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)
Theorem (Siegel’s Theorem)

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

**Theorem (Siegel’s Theorem)**

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

**Theorem (Faltings’ Theorem–Mordell Conjecture)**

Any smooth algebraic curve of genus $g > 1$ defined by a polynomial $f(x, y) \in \mathbb{Z}[x, y]$ has only finitely many rational solutions.
Pell’s Equation (genus 0)

\[ x^2 - 61y^2 = 1 \]
Pell’s Equation (genus 0)

\[ x^2 - 61y^2 = 1 \]

Smallest solution:

\( (1766319049, 226153980) \)
Pell’s Equation (genus 0)

\[ x^2 - 61y^2 = 1 \]

Smallest solution:

(1766319049, 226153980)

\[ x^2 - 991y^2 = 1 \]

Next smallest solution:

(379516400906811930638014896080, 12055735790331359447442538767)
Diophantine Equations with Enormous Solutions

Pell’s Equation (genus 0)

\[ x^2 - 61y^2 = 1 \]

Smallest solution:

\( (1766319049, 226153980) \)

\[ x^2 - 991y^2 = 1 \]

Smallest solution:

\( (379516400906811930638014896080, 12055735790331359447442538767) \)
Diophantine Equations with Enormous Solutions

Pell’s Equation (genus 0)
\[ x^2 - 61y^2 = 1 \]

Smallest solution:
\[ (1766319049, 226153980) \]

\[ x^2 - 991y^2 = 1 \]

Smallest solution:
\[ (379516400906811930638014896080, 12055735790331359447442538767) \]

Next smallest solution:
\[ (288065397114519999215772221121510725946342952839946398732799, 9150698914859994783783151874415159820056535806397752666720) \]
Edge Coloring

Definition
Theorem (Vizing’s Theorem)

Edge coloring using at most $\Delta(G) + 1$ colors exists.

Obvious lower bound is $\Delta(G)$.

Given $G$, deciding if $\Delta(G)$ colors suffice is NP-complete over
- 3-regular graphs [Holyer (1981)],
- $k$-regular graphs for $k \geq 3$ [Leven, Galil (1983)].

(No \#P-hardness from these results.)
Edge Coloring—Decision Problem

1. Easy to show

   \( k \)-regular with bridge \( \implies \) no edge \( k \)-coloring exists.

2. When planar 3-regular bridgeless, Tait (1880) proved

   edge 3-coloring exists \( \iff \) Four Color (Conjecture) Theorem.

Therefore, for planar 3-regular graphs,

   edge 3-coloring exists \( \iff \) bridgeless.
Problem: \texttt{\#}κ-\texttt{EdgeColoring}

\textbf{Input}: A graph G.

\textbf{Output}: Number of edge colorings of G using at most κ colors.
Problem: \(\#\kappa\text{-EdgeColoring}\)

Input: A graph \(G\).

Output: Number of edge colorings of \(G\) using at most \(\kappa\) colors.

Theorem

\(\#\kappa\text{-EdgeColoring}\) is \(\#P\)-hard over planar \(r\)-regular graphs for all \(\kappa \geq r \geq 3\).

Trivially tractable when \(\kappa \geq r \geq 3\) does not hold.

Proved in a framework of complexity dichotomy theorems in two cases:

1. \(\kappa = r\), and
2. \(\kappa > r\).
Three Frameworks for Counting Problems

1. Graph Homomorphisms
2. Constraint Satisfaction Problems (CSP)
3. Holant Problems

In each framework, there has been remarkable progress in the classification program of the complexity of counting problems.
Three Frameworks for Counting Problems

1. Graph Homomorphisms
2. Constraint Satisfaction Problems (CSP)
3. Holant Problems

In each framework, there has been remarkable progress in the classification program of the complexity of counting problems.
Let $AD_3$ denote the local constraint function

$$AD_3(x, y, z) = \begin{cases} 1 & \text{if } x, y, z \in [\kappa] \text{ are distinct} \\ 0 & \text{otherwise.} \end{cases}$$
Let $AD_3$ denote the local constraint function

$$AD_3(x, y, z) = \begin{cases} 
1 & \text{if } x, y, z \in [\kappa] \text{ are distinct} \\
0 & \text{otherwise.} 
\end{cases}$$

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

$$\text{Holant}(G; AD_3) = \sum_{\sigma : E(G) \to [\kappa]} \prod_{v \in V(G)} AD_3(\sigma|E(v)).$$

Clearly $\text{Holant}(G; AD_3)$ computes $\#\kappa$-EdgeColoring. Same as contracting the corresponding tensor network.
Let $\text{AD}_3$ denote the local constraint function

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

Place $\text{AD}_3$ at each vertex with incident edges $x, y, z$ in a 3-regular graph $G$.

Then we evaluate the sum of product

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

Clearly $\text{Holant}(G; \text{AD}_3)$ computes $\#\kappa$-EdgeColoring. Same as contracting the corresponding tensor network.
In general, we consider all local constraint functions

\[ f(x, y, z) = \begin{cases} 
  a & \text{if } x = y = z \in [\kappa] \\
  b & \text{if } \{|x, y, z| = 2 \\
  c & \text{if } \{|x, y, z| = 3.}
\end{cases} \]

The Holant problem is to compute

\[ \text{Holant}(G; f) = \sum_{\sigma: E(G) \rightarrow [\kappa]} \prod_{v \in V(G)} f(\sigma | E(v)) \cdot \]

Denote \( f \) by \( \langle a, b, c \rangle \).
Thus \( AD_3 = \langle 0, 0, 1 \rangle \).
L. Lovász:
Let $A = (A_{i,j}) \in \mathbb{C}^{\kappa \times \kappa}$ be a symmetric complex matrix.

