Combinatorial Nullstellensatz: Various Proofs, Extensions and Applications

Yulia Alexandr
Advised by: Professor Karen Collins

Wesleyan University, January 2019

Table of Contents

Hilbert's Nullstellensatz

Hilbert's Nullstellensatz

Theorem (Hilbert's Nullstellensatz)

Let $\mathbb{F}$ be an algebraically closed field and I be an ideal in the polynomial ring $\mathbb{F}[x_1, \cdots, x_n]$. If $f \in \mathbb{F}[x_1, \cdots, x_n]$ is a polynomial that vanishes over all common roots of the elements in I, then $f^k \in I$ for some positive integer k.

Hilbert's Nullstellensatz

Theorem (Hilbert's Nullstellensatz)

Let $\mathbb{F}$ be an algebraically closed field and I be an ideal in the polynomial ring $\mathbb{F}[x_1, \cdots, x_n]$. If $f \in \mathbb{F}[x_1, \cdots, x_n]$ is a polynomial that vanishes over all common roots of the elements in I, then $f^k \in I$ for some positive integer k.

Definition

If I is an ideal, define:

$$\sqrt{I} = \{a : a^k \in I,\ k \in \mathbb{N}^+\}.$$

An ideal I is a *radical ideal* if $\sqrt{I} = I$

Hilbert's Nullstellensatz

Theorem (Hilbert's Nullstellensatz)

Let $\mathbb{F}$ be an algebraically closed field and I be an ideal in the polynomial ring $\mathbb{F}[x_1, \cdots, x_n]$. If $f \in \mathbb{F}[x_1, \cdots, x_n]$ is a polynomial that vanishes over all common roots of the elements in I, then $f^k \in I$ for some positive integer k.

Hilbert's Nullstellensatz $\rightarrow$ Combinatorial Nullstellensatz I

- For all $i \in [n]$, define a special univariate polynomial $g_i(x_i)$.

Hilbert's Nullstellensatz

Theorem (Hilbert's Nullstellensatz)

Let $\mathbb{F}$ be an algebraically closed field and I be an ideal in the polynomial ring $\mathbb{F}[x_1, \cdots, x_n]$. If $f \in \mathbb{F}[x_1, \cdots, x_n]$ is a polynomial that vanishes over all common roots of the elements in I, then $f^k \in I$ for some positive integer k.

Hilbert's Nullstellensatz $\rightarrow$ Combinatorial Nullstellensatz I

- For all $i \in [n]$, define a special univariate polynomial $g_i(x_i)$.
- Take the ideal I to be the ideal generated by the polynomials $g_1(x_1), \cdots, g_n(x_n)$.

Hilbert's Nullstellensatz

Theorem (Hilbert's Nullstellensatz)

Let $\mathbb{F}$ be an algebraically closed field and I be an ideal in the polynomial ring $\mathbb{F}[x_1, \cdots, x_n]$. If $f \in \mathbb{F}[x_1, \cdots, x_n]$ is a polynomial that vanishes over all common roots of the elements in I, then $f^k \in I$ for some positive integer k.

Hilbert's Nullstellensatz $\rightarrow$ Combinatorial Nullstellensatz I

- For all $i \in [n]$, define a special univariate polynomial $g_i(x_i)$.
- Take the ideal I to be the ideal generated by the polynomials $g_1(x_1), \cdots, g_n(x_n)$.
- The new ideal I is radical and so $f \in I$.

Hilbert's Nullstellensatz

Theorem (Hilbert's Nullstellensatz)

Let $\mathbb{F}$ be an algebraically closed field and I be an ideal in the polynomial ring $\mathbb{F}[x_1, \cdots, x_n]$. If $f \in \mathbb{F}[x_1, \cdots, x_n]$ is a polynomial that vanishes over all common roots of the elements in I, then $f^k \in I$ for some positive integer k.

Hilbert's Nullstellensatz $\rightarrow$ Combinatorial Nullstellensatz I

- For all $i \in [n]$, define a special univariate polynomial $g_i(x_i)$.
- Take the ideal I to be the ideal generated by the polynomials $g_1(x_1), \cdots, g_n(x_n)$.
- The new ideal I is radical and so $f \in I$.
- Moreover, $\mathbb{F}$ may not be algebraically closed.

Combinatorial Nullstellensatz I

Combinatorial Nullstellensatz I

Theorem (Combinatorial Nullstellensatz I)

Let $\mathbb{F}$ be a field and let $f = f(x_1, \cdots, x_n)$ be a polynomial in $\mathbb{F}[x_1, \cdots, x_n]$. Let $A_1, \cdots, A_n$ be finite non-empty subsets of $\mathbb{F}$ and define $g_i(x_i) = \prod_{a \in A_i}(x_i - a)$. If $f(a_1, \cdots, a_n) = 0$ for all $a_i \in A_i$, then there are polynomials $h_1, \cdots, h_n \in \mathbb{F}[x_1, \cdots, x_n]$ such that:

$$f = \sum_{i=1}^{n} h_i g_i.$$

Combinatorial Nullstellensatz I Proofs

- Alon's original proof is constructive and involves analysis of polynomial roots.

Combinatorial Nullstellensatz I Proofs

- Alon's original proof is constructive and involves analysis of polynomial roots.
- Vishnoi's proof is purely algebraic and uses basic concepts in commutative algebra.

Combinatorial Nullstellensatz II

Combinatorial Nullstellensatz II

Theorem (Combinatorial Nullstellensatz II)

Let $\mathbb{F}$ be a field and $f = f(x_1, \cdots, x_n)$ be a polynomial in $\mathbb{F}[x_1, \cdots, x_n]$. For each $i \in [n]$, let t_i be a non-negative integer, and suppose $deg(f) = \sum_{i=1}^{n} t_i$. Also, suppose that the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ in f is non-zero. Then, for all subsets $A_i \subseteq \mathbb{F}$ such that $|A_i| > t_i$, $i \in [n]$, there are $a_1 \in A_1, \cdots, a_n \in A_n$ such that $f(a_1, \cdots, a_n) \neq 0$.

