Post's Problem Revisited

—

A Complexity Dichotomy Perspective

Jin-Yi Cai
Computer Sciences Dept
University of Wisconsin, Madison

Nov 6, 2012

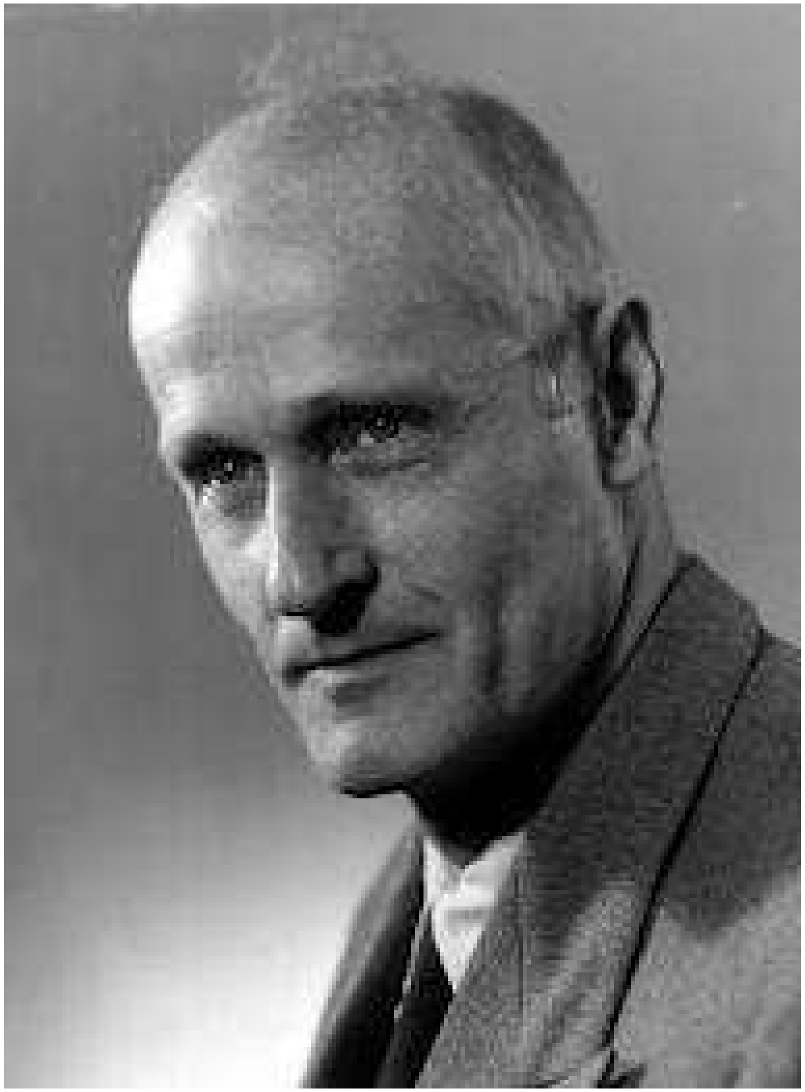
Supported by NSF CCF-0914969.

Hilbert

Entscheidungsproblem

The rigorous foundation of Computability Theory was established in the 1930s, . . .

Answering a question of Hilbert



Computable yet Not Efficiently Computable

Given N, how fast can one factor it?

$N = 57720721296971833203785791172827243$1**?**

$$\begin{aligned} N' \quad &= \quad 1375629587706555072328637871393012064224421883558006 2\\ &\quad\quad 5186902271294765416798340629392379444118675259? \end{aligned}$$

$$N = 9361973132609 \times 616544402332483406165559$$

$$\begin{aligned} N' &= 1471865453993855302660887614137521979 \times \\ &\quad 93461639715357977769163558199606896584051237541638188580280321 \end{aligned}$$

P and NP

P is deterministic polynomial time.

e.g. Determinant, Graph Matching (monomer-dimer problem), Max-Flow Min-Cut.

NP is non-deterministic polynomial time.

For any given instance x, it is a Yes instance iff there is a short proof which can be checked in P.

e.g. SATisfiability, Graph 3-Coloring, Hamiltonian Circuit, Clique, Vertex Cover, Traveling Salesman, etc.

Also, Factoring, Graph Isomorphism, etc.

Analogues of recursive and r.e.

The P vs. NP Question

It is generally conjectured that many combinatorial problems in the class NP are not computable in polynomial time.

Conjecture: $\mathrm{P} \neq \mathrm{NP}$.

$\mathrm{P} =^{?} \mathrm{NP}$ is: Is there a universal and efficient method to discover a mathematical proof when one exists?

Can “clever guesses” be systematically eliminated?

This is the analogue of $0 \neq 0'$.

