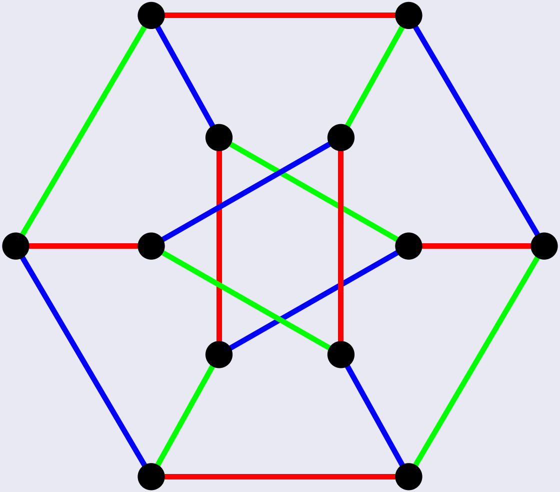
Siegel's theorem, edge coloring, and a holant dichotomy

Tyson Williams
(University of Wisconsin-Madison)

Joint with:
Jin-Yi Cai and Heng Guo
(University of Wisconsin-Madison)

Appeared at FOCS 2014

Definition



Edge Coloring–Decision Problem

Problem: κ-EdgeColoring
Input: A graph G
Output: "YES" if G has an edge coloring using at most κ colors and "NO" otherwise

Problem: κ-EdgeColoring
Input: A graph G
Output: "YES" if G has an edge coloring using at most κ colors and "NO" otherwise

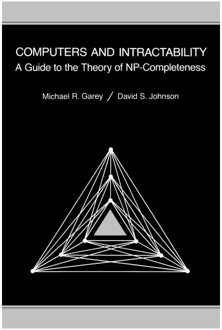
Obviously no edge coloring using less than Δ colors.

Theorem (Vizing [1964])

An edge coloring using at most $\Delta + 1$ colors exists.

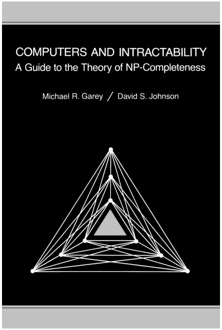
Edge Coloring–Decision Problem

What about $\kappa = \Delta$?

Complexity stated as an open problem in  [1979]

Edge Coloring–Decision Problem

What about $\kappa = \Delta$?

Complexity stated as an open problem in 

[1979]

Theorem (Holyer [1981])

3-EdgeColoring *is* **NP-hard** *over* 3*-regular graphs.*

Theorem (Leven, Galil [1983])

r-EdgeColoring *is* **NP-hard** *over* r*-regular graphs for all* $r \geq 3$.

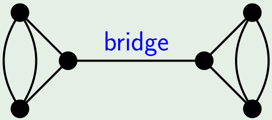
Edge Coloring–Decision Problem

Lemma (Parity Condition)

r-regular graph with a bridge $\Longrightarrow$ no edge coloring using r colors exists

Example

This graph has no edge coloring using 3 colors.



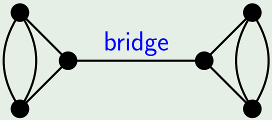
Edge Coloring–Decision Problem

Lemma (Parity Condition)

r-regular graph with a bridge $\implies$ no edge coloring using r colors exists

Example

This graph has no edge coloring using 3 colors.



Theorem (Tait [1880])

For planar 3-regular bridgeless graphs,
edge coloring using 3 colors exists $\iff$ Four Color (Conjecture) Theorem.

Corollary

For planar 3-regular graphs,
edge coloring using 3 colors exists $\iff$ bridgeless.

Edge Coloring–Decision Problem

Trivial Algorithm

$\kappa \neq \Delta$

NP-hard

$\kappa = r$ over
r-regular graphs

Simple Algorithm (Complex Proof)

$\kappa = 3$ over planar
3-regular graphs

Edge Coloring–Counting Problem

Problem: $\#\kappa$-EdgeColoring
Input: A graph G
Output: Number of edge colorings of G using at most κ colors

Edge Coloring–Counting Problem

Problem: $\#\kappa$-EdgeColoring
Input: A graph G
Output: Number of edge colorings of G using at most κ colors

Theorem (Cai, Guo, W [2014])

*$\#\kappa$-EdgeColoring is **#P-hard** over planar r-regular graphs for all $\kappa \geq r \geq 3$.*

Tractable when $\kappa \geq r \geq 3$ does not hold:

- If $\kappa < r$, then no edge colorings
- If $r < 3$, then only trivial graphs (paths and cycles)

Parallel edges allowed (and necessary when $r > 5$).

Proved in the framework of Holant problems in two cases:

1. $\kappa = r$, and
2. $\kappa > r$.

Holant Problems

Definition

Holant problems are counting problems defined over graphs that can be specified by local constraint functions on the vertices, edges, or both.

Example (Natural Holant Problems)

independent sets, vertex covers, edge covers, cycle covers, vertex colorings, edge colorings, matchings, perfect matchings, and Eulerian orientations.

NON-examples: Hamiltonian cycles and spanning trees.

NOT local.

Abundance of Holant Problems

Equivalent to:

- counting read-twice constraint satisfaction problems,
- contraction of tensor networks, and
- partition function of graphical models (in Forney normal form).

Generalizes:

- simulating quantum circuits,
- counting graph homomorphisms,
- all manner of partition functions including
  - Ising model,
  - Potts model,
  - edge-coloring model.

#κ-EdgeColoring as a Holant Problem

Let AD_3 denote the local constraint function

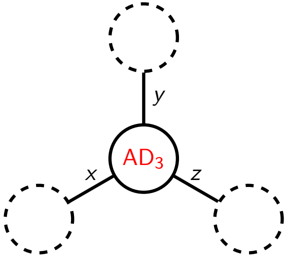
$$\text{AD}_3(x, y, z) = \begin{cases} 1 & \text{if } x, y, z \in [\kappa] \text{ are distinct} \\ 0 & \text{otherwise.} \end{cases}$$

$\#\kappa$-EdgeColoring as a Holant Problem

Let AD_3 denote the local constraint function

$$\mathrm{AD}_3(x, y, z) = \begin{cases} 1 & \text{if } x, y, z \in [\kappa] \text{ are distinct} \\ 0 & \text{otherwise.} \end{cases}$$

Place AD_3 at each vertex with incident edges x, y, z in a 3-regular graph G.

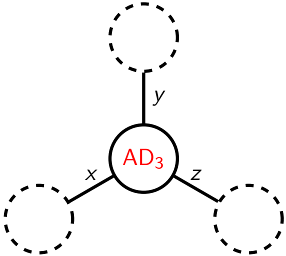


#κ-EdgeColoring as a Holant Problem

Let AD_3 denote the local constraint function

$$\mathrm{AD}_3(x,y,z) = \begin{cases} 1 & \text{if } x,y,z \in [\kappa] \text{ are distinct} \\ 0 & \text{otherwise.} \end{cases}$$

Place AD_3 at each vertex with incident edges x, y, z in a 3-regular graph G.



Then we evaluate the sum of product

$$\mathrm{Holant}_\kappa(G; \mathrm{AD}_3) = \sum_{\sigma: E(G)\to[\kappa]} \prod_{v\in V(G)} \mathrm{AD}_3\left(\sigma\mid_{E(v)}\right).$$

Clearly $\mathrm{Holant}_\kappa(-; \mathrm{AD}_3)$ computes #κ-EdgeColoring.

More Explicit Examples

Four examples with $\kappa = 2$:

$$\mathrm{Holant}_2(G; f) \text{ counts } \begin{cases} \text{matchings} & \text{when } f = \text{AT-MOST-ONE}_r \\ \text{perfect matchings} & \text{when } f = \text{EXACTLY-ONE}_r \\ \text{cycle covers} & \text{when } f = \text{EXACTLY-TWO}_r \\ \text{edge covers} & \text{when } f = \text{OR}_r \end{cases}$$

$$\mathrm{Holant}_\kappa(G; f) = \sum_{\sigma : E(G) \to \{0,1\}} \prod_{v \in V(G)} f\left(\sigma\,|_{E(v)}\right).$$

In general, we consider all local constraint functions

$$f(x,y,z) = \langle a,b,c\rangle = \begin{cases} a & \text{if } x=y=z \qquad\qquad \text{(all equal)} \\ b & \text{otherwise} \\ c & \text{if } x \neq y \neq z \neq x \qquad \text{(all distinct).} \end{cases}$$

The Holant problem is to compute

$$\text{Holant}_\kappa(G; f) = \sum_{\sigma: E(G)\to[\kappa]} \prod_{v\in V(G)} f\left(\sigma\mid_{E(v)}\right).$$

Note $\text{AD}_3 = \langle 0,0,1\rangle$.

Theorem (Main Theorem)

For any $\kappa \geq 3$ and any $a, b, c \in \mathbb{C}$,
the problem of computing $\text{Holant}_\kappa(-; \langle a, b, c \rangle)$ *is in* **P** *or* **#P-hard**,
even when the input is restricted to planar graphs.

Theorem (Main Theorem)

For any $\kappa \geq 3$ and any $a, b, c \in \mathbb{C}$,
the problem of computing $\text{Holant}_\kappa(-; \langle a, b, c\rangle)$ *is in* **P** *or* **#P-hard**,
even when the input is restricted to planar graphs.

Recall $\#\kappa$-EdgeColoring is the special case $\langle a, b, c\rangle = \langle 0, 0, 1\rangle$.

Let's prove the theorem for $\kappa = 3$ and $\langle a, b, c\rangle = \langle 0, 0, 1\rangle$.

Nontrivial Examples of Tractable Holant Problems

1. On domain size $\kappa = 3$,
   $\text{Holant}_3(-; \langle -5, -2, 4 \rangle)$ is in **P**.

1. On domain size $\kappa = 3$,
   $\text{Holant}_3(-; \langle -5, -2, 4 \rangle)$ is in **P**.

   Since

   $$\langle -5, -2, 4 \rangle = \left[(1, -2, -2)^{\otimes 3} + (-2, 1, -2)^{\otimes 3} + (-2, -2, 1)^{\otimes 3}\right],$$

   do a holographic transformation by the orthogonal matrix
   $T = \frac{1}{3}\left[\begin{smallmatrix} 1 & -2 & -2 \\ -2 & 1 & -2 \\ -2 & -2 & 1 \end{smallmatrix}\right]$.

