Proving Dichotomy Theorems for Counting Problems

Jin-Yi Cai
University of Wisconsin, Madison

May 30, 2009

In Celebration of Les Valiant

Hard to believe one man did all these . . .

- **Computational Learning Theory. PAC Learning.**
- **Complexity of the Permanent, the class #P, and the Complexity of Counting Problems.**
- **Parallel computation, routing, Bulk Synchronous Model (BSP).**
- **Superconcentrators**
  Initially aimed for super linear lower bounds, then gave a linear size construction. First use of expanders. . . . (Golden, even not played out as initially thought.)
- **Algebraic complexity theory. The Determinant vs. Permanent Problem. VP and VNP.**
- **Space is more powerful than time (with Hopcroft and Paul). Pebble games.**

- **Formal Language theory, Equivalence problem for Deterministic PDA, Lindenmeyer Systems, Boolean matrix multiplication to $o(n^3)$ context free parsing.**
- **Randomized reduction of NP to UniqueSAT (with V. Vazirani).**
- **Interpolation technique.**
- **Matchgates, Holographic Algorithms and Reductions.**
- *Circuits of the Mind*.
- **Evolvability.**

. . .

Counting Problems

Valiant defined the class #P, and established the first #P-completeness results.

Most known NP-complete problems have counting versions which are #P-complete.

Some counting problems are #P-complete even though their corresponding decision problems are in P. e.g., #2SAT, Counting Perfect Matchings.

Counting PM over planar graphs is in P (Kasteleyn).

Three Frameworks for Counting Problems

1. **Graph Homomorphisms**

2. **Constrained Satisfaction Problems (CSP)**

3. **Holant Problems**

Graph Homomorphisms

Graph Homomorphisms or H-Coloring was defined by Lovász (1967).

Let

$$H = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

be a Triangle.

A graph homomorphism from G to H, is a mapping ξ from $V(G)$ to $V(H)$ such that

$$(u, v) \in E(G) \implies (\xi(u), \xi(v)) \in E(H).$$

I.e., ξ is a $\textsc{Three-Coloring}$ **of G.**

Graph Homomorphisms

The counting graph homomorphisms is the following counting problem.

Given any $m \times m$ **(symmetric) matrix** H**, consider all** **vertex assignments** $\xi : V(G) \to [m]$**.**

$$Z_H(G) = \sum_{\xi:V(G)\to[m]} \prod_{(u,v)\in E} H_{\xi(u),\xi(v)}.$$

H **can be viewed as a single binary (edge) function.**

Constraint Satisfaction Problems (CSP)

Consider a bipartite graph $G = (U, V, E)$.

Each $u \in U$ is a variable.

Each $v \in V$ is labeled by a constraint function.

Find an assignment that satisfies all constraints.

Counting version.

Constraint functions need not be 0-1 valued.

Holant Problems: A more general framework

Given $G = (V, E)$.

Put a function f_v at each $v \in V$. They take 0-1 inputs (or from some domain $[m]$) and output values in $\mathbb{R}$ or $\mathbb{C}$.

Now consider all 0-1 (or from $[m]$) assignments σ at every edge e.

The Holant Problem is to compute

$$\mathrm{Holant}(G) = \sum_{\sigma} \prod_{v} f_v(\sigma\mid_v).$$

CSP is the special case of Holant when all $u \in U$ are labeled with the Equality **function.**

Edge assignments can simulate vertex assignments.

Holant Problems: Matchings

Consider a graph $G = (V, E)$.

Put an AT-MOST-ONE **function f_v at each vertex $v \in V$.**
Now consider all 0-1 assignments σ to each $e \in E$,

$$\sum_{\sigma} \prod_{v} f_v(\sigma \mid_v).$$

Each 0-1 assignment σ corresponds to a subset of E.

This counts the number of Matchings in G.

Holant Problems: Perfect Matchings

Again, consider G.

Put an EXACT-ONE **function f_v at each vertex, and consider all 0-1 assignments σ to each $e \in E$,**

$$\sum_{\sigma} \prod_{v} f_v(\sigma \mid_v).$$

This counts the number of Perfect Matchings in G.

Holant Problems

As edge assignments can generally simulate vertex assignments, one can also easily write every CSP problem, or graph homomorphism problem, as a Holant Problem.

E.g., Vertex Covers, Independent Sets, k-Colorings, Induced subgraph of an Odd number of edges, etc.

Schaefer's Dichotomy Theorem

Schaefer's dichotomy theorem:

Replace Boolean OR by an arbitrary set of Boolean operators in the SAT problem.

Then the generalized SAT is either solvable in P or NP-complete.

Creignou and Hermann proved a dichotomy theorem for counting SAT problems: Either solvable in P or #P-complete.

CSP Problems

The Feder and Vardi conjecture on (decision) CSP problems.

Creignou, Khanna and Sudan:

Complexity classifications of boolean constraint satisfaction problems.