What a topologist has to say

For the pure mathematician the boundary that Gödel delineated between decidable and undecidable, recursive and nonrecursive, has an attractive sharpness that declares itself as a phenomenon of absolutes. In contrast, the complexity classes of computer science for example P and NP require an asymptotic formulation and . . . demand a bit of patience before their fundamental character is appreciated.

— Michael Freedman

#P

Counting problems:

#SAT: How many satisfying assignments are there in a Boolean formula?

#PerfMatch: How many perfect matchings (Dimer Problem) are there in a graph?

#P is at least as powerful as NP, and in fact subsumes the entire polynomial time hierarchy $\cup_i \Sigma_i^p$ [Toda].

#P-completeness: #SAT, #PerfMatch, Permanent, etc.

Post’s Problem

The Turing degrees were introduced by Emil Post in 1944.

Many fundamental results were established by Kleene and Post by 1954.

The Post Problem asks whether there exists any r.e. degree strictly between 0 and 0’.

This was solved by the famous Friedberg-Muchnik Theorem.

Priority argument.

The degree structure is very complicated.

Friedberg-Muchnik like Theorems in Complexity

Ladner in 1975 showed that, if P $\neq$ NP, then there are problems in NP that are neither in the class P nor NP-complete.

The same argument proves the parallel result for #P.

However all such problems are “artificial” or otherwise uninteresting.

They are specifically constructed to be neither in P nor complete.

Schaefer's Dichotomy Theorem

If we consider Boolean satisfaction type problems, Schaefer proved a sort of anti-Friedberg-Muchnik Theorem, called a Dichotomy Theorem:

Consider any finite set S of Boolean predicates (e.g., Bollean OR, At-Most-One, Not-All-Equal, Boolean XOR, etc.)

Now consider the Constraint-Satisfaction-Problem (CSP) defined by this set S:

Input: $X = \{x_1, x_2, \ldots, x_n\}$, and a collection of constraints from S applied to X.

Output: Is there an assignment $\sigma : X \rightarrow \{0, 1\}$ such that all constraints are satisfied?

Schaefer's Dichotomy Theorem

For any finite set S of Boolean predicates the problem CSP(S) is either solvable in P or NP-complete.

Creignou-Hermann Theorem

Any finite set S of Boolean predicates defines a counting CSP problems

Input: $X = \{x_1, x_2, \ldots, x_n\}$, and a collection of constraints from S applied to X.

Output: How many assignments $\sigma : X \to \{0, 1\}$ satisfy all constraints?

Creignou-Hermann Theorem:

For any finite set S of Boolean predicates, #CSP(S) is either solvable in Polynomial time or #P-complete.

Feder-Vardi Conjecture

Any finite set S of predicates over any finite domain set D, the decision CSP problem CSP(S) is either in P or NP-complete.

Analagously, for the counting CSP problem #CSP(S).

The Feder-Vardi Conjecture is open, except for domain size 2 and 3.

For domain size 3, this is a major achievement by Bulatov.

Counting Dichotomies

Three frameworks:

- **Graph Homomorphisms.**
- **Counting CSP problems.**
- **Holant Problems.**

In all three frameworks we have proved Complexity Dichotomies.

An Example

Consider counting Vertex Covers**:**

$G = (V, E)$**.**

Attach an OR **function on two bits at every** $e \in E$**.**

Represent the OR **by a truth table** $F = (0, 1, 1, 1)$**, call it a signature.**

Consider all $\sigma : V \to \{0, 1\}$**:**

$$\sigma \textbf{ is a vertex cover} \iff \prod_{(x,y)\in E} F(\sigma(x), \sigma(y)) = 1$$

$$\sum_{\sigma} \prod_{(x,y)\in E} F(\sigma(x), \sigma(y))$$

counts the number of vertex covers.

Graph Homomorphism

Let $\mathbf{A} = (A_{i,j}) \in \mathbb{C}^{m\times m}$ be a symmetric complex matrix.

The graph homomorphism problem GH(A) is:

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

OUTPUT:

$$Z_{\mathbf{A}}(G) = \sum_{\xi: V \to [m]} \prod_{(u,v)\in E} A_{\xi(u),\xi(v)}.$$

ξ is an assignment to the vertices of G and

$$\mathbf{wt}_{\mathbf{A}}(\xi) = \prod_{(u,v)\in E} A_{\xi(u),\xi(v)}$$

is called the weight of ξ.

Some Examples

Let

$$\mathbf{A} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

This matrix is the truth table of the Boolean Or. $Z_{\mathbf{A}}$ **counts the number of** Vertex Covers **in** G**.**

Let

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

then $Z_{\mathbf{A}}$ **counts the number of** Three-Colorings **in** G**.**

Some More Examples

Let

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{pmatrix}$$

then $Z_{\mathbf{A}}$ counts the number of k-$\textsc{Colorings}$ **in G.**

Let

$$\mathbf{A} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

then $Z_{\mathbf{A}}$ is equivalent to counting the number of induced subgraphs of G with an even number of edges.

