arXiv:0903.4728v1 [cs.CC] 27 Mar 2009

Graph Homomorphisms with Complex Values: A Dichotomy Theorem

Jin-Yi Cai* Xi Chen† Pinyan Lu‡

Abstract

Graph homomorphism problem has been studied intensively. Given an $m \times m$ symmetric matrix $\mathbf{A}$, the graph homomorphism function is defined as

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

where $G = (V, E)$ is any undirected graph. The function $Z_{\mathbf{A}}(G)$ can encode many interesting graph properties, including counting vertex covers and k-colorings. We study the computational complexity of $Z_{\mathbf{A}}(G)$ for arbitrary complex valued symmetric matrices $\mathbf{A}$. Building on work by Dyer and Greenhill [6], Bulatov and Grohe [2], and especially the recent beautiful work by Goldberg, Grohe, Jerrum and Thurley [10], we prove a complete dichotomy theorem for this problem.

*University of Wisconsin-Madison: jyc@cs.wisc.edu
†Princeton University: csxichen@gmail.com
‡Microsoft Research Asia: pinyanl@microsoft.com

Contents

1 Introduction

Graph homomorphism has been studied intensively over the years [16, 12, 6, 9, 2, 5]. Given two graphs G and H, a graph homomorphism from G to H is a map f from $V(G)$ to $V(H)$ such that whenever (u,v) is an edge in G, $(f(u),f(v))$ is an edge in H. The counting problem for graph homomorphism is to compute the number of homomorphisms from G to H. For a fixed graph H, this problem is also known as the $\#H$-coloring problem. In 1967, Lovász [16] proved that H and H' are isomorphic iff for all G, the number of homomorphisms from G to H and from G to H' are the same.

In this paper all graphs considered are undirected. We follow standard definitions: G is allowed to have multiple edges but no loops; H can have loops, multiple edges, and more generally, edge weights. Formally, let $\mathbf{A}$ be an $m \times m$ symmetric matrix with entries $(A_{i,j})$, $i,j \in [m] = \{1,2,\ldots,m\}$. For any undirected graph $G=(V,E)$, we define

$$Z_{\mathbf{A}}(G) = \sum_{\xi:V\to[m]} \prod_{(u,v)\in E} A_{\xi(u),\xi(v)}. \tag{1}$$

This is also called the *partition function* from statistical physics.

Graph homomorphisms can express many natural graph properties. For example, if we take H to be a graph on two vertices $\{0,1\}$ with an edge $(0,1)$ and a loop at 1, then a graph homomorphism from G to H corresponds to a Vertex Cover of G, and the counting problem simply counts the number of vertex covers. As another example, if H is the complete graph on k vertices (without self loops), then the problem is exactly the k-Coloring problem for G. Many additional graph invariants can be expressed as $Z_{\mathbf{A}}(G)$ for appropriate $\mathbf{A}$. Consider the Hadamard matrix

$$\mathbf{H} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{2}$$

where we index the rows and columns by $0,1$. In $Z_{\mathbf{H}}(G)$, every product

$$\prod_{(u,v)\in E} H_{\xi(u),\xi(v)} = \pm 1,$$

and is -1 precisely when the induced subgraph of G on $\xi^{-1}(1)$ has an odd number of edges. Therefore $(2^n - Z_{\mathbf{H}}(G))/2$ is the number of induced subgraphs with an odd number of edges. Also expressible as $Z_{\mathbf{A}}(G)$ are S-flows where S is a subset of a finite Abelian group closed under inversion [9]. If we take

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

then $Z_{\mathbf{A}}(G) = 2^n$ if G is Eulerian and 0 otherwise. Further examples include (a scaled version of) the Tutte polynomial $\hat{T}(x,y)$ when $(x-1)(y-1)$ is a positive integer. In [9], Freedman et. al. characterized what graph functions can be expressed as $Z_{\mathbf{A}}(G)$.

In this paper, we study the computational complexity of $Z_{\mathbf{A}}(G)$, where $\mathbf{A} \in \mathbb{C}^{m\times m}$ is an arbitrary fixed symmetric matrix over the *complex numbers* and G is an input graph. The complexity question of $Z_{\mathbf{A}}(G)$ has also been intensively studied. Hell and Nešetřil [11, 12] first studied the computational complexity of the H-coloring problem (that is, given an undirected graph G, decide whether there exists a graph homomorphism from G to H) and proved that for any undirected graph H, H-coloring is either in P or NP-complete. Results of this type are called complexity *dichotomy* theorems. This includes the well-known Schaefer's theorem [18] and more generally the study on constraint satisfaction problems (CSP in short) [4]. In particular, the famous dichotomy conjecture by Vardi and Feder [7] on Decision

CSP motivated much of subsequent work. In [6] Dyer and Greenhill studied the counting version of the H-coloring problem and proved that for any 0-1 symmetric matrix $\mathbf{A}$, computing $Z_{\mathbf{A}}(G)$ is either in P or #P-hard. Bulatov and Grohe [2] generalized this result to all nonnegative symmetric matrices $\mathbf{A}$. They obtained an elegant dichotomy theorem, which basically says that $Z_{\mathbf{A}}(G)$ is computable in P iff each *block* of $\mathbf{A}$ has rank at most one, and it is #P-hard otherwise. More precisely, decompose $\mathbf{A}$ as a direct sum of $\mathbf{A}_i$ which correspond to the connected components H_i of the undirected graph H defined by the nonzero entries of $\mathbf{A}$. Then, $Z_{\mathbf{A}}(G)$ is computable in P if every $Z_{\mathbf{A}_i}(G)$ is, and #P-hard otherwise. For each non-bipartite H_i, the corresponding $Z_{\mathbf{A}_i}(G)$ is computable in P if $\mathbf{A}_i$ has rank at most one, and #P-hard otherwise. For each bipartite H_i, the corresponding $Z_{\mathbf{A}_i}(G)$ is computable in P if

$$\mathbf{A}_i = \begin{pmatrix} \mathbf{0} & \mathbf{B}_i \\ \mathbf{B}_i^T & 0 \end{pmatrix},$$

where $\mathbf{B}_i$ has rank one, and #P-hard otherwise.