Nontrivial Examples of Tractable Holant Problems

1. On domain size $\kappa = 3$,
   $\text{Holant}_3(-; \langle -5, -2, 4 \rangle)$ is in **P**.

   Since

   $$\langle -5, -2, 4 \rangle = \left[(1, -2, -2)^{\otimes 3} + (-2, 1, -2)^{\otimes 3} + (-2, -2, 1)^{\otimes 3} \right],$$

   do a holographic transformation by the orthogonal matrix
   $T = \frac{1}{3} \begin{bmatrix} 1 & -2 & -2 \\ -2 & 1 & -2 \\ -2 & -2 & 1 \end{bmatrix}$.

2. In general,
   $\text{Holant}_\kappa(G; \langle \kappa^2 - 6\kappa + 4, -2(\kappa - 2), 4 \rangle)$ is in **P**.

Nontrivial Examples of Tractable Holant Problems

1. On domain size $\kappa = 3$,
   $\text{Holant}_3(-; \langle -5, -2, 4 \rangle)$ is in **P**.

   Since

   $$\langle -5, -2, 4 \rangle = \left[(1, -2, -2)^{\otimes 3} + (-2, 1, -2)^{\otimes 3} + (-2, -2, 1)^{\otimes 3} \right],$$

   do a holographic transformation by the orthogonal matrix
   $T = \frac{1}{3} \left[\begin{smallmatrix} 1 & -2 & -2 \\ -2 & 1 & -2 \\ -2 & -2 & 1 \end{smallmatrix} \right]$.

2. In general,
   $\text{Holant}_\kappa(G; \langle \kappa^2 - 6\kappa + 4, -2(\kappa - 2), 4 \rangle)$ is in **P**.

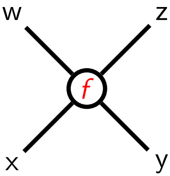
3. On domain size $\kappa = 4$,
   $\text{Holant}_4(G; \langle -3 - 4i, 1, -1 + 2i \rangle)$ is in **P**.

Hardness of $\text{Holant}_3(-; \text{AD}_3)$

Hardness of $\text{Holant}_3(-; \text{AD}_3)$ proved by the following reduction chain:

$$\begin{aligned} \#\mathbf{P} &\le_T \text{Holant}_3(-; \langle 2, 1, 0, 1, 0 \rangle) \\ &\le_T \text{Holant}_3(-; \langle 0, 1, 1, 0, 0 \rangle) \\ &\le_T \text{Holant}_3(-; \text{AD}_3) \end{aligned}$$

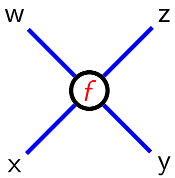
$$f\left(\begin{smallmatrix} w & z \\ x & y \end{smallmatrix}\right) = \langle a, b, c, d, e \rangle = \begin{cases} a & \text{if } w = x = y = z \\ b & \text{if } w = x \ne y = z \\ c & \text{if } w = y \ne x = z \\ d & \text{if } w = z \ne x = y \\ e & \text{otherwise.} \end{cases}$$



Hardness of $\text{Holant}_3(-; \text{AD}_3)$ proved by the following reduction chain:

$$\begin{aligned}\#\mathbf{P} &\le_T \text{Holant}_3(-; \langle 2, 1, 0, 1, 0\rangle) \\ &\le_T \text{Holant}_3(-; \langle 0, 1, 1, 0, 0\rangle) \\ &\le_T \text{Holant}_3(-; \text{AD}_3)\end{aligned}$$

$$f\left(\begin{smallmatrix} w & z \\ x & y \end{smallmatrix}\right) = \langle a, b, c, d, e\rangle = \begin{cases} a & \text{if } w = x = y = z \\ b & \text{if } w = x \neq y = z \\ c & \text{if } w = y \neq x = z \\ d & \text{if } w = z \neq x = y \\ e & \text{otherwise.} \end{cases}$$

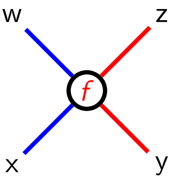


Hardness of Holant$_3$($-$; AD$_3$)

Hardness of Holant$_3$($-$; AD$_3$) proved by the following reduction chain:

$$\begin{aligned} \textbf{\#P} &\le_T \text{Holant}_3(-; \langle 2,1,0,1,0\rangle) \\ &\le_T \text{Holant}_3(-; \langle 0,1,1,0,0\rangle) \\ &\le_T \text{Holant}_3(-; \text{AD}_3) \end{aligned}$$

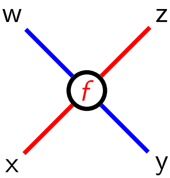
$$f\left(\begin{smallmatrix} w & z \\ x & y \end{smallmatrix}\right) = \langle a, b, c, d, e\rangle = \begin{cases} a & \text{if } w = x = y = z \\ b & \text{if } w = x \neq y = z \\ c & \text{if } w = y \neq x = z \\ d & \text{if } w = z \neq x = y \\ e & \text{otherwise.} \end{cases}$$



Hardness of $\text{Holant}_3(-; \text{AD}_3)$ proved by the following reduction chain:

$$\begin{aligned}\#\mathbf{P} &\leq_T \text{Holant}_3(-; \langle 2, 1, 0, 1, 0 \rangle) \\ &\leq_T \text{Holant}_3(-; \langle 0, 1, 1, 0, 0 \rangle) \\ &\leq_T \text{Holant}_3(-; \text{AD}_3)\end{aligned}$$

$$f\left(\begin{smallmatrix} w & z \\ x & y \end{smallmatrix}\right) = \langle a, b, c, d, e \rangle = \begin{cases} a & \text{if } w = x = y = z \\ b & \text{if } w = x \neq y = z \\ c & \text{if } w = y \neq x = z \\ d & \text{if } w = z \neq x = y \\ e & \text{otherwise.} \end{cases}$$

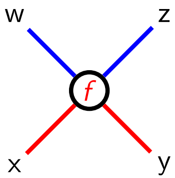


Hardness of $\text{Holant}_3(-; \text{AD}_3)$

Hardness of $\text{Holant}_3(-; \text{AD}_3)$ proved by the following reduction chain:

$$\begin{aligned} \#\mathbf{P} &\le_T \text{Holant}_3(-; \langle 2,1,0,1,0\rangle) \\ &\le_T \text{Holant}_3(-; \langle 0,1,1,0,0\rangle) \\ &\le_T \text{Holant}_3(-; \text{AD}_3) \end{aligned}$$

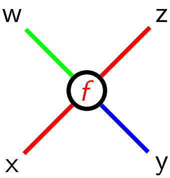
$$f\left(\begin{smallmatrix} w & z \\ x & y \end{smallmatrix}\right) = \langle a,b,c,d,e\rangle = \begin{cases} a & \text{if } w = x = y = z \\ b & \text{if } w = x \neq y = z \\ c & \text{if } w = y \neq x = z \\ d & \text{if } w = z \neq x = y \\ e & \text{otherwise.} \end{cases}$$



Hardness of $\text{Holant}_3(-; \text{AD}_3)$ proved by the following reduction chain:

$$\begin{aligned}\#\mathbf{P} &\leq_T \text{Holant}_3(-; \langle 2, 1, 0, 1, 0\rangle)\\ &\leq_T \text{Holant}_3(-; \langle 0, 1, 1, 0, 0\rangle)\\ &\leq_T \text{Holant}_3(-; \text{AD}_3)\end{aligned}$$

$$f\left(\begin{smallmatrix} w & z \\ x & y \end{smallmatrix}\right) = \langle a, b, c, d, e\rangle = \begin{cases} a & \text{if } w = x = y = z \\ b & \text{if } w = x \neq y = z \\ c & \text{if } w = y \neq x = z \\ d & \text{if } w = z \neq x = y \\ e & \text{otherwise.} \end{cases}$$



Hardness of $\text{Holant}_3(-; \text{AD}_3)$ proved by the following reduction chain:

$$\begin{aligned}\textbf{\#P} &\leq_T \text{Holant}_3(-; \langle 2,1,0,1,0\rangle)\\ &\leq_T \text{Holant}_3(-; \langle 0,1,1,0,0\rangle)\\ &\leq_T \text{Holant}_3(-; \text{AD}_3)\end{aligned}$$

- First reduction: From a **#P-hard** point on the Tutte polynomial.

Hardness of $\text{Holant}_3(-; \text{AD}_3)$ proved by the following reduction chain:

$$\begin{aligned}\#\mathbf{P} &\leq_T \text{Holant}_3(-; \langle 2,1,0,1,0\rangle)\\ &\leq_T \text{Holant}_3(-; \langle 0,1,1,0,0\rangle)\\ &\leq_T \text{Holant}_3(-; \text{AD}_3)\end{aligned}$$

- First reduction: From a **#P-hard** point on the Tutte polynomial.
- Second reduction: Via polynomial interpolation.

Hardness of $\text{Holant}_3(-; \text{AD}_3)$ proved by the following reduction chain:

$$\begin{aligned}\textbf{\#P} &\le_T \text{Holant}_3(-; \langle 2, 1, 0, 1, 0\rangle) \\ &\le_T \text{Holant}_3(-; \langle 0, 1, 1, 0, 0\rangle) \\ &\le_T \text{Holant}_3(-; \text{AD}_3)\end{aligned}$$

- First reduction: From a **#P-hard** point on the Tutte polynomial.
- Second reduction: Via polynomial interpolation.
- Third reduction: Via a gadget construction.

Hardness of $\text{Holant}_3(-; \text{AD}_3)$ proved by the following reduction chain:

$$\begin{aligned} \#\mathbf{P} &\le_T \text{Holant}_3(-; \langle 2,1,0,1,0 \rangle) \\ &\le_T \text{Holant}_3(-; \langle 0,1,1,0,0 \rangle) \\ &\le_T \text{Holant}_3(-; \text{AD}_3) \end{aligned}$$

- First reduction: From a **#P-hard** point on the Tutte polynomial.
- Second reduction: Via polynomial interpolation.
- Third reduction: Via a gadget construction.

