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
Problem: $\kappa$-\textsc{EdgeColoring}

Input: A graph $G$

Output: “YES” if $G$ has an edge coloring using at most $\kappa$ colors and “NO” otherwise
Problem: $\kappa$-EDGE-COLORING
Input: A graph $G$
Output: “YES” if $G$ has an edge coloring using at most $\kappa$ colors and “NO” otherwise

Obviously no edge coloring using less than $\Delta$ colors.

Theorem (Vizing [1964])
An edge coloring using at most $\Delta + 1$ colors exists.
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

What about $\kappa = \Delta$?

Complexity stated as an open problem in [1979]

**Theorem (Holyer [1981])**

3-\textsc{EdgeColoring} is NP-hard over 3-regular graphs.

**Theorem (Leven, Galil [1983])**

$r$-\textsc{EdgeColoring} is NP-hard over $r$-regular graphs for all $r \geq 3$. 
Lemma (Parity Condition)

\[ r\text{-regular graph with a bridge } \implies \text{no edge coloring using } r \text{ colors exists} \]

Example

This graph has no edge coloring using 3 colors.
Lemma (Parity Condition)

\[ r\)-regular graph with a bridge \implies \text{no edge coloring using } r\text{ 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:** $\#^\kappa\text{-EdgeColoring}$

**Input:** A graph $G$

**Output:** Number of edge colorings of $G$ using at most $\kappa$ colors

Theorem (Cai, Guo, W [2014])

$\#^\kappa\text{-EdgeColoring}$ 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. $\kappa = r$
2. $\kappa > r$.
Problem: \( \#\kappa\text{-EdgeColoring} \)
Input: A graph \( G \)
Output: Number of edge colorings of \( G \) using at most \( \kappa \) colors

Theorem (Cai, Guo, W [2014])

\( \#\kappa\text{-EdgeColoring} \) 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 \textit{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.
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 \( \text{AD}_3 \) 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 \( G \).
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

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

Clearly $\text{Holant}_\kappa(\cdot; AD_3)$ computes $\#\kappa$-EdgeColoring.
More Explicit Examples

Four examples with $\kappa = 2$:

$\text{Holant}_2(G; f)$ counts

\[
\begin{cases}
\text{matchings} & \text{when } f = \text{AT-MOST-ONE}_r \\
\text{perfect matchings} & \text{when } f = \text{EXACTLY-ONE}_r \\
\text{cycle covers} & \text{when } f = \text{EXACTLY-TWO}_r \\
\text{edge covers} & \text{when } f = \text{OR}_r
\end{cases}
\]

$\text{Holant}_\kappa(G; f) = \sum_{\sigma:E(G)\rightarrow\{0,1\}} \prod_{v \in V(G)} f(\sigma|_{E(v)})$. 
In general, we consider all local constraint functions

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

The Holant problem is to compute

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

Note \( AD_3 = \langle 0, 0, 1 \rangle \).
Dichotomy Theorem for Holant$_κ(−; \langle a, b, c \rangle)$

**Theorem (Main Theorem)**

For any $κ ≥ 3$ and any $a, b, c \in \mathbb{C}$, the problem of computing Holant$_κ(−; \langle a, b, c \rangle)$ is in $\mathsf{P}$ or $\mathsf{#P}$-hard, even when the input is restricted to planar graphs.
Dichotomy Theorem for \( \text{Holant}_\kappa(\neg; \langle a, b, c \rangle) \)

**Theorem (Main Theorem)**

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

Recall \( \#_\kappa\text{-EdgeColoring} \) is the special case \( \langle a, b, c \rangle = \langle 0, 0, 1 \rangle \).

Let’s prove the theorem for \( \kappa = 3 \) and \( \langle a, b, c \rangle = \langle 0, 0, 1 \rangle \).
On domain size $\kappa = 3$, $\text{Holant}_3(-; \langle -5, -2, 4 \rangle)$ is in $\mathbf{P}$. 
On domain size $\kappa = 3$, \( \text{Holant}_3(-; \langle -5, -2, 4 \rangle) \) is in \( \mathbf{P} \).