Combinatorial Nullstellensatz II Proofs

- Alon's proof uses the Combinatorial Nullstellensatz I to analyze polynomial degrees.

Combinatorial Nullstellensatz II Proofs

- Alon's proof uses the Combinatorial Nullstellensatz I to analyze polynomial degrees.
- Michałek's proof is independent of the Combinatorial Nullstellensatz I and uses induction on $\deg(f)$.

Generalized Combinatorial Nullstellensatz II

- Let $\mathbb{F}$ be an arbitrary field and let $f \in \mathbb{F}[x_1, \cdots, x_n]$ where $n \in \mathbb{N}^+$.

Generalized Combinatorial Nullstellensatz II

- Let $\mathbb{F}$ be an arbitrary field and let $f \in \mathbb{F}[x_1, \cdots, x_n]$ where $n \in \mathbb{N}^+$.
- Define the **support** of f, denoted by $S(f)$, to be the set of all $(t_1, \cdots, t_n) \in \mathbb{N}^n$ such that the coefficient of $x_1^{t_1} \cdots x_n^{t_n}$ is non-zero in f.

Generalized Combinatorial Nullstellensatz II

- Let $\mathbb{F}$ be an arbitrary field and let $f \in \mathbb{F}[x_1, \cdots, x_n]$ where $n \in \mathbb{N}^+$.
- Define the **support** of f, denoted by $S(f)$, to be the set of all $(t_1, \cdots, t_n) \in \mathbb{N}^n$ such that the coefficient of $x_1^{t_1} \cdots x_n^{t_n}$ is non-zero in f.
- Define a natural partial order on the set $S(f)$ by letting $(t_1, \cdots, t_n) \leq (s_1, \cdots, s_n)$ if and only if $t_i \leq s_i$ for all $i \in [n]$.

Generalized Combinatorial Nullstellensatz II

Theorem (Łason)

Let $\mathbb{F}$ be a field and $f \in \mathbb{F}[x_1, \cdots, x_n]$. Let $(t_1, \cdots, t_n) \in S(f)$ be a maximal element in $S(f)$. Then, for any subsets $A_i \subseteq \mathbb{F}$ such that $|A_i| \geq t_i + 1$ for all $i \in [n]$, there are $a_1 \in A_1, \cdots, a_n \in A_n$ such that $f(a_1, \cdots, a_n) \neq 0$.

Existing Applications

Cauchy-Davenport Theorem: the "Classical" Application

Definition

For any two subsets A and B of a field $\mathbb{F}$, we define their sum as follows:

$$A + B = \{a + b : a \in A, b \in B\}.$$

Cauchy-Davenport Theorem: the "Classical" Application

Definition

For any two subsets A and B of a field $\mathbb{F}$, we define their sum as follows:

$$A + B = \{a + b : a \in A, b \in B\}.$$

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

Proof 1 (Idea)

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 1 (Idea)

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 1 (Idea)

- By induction on $|A|$.

Proof 1 (Idea)

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 1 (Idea)

- By induction on $|A|$.
- Uses counting arguments and basic group theory facts.

Proof 2

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 2

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 2 via Combinatorial Nullstellensatz II

- We first claim the theorem holds when $|A|+|B| > p$.

Proof 2

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 2 via Combinatorial Nullstellensatz II

- We first claim the theorem holds when $|A|+|B| > p$.
- In this case, A and B have to intersect.

Proof 2

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 2 via Combinatorial Nullstellensatz II

- We first claim the theorem holds when $|A|+|B| > p$.
- In this case, A and B have to intersect.
- Let $q \in \mathbb{Z}/p\mathbb{Z}$ be arbitrary.

Proof 2

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 2 via Combinatorial Nullstellensatz II

- We first claim the theorem holds when $|A|+|B| > p$.
- In this case, A and B have to intersect.
- Let $q \in \mathbb{Z}/p\mathbb{Z}$ be arbitrary.
- Note $|q-B| = |B|$, so $q-B$ and A have to intersect as well.

Proof 2

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 2 via Combinatorial Nullstellensatz II

- We first claim the theorem holds when $|A|+|B| > p$.
- In this case, A and B have to intersect.
- Let $q \in \mathbb{Z}/p\mathbb{Z}$ be arbitrary.
- Note $|q-B| = |B|$, so $q-B$ and A have to intersect as well.
- Then there are some $b \in B$ and $a \in A$ such that $q-b=a$.

Proof 2

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 2 via Combinatorial Nullstellensatz II

- We first claim the theorem holds when $|A|+|B| > p$.
- In this case, A and B have to intersect.
- Let $q \in \mathbb{Z}/p\mathbb{Z}$ be arbitrary.
- Note $|q-B| = |B|$, so $q-B$ and A have to intersect as well.
- Then there are some $b \in B$ and $a \in A$ such that $q-b=a$.
- Hence, $q = a+b \in A+B$.

Proof 2

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 2 via Combinatorial Nullstellensatz II

- We first claim the theorem holds when $|A|+|B| > p$.
- In this case, A and B have to intersect.
- Let $q \in \mathbb{Z}/p\mathbb{Z}$ be arbitrary.
- Note $|q-B| = |B|$, so $q-B$ and A have to intersect as well.
- Then there are some $b \in B$ and $a \in A$ such that $q-b=a$.
- Hence, $q = a+b \in A+B$.
- Since q was arbitrary, $A+B = \mathbb{Z}/p\mathbb{Z}$.

Proof 2

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 2 via Combinatorial Nullstellensatz II

- We first claim the theorem holds when $|A|+|B| > p$.
- In this case, A and B have to intersect.
- Let $q \in \mathbb{Z}/p\mathbb{Z}$ be arbitrary.
- Note $|q-B| = |B|$, so $q-B$ and A have to intersect as well.
- Then there are some $b \in B$ and $a \in A$ such that $q-b=a$.
- Hence, $q = a+b \in A+B$.
- Since q was arbitrary, $A+B = \mathbb{Z}/p\mathbb{Z}$.
- So, $|A+B| = p$ and the theorem holds.

