

Hilbert's Nullstellensatz Certificates of Infeasibility for Combinatorial Problems

Susan Margulies
*Mathematics Department,
US Naval Academy, Annapolis, Maryland*



The Classification Program of Counting Complexity
March 31, 2016

Combinatorial problem (i.e. Partition,
graph-k-colorability, matching...)

Combinatorial problem (i.e. Partition,
graph-k-colorability, matching...)



Systems of polynomial equations

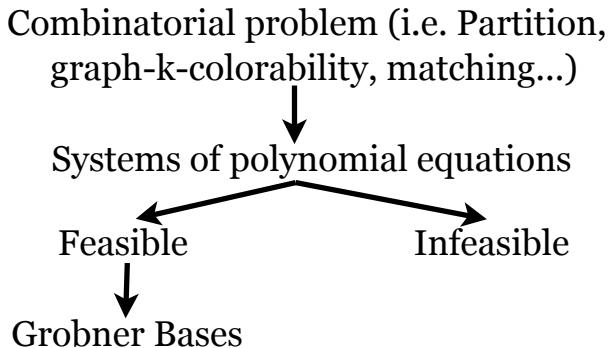
Combinatorial problem (i.e. Partition, graph-k-colorability, matching...)



Systems of polynomial equations

Feasible

Infeasible



Combinatorial problem (i.e. Partition, graph-k-colorability, matching...)



Systems of polynomial equations

Feasible

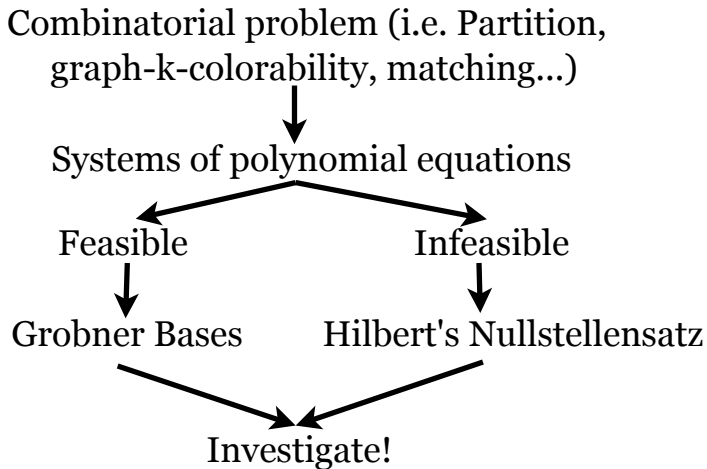
Infeasible



Grobner Bases



Hilbert's Nullstellensatz

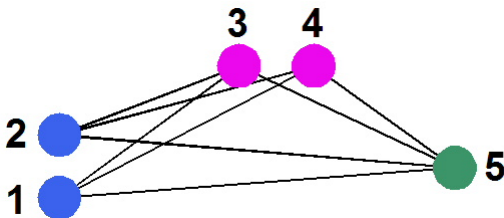


Definition of Independent Set Problem

- **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?

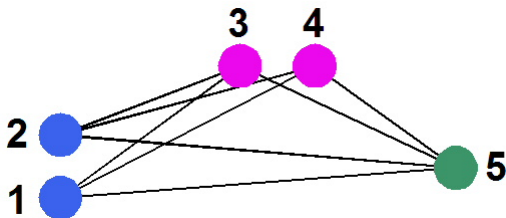
Definition of Independent Set Problem

- **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?
- **Definition:** The *stability* or *independence* number of a graph is the size of the largest independent set in the graph, and is denoted by $\alpha(G)$.
- **Turán Graph $T(5, 3)$:**



Definition of Independent Set 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?
- **Definition:** The *stability* or *independence* number of a graph is the size of the largest independent set in the graph, and is denoted by $\alpha(G)$.
- **Turán Graph** $T(5, 3)$: $\alpha(T(5, 3)) = 2$.



Given a graph G and an integer k :

- one **variable** per **vertex**: x_1, \dots, x_n
- For every vertex $i = 1, \dots, n$, let $x_i^2 - x_i = 0$.
- For every edge $(i, j) \in E(G)$, let $x_i x_j = 0$.
- Finally, let

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

Given a graph G and an integer k :

- one **variable** per **vertex**: x_1, \dots, x_n
- For every vertex $i = 1, \dots, n$, 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 $T(5, 3)$: \implies System of Polynomial Equations

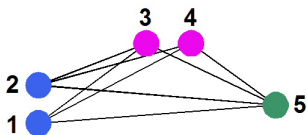


Figure: Does $T(5, 3)$ have an independent set of size 3?

$$\begin{aligned}x_1 x_3 = 0, & \quad x_1 x_4 = 0, & \quad x_1 x_5 = 0, & \quad x_2 x_3 = 0, & \quad x_1^2 - x_1 = 0, & \quad x_2^2 - x_2 = 0 \\x_2 x_4 = 0, & \quad x_2 x_5 = 0, & \quad x_3 x_5 = 0, & \quad x_4 x_5 = 0, & \quad x_3^2 - x_3 = 0, & \quad x_4^2 - x_4 = 0 \\x_1 + x_3 + x_5 + x_2 + x_4 - 3 = 0, & & & & & \quad x_5^2 - x_5 = 0\end{aligned}$$

- **Remark:** Since $T(5, 3)$ has **no** independent set of size 3, this system of polynomial equations is *infeasible*.

Hilbert's Nullstellensatz

- **Theorem (1893):** Let \mathbb{K} be an algebraically closed field and f_1, \dots, f_s be polynomials in $\mathbb{K}[x_1, \dots, x_n]$. Given a system of equations such that $\mathbf{f}_1 = \mathbf{f}_2 = \dots = \mathbf{f}_s = \mathbf{0}$, then this system has no solution if and only if there exist polynomials $\beta_1, \dots, \beta_s \in \mathbb{K}[x_1, \dots, x_n]$ such that

$$1 = \sum_{i=1}^s \beta_i \mathbf{f}_i . \quad \square$$

Hilbert's Nullstellensatz

- **Theorem (1893):** Let \mathbb{K} be an algebraically closed field and f_1, \dots, f_s be polynomials in $\mathbb{K}[x_1, \dots, x_n]$. Given a system of equations such that $\mathbf{f}_1 = \mathbf{f}_2 = \dots = \mathbf{f}_s = \mathbf{0}$, then this system has no solution if and only if there exist polynomials $\beta_1, \dots, \beta_s \in \mathbb{K}[x_1, \dots, x_n]$ such that

$$1 = \sum_{i=1}^s \beta_i \mathbf{f}_i . \quad \square$$

Hilbert's Nullstellensatz

- **Theorem (1893):** Let \mathbb{K} be an algebraically closed field and f_1, \dots, f_s be polynomials in $\mathbb{K}[x_1, \dots, x_n]$. Given a system of equations such that $\mathbf{f}_1 = \mathbf{f}_2 = \dots = \mathbf{f}_s = \mathbf{0}$, then this system has **no** solution if and only if there exist polynomials $\beta_1, \dots, \beta_s \in \mathbb{K}[x_1, \dots, x_n]$ such that

$$1 = \sum_{i=1}^s \beta_i \mathbf{f}_i . \quad \square$$

Hilbert's Nullstellensatz

- **Theorem (1893):** Let \mathbb{K} be an algebraically closed field and f_1, \dots, f_s be polynomials in $\mathbb{K}[x_1, \dots, x_n]$. Given a system of equations such that $\mathbf{f}_1 = \mathbf{f}_2 = \dots = \mathbf{f}_s = \mathbf{0}$, then this system has **no** solution if and only if there exist polynomials $\beta_1, \dots, \beta_s \in \mathbb{K}[x_1, \dots, x_n]$ such that

$$1 = \sum_{i=1}^s \beta_i \mathbf{f}_i . \quad \square$$

Hilbert's Nullstellensatz

- **Theorem (1893):** Let \mathbb{K} be an algebraically closed field and f_1, \dots, f_s be polynomials in $\mathbb{K}[x_1, \dots, x_n]$. Given a system of equations such that $\mathbf{f}_1 = \mathbf{f}_2 = \dots = \mathbf{f}_s = \mathbf{0}$, then this system has **no** solution if and only if there exist polynomials $\beta_1, \dots, \beta_s \in \mathbb{K}[x_1, \dots, x_n]$ such that

$$\mathbf{1} = \sum_{i=1}^s \beta_i \mathbf{f}_i . \quad \square$$

Hilbert's Nullstellensatz

- **Theorem (1893):** Let \mathbb{K} be an algebraically closed field and f_1, \dots, f_s be polynomials in $\mathbb{K}[x_1, \dots, x_n]$. Given a system of equations such that $\mathbf{f}_1 = \mathbf{f}_2 = \dots = \mathbf{f}_s = \mathbf{0}$, then this system has **no** solution if and only if there exist polynomials $\beta_1, \dots, \beta_s \in \mathbb{K}[x_1, \dots, x_n]$ such that

$$\mathbf{1} = \sum_{i=1}^s \beta_i \mathbf{f}_i .$$

□

Hilbert's Nullstellensatz

- **Theorem (1893):** Let \mathbb{K} be an algebraically closed field and f_1, \dots, f_s be polynomials in $\mathbb{K}[x_1, \dots, x_n]$. Given a system of equations such that $\mathbf{f}_1 = \mathbf{f}_2 = \dots = \mathbf{f}_s = \mathbf{0}$, then this system has **no** solution if and only if there exist polynomials $\beta_1, \dots, \beta_s \in \mathbb{K}[x_1, \dots, x_n]$ such that

$$\mathbf{1} = \sum_{i=1}^s \beta_i \mathbf{f}_i . \quad \square$$

Hilbert's Nullstellensatz

- **Theorem (1893):** Let \mathbb{K} be an algebraically closed field and f_1, \dots, f_s be polynomials in $\mathbb{K}[x_1, \dots, x_n]$. Given a system of equations such that $\mathbf{f}_1 = \mathbf{f}_2 = \dots = \mathbf{f}_s = \mathbf{0}$, then this system has **no** solution if and only if there exist polynomials $\beta_1, \dots, \beta_s \in \mathbb{K}[x_1, \dots, x_n]$ such that

$$\mathbf{1} = \sum_{i=1}^s \beta_i \mathbf{f}_i . \quad \square$$

$$\mathbf{1} \neq \mathbf{0}$$

Hilbert's Nullstellensatz

- **Theorem (1893):** Let \mathbb{K} be an algebraically closed field and f_1, \dots, f_s be polynomials in $\mathbb{K}[x_1, \dots, x_n]$. Given a system of equations such that $\mathbf{f}_1 = \mathbf{f}_2 = \dots = \mathbf{f}_s = \mathbf{0}$, then this system has **no** solution if and only if there exist polynomials $\beta_1, \dots, \beta_s \in \mathbb{K}[x_1, \dots, x_n]$ such that

$$\mathbf{1} = \sum_{i=1}^s \beta_i \mathbf{f}_i . \quad \square$$

$$\mathbf{1} \neq \mathbf{0}$$

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

Hilbert's Nullstellensatz

- Theorem (1893):** Let \mathbb{K} be an algebraically closed field and f_1, \dots, f_s be polynomials in $\mathbb{K}[x_1, \dots, x_n]$. Given a system of equations such that $\mathbf{f}_1 = \mathbf{f}_2 = \dots = \mathbf{f}_s = \mathbf{0}$, then this system has **no** solution if and only if there exist polynomials $\beta_1, \dots, \beta_s \in \mathbb{K}[x_1, \dots, x_n]$ such that

$$\mathbf{1} = \sum_{i=1}^s \beta_i \mathbf{f}_i . \quad \square$$

$$1 \neq 0$$

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

$$\underbrace{(-1)}_{\beta_1} \underbrace{(x_1^2 - 1)}_{f_1} + \underbrace{\left(\frac{1}{2}x_1\right)}_{\beta_2} \underbrace{(x_1 + x_2)}_{f_2} + \underbrace{\left(-\frac{1}{2}x_1\right)}_{\beta_3} \underbrace{(x_2 + x_3)}_{f_3} + \underbrace{\left(\frac{1}{2}x_1\right)}_{\beta_4} \underbrace{(x_1 + x_3)}_{f_4}$$

Hilbert's Nullstellensatz

- Theorem (1893):** Let \mathbb{K} be an algebraically closed field and f_1, \dots, f_s be polynomials in $\mathbb{K}[x_1, \dots, x_n]$. Given a system of equations such that $\mathbf{f}_1 = \mathbf{f}_2 = \dots = \mathbf{f}_s = \mathbf{0}$, then this system has **no** solution if and only if there exist polynomials $\beta_1, \dots, \beta_s \in \mathbb{K}[x_1, \dots, x_n]$ such that

$$\mathbf{1} = \sum_{i=1}^s \beta_i \mathbf{f}_i . \quad \square$$

$$1 \neq 0$$

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

$$\underbrace{(-1)}_{\beta_1} \underbrace{(x_1^2 - 1)}_{f_1} + \underbrace{\left(\frac{1}{2}x_1\right)}_{\beta_2} \underbrace{(x_1 + x_2)}_{f_2} + \underbrace{\left(-\frac{1}{2}x_1\right)}_{\beta_3} \underbrace{(x_2 + x_3)}_{f_3} + \underbrace{\left(\frac{1}{2}x_1\right)}_{\beta_4} \underbrace{(x_1 + x_3)}_{f_4}$$

$$\left(\frac{1}{2} + \frac{1}{2} - 1\right)x_1^2 + 1 + \left(\frac{1}{2} - \frac{1}{2}\right)x_1x_2 + \left(-\frac{1}{2} + \frac{1}{2}\right)x_1x_3$$

