Hilbert's Nullstellensatz, Linear Algebra and Combinatorial Problems

Susan Margulies

Mathematics Department,

US Naval Academy, Annapolis, Maryland

Visiting National Institute of Standards and Technology!

April 7, 2015

The Nullstellensatz Linear Algebra (**Nul**l**LA**) Algorithm

Let $x = \{x_1, ..., x_n\}$ and $f_i \in \mathbb{K}[x_1, \ldots, x_n]$ ($\mathbb{K}$ ususally $\mathbb{C}$ or $\overline{\mathbb{F}_2}$)

- **INPUT:**
- **OUTPUT:**

The Nullstellensatz Linear Algebra (**Nu**l**LA**) Algorithm

Let $x = \{x_1, ..., x_n\}$ and $f_i \in \mathbb{K}[x_1, \ldots, x_n]$ ($\mathbb{K}$ ususally $\mathbb{C}$ or $\overline{\mathbb{F}_2}$)

- **INPUT:** A system of polynomial equations

$$f_1(x) = 0, \quad f_2(x) = 0, \quad \ldots \quad f_s(x) = 0$$

- **OUTPUT:**

The Nullstellensatz Linear Algebra (**Nul****LA**) Algorithm

Let $x = \{x_1, ..., x_n\}$ and $f_i \in \mathbb{K}[x_1, \ldots, x_n]$ ($\mathbb{K}$ ususally $\mathbb{C}$ or $\overline{\mathbb{F}_2}$)

- **INPUT:** A system of polynomial equations

$$f_1(x) = 0, \quad f_2(x) = 0, \quad \ldots \quad f_s(x) = 0$$

- **OUTPUT:**
  1. *yes*, there is a solution.
  2. *no*, there is *no* solution

.

The Nullstellensatz Linear Algebra (**Nul****LA**) Algorithm

Let $x = \{x_1, ..., x_n\}$ and $f_i \in \mathbb{K}[x_1, \ldots, x_n]$ ($\mathbb{K}$ ususally $\mathbb{C}$ or $\overline{\mathbb{F}_2}$)

- **INPUT:** A system of polynomial equations

$$f_1(x) = 0, \quad f_2(x) = 0, \quad \ldots \quad f_s(x) = 0$$

- **OUTPUT:**
  1. *yes*, there is a solution.
  2. *no*, there is *no* solution, along with a *Nullstellensatz certificate of infeasibility*.

Hilbert's Nullstellensatz

- **Theorem (1893):** Let $\mathbb{K}$ be an algebraically closed field and $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Given a system of equations such that $\mathbf{f_1 = f_2 = \cdots = f_s = 0}$, then this system has no solution if and only if there exist polynomials $\beta_{\mathbf{1}}, \ldots, \beta_{\mathbf{s}} \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$1 = \sum_{i=1}^{s} \beta_{\mathbf{i}} \mathbf{f_i} \ . \qquad \square$$

Hilbert's Nullstellensatz

- **Theorem (1893):** Let $\mathbb{K}$ be an algebraically closed field and $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Given a system of equations such that $\mathbf{f_1 = f_2 = \cdots = f_s = 0}$, then this system has no solution if and only if there exist polynomials $\beta_{\mathbf{1}}, \ldots, \beta_{\mathbf{s}} \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$1 = \sum_{i=1}^{s} \beta_{\mathbf{i}} \mathbf{f_i} \ . \qquad \square$$

Hilbert's Nullstellensatz

- **Theorem (1893):** Let $\mathbb{K}$ be an algebraically closed field and $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Given a system of equations such that $\mathbf{f_1 = f_2 = \cdots = f_s = 0}$, then this system has **no** solution if and only if there exist polynomials $\beta_{\mathbf{1}}, \ldots, \beta_{\mathbf{s}} \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$1 = \sum_{i=1}^{s} \beta_{\mathbf{i}} \mathbf{f_i} \ . \qquad \square$$

Hilbert's Nullstellensatz

- **Theorem (1893):** Let $\mathbb{K}$ be an algebraically closed field and $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Given a system of equations such that $\mathbf{f_1 = f_2 = \cdots = f_s = 0}$, then this system has **no** solution if and only if there exist polynomials $\beta_{\mathbf{1}}, \ldots, \beta_{\mathbf{s}} \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$1 = \sum_{i=1}^{s} \beta_{\mathbf{i}} \mathbf{f_i} \ . \qquad \square$$

Hilbert's Nullstellensatz

- **Theorem (1893):** Let $\mathbb{K}$ be an algebraically closed field and $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Given a system of equations such that $\mathbf{f_1 = f_2 = \cdots = f_s = 0}$, then this system has **no** solution if and only if there exist polynomials $\beta_\mathbf{1}, \ldots, \beta_\mathbf{s} \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$\mathbf{1} = \sum_{i=1}^{s} \beta_\mathbf{i} \mathbf{f_i} \ . \qquad \square$$

Hilbert's Nullstellensatz

- **Theorem (1893):** Let $\mathbb{K}$ be an algebraically closed field and $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Given a system of equations such that $\mathbf{f_1 = f_2 = \cdots = f_s = 0}$, then this system has **no** solution if and only if there exist polynomials $\beta_{\mathbf{1}}, \ldots, \beta_{\mathbf{s}} \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$\mathbf{1} = \sum_{i=1}^{s} \beta_{\mathbf{i}} \mathbf{f_i} \ . \qquad \square$$

Hilbert's Nullstellensatz

- **Theorem (1893):** Let $\mathbb{K}$ be an algebraically closed field and $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Given a system of equations such that $\mathbf{f_1 = f_2 = \cdots = f_s = 0}$, then this system has **no** solution if and only if there exist polynomials $\beta_{\mathbf{1}}, \ldots, \beta_{\mathbf{s}} \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$\mathbf{1} = \sum_{i=1}^{s} \beta_{\mathbf{i}} \mathbf{f_i} \ . \qquad \square$$