Definition

The Tutte polynomial of an undirected graph G is

$$T(G;x,y) = \begin{cases} 1 & E(G) = \emptyset, \\ xT(G \setminus e; x, y) & e \in E(G) \text{ is a bridge}, \\ yT(G \setminus e; x, y) & e \in E(G) \text{ is a loop}, \\ T(G \setminus e; x, y) + T(G/e; x, y) & \text{otherwise}, \end{cases}$$

where $G \setminus e$ is the graph obtained by deleting e and G/e is the graph obtained by contracting e.

Definition

The Tutte polynomial of an undirected graph G is

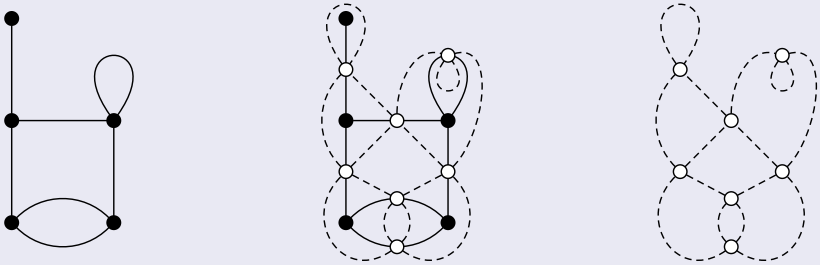
$$T(G;x,y) = \begin{cases} 1 & E(G) = \emptyset, \\ xT(G \setminus e; x, y) & e \in E(G) \text{ is a bridge}, \\ yT(G \setminus e; x, y) & e \in E(G) \text{ is a loop}, \\ T(G \setminus e; x, y) + T(G/e; x, y) & \text{otherwise}, \end{cases}$$

where $G \setminus e$ is the graph obtained by deleting e and G/e is the graph obtained by contracting e.

The chromatic polynomial is

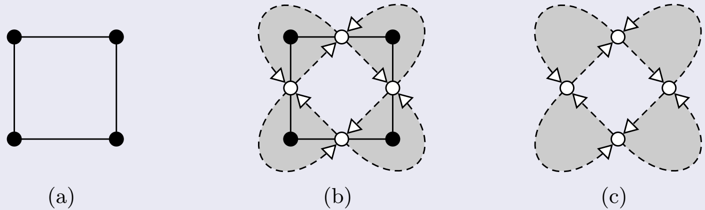
$$\chi(G;\lambda) = (-1)^{|V|-1}\lambda\, \mathrm{T}(G; 1-\lambda, 0).$$

Definition


(a) (b) (c)

A plane graph (a), its medial graph (c), and the two graphs superimposed (b).

Definition

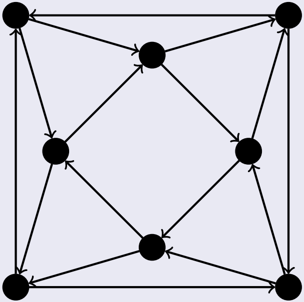


A plane graph (a), its directed medial graph (c), and the two graphs superimposed (b).

Reduction From Tutte Polynomial: Eulerian Graphs and Eulerian Partitions

Definition

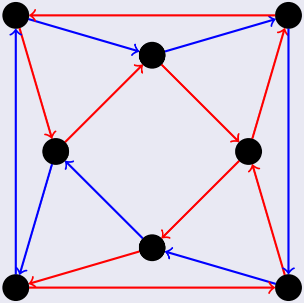
1. Digraph is Eulerian if "in degree" = "out degree".



Reduction From Tutte Polynomial: Eulerian Graphs and Eulerian Partitions

Definition

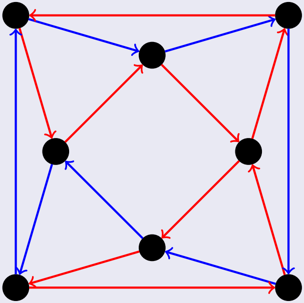
1. Digraph is Eulerian if "in degree" = "out degree".
2. Eulerian partition of an Eulerian digraph $\vec{G}$ is a partition of the edges of $\vec{G}$ such that each part induces an Eulerian digraph.



Reduction From Tutte Polynomial: Eulerian Graphs and Eulerian Partitions

Definition

1. Digraph is Eulerian if “in degree” = “out degree”.
2. Eulerian partition of an Eulerian digraph $\vec{G}$ is a partition of the edges of $\vec{G}$ such that each part induces an Eulerian digraph.
3. Let $\pi_\kappa(\vec{G})$ be the set of Eulerian partitions of $\vec{G}$ into at most κ parts.

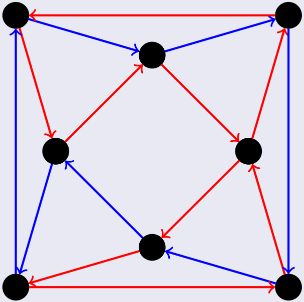


$\kappa \geq 2$

Reduction From Tutte Polynomial: Eulerian Graphs and Eulerian Partitions

Definition

1. Digraph is Eulerian if "in degree" = "out degree".
2. Eulerian partition of an Eulerian digraph $\vec{G}$ is a partition of the edges of $\vec{G}$ such that each part induces an Eulerian digraph.
3. Let $\pi_\kappa(\vec{G})$ be the set of Eulerian partitions of $\vec{G}$ into at most κ parts.
4. Let $\mu(c)$ be the number of monochromatic vertices in c.



$\kappa \geq 2$

$\mu(c) = 1$

Theorem (Ellis-Monaghan)

For a plane graph G,

$$\kappa\,\mathrm{T}(G; \kappa+1, \kappa+1) = \sum_{c \,\in\, \pi_{\kappa}(\vec{G}_m)} 2^{\mu(c)}.$$

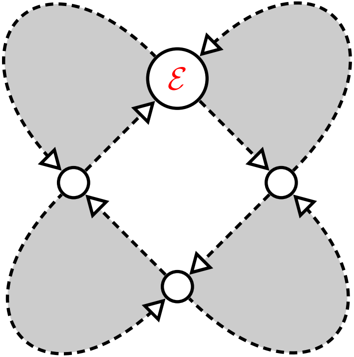
Then

$$\sum_{c \in \pi_\kappa(\vec{G}_m)} 2^{\mu(c)} = \mathrm{Holant}_\kappa(G_m; \langle 2, 1, 0, 1, 0 \rangle),$$

where

$$\mathcal{E}\left(\begin{smallmatrix} w & z \\ x & y \end{smallmatrix}\right) = \begin{cases} 2 & \text{if } w = x = y = z \\ 1 & \text{if } w = x \neq y = z \\ 0 & \text{if } w = y \neq x = z \\ 1 & \text{if } w = z \neq x = y \\ 0 & \text{otherwise,} \end{cases}$$

where $\mathcal{E} = \langle 2, 1, 0, 1, 0 \rangle$.

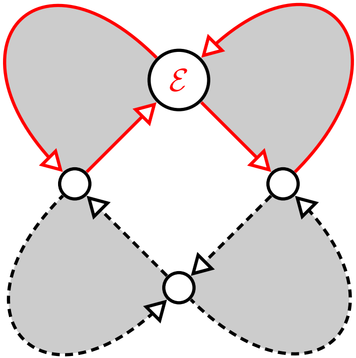


Then

$$\sum_{c \in \pi_\kappa(\vec{G}_m)} 2^{\mu(c)} = \text{Holant}_\kappa(G_m; \langle 2, 1, 0, 1, 0\rangle),$$

where

$$\mathcal{E}\left(\begin{smallmatrix} w & z \\ x & y \end{smallmatrix}\right) = \begin{cases} 2 & \text{if } w = x = y = z \\ 1 & \text{if } w = x \neq y = z \\ 0 & \text{if } w = y \neq x = z \\ 1 & \text{if } w = z \neq x = y \\ 0 & \text{otherwise,} \end{cases}$$



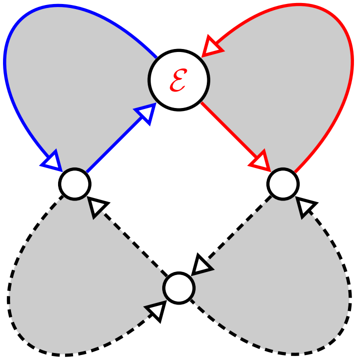
where $\mathcal{E} = \langle 2, 1, 0, 1, 0\rangle$.

Then

$$\sum_{c \in \pi_\kappa(\vec{G}_m)} 2^{\mu(c)} = \text{Holant}_\kappa(G_m; \langle 2, 1, 0, 1, 0 \rangle),$$

where

$$\mathcal{E}\left(\begin{smallmatrix} w & z \\ x & y \end{smallmatrix}\right) = \begin{cases} 2 & \text{if } w = x = y = z \\ 1 & \text{if } w = x \neq y = z \\ 0 & \text{if } w = y \neq x = z \\ 1 & \text{if } w = z \neq x = y \\ 0 & \text{otherwise,} \end{cases}$$



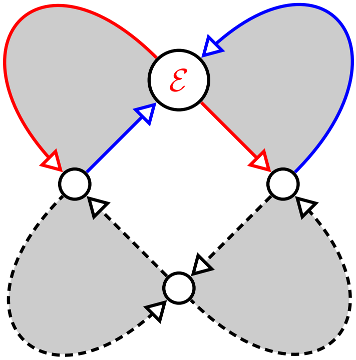
where $\mathcal{E} = \langle 2, 1, 0, 1, 0 \rangle$.

Then

$$\sum_{c \in \pi_\kappa(\vec{G}_m)} 2^{\mu(c)} = \text{Holant}_\kappa(G_m; \langle 2, 1, 0, 1, 0 \rangle),$$

where

$$\mathcal{E}\left(\begin{smallmatrix} w & z \\ x & y \end{smallmatrix}\right) = \begin{cases} 2 & \text{if } w = x = y = z \\ 1 & \text{if } w = x \neq y = z \\ 0 & \text{if } w = y \neq x = z \\ 1 & \text{if } w = z \neq x = y \\ 0 & \text{otherwise,} \end{cases}$$



where $\mathcal{E} = \langle 2, 1, 0, 1, 0 \rangle$.