Since

\[ \langle -5, -2, 4 \rangle = [(1, -2, -2) \otimes^3 + (-2, 1, -2) \otimes^3 + (-2, -2, 1) \otimes^3], \]

do a \textbf{holographic transformation} by the orthogonal matrix

\[ T = \frac{1}{3} \begin{bmatrix} 1 & -2 & -2 \\ -2 & 1 & -2 \\ -2 & -2 & 1 \end{bmatrix}. \]
On domain size $\kappa = 3$, 
$\text{Holant}_3(-; \langle -5, -2, 4 \rangle)$ is in $\mathbf{P}$.

Since  
$$\langle -5, -2, 4 \rangle = [(1, -2, -2)^\otimes 3 + (-2, 1, -2)^\otimes 3 + (-2, -2, 1)^\otimes 3],$$
do a holographic transformation by the orthogonal matrix 
$$T = \frac{1}{3} \begin{bmatrix} 1 & -2 & -2 \\ -2 & 1 & -2 \\ -2 & -2 & 1 \end{bmatrix}.$$

In general, 
$\text{Holant}_\kappa(G; \langle \kappa^2 - 6\kappa + 4, -2(\kappa - 2), 4 \rangle)$ is in $\mathbf{P}$. 
On domain size $\kappa = 3$,
Holant$_3(-; \langle -5, -2, 4 \rangle)$ is in $\mathbb{P}$.

Since
\[
\langle -5, -2, 4 \rangle = [(1, -2, -2) \otimes^3 + (-2, 1, -2) \otimes^3 + (-2, -2, 1) \otimes^3],
\]
do a holographic transformation by the orthogonal matrix
\[
T = \frac{1}{3} \begin{bmatrix}
1 & -2 & -2 \\
-2 & 1 & -2 \\
-2 & -2 & 1
\end{bmatrix}.
\]

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

On domain size $\kappa = 4$,
Holant$_4(G; \langle -3 - 4i, 1, -1 + 2i \rangle)$ is in $\mathbb{P}$. 
Hardness of Holant$_3(\neg; \text{AD}_3)$

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

\[ \#P \leq_T \text{Holant}_3(\neg; \langle 2, 1, 0, 1, 0 \rangle) \]
\[ \leq_T \text{Holant}_3(\neg; \langle 0, 1, 1, 0, 0 \rangle) \]
\[ \leq_T \text{Holant}_3(\neg; \text{AD}_3) \]

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

First reduction: From a #P-hard point on the Tutte polynomial.
Second reduction: Via polynomial interpolation.
Third reduction: Via a gadget construction.
Hardness of Holant$_3(−; AD_3)$

Hardness of Holant$_3(−; AD_3)$ proved by the following reduction chain:

\[ \#P \leq_T \text{Holant}_3(−; \langle 2, 1, 0, 1, 0 \rangle) \]
\[ \leq_T \text{Holant}_3(−; \langle 0, 1, 1, 0, 0 \rangle) \]
\[ \leq_T \text{Holant}_3(−; AD_3) \]

\[
\begin{align*}
    f(w, x, y, z) = (a, b, c, d, e) = \\
    \begin{cases} 
        a & \text{if } w = x = y = z \\
        b & \text{if } w = x \neq y = z \\
        c & \text{if } w = y \neq x = z \\
        d & \text{if } w = z \neq x = y \\
        e & \text{otherwise.}
    \end{cases}
\end{align*}
\]
Hardness of $\text{Holant}_3(\neg; \text{AD}_3)$ proved by the following reduction chain:

$$\#P \leq_T \text{Holant}_3(\neg; \langle 2, 1, 0, 1, 0 \rangle)$$
$$\leq_T \text{Holant}_3(\neg; \langle 0, 1, 1, 0, 0 \rangle)$$
$$\leq_T \text{Holant}_3(\neg; \text{AD}_3)$$

$$f(w, x, y, z) = \langle a, b, c, d, e \rangle = \begin{cases} 
    a & \text{if } w = x = y = z \\
    b & \text{if } w = x \neq y = z \\
    c & \text{if } w = y \neq x = z \\
    d & \text{if } w = z \neq x = y \\
    e & \text{otherwise.}
\end{cases}$$
Hardness of Holant$_3(\neg; AD_3)$ proved by the following reduction chain:

\[ \#P \leq_T \text{Holant}_3(\neg; \langle 2, 1, 0, 1, 0 \rangle) \]
\[ \leq_T \text{Holant}_3(\neg; \langle 0, 1, 1, 0, 0 \rangle) \]
\[ \leq_T \text{Holant}_3(\neg; AD_3) \]

\[
 f(w, x, y, z) = \langle a, b, c, d, e \rangle = \begin{cases}
    a & \text{if } w = x = y = z \\
    b & \text{if } w = x \neq y = z \\
    c & \text{if } w = y \neq x = z \\
    d & \text{if } w = z \neq x = y \\
    e & \text{otherwise.}
\end{cases}
\]
Hardness of \( \text{Holant}_3(\neg; \text{AD}_3) \)

