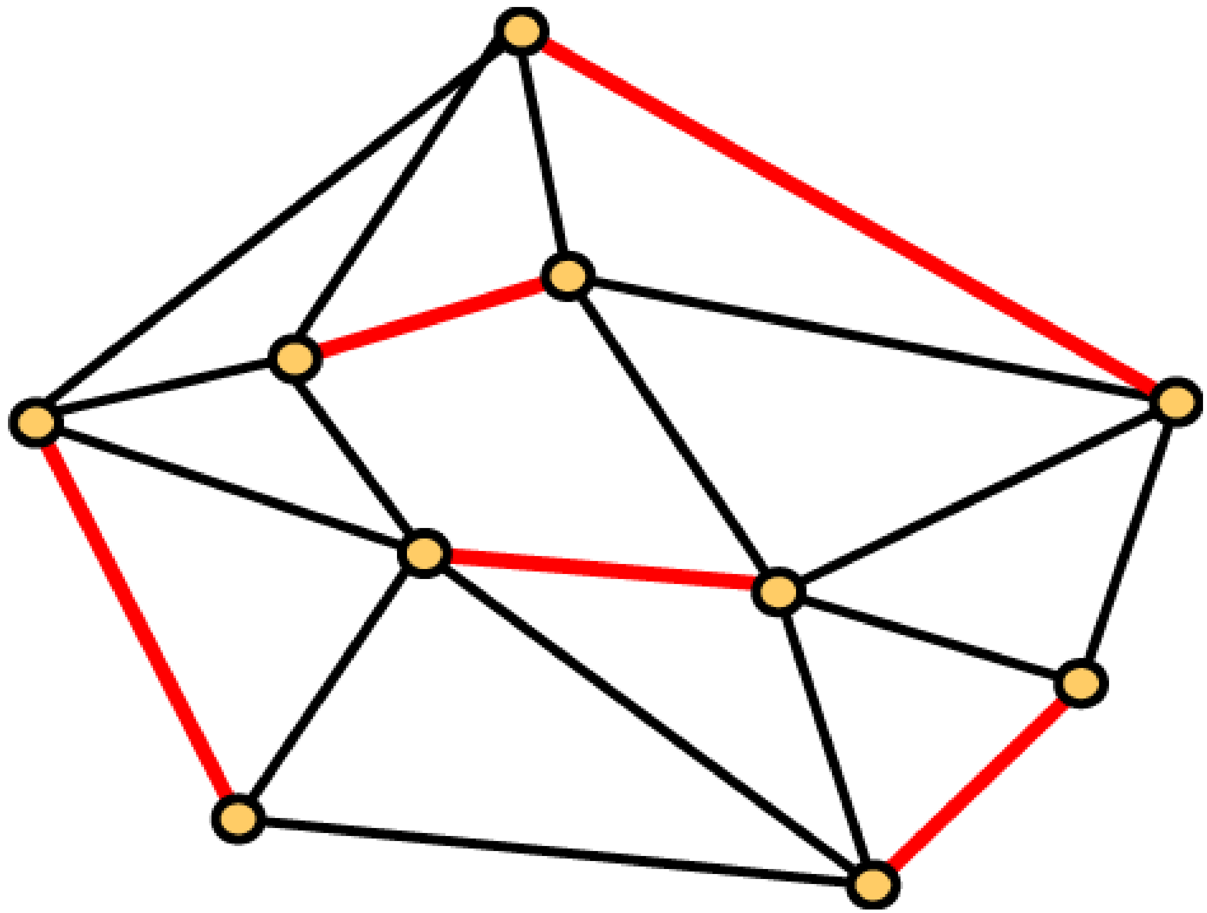
# Complexity Dichotomy Theorems for Counting Problems

**Jin-Yi Cai**
**University of Wisconsin, Madison**

**Joint work with Xi Chen, Pinyan Lu and Mingji Xia.**

## Perfect Matching



## Perfect Matching as a Holant Problem

**Let** $G = (V, E)$ **be a graph. At each** $v \in V$ **assign the function** $f_v = $EXACT-ONE**. Consider each edge** $e \in E$ **as a Boolean variable.**

$$\mathrm{Holant}(G) = \sum_{\sigma : E \to \{0,1\}} \prod_{v \in V} f_v(\sigma \mid_{E(v)}).$$