Hilbert's Nullstellensatz

- **Theorem (1893):** Let $\mathbb{K}$ be an algebraically closed field and $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Given a system of equations such that $\mathbf{f_1 = f_2 = \cdots = f_s = 0}$, then this system has **no** solution if and only if there exist polynomials $\beta_{\mathbf{1}}, \ldots, \beta_{\mathbf{s}} \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$\mathbf{1} = \sum_{i=1}^{s} \beta_{\mathbf{i}} \mathbf{f_i} \ . \qquad \square$$

$$1 \neq 0$$

Hilbert's Nullstellensatz

- **Theorem (1893):** Let $\mathbb{K}$ be an algebraically closed field and $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Given a system of equations such that $\mathbf{f_1 = f_2 = \cdots = f_s = 0}$, then this system has **no** solution if and only if there exist polynomials $\beta_\mathbf{1}, \ldots, \beta_\mathbf{s} \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$\mathbf{1} = \sum_{i=1}^{s} \beta_\mathbf{i} \mathbf{f_i} \ . \qquad \square$$

$$1 \neq 0$$

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

Hilbert's Nullstellensatz

- **Theorem (1893):** Let $\mathbb{K}$ be an algebraically closed field and $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Given a system of equations such that $\mathbf{f_1 = f_2 = \cdots = f_s = 0}$, then this system has **no** solution if and only if there exist polynomials $\beta_{\mathbf{1}}, \ldots, \beta_{\mathbf{s}} \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$\mathbf{1} = \sum_{i=1}^{s} \beta_{\mathbf{i}} \mathbf{f_i} \ . \qquad \square$$

$$1 \neq 0$$

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

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

Hilbert's Nullstellensatz

- **Theorem (1893):** Let $\mathbb{K}$ be an algebraically closed field and $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Given a system of equations such that $\mathbf{f_1 = f_2 = \cdots = f_s = 0}$, then this system has **no** solution if and only if there exist polynomials $\beta_{\mathbf{1}}, \ldots, \beta_{\mathbf{s}} \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$\mathbf{1} = \sum_{i=1}^{s} \beta_{\mathbf{i}} \mathbf{f_i} \ . \qquad \square$$

$$1 \neq 0$$

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

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

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

- **Theorem (1893):** Let $\mathbb{K}$ be an algebraically closed field and $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Given a system of equations such that $\mathbf{f_1 = f_2 = \cdots = f_s = 0}$, then this system has **no** solution if and only if there exist polynomials $\beta_\mathbf{1}, \ldots, \beta_\mathbf{s} \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$\mathbf{1} = \sum_{i=1}^{s} \beta_\mathbf{i}\mathbf{f_i} \ . \qquad \square$$

$$1 \neq 0$$

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

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

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

Hilbert's Nullstellensatz

- **Theorem (1893):** Let $\mathbb{K}$ be an algebraically closed field and $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Given a system of equations such that $\mathbf{f_1 = f_2 = \cdots = f_s = 0}$, then this system has **no** solution if and only if there exist polynomials $\beta_{\mathbf{1}}, \ldots, \beta_{\mathbf{s}} \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$\underbrace{\mathbf{1} = \sum_{i=1}^{s} \beta_{\mathbf{i}} \mathbf{f_i} \ .}$$ □

This polynomial identity is a *Nullstellensatz certificate*.

Hilbert's Nullstellensatz

- **Theorem (1893):** Let $\mathbb{K}$ be an algebraically closed field and $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Given a system of equations such that $\mathbf{f_1 = f_2 = \cdots = f_s = 0}$, then this system has **no** solution if and only if there exist polynomials $\beta_{\mathbf{1}}, \ldots, \beta_{\mathbf{s}} \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$\underbrace{\mathbf{1} = \sum_{i=1}^{s} \beta_{\mathbf{i}} \mathbf{f_i}\ .}$$ □

  This polynomial identity is a *Nullstellensatz certificate*.

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

Nullstellensatz Degree *Upper* Bounds

Recall n is the number of variables, and the number of monomials of degree d in n variables is $\binom{n+d-1}{n-1}$.

- **Theorem:** (Kollár, 1988) The $\deg(\beta_i)$ is bounded by

$$\deg(\beta_i) \leq \Big(\max \big\{ 3, \max\{\deg(f_i)\} \big\} \Big)^n .$$

(bound is tight for certain pathologically bad examples)

- **Theorem:** (Lazard 1977, Brownawell 1987) The $\deg(\beta_i)$ is bounded by

$$\deg(\beta_i) \leq n\big(\max\{\deg(f_i)\} - 1 \big) .$$

(bound applies to particular zero-dimensional ideals)

Nullstellensatz Degree *Upper* Bounds

Recall n is the number of variables, and the number of monomials of degree d in n variables is $\binom{n+d-1}{n-1}$.

- **Theorem:** (Kollár, 1988) The $\deg(\beta_i)$ is bounded by

$$\deg(\beta_i) \leq \Big(\max \big\{3, \max\{\deg(f_i)\}\big\}\Big)^n .$$

(bound is tight for certain pathologically bad examples)

- **Theorem:** (Lazard 1977, Brownawell 1987) The $\deg(\beta_i)$ is bounded by

$$\deg(\beta_i) \leq n\big(\max\{\deg(f_i)\} - 1\big) .$$

(bound applies to particular zero-dimensional ideals)

Question: What about lower bounds? How do we find them?

NulLA running on a particular instance:

- **INPUT:** A system of polynomial equations

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

NulLA running on a particular instance:

- **INPUT:** A system of polynomial equations

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

1. Construct a hypothetical Nullstellensatz certificate of degree 1

$$1 = \underbrace{(c_0 x_1 + c_1 x_2 + c_2 x_3 + c_3)}_{\beta_1}(x_1^2 - 1) + \underbrace{(c_4 x_1 + c_5 x_2 + c_6 x_3 + c_7)}_{\beta_2}(x_1 + x_2)$$
$$+ \underbrace{(c_8 x_1 + c_9 x_2 + c_{10} x_3 + c_{11})}_{\beta_3}(x_1 + x_3) + \underbrace{(c_{12} x_1 + c_{13} x_2 + c_{14} x_3 + c_{15})}_{\beta_4}(x_2 + x_3)$$

NulLA running on a particular instance:

- **INPUT:** A system of polynomial equations

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

1. Construct a hypothetical Nullstellensatz certificate of degree 1

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

2. Expand the hypothetical Nullstellensatz certificate

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

NulLA running on a particular instance:

- **INPUT:** A system of polynomial equations

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

1. Construct a hypothetical Nullstellensatz certificate of degree 1

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

2. Expand the hypothetical Nullstellensatz certificate

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

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

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

NulLA running on a particular instance:

	c_0	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}	c_{12}	c_{13}	c_{14}	c_{15}	
x_1^3	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$x_1^2 x_2$	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$x_1^2 x_3$	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
x_1^2	0	0	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0
x_2^2	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0
x_3^2	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0
$x_1 x_2$	0	0	0	0	1	1	0	0	0	1	0	0	1	0	0	0	0
$x_1 x_3$	0	0	0	0	0	0	1	0	1	0	1	0	1	0	0	0	0
$x_2 x_3$	0	0	0	0	0	0	1	0	0	1	0	0	0	1	1	0	0
x_1	-1	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0
x_2	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0
x_3	0	0	-1	0	0	0	0	0	0	0	0	1	0	0	0	1	0
1	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	1

NulLA running on a particular instance:

4. Solve the linear system, and assemble the certificate

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

NulLA running on a particular instance:

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.