Proof 2

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 2 via Combinatorial Nullstellensatz II

- So we may assume $|A|+|B| \leq p$.

Proof 2

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 2 via Combinatorial Nullstellensatz II

- So we may assume $|A|+|B| \leq p$.
- Toward a contradiction, suppose the theorem is false.

Proof 2

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 2 via Combinatorial Nullstellensatz II

- So we may assume $|A|+|B| \leq p$.
- Toward a contradiction, suppose the theorem is false.
- Since $|A|+|B|-1 < p$, it is the minimum of the two, so $|A+B| < |A|+|B|-1$. Equivalently,

$$|A+B| \leq |A|+|B|-2$$

Proof 2

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 2 via Combinatorial Nullstellensatz II

- So we may assume $|A|+|B| \leq p$.
- Toward a contradiction, suppose the theorem is false.
- Since $|A|+|B|-1 < p$, it is the minimum of the two, so $|A+B| < |A|+|B|-1$. Equivalently,

$$|A+B| \leq |A|+|B|-2$$

- Then, there exists some $C \subseteq \mathbb{Z}/p\mathbb{Z}$ such that $A+B \subseteq C$ and $|C| = |A|+|B|-2$.

Proof 2

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 2 via Combinatorial Nullstellensatz II

- Define $f(x,y) \in \mathbb{Z}/p\mathbb{Z}[x,y]$ as:

$$f = f(x,y) = \prod_{c \in C}(x+y-c).$$

Proof 2

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 2 via Combinatorial Nullstellensatz II

- Define $f(x,y) \in \mathbb{Z}/p\mathbb{Z}[x,y]$ as:

$$f = f(x,y) = \prod_{c \in C}(x+y-c).$$

- Since $A+B \subseteq C$, we have $f(a,b) = 0$ for all $(a,b) \in A \times B$.

Proof 2

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 2 via Combinatorial Nullstellensatz II

- Define $f(x,y) \in \mathbb{Z}/p\mathbb{Z}[x,y]$ as:

$$f = f(x,y) = \prod_{c \in C}(x+y-c).$$

- Since $A+B \subseteq C$, we have $f(a,b) = 0$ for all $(a,b) \in A \times B$.
- Let $t_1 = |A|-1$ and $t_2 = |B|-1$.

Proof 2

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 2 via Combinatorial Nullstellensatz II

- Define $f(x,y) \in \mathbb{Z}/p\mathbb{Z}[x,y]$ as:

$$f = f(x,y) = \prod_{c \in C}(x+y-c).$$

- Since $A+B \subseteq C$, we have $f(a,b) = 0$ for all $(a,b) \in A \times B$.
- Let $t_1 = |A|-1$ and $t_2 = |B|-1$. Note:
  - $t_1 + t_2 = |A|+|B|-2 = |C| = \deg(f)$.

Proof 2

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 2 via Combinatorial Nullstellensatz II

- Define $f(x,y) \in \mathbb{Z}/p\mathbb{Z}[x,y]$ as:

$$f = f(x,y) = \prod_{c \in C}(x+y-c).$$

- Since $A+B \subseteq C$, we have $f(a,b) = 0$ for all $(a,b) \in A \times B$.
- Let $t_1 = |A|-1$ and $t_2 = |B|-1$. Note:
  - $t_1 + t_2 = |A|+|B|-2 = |C| = \deg(f)$.
  - The coefficient of $x^{t_1}y^{t_2}$ in f is $\binom{|A|+|B|-2}{|A|-1}$, which is non-zero in $\mathbb{Z}/p\mathbb{Z}$.

Proof 2

Theorem (Cauchy-Davenport)

Let p be a prime and let A and B be two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Proof 2 via Combinatorial Nullstellensatz II

- Define $f(x,y) \in \mathbb{Z}/p\mathbb{Z}[x,y]$ as:

$$f = f(x,y) = \prod_{c \in C}(x+y-c).$$

- Since $A+B \subseteq C$, we have $f(a,b) = 0$ for all $(a,b) \in A \times B$.
- Let $t_1 = |A|-1$ and $t_2 = |B|-1$. Note:
  - $t_1 + t_2 = |A|+|B|-2 = |C| = \deg(f)$.
  - The coefficient of $x^{t_1}y^{t_2}$ in f is $\binom{|A|+|B|-2}{|A|-1}$, which is non-zero in $\mathbb{Z}/p\mathbb{Z}$.
- By the Combinatorial Nullstellensatz II, we get a contradiction. $\square$

Definitions and Notation

- For a $G = (V, E)$ on n vertices, enumerate its vertices, thus identifying $V = [n]$.

Definitions and Notation

- For a $G = (V, E)$ on n vertices, enumerate its vertices, thus identifying $V = [n]$.
- To each vertex of $v \in V(G)$, associate a variable x_v.

Definitions and Notation

- For a $G = (V, E)$ on n vertices, enumerate its vertices, thus identifying $V = [n]$.
- To each vertex of $v \in V(G)$, associate a variable x_v.
- Define the **graph polynomial** f_G of G as follows:

$$f_G(x_1, x_2, \cdots, x_n) = \prod_{\substack{i<j \\ \{v_i, v_j\} \in E(G)}} (x_i - x_j).$$

Definitions and Notation

Definitions

- A **vertex coloring** of a graph $G = (V, E)$ is a map $c : V \to C$ where C is a set of colors.

Definitions and Notation

Definitions

- A **vertex coloring** of a graph $G = (V, E)$ is a map $c : V \to C$ where C is a set of colors.
- A **proper** vertex coloring is a vertex coloring such that $c(u) \neq c(v)$ whenever $\{u, v\} \in E(G)$.