The result of Bulatov and Grohe is both sweeping and enormously applicable. It completely solves the problem for non-negative symmetric matrices. However, the Hadamard matrix $\mathbf{H}$ in (2) presents an obstacle. In general, unlike non-negative $\mathbf{A}$, when there are both positive and negative entries in $\mathbf{A}$, there can be substantial cancelations in the exponential sum $Z_{\mathbf{A}}(G)$, which may yield surprisingly efficient computations. This is not dissimilar to monotone versus non-monotone complexity. Indeed the Hadamard matrix $\mathbf{H}$ turns out to be one such case. This is the starting point of the next great chapter on the complexity of $Z_{\mathbf{A}}(G)$ by Goldberg et. al.

In a paper [10] comprising 73 pages of beautiful proofs of both exceptional depth and conceptual vision, Goldberg, Jerrum, Grohe, and Thurley proved a complexity dichotomy theorem for all real-valued symmetric matrices $\mathbf{A}$. Their result is too intricate to give a short and accurate summary here, but essentially it states that the problem of computing $Z_{\mathbf{A}}(G)$ for any real $\mathbf{A}$ is either in P or #P-hard. Again, which case it is depends on the connected components of $\mathbf{A}$. The overall statement remains that $Z_{\mathbf{A}}(G)$ is tractable (computable in P) if every connected component of $\mathbf{A}$ is, and is #P-hard otherwise. However, the exact description of tractability for connected $\mathbf{A}$ is much more technical and involved. The Hadamard matrix $\mathbf{H}$ and its tensor products $\mathbf{H} \otimes \mathbf{H} \otimes \cdots \otimes \mathbf{H}$ play a major role in the tractable case. If we index rows and columns of $\mathbf{H}$ by the finite field $\mathbb{Z}_2$, then its (x, y) entry is $(-1)^{xy}$. For the non-bipartite case, there is another 4×4 symmetric matrix $\mathbf{H}_4$, different from $\mathbf{H} \otimes \mathbf{H}$, where the rows and columns are indexed by $(\mathbb{Z}_2)^2$, and the entry at $((x_1, x_2), (y_1, y_2))$ is $(-1)^{x_1 y_2 + x_2 y_1}$. These matrices, and their arbitrary tensor products, all correspond to new tractable $Z_{\mathbf{A}}(G)$. In fact, there are some more tractable cases, starting with what can be roughly described as certain rank one modifications on these tensor products.

The proof of [10] proceeds by establishing a long sequence of successively more stringent properties that a tractable $\mathbf{A}$ must satisfy. Ultimately it arrives at a point where satisfaction of these properties implies that $Z_{\mathbf{A}}(G)$ can be computed as

$$\sum_{x_1, x_2, \ldots, x_n \in \mathbb{Z}_2} (-1)^{f(x_1, x_2, \ldots, x_n)},$$

where f is a quadratic polynomial over $\mathbb{Z}_2$. This sum is known to be computable in polynomial time [15] in n, the number of variables. In hindsight, the case with the simplest Hadamard matrix $\mathbf{H}$ which was an obstacle to the Bulatov-Grohe dichotomy theorem and was left open for some time, could have been directly solved, if one had adopted the polynomial view point of [10].

We independently came to the tractability of $Z_{\mathbf{H}}(G)$ from a slightly different angle. In [3], we were studying a certain type of Constraint Satisfaction Problems. This is motivated by investigations of a class of counting problems called *Holant* Problems, and it is connected with the technique called holographic reductions introduced by Valiant [19, 20]. Let us briefly describe this framework.

A *signature grid* $\Omega = (G, \mathcal{F})$ is a tuple, where $G = (V, E)$ is a graph, and each $v \in V$ is attached a function $F_v \in \mathcal{F}$. An edge assignment σ for every $e \in E$ gives an evaluation $\prod_{v \in V} F_v(\sigma \,|_{E(v)})$, where $E(v)$ denotes the incident edges of v. The counting problem on an input instance Ω is to compute

$$\text{Holant}(\Omega) = \sum_{\text{edge assignments } \sigma} \prod_{v \in V} F_v(\sigma \,|_{E(v)}).$$

For example, if we take $\sigma : E \to \{0, 1\}$, and attach the EXACT-ONE function at every vertex $v \in V$, then Holant(Ω) is exactly the number of perfect matchings. (Incidentally, it was proved in [9] that counting perfect matchings *cannot* be expressed as $Z_{\mathbf{A}}(G)$ for any matrix $\mathbf{A}$ over $\mathbb{R}$. However, every function $Z_{\mathbf{A}}(G)$ (vertex assignment) *can* be simulated by Holant(Ω) (edge assignment) as follows: $\mathbf{A}$ defines a function of arity 2 at every edge of G. Consider the bipartite Vertex-Edge incident graph $G' = (V(G), E(G), E')$ of G, where $(v, e) \in E'$ iff e is incident to v in G. Attach the EQUALITY function at every $v \in V(G)$ and the function defined by $\mathbf{A}$ at every $e \in E(G)$.) We denote a symmetric function on Boolean variables $x_1, \ldots, x_n$ by $[f_0, f_1, \ldots, f_n]$, where f_i is the value on inputs of Hamming weight i. Thus the EXACT-ONE function is $[0, 1, 0, \ldots, 0]$, and $\mathbf{H}$ is just $[1, 1, -1]$.