The graph homomorphism problem is:

**INPUT:** An undirected graph $G = (V, E)$.

**OUTPUT:**

$$Z_A(G) = \sum_{\xi : V \rightarrow [\kappa]} \prod_{(u,v) \in E} A_{\xi(u), \xi(v)}.$$
Examples of Graph Homomorphism

Let

\[ A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}. \]

Then \( Z_A(G) \) computes the number of vertex covers in \( G \).
Examples of Graph Homomorphism

Let
\[ A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}. \]
Then \( Z_A(G) \) computes the number of vertex covers in \( G \).

Let
\[
A = \begin{pmatrix}
0 & 1 & \cdots & 1 & 1 \\
1 & 0 & \cdots & 1 & 1 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
1 & 1 & \cdots & 0 & 1 \\
1 & 1 & \cdots & 1 & 0 \\
\end{pmatrix}.
\]
Then \( Z_A(G) \) computes the number of vertex \( \kappa \)-colorings in \( G \).
Theorem (Cai, Chen, Lu)

1. For any symmetric complex-valued matrix $A \in \mathbb{C}^{\kappa \times \kappa}$, the problem of computing $Z_A(\cdot)$ is either in $P$ or $\#P$-hard.

2. Deciding whether $Z_A(\cdot)$ is in $P$ or $\#P$-hard can be done in polynomial time (in the size of $A$).

Theorem (Cai, Chen, Lu)

1. For any symmetric complex-valued matrix \( A \in \mathbb{C}^{\kappa \times \kappa} \), the problem of computing \( Z_A(\cdot) \) is either in \( P \) or \( \#P \)-hard.

2. Deciding whether \( Z_A(\cdot) \) is in \( P \) or \( \#P \)-hard can be done in polynomial time (in the size of \( A \)).


Further generalized to all counting CSP.

Theorem (Cai, Chen)

1. For any finite set \( \mathcal{F} \) of complex-valued constraint functions over \( [\kappa] \), the corresponding counting CSP problem \( \#CSP(\mathcal{F}) \) is in \( P \) or \( \#P \)-hard.

Unweighted decision version is open (Feder-Vardi Dichotomy Conjecture).
Theorem (Main Theorem)

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

2. Deciding whether Holant($\cdot$; $\langle a, b, c \rangle$) is in P or $\#P$-hard is very easy.
Theorem (Main Theorem)

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

2. Deciding whether $\text{Holant} \left( \cdot ; \langle a, b, c \rangle \right)$ is in P or $\#P$-hard is very easy.

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

Let’s prove the theorem for this special case.
On domain size $\kappa = 3$, Holant($\cdot ; \langle -5, -2, 4 \rangle$) is in P.
On domain size $\kappa = 3$, Holant($\cdot; \langle -5, -2, 4 \rangle$) 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

$$T = \begin{bmatrix} -1 & 2 & 2 \\ 2 & -1 & 2 \\ 2 & 2 & -1 \end{bmatrix}.$$
On domain size $\kappa = 3$, Holant($\cdot;\langle -5, -2, 4 \rangle$) 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

\[
T = \begin{bmatrix}
-1 & 2 & 2 \\
2 & -1 & 2 \\
2 & 2 & -1
\end{bmatrix}.
\]

In general, Holant($G; \langle \kappa^2 - 6\kappa + 4, -2(\kappa - 2), 4 \rangle$) is in P.
On domain size $\kappa = 3$, Holant$(\cdot;\langle -5, -2, 4 \rangle)$ is in $\mathsf{P}$. 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

$$T = \begin{bmatrix} -1 & 2 & 2 \\ 2 & -1 & 2 \\ 2 & 2 & -1 \end{bmatrix}.$$

In general, Holant$(G; \langle \kappa^2 - 6\kappa + 4, -2(\kappa - 2), 4 \rangle)$ is in $\mathsf{P}$. On domain size $\kappa = 4$, Holant$(G; \langle -3 - 4i, 1, -1 + 2i \rangle)$ is in $\mathsf{P}$. 
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 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

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

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 $(x, y) \in \{(1, 1), (-1, -1), (\omega, \omega^2), (\omega^2, \omega)\}$, where $\omega = e^{2\pi i/3}$. In each of these exceptional cases, the computation can be done in polynomial time.
A plane graph (a), its medial graph (c), and the two graphs superimposed (b).
A plane graph (a), its directed medial graph (c), and the two graphs superimposed (b).
Eulerian Graphs and Eulerian Partitions

Definition

1. A graph is **Eulerian** if every vertex has an even degree.
Eulerian Graphs and Eulerian Partitions

Definition

1. A graph is Eulerian if every vertex has an even degree.
2. A digraph is Eulerian if “in degree” = “out degree” at every vertex.
Definition

1. A graph is **Eulerian** if every vertex has an even degree.
2. A digraph is **Eulerian** if “in degree” = “out degree” at every vertex.
3. An **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.

Let $\pi_\kappa(\vec{G})$ be the set of Eulerian partitions of $\vec{G}$ into at most $\kappa$ parts.
A graph is **Eulerian** if every vertex has an even degree.

A digraph is **Eulerian** if “in degree” = “out degree” at every vertex.