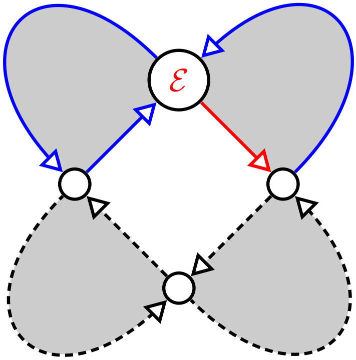
Then

$$\sum_{c \in \pi_\kappa(\vec{G}_m)} 2^{\mu(c)} = \text{Holant}_\kappa(G_m; \langle 2, 1, 0, 1, 0 \rangle),$$

where

$$\mathcal{E}\left(\begin{smallmatrix} w & z \\ x & y \end{smallmatrix}\right) = \begin{cases} 2 & \text{if } w = x = y = z \\ 1 & \text{if } w = x \neq y = z \\ 0 & \text{if } w = y \neq x = z \\ 1 & \text{if } w = z \neq x = y \\ 0 & \text{otherwise,} \end{cases}$$

where $\mathcal{E} = \langle 2, 1, 0, 1, 0 \rangle$.



Reduction From Tutte Polynomial: Upshot

Corollary

For a plane graph G,

$$\kappa T(G; \kappa+1, \kappa+1) = \mathrm{Holant}_{\kappa}(G_m; \langle 2, 1, 0, 1, 0\rangle)$$

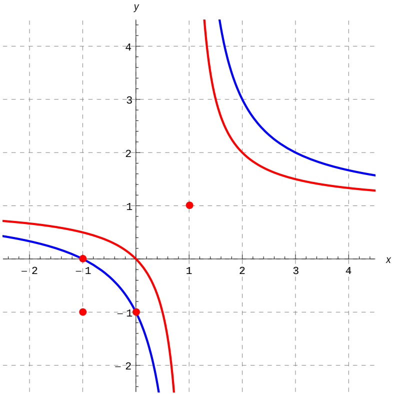
Corollary

For a plane graph G,

$$\kappa T(G; \kappa + 1, \kappa + 1) = \mathrm{Holant}_{\kappa}(G_m; \langle 2, 1, 0, 1, 0 \rangle)$$

Theorem (Vertigan)

For any $x, y \in \mathbb{C}$, the problem of evaluating the Tutte polynomial at (x, y) over planar graphs is **#P-hard** *unless $(x - 1)(y - 1) \in \{1, 2\}$ or $(x, y) \in \{(\pm 1, \pm 1), (\omega, \omega^2), (\omega^2, \omega)\}$, where $\omega = e^{2\pi i/3}$. In each of these exceptional cases, the computation can be done in polynomial time.*



Hardness of $\text{Holant}_3(-; \text{AD}_3)$ proved by the following reduction chain:

$$\begin{aligned}\#\text{P} &\le_T \text{Holant}_3(-; \langle 2,1,0,1,0\rangle) \\ &\le_T \text{Holant}_3(-; \langle 0,1,1,0,0\rangle) \\ &\le_T \text{Holant}_3(-; \text{AD}_3)\end{aligned}$$

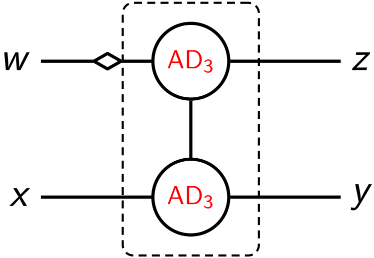
- First reduction: From a #P-hard point on the Tutte polynomial.
- Second reduction: Via polynomial interpolation.
- Third reduction: Via a gadget construction.

Hardness of $\mathrm{Holant}_3(-; \mathrm{AD}_3)$ proved by the following reduction chain:

$$\begin{aligned}\#\mathrm{P} &\leq_T \mathrm{Holant}_3(-; \langle 2,1,0,1,0\rangle)\\ &\leq_T \mathrm{Holant}_3(-; \langle 0,1,1,0,0\rangle)\\ &\leq_T \mathrm{Holant}_3(-; \mathrm{AD}_3)\end{aligned}$$

- First reduction: From a #P-hard point on the Tutte polynomial.
- Second reduction: Via polynomial interpolation.
- Third reduction: Via a gadget construction.

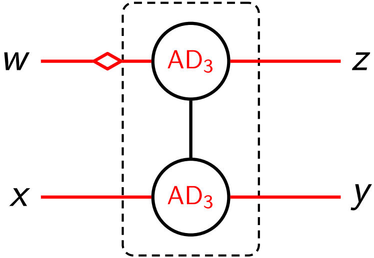
$$\text{Holant}(G; \langle 0,1,1,0,0\rangle) \leq_T \text{Holant}(G'; \text{AD}_3)$$



$$f\left(\begin{smallmatrix} w & z \\ x & y \end{smallmatrix}\right) = \langle 0,1,1,0,0\rangle = \begin{cases} 0 & \text{if } w = x = y = z \\ 1 & \text{if } w = x \neq y = z \\ 1 & \text{if } w = y \neq x = z \\ 0 & \text{if } w = z \neq x = y \\ 0 & \text{otherwise.} \end{cases}$$

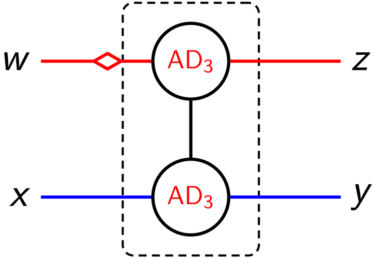
Gadget Construction

$$\text{Holant}(G; \langle 0,1,1,0,0\rangle) \le_T \text{Holant}(G'; \text{AD}_3)$$



$$f\left(\begin{smallmatrix} w & z \\ x & y \end{smallmatrix}\right) = \langle 0,1,1,0,0\rangle = \begin{cases} 0 & \text{if } w = x = y = z \\ 1 & \text{if } w = x \neq y = z \\ 1 & \text{if } w = y \neq x = z \\ 0 & \text{if } w = z \neq x = y \\ 0 & \text{otherwise.} \end{cases}$$

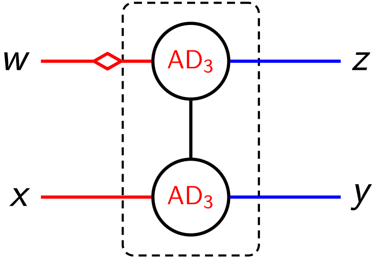
$$\text{Holant}(G; \langle 0,1,1,0,0\rangle) \leq_T \text{Holant}(G'; \text{AD}_3)$$



$$f\left(\begin{smallmatrix} w & z \\ x & y \end{smallmatrix}\right) = \langle 0,1,1,0,0\rangle = \begin{cases} 0 & \text{if } w = x = y = z \\ 1 & \text{if } w = x \neq y = z \\ 1 & \text{if } w = y \neq x = z \\ 0 & \text{if } w = z \neq x = y \\ 0 & \text{otherwise.} \end{cases}$$

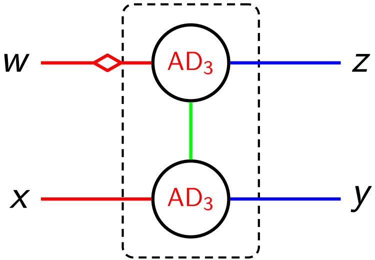
Gadget Construction

$$\text{Holant}(G; \langle 0,1,1,0,0\rangle) \leq_T \text{Holant}(G'; \text{AD}_3)$$



$$f\left(\begin{smallmatrix} w & z \\ x & y \end{smallmatrix}\right) = \langle 0,1,1,0,0\rangle = \begin{cases} 0 & \text{if } w = x = y = z \\ 1 & \text{if } w = x \neq y = z \\ 1 & \text{if } w = y \neq x = z \\ 0 & \text{if } w = z \neq x = y \\ 0 & \text{otherwise.} \end{cases}$$

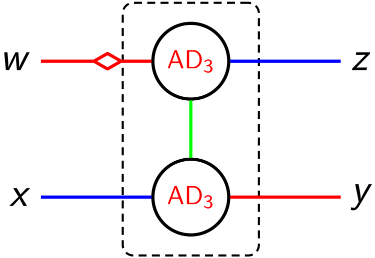
$$\text{Holant}(G; \langle 0,1,1,0,0\rangle) \leq_T \text{Holant}(G'; \text{AD}_3)$$



$$f\left(\begin{smallmatrix} w & z \\ x & y \end{smallmatrix}\right) = \langle 0,1,1,0,0\rangle = \begin{cases} 0 & \text{if } w = x = y = z \\ 1 & \text{if } w = x \neq y = z \\ 1 & \text{if } w = y \neq x = z \\ 0 & \text{if } w = z \neq x = y \\ 0 & \text{otherwise.} \end{cases}$$

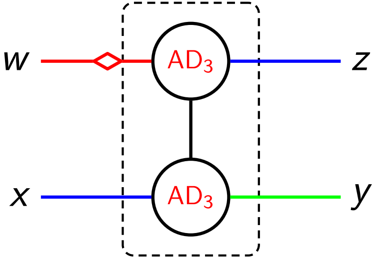
Gadget Construction

$$\text{Holant}(G; \langle 0,1,1,0,0\rangle) \leq_T \text{Holant}(G'; \text{AD}_3)$$



$$f\left(\begin{smallmatrix} w & z \\ x & y \end{smallmatrix}\right) = \langle 0,1,1,0,0\rangle = \begin{cases} 0 & \text{if } w = x = y = z \\ 1 & \text{if } w = x \neq y = z \\ 1 & \text{if } w = y \neq x = z \\ 0 & \text{if } w = z \neq x = y \\ 0 & \text{otherwise.} \end{cases}$$

$$\text{Holant}(G; \langle 0,1,1,0,0\rangle) \leq_T \text{Holant}(G'; \text{AD}_3)$$



$$f\left(\begin{smallmatrix} w & z \\ x & y \end{smallmatrix}\right) = \langle 0,1,1,0,0\rangle = \begin{cases} 0 & \text{if } w = x = y = z \\ 1 & \text{if } w = x \neq y = z \\ 1 & \text{if } w = y \neq x = z \\ 0 & \text{if } w = z \neq x = y \\ 0 & \text{otherwise.} \end{cases}$$

Hardness of $\mathrm{Holant}_3(-; \mathrm{AD}_3)$ proved by the following reduction chain:

$$\begin{aligned}\#\mathrm{P} &\le_T \mathrm{Holant}_3(-; \langle 2, 1, 0, 1, 0\rangle) \\ &\le_T \mathrm{Holant}_3(-; \langle 0, 1, 1, 0, 0\rangle) \\ &\le_T \mathrm{Holant}_3(-; \mathrm{AD}_3)\end{aligned}$$

- First reduction: From a #P-hard point on the Tutte polynomial.
- Second reduction: Via polynomial interpolation.
- Third reduction: Via a gadget construction.

