner problem: Throw away c independent sets of variables and the polynomials containing them, then find a Gröbner basis.*

Theorem (DMPRRSSS)

The strong c-partial Gröbner problem is NP-hard for every c.

Inapproximability results

Definition

Given a set of polynomials f_i and an integer c.
An independent set of variables do not pairwise co-occur in any f_i.

- *Gröbner problem: Find a Gröbner basis.*
- *Weak c-partial Gröbner problem: Throw away c variables and the polynomials containing them, then find a Gröbner basis.*
- *Strong c-partial Gröbner problem: Throw away c independent sets of variables and the polynomials containing them, then find a Gröbner basis.*

Theorem (DMPRRSSS)

The strong c-partial Gröbner problem is NP-hard for every c.

- Simpler proof holds for the weak c-partial Gröbner problem

Inapproximability results

Theorem (DMPRRSSS)

The strong c-partial Gröbner problem is NP-hard for every c.

Inapproximability results

Theorem (DMPRRSSS)

The strong c-partial Gröbner problem is NP-hard for every c.

Proof idea:

- Remove c independent sets of vertices
- Corresponds to independent sets of variables in coloring ideal
- Gröbner basis $\Rightarrow$ k-coloring of remaining vertices
- Gives $(k + c)$-coloring of graph

Inapproximability results

Theorem (DMPRRSSS)

The strong c-partial Gröbner problem is NP-hard for every c.

Proof idea:

- Remove c independent sets of vertices
- Corresponds to independent sets of variables in coloring ideal
- Gröbner basis $\Rightarrow$ k-coloring of remaining vertices
- Gives $(k + c)$-coloring of graph

Theorem (Khanna, Linial, Safra 1993)

It is NP-hard to color a k-chromatic graph with at most $k + 2\left\lfloor \frac{k}{3} \right\rfloor - 1$ colors.

Technical details

- Certain monomial orders are elimination orders
- Every lexicographic order $x_1 > \cdots > x_n$ is an elimination order
- For an elimination order, the Gröbner basis allows back-substitution, e.g.

$$x_1^3 + x_2 x_3 - x_3^2 - 1,$$
$$x_2^3 - x_2 + x_3^2 + 1,$$
$$x_2 x_3^2 - 2x_3^3 + x_3,$$
$$x_3^3 + 1.$$

Technical details

- Certain monomial orders are elimination orders
- Every lexicographic order $x_1 > \cdots > x_n$ is an elimination order
- For an elimination order, the Gröbner basis allows back-substitution, e.g.

$$x_1^3 + x_2 x_3 - x_3^2 - 1,$$
$$x_2^3 - x_2 + x_3^2 + 1,$$
$$x_2 x_3^2 - 2x_3^3 + x_3,$$
$$x_3^3 + 1.$$

- Problem: What if one cannot solve for roots of unity, e.g. over a field other than $\mathbb{R}$?

Technical details

- Certain monomial orders are elimination orders
- Every lexicographic order $x_1 > \cdots > x_n$ is an elimination order
- For an elimination order, the Gröbner basis allows back-substitution, e.g.

$$x_1^3 + x_2 x_3 - x_3^2 - 1,$$
$$x_2^3 - x_2 + x_3^2 + 1,$$
$$x_2 x_3^2 - 2x_3^3 + x_3,$$
$$x_3^3 + 1.$$

- Problem: What if one cannot solve for roots of unity, e.g. over a field other than $\mathbb{R}$?
- Solution: Do not solve numerically, merely symbolically

Summary of results

- Polytime algorithm finding Gröbner basis of graph-coloring ideal in chordal graphs
- Complexity of Nullstellensatz certificate for general graphs
- Hardness of approximate Gröbner basis computation, $\Leftarrow$ from hardness of approximate k-coloring

Questions?

Acknowledgments
This research was conducted through the AMS Mathematical Research Communities program, and was supported by the National Science Foundation under Grant Nos. DMS-1321794 and 1122374. Special thanks to Hannah Alpert, Agnes Szanto, Pablo Parrilo, Ellen Maycock, and the Simons Institute.