An **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.

Let $\pi_\kappa(\vec{G})$ be the set of Eulerian partitions of $\vec{G}$ into at most $\kappa$ parts.

Example with two **monochromatic** vertices (of degree 4).
Theorem (Ellis-Monagahan)

For a plane graph $G$,

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

where $\mu(c)$ is the number of monochromatic vertices in $c$. 
Then

\[ \sum_{c \in \pi_K(\vec{G}_m)} 2^{\mu(c)} = \text{Holant}(G_m; \mathcal{E}), \]

where

\[ \mathcal{E}(w, x, y, z) = \begin{cases} 
2 & \text{if } w = x = y = z \\
1 & \text{if } w = x \neq y = z \\
0 & \text{if } w = y \neq x = z \\
1 & \text{if } w = z \neq x = y \\
0 & \text{otherwise.} 
\end{cases} \]

Denote \( \mathcal{E} \) by \( \langle 2, 1, 0, 1, 0 \rangle \).
Then
\[ \sum_{c \in \pi_G(G_m)} 2^{\mu(c)} = \text{Holant}(G_m; \mathcal{E}), \]
where
\[ \mathcal{E}(\underline{w \ x \ z \ y}) = \begin{cases} 
2 & \text{if } w = x = y = z \\
1 & \text{if } w = x \neq y = z \\
0 & \text{if } w = y \neq x = z \\
1 & \text{if } w = z \neq x = y \\
0 & \text{otherwise.} 
\end{cases} \]
Denote \( \mathcal{E} \) by \( \langle 2, 1, 0, 1, 0 \rangle \).
Then
\[
\sum_{c \in \pi_{\kappa}(\vec{G}_m)} 2^{\mu(c)} = \text{Holant}(G_m; \mathcal{E}),
\]
where
\[
\mathcal{E}(\begin{array}{cc}
w & z \\
x & y
\end{array}) = \begin{cases}
2 & \text{if } w = x = y = z \\
1 & \text{if } w = x \neq y = z \\
0 & \text{if } w = y \neq x = z \\
1 & \text{if } w = z \neq x = y \\
0 & \text{otherwise.}
\end{cases}
\]
Denote \(\mathcal{E}\) by \(\langle 2, 1, 0, 1, 0 \rangle\).
Connection to Holant

Then

$$\sum_{c \in \pi_{\kappa}(\vec{G}_m)} 2^{\mu(c)} = \text{Holant}(G_m; \mathcal{E}),$$

where

$$\mathcal{E}(\begin{array}{c} w \\ x \\ z \end{array}) = \begin{cases} 2 & \text{if } w = x = y = z \\ 1 & \text{if } w = x \neq y = z \\ 0 & \text{if } w = y \neq x = z \\ 1 & \text{if } w = z \neq x = y \\ 0 & \text{otherwise.} \end{cases}$$

Denote $\mathcal{E}$ by $\langle 2, 1, 0, 1, 0 \rangle$. 
Then
\[ \sum_{c \in \pi_\kappa(\vec{G}_m)} 2^{\mu(c)} = \text{Holant}(G_m; \mathcal{E}), \]
where

\[ \mathcal{E}(\frac{w}{x} \frac{z}{y}) = \begin{cases} 
2 & \text{if } w = x = y = z \\
1 & \text{if } w = x \neq y = z \\
0 & \text{if } w = y = x = z \\
1 & \text{if } w = z \neq x = y \\
0 & \text{otherwise.} 
\end{cases} \]

Denote \( \mathcal{E} \) by \( \langle 2, 1, 0, 1, 0 \rangle \).
Theorem

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

Proof for $\kappa = 3$.

Reduce from Holant$(\cdot; \langle 2, 1, 0, 1, 0 \rangle)$ to Holant$(\cdot; AD_3)$ in two steps:

1. $\text{Holant}(\cdot; \langle 2, 1, 0, 1, 0 \rangle) \leq T\text{Holant}(\cdot; \langle 0, 1, 1, 0, 0 \rangle)$ (polynomial interpolation)
2. $T\text{Holant}(\cdot; \langle 0, 1, 1, 0, 0 \rangle) \leq \text{Holant}(\cdot; AD_3)$ (gadget construction)
#P-hardness of \#\(\kappa\)-EdgeColoring

**Theorem**

\(\#\kappa\text{-EdgeColoring}\) is \#P-hard over planar \(\kappa\)-regular graphs for \(\kappa \geq 3\).

**Proof for \(\kappa = 3\).**

Reduce from \(\text{Holant}(\cdot ; \langle 2, 1, 0, 1, 0 \rangle)\) to \(\text{Holant}(\cdot ; \text{AD}_3)\) in two steps:

\[
\text{Holant}(\cdot ; \langle 2, 1, 0, 1, 0 \rangle) \leq_T \text{Holant}(\cdot ; \langle 0, 1, 1, 0, 0 \rangle) \quad (\text{polynomial interpolation})
\]

\[
\leq_T \text{Holant}(\cdot ; \text{AD}_3) \quad (\text{gadget construction})
\]
Holant\((G; \langle 0, 1, 1, 0, 0 \rangle) \leq_T Holant(G'; AD_3)\)

\[
f(\frac{w}{x}, \frac{z}{y}) = \langle 0, 1, 1, 0, 0 \rangle = \begin{cases} 
0 & \text{if } w = x = y = z \\
1 & \text{if } w = x \neq y = z \\
1 & \text{if } w = y \neq x = z \\
0 & \text{if } w = z \neq x = y \\
0 & \text{otherwise.}
\end{cases}
\]
Holant\((G; \langle 0, 1, 1, 0, 0 \rangle) \leq_T \text{Holant}(G'; AD_3)\)