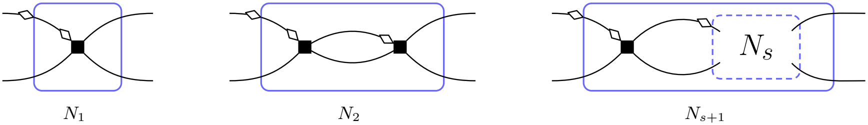
Hardness of $\text{Holant}_3(-; \text{AD}_3)$ proved by the following reduction chain:

$$\begin{aligned}\#\text{P} &\le_T \text{Holant}_3(-; \langle 2, 1, 0, 1, 0 \rangle)\\ &\le_T \text{Holant}_3(-; \langle 0, 1, 1, 0, 0 \rangle)\\ &\le_T \text{Holant}_3(-; \text{AD}_3)\end{aligned}$$

- First reduction: From a #P-hard point on the Tutte polynomial.
- Second reduction: Via polynomial interpolation.
- Third reduction: Via a gadget construction.

Polynomial Interpolation: Recursive Construction

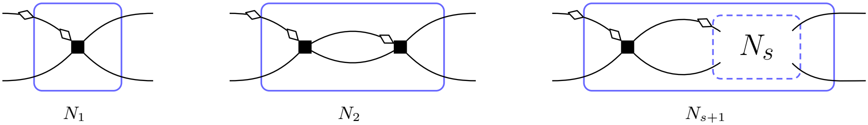
$$\text{Holant}_3(G; \langle 2, 1, 0, 1, 0\rangle) \leq_T \text{Holant}_3(G_s; \langle 0, 1, 1, 0, 0\rangle)$$



Vertices are assigned $\langle 0, 1, 1, 0, 0\rangle$.

Polynomial Interpolation: Recursive Construction

$$\text{Holant}_3(G; \langle 2,1,0,1,0\rangle) \le_T \text{Holant}_3(G_s; \langle 0,1,1,0,0\rangle)$$



Vertices are assigned $\langle 0,1,1,0,0\rangle$.

Let f_s be the function corresponding to N_s. Then $f_s = M^s f_0$, where

$$M = \begin{bmatrix} 0 & 2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad f_0 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

Obviously $f_1 = \langle 0,1,1,0,0\rangle$.

Spectral decomposition $M = P\Lambda P^{-1}$, where

$$P = \begin{bmatrix} 1 & -2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \Lambda = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Polynomial Interpolation: Eigenvectors and Eigenvalues

Spectral decomposition $M = P\Lambda P^{-1}$, where

$$P = \begin{bmatrix} 1 & -2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \Lambda = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Let $x = 2^{2s}$. Then

$$f_{2s} = P\Lambda^{2s}P^{-1}f_0 = P \begin{bmatrix} x & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} P^{-1}f_0 = \begin{bmatrix} \frac{x-1}{3} + 1 \\ \frac{x-1}{3} \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

Polynomial Interpolation: Eigenvectors and Eigenvalues

Spectral decomposition $M = P\Lambda P^{-1}$, where

$$P = \begin{bmatrix} 1 & -2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \Lambda = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Let $x = 2^{2s}$. Then

$$f(x) = f_{2s} = P\Lambda^{2s}P^{-1}f_0 = P \begin{bmatrix} x & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} P^{-1}f_0 = \begin{bmatrix} \frac{x-1}{3} + 1 \\ \frac{x-1}{3} \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

Polynomial Interpolation: Eigenvectors and Eigenvalues

Spectral decomposition $M = P\Lambda P^{-1}$, where

$$P = \begin{bmatrix} 1 & -2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \Lambda = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Let $x = 2^{2s}$. Then

$$f(x) = f_{2s} = P\Lambda^{2s}P^{-1}f_0 = P \begin{bmatrix} x & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} P^{-1}f_0 = \begin{bmatrix} \frac{x-1}{3} + 1 \\ \frac{x-1}{3} \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

Note $f(4) = \langle 2, 1, 0, 1, 0 \rangle$.

Spectral decomposition $M = P\Lambda P^{-1}$, where

$$P = \begin{bmatrix} 1 & -2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \Lambda = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Let $x = 2^{2s}$. Then

$$f(x) = f_{2s} = P\Lambda^{2s}P^{-1}f_0 = P \begin{bmatrix} x & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} P^{-1}f_0 = \begin{bmatrix} \frac{x-1}{3} + 1 \\ \frac{x-1}{3} \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

Note $f(4) = \langle 2, 1, 0, 1, 0 \rangle$.
(Side note: picking $s = 1$ so that $x = 4$ only works when $\kappa = 3$.)

Polynomial Interpolation: The Interpolation

$$\text{Holant}_3(-; \langle 2, 1, 0, 1, 0 \rangle) \leq_T \text{Holant}_3(-; \langle 0, 1, 1, 0, 0 \rangle)$$

$$\begin{aligned}
\mathrm{Holant}_3(-; \langle 2,1,0,1,0\rangle) &= \quad \mathrm{Holant}_3(-; f(4)) \\
&\leq_T \mathrm{Holant}_3(-; f(x)) \\
&\leq_T \mathrm{Holant}_3(-; \langle 0,1,1,0,0\rangle)
\end{aligned}$$

$$\begin{aligned}\mathrm{Holant}_3(-;\langle 2,1,0,1,0\rangle) = &\ \mathrm{Holant}_3(-;f(4))\\ \le_T &\ \mathrm{Holant}_3(-;f(x))\\ \le_T &\ \mathrm{Holant}_3(-;\langle 0,1,1,0,0\rangle)\end{aligned}$$

If G has n vertices, then

$$p(G,x) = \mathrm{Holant}_3(G;f(x)) \in \mathbb{Z}[x]$$

has degree n.

Polynomial Interpolation: The Interpolation

$$\begin{aligned}\text{Holant}_3(-;\langle 2,1,0,1,0\rangle) = \ & \text{Holant}_3(-;f(4)) \\ \leq_T & \ \text{Holant}_3(-;f(x)) \\ \leq_T & \ \text{Holant}_3(-;\langle 0,1,1,0,0\rangle)\end{aligned}$$

If G has n vertices, then

$$p(G,x) = \text{Holant}_3(G;f(x)) \in \mathbb{Z}[x]$$

has degree n.

Let G_{2s} be the graph obtained by replacing every vertex in G with N_{2s}. Then $\text{Holant}_3(G_{2s};\langle 0,1,1,0,0\rangle) = p(G,2^{2s})$.

$$\begin{aligned}\mathrm{Holant}_3(-;\langle 2,1,0,1,0\rangle) = &\ \mathrm{Holant}_3(-;f(4))\\ \le_T &\ \mathrm{Holant}_3(-;f(x))\\ \le_T &\ \mathrm{Holant}_3(-;\langle 0,1,1,0,0\rangle)\end{aligned}$$

If G has n vertices, then

$$p(G,x) = \mathrm{Holant}_3(G; f(x)) \in \mathbb{Z}[x]$$

has degree n.

Let G_{2s} be the graph obtained by replacing every vertex in G with N_{2s}. Then $\mathrm{Holant}_3(G_{2s}; \langle 0,1,1,0,0\rangle) = p(G, 2^{2s})$.

Using oracle for $\mathrm{Holant}_3(-;\langle 0,1,1,0,0\rangle)$, evaluate $p(G,x)$ at $n+1$ distinct points $x = 2^{2s}$ for $0 \le s \le n$.

By polynomial interpolation, efficiently compute the coefficients of $p(G,x)$. QED.

Proof Outline for Dichotomy of $\text{Holant}(-; \langle a, b, c \rangle)$

For all $a, b, c \in \mathbb{C}$,
want to show that $\text{Holant}(-; \langle a, b, c \rangle)$ is in **P** or **#P-hard**.

Proof Outline for Dichotomy of $\text{Holant}(-; \langle a, b, c\rangle)$

For all $a, b, c \in \mathbb{C}$,
want to show that $\text{Holant}(-; \langle a, b, c\rangle)$ is in **P** or **#P-hard**.

Using $\langle a, b, c\rangle$:

1. Attempt to construct a special unary constraint.
2. Attempt to interpolate all binary constraints of a special form, assuming we have the special unary constraint.
3. Construct a special ternary constraint that we show is **#P-hard**, assuming we have the special unary and binary constraints.

Proof Outline for Dichotomy of Holant$(-; \langle a, b, c \rangle)$

For all $a, b, c \in \mathbb{C}$,
want to show that Holant$(-; \langle a, b, c \rangle)$ is in **P** or **#P-hard**.

