Graph Homomorphisms with Complex Values: A Complete Dichotomy Theorem

Jin-Yi Cai

University of Wisconsin, Madison

Joint work with Xi Chen and Pinyan Lu.

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**).

Classification Program

Short of proving $\mathbf{P} \neq \mathbf{P}^{\#P}$, the best one can hope to show is to classify **every** problem in #P to be either #P-complete or solvable in P.

False, by **Ladner**'s theorem.

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.

Problem Statement

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

The **graph homomorphism problem** $\mathsf{EVAL}(\mathbf{A})$ 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

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

then EVAL($\mathbf{A}$) 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 EVAL($\mathbf{A}$) counts the number of THREE-COLORINGS in G.

Let

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

then $\mathsf{EVAL}(\mathbf{A})$ counts the number of k-COLORINGS in G.

Let

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

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

Dichotomy Theorems

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.

Dichotomy Theorems for Counting

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

Creignou, Khanna and Sudan:

Complexity Classifications of Boolean Constraint Satisfaction Problems.

SIAM Monographs on Discrete Math and Applications. 2001.

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

Some definitions

A graph homomorphism is a map f from $V(G)$ to $V(H)$ such that if $\{u, v\} \in E(G)$, then $\{f(u), f(v)\} \in E(H)$.

A symmetric 0-1 matrix is identified with its underlying (undirected) graph.

A general symmetric matrix gives a weighted (undirected) graph.

- Connected components.

- Bipartite graphs.

Non-negative Matrices

Theorem (Bulatov and Grohe)

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

- If $\mathbf{A}$ is bipartite, then $\mathsf{EVAL}(\mathbf{A})$ is in polynomial time if the rank of $\mathbf{A}$ is at most 2; otherwise $\mathsf{EVAL}(\mathbf{A})$ is #**P**-complete.

- If $\mathbf{A}$ is not bipartite, then $\mathsf{EVAL}(\mathbf{A})$ is in polynomial time if the rank of $\mathbf{A}$ is at most 1; otherwise $\mathsf{EVAL}(\mathbf{A})$ is #**P**-complete.

Real Matrices

Theorem (Goldberg, Jerrum, Grohe and Thurley)
There is a complexity dichotomy theorem for $\mathsf{EVAL}(\mathbf{A})$.

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 complexity dichotomy for partition functions with mixed signs

arXiv:0804.1932v2 [cs.CC]

http://arxiv.org/abs/0804.1932

A monumental achievement.

<p style="text-align:center"><strong style="color:magenta">Main Dichotomy Theorem</p>

Theorem (C, Chen and Lu)

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

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.

Reduction to Connected Components

Lemma

Let $\mathbf{A} \in \mathbb{C}^{m \times m}$ be a symmetric matrix with components $\mathbf{A}_1, \mathbf{A}_2, ..., \mathbf{A}_t$. Then

- **If $\mathsf{EVAL}(\mathbf{A}_i)$ is #P-hard for some $i \in [t]$ then $\mathsf{EVAL}(\mathbf{A})$ is #P-hard;**

- **Otherwise, $\mathsf{EVAL}(\mathbf{A})$ is polynomial-time computable.**

Three Pinning Lemmas.

Bipartite and Non-bipartite

The proof of the main Dichotomy Theorem is first reduced to Connected Components, and then further divided into the cases of Bipartite and Non-bipartite connected graphs.

Overview of Bipartite Case

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

The hardness part is further divided into three steps, in which we gradually "simplify" the problem $\mathsf{EVAL}(\mathbf{A})$ being considered.

One can view the three steps as three filters which remove hard $\mathsf{EVAL}(\mathbf{A})$ problems using different arguments.

In the tractability part, we show that all the EVAL problems that survive the three filters are indeed polynomial-time solvable.

General Structure of a Filter

In each of the three filters in the hardness proof, we consider an EVAL problem that is passed down by the previous step (Step 1 starts with EVAL($\mathbf{A}$) itself) and show that

- either the problem is #**P**-hard; or

- the matrix that defines the problem satisfies certain structural properties; or

- the problem is polynomial-time equivalent to a new EVAL problem and the matrix that defines the new problem satisfies certain structural properties.