We discovered that the following three families of functions

$$\begin{aligned}
\mathcal{F}_1 &= \left\{ \lambda([1, 0]^{\otimes k} + i^r [0, \;\; 1]^{\otimes k}) \;\middle|\; \lambda \in \mathbb{C},\ k = 1, 2, \ldots,\ \text{and } r = 0, 1, 2, 3 \right\}; \\
\mathcal{F}_2 &= \left\{ \lambda([1, 1]^{\otimes k} + i^r [1, -1]^{\otimes k}) \;\middle|\; \lambda \in \mathbb{C},\ k = 1, 2, \ldots,\ \text{and } r = 0, 1, 2, 3 \right\}; \\
\mathcal{F}_3 &= \left\{ \lambda([1, \;\; i]^{\otimes k} + i^r [1, -i]^{\otimes k}) \;\middle|\; \lambda \in \mathbb{C},\ k = 1, 2, \ldots,\ \text{and } r = 0, 1, 2, 3 \right\}
\end{aligned}$$

give rise to tractable problems: Holant(Ω) for any $\Omega = (G, \mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3)$ is computable in P (here we listed functions in $\mathcal{F}_i$ in the form of truth tables on k Boolean variables). In particular, we note that by taking $r = 1$, $k = 2$ and $\lambda = (1 + i)^{-1}$ in $\mathcal{F}_3$, we recover the binary function $[1, 1, -1]$ which corresponds to exactly the Hadamard matrix $\mathbf{H}$. If we take $r = 0$, $\lambda = 1$ in $\mathcal{F}_1$, we get the EQUALITY function $[1, 0, \ldots, 0, 1]$ on k bits. This shows that $Z_{\mathbf{H}}(G)$ is a special case of Holant(Ω).

However, more instructive for us is the natural way in which complex numbers appeared in such counting problems, especially when applying holographic reductions. One can say that the presence of powers of $i = \sqrt{-1}$ in $\mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3$ "reveals" the true nature of $\mathbf{H}$ (i.e., $[1, 1, -1]$) as belonging to a family of tractable counting problems, where complex numbers are the right language. In fact, the tractability of Holant(Ω) for $\Omega = (G, \mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3)$ boils down to an exponential sum of the form

$$\sum_{x_1, x_2, \ldots, x_n \in \{0,1\}} i^{L_1 + L_2 + \cdots + L_s},$$

where each L_j, $j \in [s]$, is an indicator function of an affine linear form of $x_1, x_2, \ldots, x_n$ over $\mathbb{Z}_2$. Thus the exponent of i in the equation is a mod 4 sum of mod 2 sums of $x_1, x_2, \ldots, x_n$. From here it is only natural to investigate the computational complexity of $Z_{\mathbf{A}}(G)$, for a complex matrix $\mathbf{A}$.

Our investigation of complex-valued graph homomorphisms is also motivated by partition functions in quantum physics. In classical statistical physics, the partition function is always real-valued. However in a generic quantum system, for which complex numbers are the correct language, the partition function is in general complex-valued [8]. In particular, if the physics model is over a discrete graph and is non-orientable, then the edge weights are given by a symmetric complex matrix.

Our main theorem is the following

Theorem 1.1 (Dichotomy Theorem). *Let* $\mathbf{A}$ *be a symmetric complex matrix. Then* $Z_{\mathbf{A}}(\cdot)$ *either can be computed in polynomial time or is #P-hard.*

Due to the complexity of the proof of this theorem, both in terms of its overall proof structure and in terms of technical difficulty, we will first give a high level description of the proof for the bipartite case in Section 3. We then prove the First and Second Pinning Lemmas in Section 4. A more detailed outline of the proof for the two cases (bipartite and non-bipartite) with all the definitions and theorems, is presented in Section 5 and Section 6, respectively. We prove all the theorems in the rest of the paper.

2 Preliminaries

We use $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ to denote the set of all rational, real, and complex numbers, respectively.

For a positive integer n, we use $[n]$ to denote the set $\{1,\ldots,n\}$ (when $n=0$, it is just the empty set). We also use $[m:n]$, where $m\le n$, to denote the set $\{m,m+1,\ldots,n\}$. We use $\mathbf{1}_n$ to denote the all-one vector of dimension n. We omit n when it is clear from the context.

Let $\mathbf{x}$ and $\mathbf{y}$ be two vectors in $\mathbb{C}^n$, then we use $\langle\mathbf{x},\mathbf{y}\rangle$ to denote their inner product $\sum_{i=1}^n x_i\overline{y_i}$, and $\mathbf{x}\circ\mathbf{y}$ to denote their Hadamard product: $\mathbf{z}=\mathbf{x}\circ\mathbf{y}\in\mathbb{C}^n$, where $z_i=x_i\cdot y_i$ for all $i\in[n]$.