Hilbert's Nullstellensatz

- Theorem (1893):** Let \mathbb{K} be an algebraically closed field and f_1, \dots, f_s be polynomials in $\mathbb{K}[x_1, \dots, x_n]$. Given a system of equations such that $\mathbf{f}_1 = \mathbf{f}_2 = \dots = \mathbf{f}_s = \mathbf{0}$, then this system has **no** solution if and only if there exist polynomials $\beta_1, \dots, \beta_s \in \mathbb{K}[x_1, \dots, x_n]$ such that

$$\mathbf{1} = \sum_{i=1}^s \beta_i \mathbf{f}_i . \quad \square$$

$$1 \neq 0$$

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

$$\underbrace{(-1)}_{\beta_1} \underbrace{(x_1^2 - 1)}_{f_1} + \underbrace{\left(\frac{1}{2}x_1\right)}_{\beta_2} \underbrace{(x_1 + x_2)}_{f_2} + \underbrace{\left(-\frac{1}{2}x_1\right)}_{\beta_3} \underbrace{(x_2 + x_3)}_{f_3} + \underbrace{\left(\frac{1}{2}x_1\right)}_{\beta_4} \underbrace{(x_1 + x_3)}_{f_4}$$

$$\left(\frac{1}{2} + \frac{1}{2} - 1\right)x_1^2 + 1 + \left(\frac{1}{2} - \frac{1}{2}\right)x_1x_2 + \left(-\frac{1}{2} + \frac{1}{2}\right)x_1x_3 = 1$$

Hilbert's Nullstellensatz

- **Theorem (1893):** Let \mathbb{K} be an algebraically closed field and f_1, \dots, f_s be polynomials in $\mathbb{K}[x_1, \dots, x_n]$. Given a system of equations such that $\mathbf{f}_1 = \mathbf{f}_2 = \dots = \mathbf{f}_s = \mathbf{0}$, then this system has **no** solution if and only if there exist polynomials $\beta_1, \dots, \beta_s \in \mathbb{K}[x_1, \dots, x_n]$ such that

$$\mathbf{1} = \underbrace{\sum_{i=1}^s \beta_i \mathbf{f}_i}_{\text{}} . \quad \square$$

This polynomial identity is a *Nullstellensatz certificate*.

Hilbert's Nullstellensatz

- **Theorem (1893):** Let \mathbb{K} be an algebraically closed field and f_1, \dots, f_s be polynomials in $\mathbb{K}[x_1, \dots, x_n]$. Given a system of equations such that $\mathbf{f}_1 = \mathbf{f}_2 = \dots = \mathbf{f}_s = \mathbf{0}$, then this system has **no** solution if and only if there exist polynomials $\beta_1, \dots, \beta_s \in \mathbb{K}[x_1, \dots, x_n]$ such that

$$\mathbf{1} = \underbrace{\sum_{i=1}^s \beta_i \mathbf{f}_i}_{\text{Nullstellensatz certificate}} . \quad \square$$

This polynomial identity is a *Nullstellensatz certificate*.

- **Definition:** Let $d = \max \{ \deg(\beta_1), \deg(\beta_2), \dots, \deg(\beta_s) \}$. Then d is the *degree of the Nullstellensatz certificate*.

How do we find Nullstellensatz certificates?

- A system of polynomial equations

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

How do we find Nullstellensatz certificates?

- A system of polynomial equations

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

- 1 Construct a **hypothetical** Nullstellensatz certificate of degree 1

$$\begin{aligned} 1 = & \underbrace{(c_0x_1 + c_1x_2 + c_2x_3 + c_3)}_{\beta_1} (x_1^2 - 1) + \underbrace{(c_4x_1 + c_5x_2 + c_6x_3 + c_7)}_{\beta_2} (x_1 + x_2) \\ & + \underbrace{(c_8x_1 + c_9x_2 + c_{10}x_3 + c_{11})}_{\beta_3} (x_1 + x_3) + \underbrace{(c_{12}x_1 + c_{13}x_2 + c_{14}x_3 + c_{15})}_{\beta_4} (x_2 + x_3) \end{aligned}$$

How do we find Nullstellensatz certificates?

- A system of polynomial equations

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

- Construct a **hypothetical** Nullstellensatz certificate of degree 1

$$1 = \underbrace{(c_0x_1 + c_1x_2 + c_2x_3 + c_3)}_{\beta_1}(x_1^2 - 1) + \underbrace{(c_4x_1 + c_5x_2 + c_6x_3 + c_7)}_{\beta_2}(x_1 + x_2) \\ + \underbrace{(c_8x_1 + c_9x_2 + c_{10}x_3 + c_{11})}_{\beta_3}(x_1 + x_3) + \underbrace{(c_{12}x_1 + c_{13}x_2 + c_{14}x_3 + c_{15})}_{\beta_4}(x_2 + x_3)$$

- Expand the **hypothetical** Nullstellensatz certificate

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

How do we find Nullstellensatz certificates?

- A system of polynomial equations

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

- Construct a **hypothetical** Nullstellensatz certificate of degree 1

$$1 = \underbrace{(c_0x_1 + c_1x_2 + c_2x_3 + c_3)}_{\beta_1}(x_1^2 - 1) + \underbrace{(c_4x_1 + c_5x_2 + c_6x_3 + c_7)}_{\beta_2}(x_1 + x_2) \\ + \underbrace{(c_8x_1 + c_9x_2 + c_{10}x_3 + c_{11})}_{\beta_3}(x_1 + x_3) + \underbrace{(c_{12}x_1 + c_{13}x_2 + c_{14}x_3 + c_{15})}_{\beta_4}(x_2 + x_3)$$

- Expand the **hypothetical** Nullstellensatz certificate

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

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

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

How do we find Nullstellensatz certificates?

- ④ Solve the linear system, and assemble the certificate

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

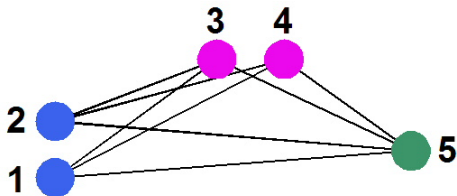
How do we find Nullstellensatz certificates?

- 4 Solve the linear system, and assemble the certificate

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

- 5 Otherwise, increment the degree and repeat.

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



$$\begin{aligned}
 1 = & \left(\frac{x_1 x_2 + x_3 x_4}{12} - \frac{x_1 + x_3 + x_5 + x_2 + x_4}{12} - \frac{1}{4} \right) (x_1 + x_3 + x_5 + x_2 + x_4 - 4) + \\
 & \left(\frac{x_4}{12} + \frac{x_2}{12} + \frac{1}{6} \right) x_1 x_3 + \left(\frac{x_2}{12} + \frac{1}{6} \right) x_1 x_4 + \left(\frac{x_2}{12} + \frac{1}{6} \right) x_1 x_5 + \left(\frac{x_4}{12} + \frac{1}{6} \right) x_2 x_3 + \\
 & \frac{x_2 x_4}{6} + \frac{x_2 x_5}{6} + \left(\frac{x_4}{12} + \frac{1}{6} \right) x_3 x_5 + \frac{x_4 x_5}{6} + \left(\frac{x_2}{12} + \frac{1}{12} \right) (x_1^2 - x_1) + \\
 & \left(\frac{x_1}{12} + \frac{1}{12} \right) (x_2^2 - x_2) + \left(\frac{x_4}{12} + \frac{1}{12} \right) (x_3^2 - x_3) + \left(\frac{x_3}{12} + \frac{1}{12} \right) (x_4^2 - x_4) + \frac{x_5^2 - x_5}{12}
 \end{aligned}$$

Nullstellensatz certificates of Independent Set have Large Degree and are Dense

- **Theorem (J. De Loera, J. Lee, S.M., S. Onn, 2007):** 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 .

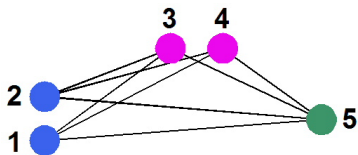
Nullstellensatz certificates of Independent Set have Large Degree and are Dense

- **Theorem (J. De Loera, J. Lee, S.M., S. Onn, 2007):** 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 .

Nullstellensatz certificates of Independent Set have Large Degree and are Dense

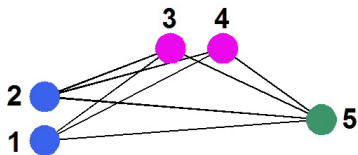
- **Theorem (J. De Loera, J. Lee, S.M., S. Onn, 2007):** For a graph G , a minimum-degree Nullstellensatz certificate for the non-existence of a independent set of size greater than $\alpha(G)$ has **degree equal to $\alpha(G)$** and contains **at least one term for every independent set** in G .

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



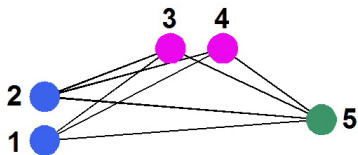
$$\begin{aligned}
 1 = & \left(\frac{x_1 x_2 + x_3 x_4}{12} - \frac{x_1 + x_3 + x_5 + x_2 + x_4}{12} - \frac{1}{4} \right) (x_1 + x_3 + x_5 + x_2 + x_4 - 4) + \\
 & \left(\frac{x_4}{12} + \frac{x_2}{12} + \frac{1}{6} \right) x_1 x_3 + \left(\frac{x_2}{12} + \frac{1}{6} \right) x_1 x_4 + \left(\frac{x_2}{12} + \frac{1}{6} \right) x_1 x_5 + \left(\frac{x_4}{12} + \frac{1}{6} \right) x_2 x_3 + \\
 & \frac{x_2 x_4}{6} + \frac{x_2 x_5}{6} + \left(\frac{x_4}{12} + \frac{1}{6} \right) x_3 x_5 + \frac{x_4 x_5}{6} + \left(\frac{x_2}{12} + \frac{1}{12} \right) (x_1^2 - x_1) + \\
 & \left(\frac{x_1}{12} + \frac{1}{12} \right) (x_2^2 - x_2) + \left(\frac{x_4}{12} + \frac{1}{12} \right) (x_3^2 - x_3) + \left(\frac{x_3}{12} + \frac{1}{12} \right) (x_4^2 - x_4) + \frac{x_5^2 - x_5}{12}
 \end{aligned}$$

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



$$\begin{aligned}
 1 = & \left(\frac{x_1 x_2 + x_3 x_4}{12} - \frac{x_1 + x_3 + x_5 + x_2 + x_4}{12} - \frac{1}{4} \right) (x_1 + x_3 + x_5 + x_2 + x_4 - 4) + \\
 & \left(\frac{x_4}{12} + \frac{x_2}{12} + \frac{1}{6} \right) x_1 x_3 + \left(\frac{x_2}{12} + \frac{1}{6} \right) x_1 x_4 + \left(\frac{x_2}{12} + \frac{1}{6} \right) x_1 x_5 + \left(\frac{x_4}{12} + \frac{1}{6} \right) x_2 x_3 + \\
 & \frac{x_2 x_4}{6} + \frac{x_2 x_5}{6} + \left(\frac{x_4}{12} + \frac{1}{6} \right) x_3 x_5 + \frac{x_4 x_5}{6} + \left(\frac{x_2}{12} + \frac{1}{12} \right) (x_1^2 - x_1) + \\
 & \left(\frac{x_1}{12} + \frac{1}{12} \right) (x_2^2 - x_2) + \left(\frac{x_4}{12} + \frac{1}{12} \right) (x_3^2 - x_3) + \left(\frac{x_3}{12} + \frac{1}{12} \right) (x_4^2 - x_4) + \frac{x_5^2 - x_5}{12}
 \end{aligned}$$

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



$$\begin{aligned}
 1 = & \left(\frac{x_1 x_2 + x_3 x_4}{12} - \frac{x_1 + x_3 + x_5 + x_2 + x_4}{12} - \frac{1}{4} \right) (x_1 + x_3 + x_5 + x_2 + x_4 - 4) + \\
 & \left(\frac{x_4}{12} + \frac{x_2}{12} + \frac{1}{6} \right) x_1 x_3 + \left(\frac{x_2}{12} + \frac{1}{6} \right) x_1 x_4 + \left(\frac{x_2}{12} + \frac{1}{6} \right) x_1 x_5 + \left(\frac{x_4}{12} + \frac{1}{6} \right) x_2 x_3 + \\
 & \frac{x_2 x_4}{6} + \frac{x_2 x_5}{6} + \left(\frac{x_4}{12} + \frac{1}{6} \right) x_3 x_5 + \frac{x_4 x_5}{6} + \left(\frac{x_2}{12} + \frac{1}{12} \right) (x_1^2 - x_1) + \\
 & \left(\frac{x_1}{12} + \frac{1}{12} \right) (x_2^2 - x_2) + \left(\frac{x_4}{12} + \frac{1}{12} \right) (x_3^2 - x_3) + \left(\frac{x_3}{12} + \frac{1}{12} \right) (x_4^2 - x_4) + \frac{x_5^2 - x_5}{12}
 \end{aligned}$$

Question:

Do the actual *numbers* within the Nullstellensatz certificates likewise have a combinatorial interpretation?