\[ f\left( \frac{w}{x} \frac{z}{y} \right) = \langle 0, 1, 1, 0, 0 \rangle = \begin{cases} 
0 & \text{if } w = x = y = z \\
1 & \text{if } w = x \neq y = z \\
1 & \text{if } w = y \neq x = z \\
0 & \text{if } w = z \neq x = y \\
0 & \text{otherwise.} 
\end{cases} \]
Holant\((G; \langle 0, 1, 1, 0, 0 \rangle) \leq_T Holant(G'; AD_3)\)

\[
f(\frac{w}{x} \frac{z}{y}) = \langle 0, 1, 1, 0, 0 \rangle = \begin{cases} 
0 & \text{if } w = x = y = z \\
1 & \text{if } w = x \neq y = z \\
1 & \text{if } w = y \neq x = z \\
0 & \text{if } w = z \neq x = y \\
0 & \text{otherwise.}
\end{cases}
\]
Gadget Construction Step

$\text{Holant}(G; \langle 0, 1, 1, 0, 0 \rangle) \leq_T \text{Holant}(G'; AD_3)$

$f(\begin{array}{c} w \\hline x \end{array} \begin{array}{c} z \\hline y \end{array}) = \langle 0, 1, 1, 0, 0 \rangle = \begin{cases} 0 & \text{if } w = x = y = z \\ 1 & \text{if } w = x \neq y = z \\ 1 & \text{if } w = y \neq x = z \\ 0 & \text{if } w = z \neq x = y \\ 0 & \text{otherwise.} \end{cases}$
Gadget Construction Step

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

\[ f(\frac{w}{x}, \frac{z}{y}) = \langle 0, 1, 1, 0, 0 \rangle = \begin{cases} 
0 & \text{if } w = x = y = z \\
1 & \text{if } w = x \neq y = z \\
1 & \text{if } w = y \neq x = z \\
0 & \text{if } w = z \neq x = y \\
0 & \text{otherwise.} 
\end{cases} \]
Holant\((G; \langle 0, 1, 1, 0, 0 \rangle) \leq_T \text{Holant}(G'; \text{AD}_3)\)

\[ f(\frac{w}{x} \frac{z}{y}) = \langle 0, 1, 1, 0, 0 \rangle = \begin{cases} 
0 & \text{if } w = x = y = z \\
1 & \text{if } w = x \neq y = z \\
1 & \text{if } w = y \neq x = z \\
0 & \text{if } w = z \neq x = y \\
0 & \text{otherwise.} 
\end{cases} \]
Gadget Construction Step

\[ \text{Holant}(G; \langle 0, 1, 1, 0, 0 \rangle) \leq T \text{ Holant}(G'; AD_3) \]

\[
f\left( \begin{array}{c} w \\ x \\ y \end{array} \right) = \langle 0, 1, 1, 0, 0 \rangle = \begin{cases} 0 & \text{if } w = x = y = z \\ 1 & \text{if } w = x \neq y = z \\ 1 & \text{if } w = y \neq x = z \\ 0 & \text{if } w = z \neq x = y \\ 0 & \text{otherwise.} \end{cases}
\]
Polynomial Interpolation Step: Recursive Construction

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

Vertices are assigned \( \langle 0, 1, 1, 0, 0 \rangle \).
Polynomial Interpolation Step: Recursive Construction

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

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

\[
M = \begin{bmatrix}
0 & 2 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1
\end{bmatrix}
\]

and

\[
f_0 = \begin{bmatrix}
1 \\
0 \\
0 \\
1 \\
0
\end{bmatrix}.
\]

Obviously \( f_1 = \langle 0, 1, 1, 0, 0 \rangle \).
Polynomial Interpolation Step: Eigenvectors and Eigenvalues

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

$$P = \begin{bmatrix} 1 & -2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

and

$$\Lambda = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$
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

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

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

Note $f^4 = \mathbf{E} = \langle 2, 1, 0, 1, 0 \rangle$.

(Side note: picking $s = 1$ so that $x = 4$ only works when $\kappa = 3$.)
Polynomial Interpolation Step: Eigenvectors and Eigenvalues

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

$$P = \begin{bmatrix} 1 & -2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

and

$$\Lambda = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

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 $f(4) = E = \langle 2, 1, 0, 1, 0 \rangle$. 
Polynomial Interpolation Step: Eigenvectors and Eigenvalues

Spectral decomposition $M = PΛP^{-1}$, where

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

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

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

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

\[ \text{Holant}(G; \langle 2, 1, 0, 1, 0 \rangle) \leq T \text{Holant}(G_s; \langle 0, 1, 1, 0, 0 \rangle) \]

If \( G \) has \( n \) vertices, then \( p(x) = \text{Holant}(G; f(x)) \in \mathbb{Z}[x] \) has degree \( n \).

Let \( G_s \) be the graph obtained by replacing every vertex in \( G \) with \( N_s \).

Then \( \text{Holant}(G_s; \langle 0, 1, 1, 0, 0 \rangle) = p(2^s) \).

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

By polynomial interpolation, efficiently compute the coefficients of \( p(x) \).