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

\[
\#P \leq_T \text{Holant}_3(\neg; \langle 2, 1, 0, 1, 0 \rangle) \\
\leq_T \text{Holant}_3(\neg; \langle 0, 1, 1, 0, 0 \rangle) \\
\leq_T \text{Holant}_3(\neg; \text{AD}_3)
\]

\[
f(w, x, y, z) = \langle a, b, c, d, e \rangle = \begin{cases} 
  a & \text{if } w = x = y = z \\
  b & \text{if } w = x \neq y = z \\
  c & \text{if } w = y \neq x = z \\
  d & \text{if } w = z \neq x = y \\
  e & \text{otherwise.}
\end{cases}
\]
Hardness of Holant$_3(\langle -; AD_3 \rangle)$ proved by the following reduction chain:

\[
\begin{align*}
\text{#P} & \leq_T \text{Holant}_3(\langle -; \langle 2, 1, 0, 1, 0 \rangle \rangle) \\
& \leq_T \text{Holant}_3(\langle -; \langle 0, 1, 1, 0, 0 \rangle \rangle) \\
& \leq_T \text{Holant}_3(\langle -; AD_3 \rangle)
\end{align*}
\]

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

\[
f(\frac{w}{x} \frac{z}{y}) = \langle a, b, c, d, e \rangle =
\begin{cases}
  a & \text{if } w = x = y = z \\
  b & \text{if } w = x \neq y = z \\
  c & \text{if } w = y \neq x = z \\
  d & \text{if } w = z \neq x = y \\
  e & \text{otherwise.}
\end{cases}
\]
Hardness of Holant$_3(−; AD_3)$

Hardness of Holant$_3(−; AD_3)$ proved by the following reduction chain:

\[
\#P \leq T \text{Holant}_3(−; \langle 2, 1, 0, 1, 0 \rangle) \\
\leq T \text{Holant}_3(−; \langle 0, 1, 1, 0, 0 \rangle) \\
\leq T \text{Holant}_3(−; AD_3)
\]

- First reduction: From a \#P-hard point on the Tutte polynomial.
Hardness of Holant$_3(−; \text{AD}_3)$

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

$$\#P \leq_T \text{Holant}_3(−; \langle 2, 1, 0, 1, 0 \rangle)$$
$$\leq_T \text{Holant}_3(−; \langle 0, 1, 1, 0, 0 \rangle)$$
$$\leq_T \text{Holant}_3(−; \text{AD}_3)$$

- First reduction: From a \textbf{#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:

\[
\#P \leq_T \text{Holant}_3(−; \langle 2, 1, 0, 1, 0 \rangle) \\
\leq_T \text{Holant}_3(−; \langle 0, 1, 1, 0, 0 \rangle) \\
\leq_T \text{Holant}_3(−; \text{AD}_3)
\]

- First reduction: From a \#P-hard point on the Tutte polynomial.
- Second reduction: Via polynomial interpolation.
- Third reduction: Via a gadget construction.
Hardness of $\text{Holant}_3(−; \text{AD}_3)$

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

$$\#P \leq_T \text{Holant}_3(−; \langle 2, 1, 0, 1, 0 \rangle)$$
$$\leq_T \text{Holant}_3(−; \langle 0, 1, 1, 0, 0 \rangle)$$
$$\leq_T \text{Holant}_3(−; \text{AD}_3)$$

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

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

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).
Reduction From Tutte Polynomial: Eulerian Graphs and Eulerian Partitions