Partition Problem: Definition and Example

- **Partition:** Given set of integers $W = \{w_1, \dots, w_n\}$, can W be partitioned into two sets, S and $W \setminus S$ such that

$$\sum_{w \in S} w = \sum_{w \in W \setminus S} w .$$

Partition Problem: Definition and Example

- **Partition:** Given set of integers $W = \{w_1, \dots, w_n\}$, can W be partitioned into two sets, S and $W \setminus S$ such that

$$\sum_{w \in S} w = \sum_{w \in W \setminus S} w .$$

- **Example:** Let $W = \{ \underbrace{1, 3, 5, 7}_S, \underbrace{7, 9}_{W \setminus S} \}$. Then

Partition Problem: Definition and Example

- **Partition:** Given set of integers $W = \{w_1, \dots, w_n\}$, can W be partitioned into two sets, S and $W \setminus S$ such that

$$\sum_{w \in S} w = \sum_{w \in W \setminus S} w .$$

- **Example:** Let $W = \{\underbrace{1, 3, 5, 7}_S, \underbrace{7, 9}_{W \setminus S}\}$. Then

$$\underbrace{1 + 3 + 5 + 7}_S .$$

Partition Problem: Definition and Example

- **Partition:** Given set of integers $W = \{w_1, \dots, w_n\}$, can W be partitioned into two sets, S and $W \setminus S$ such that

$$\sum_{w \in S} w = \sum_{w \in W \setminus S} w .$$

- **Example:** Let $W = \{\underbrace{1, 3, 5, 7}_S, \underbrace{7, 9}_{W \setminus S}\}$. Then

$$\underbrace{1 + 3 + 5 + 7}_S \quad \underbrace{7 + 9}_{W \setminus S} .$$

Partition Problem: Definition and Example

- **Partition:** Given set of integers $W = \{w_1, \dots, w_n\}$, can W be partitioned into two sets, S and $W \setminus S$ such that

$$\sum_{w \in S} w = \sum_{w \in W \setminus S} w .$$

- **Example:** Let $W = \{\underbrace{1, 3, 5, 7}_S, \underbrace{7, 9}_{W \setminus S}\}$. Then

$$16 = \underbrace{1 + 3 + 5 + 7}_S = \underbrace{7 + 9}_{W \setminus S} = 16 .$$

Partition Problem: Definition and Example

- **Partition:** Given set of integers $W = \{w_1, \dots, w_n\}$, can W be partitioned into two sets, S and $W \setminus S$ such that

$$\sum_{w \in S} w = \sum_{w \in W \setminus S} w .$$

- **Example:** Let $W = \{\underbrace{1, 3, 5, 7}_S, \underbrace{7, 9}_{W \setminus S}\}$. Then

$$16 = \underbrace{1 + 3 + 5 + 7}_S = \underbrace{7 + 9}_{W \setminus S} = 16 .$$

- The **Partition** problem is NP-complete.

Partition as a System of Polynomial Equations

Given a set of integers $W = \{w_1, \dots, w_n\}$:

- one **variable** per **integer**: x_1, \dots, x_n

Partition as a System of Polynomial Equations

Given a set of integers $W = \{w_1, \dots, w_n\}$:

- one **variable** per **integer**: x_1, \dots, x_n
- For $i = 1, \dots, n$, let $x_i^2 - 1 = 0$,

Partition as a System of Polynomial Equations

Given a set of integers $W = \{w_1, \dots, w_n\}$:

- one **variable** per **integer**: x_1, \dots, x_n
- For $i = 1, \dots, n$, let $x_i^2 - 1 = 0$,
- and,

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

Partition as a System of Polynomial Equations

Given a set of integers $W = \{w_1, \dots, w_n\}$:

- one **variable** per **integer**: x_1, \dots, x_n
- For $i = 1, \dots, n$, let $x_i^2 - 1 = 0$,
- and,

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

- **Proposition:** Given a set of integers $W = \{w_1, \dots, w_n\}$, the above system of $n + 1$ polynomial equations has a solution if and only if there exists a partition of W into two sets, $S \subseteq W$ and $W \setminus S$, such that $\sum_{w \in S} w = \sum_{w \in W \setminus S} w$.

Partition as a System of Polynomial Equations

Given a set of integers $W = \{w_1, \dots, w_n\}$:

- one **variable** per **integer**: x_1, \dots, x_n
- For $i = 1, \dots, n$, let $x_i^2 - 1 = 0$,
- and,

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

- **Proposition:** Given a set of integers $W = \{w_1, \dots, w_n\}$, the above system of $n + 1$ polynomial equations has a solution if and only if there exists a partition of W into two sets, $S \subseteq W$ and $W \setminus S$, such that $\sum_{w \in S} w = \sum_{w \in W \setminus S} w$.

Question: Let $W = \{1, 3, 5, 2\}$. Is W partitionable?

$$x_1^2 - 1 = 0, \quad x_2^2 - 1 = 0, \quad x_3^2 - 1 = 0, \quad x_4^2 - 1 = 0, \\ x_1 + 3x_2 + 5x_3 + 2x_4 = 0 .$$

Minimum-degree Nullstellensatz Certificates Example

Question: Let $W = \{1, 3, 5, 2\}$. Is W partitionable?

$$x_1^2 - 1 = 0, \quad x_2^2 - 1 = 0, \quad x_3^3 - 1 = 0, \quad x_4^2 - 1 = 0, \\ x_1 + 3x_2 + 5x_3 + 2x_4 = 0.$$

Minimum-degree Nullstellensatz Certificates Example

Question: Let $W = \{1, 3, 5, 2\}$. Is W partitionable? Answer: No!

$$x_1^2 - 1 = 0, \quad x_2^2 - 1 = 0, \quad x_3^3 - 1 = 0, \quad x_4^2 - 1 = 0, \\ x_1 + 3x_2 + 5x_3 + 2x_4 = 0.$$

Minimum-degree Nullstellensatz Certificates Example

Question: Let $W = \{1, 3, 5, 2\}$. Is W partitionable? Answer: No!

$$x_1^2 - 1 = 0, \quad x_2^2 - 1 = 0, \quad x_3^3 - 1 = 0, \quad x_4^2 - 1 = 0, \\ x_1 + 3x_2 + 5x_3 + 2x_4 = 0.$$

$$\begin{aligned} 1 = & \left(-\frac{155}{693} + \frac{842}{3465}x_2x_3 - \frac{188}{693}x_2x_4 + \frac{908}{3465}x_3x_4 \right) (x_1^2 - 1) \\ & + \left(-\frac{1}{231} + \frac{842}{1155}x_1x_3 - \frac{188}{231}x_1x_4 + \frac{292}{1155}x_3x_4 \right) (x_2^2 - 1) \\ & + \left(-\frac{467}{693} + \frac{842}{693}x_1x_2 + \frac{908}{693}x_1x_4 + \frac{292}{693}x_2x_4 \right) (x_3^2 - 1) \\ & + \left(-\frac{68}{693} - \frac{376}{693}x_1x_2 + \frac{1816}{3465}x_1x_3 + \frac{584}{3465}x_2x_3 \right) (x_4^2 - 1) \\ & + \left(\frac{155}{693}x_1 + \frac{1}{693}x_2 + \frac{467}{3465}x_3 + \frac{34}{693}x_4 - \frac{842}{3465}x_1x_2x_3 \right. \\ & \left. + \frac{188}{693}x_1x_2x_4 - \frac{908}{3465}x_1x_3x_4 - \frac{292}{3465}x_2x_3x_4 \right) (x_1 + 3x_2 + 5x_3 + 2x_4). \end{aligned}$$

Minimum-degree *Partition* Nullstellensatz Certificates

Let S_k^n denote the set of k -subsets of $\{1, \dots, n\}$ (i.e., $|S_k^n| = \binom{n}{k}$)

Minimum-degree Nullstellensatz Certificates

Let S_k^n denote the set of k -subsets of $\{1, \dots, n\}$ (i.e., $|S_k^n| = \binom{n}{k}$)

Theorem (S.M., S. Onn, 2012)

Given a set of non-partitionable integers $W = \{w_1, \dots, w_n\}$ encoded as a system of polynomial equations as above, there exists a **minimum-degree** Nullstellensatz certificate for the non-existence of a partition of W as follows:

$$1 = \sum_{i=1}^n \left(\sum_{\substack{k \text{ even} \\ k \leq n-1}} \sum_{s \in S_k^{n \setminus i}} c_{i,s} x^s \right) (x_i^2 - 1) + \left(\sum_{\substack{k \text{ odd} \\ k \leq n}} \sum_{s \in S_k^n} b_s x^s \right) \left(\sum_{i=1}^n w_i x_i \right).$$

Moreover, every Nullstellensatz certificate associated with the above system of polynomial equations contains **exactly one monomial** for **each** of the **even parity subsets** of $S_k^{n \setminus i}$, and **exactly one monomial** for **each** of the **odd parity subsets** of S_k^n .

Minimum-degree Nullstellensatz Certificates

Let S_k^n denote the set of k -subsets of $\{1, \dots, n\}$ (i.e., $|S_k^n| = \binom{n}{k}$)

Theorem (S.M., S. Onn, 2012)

Given a set of non-partitionable integers $W = \{w_1, \dots, w_n\}$ encoded as a system of polynomial equations as above, there exists a **minimum-degree** Nullstellensatz certificate for the non-existence of a partition of W as follows:

$$1 = \sum_{i=1}^n \left(\sum_{\substack{k \text{ even} \\ k \leq n-1}} \sum_{s \in S_k^{n \setminus i}} c_{i,s} x^s \right) (x_i^2 - 1) + \left(\sum_{\substack{k \text{ odd} \\ k \leq n}} \sum_{s \in S_k^n} b_s x^s \right) \left(\sum_{i=1}^n w_i x_i \right).$$

Moreover, every Nullstellensatz certificate associated with the above system of polynomial equations contains **exactly one monomial** for **each** of the **even parity subsets** of $S_k^{n \setminus i}$, and **exactly one monomial** for **each** of the **odd parity subsets** of S_k^n .

Note: certificate is both high degree and dense.

Minimum-degree Nullstellensatz Certificates Example

Question: Let $W = \{1, 3, 5, 2\}$. Is W partitionable? Answer: No!

$$x_1^2 - 1 = 0, \quad x_2^2 - 1 = 0, \quad x_3^3 - 1 = 0, \quad x_4^2 - 1 = 0, \\ x_1 + 3x_2 + 5x_3 + 2x_4 = 0.$$

$$\begin{aligned} 1 = & \left(-\frac{155}{693} + \frac{842}{3465}x_2x_3 - \frac{188}{693}x_2x_4 + \frac{908}{3465}x_3x_4 \right) (x_1^2 - 1) \\ & + \left(-\frac{1}{231} + \frac{842}{1155}x_1x_3 - \frac{188}{231}x_1x_4 + \frac{292}{1155}x_3x_4 \right) (x_2^2 - 1) \\ & + \left(-\frac{467}{693} + \frac{842}{693}x_1x_2 + \frac{908}{693}x_1x_4 + \frac{292}{693}x_2x_4 \right) (x_3^2 - 1) \\ & + \left(-\frac{68}{693} - \frac{376}{693}x_1x_2 + \frac{1816}{3465}x_1x_3 + \frac{584}{3465}x_2x_3 \right) (x_4^2 - 1) \\ & + \left(\frac{155}{693}x_1 + \frac{1}{693}x_2 + \frac{467}{3465}x_3 + \frac{34}{693}x_4 - \frac{842}{3465}x_1x_2x_3 \right. \\ & \left. + \frac{188}{693}x_1x_2x_4 - \frac{908}{3465}x_1x_3x_4 - \frac{292}{3465}x_2x_3x_4 \right) (x_1 + 3x_2 + 5x_3 + 2x_4). \end{aligned}$$

Minimum-degree Nullstellensatz Certificates Example

Question: Let $W = \{1, 3, 5, 2\}$. Is W partitionable? Answer: No!

$$x_1^2 - 1 = 0, \quad x_2^2 - 1 = 0, \quad x_3^3 - 1 = 0, \quad x_4^2 - 1 = 0, \\ x_1 + 3x_2 + 5x_3 + 2x_4 = 0.$$

$$\begin{aligned} 1 = & \left(-\frac{155}{693} + \frac{842}{3465}x_2x_3 - \frac{188}{693}x_2x_4 + \frac{908}{3465}x_3x_4 \right) (x_1^2 - 1) \\ & + \left(-\frac{1}{231} + \frac{842}{1155}x_1x_3 - \frac{188}{231}x_1x_4 + \frac{292}{1155}x_3x_4 \right) (x_2^2 - 1) \\ & + \left(-\frac{467}{693} + \frac{842}{693}x_1x_2 + \frac{908}{693}x_1x_4 + \frac{292}{693}x_2x_4 \right) (x_3^2 - 1) \\ & + \left(-\frac{68}{693} - \frac{376}{693}x_1x_2 + \frac{1816}{3465}x_1x_3 + \frac{584}{3465}x_2x_3 \right) (x_4^2 - 1) \\ & + \left(\frac{155}{693}x_1 + \frac{1}{693}x_2 + \frac{467}{3465}x_3 + \frac{34}{693}x_4 - \frac{842}{3465}x_1x_2x_3 \right. \\ & \left. + \frac{188}{693}x_1x_2x_4 - \frac{908}{3465}x_1x_3x_4 - \frac{292}{3465}x_2x_3x_4 \right) (x_1 + 3x_2 + 5x_3 + 2x_4). \end{aligned}$$

The Partition Matrix: Extract a Square Linear System

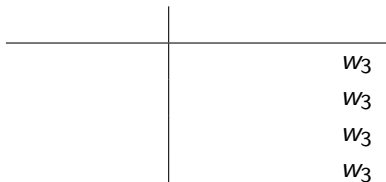
Let $W = \{w_1, w_2, w_3\}$.

$$\begin{bmatrix} w_3 & w_2 & w_1 & 0 \\ w_2 & w_3 & 0 & w_1 \\ w_1 & 0 & w_3 & w_2 \\ 0 & w_1 & w_2 & w_3 \end{bmatrix}$$

The Partition Matrix: Extract a Square Linear System

Let $W = \{w_1, w_2, w_3\}$.