QED.
Polynomial Interpolation Step: The Interpolation

\[
\text{Holant}(G; \langle 2, 1, 0, 1, 0 \rangle) = \text{Holant}(G; f(4)) \\
\leq_T \text{Holant}(G; f(x)) \\
\leq_T \text{Holant}(G_s; \langle 0, 1, 1, 0, 0 \rangle)
\]
Polynomial Interpolation Step: The Interpolation

\[
\text{Holant}(G; \langle 2, 1, 0, 1, 0 \rangle) = \text{Holant}(G; f(4)) \\
\leq_T \text{Holant}(G; f(x)) \\
\leq_T \text{Holant}(G_s; \langle 0, 1, 1, 0, 0 \rangle)
\]

If \( G \) has \( n \) vertices, then

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

has degree \( n \).
Polynomial Interpolation Step: The Interpolation

\[ \text{Holant}(G; \langle 2, 1, 0, 1, 0 \rangle) = \text{Holant}(G; f(4)) \leq T \text{Holant}(G; f(x)) \leq T \text{Holant}(G_s; \langle 0, 1, 1, 0, 0 \rangle) \]

If \( G \) has \( n \) vertices, then

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

has degree \( n \).

Let \( G_s \) be the graph obtained by replacing every vertex in \( G \) with \( N_s \). Then \( \text{Holant}(G_{2s}; \langle 0, 1, 1, 0, 0 \rangle) = p(2^{2s}). \)
Polynomial Interpolation Step: The Interpolation

\[
\text{Holant}(G; \langle 2, 1, 0, 1, 0 \rangle) = \text{Holant}(G; f(4)) \\
\leq_T \text{Holant}(G; f(x)) \\
\leq_T \text{Holant}(G_s; \langle 0, 1, 1, 0, 0 \rangle)
\]

If \( G \) has \( n \) vertices, then

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

has degree \( n \).

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

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

By polynomial interpolation, efficiently compute the coefficients of \( p(x) \). QED.
Proof Outline for Dichotomy of Holant(·; ⟨a, b, c⟩)

For all \(a, b, c \in \mathbb{C}\),
want to show that Holant(·; ⟨a, b, c⟩) is in \(\text{P}\) or \(#\text{P}\)-hard.
Proof Outline for Dichotomy of Holant($\cdot$; $\langle a, b, c \rangle$)

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

1. **Attempt to construct** a special arity 1 local constraint using $\langle a, b, c \rangle$.
2. **Attempt to interpolate** all arity 2 local constraints of a certain form, assuming we have the special arity 1 local constraint.
3. **Construct** a ternary local constraint that we show is #P-hard, assuming we have these arity 2 local constraints.
Proof Outline for Dichotomy of Holant\((\cdot; \langle a, b, c \rangle)\)

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

1. **Attempt to construct** a special arity 1 local constraint using \(\langle a, b, c \rangle\).
2. **Attempt to interpolate** all arity 2 local constraints of a certain form, assuming we have the special arity 1 local constraint.
3. **Construct** a ternary local constraint that we show is \#P-hard, assuming we have these arity 2 local 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.
Interpolating Multivariate Polynomials

Let $p_d(X) \in \mathbb{Z}[X]$ be a polynomial of degree $d$.

Can interpolate $p_d(X)$ from $p_d(x_0), p_d(x_1), \ldots, p_d(x_d)$ if $x_0, x_1, \ldots, x_d$ are distinct.
Let \( p_d(X) \in \mathbb{Z}[X] \) be a polynomial of degree \( d \).

\[
\forall d \in \mathbb{N}, \text{ Can interpolate } p_d(X) \text{ from } p_d(x_0), p_d(x_1), \ldots, p_d(x_d) \nur{\Leftrightarrow} x_0, x_1, \ldots \text{ are distinct}
\]
Let $p_d(X) \in \mathbb{Z}[X]$ be a polynomial of degree $d$.

\[ \forall d \in \mathbb{N}, \text{Can interpolate } p_d(X) \text{ from } p_d(x^0), p_d(x^1), \ldots, p_d(x^d) \]

\[ \uparrow \]

\[ x^0, x^1, \ldots \text{ are distinct} \]
Let $p_d(X) \in \mathbb{Z}[X]$ be a polynomial of degree $d$.

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

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

$\iff x$ is not a root of unity
Interpolating Multivariate Polynomials

Let \( p_d(X) \in \mathbb{Z}[X] \) be a polynomial of degree \( d \).

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

Let \( q_d(X, Y) \in \mathbb{Z}[X, Y] \) be a homogeneous polynomial of degree \( d \).

\[
\forall d \in \mathbb{N}, \text{ Can interpolate } q_d(X, Y) \text{ from } q_d(x_0, y_0), q_d(x_1, y_1), \ldots, q_d(x_d, y_d) \\
\iff \quad ?
\]
Interpolating Multivariate Polynomials

Let \( p_d(X) \in \mathbb{Z}[X] \) be a polynomial of degree \( d \).

\[
\forall d \in \mathbb{N}, \text{ Can interpolate } p_d(X) \text{ from } p_d(x^0), p_d(x^1), \ldots, p_d(x^d)
\]

\[
\Leftrightarrow \quad x^0, x^1, \ldots \text{ are distinct}
\]

\[
\Leftrightarrow \quad x \text{ is not a root of unity}
\]

Let \( q_d(X, Y) \in \mathbb{Z}[X, Y] \) be a \textbf{homogeneous} polynomial of degree \( d \).

\[
\forall d \in \mathbb{N}, \text{ Can interpolate } q_d(X, Y) \text{ from } q_d(x^0, y^0), q_d(x^1, y^1), \ldots, q_d(x^d, y^d)
\]
Let $p_d(X) \in \mathbb{Z}[X]$ be a polynomial of degree $d$.