**Clearly** $\mathrm{Holant}(G)$ **counts the number of perfect matchings.**

**If we assign the function** $f_v = $AT-MOST-ONE**, then** $\mathrm{Holant}(G)$ **counts the number of all matchings.**

## FKT

**Count the number of perfect matchings in a planar graph [Fisher, Kasteleyn, Temperley] is computable in P.**

**It is #P-hard on general or bipartite graphs [Valiant].**

**Count the number of all (not necessarily perfect) matchings in a planar graph is still #P-complete [Jerrum].**

## Holographic Algorithms with Matchgates

**Valiant's holographic algorithm with matchgates can be understood as follows:**

**For a desired computation expressed as** $\text{Holant}(G)$**, find a suitable holographic transformation so that**

$$\text{Holant}(G) = \text{Holant}(G')$$

**where** $G'$ **is planar and uses** Exact-One**.**

**Another family of Holographic Algorithms based on Fibonacci Gates** [**C., Lu, Xia**]

## Reductions

**So Holographic Algorithms are reductions from an (unsolved) problem $X$ to a solved problem: Either planar Perfect Matching, and then apply FKT; Or Fibonacci Gates.**

**But a reduction method can be used in the opposite direction—to prove hardness:**

**We start with a problem $Y$ already known to be #P-hard, and then use a suitable holographic transformation to reduce $Y$ to $X$, thereby proving that $X$ is also #P-hard.**

## Classification Program for Counting Problems

**To classify every problem in a broad class of counting problems, to be either solvable in P or #P-hard.**

**Such theorems are called dichotomy theorems.**

## Three Frameworks for Counting Problems

1. **Holant Problems**
2. **Graph Homomorphisms**
3. **Constraint Satisfaction Problems (CSP)**
   **(Bulatov, Dyer-Richerby, C.-Chen)**

**In each framework, there has been remarkable progress in the classification program.**

## Some Tractable Function Families

**We discovered that the following three families of functions**

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

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

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

**give rise to tractable problems.**

**Theorem [C., Lu, Xia]**
**For every $G$ where $V(G)$ is labeled by $\mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3$,** $\mathrm{Holant}(G)$ **is computable in P.**

## A Particular Case of Graph Homomorphism

**Let**

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

**Consider the Spin System** $G = (V, E)$ **where each** $v \in V$ **can take values in** $\{0, 1\}$**, and each** $e \in E$ **is assigned the binary function** $H$**.**

**Then the partition function is**

$$Z_{\mathbf{H}}(G) = \sum_{\xi : V \to \{0,1\}} \prod_{(u,v) \in E} H_{\xi(u),\xi(v)}.$$

## A Particular Case of Graph Homomorphism

$\prod_{(u,v)\in E} H_{\xi(u),\xi(v)} \in \{1, -1\}$, **and is** $-1$ **precisely when the induced subgraph of** $G$ **on** $\xi^{-1}(1)$ **has an odd number of edges. Therefore,**