$$\begin{bmatrix} w_3 & w_2 & w_1 & 0 \\ w_2 & w_3 & 0 & w_1 \\ w_1 & 0 & w_3 & w_2 \\ 0 & w_1 & w_2 & w_3 \end{bmatrix}$$



w_3
 w_3
 w_3
 w_3

The Partition Matrix: Extract a Square Linear System

Let $W = \{w_1, w_2, w_3\}$.

$$\begin{bmatrix} w_3 & w_2 & w_1 & 0 \\ w_2 & w_3 & 0 & w_1 \\ w_1 & 0 & w_3 & w_2 \\ 0 & w_1 & w_2 & w_3 \end{bmatrix}$$

	w_1	w_2	w_3
			w_3
			w_3
			w_3

The Partition Matrix: Extract a Square Linear System

Let $W = \{w_1, w_2, w_3\}$.

$$\begin{bmatrix} w_3 & w_2 & w_1 & 0 \\ w_2 & w_3 & 0 & w_1 \\ w_1 & 0 & w_3 & w_2 \\ 0 & w_1 & w_2 & w_3 \end{bmatrix}$$

		w_1	w_2	w_3
			w_2	w_3
				w_3
				w_3
w_1				

The Partition Matrix: Extract a Square Linear System

Let $W = \{w_1, w_2, w_3\}$.

$$\begin{bmatrix} w_3 & w_2 & w_1 & 0 \\ w_2 & w_3 & 0 & w_1 \\ w_1 & 0 & w_3 & w_2 \\ 0 & w_1 & w_2 & w_3 \end{bmatrix}$$

		w_1	w_2	w_3
w_1			w_2	w_3
	w_2	w_1		w_3
				w_3

The Partition Matrix: Extract a Square Linear System

Let $W = \{w_1, w_2, w_3\}$.

$$\begin{bmatrix} w_3 & w_2 & w_1 & 0 \\ w_2 & w_3 & 0 & w_1 \\ w_1 & 0 & w_3 & w_2 \\ 0 & w_1 & w_2 & w_3 \end{bmatrix}$$

		w_1	w_2	w_3
	w_1		w_2	w_3
		w_1		w_3
w_1	w_2			w_3

The Partition Matrix: Extract a Square Linear System

Let $W = \{w_1, w_2, w_3\}$.

$$\begin{bmatrix} w_3 & w_2 & w_1 & 0 \\ w_2 & w_3 & 0 & w_1 \\ w_1 & 0 & w_3 & w_2 \\ 0 & w_1 & w_2 & w_3 \end{bmatrix}$$

-	
	+
	$w_1 + w_2 + w_3$
$- w_1$	$+ w_2 + w_3$
$- w_2$	$+ w_1 + w_3$
$- w_1 - w_2$	$+ w_3$

The Partition Matrix: Extract a Square Linear System

Let $W = \{w_1, w_2, w_3\}$.

$$\begin{bmatrix} w_3 & w_2 & w_1 & 0 \\ w_2 & w_3 & 0 & w_1 \\ w_1 & 0 & w_3 & w_2 \\ 0 & w_1 & w_2 & w_3 \end{bmatrix}$$

	-		+
			$w_1 + w_2 + w_3$
-	w_1		$+ w_2 + w_3$
	$- w_2$		$+ w_1 + w_3$
-	$w_1 - w_2$		$+ w_3$

$$\underbrace{(w_1 + w_2 + w_3)(-w_1 + w_2 + w_3)(w_1 - w_2 + w_3)(-w_1 - w_2 + w_3)}_{\text{partition polynomial}}$$

The Partition Matrix: Extract a Square Linear System

Let $W = \{w_1, w_2, w_3\}$.

$$\begin{bmatrix} w_3 & w_2 & w_1 & 0 \\ w_2 & w_3 & 0 & w_1 \\ w_1 & 0 & w_3 & w_2 \\ 0 & w_1 & w_2 & w_3 \end{bmatrix}$$

	-		+
			$w_1 + w_2 + w_3$
-	w_1		$+ w_2 + w_3$
	$- w_2$		$+ w_1 + w_3$
-	$w_1 - w_2$		$+ w_3$

$$\underbrace{(w_1 + w_2 + w_3)(-w_1 + w_2 + w_3)(w_1 - w_2 + w_3)(-w_1 - w_2 + w_3)}_{\text{partition polynomial}}$$

The Partition Matrix: Extract a Square Linear System

Let $W = \{w_1, w_2, w_3\}$.

$$\begin{bmatrix} w_3 & w_2 & w_1 & 0 \\ w_2 & w_3 & 0 & w_1 \\ w_1 & 0 & w_3 & w_2 \\ 0 & w_1 & w_2 & w_3 \end{bmatrix}$$

	-		+
			$w_1 + w_2 + w_3$
-	w_1		$+ w_2 + w_3$
	$- w_2$		$+ w_1 + w_3$
-	$w_1 - w_2$		$+ w_3$

The **determinant** of the above **partition matrix** is the

$$\underbrace{(w_1 + w_2 + w_3)(-w_1 + w_2 + w_3)(w_1 - w_2 + w_3)(-w_1 - w_2 + w_3)}_{\text{partition polynomial}}$$

Another Example of the Partition Matrix

Let $W = \{w_1, \dots, w_4\}$. The partition matrix P is

$$P = \begin{bmatrix} w_4 & w_3 & w_2 & w_1 & 0 & 0 & 0 & 0 \\ w_3 & w_4 & 0 & 0 & w_2 & w_1 & 0 & 0 \\ w_2 & 0 & w_4 & 0 & w_3 & 0 & w_1 & 0 \\ w_1 & 0 & 0 & w_4 & 0 & w_3 & w_2 & 0 \\ 0 & w_2 & w_3 & 0 & w_4 & 0 & 0 & w_1 \\ 0 & w_1 & 0 & w_3 & 0 & w_4 & 0 & w_2 \\ 0 & 0 & w_1 & w_2 & 0 & 0 & w_4 & w_3 \\ 0 & 0 & 0 & 0 & w_1 & w_2 & w_3 & w_4 \end{bmatrix},$$

Another Example of the Partition Matrix

Let $W = \{w_1, \dots, w_4\}$. The partition matrix P is

$$P = \begin{bmatrix} w_4 & w_3 & w_2 & w_1 & 0 & 0 & 0 & 0 \\ w_3 & w_4 & 0 & 0 & w_2 & w_1 & 0 & 0 \\ w_2 & 0 & w_4 & 0 & w_3 & 0 & w_1 & 0 \\ w_1 & 0 & 0 & w_4 & 0 & w_3 & w_2 & 0 \\ 0 & w_2 & w_3 & 0 & w_4 & 0 & 0 & w_1 \\ 0 & w_1 & 0 & w_3 & 0 & w_4 & 0 & w_2 \\ 0 & 0 & w_1 & w_2 & 0 & 0 & w_4 & w_3 \\ 0 & 0 & 0 & 0 & w_1 & w_2 & w_3 & w_4 \end{bmatrix},$$

$$\begin{aligned} \det(P) &= (w_1 + w_2 + w_3 + w_4)(-w_1 + w_2 + w_3 + w_4)(w_1 - w_2 + w_3 + w_4) \\ &\quad (w_1 + w_2 - w_3 + w_4)(-w_1 + w_2 - w_3 + w_4)(-w_1 - w_2 + w_3 + w_4) \\ &\quad (w_1 - w_2 - w_3 + w_4)(-w_1 - w_2 - w_3 + w_4). \end{aligned}$$

“partition polynomial”

Determinant and Partition Polynomial

Theorem (S.M., S. Onn, 2012)

The determinant of the partition matrix is the partition polynomial.

Hilbert's Nullstellensatz *Numeric* Coefficients and the Partition Polynomial

Given a square non-singular matrix A , Cramer's rule states that $Ax = b$ can be solved according to the formula

$$x_i = \frac{\det(A|_b^i)}{\det(A)},$$

where $A|_b^i$ is the matrix A with the i -th column replaced with the right-hand side vector b .

Recall the non-partitionable $W = \{1, 3, 5, 2\}$:

$$\begin{aligned} 1 = & \left(-\frac{155}{693} + \frac{842}{3465}x_2x_3 - \frac{188}{693}x_2x_4 + \frac{908}{3465}x_3x_4 \right) (x_1^2 - 1) \\ & + \left(-\frac{1}{231} + \frac{842}{1155}x_1x_3 - \frac{188}{231}x_1x_4 + \frac{292}{1155}x_3x_4 \right) (x_2^2 - 1) \\ & + \left(-\frac{467}{693} + \frac{842}{693}x_1x_2 + \frac{908}{693}x_1x_4 + \frac{292}{693}x_2x_4 \right) (x_3^2 - 1) \\ & + \left(-\frac{68}{693} - \frac{376}{693}x_1x_2 + \frac{1816}{3465}x_1x_3 + \frac{584}{3465}x_2x_3 \right) (x_4^2 - 1) \\ & + \left(\frac{155}{693}x_1 + \frac{1}{693}x_2 + \frac{467}{3465}x_3 + \frac{34}{693}x_4 - \frac{842}{3465}x_1x_2x_3 \right. \\ & \left. + \frac{188}{693}x_1x_2x_4 - \frac{908}{3465}x_1x_3x_4 - \frac{292}{3465}x_2x_3x_4 \right) (x_1 + 3x_2 + 5x_3 + 2x_4) . \end{aligned}$$

Recall the non-partitionable $W = \{1, 3, 5, 2\}$:

$$\begin{aligned} 1 = & \left(-\frac{155}{693} + \frac{842}{3465}x_2x_3 - \frac{188}{693}x_2x_4 + \frac{908}{3465}x_3x_4 \right) (x_1^2 - 1) \\ & + \left(-\frac{1}{231} + \frac{842}{1155}x_1x_3 - \frac{188}{231}x_1x_4 + \frac{292}{1155}x_3x_4 \right) (x_2^2 - 1) \\ & + \left(-\frac{467}{693} + \frac{842}{693}x_1x_2 + \frac{908}{693}x_1x_4 + \frac{292}{693}x_2x_4 \right) (x_3^2 - 1) \\ & + \left(-\frac{68}{693} - \frac{376}{693}x_1x_2 + \frac{1816}{3465}x_1x_3 + \frac{584}{3465}x_2x_3 \right) (x_4^2 - 1) \\ & + \left(\frac{155}{693}x_1 + \frac{1}{693}x_2 + \frac{467}{3465}x_3 + \frac{34}{693}x_4 - \frac{842}{3465}x_1x_2x_3 \right. \\ & \left. + \frac{188}{693}x_1x_2x_4 - \frac{908}{3465}x_1x_3x_4 - \frac{292}{3465}x_2x_3x_4 \right) (x_1 + 3x_2 + 5x_3 + 2x_4) . \end{aligned}$$

Recall the non-partitionable $W = \{1, 3, 5, 2\}$:

$$\begin{aligned}
 1 = & \left(-\frac{155}{693} + \frac{842}{3465}x_2x_3 - \frac{188}{693}x_2x_4 + \frac{908}{3465}x_3x_4 \right) (x_1^2 - 1) \\
 & + \left(-\frac{1}{231} + \frac{842}{1155}x_1x_3 - \frac{188}{231}x_1x_4 + \frac{292}{1155}x_3x_4 \right) (x_2^2 - 1) \\
 & + \left(-\frac{467}{693} + \frac{842}{693}x_1x_2 + \frac{908}{693}x_1x_4 + \frac{292}{693}x_2x_4 \right) (x_3^2 - 1) \\
 & + \left(-\frac{68}{693} - \frac{376}{693}x_1x_2 + \frac{1816}{3465}x_1x_3 + \frac{584}{3465}x_2x_3 \right) (x_4^2 - 1) \\
 & + \left(\frac{155}{693}x_1 + \frac{1}{693}x_2 + \frac{467}{3465}x_3 + \frac{34}{693}x_4 - \frac{842}{3465}x_1x_2x_3 \right. \\
 & \left. + \frac{188}{693}x_1x_2x_4 - \frac{908}{3465}x_1x_3x_4 - \frac{292}{3465}x_2x_3x_4 \right) (x_1 + 3x_2 + 5x_3 + 2x_4) . \\
 -51975 = & (1 + 3 + 5 + 2)(-1 + 3 + 5 + 2)(1 - 3 + 5 + 2)(1 + 3 - 5 + 2) \\
 & (-1 - 3 + 5 + 2)(-1 + 3 - 5 + 2)(1 - 3 - 5 + 2)(-1 - 3 - 5 + 2) .
 \end{aligned}$$

Recall the non-partitionable $W = \{1, 3, 5, 2\}$:

$$\begin{aligned}
 1 = & \left(-\frac{155}{693} + \frac{842}{3465}x_2x_3 - \frac{188}{693}x_2x_4 + \frac{908}{3465}x_3x_4 \right) (x_1^2 - 1) \\
 & + \left(-\frac{1}{231} + \frac{842}{1155}x_1x_3 - \frac{188}{231}x_1x_4 + \frac{292}{1155}x_3x_4 \right) (x_2^2 - 1) \\
 & + \left(-\frac{467}{693} + \frac{842}{693}x_1x_2 + \frac{908}{693}x_1x_4 + \frac{292}{693}x_2x_4 \right) (x_3^2 - 1) \\
 & + \left(-\frac{68}{693} - \frac{376}{693}x_1x_2 + \frac{1816}{3465}x_1x_3 + \frac{584}{3465}x_2x_3 \right) (x_4^2 - 1) \\
 & + \left(\frac{155}{693}x_1 + \frac{1}{693}x_2 + \frac{467}{3465}x_3 + \frac{34}{693}x_4 - \frac{842}{3465}x_1x_2x_3 \right. \\
 & \left. + \frac{188}{693}x_1x_2x_4 - \frac{908}{3465}x_1x_3x_4 - \frac{292}{3465}x_2x_3x_4 \right) (x_1 + 3x_2 + 5x_3 + 2x_4) . \\
 -51975 = & (1 + 3 + 5 + 2)(-1 + 3 + 5 + 2)(1 - 3 + 5 + 2)(1 + 3 - 5 + 2) \\
 & (-1 - 3 + 5 + 2)(-1 + 3 - 5 + 2)(1 - 3 - 5 + 2)(-1 - 3 - 5 + 2) .
 \end{aligned}$$