Let $\mathbf{A}=(A_{i,j})$ be a $k\times\ell$ matrix and $\mathbf{B}=(B_{i,j})$ be an $m\times n$ matrix. We use $\mathbf{A}_{i,*}$, $i\in[k]$, to denote the ith row vector, and $\mathbf{A}_{*,j}$, $j\in[\ell]$, to denote the jth column vector of $\mathbf{A}$. We let $\mathbf{C}=\mathbf{A}\otimes\mathbf{B}$ denote the tensor product of $\mathbf{A}$ and $\mathbf{B}$: $\mathbf{C}$ is a $km\times\ell n$ matrix whose rows and columns are indexed by $[k]\times[m]$ and $[\ell]\times[n]$, respectively, and satisfies

$$C_{(i_1,i_2),(j_1,j_2)}=A_{i_1,j_1}\cdot B_{i_2,j_2},\quad\text{for all } i_1\in[k],\ i_2\in[m],\ j_1\in[\ell] \text{ and } j_2\in[n].$$

Let $\mathbf{A}$ be an $n\times n$ symmetric complex matrix. We build an undirected graph $G=(V,E)$ from $\mathbf{A}$ as follows: $V=[n]$, and $ij\in E$ iff $A_{i,j}\ne 0$. We say $\mathbf{A}$ is *connected* if G is connected; and we say $\mathbf{A}$ has connected components $\mathbf{A}_1,\ldots,\mathbf{A}_s$, if the connected components of G are $V_1,\ldots,V_s$ and $\mathbf{A}_i$ is the $|V_i|\times|V_i|$ sub-matrix of $\mathbf{A}$ restricted by $V_i\subseteq[n]$, for all $i\in[s]$. Moreover, we say $\mathbf{A}$ is *bipartite* if the graph G is bipartite; otherwise, $\mathbf{A}$ is *non-bipartite*. Let Σ and Π be two permutations from $[n]$ to itself, then we use $\mathbf{A}_{\Sigma,\Pi}$ to denote the $n\times n$ matrix whose $(i,j)th$ entry, where $i,j\in[n]$, is $A_{\Sigma(i),\Pi(j)}$.

We say $\mathbf{C}$ is the bipartisation of a matrix $\mathbf{F}$ if

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

Note that $\mathbf{C}$ is always a symmetric matrix no matter whether $\mathbf{F}$ is or is not. For a positive integer N we use ω_N to denote $e^{2\pi i/N}$, a primitive Nth root of unity. We say a problem $\mathcal{A}$ is tractable if it can be solved in polynomial time. Given two problems $\mathcal{A}$ and $\mathcal{B}$, we say $\mathcal{A}$ is polynomial-time reducible to $\mathcal{B}$ (or $\mathcal{A}\le\mathcal{B}$), if there is an algorithm that solves $\mathcal{A}$ in polynomial time using an oracle for $\mathcal{B}$.

One technical issue is the model of computation with complex numbers. We can take any reasonable model of real or complex number computation, as long as arithmetic operations such as $+$ and $\times$ are computable, and equality is decidable [1, 13]. For the most part this issue of computation model seems not central to this paper, in part because we consider the matrix $\mathbf{A}$ to be fixed and the complexity measure is on the size of the input graph G. In the most restrictive sense we can require entries of $\mathbf{A}$ to be algebraic numbers. Over the algebraic numbers, our dichotomy theorem gives a decidable criterion.

2.1 Definitions of $\mathsf{EVAL}(\mathbf{A})$ and $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$

Let $\mathbf{A}\in\mathbb{C}^{m\times m}$ be a symmetric complex matrix with entries $(A_{i,j})$. It defines a graph homomorphism problem $\mathsf{EVAL}(\mathbf{A})$ as follows: Given an undirected graph $G=(V,E)$, compute

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

We call ξ an *assignment* to the vertices of G, and $\text{wt}_{\mathbf{A}}(\xi)$ the *weight* of ξ.

To study $\mathsf{EVAL}(\mathbf{A})$, we define a new and larger class of EVAL problems. It is a generalization of the edge-vertex weight problems introduced in [10]. See also [17].

Definition 2.1. *Let $\mathbf{C} \in \mathbb{C}^{m\times m}$ be a symmetric matrix, and*

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

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

$$Z_{\mathbf{C},\mathfrak{D}}(G) = \sum_{\xi: V\to[m]} \text{wt}_{\mathbf{C},\mathfrak{D}}(\xi),$$

where

$$\text{wt}_{\mathbf{C},\mathfrak{D}}(\xi) = \left(\prod_{(u,v)\in E} C_{\xi(u),\xi(v)}\right)\left(\prod_{v\in V} D_{\xi(v)}^{[\deg(v) \bmod N]}\right).$$

Let G be an undirected graph, and $G_1, \ldots, G_s$ be its connected components. Then

Lemma 2.1. *$Z_{\mathbf{C},\mathfrak{D}}(G) = Z_{\mathbf{C},\mathfrak{D}}(G_1) \times \ldots \times Z_{\mathbf{C},\mathfrak{D}}(G_s)$.*

Lemma 2.1 implies that, if we want to design an efficient algorithm for computing $Z_{\mathbf{C},\mathfrak{D}}(\cdot)$, we only need to focus on connected graphs. Furthermore if we want to construct a reduction from one problem $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ to another $\mathsf{EVAL}(\mathbf{C}',\mathfrak{D}')$, we only need to consider input graphs that are connected. Also note that, since $\mathsf{EVAL}(\mathbf{A})$ is a special case of $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ (in which every $\mathbf{D}^{[i]}$ is the identity matrix), Lemma 2.1 and the remarks above also apply to $Z_{\mathbf{A}}$ and $\mathsf{EVAL}(\mathbf{A})$.