$$\left(2^n - Z_{\mathbf{H}}(G)\right)\Big/2$$

**is the number of induced subgraphs of** $G$ **with an odd number of edges.**

## Notation

**Suppose $f$ is a symmetric function on Boolean variables $x_1, x_2, \ldots, x_n$.**

**We denote it as**

$$[f_0, f_1, \ldots, f_n]$$

**where $f_i$ is the value of $f$ on inputs of Hamming weight $i$.**

**For example, The** Exact-One **function is**

$$[0, 1, 0, \ldots, 0].$$

$$\mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3$$

**1.** $[1, 0, 0, \ldots, 0, \pm 1]$; $\quad (\mathcal{F}_1, r = 0, 2)$

**2.** $[1, 0, 0, \ldots, 0, \pm i]$; $\quad (\mathcal{F}_1, r = 1, 3)$

**3.** $[1, 0, 1, 0, \ldots, 0$ **or** $1]$; $\quad (\mathcal{F}_2, r = 0)$

**4.** $[0, 1, 0, 1, \ldots, 0$ **or** $1]$; $\quad (\mathcal{F}_2, r = 2)$

**5.** $[1, i, 1, i, \ldots, i$ **or** $1]$; $\quad (\mathcal{F}_2, r = 3)$

**6.** $[1, -i, 1, -i, \ldots, (-i)$ **or** $1]$; $\quad (\mathcal{F}_2, r = 1)$

**7.** $[1, 0, -1, 0, 1, 0, -1, 0, \ldots, 0$ **or** $1$ **or** $(-1)]$; $\quad (\mathcal{F}_3, r = 0)$

**8.** $[1, 1, -1, -1, 1, 1, -1, -1, \ldots, 1$ **or** $(-1)]$; $\quad (\mathcal{F}_3, r = 1)$

**9.** $[0, 1, 0, -1, 0, 1, 0, -1, \ldots, 0$ **or** $1$ **or** $(-1)]$; $\quad (\mathcal{F}_3, r = 2)$

**10.** $[1, -1, -1, 1, 1, -1, -1, 1, \ldots, 1$ **or** $(-1)]$. $\quad (\mathcal{F}_3, r = 3)$

$\mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3$

**1.** $[1, 0, 0, \ldots, 0, \pm 1]$; $(\mathcal{F}_1, r = 0, 2)$

**2.** $[1, 0, 0, \ldots, 0, \pm i]$; $(\mathcal{F}_1, r = 1, 3)$

**3.** $[1, 0, 1, 0, \ldots, 0$ **or** $1]$; $(\mathcal{F}_2, r = 0)$

**4.** $[0, 1, 0, 1, \ldots, 0$ **or** $1]$; $(\mathcal{F}_2, r = 2)$

**5.** $[1, i, 1, i, \ldots, i$ **or** $1]$; $(\mathcal{F}_2, r = 3)$

**6.** $[1, -i, 1, -i, \ldots, (-i)$ **or** $1]$; $(\mathcal{F}_2, r = 1)$

**7.** $[1, 0, -1, 0, 1, 0, -1, 0, \ldots, 0$ **or** $1$ **or** $(-1)]$; $(\mathcal{F}_3, r = 0)$

**8.** $[1, 1, -1, -1, 1, 1, -1, -1, \ldots, 1$ **or** $(-1)]$; $(\mathcal{F}_3, r = 1)$

**9.** $[0, 1, 0, -1, 0, 1, 0, -1, \ldots, 0$ **or** $1$ **or** $(-1)]$; $(\mathcal{F}_3, r = 2)$

**10.** $[1, -1, -1, 1, 1, -1, -1, 1, \ldots, 1$ **or** $(-1)]$. $(\mathcal{F}_3, r = 3)$

## $Z_{\mathbf{H}}(G)$ and $\text{Holant}$ with $\mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3$

**$Z_{\mathbf{H}}(G)$ is a special case of $\text{Holant}$ with $\mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3$:**

**$\mathbf{H}$ is included in $\mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3$.**

**Take the Incidence Graph $I(G)$ of $G$.**

**$\mathbf{H} = [1, 1, -1]$.**

**We can take $r = 1$, $k = 2$ and $\lambda = (1 + i)^{-1}$ in $\mathcal{F}_3$, to get the binary function $[1, 1, -1]$.**

**If we take $r = 0$, $\lambda = 1$ in $\mathcal{F}_1$, we get the** EQUALITY **function $[1, 0, \ldots, 0, 1]$ on $k$ bits.**

**So $Z_{\mathbf{H}}(\cdot)$ is computable in P.**

## Planar CSP Dichotomy Theorem

**Theorem (C., Lu, Xia)**
**Let $\mathscr{F}$ be any set of real symmetric functions over Boolean variables.** $\#\text{Pl-CSP}(\mathscr{F})$ **is #P-hard unless $\mathscr{F}$ satisfies one of the following conditions, in which case it is in P:**

1. $\#\text{CSP}(\mathscr{F})$ **is tractable (for which we have an effective dichotomy (C.-Lu-Xia, STOC 2009)); or**