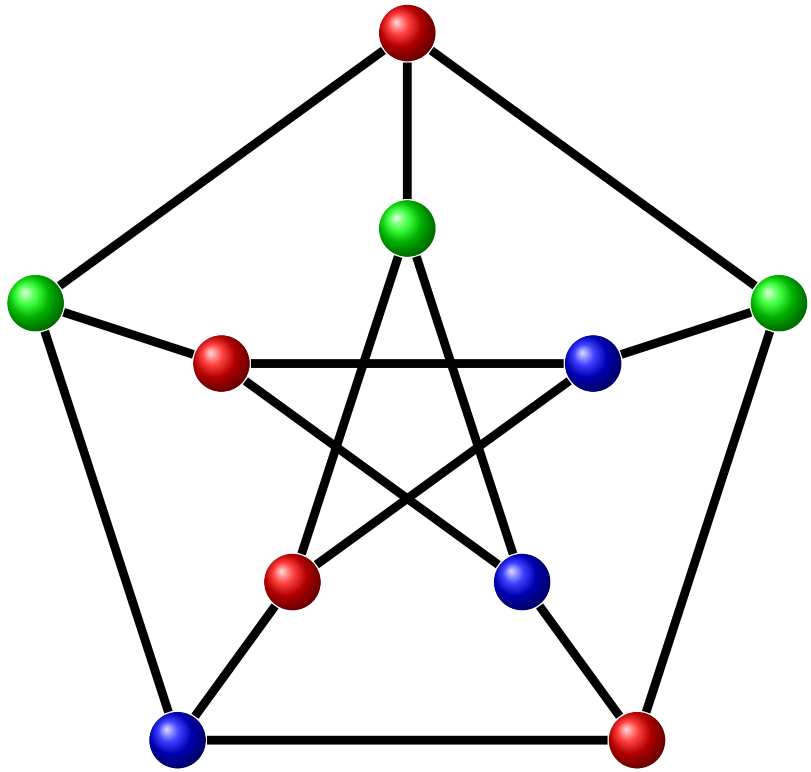
Definitions and Notation

Definitions

- A **vertex coloring** of a graph $G = (V, E)$ is a map $c : V \to C$ where C is a set of colors.
- A **proper** vertex coloring is a vertex coloring such that $c(u) \neq c(v)$ whenever $\{u, v\} \in E(G)$.
- A graph G is k-**colorable** if there exists a proper coloring of G that uses k colors or less.

Example: the Petersen Graph

- A proper coloring of the Petersen Graph:
- The Petersen Graph is 3-colorable.
- It can be proven that the Petersen graph is not 2-colorable.



Graph Coloring

Theorem (Alon)

A graph $G = (V, E)$ is not k-colorable if and only if the graph polynomial f_G lies in the ideal generated by $\{x_v^k - 1 : v \in V\}$.

Graph Coloring

Theorem (Alon)

A graph $G = (V, E)$ is not k-colorable if and only if the graph polynomial f_G lies in the ideal generated by $\{x_v^k - 1 : v \in V\}$.

Proof

Recall the graph polynomial is defined as:

$$f_G(x_1, x_2, \cdots, x_n) = \prod_{\substack{i<j \\ \{v_i, v_j\} \in E(G)}} (x_i - x_j).$$

Graph Coloring

Theorem

A graph $G = (V, E)$ is not k-colorable if and only if the graph polynomial f_G lies in the ideal generated by $\{x_v^k - 1 : v \in V\}$.

Proof

$\Longrightarrow$

- First, suppose G is not k-colorable.

Graph Coloring

Theorem

A graph $G = (V, E)$ is not k-colorable if and only if the graph polynomial f_G lies in the ideal generated by $\{x_v^k - 1 : v \in V\}$.

Proof

$\Longrightarrow$

- First, suppose G is not k-colorable.
- Let A be the set of all kth roots of unity.

Graph Coloring

Theorem

A graph $G = (V, E)$ is not k-colorable if and only if the graph polynomial f_G lies in the ideal generated by $\{x_v^k - 1 : v \in V\}$.

Proof

$\Longrightarrow$

- First, suppose G is not k-colorable.
- Let A be the set of all kth roots of unity.
- For each $v \in V$, define

$$g_v(x_v) = \prod_{a \in A}(x_v - a) = x_v^k - 1.$$

Graph Coloring

Theorem

A graph $G = (V, E)$ is not k-colorable if and only if the graph polynomial f_G lies in the ideal generated by $\{x_v^k - 1 : v \in V\}$.

Proof

$\Longrightarrow$

- First, suppose G is not k-colorable.
- Let A be the set of all kth roots of unity.
- For each $v \in V$, define

$$g_v(x_v) = \prod_{a \in A}(x_v - a) = x_v^k - 1.$$

- Note that any coloring c of G gives an evaluation of the polynomial f_G, namely $f_G(c(x_1), \cdots, c(x_n))$.

Graph Coloring

Theorem

A graph $G = (V, E)$ is not k-colorable if and only if the graph polynomial f_G lies in the ideal generated by $\{x_v^k - 1 : v \in V\}$.

Proof

$\Longrightarrow$

- First, suppose G is not k-colorable.
- Let A be the set of all kth roots of unity.
- For each $v \in V$, define

$$g_v(x_v) = \prod_{a \in A}(x_v - a) = x_v^k - 1.$$

- Note that any coloring c of G gives an evaluation of the polynomial f_G, namely $f_G(c(x_1), \cdots, c(x_n))$.
- G is not k-colorable, so any coloring of its vertices with the kth roots of unity has two adjacent vertices sharing the same color.

Graph Coloring

Theorem

A graph $G = (V, E)$ is not k-colorable if and only if the graph polynomial f_G lies in the ideal generated by $\{x_v^k - 1 : v \in V\}$.

Proof

$\Longrightarrow$

- First, suppose G is not k-colorable.
- Let A be the set of all kth roots of unity.
- For each $v \in V$, define

$$g_v(x_v) = \prod_{a \in A}(x_v - a) = x_v^k - 1.$$

- Note that any coloring c of G gives an evaluation of the polynomial f_G, namely $f_G(c(x_1), \cdots, c(x_n))$.
- G is not k-colorable, so any coloring of its vertices with the kth roots of unity has two adjacent vertices sharing the same color.
- Then the graph polynomial f_G vanishes for any assignment of elements in A^n to $(x_1, \cdots, x_n)$.