NulLA Summary

- **INPUT:** A system of polynomial equations
  1. Construct a hypothetical Nullstellensatz certificate of degree d
  2. Expand the hypothetical Nullstellensatz certificate
  3. Extract a *linear* system of equations from expanded certificate
  4. Solve the linear system.
     1. If there is a solution, assemble the certificate.
     2. Otherwise, loop and repeat with a larger degree d until known upper bounds are exceeded.
- **OUTPUT:**
  1. *yes*, there is a solution.
  2. *no*, there is *no* solution, along with a *certificate of infeasibility*.

Partition Problem: Definition and Example

- **Partition:** Given set of integers $W = \{w_1, \ldots, w_n\}$, 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 $W = \{w_1, \ldots, w_n\}$, 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 $W = \{w_1, \ldots, w_n\}$, 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

$$\underbrace{1 + 3 + 5 + 7}_{S} \qquad\qquad\qquad .$$

Partition Problem: Definition and Example

- **Partition:** Given set of integers $W = \{w_1, \ldots, w_n\}$, 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

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

Partition Problem: Definition and Example

- **Partition:** Given set of integers $W = \{w_1, \ldots, w_n\}$, 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 as a System of Polynomial Equations

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

- one **variable** per **integer**: $x_1, \ldots, x_n$

Partition as a System of Polynomial Equations

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

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

Partition as a System of Polynomial Equations

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

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

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

Partition as a System of Polynomial Equations

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

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

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

- **Proposition:** Given a set of integers $W = \{w_1, \ldots, w_n\}$, 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 $W = \{w_1, \ldots, w_n\}$:

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

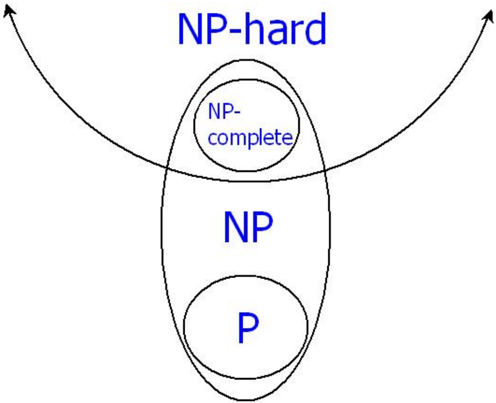
$$\sum_{i=1}^{n} w_i x_i = 0 \ .$$

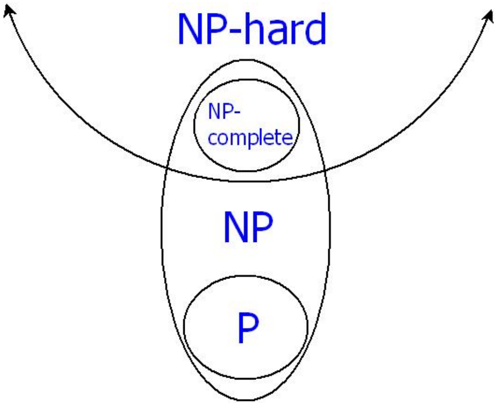
- **Proposition:** Given a set of integers $W = \{w_1, \ldots, w_n\}$, the above system of $n+1$ polynomial equations has a solution if and only if there exists a partition of W into two sets, $S \subseteq W$ and $W \setminus S$, such that $\sum_{w \in S} w = \sum_{w \in W \setminus S} w$.

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

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

NP, coNP and the Nullstellensatz

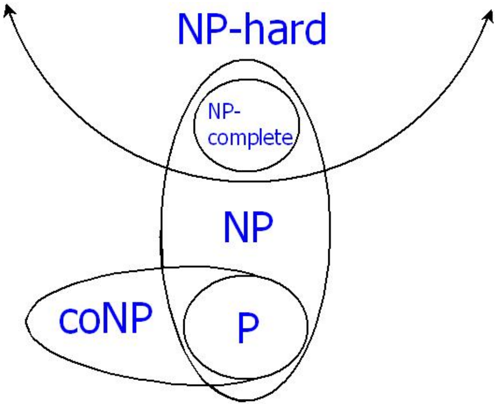




Definition

NP is the class of problems whose solutions can be verified in polynomial-time.

NP, coNP and the Nullstellensatz



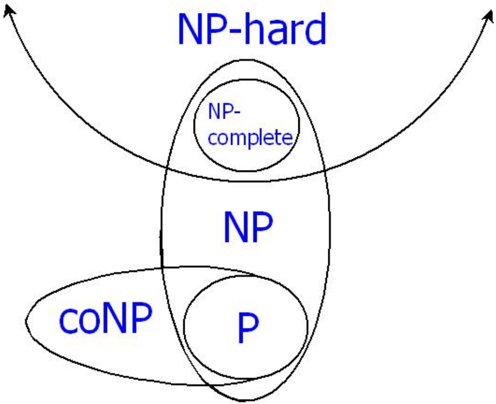
Definition

NP is the class of problems whose solutions can be verified in polynomial-time.

Definition

coNP is the class of problems whose complements are in NP.

NP, coNP and the Nullstellensatz



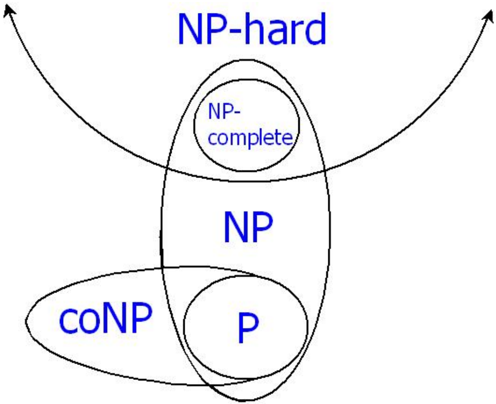
Definition

NP is the class of problems whose solutions can be verified in polynomial-time.

Definition

coNP is the class of problems whose complements are in NP.

It is widely believed that $\mathrm{coNP} \neq \mathrm{NP}$.



Definition

NP is the class of problems whose solutions can be verified in polynomial-time.