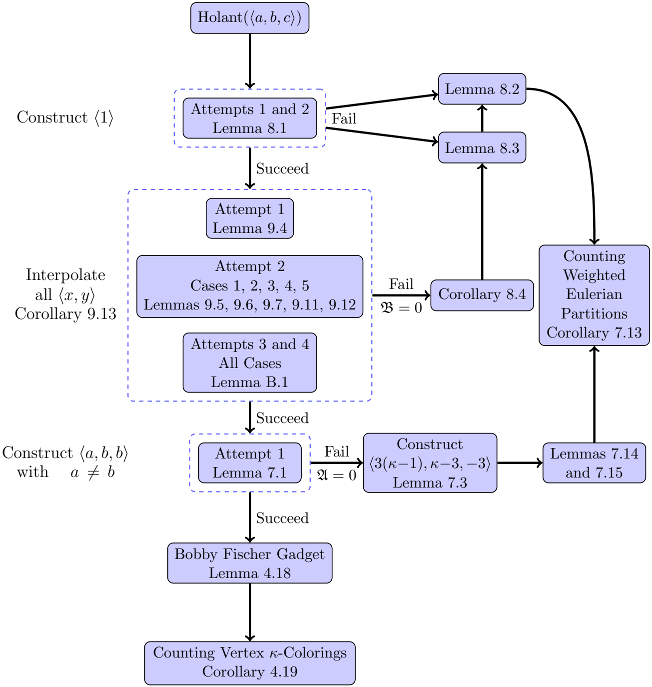
Using $\langle a, b, c \rangle$:

1. Attempt to construct a special unary constraint.
2. Attempt to interpolate all binary constraints of a special form, assuming we have the special unary constraint.
3. Construct a special ternary constraint that we show is **#P-hard**, assuming we have the special unary and binary constraints.

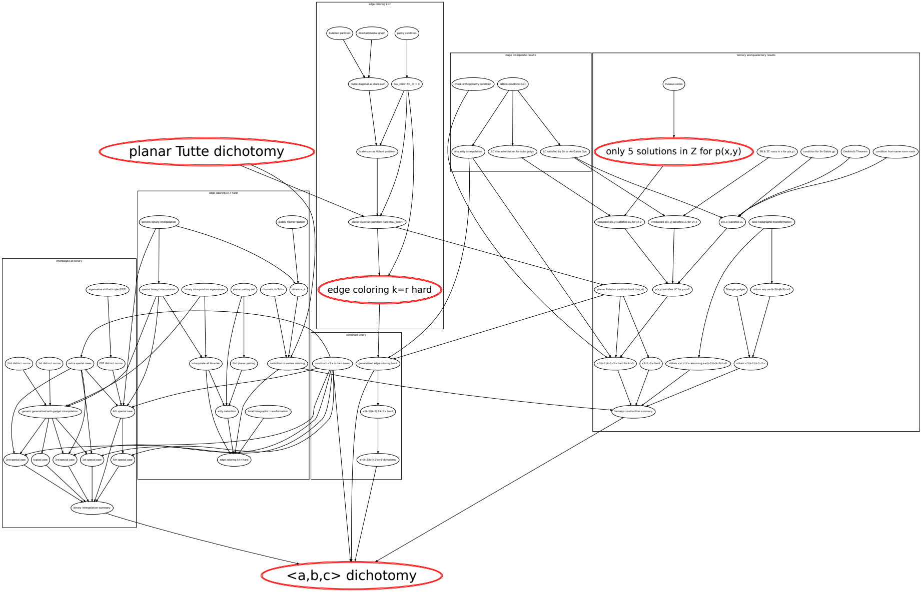
For some $a, b, c \in \mathbb{C}$, our attempts fail.

In those cases, we either

1. show the problem is in **P** or
2. prove **#P-hardness** without the help of additional signatures.


Holant($\langle a,b,c\rangle$)
Construct $\langle 1\rangle$
Attempts 1 and 2
Lemma 8.1
Fail
Lemma 8.2
Lemma 8.3
Succeed
Interpolate all $\langle x,y\rangle$ Corollary 9.13
Attempt 1
Lemma 9.4
Attempt 2
Cases 1, 2, 3, 4, 5
Lemmas 9.5, 9.6, 9.7, 9.11, 9.12
Attempts 3 and 4
All Cases
Lemma B.1
Fail
$\mathfrak{B} = 0$
Corollary 8.4
Counting Weighted Eulerian Partitions Corollary 7.13
Succeed
Construct $\langle a,b,b\rangle$ with $a \neq b$
Attempt 1
Lemma 7.1
Fail
$\mathfrak{A} = 0$
Construct $\langle 3(\kappa-1), \kappa-3, -3\rangle$ Lemma 7.3
Lemmas 7.14 and 7.15
Succeed
Bobby Fischer Gadget
Lemma 4.18
Counting Vertex κ-Colorings
Corollary 4.19

Logical Dependencies in Dichotomy of $\mathrm{Holant}_\kappa(-; \langle a, b, c \rangle)$

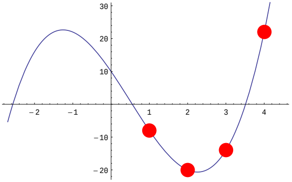


Polynomial Interpolation

Evaluate

$x \in \{1,2,3,4\}$

$$p(x) = 2x^3 - 3x^2 - 17x + 10$$



Interpolate

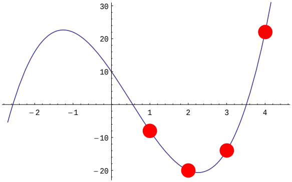
$$
\begin{aligned}
p(1) &= 2 \cdot 1^3 - 3 \cdot 1^2 - 17 \cdot 1 + 10 = -8\\
p(2) &= 2 \cdot 2^3 - 3 \cdot 2^2 - 17 \cdot 2 + 10 = -20\\
p(3) &= 2 \cdot 3^3 - 3 \cdot 3^2 - 17 \cdot 3 + 10 = -14\\
p(4) &= 2 \cdot 4^3 - 3 \cdot 4^2 - 17 \cdot 4 + 10 = 22
\end{aligned}
$$

Polynomial Interpolation

Evaluate

$x \in \{1,2,3,4\}$

$p(x) = 2x^3 - 3x^2 - 17x + 10$



Interpolate

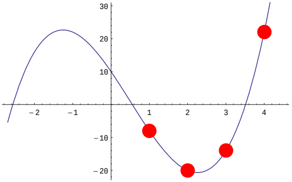
$$\begin{bmatrix} 1^3 & 1^2 & 1^1 & 1^0 \\ 2^3 & 2^2 & 2^1 & 2^0 \\ 3^3 & 3^2 & 3^1 & 3^0 \\ 4^3 & 4^2 & 4^1 & 4^0 \end{bmatrix} \begin{bmatrix} 2 \\ -3 \\ -17 \\ 10 \end{bmatrix} = \begin{bmatrix} -8 \\ -20 \\ -14 \\ 22 \end{bmatrix}$$

Vandermonde system

Evaluate

$x \in \{1,2,3,4\}$

$p(x) = 2x^3 - 3x^2 - 17x + 10$



Interpolate

$$\begin{bmatrix} 1^3 & 1^2 & 1^1 & 1^0 \\ 2^3 & 2^2 & 2^1 & 2^0 \\ 3^3 & 3^2 & 3^1 & 3^0 \\ 4^3 & 4^2 & 4^1 & 4^0 \end{bmatrix} \begin{bmatrix} ? \\ ? \\ ? \\ ? \end{bmatrix} = \begin{bmatrix} -8 \\ -20 \\ -14 \\ 22 \end{bmatrix}$$

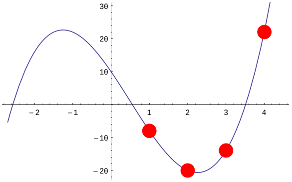
Vandermonde system

Polynomial Interpolation

Evaluate

$x \in \{1,2,3,4\}$

$$p(x) = 2x^3 - 3x^2 - 17x + 10$$



Interpolate

$$\begin{bmatrix} ? \\ ? \\ ? \\ ? \end{bmatrix} = \begin{bmatrix} 1^3 & 1^2 & 1^1 & 1^0 \\ 2^3 & 2^2 & 2^1 & 2^0 \\ 3^3 & 3^2 & 3^1 & 3^0 \\ 4^3 & 4^2 & 4^1 & 4^0 \end{bmatrix}^{-1} \begin{bmatrix} -8 \\ -20 \\ -14 \\ 22 \end{bmatrix}$$

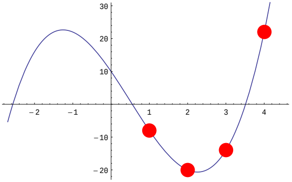
Vandermonde system

Polynomial Interpolation

Evaluate

$x \in \{1,2,3,4\}$

$$p(x) = 2x^3 - 3x^2 - 17x + 10$$



Interpolate

$$\begin{bmatrix} 2 \\ -3 \\ -17 \\ 10 \end{bmatrix} = \begin{bmatrix} 1^3 & 1^2 & 1^1 & 1^0 \\ 2^3 & 2^2 & 2^1 & 2^0 \\ 3^3 & 3^2 & 3^1 & 3^0 \\ 4^3 & 4^2 & 4^1 & 4^0 \end{bmatrix}^{-1} \begin{bmatrix} -8 \\ -20 \\ -14 \\ 22 \end{bmatrix}$$

Vandermonde system

Interpolating Univariate Polynomials

Let $p_d(X) = c_0 + c_1 X + \cdots + c_d X^d \in \mathbb{Z}[X]$.

$$\begin{gathered}\text{Can interpolate } p_d(X) \text{ from} \\ p_d(x_0), p_d(x_1), \ldots, p_d(x_d) \\ \Updownarrow \\ x_0, x_1, \ldots, x_d \text{ are distinct}\end{gathered}$$

$$\begin{bmatrix} (x_0)^0 & (x_0)^1 & \cdots & (x_0)^d \\ (x_1)^0 & (x_1)^1 & \cdots & (x_1)^d \\ \vdots & \vdots & \ddots & \vdots \\ (x_d)^0 & (x_d)^1 & \cdots & (x_d)^d \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_d \end{bmatrix} = \begin{bmatrix} p_d(x_0) \\ p_d(x_1) \\ \vdots \\ p_d(x_d) \end{bmatrix}$$

Vandermonde system

Interpolating Univariate Polynomials

Let $p_d(X) = c_0 + c_1 X + \cdots + c_d X^d \in \mathbb{Z}[X]$.

$$\forall d \in \mathbb{N}, \text{ Can interpolate } p_d(X) \text{ from}$$
$$p_d(x_0), p_d(x_1), \ldots, p_d(x_d)$$
$$\Updownarrow$$
$$x_0, x_1, \ldots \quad \text{are distinct}$$

$$\begin{bmatrix} (x_0)^0 & (x_0)^1 & \cdots & (x_0)^d \\ (x_1)^0 & (x_1)^1 & \cdots & (x_1)^d \\ \vdots & \vdots & \ddots & \vdots \\ (x_d)^0 & (x_d)^1 & \cdots & (x_d)^d \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_d \end{bmatrix} = \begin{bmatrix} p_d(x_0) \\ p_d(x_1) \\ \vdots \\ p_d(x_d) \end{bmatrix}$$

Vandermonde system

Let $p_d(X) = c_0 + c_1 X + \cdots + c_d X^d \in \mathbb{Z}[X]$.