Graph Coloring

Theorem

A graph $G = (V, E)$ is not k-colorable if and only if the graph polynomial f_G lies in the ideal generated by $\{x_v^k - 1 : v \in V\}$.

Proof

$\Longrightarrow$

- Hence, it vanishes at all common zeros of g_v for all $v \in$ V.

Graph Coloring

Theorem

A graph $G = (V, E)$ is not k-colorable if and only if the graph polynomial f_G lies in the ideal generated by $\{x_v^k - 1 : v \in V\}$.

Proof

$\Longrightarrow$

- Hence, it vanishes at all common zeros of g_v for all $v \in$ V.
- The result follows from the Combinatorial Nullstellensatz I.

Graph Coloring

Theorem

A graph $G = (V, E)$ is not k-colorable if and only if the graph polynomial f_G lies in the ideal generated by $\{x_v^k - 1 : v \in V\}$.

Proof

$\Longrightarrow$

- Hence, it vanishes at all common zeros of g_v for all $v \in V$.
- The result follows from the Combinatorial Nullstellensatz I.

$\Longleftarrow$

- Suppose that f_G is in the specified ideal.

Graph Coloring

Theorem

A graph $G = (V, E)$ is not k-colorable if and only if the graph polynomial f_G lies in the ideal generated by $\{x_v^k - 1 : v \in V\}$.

Proof

$\Longrightarrow$

- Hence, it vanishes at all common zeros of g_v for all $v \in V$.
- The result follows from the Combinatorial Nullstellensatz I.

$\Longleftarrow$

- Suppose that f_G is in the specified ideal.
- Then, it is a combination of the polynomials $x_v^k - 1$, $v \in V$.

Graph Coloring

Theorem

A graph $G = (V, E)$ is not k-colorable if and only if the graph polynomial f_G lies in the ideal generated by $\{x_v^k - 1 : v \in V\}$.

Proof

$\Longrightarrow$

- Hence, it vanishes at all common zeros of g_v for all $v \in V$.
- The result follows from the Combinatorial Nullstellensatz I.

$\Longleftarrow$

- Suppose that f_G is in the specified ideal.
- Then, it is a combination of the polynomials $x_v^k - 1$, $v \in V$.
- Hence, f_G vanishes whenever each x_v attains a value that is a kth root of unity.

Graph Coloring

Theorem

A graph $G = (V, E)$ is not k-colorable if and only if the graph polynomial f_G lies in the ideal generated by $\{x_v^k - 1 : v \in V\}$.

Proof

$\Longrightarrow$

- Hence, it vanishes at all common zeros of g_v for all $v \in V$.
- The result follows from the Combinatorial Nullstellensatz I.

$\Longleftarrow$

- Suppose that f_G is in the specified ideal.
- Then, it is a combination of the polynomials $x_v^k - 1$, $v \in V$.
- Hence, f_G vanishes whenever each x_v attains a value that is a kth root of unity.
- Thus, every coloring of f_G with the kth roots of unity makes f_G vanish.

Graph Coloring

Theorem

A graph $G = (V, E)$ is not k-colorable if and only if the graph polynomial f_G lies in the ideal generated by $\{x_v^k - 1 : v \in V\}$.

Proof

$\Longrightarrow$

- Hence, it vanishes at all common zeros of g_v for all $v \in V$.
- The result follows from the Combinatorial Nullstellensatz I.

$\Longleftarrow$

- Suppose that f_G is in the specified ideal.
- Then, it is a combination of the polynomials $x_v^k - 1$, $v \in V$.
- Hence, f_G vanishes whenever each x_v attains a value that is a kth root of unity.
- Thus, every coloring of f_G with the kth roots of unity makes f_G vanish.
- Hence, for any such coloring, there is an edge whose adjacent vertices are colored the same.

Graph Coloring

Theorem

A graph $G = (V, E)$ is not k-colorable if and only if the graph polynomial f_G lies in the ideal generated by $\{x_v^k - 1 : v \in V\}$.

Proof

$\Longrightarrow$

- Hence, it vanishes at all common zeros of g_v for all $v \in V$.
- The result follows from the Combinatorial Nullstellensatz I.

$\Longleftarrow$

- Suppose that f_G is in the specified ideal.
- Then, it is a combination of the polynomials $x_v^k - 1$, $v \in V$.
- Hence, f_G vanishes whenever each x_v attains a value that is a kth root of unity.
- Thus, every coloring of f_G with the kth roots of unity makes f_G vanish.
- Hence, for any such coloring, there is an edge whose adjacent vertices are colored the same.
- So G is not k-colorable. $\square$

New Applications

Hypergraph-related Definitions

Definitions

1. A **hypergraph** $H = (V, E)$ is the finite set V (vertices) and a collection E of non-empty subsets of vertices (hyperedges).