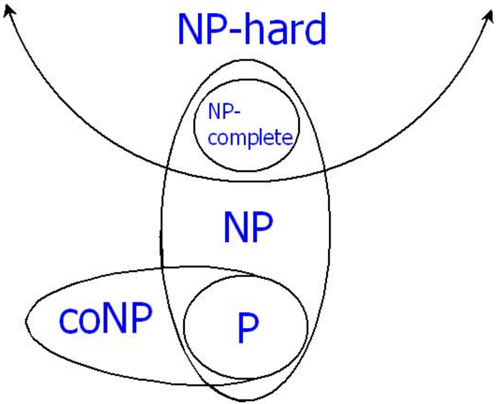
(hard to find)

Definition

coNP is the class of problems whose complements are in NP.

It is widely believed that coNP $\neq$ NP.

NP, coNP and the Nullstellensatz



Definition

NP is the class of problems whose solutions can be verified in polynomial-time.

(hard to find)

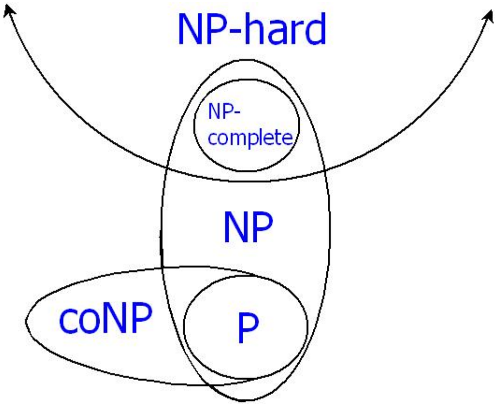
Definition

coNP is the class of problems whose complements are in NP.

(hard to verify)

It is widely believed that $\text{coNP} \neq \text{NP}$.

NP, coNP and the Nullstellensatz



Definition

NP is the class of problems whose solutions can be verified in polynomial-time.

(hard to find)

Definition

coNP is the class of problems whose complements are in NP.

(hard to verify)

Observation

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

It is widely believed that $\mathrm{coNP} \neq \mathrm{NP}$.

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!

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

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

Minimum-degree *Partition* Nullstellensatz Certificates

Let S_k^n denote the set of k-subsets of $\{1, \ldots, n\}$

Minimum-degree *Partition* Nullstellensatz Certificates

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

Minimum-degree *Partition* Nullstellensatz Certificates

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

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

Given a set of non-partitionable integers $W = \{w_1,\ldots,w_n\}$ 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:

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

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 *Partition* Nullstellensatz Certificates

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

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

Given a set of non-partitionable integers $W = \{w_1, \ldots, w_n\}$ 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:

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

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 *Partition* Nullstellensatz Certificates

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

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

Given a set of non-partitionable integers $W = \{w_1, \ldots, w_n\}$ 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:

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

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: degree is n for n odd and $n - 1$ for n even.

Minimum-degree *Partition* Nullstellensatz Certificates

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

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

Given a set of non-partitionable integers $W = \{w_1, \ldots, w_n\}$ 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:

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

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: degree is n for n odd and $n-1$ for n even.

Minimum-degree *Partition* Nullstellensatz Certificates

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

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

Given a set of non-partitionable integers $W = \{w_1, \ldots, w_n\}$ 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:

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

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: degree is n for n odd and $n-1$ for n even.

Minimum-degree *Partition* Nullstellensatz Certificates

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

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

Given a set of non-partitionable integers $W = \{w_1,\ldots,w_n\}$ 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:

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

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: degree is n for n odd and $n-1$ for n even.

Minimum-degree *Partition* Nullstellensatz Certificates

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

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

Given a set of non-partitionable integers $W = \{w_1, \ldots, w_n\}$ 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:

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

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: degree is n for n odd and $n-1$ for n even.

Minimum-degree *Partition* Nullstellensatz Certificates

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

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

Given a set of non-partitionable integers $W = \{w_1,\ldots,w_n\}$ 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:

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

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: degree is n for n odd and $n-1$ for n even.

Minimum-degree *Partition* Nullstellensatz Certificates

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

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

Given a set of non-partitionable integers $W = \{w_1,\ldots,w_n\}$ 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:

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

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: degree is n for n odd and $n-1$ for n even.

Minimum-degree *Partition* Nullstellensatz Certificates

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

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

Given a set of non-partitionable integers $W = \{w_1, \ldots, w_n\}$ 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:

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

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?

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

Minimum-degree Nullstellensatz Certificates Example

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

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

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

Minimum-degree Nullstellensatz Certificates Example

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

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

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

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_1		w_2	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_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_2	w_1		w_3
w_1	w_2			w_3

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

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

$-$	$+$
	$w_1 + w_2 + w_3$
$-w_1$	$+ w_2 + w_3$
$- w_2$	$+ w_1 \quad + w_3$
$-w_1 - w_2$	$+ w_3$

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

The Partition Matrix: Extract a Square Linear System

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

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

$-$	$+$
	$w_1 + w_2 + w_3$
$-w_1$	$+ w_2 + w_3$
$-w_2$	$+ w_1 \quad + w_3$
$-w_1 - w_2$	$+ w_3$

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

The Partition Matrix: Extract a Square Linear System

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

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

$-$	$+$
	$w_1 + w_2 + w_3$
$-w_1$	$+w_2 + w_3$
$-w_2$	$+w_1 \quad + w_3$
$-w_1 - w_2$	$+w_3$

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

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

Another Example of the Partition Matrix

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

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

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

"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 $W = \{1, 3, 5, 2\}$:

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

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

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

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

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

$$
\begin{aligned}
-51975 = & (1+3+5+2)(-1+3+5+2)(1-3+5+2)(1+3-5+2) \\
& (-1-3+5+2)(-1+3-5+2)(1-3-5+2)(-1-3-5+2) \; .
\end{aligned}
$$

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

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

$$-51975 = (1+3+5+2)(-1+3+5+2)(1-3+5+2)(1+3-5+2)$$
$$(-1-3+5+2)(-1+3-5+2)(1-3-5+2)(-1-3-5+2) \,.$$

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

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

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

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

$$
\begin{aligned}
-51975 = &(1+3+5+2)(-1+3+5+2)(1-3+5+2)(1+3-5+2)\\
&(-1-3+5+2)(-1+3-5+2)(1-3-5+2)(-1-3-5+2)\ .
\end{aligned}
$$

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

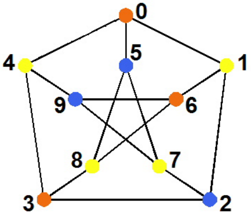
$$b_4 = \frac{-2550}{-51975} = \frac{34}{693}\ .$$

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 3-Coloring as a System of Polynomial Equations over $\mathbb{C}$ (D. Bayer)

- one **variable** per **vertex**: $x_1, \ldots, x_n$

Graph 3-Coloring as a System of Polynomial Equations over $\mathbb{C}$ (D. Bayer)