Definition

1. Digraph is **Eulerian** if “in degree” = “out degree”.

![Diagram of an Eulerian graph]

\[ \text{Let } \pi(\vec{G}) \text{ be the set of Eulerian partitions of } \vec{G} \text{ into at most } \kappa \text{ parts.} \]

\[ \text{Let } \mu(c) \text{ be the number of monochromatic vertices in } c \text{.} \]

\[ \mu(c) \geq \frac{19}{43} \]
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.
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 $\kappa$ parts.
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 $\kappa$ parts.
4. Let $\mu(c)$ be the number of **monochromatic** vertices in $c$.

$$\kappa \geq 2$$
$$\mu(c) = 1$$
For a plane graph $G$, 
\[
\kappa T(G; \kappa + 1, \kappa + 1) = \sum_{c \in \pi_\kappa(\tilde{G}_m)} 2^\mu(c).
\]
Then
\[ \sum_{c \in \pi_\kappa(\bar{G}_m)} 2^{\mu(c)} = \text{Holant}_\kappa(G_m; \langle 2, 1, 0, 1, 0 \rangle), \]

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

where \( \mathcal{E} = \langle 2, 1, 0, 1, 0 \rangle. \)
Then

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

where

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

where \( E = \langle 2, 1, 0, 1, 0 \rangle \).
Then

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

where

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

where \( E = \langle 2, 1, 0, 1, 0 \rangle. \)
Then
\[ \sum_{c \in \pi_{\kappa}(\tilde{G}_m)} 2^{\mu(c)} = \text{Holant}_{\kappa}(G_m; \langle 2, 1, 0, 1, 0 \rangle), \]
where
\[ E(w, x, y) = \begin{cases} 
2 & \text{if } w = x = y = z \\
1 & \text{if } w = x \neq y = z \\
0 & \text{if } w = y \neq x = z \\
1 & \text{if } w = z \neq x = y \\
0 & \text{otherwise},
\end{cases} \]
where \( E = \langle 2, 1, 0, 1, 0 \rangle. \)
Then

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

where

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

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

For a plane graph $G$,

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

For a plane graph $G$,

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

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 Holant\(_3(\neg; AD_3)\) proved by the following reduction chain:

\[
\#P \leq \tau \text{Holant}_3(\neg; \langle 2, 1, 0, 1, 0 \rangle) \\
\leq \tau \text{Holant}_3(\neg; \langle 0, 1, 1, 0, 0 \rangle) \\
\leq \tau \text{Holant}_3(\neg; AD_3)
\]

- **First reduction**: From a \#P-hard point on the Tutte polynomial.
- **Second reduction**: Via polynomial interpolation.
- **Third reduction**: Via a gadget construction.
Hardness of Holant$_3(\neg; AD_3)$

Hardness of Holant$_3(\neg; AD_3)$ proved by the following reduction chain:

\[
\#P \leq T \text{Holant}_3(\neg; \langle 2, 1, 0, 1, 0 \rangle) \\
\leq T \text{Holant}_3(\neg; \langle 0, 1, 1, 0, 0 \rangle) \\
\leq T \text{Holant}_3(\neg; AD_3)
\]

- First reduction: From a $\#P$-hard point on the Tutte polynomial.
- Second reduction: Via polynomial interpolation.
- Third reduction: Via a gadget construction.
$$\text{Holant}(G; \langle 0, 1, 1, 0, 0 \rangle) \leq_T \text{Holant}(G'; \text{AD}_3)$$

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

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

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

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

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

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

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

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

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

$$f(\frac{w}{x} \frac{z}{y}) = \langle 0, 1, 1, 0, 0 \rangle = \begin{cases} 
0 & \text{if } w = x = y = z \\
1 & \text{if } w = x \neq y = z \\
1 & \text{if } w = y \neq x = z \\
0 & \text{if } w = z \neq x = y \\
0 & \text{otherwise.}
\end{cases}$$
Hardness of $\text{Holant}_3(-; \text{AD}_3)$ proved by the following reduction chain:

\[
\#P \leq \tau \text{ Holant}_3(-; \langle 2, 1, 0, 1, 0 \rangle) \\
\leq \tau \text{ Holant}_3(-; \langle 0, 1, 1, 0, 0 \rangle) \\
\leq \tau \text{ Holant}_3(-; \text{AD}_3)
\]

- First reduction: From a $\#P$-hard point on the Tutte polynomial.
- Second reduction: Via polynomial interpolation.
- Third reduction: Via a gadget construction.
Hardness of $\text{Holant}_3(\neg; \text{AD}_3)$

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

$$\#P \leq_T \text{Holant}_3(\neg; \langle 2, 1, 0, 1, 0 \rangle)$$
$$\leq_T \text{Holant}_3(\neg; \langle 0, 1, 1, 0, 0 \rangle)$$
$$\leq_T \text{Holant}_3(\neg; \text{AD}_3)$$

- 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 $\langle 0, 1, 1, 0, 0 \rangle$. 

$$f_s = M_s f_0,$$

where $M_s = \begin{bmatrix} 0 & 2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$ and $f_0 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$. 