A Purified Matrix

A is purified bipartite, if there exists an $k \times (m-k)$ matrix **B** of the form

$$
\mathbf{B} =
\begin{pmatrix}
c_1 & & & \\
& c_2 & & \\
& & \ddots & \\
& & & c_k
\end{pmatrix}
\begin{pmatrix}
\zeta_{1,1} & \zeta_{1,2} & \cdots & \zeta_{1,m-k} \\
\zeta_{2,1} & \zeta_{2,2} & \cdots & \zeta_{2,m-k} \\
\vdots & \vdots & \ddots & \vdots \\
\zeta_{k,1} & \zeta_{k,2} & \cdots & \zeta_{k,m-k}
\end{pmatrix}
\begin{pmatrix}
c_{k+1} & & & \\
& c_{k+2} & & \\
& & \ddots & \\
& & & c_m
\end{pmatrix}
$$

where every $c_i > 0$, every $\zeta_{i,j}$ is a root of unity, and **A** is the bipartisation of **B**:

$$
\mathbf{A} =
\begin{pmatrix}
\mathbf{0} & \mathbf{B} \\
\mathbf{B}^{\mathrm{T}} & \mathbf{0}
\end{pmatrix}.
$$

Step 1: Purification of Matrix A

Start with problem $\mathsf{EVAL}(\mathbf{A})$ in which $\mathbf{A} \in \mathbb{C}^{m \times m}$ is a symmetric, connected and bipartite matrix.

Theorem

Let $\mathbf{A} \in \mathbb{C}^{m \times m}$ be a symmetric, connected, and bipartite matrix. Then either $\mathsf{EVAL}(\mathbf{A})$ is #**P**-hard or there exists an $m \times m$ purified bipartite matrix $\mathbf{A}'$ such that $\mathsf{EVAL}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{A}')$.

Step 2: Reduction to Discrete Unitary Matrix

Now let $\mathbf{A} \in \mathbb{C}^{m \times m}$ denote a purified bipartite matrix.

To study EVAL($\mathbf{A}$), we define a new and larger class of EVAL problems.

These EVAL problems have edge weights as well as vertex weights. Moreover the vertex weights are partitioned into modular classes according to the $\deg(v)$.

Definition

Let $\mathbf{C} \in \mathbb{C}^{m \times m}$ be a symmetric matrix, and

$$\mathfrak{D} = \{\mathbf{D}^{[0]}, \mathbf{D}^{[1]}, ..., \mathbf{D}^{[N-1]}\}$$

be a sequence of diagonal matrices in $\mathbb{C}^{m \times m}$ for some $N \geq 1$ (we use $D_i^{[t]}$ to denote the $(i, i)^{th}$ entry of $\mathbf{D}^{[t]}$). We define the following problem $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$: Given an undirected graph $G = (V, E)$, compute $Z_{\mathbf{C}, \mathfrak{D}}(G)$

$$\sum_{\xi : V \to [m]} \left(\prod_{(u,v) \in E} A_{\xi(u), \xi(v)} \right) \left(\prod_{i=0}^{N-1} \left(\prod_{v \in V, \ \deg(v) \equiv i \bmod N} D_{\xi(v)}^{[i]} \right) \right)$$

Define the inner product of u and v $\in \mathbb{C}^m$ to be

$$\langle \mathbf{u}, \mathbf{v} \rangle = \sum_{k=1}^{m} \mathbf{u}_k \overline{\mathbf{v}_k}.$$

Definition

Let $\mathbf{F} \in \mathbb{C}^{m \times m}$ be a (not necessarily symmetric) matrix with entries $(F_{i,j})$. We say $\mathbf{F}$ is an M-discrete unitary matrix, for some positive integer M, if it satisfies the following conditions:

1. **Every entry $F_{i,j}$ is a power of $\omega_M = e^{2\pi\sqrt{-1}/M}$ (the Mth root of unity);**