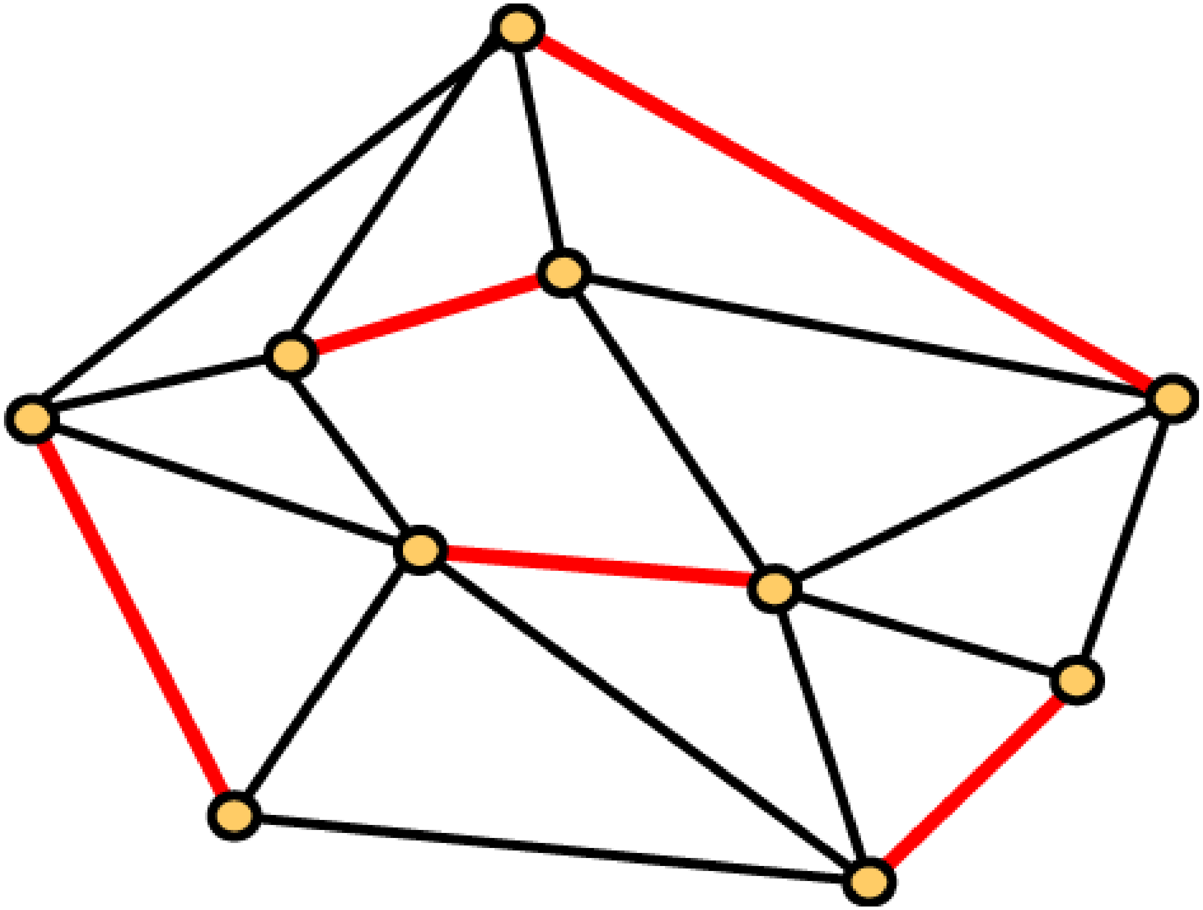
Graph homomorphism

Lovász first studied Graph homomorphisms.