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

$N_1$ $N_2$ $N_{s+1}$
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 \( \langle 0, 1, 1, 0, 0 \rangle \).

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 \( f_1 = \langle 0, 1, 1, 0, 0 \rangle \).
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 $M = PΛP^{-1}$, 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

$$f_{2s} = PΛ^sP^{-1}f_0 = P \begin{bmatrix} x & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} P^{-1}f_0 = \begin{bmatrix} \frac{x-1}{3} + 1 \\ \frac{x-1}{3} \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$
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 $M = PΛP^{-1}$, 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 $x = 2^s$. Then

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

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

(Side note: picking $s = 1$ so that $x = 4$ only works when $κ = 3$.)
Polynomial Interpolation: 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 $x = 2^s$. Then

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

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

(Side note: picking $s = 1$ so that $x = 4$ only works when $κ = 3$.)
Holant$_3$($-$; $\langle 2, 1, 0, 1, 0 \rangle$) $\leq_T$ Holant$_3$($-$; $\langle 0, 1, 1, 0, 0 \rangle$)
Polynomial Interpolation: The Interpolation

\[ \text{Holant}_3(-; \langle 2, 1, 0, 1, 0 \rangle) = \text{Holant}_3(-; f(4)) \]
\[ \leq_T \text{Holant}_3(-; f(x)) \]
\[ \leq_T \text{Holant}_3(-; \langle 0, 1, 1, 0, 0 \rangle) \]
Polynomial Interpolation: The Interpolation

Holant$_3(−; \langle 2, 1, 0, 1, 0 \rangle) = \ Holant$_3(−; f(4))$

\[ \leq_T Holant$_3(−; f(x)) \]

\[ \leq_T Holant$_3(−; \langle 0, 1, 1, 0, 0 \rangle) \]

If $G$ has $n$ vertices, then

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

has degree $n$. 
Polynomial Interpolation: The Interpolation

\[ \text{Holant}_3(\neg; \langle 2, 1, 0, 1, 0 \rangle) = \text{Holant}_3(\neg; f(4)) \]
\[ \leq_T \text{Holant}_3(\neg; f(x)) \]
\[ \leq_T \text{Holant}_3(\neg; \langle 0, 1, 1, 0, 0 \rangle) \]

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: The Interpolation

\[
\text{Holant}_3(-; \langle 2, 1, 0, 1, 0 \rangle) = \text{Holant}_3(-; f(4)) \\
\leq_T \text{Holant}_3(-; f(x)) \\
\leq_T \text{Holant}_3(-; \langle 0, 1, 1, 0, 0 \rangle)
\]

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.
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 P or $\#P$-hard.
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.
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 \( \#\text{P-hard} \).

Using \( ⟨a, b, c⟩ \):

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 \( \#\text{P-hard} \), 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 \( \text{P} \) or
2. prove \( \#\text{P-hardness} \) without the help of additional signatures.
Attempts 1 and 2
Lemma 8.1

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

Construct \langle 1 \rangle

Interpolate all \langle x, y \rangle
Corollary 9.13

Construct \langle a, b, c \rangle
with \ a \neq b

Bobby Fischer Gadget
Lemma 4.18

Counting Vertex \kappa-Colorings
Corollary 4.19

Counting Weighted Eulerian Partitions
Corollary 7.13

Lemmas 7.14 and 7.15

Succeed

Succeed

Succeed

Fail

\mathcal{B} = 0

\mathcal{A} = 0

Fail

Holant(\langle a, b, c \rangle)
Lemma 8.2
Lemma 8.3
Corollary 8.4

Lemma 7.3

Lemma 7.1

Logical Dependencies in Dichotomy of $\text{Holant}_\kappa^\tau(-; \langle a, b, c \rangle)$
Polynomial Interpolation