2. **$M = $ lcm of the orders of $F_{i,j}$;**

3. **$F_{1,i} = F_{i,1} = 1$ for all $i \in [m]$;**

4. **For all $i \neq j \in [m]$, $\langle \mathbf{F}_{i,*}, \mathbf{F}_{j,*} \rangle = 0$ and $\langle \mathbf{F}_{*,i}, \mathbf{F}_{*,j} \rangle = 0$.**

Some Simple Examples of Discrete Unitary Matrices

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

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

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

Discrete Unitary Matrix

We prove that $\mathsf{EVAL}(\mathbf{A})$ is either #**P**-hard or polynomial-time equivalent to $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ in which $\mathbf{C}$ is the bipartisation of a discrete unitary matrix $\mathbf{F}$:

$$\mathbf{C} = \begin{pmatrix} \mathbf{0} & \mathbf{F} \\ \mathbf{F}^{\mathrm{T}} & \mathbf{0} \end{pmatrix}.$$

Theorem

Let $\mathbf{A} \in \mathbb{C}^{m \times m}$ be a purified bipartite matrix, then either problem $\mathsf{EVAL}(\mathbf{A})$ is #**P**-hard or there exists a triple $((M, N), \mathbf{C}, \mathfrak{D})$ such that $\mathsf{EVAL}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ and $((M, N), \mathbf{C}, \mathfrak{D})$ satisfies the following condition $(\mathcal{U})$:

$(\mathcal{U}_1)$ M and N are positive integers that satisfy $M \,|\, N$. $\mathbf{C}$ is a $2n \times 2n$ complex matrix for some $n \geq 1$ and $\mathfrak{D} = \{\mathbf{D}^{[0]}, \mathbf{D}^{[1]}, ..., \mathbf{D}^{[N-1]}\}$ is a sequence of N $2n \times 2n$ diagonal matrices;

$(\mathcal{U}_2)$ $\mathbf{C}$ is the bipartisation of an M-**discrete unitary matrix** $\mathbf{F} \in \mathbb{C}^{n \times n}$;

$(\mathcal{U}_3)$ For all $i \in [2n]$, $D_i^{[0]} = 1$, and for all r and $i \in [2n]$, $D_i^{[r]}$ is either zero or a power of ω_N.

Step 3: Canonical Form of C, F and D

After the first two steps, the original problem $\mathsf{EVAL}(\mathbf{A})$ is either shown to be **#P-hard** or reduced to a new problem $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$. We also know there exist positive integers M, N such that $((M, N), \mathbf{C}, \mathfrak{D})$ satisfies condition $(\mathcal{U})$.

Now we number rows and columns from $\{0, 1, \ldots, m - 1\}$.

We also denote the upper-right $m \times m$ block of $\mathbf{C}$ by $\mathbf{F}$.

If $M = 1$, then since $\mathbf{F}$ is M-discrete unitary, m has to be 1. In this case, it is easy to check that problem $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is tractable.

Now assume $M > 1$.

First, we show that either $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is hard or we can permute the rows and columns of $\mathbf{F}$ so that the new $\mathbf{F}$ is the tensor product of a collection of ***Fourier matrices***.

Definition

Let $q > 1$ be a prime power. We call the following $q \times q$ matrix $\mathcal{F}_q$ a q-**Fourier matrix** : The $(x, y)^{th}$ entry, where $x, y \in [0 : q - 1]$, is

$$\omega_q^{xy} = e^{2\pi i\left(xy/q\right)}.$$

Theorem

Suppose $((M, N), \mathbf{C}, \mathfrak{D})$ satisfies condition $(\mathcal{U})$ and $M > 1$. Then either $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is #**P**-hard or there exist

1. two permutations Σ and Π from $[0 : m - 1]$ to $[0 : m - 1]$; and

2. a sequence $q_1, q_2, ..., q_k$ of k prime powers, for some $k \geq 1$,

such that
$$\mathbf{F}_{\Sigma, \Pi} = \bigotimes_{i \in [k]} \boldsymbol{\mathcal{F}}_{q_i}. \tag{1}$$