L. Lovász: Operations with structures, Acta Math. Hung. 18 (1967), 321-328.

`http://www.cs.elte.hu/~lovasz/hom-paper.html`

Perfect Matchings



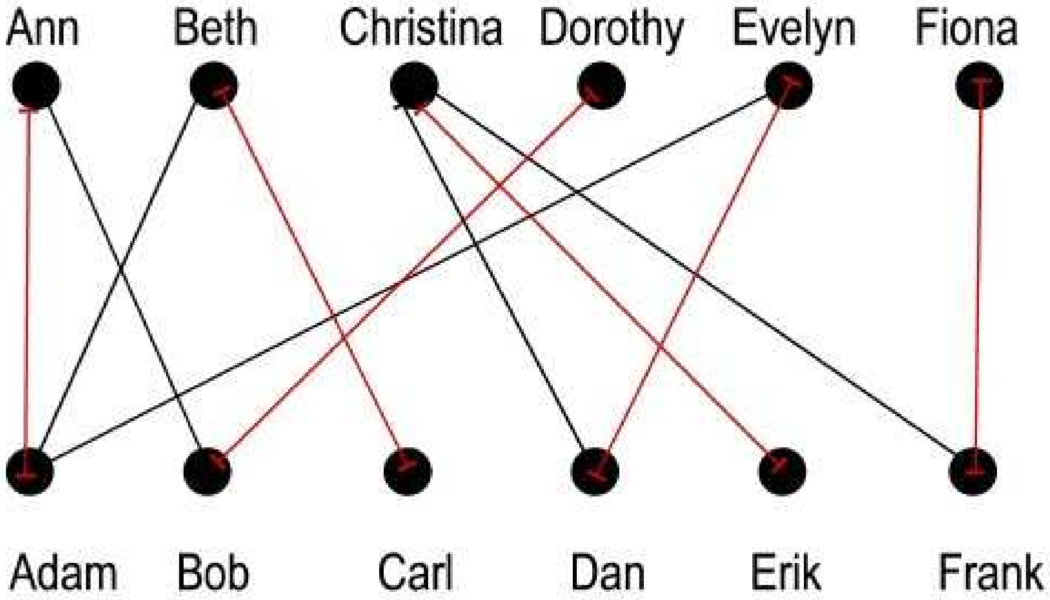


Figure 2 A perfect matching

Edge Assignments

$G = (V, E)$.

Now attach $F =$ the EXACT-ONE function at each $v \in V$.

Consider all edge assignments $\sigma : E \to \{0, 1\}$:

$$\sigma \text{ is a } \textbf{perfect matching} \iff \prod_{v \in V} F(\sigma|_{E(v)}) = 1$$

$$\text{Holant}(G) = \sum_{\sigma} \prod_{v \in V} F(\sigma|_{E(v)})$$

counts the number of perfect matchings. Here $E(v)$ are the incident edges of v.

Edge assignments are more general, can simulate vertex assignments.

Graph Homomorphisms with 0-1 Matrices

Theorem (Dyer and Geenhill)

Let $\mathbf{A} \in \mathbb{R}^{m \times m}$ be a symmetric 0-1 matrix. Let H be the graph whose adjacency matrix is $\mathbf{A}$.

Then $Z_{\mathbf{A}}$ is either computable in P-time, or #P-complete.

Dichotomy criterion: Each connected component of H is either a complete graph with all self-loops present, or a complete bipartite graph with no self-loops.

Non-negative Matrices

Theorem (Bulatov and Grohe)

Let A $\in \mathbb{R}^{m\times m}$ be a symmetric and connected matrix with non-negative entries:

- **If A is bipartite, then GH(A) is in polynomial time if the rank of A is at most 2; otherwise GH(A) is #P-hard.**
- **If A is not bipartite, then GH(A) is in polynomial time if the rank of A is at most 1; otherwise GH(A) is #P-hard.**

Real Matrices

Theorem (Goldberg, Jerrum, Grohe and Thurley)
There is a complexity dichotomy theorem for GH(A).

For any symmetric real matrix $\mathbf{A} \in \mathbb{R}^{m \times m}$, the problem of computing $Z_{\mathbf{A}}(G)$, for any input G, is either in P or #P-hard.

A Complete Dichotomy Theorem for GH

Theorem (C, Chen and Lu)

There is a complexity dichotomy theorem for GH($\mathbf{A}$).

For any symmetric complex vlaued matrix $\mathbf{A} \in \mathbb{C}^{m\times m}$, the problem of computing $Z_{\mathbf{A}}(G)$, for any input G, is either in P or #P-hard.

The tractability criterion is decidable.

http://arxiv.org/abs/0903.4728

(121 pages.)

Overview

The proof consists of two parts: the hardness part and the tractability part.

The hardness part can be viewed as three filters which remove hard $Z_{\mathbf{A}}$ problems using different arguments.

In the tractability part, we show that all the $Z_{\mathbf{A}}$ problems that survive the three filters are indeed polynomial-time solvable.

Ultimately, tractable $Z_{\mathbf{A}}$ problems *roughly* correspond to rank one modifications of tensor products of Fourier matrices. (… Not quite true literally …).

A Peek Under the Hood

“A mathematics lecture without a proof is like a movie without a love scene.”

— Hendrik Lenstra

Discrete Unitary

Definition

Let $\mathbf{A} = (A_{i,j}) \in \mathbb{C}^{m\times m}$. We say $\mathbf{A}$ is an M-discrete unitary matrix, for some positive integer M, if

1. **Every entry $A_{i,j}$ is a power of $\omega_M = e^{2\pi\sqrt{-1}/M}$;**
2. **M = lcm of the orders of $F_{i,j}$;**
3. **$A_{1,i} = A_{i,1} = 1$ for all $i \in [m]$;**
4. **For all $i \neq j \in [m]$, $\langle \mathbf{A}_{i,*}, \mathbf{A}_{j,*}\rangle = 0$ and $\langle \mathbf{A}_{*,i}, \mathbf{A}_{*,j}\rangle = 0$.**

Inner product $\langle \mathbf{A}_{i,*}, \mathbf{A}_{j,*}\rangle = \sum_{k=1}^{m} \mathbf{A}_{i,k}\overline{\mathbf{A}_{j,k}}$.