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

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

\[
\forall d \in \mathbb{N}, \text{ Can interpolate } q_d(X, Y) \text{ from } \\
q_d(x^0, y^0), q_d(x^1, y^1), \ldots, q_d(x^d, y^d) \\
\Leftrightarrow \\
lattice condition
\]
**Definition**

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

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

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

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

we have

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

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.
If there exists an infinite sequence of $\mathcal{F}$-gates defined by an initial signature $s \in \mathbb{C}^{n\times 1}$ and a recurrence matrix $M \in \mathbb{C}^{n\times n}$ satisfying the following conditions,

1. $M$ is diagonalizable with $n$ linearly independent eigenvectors;
2. $s$ is not orthogonal to exactly $\ell$ of these linearly independent row eigenvectors of $M$ with eigenvalues $\lambda_1, \ldots, \lambda_\ell$;
3. $\lambda_1, \ldots, \lambda_\ell$ satisfy the lattice condition;

then

$$\text{Holant}(\cdot; \mathcal{F} \cup \{f\}) \leq_T \text{Holant}(\cdot; \mathcal{F})$$

for any signature $f$ that is orthogonal to the $n - \ell$ of these linearly independent eigenvectors of $M$ to which $s$ is also orthogonal.
Lemma

If there exists an infinite sequence of $\mathcal{F}$-gates defined by an initial signature $s \in \mathbb{C}^{n \times 1}$ and a recurrence matrix $M \in \mathbb{C}^{n \times n}$ satisfying the following conditions,

1. $M$ is diagonalizable with $n$ linearly independent eigenvectors;
2. $s$ is not orthogonal to exactly $\ell$ of these linearly independent row eigenvectors of $M$ with eigenvalues $\lambda_1, \ldots, \lambda_\ell$;
3. $\lambda_1, \ldots, \lambda_\ell$ satisfy the lattice condition;

then

$$\text{Holant}(\cdot \ ; \mathcal{F} \cup \{f\}) \leq_T \text{Holant}(\cdot \ ; \mathcal{F})$$

for any signature $f$ that is orthogonal to the $n - \ell$ of these linearly independent eigenvectors of $M$ to which $s$ is also orthogonal.

Our proof applies this with $n = 9$ and $\ell = 5$. 
The Recurrence Matrix

\[
\begin{bmatrix}
(k-1)(k^2+9k-9) & 12(k-3)(k-1)^2 & (k-3)^2(k-1) & 2(k-3)^2(k-2)(k-1) & (k-3)^2(k-1) & 2(k-3)^2(k-2)(k-1) & (k-1)(2k-3)(4k-3) & 6(k-3)(k-2)(k-1)^2 & (k-3)^3(k-2)(k-1) \\
3(k-3)(k-1) & 3k^3-28k^2+60k-36 & -(k-3)(2k-3) & -2(k-3)(k-2)(2k-3) & -(k-3)(2k-3) & -2(k-3)(k-2)(2k-3) & 3(k-3)(k-1)^2 & -(k-2)(k^3-14k^2+30k-18) & -(k-3)^2(k-2)(2k-3) \\
(2k-3)(4k-3) & 12(k-3)(k-1)^2 & (k-3)^2(k-1) & 2(k-3)^2(k-2)(k-1) & (k-3)^2(k-1) & 2(k-3)^2(k-2)(k-1) & 9k^3-26k^2+27k-9 & 6(k-3)(k-2)(k-1)^2 & (k-3)^3(k-2)(k-1) \\
3(k-3)(k-1) & 2(k^3-14k^2+30k-18) & -(k-3)(2k-3) & -2(k-3)(k-2)(2k-3) & -(k-3)(2k-3) & -2(k-3)(k-2)(2k-3) & 3(k-3)(k-1)^2 & (k-3)(k^3-12k^2+22k-12) & -(k-3)^2(k-2)(2k-3) \\
(k-3)^2 & -4(k-3)(2k-3) & 3(k-3) & 6(k-3)(k-2) & k^3+3k-9 & 6(k-3)(k-2) & (k-3)^2(k-1) & -2(k-3)(k-2)(2k-3) & 3(k-3)^2(k-2) \\
(k-3)^2 & -4(k-3)(2k-3) & 3(k-3) & 6(k-3)(k-2) & 3(k-3) & k^3+6k^2-30k+36 & (k-3)^2(k-1) & -2(k-3)(k-2)(2k-3) & 3(k-3)^2(k-2) \\
(k-3)^2 & -4(k-3)(2k-3) & \kappa^3+3\kappa-9 & 6(k-3)(k-2) & 3(k-3) & 6(k-3)(k-2) & (k-3)^2(k-1) & -2(k-3)(k-2)(2k-3) & 3(k-3)^2(k-2) \\
(k-3)^2 & -4(k-3)(2k-3) & 3(k-3) & \kappa^3+6\kappa^2-30\kappa+36 & 3(k-3) & 6(k-3)(k-2) & (k-3)^2(k-1) & -2(k-3)(k-2)(2k-3) & 3(k-3)^2(k-2) \\
(k-3)^2 & -4(k-3)(2k-3) & 3(k-3) & 6(k-3)(k-2) & 3(k-3) & 6(k-3)(k-2) & (k-3)^2(k-1) & -2(k-3)(k-2)(2k-3) & (2k-3)(2k^2-9k+18)
\end{bmatrix}
\]
Characteristic polynomial is \((x - \kappa^3)^4 f(x, \kappa)\), where \(f(x, \kappa) = \)