Via Cramer's rule, we see that the unknown b_4 is equal to

$$b_4 = \frac{-2550}{-51975}$$

Recall the non-partitionable $W = \{1, 3, 5, 2\}$:

$$\begin{aligned} 1 &= \left(-\frac{155}{693} + \frac{842}{3465}x_2x_3 - \frac{188}{693}x_2x_4 + \frac{908}{3465}x_3x_4 \right) (x_1^2 - 1) \\ &+ \left(-\frac{1}{231} + \frac{842}{1155}x_1x_3 - \frac{188}{231}x_1x_4 + \frac{292}{1155}x_3x_4 \right) (x_2^2 - 1) \\ &+ \left(-\frac{467}{693} + \frac{842}{693}x_1x_2 + \frac{908}{693}x_1x_4 + \frac{292}{693}x_2x_4 \right) (x_3^2 - 1) \\ &+ \left(-\frac{68}{693} - \frac{376}{693}x_1x_2 + \frac{1816}{3465}x_1x_3 + \frac{584}{3465}x_2x_3 \right) (x_4^2 - 1) \\ &+ \left(\frac{155}{693}x_1 + \frac{1}{693}x_2 + \frac{467}{3465}x_3 + \frac{34}{693}x_4 - \frac{842}{3465}x_1x_2x_3 \right. \\ &\quad \left. + \frac{188}{693}x_1x_2x_4 - \frac{908}{3465}x_1x_3x_4 - \frac{292}{3465}x_2x_3x_4 \right) (x_1 + 3x_2 + 5x_3 + 2x_4) . \\ -51975 &= (1 + 3 + 5 + 2)(-1 + 3 + 5 + 2)(1 - 3 + 5 + 2)(1 + 3 - 5 + 2) \\ &\quad (-1 - 3 + 5 + 2)(-1 + 3 - 5 + 2)(1 - 3 - 5 + 2)(-1 - 3 - 5 + 2) . \end{aligned}$$

Via Cramer's rule, we see that the unknown b_4 is equal to

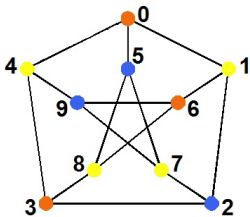
$$b_4 = \frac{-2550}{-51975} = \frac{34}{693} .$$

Definition of Graph Coloring

- **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?

Definition of Graph Coloring

- **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?
- **Petersen Graph: 3-colorable**



Graph- k -Coloring as a System of Polynomial Equations (D. Bayer and De Loera et al.)

- Let \mathbb{K} be a field such that $\text{char}(\mathbb{K})$ is relatively prime to k .

Graph- k -Coloring as a System of Polynomial Equations (D. Bayer and De Loera et al.)

- Let \mathbb{K} be a field such that $\text{char}(\mathbb{K})$ is relatively prime to k .
(3-colorability over \mathbb{F}_2 , 4-colorability over \mathbb{F}_3 , etc.)

Graph- k -Coloring as a System of Polynomial Equations (D. Bayer and De Loera et al.)

- Let \mathbb{K} be a field such that $\text{char}(\mathbb{K})$ is relatively prime to k .
(3-colorability over \mathbb{F}_2 , 4-colorability over \mathbb{F}_3 , etc.)
- one **variable** per **vertex**: x_1, \dots, x_n

Graph- k -Coloring as a System of Polynomial Equations (D. Bayer and De Loera et al.)

- Let \mathbb{K} be a field such that $\text{char}(\mathbb{K})$ is relatively prime to k .
(3-colorability over \mathbb{F}_2 , 4-colorability over \mathbb{F}_3 , etc.)
- one **variable** per **vertex**: x_1, \dots, x_n
- **vertex polynomials**: For every vertex $i = 1, \dots, n$,

$$x_i^k - 1 = 0$$

Graph- k -Coloring as a System of Polynomial Equations (D. Bayer and De Loera et al.)

- Let \mathbb{K} be a field such that $\text{char}(\mathbb{K})$ is relatively prime to k .
(3-colorability over \mathbb{F}_2 , 4-colorability over \mathbb{F}_3 , etc.)
- one **variable** per **vertex**: x_1, \dots, x_n
- **vertex polynomials**: For every vertex $i = 1, \dots, n$,

$$\mathbf{v}_i := x_i^k - 1 = 0$$

Graph- k -Coloring as a System of Polynomial Equations (D. Bayer and De Loera et al.)

- Let \mathbb{K} be a field such that $\text{char}(\mathbb{K})$ is relatively prime to k .
(3-colorability over \mathbb{F}_2 , 4-colorability over \mathbb{F}_3 , etc.)
- one **variable** per **vertex**: x_1, \dots, x_n
- **vertex polynomials**: For every vertex $i = 1, \dots, n$,

$$\mathbf{v}_i := x_i^k - 1 = 0$$

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

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

Graph- k -Coloring as a System of Polynomial Equations (D. Bayer and De Loera et al.)

- Let \mathbb{K} be a field such that $\text{char}(\mathbb{K})$ is relatively prime to k . (3-colorability over \mathbb{F}_2 , 4-colorability over \mathbb{F}_3 , etc.)
- one **variable** per **vertex**: x_1, \dots, x_n
- **vertex polynomials**: For every vertex $i = 1, \dots, n$,

$$\mathbf{v}_i := x_i^k - 1 = 0$$

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

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

Graph- k -Coloring as a System of Polynomial Equations (D. Bayer and De Loera et al.)

- Let \mathbb{K} be a field such that $\text{char}(\mathbb{K})$ is relatively prime to k . (3-colorability over \mathbb{F}_2 , 4-colorability over \mathbb{F}_3 , etc.)
- one **variable** per **vertex**: x_1, \dots, x_n
- **vertex polynomials**: For every vertex $i = 1, \dots, n$,

$$\mathbf{v}_i := x_i^k - 1 = 0$$

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

$$\mathbf{e}_{ij} := \frac{x_i^k - x_j^k}{x_i - x_j} = x_i^{k-1} + x_i^{k-2}x_j + \dots + x_i x_j^{k-2} + x_j^{k-1} = 0$$

Graph- k -Coloring as a System of Polynomial Equations (D. Bayer and De Loera et al.)

- Let \mathbb{K} be a field such that $\text{char}(\mathbb{K})$ is relatively prime to k . (3-colorability over \mathbb{F}_2 , 4-colorability over \mathbb{F}_3 , etc.)
- one **variable** per **vertex**: x_1, \dots, x_n
- **vertex polynomials**: For every vertex $i = 1, \dots, n$,

$$\mathbf{v}_i := x_i^k - 1 = 0$$

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

$$\mathbf{e}_{ij} := \frac{x_i^k - x_j^k}{x_i - x_j} = x_i^{k-1} + x_i^{k-2}x_j + \dots + x_ix_j^{k-2} + x_j^{k-1} = 0$$

- **Theorem**: Let G be a graph encoded as the above $(n + m)$ system of equations over \mathbb{K} . Then this system has a solution over $\overline{\mathbb{K}}$ if and only if G is k -colorable.

Graph- k -Coloring as a System of Polynomial Equations (D. Bayer and De Loera et al.)

- Let \mathbb{K} be a field such that $\text{char}(\mathbb{K})$ is relatively prime to k . (3-colorability over \mathbb{F}_2 , 4-colorability over \mathbb{F}_3 , etc.)
- one **variable** per **vertex**: x_1, \dots, x_n
- **vertex polynomials**: For every vertex $i = 1, \dots, n$,

$$\mathbf{v}_i := x_i^k - 1 = 0$$

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

$$\mathbf{e}_{ij} := \frac{x_i^k - x_j^k}{x_i - x_j} = x_i^{k-1} + x_i^{k-2}x_j + \dots + x_i x_j^{k-2} + x_j^{k-1} = 0$$

- **Theorem**: Let G be a graph encoded as the above $(n + m)$ system of equations over \mathbb{K} . Then this system has a solution over $\overline{\mathbb{K}}$ if and only if G is k -colorable.
- Graph-3-colorability is NP-complete.

Petersen Graph \implies System of Polynomial Equations

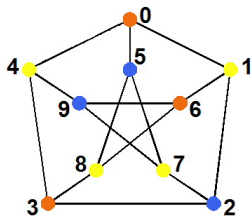


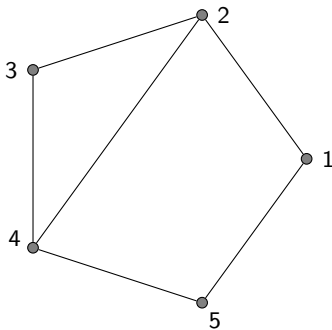
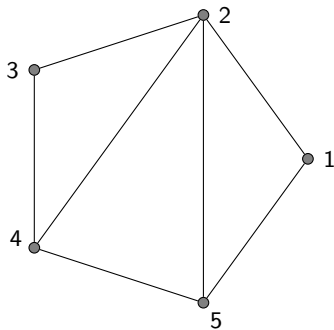
Figure: Is the Petersen graph 3-colorable?

$$\begin{array}{ll} x_0^3 - 1 = 0, x_1^3 - 1 = 0, & x_0^2 + x_0x_1 + x_1^2 = 0, x_0^2 + x_0x_4 + x_4^2 = 0 \\ x_2^3 - 1 = 0, x_3^3 - 1 = 0, & x_0^2 + x_0x_5 + x_5^2 = 0, x_1^2 + x_1x_2 + x_2^2 = 0 \\ x_4^3 - 1 = 0, x_5^3 - 1 = 0, & x_1^2 + x_1x_6 + x_6^2 = 0, x_2^2 + x_2x_3 + x_3^2 = 0 \\ x_6^3 - 1 = 0, x_7^3 - 1 = 0, & \dots\dots\dots \quad \dots\dots\dots \\ x_8^3 - 1 = 0, x_9^3 - 1 = 0, & x_6^2 + x_6x_8 + x_8^2 = 0, x_7^2 + x_7x_9 + x_9^2 = 0 \end{array}$$

Chordal Graphs and Gröbner Bases

Definition

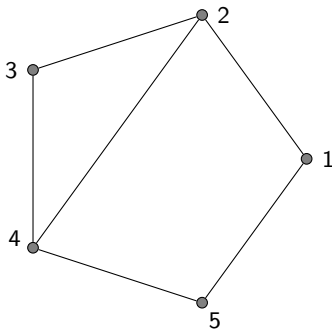
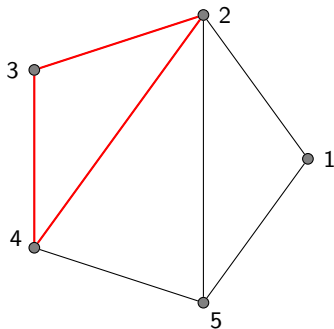
A graph G is *chordal* if every cycle of length *greater* than three has a chord, i.e., every induced cycle has length at most 3.



Chordal Graphs and Gröbner Bases

Definition

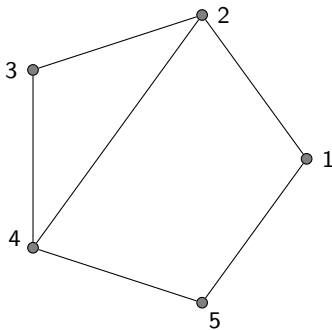
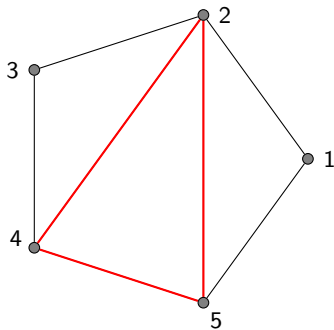
A graph G is *chordal* if every cycle of length *greater* than three has a chord, i.e., every induced cycle has length at most 3.



Chordal Graphs and Gröbner Bases

Definition

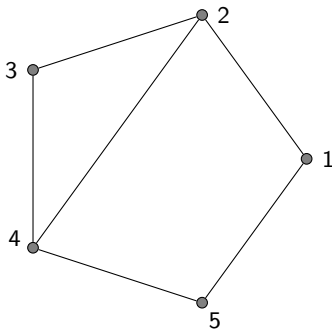
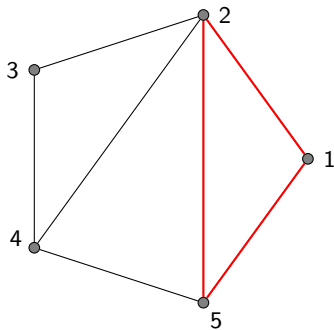
A graph G is *chordal* if every cycle of length *greater* than three has a chord, i.e., every induced cycle has length at most 3.



Chordal Graphs and Gröbner Bases

Definition

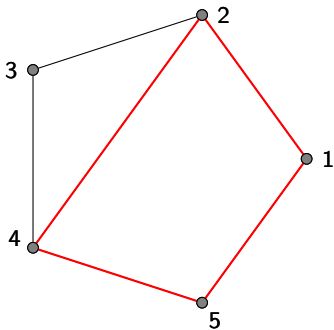
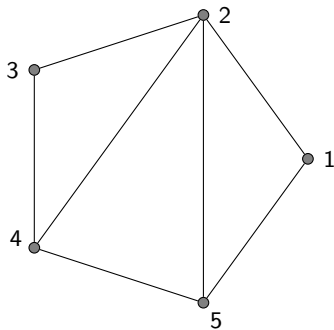
A graph G is *chordal* if every cycle of length *greater* than three has a chord, i.e., every induced cycle has length at most 3.