SIAM Monographs on Discrete Mathematics and Applications. 2001.

Bulatov's Dichotomy Theorem

Consider any set of 0-1 valued constrained functions.

Dichotomy theorem for #CSP (for 0-1 valued functions) by Bulatov (2008).

Every problem in this class is either solvable in P or is #P-complete.

Proof involves deep results from the structural theory of universal algebra.

May not be effective.

Dichotomy Theorems for more general Constraint Functions

Dyer, Goldberg and Jerrum (2007) gave a Dichotomy Theorem for all Boolean #CSP, where all functions take real values.

Cai, Lu and Xia (2008) gave a Dichotomy Theorem for all Boolean #CSP, where all functions take complex values.

With positive and negative values, or more generally with complex values, there are possible cancelations, and this could yield new interesting tractable computations.

Constrast that with permanent vs. determinant
or generally monotone vs. non-monotone complexity.

Dichotomy Theorems for Graph Homomorphisms

Theorem (Hell and Nešetřil)
Dichotomy Theorem for the decision Graph Homomorphism problem: Either in P or NP-complete.

Theorem (Dyer and Greenhill)
Dichotomy Theorem for $Z_H(G)$, for all 0-1 H: Either in P or #P-hard.

Theorem (Bulatov and Grohe)
Dichotomy Theorem for $Z_H(G)$, for all non-negative H.

Theorem (Dyer, Goldberg and Paterson)
Dichotomy Theorem for all directed and acyclic H.

Graph Homomorphisms when cancelations happen

When cancelations happen, there are new non-trivial tractable cases.

Dichotomy Theorems are harder to prove: Essentially it will amount to the claim that what we don't know how to solve efficiently must be provably hard.

Theorem (Goldberg, Grohe, Jerrum and Thurley)
Dichotomy Theorem for $Z_H(G)$, for all real H.

Theorem (Cai, Chen and Lu)
Dichotomy Theorem for $Z_H(G)$, for all complex H.

Three Families by Holographic Algorithms

Using holographic algorithms we discovered that

$$\mathcal{F}_1 = \{\, \lambda([1,0]^{\otimes k} + i^r[0, \quad 1]^{\otimes k}) \mid \lambda \in \mathbb{C},\ k = 1, 2, \ldots, \&\ r = 0, 1, 2, 3 \,\}$$

$$\mathcal{F}_2 = \{\, \lambda([1,1]^{\otimes k} + i^r[1, -1]^{\otimes k}) \mid \lambda \in \mathbb{C},\ k = 1, 2, \ldots, \&\ r = 0, 1, 2, 3 \,\}$$

$$\mathcal{F}_3 = \{\, \lambda([1, \ i]^{\otimes k} + i^r[1, -i]^{\otimes k}) \mid \lambda \in \mathbb{C},\ k = 1, 2, \ldots, \&\ r = 0, 1, 2, 3 \,\}$$

give rise to tractable problems:

Holant(Ω) **for any** $\Omega = (G, \mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3)$ **is in P.**

2-3 Regular Bipartite Graphs

$G = (U, V, E), \qquad \deg(u) = 3 \quad \forall u \in U,$ **and** $\deg(v) = 2 \quad \forall v \in V.$

The most restrictive family where hardness occurs.

Consider the complexity of Holant problems, where

$$\text{Holant}(\Omega) = \sum_{\sigma} \prod_{v \in V} F_v(\sigma \mid_{E(v)}).$$

Notation for symmetric signatures: $[f_0, f_1, \ldots, f_n]$**.**

Let's consider Boolean signatures: $f_i = 0, 1$**.**

Includes Vertex Cover, Perfect Matching etc.

A Dichotomy Theorem

Theorem

Every counting problem $\text{Holant}([x_0, x_1, x_2] \,|\, [y_0, y_1, y_2, y_3])$**, where** $[x_0, x_1, x_2]$ **and** $[y_0, y_1, y_2, y_3]$ **are Boolean signatures, is either**

- **in P; or**
- **#P-complete but solvable in P for planar graphs; or**
- **#P-complete even for planar graphs.**

Two brilliant ideas of Valiant

To prove this dichotomy theorem, we will use, not one, but two great ideas of Valiant.

The First Step: Holographic algorithms and reductions.

To show $\text{Holant}([x_0, x_1, x_2] \big| [y_0, y_1, y_2, y_3])$ **is #P-Complete, we use holographic reductions to reduce either**

$$[0, 1, 1] \big| [1, 0, 0, 1]$$

or

$$[1, 0, 1] \big| [1, 1, 0, 0]$$

to

$$[z_0, z_1, z_2] \big| [y_0, y_1, y_2, y_3]$$

for some z_0, z_1 **and** z_2**.**

The first is Vertex Cover, the second is Matching.