\[x^5 - \kappa^6(2\kappa - 1)x^3 - \kappa^9(\kappa^2 - 2\kappa + 3)x^2 + (\kappa - 2)(\kappa - 1)\kappa^{12}x + (\kappa - 1)^3\kappa^{15}.\]
The Recurrence Matrix

\[
\begin{pmatrix}
(k-1)(k^2+9k-9) & 12(k-3)(k-1)^2 & (k-3)^2(k-1) & 2(k-3)^2(k-2)(k-1) & (k-3)^2(k-1) & 2(k-3)^2(k-2)(k-1) & (k-1)(2k-3)(4k-3) & 6(k-3)(k-2)(k-1)^2 & (k-3)^3(k-2)(k-1) \\
3(k-3)(k-1) & 3k^2+28k^3+60k-36 & -(k-3)(2k-3) & -2(k-3)(k-2)(2k-3) & -(k-3)(2k-3) & -2(k-3)(k-2)(2k-3) & 3(k-3)(k-1)^2 & -(k-2)(k^3-14k^2+30k-18) & -(k-3)^2(k-2)(2k-3) \\
3(k-3)(4k-3) & 12(k-3)(k-1)^2 & (k-3)^2(k-1) & 2(k-3)^2(k-2)(k-1) & (k-3)^2(k-1) & 2(k-3)^2(k-2)(k-1) & 9k^3-26k^2+27k-9 & 6(k-3)(k-2)(k-1)^2 & -(k-3)^3(k-2)(k-1) \\
3(k-3)(k-1) & 2(k^3-14k^2+30k-18) & -(k-3)(2k-3) & -2(k-3)(k-2)(2k-3) & -(k-3)(2k-3) & -2(k-3)(k-2)(2k-3) & 3(k-3)(k-1)^2 & -(k-3)(k^3-12k^2+22k-12) & -(k-3)^2(k-2)(2k-3) \\
(k-3)^2 & -4(k-3)(2k-3) & 3(k-3) & 6(k-3)(k-2) & k^3+3k-9 & 6(k-3)(k-2) & -(k-3)^2(k-1) & -2(k-3)(k-2)(2k-3) & 3(k-3)^2(k-2) \\
(k-3)^2 & -4(k-3)(2k-3) & 3(k-3) & 6(k-3)(k-2) & 3(k-3) & k^3+6k^2-30k+36 & 6(k-3)(k-2) & 3(k-3)^2(k-1) & -(k-3)(k-2)(2k-3) \\
(k-3)^2 & -4(k-3)(2k-3) & k^3+3k-9 & 6(k-3)(k-2) & 3(k-3) & 6(k-3)(k-2) & 3(k-3)^2(k-1) & -(k-3)(k-2)(2k-3) & 3(k-3)^2(k-2) \\
(k-3)^2 & -4(k-3)(2k-3) & 3(k-3) & k^3+6k^2-30k+36 & 3(k-3) & 6(k-3)(k-2) & 3(k-3)^2(k-1) & -(k-3)(k-2)(2k-3) & 3(k-3)^2(k-2) \\
(k-3)^2 & -4(k-3)(2k-3) & 3(k-3) & 6(k-3)(k-2) & 3(k-3) & 6(k-3)(k-2) & 3(k-3)^2(k-1) & -(k-3)(k-2)(2k-3) & (2k-3)(2k^2-9k+18)
\end{pmatrix}
\]

Characteristic polynomial is \((x - \kappa^3)^4 f(x, \kappa)\), where \(f(x, \kappa) = \)

\[x^5 - \kappa^6(2\kappa - 1)x^3 - \kappa^9(\kappa^2 - 2\kappa + 3)x^2 + (\kappa - 2)(\kappa - 1)\kappa^{12}x + (\kappa - 1)^3 \kappa^{15}.
\]

After replacing \(\kappa\) by \(y + 1\) in \(\frac{1}{\kappa^{15}} f(\kappa^3 x, \kappa)\), we get

\[p(x, y) = x^5 - (2y + 1)x^3 - (y^2 + 2)x^2 + (y - 1)yx + y^3.
\]
The Recurrence Matrix

Characteristic polynomial is \((x - \kappa^3)^4 f(x, \kappa)\), where

\[
x^5 - \kappa^6 (2\kappa - 1)x^3 - \kappa^9 (\kappa^2 - 2\kappa + 3)x^2 + (\kappa - 2)(\kappa - 1)\kappa^{12}x + (\kappa - 1)^3\kappa^{15}.
\]

After replacing \(\kappa\) by \(y + 1\) in \(\frac{1}{\kappa^{15}} f(\kappa^3 x, \kappa)\), we get

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

Want to prove:

for all integers \(y \geq 4\), the roots of \(p(x, y)\) satisfy the lattice condition.
We suspect that for any integer $y \geq 4$, $p(x, y)$ is irreducible in $\mathbb{Q}[x]$. 
We suspect that for any integer $y \geq 4$, $p(x, y)$ is irreducible in $\mathbb{Q}[x]$.