Hypergraph-related Definitions

Definitions

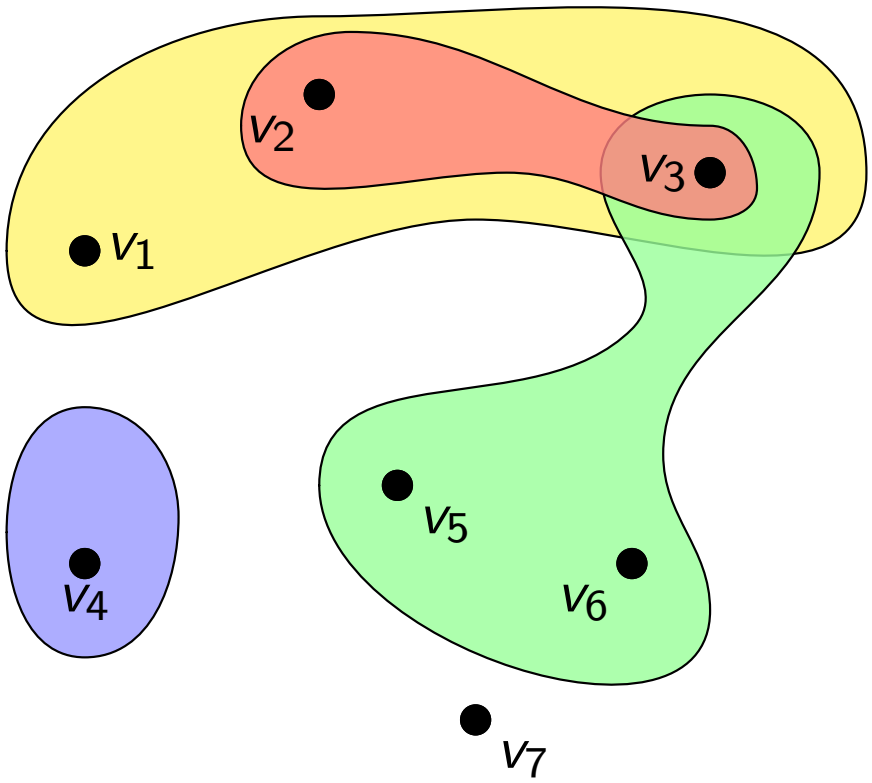
1. A **hypergraph** $H = (V, E)$ is the finite set V (vertices) and a collection E of non-empty subsets of vertices (hyperedges).
2. A hypergraph is m-**uniform** for some positive integer m if each hyperedge has cardinality m.

Hypergraph-related Definitions

Definitions

1. A **hypergraph** $H = (V, E)$ is the finite set V (vertices) and a collection E of non-empty subsets of vertices (hyperedges).
2. A hypergraph is m-**uniform** for some positive integer m if each hyperedge has cardinality m.
3. We say that a hypergraph H is k-**colorable** if there exists a coloring of its vertices with k or less colors such that no hyperedge is monochromatic.

Example of a Hypergraph



Hypergraph Coloring

Theorem (Alon)

A 3-uniform hypergraph $H = (V, E)$ is not 2-colorable if and only if the polynomial

$$g_H = \prod_{e \in E} \left(\left(\sum_{v \in e} x_v \right)^2 - 9 \right)$$

lies in the ideal generated by $\{x_v^2 - 1 : v \in V\}$.

Hypergraph Coloring

Theorem (Alon)

A 3-uniform hypergraph $H = (V, E)$ is not 2-colorable if and only if the polynomial

$$g_H = \prod_{e \in E} \left(\left(\sum_{v \in e} x_v \right)^2 - 9 \right)$$

lies in the ideal generated by $\{x_v^2 - 1 : v \in V\}$.

Theorem

An m-uniform hypergraph is not k-colorable if and only if the polynomial

$$g_H = \prod_{e \in E} \left(\left(\sum_{v \in e} x_v \right)^k - m^k \right)$$

lies in the ideal generated by $\{x_v^k - 1 : v \in V\}$.

Hypergraph Coloring

Theorem (Alon)

A 3-uniform hypergraph $H = (V, E)$ is not 2-colorable if and only if the polynomial

$$g_H = \prod_{e \in E} \left(\left(\sum_{v \in e} x_v \right)^2 - 9 \right)$$

lies in the ideal generated by $\{x_v^2 - 1 : v \in V\}$.

Hypergraph Coloring

Theorem (Alon)

A 3-uniform hypergraph $H = (V, E)$ is not 2-colorable if and only if the polynomial

$$g_H = \prod_{e \in E} \left(\left(\sum_{v \in e} x_v \right)^2 - 9 \right)$$

lies in the ideal generated by $\{x_v^2 - 1 : v \in V\}$.

Proof

$\Longrightarrow$

- Suppose H is not 2-colorable.

Hypergraph Coloring

Theorem (Alon)

A 3-uniform hypergraph $H = (V, E)$ is not 2-colorable if and only if the polynomial

$$g_H = \prod_{e \in E} \left(\left(\sum_{v \in e} x_v \right)^2 - 9 \right)$$

lies in the ideal generated by $\{x_v^2 - 1 : v \in V\}$.

Proof

$\Longrightarrow$

- Suppose H is not 2-colorable.
- Then, any coloring with the colors in $\{1, -1\}$ produces a monochromatic hyperedge.

Hypergraph Coloring

Theorem (Alon)

A 3-uniform hypergraph $H = (V, E)$ is not 2-colorable if and only if the polynomial

$$g_H = \prod_{e \in E} \left(\left(\sum_{v \in e} x_v \right)^2 - 9 \right)$$

lies in the ideal generated by $\{x_v^2 - 1 : v \in V\}$.

Proof

$\Longrightarrow$

- Suppose H is not 2-colorable.
- Then, any coloring with the colors in $\{1, -1\}$ produces a monochromatic hyperedge.
- So, for any such coloring, there is a hyperedge all three of whose vertices are colored either 1 or -1.

Hypergraph Coloring

Theorem (Alon)

A 3-uniform hypergraph $H = (V, E)$ is not 2-colorable if and only if the polynomial

$$g_H = \prod_{e \in E} \left(\left(\sum_{v \in e} x_v \right)^2 - 9 \right)$$

lies in the ideal generated by $\{x_v^2 - 1 : v \in V\}$.

Proof

$\Longrightarrow$

- Suppose H is not 2-colorable.
- Then, any coloring with the colors in $\{1, -1\}$ produces a monochromatic hyperedge.
- So, for any such coloring, there is a hyperedge all three of whose vertices are colored either 1 or -1.
- Hence g_H vanishes for any such coloring.

Hypergraph Coloring

Theorem (Alon)

A 3-uniform hypergraph $H = (V, E)$ is not 2-colorable if and only if the polynomial

$$g_H = \prod_{e \in E} \left(\left(\sum_{v \in e} x_v \right)^2 - 9 \right)$$

lies in the ideal generated by $\{x_v^2 - 1 : v \in V\}$.