Suppose there do exist Σ, Π, q_i such that **F** satisfies (1), then we let $\mathbf{C}_{\Sigma,\Pi}$ denote the bipartisation of $\mathbf{F}_{\Sigma,\Pi}$, and $\mathfrak{D}_{\Sigma,\Pi}$ denote a sequence of N $2m \times 2m$ diagonal matrices in which the rth matrix is

$$
\begin{pmatrix}
D^{[r]}_{\Sigma(0)} & & & & & \\
& \ddots & & & & \\
& & D^{[r]}_{\Sigma(m-1)} & & & \\
& & & D^{[r]}_{\Pi(0)+m} & & \\
& & & & \ddots & \\
& & & & & D^{[r]}_{\Pi(m-1)+m}
\end{pmatrix}.
$$

The tensor product decomposition

$$\mathbf{F} = \bigotimes_{i \in [k]} \mathcal{F}_{q_i}.$$

gives $\mathbf{p}, \mathbf{t}, \mathbf{q}$ such that $((M, N), \mathbf{C}, \mathfrak{D}, (\mathbf{p}, \mathbf{t}, \mathbf{q}))$ satisfies the following condition $(\mathcal{R})$:

$(\mathcal{R}_1)$ $\mathbf{p} = (p_1, ..., p_s)$ **is a sequence of primes such that** $p_1 < p_2 < ... < p_s$; $\mathbf{t} = (t_1, ..., t_s)$ **is a sequence of positive integers;** $\mathfrak{q} = (\mathbf{q}_i, i \in [s])$ **is a collection of** s **sequences in which every** $\mathbf{q}_i$ **is a sequence** $(q_{i,1}, ..., q_{i,t_i})$ **of powers of** p_i **such that** $q_{i,1} \geq ... \geq q_{i,t_i}$;

$(\mathcal{R}_2)$ $\mathbf{C} \in \mathbb{C}^{2m \times 2m}$ **is the bipartisation of** $\mathbf{F}$, $m = \prod_{i \in [s], j \in [t_i]} q_{i,j}$, **and** $((M, N), \mathbf{C}, \mathfrak{D})$ **satisfies** $(\mathcal{U})$;

$(\mathcal{R}_3)$ **There is a one-to-one correspondence** ρ **from** $[0 : m - 1]$ **to** $\mathbb{Z}_{\mathfrak{q}}$ **such that**

$$F_{a,b} = \prod_{i \in [s], j \in [t_i]} \omega_{q_{i,j}}^{x_{i,j}\, y_{i,j}}, \quad \text{for all } a, b \in [0 : m - 1];$$

where

$$\rho(a) = (x_{i,j}, i \in [s], j \in [t_i]), \qquad \rho(b) = (y_{i,j}, i \in [s], j \in [t_i]),$$

$$\mathbb{Z}_{\mathsf{q}} \equiv \prod_{i \in [s], j \in [t_i]} \mathbb{Z}_{q_{i,j}} \quad \equiv \quad \mathbb{Z}_{q_{1,1}} \times \cdots \times \mathbb{Z}_{q_{1,t_1}} \times$$

$$\vdots$$

$$\mathbb{Z}_{q_{s,1}} \times \cdots \times \mathbb{Z}_{q_{s,t_s}}$$

Step 3.2

Now we have a 4-tuple that satisfies condition $(\mathcal{R})$. In this step, we show for every $r \in [N-1]$ (recall that $\mathbf{D}^{[0]}$ is already known to be the identity matrix), the nonzero entries of the rth matrix $\mathbf{D}^{[r]}$ in $\mathfrak{D}$ must have a very nice "*group*" structure, otherwise $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is #P-hard.

