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

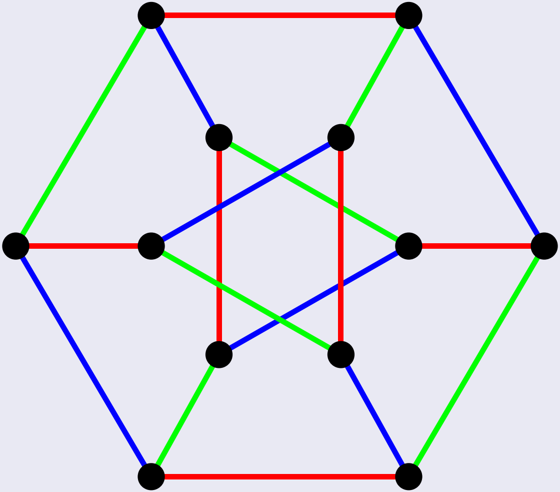
Tyson Williams
(University of Wisconsin-Madison)

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

Appeared at FOCS 2014

Edge Coloring

Definition



Counting Edge Colorings

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

Counting Edge Colorings

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

Theorem

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

Counting Edge Colorings

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

Theorem

$\#\kappa$-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. $\kappa > r$.

Definition (Intuitive)

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

Definition (Intuitive)

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

Example (Natural problems)

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

Definition (Intuitive)

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

Example (Natural problems)

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

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

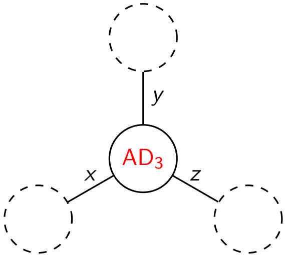
Let AD_3 denote the local constraint function

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

Let AD_3 denote the local constraint function

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

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

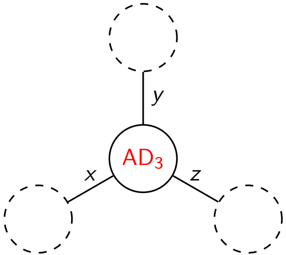


#κ-EdgeColoring as a Holant Problem

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

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

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

In general, we consider all local constraint functions

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

The Holant problem is to compute

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

Denote f by $\langle a, b, c \rangle$.
Thus $\text{AD}_3 = \langle 0, 0, 1 \rangle$.

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
   $T = \frac{1}{3} \left[\begin{smallmatrix} 1 & -2 & -2 \\ -2 & 1 & -2 \\ -2 & -2 & 1 \end{smallmatrix} \right]$.

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

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.

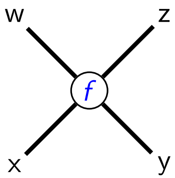
3. On domain size $\kappa = 4$,
   $\text{Holant}_4(G; \langle -3 - 4i, 1, -1 + 2i \rangle)$ is in P.

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

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

$\langle a, b, c, d, e \rangle$ denotes an arity-4 function f

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

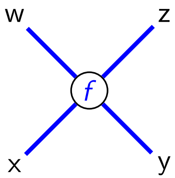


Hardness of $\text{Holant}_3(-; \text{AD}_3)$ proved by the following reduction chain:

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

$\langle a,b,c,d,e\rangle$ denotes an arity-4 function f

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

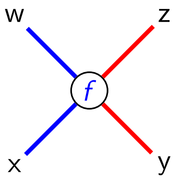


Hardness of $\text{Holant}_3(-; \text{AD}_3)$ proved by the following reduction chain:

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

$\langle a, b, c, d, e \rangle$ denotes an arity-4 function f

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

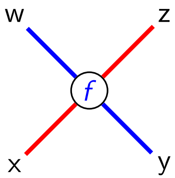


Hardness of $\text{Holant}_3(-; \text{AD}_3)$ proved by the following reduction chain:

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

$\langle a, b, c, d, e \rangle$ denotes an arity-4 function f

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

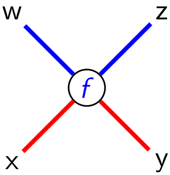


Hardness of $\mathrm{Holant}_3(-; \mathrm{AD}_3)$ proved by the following reduction chain:

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

$\langle a, b, c, d, e\rangle$ denotes an arity-4 function f

$$f\begin{pmatrix} w & z \\ x & y \end{pmatrix} = \begin{cases} a & \text{if } w = x = y = z \\ b & \text{if } w = x \neq y = z \\ c & \text{if } w = y \neq x = z \\ d & \text{if } w = z \neq x = y \\ e & \text{otherwise.} \end{cases}$$