Proof

$\Longrightarrow$

- Suppose H is not 2-colorable.
- Then, any coloring with the colors in $\{1, -1\}$ produces a monochromatic hyperedge.
- So, for any such coloring, there is a hyperedge all three of whose vertices are colored either 1 or -1.
- Hence g_H vanishes for any such coloring.
- Define $g_v = (x_v - 1)(x_v + 1) = x_v^2 - 1$ for all $v \in V$.

Hypergraph Coloring

Theorem (Alon)

A 3-uniform hypergraph $H = (V, E)$ is not 2-colorable if and only if the polynomial

$$g_H = \prod_{e \in E} \left(\left(\sum_{v \in e} x_v \right)^2 - 9 \right)$$

lies in the ideal generated by $\{x_v^2 - 1 : v \in V\}$.

Proof

$\Longrightarrow$

- Suppose H is not 2-colorable.
- Then, any coloring with the colors in $\{1, -1\}$ produces a monochromatic hyperedge.
- So, for any such coloring, there is a hyperedge all three of whose vertices are colored either 1 or -1.
- Hence g_H vanishes for any such coloring.
- Define $g_v = (x_v - 1)(x_v + 1) = x_v^2 - 1$ for all $v \in V$.
- By the Combinatorial Nullstellensatz I, g_H is in the specified ideal.

Hypergraph Coloring

Theorem (Alon)

A 3-uniform hypergraph $H = (V, E)$ is not 2-colorable if and only if the polynomial

$$g_H = \prod_{e \in E} \left(\left(\sum_{v \in e} x_v \right)^2 - 9 \right)$$

lies in the ideal generated by $\{x_v^2 - 1 : v \in V\}$.

Proof

$\Longleftarrow$

- Suppose g_H is in the specified ideal.

Hypergraph Coloring

Theorem (Alon)

A 3-uniform hypergraph $H = (V, E)$ is not 2-colorable if and only if the polynomial

$$g_H = \prod_{e \in E} \left(\left(\sum_{v \in e} x_v \right)^2 - 9 \right)$$

lies in the ideal generated by $\{x_v^2 - 1 : v \in V\}$.

Proof

$\Longleftarrow$

- Suppose g_H is in the specified ideal.
- Then it vanishes whenever each x_v attains a value in $\{1, -1\}$.

Hypergraph Coloring

Theorem (Alon)

A 3-uniform hypergraph $H = (V, E)$ is not 2-colorable if and only if the polynomial

$$g_H = \prod_{e \in E} \left(\left(\sum_{v \in e} x_v \right)^2 - 9 \right)$$

lies in the ideal generated by $\{x_v^2 - 1 : v \in V\}$.

Proof

$\Longleftarrow$

- Suppose g_H is in the specified ideal.
- Then it vanishes whenever each x_v attains a value in $\{1, -1\}$.
- So, for some edge, we have

$$\left(\sum_{v \in e} c(x_v) \right)^2 = 9.$$

Hypergraph Coloring

Theorem (Alon)

A 3-uniform hypergraph $H = (V, E)$ is not 2-colorable if and only if the polynomial

$$g_H = \prod_{e \in E} \left(\left(\sum_{v \in e} x_v \right)^2 - 9 \right)$$

lies in the ideal generated by $\{x_v^2 - 1 : v \in V\}$.

Proof

$\Longleftarrow$

- Suppose g_H is in the specified ideal.
- Then it vanishes whenever each x_v attains a value in $\{1, -1\}$.
- So, for some edge, we have

$$\left(\sum_{v \in e} c(x_v) \right)^2 = 9.$$

- So there is a monochromatic hyperedge in every coloring by $\{1, -1\}$.

Hypergraph Coloring

Theorem (Alon)

A 3-uniform hypergraph $H = (V, E)$ is not 2-colorable if and only if the polynomial

$$g_H = \prod_{e \in E} \left(\left(\sum_{v \in e} x_v \right)^2 - 9 \right)$$

lies in the ideal generated by $\{x_v^2 - 1 : v \in V\}$.

Proof

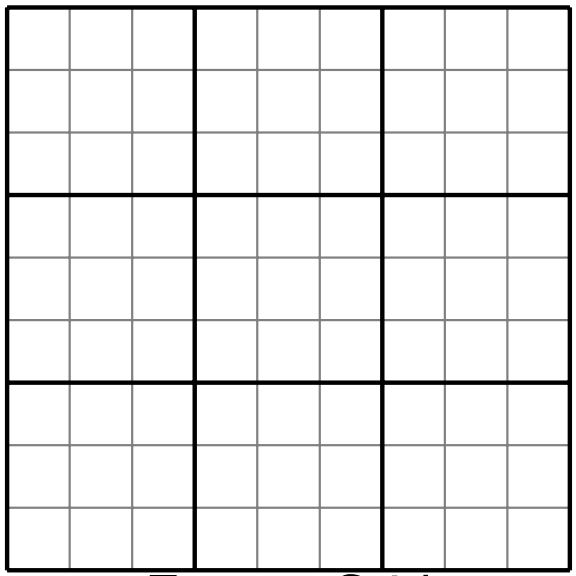
$\Longleftarrow$

- Suppose g_H is in the specified ideal.
- Then it vanishes whenever each x_v attains a value in $\{1, -1\}$.
- So, for some edge, we have

$$\left(\sum_{v \in e} c(x_v) \right)^2 = 9.$$

- So there is a monochromatic hyperedge in every coloring by $\{1, -1\}$.
- Therefore, H is not 2-colorable. $\square$

Sudoku



Empty Grid

Sudoku

			4					
	5		7					9
			9			6		1
9	6	4					8	
		7				9		
3	1				2			
			8					7
2						1		3

Grid with Restrictions

Sudoku

1	8	9	4	2	6	7	3	5
6	5	2	7	1	3	8	4	9
7	4	3	9	8	5	6	2	1
9	6	4	1	5	7	3	8	2
5	2	7	3	4	8	9	1	6
8	3	1	2	6	9	5	7	4
3	1	5	6	7	2	4	9	8
4	9	6	8	3	1	2	5	7
2	7	8	5	9	4	1	6	3

Completed Puzzle

Sudoku Graph

- We define the **Sudoku graph** S by associating a vertex to each cell in the grid and placing an edge between two vertices if and only if they are in the same *row* or the same *column* or the same *block*.