Some Simple Examples

$$\mathbf{H_2} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \mathbf{H_4} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},$$

$$\boldsymbol{\mathcal{F}}_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, \quad \boldsymbol{\mathcal{F}}_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \zeta & \zeta^{-1} & \zeta^2 & \zeta^{-2} \\ 1 & \zeta^2 & \zeta^{-2} & \zeta^{-1} & \zeta \\ 1 & \zeta^{-1} & \zeta & \zeta^{-2} & \zeta^2 \\ 1 & \zeta^{-2} & \zeta^2 & \zeta & \zeta^{-1} \end{pmatrix},$$

where $\omega = e^{2\pi i/3}$ **and** $\zeta = e^{2\pi i/5}$**.**

A Group Condition

Theorem

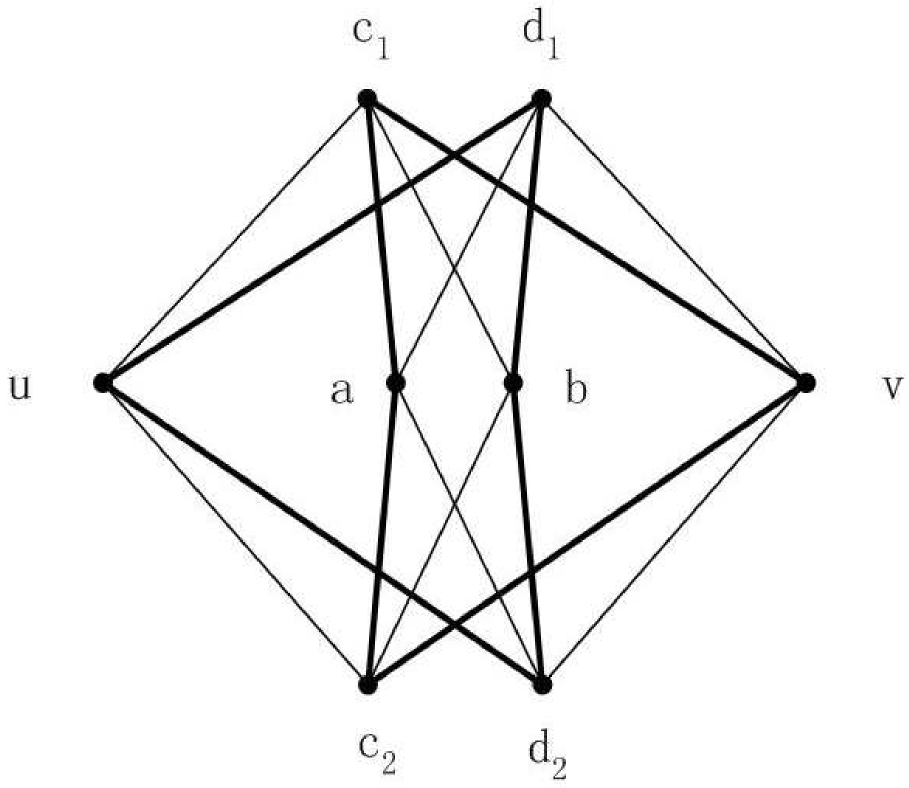
Let A be a symmetric M-discrete unitary matrix. Then

- **either $Z_{\mathbf{A}}(\cdot)$ is #P-hard,**
- **or A must satisfy the following Group-Condition *(GC)*:**

  $\forall\ i, j \in [0 : m-1]$, $\exists\ k \in [0 : m-1]$ such that $\mathbf{A}_{k,*} = \mathbf{A}_{i,*} \circ \mathbf{A}_{j,*}$.

$\mathbf{v} = \mathbf{A}_{i,*} \circ \mathbf{A}_{j,*}$ is the Hadamard product with $v_\ell = \mathbf{A}_{i,\ell} \cdot \mathbf{A}_{j,\ell}$.

A Gadget Construction



Special case $p = 2$. Thick edges denote $M - 1$ parallel edges.