For every $r \in [N-1]$, we define Λ_r and $\Gamma_r \subset \mathbb{Z}_{\mathfrak{q}}$ as

$$\Lambda_r = \left\{ \mathbf{x} \in \mathbb{Z}_{\mathfrak{q}}, D^{[r]}_{(0,\mathbf{x})} \neq 0 \right\} \qquad \Gamma_r = \left\{ \mathbf{x} \in \mathbb{Z}_{\mathfrak{q}}, D^{[r]}_{(1,\mathbf{x})} \neq 0 \right\}.$$

Theorem

Let $((M,N), \mathbf{C}, \mathfrak{D}, (\mathbf{p}, \mathbf{t}, \mathfrak{q}))$ be a 4-tuple that satisfies $(\mathcal{R})$. Then either $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is #P-hard or sets $\Lambda_r \subset \mathbb{Z}_{\mathfrak{q}}$ and $\Gamma_r \subset \mathbb{Z}_{\mathfrak{q}}$ satisfy the following condition $(\mathcal{L})$:

$(\mathcal{L}_1)$ For every $r \in \mathcal{S}$, $\Lambda_r = \prod_{i=1}^{s} \Lambda_{r,i}$, where for every $i \in [s]$, $\Lambda_{r,i}$ is a coset in $\mathbb{Z}_{\mathbf{q}_i}$; and

$(\mathcal{L}_2)$ For every $r \in \mathcal{T}$, $\Gamma_r = \prod_{i=1}^{s} \Gamma_{r,i}$, where for every $i \in [s]$, $\Gamma_{r,i}$ is a coset in $\mathbb{Z}_{\mathbf{q}_i}$.

Step 3.3

In the final step, we show that, for every $r \in [N-1]$, the nonzero entries of $\mathbf{D}^{[r]}$ must have a **quadratic structure**, called Condition $(\mathcal{D})$, otherwise $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is **#P-hard**.

This is the most difficult part of the proof for the bipartite case.

<div align="center">**Tractability**</div>

Theorem

Let $((M, N), \mathbf{C}, \mathfrak{D}, (\mathbf{p}, \mathbf{t}, \mathfrak{q}))$ be a 4-tuple that satisfies all the three conditions $(\mathcal{R}), (\mathcal{L})$ and $(\mathcal{D})$, then problem $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ can be solved in polynomial time.

Quadratic Polynomial

Let $q = p^k$ be a prime power for some prime p and positive integer k. 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 $a_{i,j} \in \mathbb{Z}_q$ for all i, j; and the output is

$$Z_q(f) = \sum_{x_1, \ldots, x_n \in \mathbb{Z}_q} \omega_q^{f(x_1, \ldots, x_n)}.$$

Theorem

This problem can be solved in polynomial time.

... 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 ...").

—(Name that person)

Gauss Sums

For a prime p, the Gauss quadratic sum is

$$\sum_{x \in \mathbb{Z}_p} \omega_p^{cx^2} = \begin{cases} p, & \text{if } c = 0 \bmod p \\ \left(\frac{c}{p} \right) \cdot G, & \text{if } c \neq 0 \bmod p \end{cases}$$

where

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

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

G has the closed form

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

"Elegant Theorem" of the Sign

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

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

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

Back to 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. $M = \mathbf{lcm}$ 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 $\langle \mathbf{A}_{i,*}, \mathbf{A}_{j,*} \rangle = \sum_{k=1}^{m} \mathbf{A}_{i,k} \overline{\mathbf{A}_{j,k}}$.