Sudoku Graph

- We define the **Sudoku graph** S by associating a vertex to each cell in the grid and placing an edge between two vertices if and only if they are in the same *row* or the same *column* or the same *block*.
- S has 81 vertices and each cell/row/block is associated to a complete subgraph on 9 vertices.

Sudoku Graph

- We define the **Sudoku graph** S by associating a vertex to each cell in the grid and placing an edge between two vertices if and only if they are in the same *row* or the same *column* or the same *block*.
- S has 81 vertices and each cell/row/block is associated to a complete subgraph on 9 vertices.
- There are 27 such subgraphs in total; denote each of them by H_i, where $i \in [27]$.

Sudoku Graph

- Restrictions in a puzzle correspond to a partial coloring of vertices in the Sudoku graph S.

Sudoku Graph

- Restrictions in a puzzle correspond to a partial coloring of vertices in the Sudoku graph S.
- Let S_R denote the graph S with the partial vertex coloring that corresponds to the restrictions, denoted by R, of a given puzzle.

Sudoku Graph

- Restrictions in a puzzle correspond to a partial coloring of vertices in the Sudoku graph S.
- Let S_R denote the graph S with the partial vertex coloring that corresponds to the restrictions, denoted by R, of a given puzzle.
- A puzzle with restrictions R has solutions if and only if S_R is 9-colorable with the colors in $[9]$.

Setup

- To each vertex v of S, we will associate a variable x_v.

Setup

- To each vertex v of S, we will associate a variable x_v.
- For each $i \in [27]$, let:

$$q_i = \prod_{\substack{v<w \\ \{v,w\} \in E(H_i)}} (x_v - x_w).$$

Setup

- To each vertex v of S, we will associate a variable x_v.
- For each $i \in [27]$, let:

$$q_i = \prod_{\substack{v<w \\ \{v,w\} \in E(H_i)}} (x_v - x_w).$$

- For each vertex $u \in V(S)$ that must be colored $k_u \in [9]$ by restrictions, let $H_{i_1}, H_{i_2}, H_{i_3}$ be the subgraphs in which u appears.

Setup

- To each vertex v of S, we will associate a variable x_v.
- For each $i \in [27]$, let:

$$q_i = \prod_{\substack{v<w \\ \{v,w\} \in E(H_i)}} (x_v - x_w).$$

- For each vertex $u \in V(S)$ that must be colored $k_u \in [9]$ by restrictions, let $H_{i_1}, H_{i_2}, H_{i_3}$ be the subgraphs in which u appears.
- For each of these subgraphs, we modify its polynomial by replacing the variable x_u by the value k_u.

Setup

- To each vertex v of S, we will associate a variable x_v.
- For each $i \in [27]$, let:

$$q_i = \prod_{\substack{v<w \\ \{v,w\} \in E(H_i)}} (x_v - x_w).$$

- For each vertex $u \in V(S)$ that must be colored $k_u \in [9]$ by restrictions, let $H_{i_1}, H_{i_2}, H_{i_3}$ be the subgraphs in which u appears.
- For each of these subgraphs, we modify its polynomial by replacing the variable x_u by the value k_u.
- We modify the polynomials repeatedly for all restrictions, keeping all the changes in previous steps.

Setup

- To each vertex v of S, we will associate a variable x_v.
- For each $i \in [27]$, let:

$$q_i = \prod_{\substack{v<w \\ \{v,w\} \in E(H_i)}} (x_v - x_w).$$

- For each vertex $u \in V(S)$ that must be colored $k_u \in [9]$ by restrictions, let $H_{i_1}, H_{i_2}, H_{i_3}$ be the subgraphs in which u appears.
- For each of these subgraphs, we modify its polynomial by replacing the variable x_u by the value k_u.
- We modify the polynomials repeatedly for all restrictions, keeping all the changes in previous steps.
- We keep polynomials unchanged if a cell does not have a restriction.

Setup

- To each vertex v of S, we will associate a variable x_v.
- For each $i \in [27]$, let:

$$q_i = \prod_{\substack{v<w \\ \{v,w\} \in E(H_i)}} (x_v - x_w).$$

- For each vertex $u \in V(S)$ that must be colored $k_u \in [9]$ by restrictions, let $H_{i_1}, H_{i_2}, H_{i_3}$ be the subgraphs in which u appears.
- For each of these subgraphs, we modify its polynomial by replacing the variable x_u by the value k_u.
- We modify the polynomials repeatedly for all restrictions, keeping all the changes in previous steps.
- We keep polynomials unchanged if a cell does not have a restriction.
- After doing so for all vertices, let f_i be the new modified polynomials for all $i \in [27]$.

Theorem

- Define

$$h_R = \prod_{i=1}^{27} f_i.$$

Theorem

- Define

$$h_R = \prod_{i=1}^{27} f_i.$$

- Pick any bijection between $\{1, \cdots, 9\}$ and the 9th roots of unity.

Theorem

- Define
$$h_R = \prod_{i=1}^{27} f_i.$$
- Pick any bijection between $\{1, \cdots, 9\}$ and the 9th roots of unity.

Theorem

S_R is not 9-colorable if and only if h_R lies in the ideal generated by $\{x_v^9 - 1 : v \in [81]\}$.

Theorem

- Define
$$h_R = \prod_{i=1}^{27} f_i.$$
- Pick any bijection between $\{1, \cdots, 9\}$ and the 9th roots of unity.

Theorem

S_R is not 9-colorable if and only if h_R lies in the ideal generated by $\{x_v^9 - 1 : v \in [81]\}$.

Proof

Exercise.

Other Applications

- Minimum Bandwidth of a Graph
- f-choosability of Graphs
- Lucky Labeling

Questions?