An Edge Gets Replaced

Replacing every edge e by the gadget . . .

$$G \quad \Longrightarrow \quad G^{[p]}.$$

Define $G^{[p]} = (V^{[p]}, E^{[p]})$ **as**

$$V^{[p]} = V \cup \{a_e, b_e, c_{e,1}, \ldots, c_{e,p}, d_{e,1}, \ldots, d_{e,p} \mid e \in E\}$$

and $E^{[p]}$ **contains exactly the following edges:** $\forall e = uv \in E$**, and** $\forall 1 \le i \le p$**,**

1. **One edge between** $(u, c_{e,i})$**,** $(c_{e,i}, b_e)$**,** $(d_{e,i}, a_e)$**, and** $(d_{e,i}, v)$**;**
2. $M - 1$ **edges between** $(c_{e,i}, v)$**,** $(c_{e,i}, a_e)$**,** $(d_{e,i}, b_e)$**, and** $(d_{e,i}, u)$**.**

A Reduction

$\forall p \geq 1$, there is a symmetric matrix $\mathbf{A}^{[p]} \in \mathbb{C}^{2m \times 2m}$ which only depends on $\mathbf{A}$, such that

$$Z_{\mathbf{A}^{[p]}}(G) = Z_{\mathbf{A}}(G^{[p]}), \quad \textbf{for all } G.$$

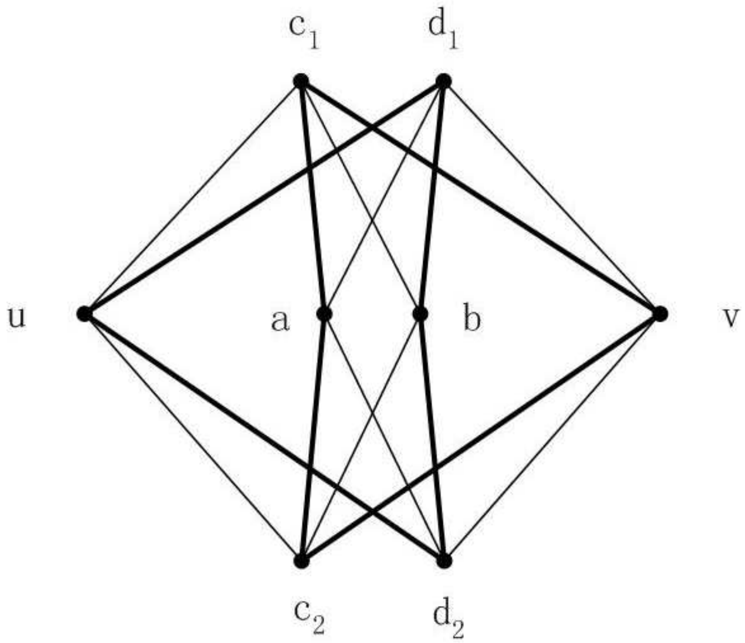
Thus $Z_{\mathbf{A}^{[p]}}(\cdot)$ is reducible to $Z_{\mathbf{A}}(\cdot)$, and therefore

$Z_{\mathbf{A}}(\cdot)$ **is not #P-hard**

$$\Longrightarrow$$

$Z_{\mathbf{A}^{[p]}}(\cdot)$ **is not #P-hard for all $p \geq 1$.**

Expression for $\mathbf{A}^{[p]}$



The $(i,j)^{th}$ entry of $\mathbf{A}^{[p]}$, where $i,j \in [0:m-1]$, is

$$A_{i,j}^{[p]} = \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \left(\sum_{c=0}^{m-1} A_{i,c} \overline{A_{a,c}} A_{b,c} \overline{A_{j,c}} \right)^p \left(\sum_{d=0}^{m-1} \overline{A_{i,d}} A_{a,d} \overline{A_{b,d}} A_{j,d} \right)^p .$$

Note $(A_{a,c})^{M-1} = \overline{A_{a,c}}$, etc.

Properties of $\mathbf{A}^{[p]}$

$$\begin{aligned} A^{[p]}_{i,j} &= \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \left| \sum_{c=0}^{m-1} A_{i,c} \overline{A_{a,c}} A_{b,c} \overline{A_{j,c}} \right|^{2p} \\ &= \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \left| \langle \mathbf{A}_{i,*} \circ \overline{\mathbf{A}_{j,*}}, \mathbf{A}_{a,*} \circ \overline{\mathbf{A}_{b,*}} \rangle \right|^{2p}, \end{aligned}$$

$\mathbf{A}^{[p]}$ is symmetric and non-negative. In fact $A^{[p]}_{i,j} > 0$. (By taking $a = i$ and $b = j$).

Diagonal and Off-Diagonal

$$A^{[p]}_{i,i} = \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \left| \langle \mathbf{1}, \mathbf{A}_{a,*} \circ \overline{\mathbf{A}_{b,*}} \rangle \right|^{2p} = \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} |\langle \mathbf{A}_{a,*}, \mathbf{A}_{b,*} \rangle|^{2p} .$$