$\forall d \in \mathbb{N}$, Can interpolate $p_d(X)$ from
$p_d(x^0), p_d(x^1), \ldots, p_d(x^d)$
$\Updownarrow$
$x^0, x^1, \ldots$ are distinct

$$\begin{bmatrix} (x^0)^0 & (x^0)^1 & \cdots & (x^0)^d \\ (x^1)^0 & (x^1)^1 & \cdots & (x^1)^d \\ \vdots & \vdots & \ddots & \vdots \\ (x^d)^0 & (x^d)^1 & \cdots & (x^d)^d \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_d \end{bmatrix} = \begin{bmatrix} p_d(x^0) \\ p_d(x^1) \\ \vdots \\ p_d(x^d) \end{bmatrix}$$

Vandermonde system

Interpolating Univariate Polynomials

Let $p_d(X) = c_0 + c_1 X + \cdots + c_d X^d \in \mathbb{Z}[X]$.

$$\forall d \in \mathbb{N}, \text{ Can interpolate } p_d(X) \text{ from}$$
$$p_d(x^0), p_d(x^1), \ldots, p_d(x^d)$$
$$\Updownarrow$$
$$x^0, x^1, \ldots \quad \text{are distinct}$$
$$\Updownarrow$$
$$x \text{ is not a root of unity}$$

$$\begin{bmatrix} (x^0)^0 & (x^0)^1 & \cdots & (x^0)^d \\ (x^1)^0 & (x^1)^1 & \cdots & (x^1)^d \\ \vdots & \vdots & \ddots & \vdots \\ (x^d)^0 & (x^d)^1 & \cdots & (x^d)^d \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_d \end{bmatrix} = \begin{bmatrix} p_d(x^0) \\ p_d(x^1) \\ \vdots \\ p_d(x^d) \end{bmatrix}$$

Vandermonde system

Let

$$p_d(X,Y,Z) = c_{0,0,d}\ X^0Y^0Z^d + \cdots + c_{d,0,0}\ X^dY^0Z^0 \in \mathbb{Z}[X,Y,Z]$$

be a homogeneous multivariate polynomial of degree d.

$$\forall d \in \mathbb{N},\ \text{Can interpolate } p_d(X,Y,Z) \text{ from}$$
$$p_d(x_0,y_0,z_0), p_d(x_1,y_1,z_1), \ldots$$
$$\Updownarrow$$
$$?$$

$$\begin{bmatrix} (x_0)^0(y_0)^0(z_0)^d & \cdots & (x_0)^d(y_0)^0(z_0)^0 \\ (x_1)^0(y_1)^0(z_1)^d & \cdots & (x_1)^d(y_1)^0(z_1)^0 \\ \vdots & \vdots & \vdots \end{bmatrix} \begin{bmatrix} c_{0,0,d} \\ \vdots \\ c_{d,0,0} \end{bmatrix} = \begin{bmatrix} p_d(x_0,y_0,z_0) \\ p_d(x_1,y_1,z_1) \\ \vdots \end{bmatrix}$$

Interpolating Multivariate Polynomials

Let

$$p_d(X,Y,Z) = c_{0,0,d}\ X^0Y^0Z^d + \cdots + c_{d,0,0}\ X^dY^0Z^0 \in \mathbb{Z}[X,Y,Z]$$

be a homogeneous multivariate polynomial of degree d.

$$\forall d \in \mathbb{N}, \text{ Can interpolate } p_d(X,Y,Z) \text{ from}$$
$$p_d(x^0,y^0,z^0), p_d(x^1,y^1,z^1), \ldots$$
$$\Updownarrow$$

$$\begin{bmatrix} (x^0)^0(y^0)^0(z^0)^d & \cdots & (x^0)^d(y^0)^0(z^0)^0 \\ (x^1)^0(y^1)^0(z^1)^d & \cdots & (x^1)^d(y^1)^0(z^1)^0 \\ \vdots & \vdots & \vdots \end{bmatrix} \begin{bmatrix} c_{0,0,d} \\ \vdots \\ c_{d,0,0} \end{bmatrix} = \begin{bmatrix} p_d(x^0,y^0,z^0) \\ p_d(x^1,y^1,z^1) \\ \vdots \end{bmatrix}$$

Vandermonde system

Let

$$p_d(X,Y,Z) = c_{0,0,d}\ X^0Y^0Z^d + \cdots + c_{d,0,0}\ X^dY^0Z^0 \in \mathbb{Z}[X,Y,Z]$$

be a homogeneous multivariate polynomial of degree d.

$$\forall d \in \mathbb{N},\ \text{Can interpolate } p_d(X,Y,Z) \text{ from}$$
$$p_d(x^0,y^0,z^0), p_d(x^1,y^1,z^1), \ldots$$
$$\Updownarrow$$

$$\begin{bmatrix} (x^0y^0z^d)^0 & \cdots & (x^dy^0z^0)^0 \\ (x^0y^0z^d)^1 & \cdots & (x^dy^0z^0)^1 \\ \vdots & \vdots & \vdots \end{bmatrix} \begin{bmatrix} c_{0,0,d} \\ \vdots \\ c_{d,0,0} \end{bmatrix} = \begin{bmatrix} p_d(x^0,y^0,z^0) \\ p_d(x^1,y^1,z^1) \\ \vdots \end{bmatrix}$$

Vandermonde system

Interpolating Multivariate Polynomials

Let

$$p_d(X, Y, Z) = c_{0,0,d}\ X^0 Y^0 Z^d + \cdots + c_{d,0,0}\ X^d Y^0 Z^0 \in \mathbb{Z}[X, Y, Z]$$

be a homogeneous multivariate polynomial of degree d.

$$\begin{gathered}\forall d \in \mathbb{N},\ \text{Can interpolate } p_d(X, Y, Z) \text{ from} \\ p_d(x^0, y^0, z^0), p_d(x^1, y^1, z^1), \ldots \\ \Updownarrow \\ \text{lattice condition}\end{gathered}$$

$$\begin{bmatrix} (x^0 y^0 z^d)^0 & \cdots & (x^d y^0 z^0)^0 \\ (x^0 y^0 z^d)^1 & \cdots & (x^d y^0 z^0)^1 \\ \vdots & \vdots & \vdots \end{bmatrix} \begin{bmatrix} c_{0,0,d} \\ \vdots \\ c_{d,0,0} \end{bmatrix} = \begin{bmatrix} p_d(x^0, y^0, z^0) \\ p_d(x^1, y^1, z^1) \\ \vdots \end{bmatrix}$$

Vandermonde system

Lattice Condition

Definition

We say that $\lambda_1, \lambda_2, \ldots, \lambda_\ell \in \mathbb{C} - \{0\}$ satisfy the lattice condition if

$$\forall x \in \mathbb{Z}^\ell - \{\mathbf{0}\} \qquad \text{with} \qquad \sum_{i=1}^{\ell} x_i = 0,$$

we have

$$\prod_{i=1}^{\ell} \lambda_i^{x_i} \neq 1.$$

Lattice Condition

Definition

We say that $\lambda_1, \lambda_2, \ldots, \lambda_\ell \in \mathbb{C} - \{0\}$ satisfy the lattice condition if

$$\forall x \in \mathbb{Z}^\ell - \{\mathbf{0}\} \qquad \text{with} \qquad \sum_{i=1}^{\ell} x_i = 0,$$

we have

$$\prod_{i=1}^{\ell} \lambda_i^{x_i} \neq 1.$$

Example (Easy)

For any $i, j, k \in \mathbb{Z}$ such that

- $i + j + k = 0$ and
- $(i, j, k) \neq (0, 0, 0)$,

it follows that

$$2^i 3^j 5^k \neq 1.$$

Lattice Condition: Another Example

Example (Medium)

For any $i, j, k \in \mathbb{Z}$ such that

- $i + j + k = 0$ and
- $(i, j, k) \neq (0, 0, 0)$,

it follows that

$$1^{i} \left(3 + \sqrt{2}\right)^{j} \left(3 - \sqrt{2}\right)^{k} \neq 1.$$

Example (Medium)

For any $i, j, k \in \mathbb{Z}$ such that

- $i + j + k = 0$ and
- $(i, j, k) \neq (0, 0, 0)$,

it follows that

$$1^{i} \left(3 + \sqrt{2}\right)^{j-k} 7^{k} = 1^{i} \left(3 + \sqrt{2}\right)^{j} \left(3 - \sqrt{2}\right)^{k} \neq 1.$$

Lattice Condition: Another Example

Example (Medium)

For any $i, j, k \in \mathbb{Z}$ such that

- $i + j + k = 0$ and
- $(i, j, k) \neq (0, 0, 0)$,

it follows that

$$1^{i}\left(3+\sqrt{2}\right)^{j-k}7^{k} = 1^{i}\left(3+\sqrt{2}\right)^{j}\left(3-\sqrt{2}\right)^{k} \neq 1.$$

Suppose

$$1^{i}\left(3+\sqrt{2}\right)^{j-k}7^{k} = 1.$$

Lattice Condition: Another Example

Example (Medium)

For any $i, j, k \in \mathbb{Z}$ such that

- $i + j + k = 0$ and
- $(i, j, k) \neq (0, 0, 0)$,

it follows that

$$1^i \left(3 + \sqrt{2}\right)^{j-k} 7^k = 1^i \left(3 + \sqrt{2}\right)^j \left(3 - \sqrt{2}\right)^k \neq 1.$$

Suppose

$$1^i \left(3 + \sqrt{2}\right)^{j-k} 7^k = 1.$$

Then

$$j - k = 0 \qquad k = 0 \qquad j = 0 \qquad i = 0.$$

Contradiction!