Chordal Graphs and Gröbner Bases

Definition

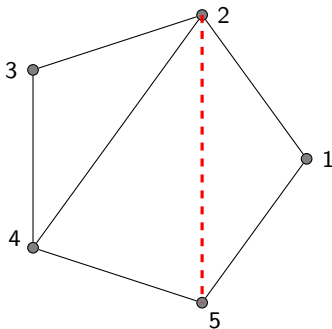
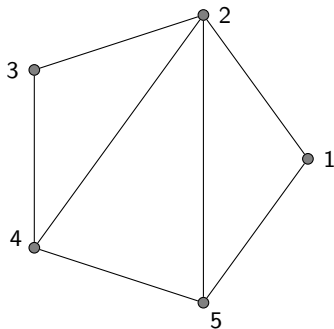
A graph G is *chordal* if every cycle of length *greater* than three has a chord, i.e., every induced cycle has length at most 3.



Chordal Graphs and Gröbner Bases

Definition

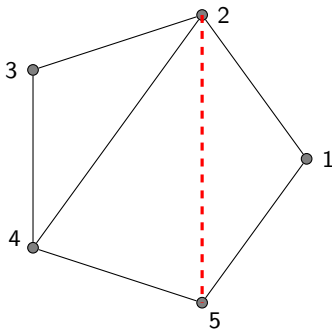
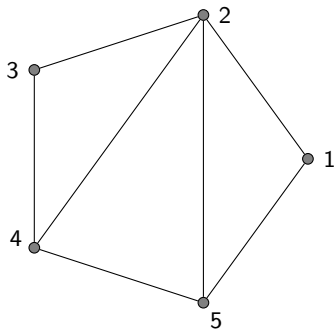
A graph G is *chordal* if every cycle of length *greater* than three has a chord, i.e., every induced cycle has length at most 3.



Chordal Graphs and Gröbner Bases

Definition

A graph G is *chordal* if every cycle of length *greater* than three has a chord, i.e., every induced cycle has length at most 3.



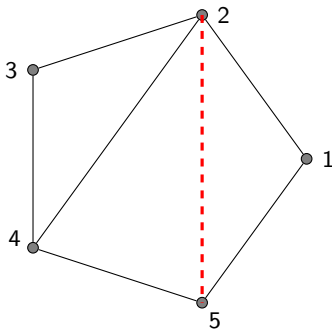
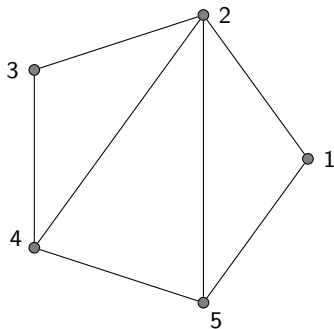
Theorem (2015, J.A. De Loera, M., M. Pernpeintner, E. Riedl, D. Rolnick, G. Spencer, D. Stasi, J. Swenson)

Let G be a chordal graph on n vertices. Then there exists a polynomial-time computable Gröbner basis for the k -coloring ideal.

Chordal Graphs and Gröbner Bases

Definition

A graph G is *chordal* if every cycle of length *greater* than three has a chord, i.e., every induced cycle has length at most 3.



Theorem (2015, J.A. De Loera, M., M. Pernpeintner, E. Riedl, D. Rolnick, G. Spencer, D. Stasi, J. Swenson (MRC: Snowbird, Utah))

Let G be a chordal graph on n vertices. Then there exists a polynomial-time computable Gröbner basis for the k -coloring ideal.

Gröbner Bases and Chordal Graphs: A Visual Proof

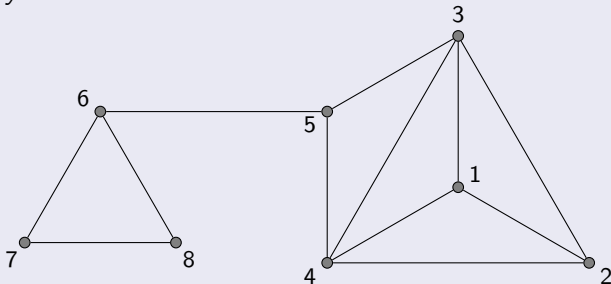
Let $S_r(x_1, \dots, x_n) := \sum_{1 \leq j_1 \leq \dots \leq j_r \leq n} x_{j_1} \cdots x_{j_r}$.

Gröbner Bases and Chordal Graphs: A Visual Proof

Let $S_r(x_1, \dots, x_n) := \sum_{1 \leq j_1 \leq \dots \leq j_r \leq n} x_{j_1} \cdots x_{j_r}$.

Lemma

Every chordal graph (and corresponding Gröbner basis) can be iteratively constructed:



Gröbner Bases and Chordal Graphs: A Visual Proof

Let $S_r(x_1, \dots, x_n) := \sum_{1 \leq j_1 \leq \dots \leq j_r \leq n} x_{j_1} \cdots x_{j_r}$.

Lemma

Every chordal graph (and corresponding Gröbner basis) can be iteratively constructed:

• 1

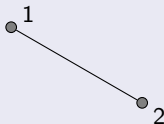
Gröbner basis = $\{v_1\}$

Gröbner Bases and Chordal Graphs: A Visual Proof

Let $S_r(x_1, \dots, x_n) := \sum_{1 \leq j_1 \leq \dots \leq j_r \leq n} x_{j_1} \cdots x_{j_r}$.

Lemma

Every chordal graph (and corresponding Gröbner basis) can be iteratively constructed:



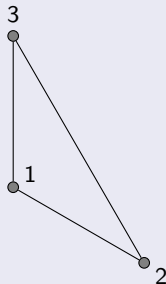
Gröbner basis = $\{v_1, S_3(x_1, x_2)\}$

Gröbner Bases and Chordal Graphs: A Visual Proof

Let $S_r(x_1, \dots, x_n) := \sum_{1 \leq j_1 \leq \dots \leq j_r \leq n} x_{j_1} \cdots x_{j_r}$.

Lemma

Every chordal graph (and corresponding Gröbner basis) can be iteratively constructed:



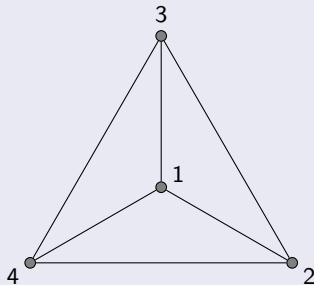
Gröbner basis = $\{v_1, S_3(x_1, x_2), S_2(x_1, x_2, x_3)\}$

Gröbner Bases and Chordal Graphs: A Visual Proof

Let $S_r(x_1, \dots, x_n) := \sum_{1 \leq j_1 \leq \dots \leq j_r \leq n} x_{j_1} \cdots x_{j_r}$.

Lemma

Every chordal graph (and corresponding Gröbner basis) can be iteratively constructed:



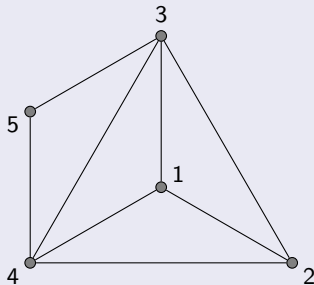
Gröbner basis = $\{v_1, S_3(x_1, x_2), S_2(x_1, x_2, x_3), S_1(x_1, x_2, x_3, x_4)\}$

Gröbner Bases and Chordal Graphs: A Visual Proof

Let $S_r(x_1, \dots, x_n) := \sum_{1 \leq j_1 \leq \dots \leq j_r \leq n} x_{j_1} \cdots x_{j_r}$.

Lemma

Every chordal graph (and corresponding Gröbner basis) can be iteratively constructed:



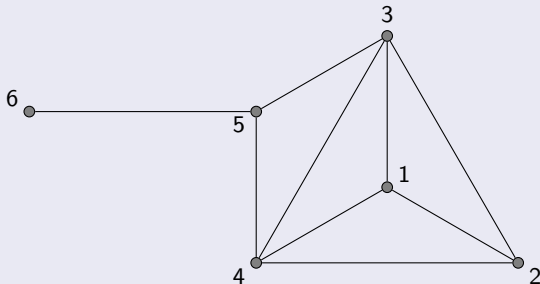
Gröbner basis = $\{v_1, S_3(x_1, x_2), S_2(x_1, x_2, x_3), S_1(x_1, x_2, x_3, x_4), S_2(x_3, x_4, x_5)\}$

Gröbner Bases and Chordal Graphs: A Visual Proof

Let $S_r(x_1, \dots, x_n) := \sum_{1 \leq j_1 \leq \dots \leq j_r \leq n} x_{j_1} \cdots x_{j_r}$.

Lemma

Every chordal graph (and corresponding Gröbner basis) can be iteratively constructed:



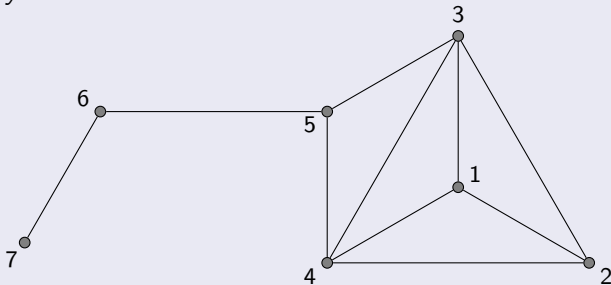
Gröbner basis = $\{v_1, S_3(x_1, x_2), S_2(x_1, x_2, x_3), S_1(x_1, x_2, x_3, x_4), S_2(x_3, x_4, x_5), S_3(x_5, x_6)\}$

Gröbner Bases and Chordal Graphs: A Visual Proof

Let $S_r(x_1, \dots, x_n) := \sum_{1 \leq j_1 \leq \dots \leq j_r \leq n} x_{j_1} \cdots x_{j_r}$.

Lemma

Every chordal graph (and corresponding Gröbner basis) can be iteratively constructed:



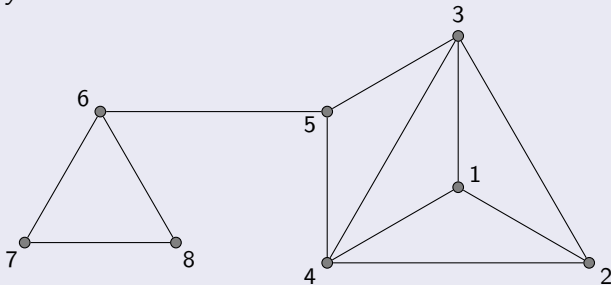
Gröbner basis = $\{v_1, S_3(x_1, x_2), S_2(x_1, x_2, x_3), S_1(x_1, x_2, x_3, x_4), S_2(x_3, x_4, x_5), S_3(x_5, x_6), S_3(x_6, x_7)\}$

Gröbner Bases and Chordal Graphs: A Visual Proof

Let $S_r(x_1, \dots, x_n) := \sum_{1 \leq j_1 \leq \dots \leq j_r \leq n} x_{j_1} \cdots x_{j_r}$.

Lemma

Every chordal graph (and corresponding Gröbner basis) can be iteratively constructed:



Gröbner basis = $\{v_1, S_3(x_1, x_2), S_2(x_1, x_2, x_3), S_1(x_1, x_2, x_3, x_4), S_2(x_3, x_4, x_5), S_3(x_5, x_6), S_3(x_6, x_7), S_2(x_6, x_7, x_8)\}$

Nullstellensatz Certificates of Non-3-colorability

Theorem (S.M., 2008)

The minimum-degree certificate for non-3-colorability grows as 1, 4, 7, 10,

Nullstellensatz Certificates of Non-3-colorability

Theorem (S.M., 2008)

The minimum-degree certificate for non-3-colorability grows as 1, 4, 7, 10,

- **Degree One Certificates:**

Theorem (S.M., 2008)

The minimum-degree certificate for non-3-colorability grows as 1, 4, 7, 10,

- **Degree One Certificates:**

- *Directed Edge Cover* interpretation (De Loera, Hillar, Malkin, Omar, “Recognizing Graph Theoretic Properties with Polynomial Ideals”, **2010**)

Theorem (S.M., 2008)

The minimum-degree certificate for non-3-colorability grows as 1, 4, 7, 10,

- **Degree One Certificates:**

- *Directed Edge Cover* interpretation (De Loera, Hillar, Malkin, Omar, “Recognizing Graph Theoretic Properties with Polynomial Ideals”, **2010**)
- *2-path cover* interpretation, (Li, Lowenstein, Omar, “Low degree Nullstellensatz certificates for 3-colorability”, **2015**)

Nullstellensatz Certificates of Non-3-colorability

Theorem (S.M., 2008)

The minimum-degree certificate for non-3-colorability grows as 1, 4, 7, 10,

- **Degree One Certificates:**

- *Directed Edge Cover* interpretation (De Loera, Hillar, Malkin, Omar, “Recognizing Graph Theoretic Properties with Polynomial Ideals”, **2010**)
- *2-path cover* interpretation, (Li, Lowenstein, Omar, “Low degree Nullstellensatz certificates for 3-colorability”, **2015**)

- **Degree Four Certificates:**

Nullstellensatz Certificates of Non-3-colorability

Theorem (S.M., 2008)

The minimum-degree certificate for non-3-colorability grows as 1, 4, 7, 10,

- **Degree One Certificates:**

- *Directed Edge Cover* interpretation (De Loera, Hillar, Malkin, Omar, “Recognizing Graph Theoretic Properties with Polynomial Ideals”, **2010**)
- *2-path cover* interpretation, (Li, Lowenstein, Omar, “Low degree Nullstellensatz certificates for 3-colorability”, **2015**)

- **Degree Four Certificates:** Open Question!!