- one **variable** per **vertex**: $x_1, \ldots, x_n$
- **vertex polynomials:** For every vertex $i = 1, \ldots, n$,

$$x_i^3 - 1 = 0$$

Graph 3-Coloring as a System of Polynomial Equations over $\mathbb{C}$ (D. Bayer)

- one **variable** per **vertex**: $x_1, \ldots, x_n$
- **vertex polynomials:** For every vertex $i = 1, \ldots, n$,

$$x_i^3 - 1 = 0$$

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

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

Graph 3-Coloring as a System of Polynomial Equations over $\mathbb{C}$ (D. Bayer)

- one **variable** per **vertex**: $x_1, \ldots, x_n$
- **vertex polynomials:** For every vertex $i = 1, \ldots, n$,

$$x_i^3 - 1 = 0$$

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

$$\frac{x_i^3 - x_j^3}{x_i - x_j} = x_i^2 + x_i x_j + x_j^2 = 0$$

Graph 3-Coloring as a System of Polynomial Equations over $\mathbb{C}$ (D. Bayer)

- one **variable** per **vertex**: $x_1, \ldots, x_n$
- **vertex polynomials:** For every vertex $i = 1, \ldots, n$,

$$x_i^3 - 1 = 0$$

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

$$\frac{x_i^3 - x_j^3}{x_i - x_j} = x_i^2 + x_i x_j + x_j^2 = 0$$

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

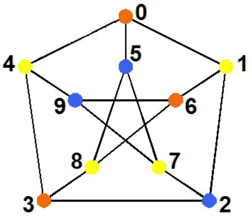


Figure: Is the Petersen graph 3-colorable?

$$x_0^3 - 1 = 0, x_1^3 - 1 = 0, \qquad x_0^2 + x_0x_1 + x_1^2 = 0, x_0^2 + x_0x_4 + x_4^2 = 0$$
$$x_2^3 - 1 = 0, x_3^3 - 1 = 0, \qquad x_0^2 + x_0x_5 + x_5^2 = 0, x_1^2 + x_1x_2 + x_2^2 = 0$$
$$x_4^3 - 1 = 0, x_5^3 - 1 = 0, \qquad x_1^2 + x_1x_6 + x_6^2 = 0, x_2^2 + x_2x_3 + x_3^2 = 0$$
$$x_6^3 - 1 = 0, x_7^3 - 1 = 0, \qquad \cdots\cdots \qquad \cdots\cdots$$
$$x_8^3 - 1 = 0, x_9^3 - 1 = 0, \qquad x_6^2 + x_6x_8 + x_8^2 = 0, x_7^2 + x_7x_9 + x_9^2 = 0$$

Where is the Infinite Family of Graphs that Grow over $\mathbb{C}$?

4

Where is the Infinite Family of Graphs that Grow over $\mathbb{C}$?

4

- Flower, Kneser, Grötzsch, Jin, Mycielski graphs have degree 4.

Where is the Infinite Family of Graphs that Grow over $\mathbb{C}$?

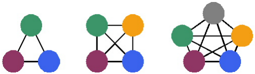
4

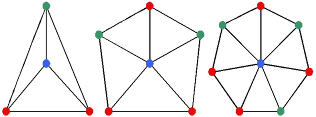
- Flower, Kneser, Grötzsch, Jin, Mycielski graphs have degree 4.
- **Theorem:** Every Nullstellensatz certificate of a non-3-colorable graph has degree *at least* four.

Where is the Infinite Family of Graphs that Grow over $\mathbb{C}$?

4

- Flower, Kneser, Grötzsch, Jin, Mycielski graphs have degree 4.
- **Theorem:** Every Nullstellensatz certificate of a non-3-colorable graph has degree *at least* four.
- **Theorem:** For $n \geq 4$, a minimum-degree Nullstellensatz certificate of non-3-colorability for cliques and odd wheels has degree exactly four.





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

- one **variable** per **vertex**: $x_1, \ldots, x_n$
- **vertex polynomials:** For every vertex $i = 1, \ldots, n$,

$$x_i^3 + 1 = 0$$

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

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

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

1

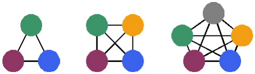
Where is the Infinite Family of Graphs that Grow over $\overline{\mathbb{F}_2}$?

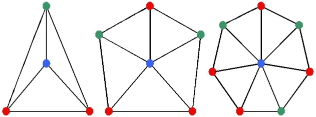
1

- **Theorem:** Every Nullstellensatz certificate of a non-3-colorable graph has degree *at least* one.

1

- **Theorem:** Every Nullstellensatz certificate of a non-3-colorable graph has degree *at least* one.
- **Theorem:** For $n \geq 4$, a minimum-degree Nullstellensatz certificate of non-3-colorability for cliques and odd wheels has degree exactly one.





Experimental results for NulLA 3-colorability

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

Table: Graphs without 4-cliques.

Experimental results for NulLA 3-colorability

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

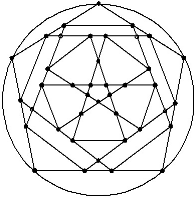
Table: Graphs without 4-cliques.

Experimental results for NulLA 3-colorability

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

Table: Graphs without 4-cliques.

What if the Nullstellensatz certificate is *not* degree 1?

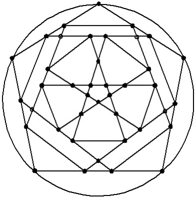


degree 4 certificate

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

over 4 hours

What if the Nullstellensatz certificate is *not* degree 1?



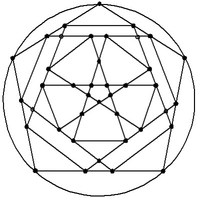
degree 4 certificate

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

over 4 hours

$\Longrightarrow$ 25 triangles

What if the Nullstellensatz certificate is *not* degree 1?

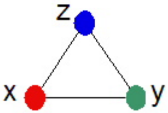


degree 4 certificate

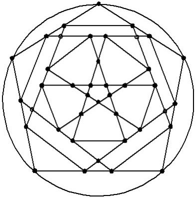
$7,585,826 \times 9,887,481$

over 4 hours

$\Longrightarrow$ 25 triangles

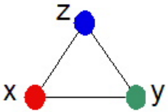


What if the Nullstellensatz certificate is *not* degree 1?



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

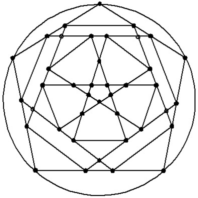
$\Longrightarrow$ 25 triangles



"Triangle" equation:

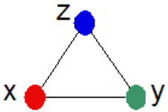
$$0 = x + y + z$$

What if the Nullstellensatz certificate is *not* degree 1?