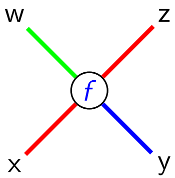


Hardness of $\text{Holant}_3(-; \text{AD}_3)$ proved by the following reduction chain:

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

$\langle a, b, c, d, e \rangle$ denotes an arity-4 function f

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



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

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

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

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

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

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

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

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

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

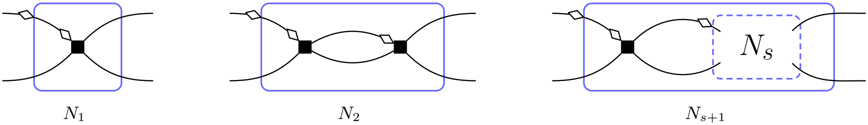
Hardness of $\mathrm{Holant}_3(-; \mathrm{AD}_3)$ proved by the following reduction chain:

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

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

Polynomial Interpolation Step: Recursive Construction

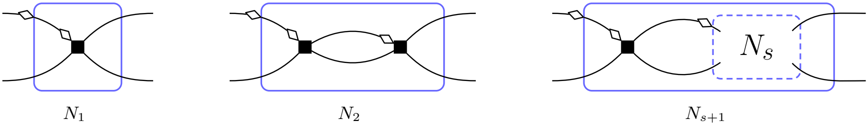
$$\text{Holant}_3(G; \langle 2, 1, 0, 1, 0\rangle) \leq_T \text{Holant}_3(G_s; \langle 0, 1, 1, 0, 0\rangle)$$



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

Polynomial Interpolation Step: 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 $\langle 0,1,1,0,0\rangle$.

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

Polynomial Interpolation Step: Eigenvectors and Eigenvalues

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

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

Polynomial Interpolation Step: 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

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

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

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

Polynomial Interpolation Step: The Interpolation

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

Polynomial Interpolation Step: The Interpolation

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

Polynomial Interpolation Step: The Interpolation

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

If G has n vertices, then

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

has degree n.

Polynomial Interpolation Step: The Interpolation

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

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 $\text{Holant}_3(G_{2s}; \langle 0,1,1,0,0\rangle) = p(G, 2^{2s})$.

Polynomial Interpolation Step: 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

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

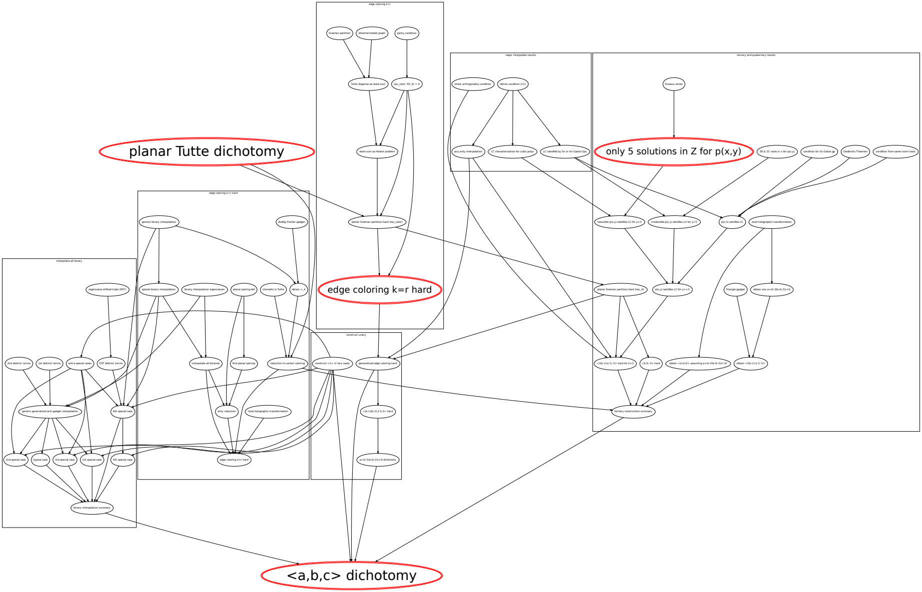
has degree n.