2. **Every function in $\mathscr{F}$ is realizable by some matchgate under a holographic transformation (for which we have an effective dichotomy (C.-Choudhary-Lu, Complexity 2007, C.-Lu, STOC 2007)).**

## Planar CSP Dichotomy Theorem

**Theorem (C., Lu, Xia)**

**Let $\mathscr{F}$ be any set of real symmetric functions over Boolean variables. We can effectively classify all Constraint Satisfaction Problems with local constraints from $\mathscr{F}$ into three categories:**

1. $\#\mathrm{CSP}(\mathscr{F})$ **is tractable; or**
2. $\#\mathrm{CSP}(\mathscr{F})$ **is #P-hard in general, but** $\#\mathrm{Pl\text{-}CSP}(\mathscr{F})$ **is tractable; or**
3. $\#\mathrm{Pl\text{-}CSP}(\mathscr{F})$ **remains #P-hard.**

**Case 2. is precisely when every $f \in \mathscr{F}$ is realizable by some matchgate under a holographic transformation, and** $\mathrm{Pl\text{-}\#CSP}(\mathscr{F})$ **is solvable by Valiant's holographic algorithm.**

## Graph Homomorphism: Problem Statement

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

**The graph homomorphism problem is to compute the partition function:**

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

OUTPUT:

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

**$\xi$ 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 $\xi$.**

## Some Examples

**Let**

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

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

**Let**

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

**then** $Z_{\mathbf{A}}$ **counts the number of** Vertex Covers **in** $G$**.**

**Also** Independent Sets**.**

## Some More Examples

**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

**If $\mathbf{A}$ is $k$ by $k$,**

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

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

## 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`

## A combinatorial view of GH

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

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

**Then**

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

**counts the number of graph homomorphisms.**

## Non-negative Matrices

**Theorem (Dyer and Greenhill)**
**For any symmetric 0-1 matrix $\mathbf{A}$, $Z_{\mathbf{A}}$ is either computable in polynomial time or #P-hard.**

**Theorem (Bulatov and Grohe)**
**For any non-negative symmetric matrix $\mathbf{A}$, $Z_{\mathbf{A}}$ is either computable in polynomial time or #P-hard.**

**Bulatov-Grohe Criterion:** **If there exist $i < j$ such that at least three entries among $\begin{pmatrix} A_{i,i} & A_{i,j} \\ A_{j,i} & A_{j,j} \end{pmatrix}$ are non-zero, then**

$$\det \begin{pmatrix} A_{i,i} & A_{i,j} \\ A_{j,i} & A_{j,j} \end{pmatrix} \neq 0 \quad \Longrightarrow \quad Z_{\mathbf{A}} \text{ is \#P-hard.}$$

## Positive and Negative Real Matrices

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

**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*

`http://arxiv.org/abs/0804.1932`

**A monumental achievement.**

## Dichotomy Theorem for complex A

**Theorem (C., Chen and Lu)**
**There is a complexity dichotomy theorem for $Z_{\mathbf{A}}$.**

**For any symmetric complex valued 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.**

**Given A, the problem of deciding which case $Z_{\mathbf{A}}(\cdot)$ belongs to is decidable in P.**

`http://arxiv.org/abs/0903.4728`

## 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.**

## 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 ...).**

## Fourier Matrices

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

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

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

## 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**

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

## “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.)**

# Discrete Unitary Matrix

## 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 $A_{i,j}$;**
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 of Discrete Unitary Matrices