Nullstellensatz Certificates of Non-3-colorability

Theorem (S.M., 2008)

The minimum-degree certificate for non-3-colorability grows as 1, 4, 7, 10,

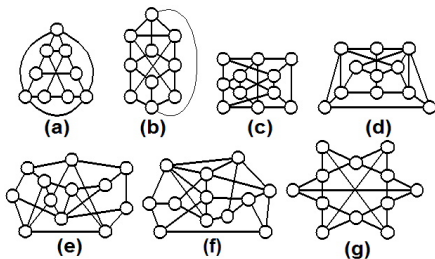
- **Conjecture:** The Mishihara-Nizuno infinite family of graphs follows this pattern.

Nullstellensatz Certificates of Non-3-colorability

Theorem (S.M., 2008)

The minimum-degree certificate for non-3-colorability grows as 1, 4, 7, 10, . . .

- **Conjecture:** The Mishihara-Nizuno infinite family of graphs follows this pattern.

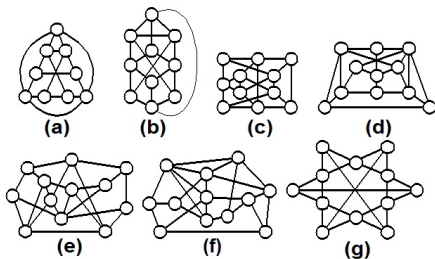


Nullstellensatz Certificates of Non-3-colorability

Theorem (S.M., 2008)

The minimum-degree certificate for non-3-colorability grows as 1, 4, 7, 10,

- Conjecture:** The Mishihara-Nizuno infinite family of graphs follows this pattern.



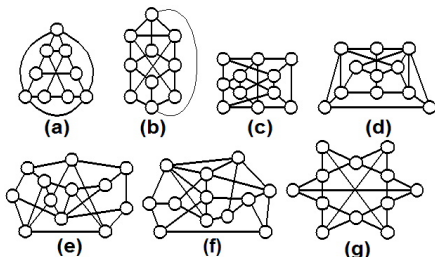
G	n	m	deg	G	n	m	deg	G	n	m	deg
G_0	10	18		G_2	30	55		G_4	49	90	
G_1	20	37		G_3	39	72					

Nullstellensatz Certificates of Non-3-colorability

Theorem (S.M., 2008)

The minimum-degree certificate for non-3-colorability grows as 1, 4, 7, 10, . . .

- Conjecture:** The Mishihara-Nizuno infinite family of graphs follows this pattern.



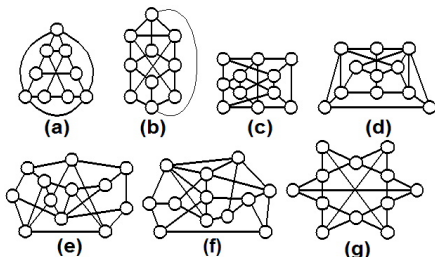
G	n	m	deg	G	n	m	deg	G	n	m	deg
G_0	10	18	1	G_2	30	55		G_4	49	90	
G_1	20	37		G_3	39	72					

Nullstellensatz Certificates of Non-3-colorability

Theorem (S.M., 2008)

The minimum-degree certificate for non-3-colorability grows as 1, 4, 7, 10, . . .

- Conjecture:** The Mishihara-Nizuno infinite family of graphs follows this pattern.



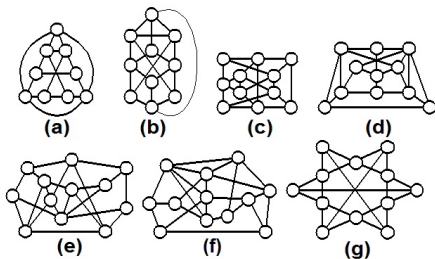
G	n	m	deg	G	n	m	deg	G	n	m	deg
G_0	10	18	1	G_2	30	55	4	G_4	49	90	
G_1	20	37	4	G_3	39	72	4				

Nullstellensatz Certificates of Non-3-colorability

Theorem (S.M., 2008)

The minimum-degree certificate for non-3-colorability grows as 1, 4, 7, 10, . . .

- Conjecture:** The Mishihara-Nizuno infinite family of graphs follows this pattern.



G	n	m	deg	G	n	m	deg	G	n	m	deg
G_0	10	18	1	G_2	30	55	4	G_4	49	90	≥ 7
G_1	20	37	4	G_3	39	72	4				

Nullstellensatz Certificates for Problems in P

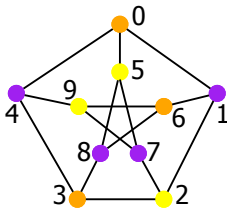
Question

Given a combinatorial problem in P, does there **exist** an encoding such that the Nullstellensatz certificates have polynomial size?

Question

Given a combinatorial problem in P, does there **exist** an encoding such that the Nullstellensatz certificates have polynomial size?

- **Petersen Graph: 3-colorable**

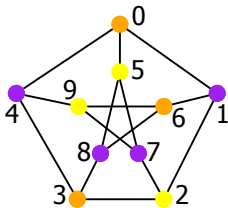


Nullstellensatz Certificates for Problems in P

Question

Given a combinatorial problem in P, does there **exist** an encoding such that the Nullstellensatz certificates have polynomial size?

- **Petersen Graph: 3-colorable, not-2-colorable**

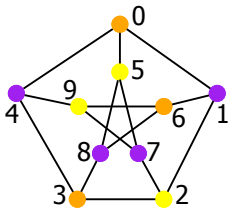


Nullstellensatz Certificates for Problems in P

Question

Given a combinatorial problem in P, does there **exist** an encoding such that the Nullstellensatz certificates have polynomial size?

- **Petersen Graph: 3-colorable, not-2-colorable**



Fact

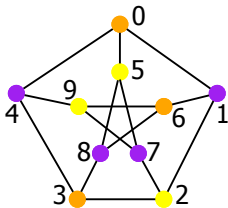
A graph G is not-2-colorable
 $\iff G$ contains an odd cycle.

Nullstellensatz Certificates for Problems in P

Question

Given a combinatorial problem in P, does there **exist** an encoding such that the Nullstellensatz certificates have polynomial size?

- **Petersen Graph: 3-colorable, not-2-colorable**



Fact

A graph G is not-2-colorable
 $\iff G$ contains an odd cycle.

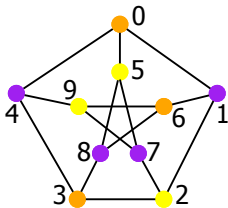
- $(x_i^2 - 1) = 0, \forall i \in V(G)$ and $(x_i + x_j) = 0, \forall (i, j) \in E(G)$ (\mathbb{C})

Nullstellensatz Certificates for Problems in P

Question

Given a combinatorial problem in P, does there **exist** an encoding such that the Nullstellensatz certificates have polynomial size?

- **Petersen Graph: 3-colorable, not-2-colorable**



Fact

A graph G is not-2-colorable
 $\iff G$ contains an odd cycle.

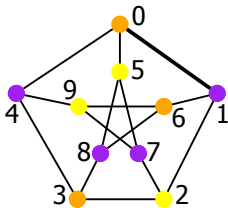
- $(x_i^2 - 1) = 0, \forall i \in V(G)$ and $(x_i + x_j) = 0, \forall (i, j) \in E(G)$ (\mathbb{C})
 $-(x_0^2 - 1)$

Nullstellensatz Certificates for Problems in P

Question

Given a combinatorial problem in P, does there **exist** an encoding such that the Nullstellensatz certificates have polynomial size?

- **Petersen Graph: 3-colorable, not-2-colorable**



Fact

A graph G is not-2-colorable
 $\iff G$ contains an odd cycle.

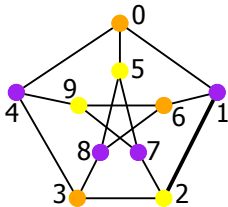
- $(x_i^2 - 1) = 0, \forall i \in V(G)$ and $(x_i + x_j) = 0, \forall (i,j) \in E(G) (\mathbb{C})$
 $-(x_0^2 - 1) + \frac{1}{2}x_0(x_0 + x_1)$

Nullstellensatz Certificates for Problems in P

Question

Given a combinatorial problem in P, does there **exist** an encoding such that the Nullstellensatz certificates have polynomial size?

- **Petersen Graph: 3-colorable, not-2-colorable**



Fact

A graph G is not-2-colorable
 $\iff G$ contains an odd cycle.

- $(x_i^2 - 1) = 0, \forall i \in V(G)$ and $(x_i + x_j) = 0, \forall (i, j) \in E(G) (\mathbb{C})$

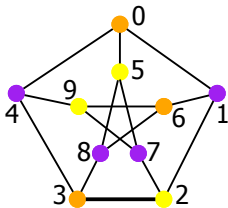
$$-(x_0^2 - 1) + \frac{1}{2}x_0(x_0 + x_1) - \frac{1}{2}x_0(x_1 + x_2)$$

Nullstellensatz Certificates for Problems in P

Question

Given a combinatorial problem in P, does there **exist** an encoding such that the Nullstellensatz certificates have polynomial size?

- **Petersen Graph: 3-colorable, not-2-colorable**



Fact

A graph G is not-2-colorable
 $\iff G$ contains an odd cycle.

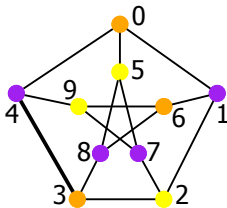
- $(x_i^2 - 1) = 0, \forall i \in V(G)$ and $(x_i + x_j) = 0, \forall (i, j) \in E(G) (\mathbb{C})$
$$-(x_0^2 - 1) + \frac{1}{2}x_0(x_0 + x_1) - \frac{1}{2}x_0(x_1 + x_2) + \frac{1}{2}x_0(x_2 + x_3)$$

Nullstellensatz Certificates for Problems in P

Question

Given a combinatorial problem in P, does there **exist** an encoding such that the Nullstellensatz certificates have polynomial size?

- **Petersen Graph: 3-colorable, not-2-colorable**



Fact

A graph G is not-2-colorable
 $\iff G$ contains an odd cycle.

- $(x_i^2 - 1) = 0, \forall i \in V(G)$ and $(x_i + x_j) = 0, \forall (i, j) \in E(G) (\mathbb{C})$

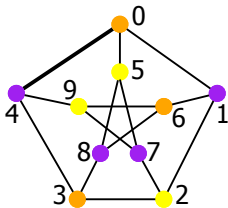
$$\begin{aligned} & - (x_0^2 - 1) + \frac{1}{2}x_0(x_0 + x_1) - \frac{1}{2}x_0(x_1 + x_2) + \frac{1}{2}x_0(x_2 + x_3) \\ & \quad - \frac{1}{2}x_0(x_3 + x_4) \end{aligned}$$

Nullstellensatz Certificates for Problems in P

Question

Given a combinatorial problem in P, does there **exist** an encoding such that the Nullstellensatz certificates have polynomial size?

- **Petersen Graph: 3-colorable, not-2-colorable**



Fact

A graph G is not-2-colorable
 $\iff G$ contains an odd cycle.

- $(x_i^2 - 1) = 0, \forall i \in V(G)$ and $(x_i + x_j) = 0, \forall (i, j) \in E(G) (\mathbb{C})$

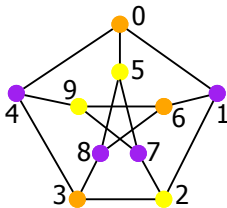
$$\begin{aligned} & - (x_0^2 - 1) + \frac{1}{2}x_0(x_0 + x_1) - \frac{1}{2}x_0(x_1 + x_2) + \frac{1}{2}x_0(x_2 + x_3) \\ & \quad - \frac{1}{2}x_0(x_3 + x_4) + \frac{1}{2}x_0(x_4 + x_0) \end{aligned}$$

Nullstellensatz Certificates for Problems in P

Question

Given a combinatorial problem in P, does there **exist** an encoding such that the Nullstellensatz certificates have polynomial size?

- **Petersen Graph: 3-colorable, not-2-colorable**



Fact

A graph G is not-2-colorable
 $\iff G$ contains an odd cycle.

- $(x_i^2 - 1) = 0, \forall i \in V(G)$ and $(x_i + x_j) = 0, \forall (i, j) \in E(G)$ (\mathbb{C})

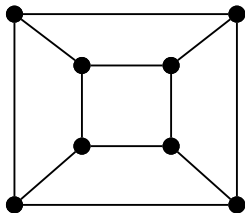
$$1 = - (x_0^2 - 1) + \frac{1}{2}x_0(x_0 + x_1) - \frac{1}{2}x_0(x_1 + x_2) + \frac{1}{2}x_0(x_2 + x_3) \\ - \frac{1}{2}x_0(x_3 + x_4) + \frac{1}{2}x_0(x_4 + x_0)$$

Perfect Matching: Definition and Example

- **Perfect Matching:** A graph G has a perfect matching if there **exists** a set of **matched** edges such that every vertex is incident on a **matched** edge.

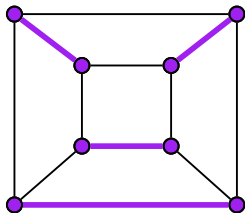
Perfect Matching: Definition and Example

- **Perfect Matching:** A graph G has a perfect matching if there **exists** a set of **matched** edges such that every vertex is incident on a **matched** edge.
- **Example:** Does this graph have a perfect matching?