Now suppose $\mathbf{C}$ is the bipartisation of an $m \times n$ matrix $\mathbf{F}$ (so $\mathbf{C}$ is $(m+n)\times(m+n)$). For any graph G and vertex u in G, we define $Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}(G,u)$ and $Z^{\leftarrow}_{\mathbf{C},\mathfrak{D}}(G,u)$ as follows. Let Ξ_1 denote the set of $\xi : V \to [m+n]$ with $\xi(u) \in [m]$, and Ξ_2 denote the set of ξ with $\xi(u) \in [m+1 : m+n]$, then

$$Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}(G,u) = \sum_{\xi\in\Xi_1} \text{wt}_{\mathbf{C},\mathfrak{D}}(\xi) \quad \text{and} \quad Z^{\leftarrow}_{\mathbf{C},\mathfrak{D}}(G,u) = \sum_{\xi\in\Xi_2} \text{wt}_{\mathbf{C},\mathfrak{D}}(\xi).$$

It then follows from the definition of $Z_{\mathbf{C},\mathfrak{D}}$, $Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}$ and $Z^{\leftarrow}_{\mathbf{C},\mathfrak{D}}$ that

Lemma 2.2. *For any graph G and vertex $u \in G$, $Z_{\mathbf{C},\mathfrak{D}}(G) = Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}(G,u) + Z^{\leftarrow}_{\mathbf{C},\mathfrak{D}}(G,u)$.*

The reason we introduce $Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}$ and $Z^{\leftarrow}_{\mathbf{C},\mathfrak{D}}$ is because of the following useful lemma.

Lemma 2.3. *For each $i \in \{0,1,2\}$, $\mathbf{F}^{[i]}$ is an $m_i \times n_i$ complex matrix for some positive integers m_i, n_i; $\mathbf{C}^{[i]}$ is the bipartisation of $\mathbf{F}^{[i]}$; and*

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

is a sequence of $(m_i+n_i)\times(m_i+n_i)$ diagonal matrices for some positive integer N, where

$$\mathbf{D}^{[i,r]} = \begin{pmatrix} \mathbf{P}^{[i,r]} & \\ & \mathbf{Q}^{[i,r]} \end{pmatrix}$$

and $\mathbf{P}^{[i,r]}$, $\mathbf{Q}^{[i,r]}$ are $m_i \times m_i$, $n_i \times n_i$ diagonal matrices, respectively. Suppose $m_0 = m_1 m_2$, $n_0 = n_1 n_2$,

$$\mathbf{F}^{[0]} = \mathbf{F}^{[1]} \otimes \mathbf{F}^{[2]}, \quad \mathbf{P}^{[0,r]} = \mathbf{P}^{[1,r]} \otimes \mathbf{P}^{[2,r]}, \quad \text{and} \quad \mathbf{Q}^{[0,r]} = \mathbf{Q}^{[1,r]} \otimes \mathbf{Q}^{[2,r]}, \quad \text{for all } r \in [0 : N-1].$$

Then for any connected *graph G and any vertex u^* in G, we have*

$$Z^{\rightarrow}_{\mathbf{C}^{[0]},\mathfrak{D}^{[0]}}(G,u^*) = Z^{\rightarrow}_{\mathbf{C}^{[1]},\mathfrak{D}^{[1]}}(G,u^*) \cdot Z^{\rightarrow}_{\mathbf{C}^{[2]},\mathfrak{D}^{[2]}}(G,u^*) \quad \textit{and} \tag{3}$$
$$Z^{\leftarrow}_{\mathbf{C}^{[0]},\mathfrak{D}^{[0]}}(G,u^*) = Z^{\leftarrow}_{\mathbf{C}^{[1]},\mathfrak{D}^{[1]}}(G,u^*) \cdot Z^{\leftarrow}_{\mathbf{C}^{[2]},\mathfrak{D}^{[2]}}(G,u^*).$$

Proof. We only prove (3) about $Z^{\rightarrow}$. First note that, if G is not bipartite then $Z^{\rightarrow}_{\mathbf{C}^{[i]},\mathfrak{D}^{[i]}}(G,u^*) = 0$ for all $i \in \{0,1,2\}$, and (3) holds trivially.

Now suppose $G = (U \cup V, E)$ is a bipartite graph, $u^* \in U$, and every edge $uv \in E$ has one vertex u from U and one vertex v from V. We let Ξ_i, $i \in \{0,1,2\}$, denote the set of assignments ξ_i from $U \cup V$ to $[m_i + n_i]$ such that $\xi_i(u) \in [m_i]$ for all $u \in U$ and $\xi_i(v) \in [m_i + 1 : m_i + n_i]$ for all $v \in V$. Since G is *connected*, we have

$$Z^{\rightarrow}_{\mathbf{C}^{[i]},\mathfrak{D}^{[i]}}(G,u^*) = \sum_{\xi_i \in \Xi_i} \text{wt}_{\mathbf{C}^{[i]},\mathfrak{D}^{[i]}}(\xi_i), \quad \text{for } i \in \{0,1,2\}.$$