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

$\Longrightarrow$ 25 triangles



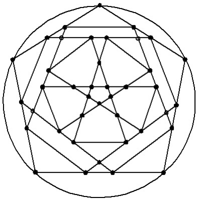
"Triangle" equation:

$$0 = x + y + z$$

Degree two triangle equation:

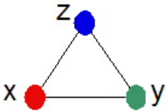
$$0 = x^2 + y^2 + z^2$$

What if the Nullstellensatz certificate is *not* degree 1?



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

$\Longrightarrow$ 25 triangles



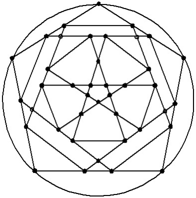
"Triangle" equation:

$$0 = x + y + z$$

Degree two triangle equation:

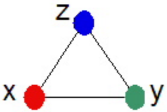
$$0 = x^2 + y^2 + z^2$$

What if the Nullstellensatz certificate is *not* degree 1?



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

$\Longrightarrow$ 25 triangles



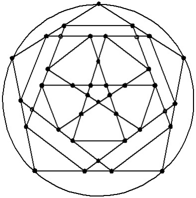
"Triangle" equation:

$$0 = x + y + z$$

Degree two triangle equation:

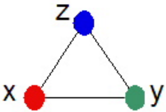
$$0 = x^2 + y^2 + z^2$$

What if the Nullstellensatz certificate is *not* degree 1?



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

$\Longrightarrow$ 25 triangles



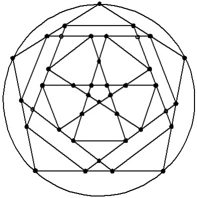
"Triangle" equation:

$$0 = x + y + z$$

Degree two triangle equation:

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

What if the Nullstellensatz certificate is *not* degree 1?



degree 4 certificate

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

over 4 hours

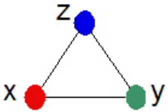
$\Downarrow$

degree 1 certificate

$4,626 \times 4,3464$

.2 seconds

$\Longrightarrow$ 25 triangles



"Triangle" equation:

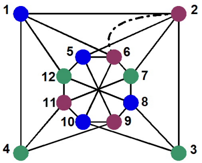
$$0 = x + y + z$$

Degree two triangle equation:

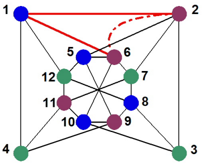
$$0 = x^2 + y^2 + z^2$$

Appending equations to the system can *reduce* the degree!

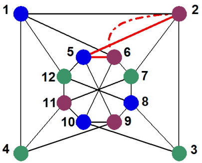
What if the Nullstellensatz certificate is *still* not degree 1?



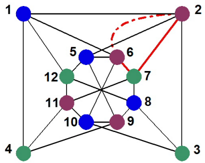
What if the Nullstellensatz certificate is *still* not degree 1?



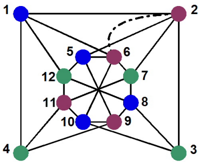
What if the Nullstellensatz certificate is *still* not degree 1?



What if the Nullstellensatz certificate is *still* not degree 1?



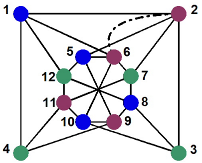
What if the Nullstellensatz certificate is *still* not degree 1?



Alternative Nullstellensätze

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

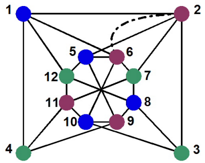
What if the Nullstellensatz certificate is *still* not degree 1?



Alternative Nullstellensätze

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

non-zero $\neq 0$



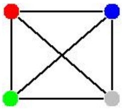
Alternative Nullstellensätze

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

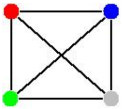
non-zero $\neq 0$

$$\begin{aligned} x_1x_8x_9 = {} & (x_1 + x_2)(x_1^2 + x_1x_2 + x_2^2) + (x_4 + x_9 + x_{12})(x_1^2 + x_1x_4 + x_4^2) + \cdots + \\ & + (x_1 + x_4 + x_8)(x_1^2 + x_1x_{12} + x_{12}^2) + (x_2 + x_7 + x_8)(x_2^2 + x_2x_3 + x_3^2) \\ & + (x_8 + x_9)\underbrace{(x_1^2 + x_2^2 + x_6^2)}_{\text{triangle equation}} + (x_9)\underbrace{(x_2^2 + x_5^2 + x_6^2)}_{\text{triangle equation}} + (x_8)\underbrace{(x_2^2 + x_6^2 + x_7^2)}_{\text{triangle equation}}. \end{aligned}$$

Using Symmetry to Reduce the Size of the Linear System



Consider the complete graph K_4.



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

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

Matrix associated with K_4 Nullstellensatz Certificate: $M_{F,1}$

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

Using Symmetry to Reduce the Size of the Linear System

Suppose a finite permutation group G acts on the variables $x_1, \ldots, x_n$.

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

Using Symmetry to Reduce the Size of the Linear System

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

We will use this group to reduce the size of the matrix.

Matrix associated with K_4 Nullstellensatz Certificate: $M_{F,1}$

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

Action of Z_3 by $(2,3,4)$: each row block represents an orbit.

Matrix associated with K_4 Nullstellensatz Certificate: $M_{F,1,G}$

	$\bar{c}_0$	$\bar{c}_{12}^1$	$\bar{c}_{12}^2$	$\bar{c}_{12}^3$	$\bar{c}_{12}^4$	$\bar{c}_{23}^1$	$\bar{c}_{23}^2$	$\bar{c}_{24}^2$	$\bar{c}_{34}^2$
$Orb(1)$	1	0	0	0	0	0	0	0	0
$Orb(x_1^3)$	1	**3**	0	0	0	0	0	0	0
$Orb(x_1^2x_2)$	0	1	1	1	1	0	0	0	0
$Orb(x_1x_2^2)$	0	1	1	0	0	**2**	0	0	0
$Orb(x_1x_2x_3)$	0	0	0	1	1	1	0	0	0
$Orb(x_2^3)$	0	0	1	0	0	0	1	1	0
$Orb(x_2^2x_3)$	0	0	0	1	0	0	1	1	1
$Orb(x_2^2x_4)$	0	0	0	0	1	0	1	1	1
$Orb(x_2x_3x_4)$	0	0	0	0	0	0	0	0	**3**