As A is a discrete unitary matrix, we have $A^{[p]}_{i,i} = m \cdot m^{2p}$**.**

$Z_{\mathbf{A}}(\cdot)$ **is not #P-hard**

$\Longrightarrow$ **(by a known result for non-negative matrices)**

$$\det \begin{pmatrix} A^{[p]}_{i,i} & A^{[p]}_{i,j} \\ A^{[p]}_{j,i} & A^{[p]}_{j,j} \end{pmatrix} = 0.$$

and thus $A^{[p]}_{i,j} = m^{2p+1}$ **for all** $i, j \in [0 : m - 1]$**.**

Another Way to Sum $A_{i,j}^{[p]}$

$$\begin{aligned} A_{i,j}^{[p]} &= \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \left| \langle \mathbf{A}_{i,*} \circ \overline{\mathbf{A}_{j,*}}, \mathbf{A}_{a,*} \circ \overline{\mathbf{A}_{b,*}} \rangle \right|^{2p} \\ &= \sum_{x \in X_{i,j}} s_{i,j}^{[x]} \cdot x^{2p}, \end{aligned}$$

where $s_{i,j}^{[x]}$ is the number of pairs (a, b) such that

$$x = \left| \langle \mathbf{A}_{i,*} \circ \overline{\mathbf{A}_{j,*}}, \mathbf{A}_{a,*} \circ \overline{\mathbf{A}_{b,*}} \rangle \right|.$$

Note that $s_{i,j}^{[x]}$, for all x, do not depend on p.

A Linear System

So

$$A_{i,j}^{[p]} = \sum_{x \in X_{i,j}} s_{i,j}^{[x]} \cdot x^{2p}.$$

Meanwhile, it is also known that for all $p \geq 1$,

$$A_{i,j}^{[p]} = m^{2p+1}.$$

We can view, for each i and j fixed,

$$\sum_{x \in X_{i,j}} s_{i,j}^{[x]} \cdot x^{2p} = m^{2p+1}$$

as a linear system $(p = 1, 2, 3, \ldots)$ in the unknowns $s_{i,j}^{[x]}$.

A Vandermonde System

It is a Vandermonde system.

We can "solve" it, and get $X_{i,j} = \{0, m\}$,

$$s_{i,j}^{[m]} = m \quad \textbf{and} \quad s_{i,j}^{[0]} = m^2 - m, \quad \textbf{for all } i, j \in [0 : m-1].$$

This implies that for all $i, j, a, b \in [0 : m-1]$,

$$|\langle \mathbf{A}_{i,*} \circ \overline{\mathbf{A}_{j,*}}, \mathbf{A}_{a,*} \circ \overline{\mathbf{A}_{b,*}} \rangle| \textbf{ is either } m \textbf{ or } 0.$$

Toward Group Condition

Set $j = 0$. **Because** $\mathbf{A}_{0,*} = \mathbf{1}$, **we have**

$$|\langle \mathbf{A}_{i,*} \circ \mathbf{1}, \mathbf{A}_{a,*} \circ \overline{\mathbf{A}_{b,*}} \rangle| = |\langle \mathbf{A}_{i,*} \circ \mathbf{A}_{b,*}, \mathbf{A}_{a,*} \rangle|,$$

which is either m **or** 0, **for all** $i, a, b \in [0 : m-1]$.

Meanwhile, as $\{\mathbf{A}_{a,*}, a \in [0 : m-1]\}$ **is an orthogonal basis, where each** $||\mathbf{A}_{a,*}||^2 = m$, **by Parseval's Equality, we have**

$$\sum_a |\langle \mathbf{A}_{i,*} \circ \mathbf{A}_{b,*}, \mathbf{A}_{a,*} \rangle|^2 = m\|\mathbf{A}_{i,*} \circ \mathbf{A}_{b,*}\|^2.$$

Consequence of Parseval

Since every entry of $\mathbf{A}_{i,*} \circ \mathbf{A}_{b,*}$ is a root of unity, $\|\mathbf{A}_{i,*} \circ \mathbf{A}_{b,*}\|^2 = m$. Hence

$$\sum_a |\langle \mathbf{A}_{i,*} \circ \mathbf{A}_{b,*}, \mathbf{A}_{a,*} \rangle|^2 = m^2.$$

Recall

$$|\langle \mathbf{A}_{i,*} \circ \mathbf{A}_{b,*}, \mathbf{A}_{a,*} \rangle| \text{ **is either** } m \text{ **or** } 0.$$

As a result, for all $i, b \in [0 : m-1]$, there exists a unique a such that $|\langle \mathbf{A}_{i,*} \circ \mathbf{A}_{b,*}, \mathbf{A}_{a,*} \rangle| = m$.

A Sum of Roots of Unity

Every entry of $\mathbf{A}_{i,*}, \mathbf{A}_{b,*}$ and $\mathbf{A}_{a,*}$ is a root of unity.

Denote the inner product of rows $\langle \mathbf{A}_{i,*} \circ \mathbf{A}_{b,*}, \mathbf{A}_{a,*} \rangle$ is a sum of m terms each of complex norm 1. To sum to a compelx number of norm m, they must be all aligned exactly the same.