To prove (3), we define the following map $\rho : \Xi_1 \times \Xi_2 \rightarrow \Xi_0$: $\rho(\xi_1,\xi_2) = \xi_0$, where for every $u \in U$, $\xi_0(u)$ is the row index of $\mathbf{F}^{[0]}$ that corresponds to row $\xi_1(u)$ of $\mathbf{F}^{[1]}$ and row $\xi_2(u)$ of $\mathbf{F}^{[2]}$ in the tensor product $\mathbf{F}^{[0]} = \mathbf{F}^{[1]} \otimes \mathbf{F}^{[2]}$; and similarly, for every $v \in V$, $\xi_0(v) - m_0$ is the column index of $\mathbf{F}^{[0]}$ that corresponds to column $\xi_1(v) - m_1$ of $\mathbf{F}^{[1]}$ and column $\xi_2(v) - m_2$ of $\mathbf{F}^{[2]}$ in the tensor product. One can check that ρ is a bijection, and

$$\text{wt}_{\mathbf{C}^{[0]},\mathfrak{D}^{[0]}}(\xi_0) = \text{wt}_{\mathbf{C}^{[1]},\mathfrak{D}^{[1]}}(\xi_1) \cdot \text{wt}_{\mathbf{C}^{[2]},\mathfrak{D}^{[2]}}(\xi_2), \quad \text{if } \rho(\xi_1,\xi_2) = \xi_0.$$

Equation (3) then follows. □

2.2 Basic #P-Hardness

We state the complexity dichotomy theorem of Bulatov and Grohe as follows:

Theorem 2.1 (Bulatov and Grohe [2]). *Let $\mathbf{A}$ be a symmetric and connected matrix with non-negative entries, then* $\mathsf{EVAL}(\mathbf{A})$ *is either in P or #P-complete. More precisely,*

- *If $\mathbf{A}$ is bipartite, then* $\mathsf{EVAL}(\mathbf{A})$ *is in polynomial time if the rank of $\mathbf{A}$ is 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.*

Theorem 2.1 gives us the following useful corollary:

Corollary 2.1. *Let $\mathbf{A}$ be a symmetric and connected matrix with non-negative entries. If*

$$\begin{pmatrix} A_{i,k} & A_{i,\ell} \\ A_{j,k} & A_{j,\ell} \end{pmatrix}$$

is a 2×2 sub-matrix of $\mathbf{A}$ such that all of its four entries are nonzero and $A_{i,k}A_{j,\ell} \neq A_{i,\ell}A_{j,k}$, then the problem $\mathsf{EVAL}(\mathbf{A})$ *is #P-complete.*

3 A High Level Description of the Proof

The first step in the proof of Theorem 1.1 is to reduce the problem to connected graphs/matrices.

Let $\mathbf{A}$ be an $m \times m$ symmetric complex matrix. It is clear that if G has connected components G_i, then

$$Z_{\mathbf{A}}(G) = \prod_i Z_{\mathbf{A}}(G_i);$$

and if G is connected and $\mathbf{A}$ has connected components $\mathbf{A}_j$, then $Z_{\mathbf{A}}(G) = \sum_j Z_{\mathbf{A}_j}(G)$. Hence if every $Z_{\mathbf{A}_j}(\cdot)$ is computable in P, then so is $Z_{\mathbf{A}}(\cdot)$.

The hardness direction is less obvious: suppose $Z_{\mathbf{A}_j}(\cdot)$ is #P-hard for some j, we want to show that $Z_{\mathbf{A}}(\cdot)$ is also #P-hard. We do this by showing that computing $Z_{\mathbf{A}_j}(\cdot)$ is reducible to computing $Z_{\mathbf{A}}(\cdot)$. Let G be an arbitrary input graph. To compute $Z_{\mathbf{A}_j}(G)$ it suffices to compute $Z_{\mathbf{A}_j}(G_i)$ for all connected components G_i of G. Therefore, we may assume that G is connected. Define a *pinning* version of the $Z_{\mathbf{A}}(\cdot)$ function as follows. For any chosen vertex $w \in V(G)$, and any $k \in [m]$, let

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

Then we can prove a *Pinning Lemma* (Lemma 4.1) which states that the problem of computing $Z_{\mathbf{A}}(\cdot)$ is polynomial-time equivalent to computing $Z_{\mathbf{A}}(\cdot, \cdot, \cdot)$. Note that if V_j denotes the subset of $[m]$ where $\mathbf{A}_j$ is the sub-matrix of $\mathbf{A}$ restricted by V_j, then for a connected G, $Z_{\mathbf{A}_j}(G) = \sum_{k \in V_j} Z_{\mathbf{A}}(G, w, k)$.

The proof of this Pinning Lemma (Lemma 4.1) is a standard adaptation to the complex numbers of the one proved in [10]. However, for technical reasons we will need a total of three Pinning Lemmas (Lemma 4.1, 4.2 and 8.2) where some proofs are a bit more involved. We also remark that the Pinning Lemma proves the *existence* of polynomial-time reductions between $Z_{\mathbf{A}}(\cdot)$ and $Z_{\mathbf{A}}(\cdot, \cdot, \cdot)$, but the lemma does not constructively produce such a reduction, given $\mathbf{A}$. The proof of the Pinning Lemma in [10] uses a recent result by Lovász [17], which was proved for real matrices. We give a direct proof without using this result of Lovász.