Second Step

Second, to show that $\text{Holant}([x_0, x_1, x_2] \big| [y_0, y_1, y_2, y_3])$ **is #P-Complete, we show how the pair**

$$[x_0, x_1, x_2] \big| [y_0, y_1, y_2, y_3]$$

can "simulate" (or "interpolate")

$$[z_0, z_1, z_2] \big| [y_0, y_1, y_2, y_3]$$

In fact, we show how to "simulate" $[x, y, z] \big| [y_0, y_1, y_2, y_3]$ **for all** $[x, y, z]$**.**

Interpolation Method

The second idea is also due to Valiant: Interpolation.

This has been further developed by

- **Vadhan**
- **Dyer**
- **Greenhill**
- **Bulatov**
- **Dalmau**
- **Grohe**
- **Creignou**
- **Hermann**
- **Goldberg**

- **Jerrum**
- **Xia-Zhang-Zhao**
- **Goldberg-Grohe-Jerrum-Thurley, . . .**

Interpolation Method

Given $\Omega = (G, [x, y, z] \Big| [y_0, y_1, y_2, y_3])$**. Let**

$$f = [x, y, z].$$

$f(00) = x$**,** $f(01) = f(10) = y$ **and** $f(11) = z$**.**

$V_f =$ **the subset of** V **assigned** f **in** Ω**.**

$|V_f| = n$**.**

An Expression for Holant

$$\text{Holant}(\Omega) = \sum_{i+j+k=n} c_{i,j,k} x^i y^j z^k,$$

$c_{i,j,k} =$ **is the sum over all edge assignments σ, of products of evaluations at all $v \in V(G) - V_f$, where σ satisfies the property that the number of vertices in V_f having exactly 0 or 1 or 2 incident edges assigned 1 is i or j or k, respectively.**

Holant(Ω_s)

A sequence of gadgets N_s will be recursively constructed, not using f, having signature $f_s = [x_s, y_s, z_s]$.

Replace f by f_s in Ω.

$$\text{Holant}(\Omega_s) = \sum_{i+j+k=n} c_{i,j,k} x_s^i y_s^j z_s^k. \tag{1}$$

The same set of values $c_{i,j,k}$ occur.

$c_{i,j,k}$ is independent of s.

Now consider (1) as a linear system in the unknowns $c_{i,j,k}$.

Recursive Relation

With some initial gadget, the sequence of gadgets N_s will have signatures $f_s = [x_s, y_s, z_s]$ satisfying

$$\begin{bmatrix} x_s \\ y_s \\ z_s \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} x_{s-1} \\ y_{s-1} \\ z_{s-1} \end{bmatrix}. \qquad (2)$$

Interpolation Theorem

Theorem

Suppose the recurrence matrix A satisfies

1. $\det(A) \neq 0$**,**
2. **The initial signature $[x_0, y_0, z_0]$ is not orthogonal to any row eigenvector of A, and**
3. **For all $(i, j, k) \in \mathbf{Z}^3 - \{(0,0,0)\}$ with $i + j + k = 0$,**

$$\alpha^i \beta^j \gamma^k \neq 1.$$

Then all $c_{i,j,k}$ can be computed in polynomial time.

An Algebraic Condition via Galois Theory

The key condition is the lattice condition:

For all $(i, j, k) \in \mathbf{Z}^3 - \{(0,0,0)\}$ **with** $i + j + k = 0$**,**

$$\alpha^i \beta^j \gamma^k \neq 1.$$

Lemma

Let $f(x) = x^3 + c_2 x^2 + c_1 x + c_0 \in \mathbf{Q}[x]$**, with roots** α**,** β **and** γ**.**

It is decidable in P whether the lattice condition holds.

If f **is irreducible, except of the form** $x^3 + c$ **for some** $c \in \mathbf{Q}$**, the condition holds.**

An example

The counting problem $\text{Holant}([1,1,0]\big|[1,1,1,0])$**.**

A recursive construction gives the following recursive relation:

$$\begin{bmatrix} a_i \\ b_i \\ c_i \end{bmatrix} = \begin{bmatrix} 7191 & 12618 & 5535 \\ 3816 & 6723 & 2961 \\ 2025 & 3582 & 1584 \end{bmatrix} \begin{bmatrix} a_{i-1} \\ b_{i-1} \\ c_{i-1} \end{bmatrix}.$$

Characteristic polynomial

$$\chi(x) = x^3 - 15498x^2 + 419904x - 19683.$$

$$\Longrightarrow$$

#P-complete

The complexity of complexity proof

One can easily contemplate moderately sized gadgets with over 50 or 100 edges, say, and then to verify a particular gadget works, it may require the computation of 2^{100} steps, far exceeding most cryptosystems such as DES.

Is 2^{100}-step computation as part of the proof a constant?

Are we getting a glimpse at a structural asymptotic intractability only perceivable with 2^{100}-step computation?

HAPPY BIRTHDAY, LES!