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

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

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

Dichotomy of $\text{Holant}_\kappa(-; \langle a, b, c\rangle)$



Interpolating Univariate Polynomials

Let $p_d(X) = c_0 + c_1 X + c_2 X^2 + \cdots + c_{d-1} X^{d-1} + c_d X^d \in \mathbb{Z}[X]$.

$$\text{Can interpolate } p_d(X) \text{ from}$$
$$p_d(x_0), p_d(x_1), p_d(x_2), \ldots, p_d(x_{d-1}), p_d(x_d)$$
$$\Updownarrow$$
$$x_0, x_1, x_2, \ldots, x_{d-1}, x_d \text{ are distinct}$$

$$\begin{bmatrix} (x_0)^0 & (x_0)^1 & (x_0)^2 & \cdots & (x_0)^{d-1} & (x_0)^d \\ (x_1)^0 & (x_1)^1 & (x_1)^2 & \cdots & (x_1)^{d-1} & (x_1)^d \\ (x_2)^0 & (x_2)^1 & (x_2)^2 & \cdots & (x_2)^{d-1} & (x_2)^d \\ & & & \vdots & & \\ (x_{(d-1)})^0 & (x_{(d-1)})^1 & (x_{(d-1)})^2 & \cdots & (x_{(d-1)})^{d-1} & (x_{(d-1)})^d \\ (x_d)^0 & (x_d)^1 & (x_d)^2 & \cdots & (x_d)^{d-1} & (x_d)^d \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{d-1} \\ c_d \end{bmatrix} = \begin{bmatrix} p_d(x_0) \\ p_d(x_1) \\ p_d(x_2) \\ \vdots \\ p_d(x_{d-1}) \\ p_d(x_d) \end{bmatrix}$$

Interpolating Univariate Polynomials

Let $p_d(X) = c_0 + c_1X + c_2X^2 + \cdots + c_{d-1}X^{d-1} + c_dX^d \in \mathbb{Z}[X]$.

$$\forall d \in \mathbb{N}, \text{ Can interpolate } p_d(X) \text{ from}$$
$$p_d(x_0), p_d(x_1), p_d(x_2), \ldots, p_d(x_{d-1}), p_d(x_d)$$
$$\Updownarrow$$
$$x_0, x_1, x_2, \ldots \qquad \text{are distinct}$$

$$\begin{bmatrix} (x_0)^0 & (x_0)^1 & (x_0)^2 & \cdots & (x_0)^{d-1} & (x_0)^d \\ (x_1)^0 & (x_1)^1 & (x_1)^2 & \cdots & (x_1)^{d-1} & (x_1)^d \\ (x_2)^0 & (x_2)^1 & (x_2)^2 & \cdots & (x_2)^{d-1} & (x_2)^d \\ & & & \vdots & & \\ (x_{(d-1)})^0 & (x_{(d-1)})^1 & (x_{(d-1)})^2 & \cdots & (x_{(d-1)})^{d-1} & (x_{(d-1)})^d \\ (x_d)^0 & (x_d)^1 & (x_d)^2 & \cdots & (x_d)^{d-1} & (x_d)^d \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{d-1} \\ c_d \end{bmatrix} = \begin{bmatrix} p_d(x_0) \\ p_d(x_1) \\ p_d(x_2) \\ \vdots \\ p_d(x_{d-1}) \\ p_d(x_d) \end{bmatrix}$$

Interpolating Univariate Polynomials

Let $p_d(X) = c_0 + c_1 X + c_2 X^2 + \cdots + c_{d-1} X^{d-1} + c_d X^d \in \mathbb{Z}[X]$.

$$\forall d \in \mathbb{N}, \text{ Can interpolate } p_d(X) \text{ from}$$
$$p_d(x^0), p_d(x^1), p_d(x^2), \ldots, p_d(x^{d-1}), p_d(x^d)$$
$$\Updownarrow$$
$$x^0, x^1, x^2, \ldots \qquad \text{are distinct}$$

$$\begin{bmatrix} (x^0)^0 & (x^0)^1 & (x^0)^2 & \cdots & (x^0)^{d-1} & (x^0)^d \\ (x^1)^0 & (x^1)^1 & (x^1)^2 & \cdots & (x^1)^{d-1} & (x^1)^d \\ (x^2)^0 & (x^2)^1 & (x^2)^2 & \cdots & (x^2)^{d-1} & (x^2)^d \\ & & & \vdots & & \\ (x^{(d-1)})^0 & (x^{(d-1)})^1 & (x^{(d-1)})^2 & \cdots & (x^{(d-1)})^{d-1} & (x^{(d-1)})^d \\ (x^d)^0 & (x^d)^1 & (x^d)^2 & \cdots & (x^d)^{d-1} & (x^d)^d \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{d-1} \\ c_d \end{bmatrix} = \begin{bmatrix} p_d(x^0) \\ p_d(x^1) \\ p_d(x^2) \\ \vdots \\ p_d(x^{d-1}) \\ p_d(x^d) \end{bmatrix}$$