After this preliminary step, we restrict to connected $\mathbf{A}$. As indicated, to our work the two most influential predecessor papers are by Bulatov and Grohe [2] and by Goldberg et. al. [10]. In both papers the polynomial-time algorithms for the tractable cases are relatively straightforward. The difficult part of the proof is to show that in all other cases the problem is #P-hard. Our proof follows a similar overall conceptual framework to that of Goldberg et. al. [10]. However due to the difficulties introduced by the complex numbers, both the overall organization and the substantive part of the proof have to be done separately. This difficulty starts with the most basic proof technique called gadget constructions, to be discussed shortly. Technically, it turns out that all our hardness proofs are reductions to the non-negative case using Bulatov-Grohe [2] rather than to [10]. The difficulty with proving hardness for complex matrices goes deeper than appearance. Intuitively, the complex numbers afford a much richer variety of cancelations, which could lead to very efficient algorithms. It turns out that this is indeed the case, and we obtain more non-trivial tractable cases. These boil down to certain exponential sums over rings of a quadratic polynomial with a base that is a root of unity. While the corresponding sum for finite fields is known [15], the corresponding result over rings appears to be new and is of independent interest. (Odd prime powers behave somewhat differently than powers of 2. The dichotomy theorem of [10] can be considered as the special case where the only root of unity is -1.)

We now briefly describe the proof structure for connected $\mathbf{A}$. As has already been used many times before, a key tool in the proof of hardness is to design graph gadgets, which takes any input graph G and produces a modified graph G^* with the following property: One can transform the fixed matrix $\mathbf{A}$ to a suitably modified matrix $\mathbf{A}^*$, such that $Z_{\mathbf{A}^*}(G) = Z_{\mathbf{A}}(G^*)$. A simple example of this maneuver is called *thickening* where one replaces each edge in G by t parallel edges to get G^*. Then it is easy to see that $\mathbf{A}^*$ is obtained from $\mathbf{A}$ by replacing each entry $A_{i,j}$ by its t^{th} power $(A_{i,j})^t$. In particular, if $\mathbf{A}$ is real and t is even, this produces a non-negative matrix $\mathbf{A}^*$, to which one may apply the Bulatov-Grohe result. The equality $Z_{\mathbf{A}^*}(G) = Z_{\mathbf{A}}(G^*)$ shows that if $Z_{\mathbf{A}^*}(\cdot)$ is #P-hard then so is $Z_{\mathbf{A}}(\cdot)$.

For Theorem 1.1, we immediately encountered the following difficulty. Any gadget construction will only produce a matrix $\mathbf{A}^*$ whose entries are obtained from entries of $\mathbf{A}$ by arithmetic operations $+$ and $\times$. While for real numbers any even power guarantees a non-negative quantity, as was done in [10], no obvious arithmetic operations on the complex numbers have this property. Pointedly, conjugation is not an arithmetic operation. However, it is also clear that for roots of unity, one *can* always produce conjugation by multiplication.

Thus, our proof starts with a process to replace an arbitrary complex matrix by a *purified* complex matrix which has a special form. It turns out that we must separate out the cases where the graph of the matrix $\mathbf{A}$ is bipartite or non-bipartite. A purified bipartite (and symmetric, connected) matrix takes the following form

$$\begin{pmatrix} \mathbf{0} & \mathbf{B} \\ \mathbf{B}^T & \mathbf{0} \end{pmatrix},$$

where

$$\mathbf{B} = \begin{pmatrix} \mu_1 & & & \\ & \mu_2 & & \\ & & \ddots & \\ & & & \mu_k \end{pmatrix} \begin{pmatrix} \zeta_{1,1} & \zeta_{1,2} & \cdots & \zeta_{1,m-k} \\ \zeta_{2,1} & \zeta_{2,2} & \cdots & \zeta_{2,m-k} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_{k,1} & \zeta_{k,2} & \cdots & \zeta_{k,m-k} \end{pmatrix} \begin{pmatrix} \mu_{k+1} & & & \\ & \mu_{k+2} & & \\ & & \ddots & \\ & & & \mu_m \end{pmatrix},$$

for some $1 \le k < m$, in which every $\mu_i > 0$ and every $\zeta_{i,j}$ is a root of unity.

The claim is that for every symmetric, connected and bipartite matrix $\mathbf{A} \in \mathbb{C}^{m\times m}$, either we can already prove the #P-hardness of computing $Z_{\mathbf{A}}(\cdot)$ or there exists a symmetric, connected and *purified* bipartite matrix $\mathbf{A}' \in \mathbb{C}^{m\times m}$ such that computing $Z_{\mathbf{A}'}(\cdot)$ is polynomial time equivalent to computing $Z_{\mathbf{A}}(\cdot)$ (see Theorem 5.1). For non-bipartite $\mathbf{A}$, a corresponding statement holds (see Theorem 6.1). For convenience, in the discussion below, we only focus on the bipartite case.

Continuing now with a purified bipartite matrix $\mathbf{A}$, the next step is to further regularize its entries. In particular we need to combine those rows and columns of the matrix where they are essentially the same apart from a multiple of a root of unity. This process is called *Cyclotomic* Reduction. In order to carry out this process, we need to use the more general counting problem $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ defined in Section 2.1. We also need to introduce the following type of matrices called *discrete unitary* matrices:

Definition 3.1 (Discrete Unitary Matrix)**.** *Let $\mathbf{F} \in \mathbb{C}^{m\times m}$ be a 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 $F_{i,j}$ of $\mathbf{F}$ is a root of unity, and $M = \text{lcm}\big\{\text{the order of } F_{i,j} : i, j \in [m]\big\}$;*
2. *$F_{1,i} = F_{i,1} = 1$ for all $i \in [m]$; and*
3. *For all $i \ne j \in [m]$, $\langle \mathbf{F}_{i,*}, \mathbf{F}_{j,*}\rangle = 0$ and $\langle \mathbf{F}_{*,i}, \mathbf{F}_{*,j}\rangle = 0$.*

Some simplest examples of discrete unitary matrices are as follows:

$$\mathbf{H} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \ \mathbf{H_4} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, \ \mathbf{F}_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, \ \mathbf{F}_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \zeta & \zeta^{-1} & \zeta^2 & \zeta^{-2} \\ 1 & \zeta^2 & \zeta^{-2} & \zeta^{-1} & \zeta \\ 1 & \zeta^{-1} & \zeta & \zeta^{-2} & \zeta^2 \\ 1 & \zeta^{-2} & \zeta^2 & \zeta & \zeta^{-1} \end{pmatrix},$$

where $\omega = e^{2\pi i/3}$ and $\zeta = e^{2\pi i/5}$. Also note that any tensor product of discrete unitary matrices is also a discrete unitary matrix. These matrices play a major role in our proof.