Perfect Matching: Definition and Example

- **Perfect Matching:** A graph G has a perfect matching if there **exists** a set of **matched** edges such that every vertex is incident on a **matched** edge.
- **Example:** Does this graph have a perfect matching? **Yes!**



Perfect Matching as a System of Polynomial Equations

- **Proposition:** A graph G has a perfect matching if and only if the following system of polynomial equations over \mathbb{C} has a solution.

$$\sum_{j \in N(i)} x_{ij} + 1 = 0 \quad \forall i \in V(G)$$

Perfect Matching as a System of Polynomial Equations

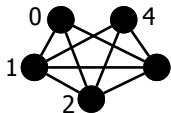
- **Proposition:** A graph G has a perfect matching if and only if the following system of polynomial equations over \mathbb{C} has a solution.

$$\sum_{j \in N(i)} x_{ij} + 1 = 0, \quad x_{ij}x_{ik} = 0 \quad \forall i \in V(G), \forall j, k \in N(i)$$

Perfect Matching as a System of Polynomial Equations

- **Proposition:** A graph G has a perfect matching if and only if the following system of polynomial equations over \mathbb{C} has a solution.

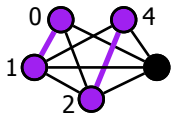
$$\sum_{j \in N(i)} x_{ij} + 1 = 0, \quad x_{ij}x_{ik} = 0 \quad \forall i \in V(G), \forall j, k \in N(i)$$



Perfect Matching as a System of Polynomial Equations

- **Proposition:** A graph G has a perfect matching if and only if the following system of polynomial equations over \mathbb{C} has a solution.

$$\sum_{j \in N(i)} x_{ij} + 1 = 0, \quad x_{ij}x_{ik} = 0 \quad \forall i \in V(G), \forall j, k \in N(i)$$

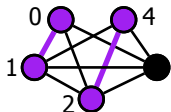


Perfect Matching as a System of Polynomial Equations

- Proposition:** A graph G has a perfect matching if and only if the following system of polynomial equations over \mathbb{C} has a solution.

$$\sum_{j \in N(i)} x_{ij} + 1 = 0, \quad x_{ij}x_{ik} = 0 \quad \forall i \in V(G), \forall j, k \in N(i)$$

$$\begin{aligned} 1 = & \left(-\frac{2}{5}x_{12} - \frac{2}{5}x_{13} - \frac{2}{5}x_{14} - \frac{2}{5}x_{23} - \frac{2}{5}x_{24} - \frac{2}{5}x_{34} - \frac{1}{5}\right)(-1 + x_{01} + x_{02} + x_{03}) \\ & + \left(-\frac{4}{5}x_{02} - \frac{4}{5}x_{03} + 2x_{23} - \frac{1}{5}\right)(-1 + x_{01} + x_{12} + x_{13} + x_{14}) \\ & + \left(-\frac{4}{5}x_{01} - \frac{4}{5}x_{03} + 2x_{13} - \frac{1}{5}\right)(-1 + x_{02} + x_{12} + x_{23} + x_{24}) \\ & + \left(-\frac{4}{5}x_{01} - \frac{4}{5}x_{02} + 2x_{12} - \frac{1}{5}\right)(-1 + x_{03} + x_{13} + x_{23} + x_{34}) \\ & + \left(\frac{6}{5}x_{01} + \frac{6}{5}x_{02} + \frac{6}{5}x_{03} - 2x_{12} - 2x_{13} - 2x_{23} - \frac{1}{5}\right)(-1 + x_{14} + x_{24} + x_{34}) \\ & + \frac{8}{5}x_{01}x_{02} + \frac{8}{5}x_{01}x_{03} + \frac{6}{5}x_{01}x_{12} + \frac{6}{5}x_{01}x_{13} - \frac{4}{5}x_{01}x_{14} + \frac{8}{5}x_{02}x_{03} + \frac{6}{5}x_{02}x_{12} \\ & + \frac{6}{5}x_{03}x_{13} + \frac{6}{5}x_{03}x_{23} - \frac{4}{5}x_{03}x_{34} - 4x_{12}x_{13} + 2x_{12}x_{14} - 4x_{12}x_{23} + 2x_{13}x_{14} - \\ & + 2x_{23}x_{24} + 2x_{23}x_{34} + 2x_{12}x_{24}; \end{aligned}$$

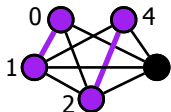


Perfect Matching as a System of Polynomial Equations

- Proposition:** A graph G has a perfect matching if and only if the following system of polynomial equations over \mathbb{F}_2 has a solution.

$$\sum_{j \in N(i)} x_{ij} + 1 = 0, \quad x_{ij}x_{ik} = 0 \quad \forall i \in V(G), \forall j, k \in N(i)$$

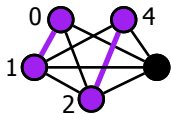
$$\begin{aligned} 1 = & \left(-\frac{2}{5}x_{12} - \frac{2}{5}x_{13} - \frac{2}{5}x_{14} - \frac{2}{5}x_{23} - \frac{2}{5}x_{24} - \frac{2}{5}x_{34} - \frac{1}{5}\right)(-1 + x_{01} + x_{02} + x_{03}) \\ & + \left(-\frac{4}{5}x_{02} - \frac{4}{5}x_{03} + 2x_{23} - \frac{1}{5}\right)(-1 + x_{01} + x_{12} + x_{13} + x_{14}) \\ & + \left(-\frac{4}{5}x_{01} - \frac{4}{5}x_{03} + 2x_{13} - \frac{1}{5}\right)(-1 + x_{02} + x_{12} + x_{23} + x_{24}) \\ & + \left(-\frac{4}{5}x_{01} - \frac{4}{5}x_{02} + 2x_{12} - \frac{1}{5}\right)(-1 + x_{03} + x_{13} + x_{23} + x_{34}) \\ & + \left(\frac{6}{5}x_{01} + \frac{6}{5}x_{02} + \frac{6}{5}x_{03} - 2x_{12} - 2x_{13} - 2x_{23} - \frac{1}{5}\right)(-1 + x_{14} + x_{24} + x_{34}) \\ & + \frac{8}{5}x_{01}x_{02} + \frac{8}{5}x_{01}x_{03} + \frac{6}{5}x_{01}x_{12} + \frac{6}{5}x_{01}x_{13} - \frac{4}{5}x_{01}x_{14} + \frac{8}{5}x_{02}x_{03} + \frac{6}{5}x_{02}x_{12} \\ & + \frac{6}{5}x_{03}x_{13} + \frac{6}{5}x_{03}x_{23} - \frac{4}{5}x_{03}x_{34} - 4x_{12}x_{13} + 2x_{12}x_{14} - 4x_{12}x_{23} + 2x_{13}x_{14} - \\ & + 2x_{23}x_{24} + 2x_{23}x_{34} + 2x_{12}x_{24}; \end{aligned}$$



Perfect Matching as a System of Polynomial Equations

- Proposition:** A graph G has a perfect matching if and only if the following system of polynomial equations over \mathbb{F}_2 has a solution.

$$\sum_{j \in N(i)} x_{ij} + 1 = 0, \quad x_{ij}x_{ik} = 0 \quad \forall i \in V(G), \forall j, k \in N(i)$$

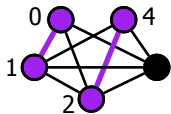


$$\begin{aligned} 1 &= (x_{01} + x_{02} + x_{03} + 1) + (x_{01} + x_{12} + x_{13} + 1) \\ &\quad + (x_{02} + x_{12} + x_{23} + x_{24} + 1) \\ &\quad + (x_{03} + x_{13} + x_{23} + x_{34} + 1) \\ &\quad + (x_{24} + x_{34} + 1) \pmod 2 \end{aligned}$$

Perfect Matching as a System of Polynomial Equations

- **Proposition:** A graph G has a perfect matching if and only if the following system of polynomial equations over \mathbb{F}_2 has a solution.

$$\sum_{j \in N(i)} x_{ij} + 1 = 0, \quad x_{ij}x_{ik} = 0 \quad \forall i \in V(G), \forall j, k \in N(i)$$



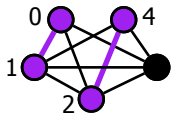
$$\begin{aligned} 1 &= (x_{01} + x_{02} + x_{03} + 1) + (x_{01} + x_{12} + x_{13} + 1) \\ &\quad + (x_{02} + x_{12} + x_{23} + x_{24} + 1) \\ &\quad + (x_{03} + x_{13} + x_{23} + x_{34} + 1) \\ &\quad + (x_{24} + x_{34} + 1) \pmod 2 \end{aligned}$$

- **Theorem:** If a graph G has an odd number of vertices, there exists a **degree zero** Nullstellensatz certificate.

Perfect Matching as a System of Polynomial Equations

- **Proposition:** A graph G has a perfect matching if and only if the following system of polynomial equations over \mathbb{F}_2 has a solution.

$$\sum_{j \in N(i)} x_{ij} + 1 = 0, \quad x_{ij}x_{ik} = 0 \quad \forall i \in V(G), \forall j, k \in N(i)$$



$$\begin{aligned} 1 &= (x_{01} + x_{02} + x_{03} + 1) + (x_{01} + x_{12} + x_{13} + 1) \\ &\quad + (x_{02} + x_{12} + x_{23} + x_{24} + 1) \\ &\quad + (x_{03} + x_{13} + x_{23} + x_{34} + 1) \\ &\quad + (x_{24} + x_{34} + 1) \pmod 2 \end{aligned}$$

- **Theorem:** If a graph G has an odd number of vertices, there exists a **degree zero** Nullstellensatz certificate.
- **Question:** What about graphs with an even number of vertices?

The Degree Grows!

Theorem (Tutte, 1947)

*A graph, $G = (V, E)$, has a perfect matching if and only if for every subset U of $V[G]$, the subgraph induced by $V \setminus U$ has at most $|U|$ connected components with an **odd** number of vertices.*

The Degree Grows!

Theorem (Tutte, 1947)

*A graph, $G = (V, E)$, has a perfect matching if and only if for every subset U of $V[G]$, the subgraph induced by $V \setminus U$ has at most $|U|$ connected components with an **odd** number of vertices.*

- Construct an infinite family of graphs with $|V[G]|$ even based on Tutte's theorem.

The Degree Grows!

Theorem (Tutte, 1947)

*A graph, $G = (V, E)$, has a perfect matching if and only if for every subset U of $V[G]$, the subgraph induced by $V \setminus U$ has at most $|U|$ connected components with an **odd** number of vertices.*

- Construct an infinite family of graphs with $|V[G]|$ even based on Tutte's theorem.
- Run experiments and record the degree.

The Degree Grows!

Theorem (Tutte, 1947)

*A graph, $G = (V, E)$, has a perfect matching if and only if for every subset U of $V[G]$, the subgraph induced by $V \setminus U$ has at most $|U|$ connected components with an **odd** number of vertices.*

- Construct an infinite family of graphs with $|V[G]|$ even based on Tutte's theorem.
- Run experiments and record the degree.

name	$ V $	$ E $	deg
1,1	4	3	1
2,1	6	9	1
3,1	8	18	2
4,1	10	30	2
5,1	12	45	3
6,1	14	63	3
7,1	16	84	≥ 4

- 1 J. A. De Loera, J. Lee, S. Margulies, S. Onn. *Expressing Combinatorial Optimization Problems by Systems of Polynomial Equations and Hilbert's Nullstellensatz*, *Combinatorics, Probability and Computing*, 18(4), pp. 551-582, 2009.
- 2 S. Margulies, S. Onn, D.V. Pasechnik, *On the Complexity of Hilbert Refutations for Partition*, *Journal of Symbolic Computation*, 66, 70–83, February 2015.
- 3 J.A. De Loera, S. Margulies, M. Pernpeintner, E. Riedl, D. Rolnick, G. Spencer, D. Stasi, J. Swenson *Graph-Coloring Ideals: Nullstellensatz Certificates, Gröbner Bases for Chordal Graphs, and Hardness of Gröbner Bases*, *Interntl. Symposium on Symbolic and Algebraic Computation (ISSAC 2015)*.

- 1 J. A. De Loera, J. Lee, S. Margulies, S. Onn. *Expressing Combinatorial Optimization Problems by Systems of Polynomial Equations and Hilbert's Nullstellensatz*, *Combinatorics, Probability and Computing*, 18(4), pp. 551-582, 2009.
- 2 S. Margulies, S. Onn, D.V. Pasechnik, *On the Complexity of Hilbert Refutations for Partition*, *Journal of Symbolic Computation*, 66, 70–83, February 2015.
- 3 J.A. De Loera, S. Margulies, M. Pernpeintner, E. Riedl, D. Rolnick, G. Spencer, D. Stasi, J. Swenson *Graph-Coloring Ideals: Nullstellensatz Certificates, Gröbner Bases for Chordal Graphs, and Hardness of Gröbner Bases*, *Interntl. Symposium on Symbolic and Algebraic Computation (ISSAC 2015)*.

<http://www.usna.edu/Users/math/margulies>

- 1 J. A. De Loera, J. Lee, S. Margulies, S. Onn. *Expressing Combinatorial Optimization Problems by Systems of Polynomial Equations and Hilbert's Nullstellensatz*, *Combinatorics, Probability and Computing*, 18(4), pp. 551-582, 2009.
- 2 S. Margulies, S. Onn, D.V. Pasechnik, *On the Complexity of Hilbert Refutations for Partition*, *Journal of Symbolic Computation*, 66, 70–83, February 2015.
- 3 J.A. De Loera, S. Margulies, M. Pernpeintner, E. Riedl, D. Rolnick, G. Spencer, D. Stasi, J. Swenson *Graph-Coloring Ideals: Nullstellensatz Certificates, Gröbner Bases for Chordal Graphs, and Hardness of Gröbner Bases*, *Interntl. Symposium on Symbolic and Algebraic Computation (ISSAC 2015)*.

<http://www.usna.edu/Users/math/margulies>

Thank you for your attention!
Questions and **comments** are most welcome!