Evaluate

\[ x \in \{1, 2, 3, 4\} \]

\[ p(x) = 2x^3 - 3x^2 - 17x + 10 \]

Interpolate

\[ p(1) = 2 \cdot 1^3 - 3 \cdot 1^2 - 17 \cdot 1 + 10 = -8 \]
\[ p(2) = 2 \cdot 2^3 - 3 \cdot 2^2 - 17 \cdot 2 + 10 = -20 \]
\[ p(3) = 2 \cdot 3^3 - 3 \cdot 3^2 - 17 \cdot 3 + 10 = -14 \]
\[ p(4) = 2 \cdot 4^3 - 3 \cdot 4^2 - 17 \cdot 4 + 10 = 22 \]
Polynomial Interpolation

\[ p(x) = 2x^3 - 3x^2 - 17x + 10 \]

Evaluate \( x \in \{1, 2, 3, 4\} \)

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
Polynomial Interpolation

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

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

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

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

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

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.

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

Vandermonde system
Let $p_d(X) = c_0 + c_1X + \cdots + c_dX^d \in \mathbb{Z}[X]$.

$\forall d \in \mathbb{N}$, Can interpolate $p_d(X)$ from $p_d(x_0), p_d(x_1), \ldots, p_d(x_d)$ if $x_0, x_1, \ldots$ 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
Let \( p_d(X) = c_0 + c_1X + \cdots + c_dX^d \in \mathbb{Z}[X] \).

For all \( d \in \mathbb{N} \), 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

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

Vandermonde system
Interpolating Univariate Polynomials

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

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

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

Vandermonde system
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 \textit{homogeneous} multivariate polynomial of degree \(d\).

\[ \forall d \in \mathbb{N}, \text{ Can interpolate } p_d(X, Y, Z) \text{ from } \]

\[ p_d(x_0, y_0, z_0), p_d(x_1, y_1, z_1), \ldots \]

\[ \uparrow \]

\[ ? \]

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

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

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

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 \( d \).

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

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

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 \( d \).

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

\[ p_d(x^0, y^0, z^0), p_d(x^1, y^1, z^1), \ldots \]

\[ \updownarrow \]

lattice condition

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

Vandermonde system
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

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

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

\[
2^i 3^j 5^k \neq 1.
\]
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

1. $i + j + k = 0$ and
2. $(i, j, k) \neq (0, 0, 0)$,

it follows that

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

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

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

Contradiction!
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.
“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.

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 $A_n$
Factorizations and Roots

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 $\mathbb{Z}$
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 \( \mathbb{Z} \)
Factorizations and Roots

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

$\Downarrow$

$p$ is irreducible over $\mathbb{Q}$

$\Uparrow$ (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 $p(x, y)$?

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

**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.
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

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

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

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

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

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

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

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

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

\begin{enumerate}
  \item \((a, b)\) integer solution to \( p(x, y) = 0 \) implies \( g_i(a, b) \in \mathbb{Z} \)
  \item \( g_i(x, y; i(x)) = o(1) \)
\end{enumerate}

Thus, \( g_i(x, y; i(x)) \notin \mathbb{Z} \) as \( x \to \infty \)
Proof Sketch

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

\[
\begin{align*}
    y_1(x) &= x^2 + 2x^{-1} + 2x^{-2} - 6x^{-4} - 18x^{-5} + O(x^{-6}), \\
    y_2(x) &= x^{3/2} - \frac{1}{2}x + \frac{1}{8}x^{1/2} - \frac{65}{128}x^{-1/2} - x^{-1} - \frac{1471}{1024}x^{-3/2} - x^{-2} + O(x^{-5/2}), \\
    y_3(x) &= -x^{3/2} - \frac{1}{2}x - \frac{1}{8}x^{1/2} + \frac{65}{128}x^{-1/2} - x^{-1} + \frac{1471}{1024}x^{-3/2} - x^{-2} + O(x^{-5/2}).
\end{align*}
\]

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

\[
    g_2(x, y_2(x)) = \Theta\left(\sqrt{x}\right)
\]
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 \( g_2(x, y) = \frac{y^2 + xy - x^3 + x}{x} = \frac{y^2}{x} + y - x^2 + 1 \)

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

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

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

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

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

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, $g_i(x,y_i(x)) \not\in \mathbb{Z}$ 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