Thus,

$$\mathbf{A}_{i,*} \circ \mathbf{A}_{b,*} = e^{i\theta} \mathbf{A}_{a,*}.$$

But $\mathbf{A}_{i,1} = \mathbf{A}_{a,1} = \mathbf{A}_{b,1} = 1$. Hence

$$\mathbf{A}_{i,*} \circ \mathbf{A}_{b,*} = \mathbf{A}_{a,*}.$$

What is Polynomial Time Computable?

A peek of what is tractable.

Fourier Matrices

Let $m \geq 1$**. Let** $k \geq 1$ **and** $\gcd(k, m) = 1$**.**

Let $\omega = e^{2\pi ik/m}$ **and** $x, y \in [0 : m-1]$**. Then A is an** $m \times m$ **Fourier matrix if the** $(x, y)^{th}$ **entry is** ω^{xy}**.**

$$\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \omega & \omega^2 & \ldots & \omega^{m-1} \\ 1 & \omega^2 & \omega^4 & \ldots & \omega^{2(m-1)} \\ 1 & \omega^3 & \omega^6 & \ldots & \omega^{3(m-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{m-1} & \omega^{2(m-1)} & \ldots & \omega^{(m-1)^2} \end{pmatrix}$$

Quadratic Polynomial

Let m be any positive integer. The input is a quadratic polynomial

$$f(x_1, x_2, \ldots, x_n) = \sum_{i,j \in [n]} a_{i,j} x_i x_j,$$

where $a_{i,j} \in \mathbb{Z}_m$ for all i, j; and the output is

$$Z_m(f) = \sum_{x_1,\ldots,x_n \in \mathbb{Z}_m} \omega_m^{f(x_1,\ldots,x_n)}.$$

Theorem

This problem can be solved in polynomial time.

Use Gauss sums.

Gauss Sums

For a prime p, the Gauss sum is

$$G_p = \sum_{x \in \mathbb{Z}_p} \left(\frac{x}{p}\right) \omega^x,$$

where $\left(\frac{c}{p}\right)$ is the Legendre symbol.

G_p has the closed form

$$G_p = \begin{cases} \pm\sqrt{p}, & \textbf{if } p \equiv 1 \bmod 4 \\ \pm i\sqrt{p}, & \textbf{if } p \equiv 3 \bmod 4 \end{cases}$$

Gauss Sums

For a prime p, the Gauss sum is

$$G_p = \sum_{x \in \mathbb{Z}_p} \left(\frac{x}{p}\right) \omega^x,$$

where $\left(\frac{c}{p}\right)$ is the Legendre symbol.

G_p has the closed form

$$G_p = \begin{cases} +\sqrt{p}, & \textbf{if } p \equiv 1 \bmod 4 \\ +i\sqrt{p}, & \textbf{if } p \equiv 3 \bmod 4 \end{cases}$$

“Elegant Theorem” of the Sign

Gauss knew since 1801 that $G_p^2 = \left(\frac{-1}{p}\right) p$**. Thus**

$$G_p = \begin{cases} \pm\sqrt{p}, & \textbf{if } p \equiv 1 \bmod 4 \\ \pm i\sqrt{p}, & \textbf{if } p \equiv 3 \bmod 4 \end{cases}$$

The fact that G_p **always takes the sign** $+$ **was conjectured by Gauss in his diary in May 1801, and solved on Sept 3, 1805.**

... Seldom had a week passed for four years that I had not tried in vein to prove this very elegant theorem mentioned in 1801 ...
"Wie der Blitz einschlägt, hat sich das Räthsel gelöst ..."
("as lightning strikes, was the puzzle solved ...").

—**C. F. Gauss, Sept. 3, 1805.)**

A Complexity Trichotomy for Planar CSP

Theorem

Let $\mathcal{F}$ be any finite set of real-valued symmetric constraint functions on Boolean variables. Then there are precisely three classes of #CSP($\mathcal{F}$) problems, depending on $\mathcal{F}$.
(1) #CSP($\mathcal{F}$) is in P.
(2) #CSP($\mathcal{F}$) is #P-hard, but solvable in P for planar inputs.
(3) #CSP($\mathcal{F}$) is #P-hard even for planar inputs.

Furthermore $\mathcal{F}$ is in class (2) iff there is a holographic algorithm based on matchgates and the planar problems are solved by the FKT algorithm for Perfect Matchings.

Back to Post's Problem

Is there a subclass of problems, which are "natural", "interesting", and "non-artificial", which one can carve out of r.e. sets in Recursion Theory, for which one can develop a parallel theory, where the answer to Post's Problem is opposite of the Friedberg-Muchnik Theorem.

If yes, I hope the theory is mathematically deep, and with many connections to other parts of mathematics.

Is there an opportunity for Complexity Theory and Recursion Theory get back together again?

Some References

Some papers can be found on my web site

`http://www.cs.wisc.edu/~jyc`

THANK YOU!