A Group Condition

Theorem

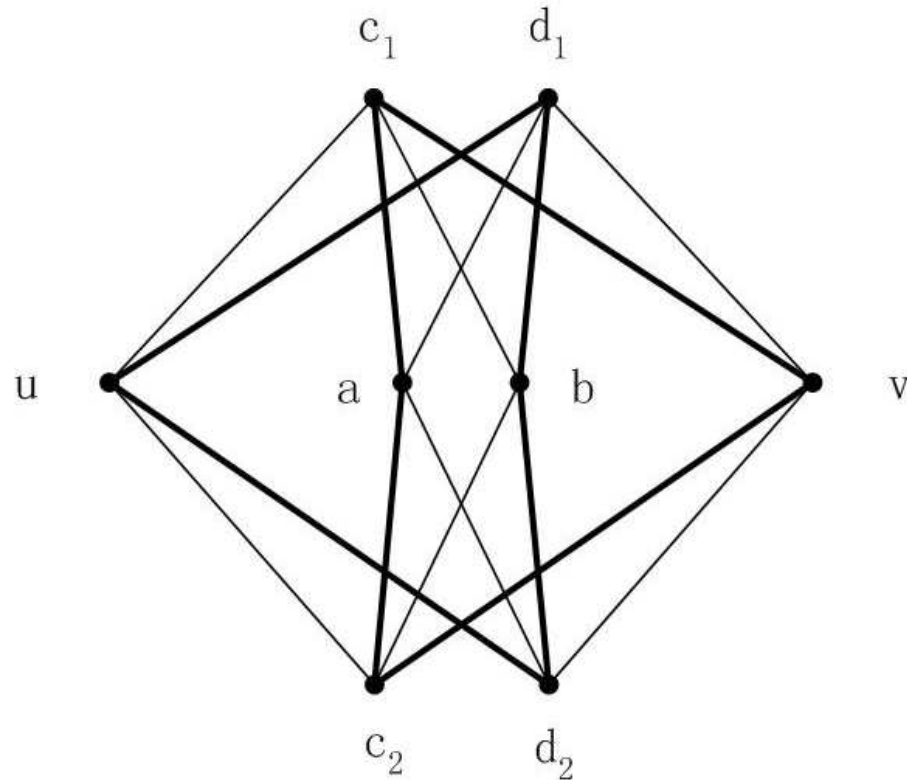Let $\mathbf{A}$ be a symmetric M-discrete unitary matrix. Then

- **either** $Z_{\mathbf{A}}(\cdot)$ is #P-hard,

- **or** $\mathbf{A}$ 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 ...

$$G \implies G^{[p]}.$$

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

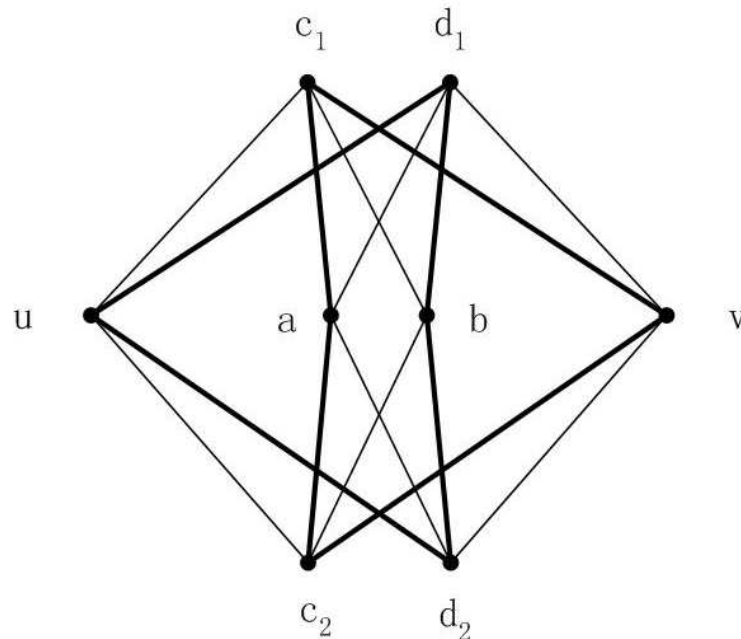$$Z_{\mathbf{A}^{[p]}}(G) = Z_{\mathbf{A}}(G^{[p]}), \quad \text{for all } G.$$

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

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

$$\Longrightarrow$$

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

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

(Imagine $u \to i$ and $v \to j$, where $i, j \in [0 : m-1]$.)

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

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

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

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

$\mathbf{A}^{[p]}$ is symmetric and non-negative.

In fact $A_{i,j}^{[p]} > 0$. (By taking $a = i$ and $b = j$).

Diagonal and Off-Diagonal

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

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

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

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

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

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

49

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

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

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

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 $X_{i,j} = \{0, m\}$,

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

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

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

Toward GC

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.

Note that 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

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

When A is not Bipartite . . .

. . . more proofs . . .

Some References

Some papers can be found on my web site

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

THANK YOU!