Matrix associated with K_4 Nullstellensatz Certificate: $M_{F,1,G}$

	$\bar{c}_0$	$\bar{c}_{12}^1$	$\bar{c}_{12}^2$	$\bar{c}_{12}^3$	$\bar{c}_{12}^4$	$\bar{c}_{23}^1$	$\bar{c}_{23}^2$	$\bar{c}_{24}^2$	$\bar{c}_{34}^2$
$Orb(1)$	1	0	0	0	0	0	0	0	0
$Orb(x_1^3)$	1	**3**	0	0	0	0	0	0	0
$Orb(x_1^2x_2)$	0	1	1	1	1	0	0	0	0
$Orb(x_1x_2^2)$	0	1	1	0	0	**2**	0	0	0
$Orb(x_1x_2x_3)$	0	0	0	1	1	1	0	0	0
$Orb(x_2^3)$	0	0	1	0	0	0	1	1	0
$Orb(x_2^2x_3)$	0	0	0	1	0	0	1	1	1
$Orb(x_2^2x_4)$	0	0	0	0	1	0	1	1	1
$Orb(x_2x_3x_4)$	0	0	0	0	0	0	0	0	**3**

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

	$\bar{c}_0$	$\bar{c}_{12}^1$	$\bar{c}_{12}^2$	$\bar{c}_{12}^3$	$\bar{c}_{12}^4$	$\bar{c}_{23}^1$	$\bar{c}_{23}^2$	$\bar{c}_{24}^2$	$\bar{c}_{34}^2$
$Orb(1)$	1	0	0	0	0	0	0	0	0
$Orb(x_1^3)$	1	1	0	0	0	0	0	0	0
$Orb(x_1^2x_2)$	0	1	1	1	1	0	0	0	0
$Orb(x_1x_2^2)$	0	1	1	0	0	0	0	0	0
$Orb(x_1x_2x_3)$	0	0	0	1	1	1	0	0	0
$Orb(x_2^3)$	0	0	1	0	0	0	1	1	0
$Orb(x_2^2x_3)$	0	0	0	1	0	0	1	1	1
$Orb(x_2^2x_4)$	0	0	0	0	1	0	1	1	1
$Orb(x_2x_3x_4)$	0	0	0	0	0	0	0	0	1

Solution to Orbit Matrix Proves Certificate Existence

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

Solution to Orbit Matrix Proves Certificate Existence

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

In other words, if the orbit matrix has a solution, so does the original matrix.

Nullstellensatz Certificates for Problems in P

Question

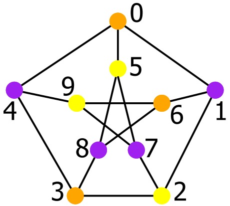
Given a combinatorial problem in P, does there **exist** an encoding such that the Nullstellensatz certificates have polynomial size?

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**

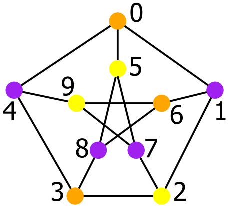


Nullstellensatz Certificates for Problems in P

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**

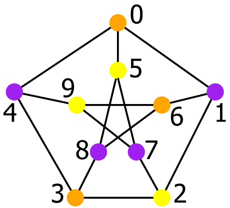


Nullstellensatz Certificates for Problems in P

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

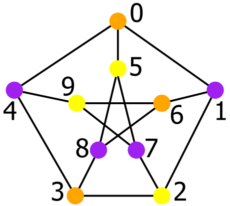
A graph G is not-2-colorable $\iff$ G contains an odd cycle.

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.

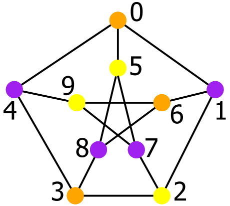
- $(x_i^2 - 1) = 0$, $\forall i \in V(G)$ and $(x_i + x_j) = 0$, $\forall (i,j) \in E(G)$ $(\mathbb{C})$

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.

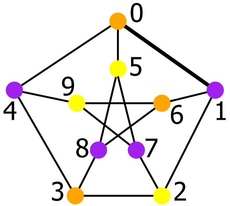
- $(x_i^2 - 1) = 0 \ , \forall i \in V(G)$ and $(x_i + x_j) = 0 \ , \forall (i,j) \in E(G)$ $(\mathbb{C})$

$$-\,(x_0^2 - 1)$$

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 $(x_i + x_j) = 0$, $\forall (i,j) \in E(G)$ $(\mathbb{C})$

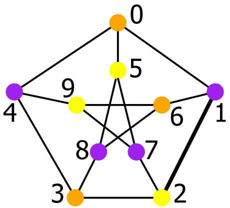
$$-(x_0^2 - 1) + \frac{1}{2}x_0(x_0 + x_1)$$

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 $(x_i + x_j) = 0 \ , \forall (i,j) \in E(G)$ ($\mathbb{C}$)

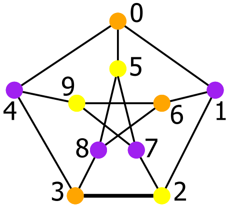
$$-(x_0^2 - 1) + \frac{1}{2}x_0(x_0 + x_1) - \frac{1}{2}x_0(x_1 + x_2)$$

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 $(x_i + x_j) = 0 \ , \forall (i,j) \in E(G)$ $(\mathbb{C})$

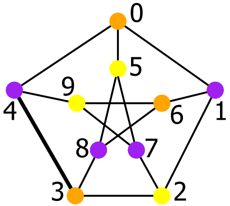
$$-(x_0^2 - 1) + \frac{1}{2}x_0(x_0 + x_1) - \frac{1}{2}x_0(x_1 + x_2) + \frac{1}{2}x_0(x_2 + x_3)$$

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 $(x_i + x_j) = 0 \; , \forall (i,j) \in E(G)$ $(\mathbb{C})$

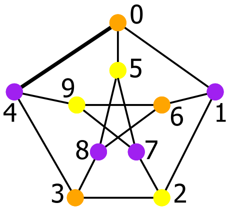
$$-(x_0^2 - 1) + \frac{1}{2}x_0(x_0 + x_1) - \frac{1}{2}x_0(x_1 + x_2) + \frac{1}{2}x_0(x_2 + x_3) - \frac{1}{2}x_0(x_3 + x_4)$$

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 $(x_i + x_j) = 0\ ,\forall (i,j) \in E(G)$ $(\mathbb{C})$

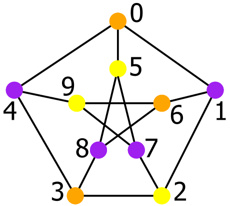
$$-(x_0^2 - 1) + \frac{1}{2}x_0(x_0 + x_1) - \frac{1}{2}x_0(x_1 + x_2) + \frac{1}{2}x_0(x_2 + x_3) - \frac{1}{2}x_0(x_3 + x_4) + \frac{1}{2}x_0(x_4 + x_0)$$

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 $(x_i + x_j) = 0\ ,\forall (i,j) \in E(G)$ $(\mathbb{C})$

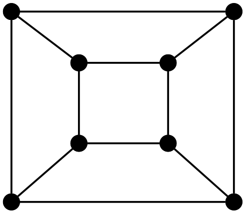
$$1 = \; -(x_0^2 - 1) + \frac{1}{2}x_0(x_0 + x_1) - \frac{1}{2}x_0(x_1 + x_2) + \frac{1}{2}x_0(x_2 + x_3) - \frac{1}{2}x_0(x_3 + x_4) + \frac{1}{2}x_0(x_4 + x_0)$$

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.