“Hard” Lattice Condition Example

Want to prove:

For all integers $y \geq 4$, the roots of

$$p(x, y) = x^5 - (2y + 1)x^3 - (y^2 + 2)x^2 + (y - 1)yx + y^3.$$

satisfy the lattice condition.

Want to prove:

For all integers $y \geq 4$, the roots of

$$p(x,y) = x^5 - (2y+1)x^3 - (y^2+2)x^2 + (y-1)yx + y^3.$$

satisfy the lattice condition.

Lemma

Let $p(x) \in \mathbb{Q}[x]$ be a polynomial of degree $n \geq 2$. If

1. *the Galois group of p over $\mathbb{Q}$ is S_n or A_n and*
2. *the roots of p do not all have the same complex norm,*

then the roots of p satisfy the lattice condition.

Galois group of p over $\mathbb{Q}$ is S_n or A_n

$$\text{Galois group of } p \text{ over } \mathbb{Q} \text{ is } S_n \text{ or } A_n$$
$$\Downarrow$$
$$p \text{ is irreducible over } \mathbb{Q}$$

$$\begin{array}{c} \text{Galois group of } p \text{ over } \mathbb{Q} \text{ is } S_n \text{ or } A_n \\ \Downarrow \\ p \text{ is irreducible over } \mathbb{Q} \\ \Updownarrow \text{ (Gauss' Lemma)} \\ p \text{ is irreducible over } \mathbb{Z} \end{array}$$

Factorizations and Roots

Galois group of p over $\mathbb{Q}$ is S_n or A_n

$\Downarrow$

p is irreducible over $\mathbb{Q}$

$\Updownarrow$ (Gauss' Lemma)

p is irreducible over $\mathbb{Z}$

$\Downarrow$

p has no root in $\mathbb{Z}$

$$\begin{array}{c}\text{Galois group of } p \text{ over } \mathbb{Q} \text{ is } S_n \text{ or } A_n\\ \Downarrow\\ p \text{ is irreducible over } \mathbb{Q}\\ \Updownarrow \text{ (Gauss' Lemma)}\\ p \text{ is irreducible over } \mathbb{Z}\\ \Downarrow\\ p \text{ has no root in } \mathbb{Z}\end{array}$$

What are the known nontrivial factorizations of $p(x, y)$?
What are the known integer roots of $p(x, y)$?

$$p(x,y) = \begin{cases} (x-1)(x^4+x^3+2x^2-x+1) & y=-1\\ x^2(x^3-x-2) & y=0\\ (x+1)(x^4-x^3-2x^2-x+1) & y=1\\ (x-1)(x^2-x-4)(x^2+2x+2) & y=2\\ (x-3)(x^4+3x^3+2x^2-5x-9) & y=3. \end{cases}$$

Theorem (Siegel's Theorem)

Any smooth algebraic curve of genus $g > 0$ defined by a polynomial in $\mathbb{Z}[x, y]$ has only finitely many integer solutions.

Theorem (Siegel's Theorem)

Any smooth algebraic curve of genus $g > 0$ defined by a polynomial in $\mathbb{Z}[x, y]$ has only finitely many integer solutions.

- p(x,y) has genus 3, satisfies hypothesis
- Bad news is that Siegel's theorem is not effective
- Several effective versions, but the best bound we found is 10^{20000}
- Integer solutions could be enormous

Pell's Equation (genus 0)

$$x^2 - 991y^2 = 1$$

Smallest solution:

$$(379516400906811930638014896080,$$
$$12055735790331359447442538767)$$

Next smallest solution:

$$(288065397114519999215772221121510725946342952839946398732799,$$
$$9150698914859994783783151874415159820056535806397752666720)$$

Conjecture

For any integer $y \geq 4$, $p(x, y)$ *is irreducible in* $\mathbb{Z}[x]$.

Don't know how to prove this.

What We Believe versus What We Can Prove

Conjecture

For any integer $y \geq 4$, $p(x, y)$ *is irreducible in* $\mathbb{Z}[x]$.

Don't know how to prove this.

Lemma

Only integer solutions to $p(x, y) = 0$ *are*

$$(1, -1), (0, 0), (-1, 1), (1, 2), (3, 3).$$

Proof Sketch

Puiseux series expansions for $p(x, y)$ are

$$y_1(x) = x^2 + 2x^{-1} + 2x^{-2} - 6x^{-4} - 18x^{-5} + O(x^{-6}),$$

$$y_2(x) = \quad x^{3/2} - \frac{1}{2}x + \frac{1}{8}x^{1/2} - \frac{65}{128}x^{-1/2} - x^{-1} - \frac{1471}{1024}x^{-3/2} - x^{-2} + O(x^{-5/2}),$$

$$y_3(x) = -x^{3/2} - \frac{1}{2}x - \frac{1}{8}x^{1/2} + \frac{65}{128}x^{-1/2} - x^{-1} + \frac{1471}{1024}x^{-3/2} - x^{-2} + O(x^{-5/2}).$$

Proof Sketch

Puiseux series expansions for $p(x, y)$ are

$$y_1(x) = x^2 + 2x^{-1} + 2x^{-2} - 6x^{-4} - 18x^{-5} + O(x^{-6}),$$

$$y_2(x) = \quad x^{3/2} - \frac{1}{2}x + \frac{1}{8}x^{1/2} - \frac{65}{128}x^{-1/2} - x^{-1} - \frac{1471}{1024}x^{-3/2} - x^{-2} + O(x^{-5/2}),$$

$$y_3(x) = -x^{3/2} - \frac{1}{2}x - \frac{1}{8}x^{1/2} + \frac{65}{128}x^{-1/2} - x^{-1} + \frac{1471}{1024}x^{-3/2} - x^{-2} + O(x^{-5/2}).$$

We pick functions $g_i(x, y)$ such that

1. (a, b) integer solution to $p(x, y) = 0$ implies $g_i(a, b) \in \mathbb{Z}$
2. $g_i(x, y_i(x)) = o(1)$

Thus, $g_i(x, y_i(x)) \notin \mathbb{Z}$ as $x \to \infty$

Proof Sketch

Puiseux series expansions for $p(x, y)$ are

$$y_1(x) = x^2 + 2x^{-1} + 2x^{-2} - 6x^{-4} - 18x^{-5} + O(x^{-6}),$$

$$y_2(x) = \quad x^{3/2} - \frac{1}{2}x + \frac{1}{8}x^{1/2} - \frac{65}{128}x^{-1/2} - x^{-1} - \frac{1471}{1024}x^{-3/2} - x^{-2} + O(x^{-5/2}),$$

$$y_3(x) = -x^{3/2} - \frac{1}{2}x - \frac{1}{8}x^{1/2} + \frac{65}{128}x^{-1/2} - x^{-1} + \frac{1471}{1024}x^{-3/2} - x^{-2} + O(x^{-5/2}).$$

We pick functions $g_i(x, y)$ such that

1. (a, b) integer solution to $p(x, y) = 0$ implies $g_i(a, b) \in \mathbb{Z}$
2. $g_i(x, y_i(x)) = o(1)$

Thus, $g_i(x, y_i(x)) \notin \mathbb{Z}$ as $x \to \infty$

Consider $g_2(x, y) = y^2 + xy - x^3 + x$

$$g_2\left(x, y_2(x)\right) = \Theta\left(\sqrt{x}\right)$$

Proof Sketch

Puiseux series expansions for $p(x, y)$ are

$$y_1(x) = x^2 + 2x^{-1} + 2x^{-2} - 6x^{-4} - 18x^{-5} + O(x^{-6}),$$

$$y_2(x) = x^{3/2} - \frac{1}{2}x + \frac{1}{8}x^{1/2} - \frac{65}{128}x^{-1/2} - x^{-1} - \frac{1471}{1024}x^{-3/2} - x^{-2} + O(x^{-5/2}),$$

$$y_3(x) = -x^{3/2} - \frac{1}{2}x - \frac{1}{8}x^{1/2} + \frac{65}{128}x^{-1/2} - x^{-1} + \frac{1471}{1024}x^{-3/2} - x^{-2} + O(x^{-5/2}).$$

We pick functions $g_i(x, y)$ such that

1. (a, b) integer solution to $p(x, y) = 0$ implies $g_i(a, b) \in \mathbb{Z}$
2. $g_i(x, y_i(x)) = o(1)$

Thus, $g_i(x, y_i(x)) \notin \mathbb{Z}$ as $x \to \infty$

Consider $g_2(x, y) = \frac{y^2+xy-x^3+x}{x} = \frac{y^2}{x} + y - x^2 + 1$

$$g_2\left(x, y_2(x)\right) = \Theta\left(\frac{1}{\sqrt{x}}\right)$$

Proof Sketch

Puiseux series expansions for $p(x, y)$ are

$$y_1(x) = x^2 + 2x^{-1} + 2x^{-2} - 6x^{-4} - 18x^{-5} + O(x^{-6}),$$

$$y_2(x) = \quad x^{3/2} - \frac{1}{2}x + \frac{1}{8}x^{1/2} - \frac{65}{128}x^{-1/2} - x^{-1} - \frac{1471}{1024}x^{-3/2} - x^{-2} + O(x^{-5/2}),$$

$$y_3(x) = -x^{3/2} - \frac{1}{2}x - \frac{1}{8}x^{1/2} + \frac{65}{128}x^{-1/2} - x^{-1} + \frac{1471}{1024}x^{-3/2} - x^{-2} + O(x^{-5/2}).$$

We pick functions $g_i(x, y)$ such that

1. (a, b) integer solution to $p(x, y) = 0$ implies $g_i(a, b) \in \mathbb{Z}$
2. $g_i(x, y_i(x)) = o(1)$

Thus, $g_i(x, y_i(x)) \notin \mathbb{Z}$ as $x \to \infty$

Consider $g_2(x, y) = \frac{y^2+xy-x^3+x}{x} = \frac{y^2}{x} + y - x^2 + 1$

$$g_2\left(x, y_2(x)\right) = \Theta\left(\frac{1}{\sqrt{x}}\right)$$

If $|a| > 16$, then $g_2(a, y_2(a))$ is not an integer.

Thank You

Thank You

Paper and slides available on my website:
`www.cs.wisc.edu/~tdw`