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

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

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

## It Must Be A Group!

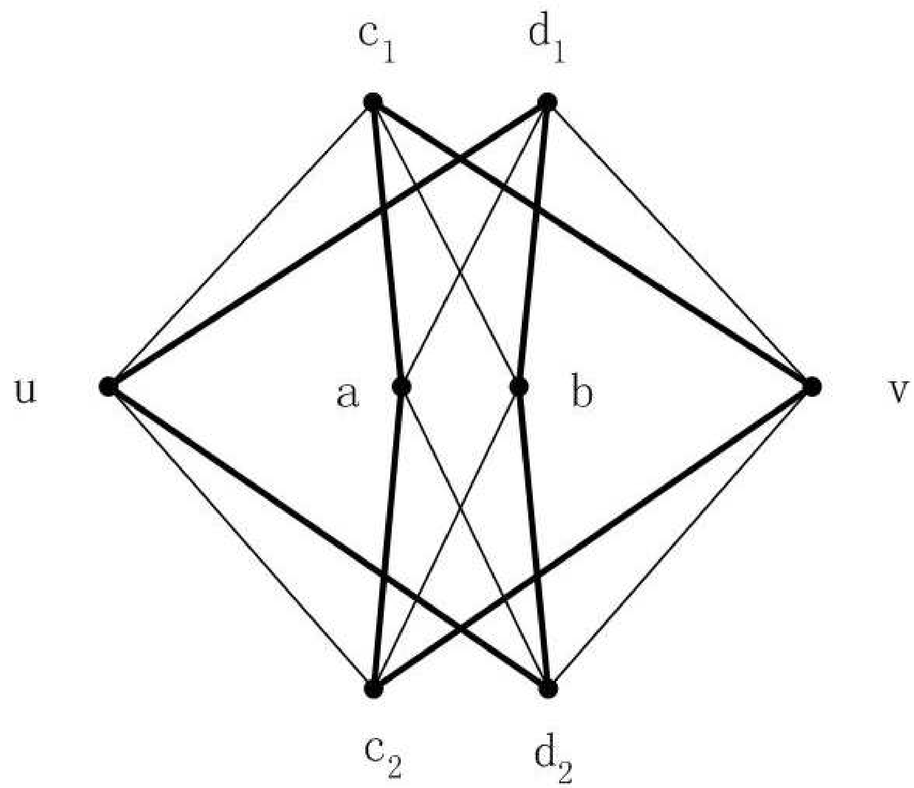
**Theorem**

**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:** $\forall\ i, j \in [0 : m-1]$**,** $\exists\ k \in [0 : m-1]$ **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 ...**

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

## 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**

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

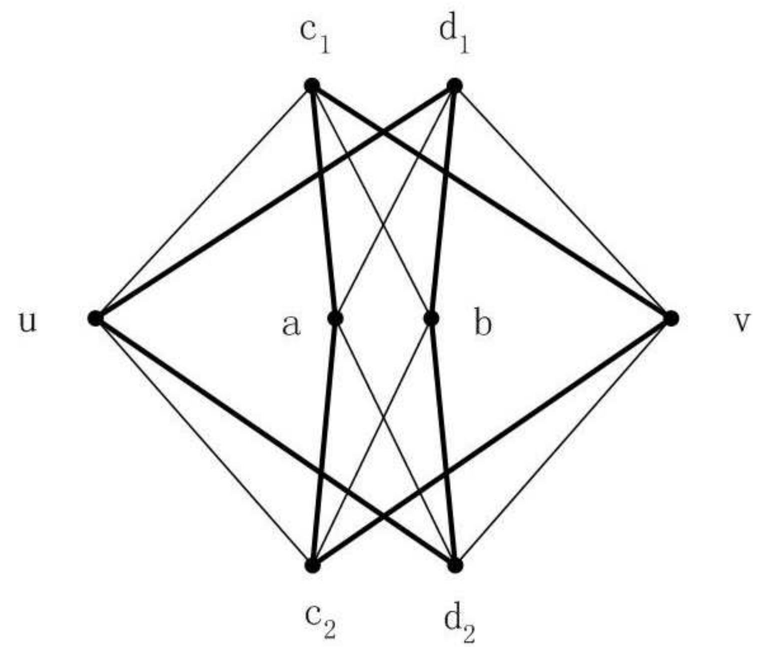
**Thus $Z_{\mathbf{A}^{[p]}}(\cdot)$ is reducible to $Z_{\mathbf{A}}(\cdot)$, and therefore**

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

$$\Longrightarrow$$

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

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




(*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 $\mathbf{A}^{[p]}$

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

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

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

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

## Diagonal and Off-Diagonal

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

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

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

$\Longrightarrow$ **(by the Bulatov-Grohe Criterion)**

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

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

## 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**

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

**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.**

**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 complex 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**

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

## Some References

**Some papers can be found on my web site**

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

**THANK YOU!**