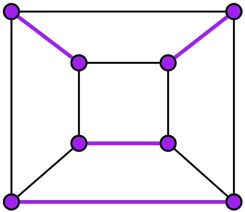
Perfect Matching: Definition and Example

- **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.

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

Perfect Matching as a System of Polynomial Equations

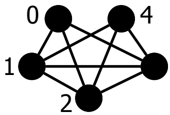
- **Proposition:** A graph G has a perfect matching if and only if the following system of polynomial equations over $\mathbb{C}$ has a solution.

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

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.

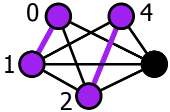
$$\sum_{j \in N(i)} x_{ij} + 1 = 0 \ , \quad x_{ij}x_{ik} = 0 \quad \forall i \in V(G) \ , \forall j,k \in N(i)$$



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.

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

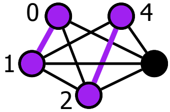


Perfect Matching as a System of Polynomial Equations

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

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

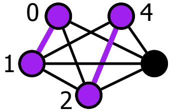
$$\begin{aligned}
1 = {} & (-\frac{2}{5}x_{12} - \frac{2}{5}x_{13} - \frac{2}{5}x_{14} - \frac{2}{5}x_{23} - \frac{2}{5}x_{24} - \frac{2}{5}x_{34} - \frac{1}{5})(-1 + x_{01} + x_{02} + x_{03}) \\
& + (-\frac{4}{5}x_{02} - \frac{4}{5}x_{03} + 2x_{23} - \frac{1}{5})(-1 + x_{01} + x_{12} + x_{13} + x_{14})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



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 $\overline{\mathbb{F}_2}$ has a solution.

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

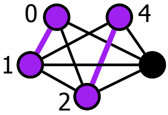


$$\begin{aligned}
1 = & \left(-\frac{2}{5}x_{12} - \frac{2}{5}x_{13} - \frac{2}{5}x_{14} - \frac{2}{5}x_{23} - \frac{2}{5}x_{24} - \frac{2}{5}x_{34} - \frac{1}{5}\right)(-1 + x_{01} + x_{02} + x_{03}) \\
& + \left(-\frac{4}{5}x_{02} - \frac{4}{5}x_{03} + 2x_{23} - \frac{1}{5}\right)(-1 + x_{01} + x_{12}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

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 $\overline{\mathbb{F}_2}$ has a solution.

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

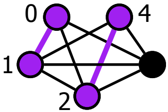


$$\begin{aligned} 1 = & (x_{01} + x_{02} + x_{03} + 1) + (x_{01} + x_{12} + x_{13} + 1) \\ & + (x_{02} + x_{12} + x_{23} + x_{24} + 1) \\ & + (x_{03} + x_{13} + x_{23} + x_{34} + 1) \\ & + (x_{24} + x_{34} + 1) \mod 2 \end{aligned}$$

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 $\overline{\mathbb{F}_2}$ has a solution.

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



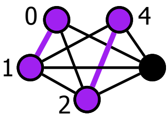
$$\begin{aligned} 1 = & (x_{01} + x_{02} + x_{03} + 1) + (x_{01} + x_{12} + x_{13} + 1) \\ & + (x_{02} + x_{12} + x_{23} + x_{24} + 1) \\ & + (x_{03} + x_{13} + x_{23} + x_{34} + 1) \\ & + (x_{24} + x_{34} + 1) \mod 2 \end{aligned}$$

- **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 $\overline{\mathbb{F}_2}$ has a solution.

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



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

- **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?

Winner of the INFORMS Computing Society Prize 2010

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. J. A. De Loera, J. Lee, P.N. Malkin, S. Margulies. *Hilbert's Nullstellensatz and an Algorithm for Proving Combinatorial Infeasibility*, ISSAC 2008, Hagenberg, Austria, ACM, 197-206, 2008.
3. J. A. De Loera, J. Lee, P.N. Malkin, S. Margulies. *Computing Infeasibility Certificates for Combinatorial Problems through Hilbert's Nullstellensatz*, JSC 46(11), pg. 1260-1283, 2011.
4. S. M., S. Onn, *On the Complexity of Hilbert Refutations for Partition*, accepted to Journal of Symbolic Computation July 2013.

Winner of the INFORMS Computing Society Prize 2010

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. J. A. De Loera, J. Lee, P.N. Malkin, S. Margulies. *Hilbert's Nullstellensatz and an Algorithm for Proving Combinatorial Infeasibility*, ISSAC 2008, Hagenberg, Austria, ACM, 197-206, 2008.
3. J. A. De Loera, J. Lee, P.N. Malkin, S. Margulies. *Computing Infeasibility Certificates for Combinatorial Problems through Hilbert's Nullstellensatz*, JSC 46(11), pg. 1260-1283, 2011.
4. S. M., S. Onn, *On the Complexity of Hilbert Refutations for Partition*, accepted to Journal of Symbolic Computation July 2013.

`http://www.usna.edu/Users/math/marguile`

Winner of the INFORMS Computing Society Prize 2010

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. J. A. De Loera, J. Lee, P.N. Malkin, S. Margulies. *Hilbert's Nullstellensatz and an Algorithm for Proving Combinatorial Infeasibility*, ISSAC 2008, Hagenberg, Austria, ACM, 197-206, 2008.
3. J. A. De Loera, J. Lee, P.N. Malkin, S. Margulies. *Computing Infeasibility Certificates for Combinatorial Problems through Hilbert's Nullstellensatz*, JSC 46(11), pg. 1260-1283, 2011.
4. S. M., S. Onn, *On the Complexity of Hilbert Refutations for Partition*, accepted to Journal of Symbolic Computation July 2013.

`http://www.usna.edu/Users/math/marguile`

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