Don’t know how to prove this.
Irreducible Quintic

<table>
<thead>
<tr>
<th>Lemma</th>
</tr>
</thead>
<tbody>
<tr>
<td>For any integer ( y \geq 1 ), the polynomial ( p(x, y) ) in ( x ) has three distinct real roots and two nonreal complex conjugate roots.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proof.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discriminant.</td>
</tr>
</tbody>
</table>
Irreducible Quintic

**Lemma**

For any integer $y \geq 1$, the polynomial $p(x, y)$ in $x$ has three distinct real roots and two nonreal complex conjugate roots.

**Proof.**

Discriminant.

**Lemma**

For any integer $y \geq 4$, if $p(x, y)$ is irreducible in $\mathbb{Q}[x]$, then the roots of $p(x, y)$ satisfy the lattice condition.

**Proof.**

Three distinct real roots do not have the same norm. An irreducible polynomial of prime degree $n$ with exactly two nonreal roots has $S_n$ as its Galois group over $\mathbb{Q}$. Hence the roots satisfy the lattice condition.
What if Reducible?

We know five integer solutions to \( p(x, y) = 0 \). For these solutions, \( p(x, y) \) is reducible:

\[
\begin{align*}
p(x, y) &= (x - 1)(x^4 + x^3 + 2x^2 - x + 1) y = -1 \quad x^2 (x^3 - x - 2) y = 0 \quad (x + 1)(x^4 - x^3 - 2x^2 - x + 1) y = 1 \quad (x - 1)(x^2 - x - 4)(x^2 + 2x + 2) y = 2 \quad (x - 3)(x^4 + 3x^3 + 2x^2 - 5x - 9) y = 3.
\end{align*}
\]
What if Reducible?

We know five integer solutions to \( p(x, y) = 0 \). For these solutions, \( p(x, y) \) is reducible:

\[
p(x, y) = \begin{cases} 
(x - 1)(x^4 + x^3 + 2x^2 - x + 1) & y = -1 \\
x^2(x^3 - x - 2) & y = 0 \\
(x + 1)(x^4 - x^3 - 2x^2 - x + 1) & y = 1 \\
(x - 1)(x^2 - x - 4)(x^2 + 2x + 2) & y = 2 \\
(x - 3)(x^4 + 3x^3 + 2x^2 - 5x - 9) & y = 3.
\end{cases}
\]
We know five integer solutions to \( p(x, y) = 0 \).

For these solutions, \( p(x, y) \) is reducible:

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

**Lemma**

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

\[(1, -1), (0, 0), (-1, 1), (1, 2), (3, 3).\]
Lemma

For any integer $y \geq 4$, if $p(x, y)$ is reducible in $\mathbb{Q}[x]$, then the roots of $p(x, y)$ satisfy the lattice condition.

Proof.

By previous lemma, no linear factor over $\mathbb{Z}$.

By Gauss’ Lemma, no linear factor over $\mathbb{Q}$.

Then more Galois theory if $p(x, y)$ factors as a product of two irreducible polynomials of degrees 2 and 3.
Effective Siegel’s Theorem

\[ p(x, y) = x^5 - (2y + 1)x^3 - (y^2 + 2)x^2 + (y - 1)yx + y^3. \]
Effective Siegel’s Theorem

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

Let \((a, b)\) be an integer solution to \(p(x, y) = 0\) with \(a \neq 0\).
Effective Siegel’s Theorem

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

Let \((a, b)\) be an integer solution to \(p(x, y) = 0\) with \(a \neq 0\). One can show that \(a \mid b^2\).
Effective Siegel’s Theorem

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

Let \((a, b)\) be an integer solution to \(p(x, y) = 0\) with \(a \neq 0\). One can show that \(a|b^2\).

Consider

\[ g_1(x, y) = y - x^2 \quad \text{and} \quad g_2(x, y) = \frac{y^2}{x} + y - x^2 + 1. \]

(This particular choice is due to Aaron Levin.)

Then \(g_1(a, b)\) and \(g_2(a, b)\) are integers.
Effective Siegel’s Theorem

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

Let \((a, b)\) be an integer solution to \(p(x, y) = 0\) with \(a \neq 0\). One can show that \(a|b^2\).

Consider

\[ g_1(x, y) = y - x^2 \quad \text{and} \quad g_2(x, y) = \frac{y^2}{x} + y - x^2 + 1. \]

(This particular choice is due to Aaron Levin.)

Then \(g_1(a, b)\) and \(g_2(a, b)\) are integers.

However, if \(|a| > 16\), then either \(g_1(a, b)\) or \(g_2(a, b)\) is not an integer.
Puiseux series expansions for \( p(x, y) \) are

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

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

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

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

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

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

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

For example,

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

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

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

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

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

For example,

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

**Truncate** \( y_2(x) \) to get \( y_2^-(x) \) such that \( p(x, y_2^-(x)) < p(x, y_2(x)) \).

Then

\[
-1 < g_2(x, y_2^-(x)) \leq g_2(x, y_2(x)) < 0
\]

for \( x > 16 \).
Puiseux Series

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

\begin{align*}
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}).
\end{align*}

For example,

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

**Truncate** $y_2(x)$ to get $y_2^-(x)$ such that $p(x, y_2^-(x)) < p(x, y_2(x))$. Then

\[-1 < g_2(x, y_2^-(x)) \leq g_2(x, y_2(x)) < 0 \]

for $x > 16$.

So for “large” $x$, $g_2(x, y_2(x))$ is not an integer. Therefore, no “large” integral solutions.
Thank You
Thank You

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