Interpolating Univariate Polynomials

Let $p_d(X) = c_0 + c_1 X + c_2 X^2 + \cdots + c_{d-1} X^{d-1} + c_d X^d \in \mathbb{Z}[X]$.

$\forall d \in \mathbb{N}$, Can interpolate $p_d(X)$ from

$p_d(x^0), p_d(x^1), p_d(x^2), \ldots, p_d(x^{d-1}), p_d(x^d)$

$\Updownarrow$

$x^0, x^1, x^2, \ldots$ are distinct

$\Updownarrow$

x is not a root of unity

$$\begin{bmatrix} (x^0)^0 & (x^0)^1 & (x^0)^2 & \cdots & (x^0)^{d-1} & (x^0)^d \\ (x^1)^0 & (x^1)^1 & (x^1)^2 & \cdots & (x^1)^{d-1} & (x^1)^d \\ (x^2)^0 & (x^2)^1 & (x^2)^2 & \cdots & (x^2)^{d-1} & (x^2)^d \\ & & & \vdots & & \\ (x^{(d-1)})^0 & (x^{(d-1)})^1 & (x^{(d-1)})^2 & \cdots & (x^{(d-1)})^{d-1} & (x^{(d-1)})^d \\ (x^d)^0 & (x^d)^1 & (x^d)^2 & \cdots & (x^d)^{d-1} & (x^d)^d \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{d-1} \\ c_d \end{bmatrix} = \begin{bmatrix} p_d(x^0) \\ p_d(x^1) \\ p_d(x^2) \\ \vdots \\ p_d(x^{d-1}) \\ p_d(x^d) \end{bmatrix}$$

Interpolating Multivariate Polynomials

Let

$$q_d(X, Y, Z) = c_{0,0,d}\ X^0 Y^0 Z^d + c_{0,1,d-1}\ X^0 Y^1 Z^{d-1} + \cdots + c_{d,0,0}\ X^d Y^0 Z^0$$

in $\mathbb{Z}[X, Y, Z]$ be a homogeneous polynomial of degree d.

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

Interpolating Multivariate Polynomials

Let

$$q_d(X,Y,Z) = c_{0,0,d}\ X^0 Y^0 Z^d + c_{0,1,d-1}\ X^0 Y^1 Z^{d-1} + \cdots + c_{d,0,0}\ X^d Y^0 Z^0$$

in $\mathbb{Z}[X,Y,Z]$ be a homogeneous polynomial of degree d.

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

Let

$$q_d(X, Y, Z) = c_{0,0,d}\ X^0 Y^0 Z^d + c_{0,1,d-1}\ X^0 Y^1 Z^{d-1} + \cdots + c_{d,0,0}\ X^d Y^0 Z^0$$

in $\mathbb{Z}[X, Y, Z]$ be a homogeneous polynomial of degree d.

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

$\Updownarrow$

lattice condition

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

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

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

Actual "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.

Actual "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.

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

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

$$\Downarrow$$

p is irreducible over $\mathbb{Q}$

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 $\mathbb{Z}$

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

Factorizations and Roots

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

$$\Downarrow$$

p is irreducible over $\mathbb{Q}$

$$\Updownarrow \text{(Gauss' Lemma)}$$

p is irreducible over $\mathbb{Z}$

$$\Downarrow$$

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

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 the condition
- 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)

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

Diophantine Equations with Enormous Solutions

Pell's Equation (genus 0)

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

Smallest solution:

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

Diophantine Equations with Enormous Solutions

Pell's Equation (genus 0)

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

Smallest solution:

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

Next smallest solution:

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

What We Believe vs. What We Can Prove

Conjecture

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

What We Believe vs. 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.

What We Believe vs. 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*

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

Puiseux Series

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

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

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

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

Puiseux Series

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

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

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

Puiseux Series

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

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

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

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

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

Puiseux Series

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

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

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

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

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

Puiseux Series

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

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

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

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

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

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`