Now we come back to the proof outline. We show that $Z_{\mathbf{A}}(\cdot)$ is either #P-hard or polynomial time equivalent to $Z_{\mathbf{C},\mathfrak{D}}(\cdot)$ for some $\mathbf{C} \in \mathbb{C}^{2n\times 2n}$ and some $\mathfrak{D}$ of diagonal matrices from $\mathbb{C}^{2n\times 2n}$, where $\mathbf{C}$ is the bipartisation of a discrete unitary matrix, for some positive integer n. In addition to requiring $\mathbf{C}$ to be the bipartisation of a discrete unitary matrix, there are further stringent requirements for $\mathfrak{D}$, otherwise $Z_{\mathbf{A}}$ is #P-hard. The detailed statements can be found in Theorem 5.2 and 5.3, summarized in properties $(\mathcal{U}_1)$ to $(\mathcal{U}_5)$. Roughly speaking, the first matrix $\mathbf{D}^{[0]}$ in $\mathfrak{D}$ must be the identity matrix; and for any matrix $\mathbf{D}^{[r]}$ in $\mathfrak{D}$, every entry of $\mathbf{D}^{[r]}$ is either zero or a root of unity. We call all of these requirements, with some abuse of terminology, the discrete unitary requirements.

Now assume that we have a problem $(\mathbf{C},\mathfrak{D})$ satisfying the discrete unitary requirements.

Definition 3.2. *Let $q > 1$ be a prime power, then the following $q \times q$ matrix $\boldsymbol{\mathcal{F}}_q$ is called the q-*Fourier matrix*: The (x, y)th entry of $\boldsymbol{\mathcal{F}}_q$, where $x, y \in [0 : q-1]$, is ω_q^{xy}.*

We next show that either $Z_{\mathbf{C},\mathfrak{D}}(\cdot)$ is #P-hard or after a permutation of rows and columns, $\mathbf{C}$ is the bipartisation of a matrix which is a tensor product of suitable Fourier matrices. This tensor product decomposition into Fourier matrices gives us a canonical way of writing the elements of the matrix $\mathbf{C}$ in a closed form. After obtaining this canonical expression, we further inquire the structure of $\mathfrak{D}$. The canonical tensor product decomposition gives us a way to index the rows and columns of $\mathbf{C}$ and every diagonal matrix in $\mathfrak{D}$ using elements from a suitable Abelian group. More precisely, the first half and the second half of the entries of each $\mathbf{D}^{[r]}$ in $\mathfrak{D}$ are indexed by $(0,\mathbf{x})$ and $(1,\mathbf{x})$ respectively, where $\mathbf{x}$ is from the group. It turns out that there are two more properties that we can prove about $\mathfrak{D}$; otherwise the problem of computing $Z_{\mathbf{C},\mathfrak{D}}(\cdot)$ is #P-hard.

First, for each r, we define Λ_r and Δ_r to be the support of $\mathbf{D}^{[r]}$, where Λ_r refers to the first half of the entries and Δ_r refers to the second half of the entries:

$$\Lambda_r = \big\{\mathbf{x} \mid D^{[r]}_{(0,\mathbf{x})} \neq 0\big\} \quad \text{and} \quad \Delta_r = \big\{\mathbf{x} \mid D^{[r]}_{(1,\mathbf{x})} \neq 0\big\}.$$

We let $\mathcal{S}$ denote the set of subscripts r such that $\Lambda_r \neq \emptyset$ and $\mathcal{T}$ denote the set of r such that $\Delta_r \neq \emptyset$. We can prove that for every $r \in \mathcal{S}$, $\Lambda_r = \prod_{i=1}^{s} \Lambda_{r,i}$ is a direct product of cosets in the Abelian group, where $i = 1, \ldots, s$ correspond to the constituent prime powers of the group. Similarly for every $r \in \mathcal{T}$, $\Delta_r = \prod_{i=1}^{s} \Delta_{r,i}$ is also a direct product of cosets in the same Abelian group; Otherwise, $Z_{\mathbf{C},\mathfrak{D}}(\cdot)$ is #P-hard.

Second we show that for each $r \in \mathcal{S}$ and $r \in \mathcal{T}$, respectively, $\mathbf{D}^{[r]}$ on its support Λ_r for the first half of its entries and on Δ_r for the second half of its entries, respectively, possesses a *quadratic* structure; otherwise $Z_{\mathbf{C},\mathfrak{D}}(\cdot)$ is #P-hard. We can express this quadratic structure as a set of *exponential difference equations* over bases which are appropriate roots of unity of orders equal to various prime powers.

After all these necessary conditions, we prove that if $\mathbf{C}$ and $\mathfrak{D}$ satisfy all these requirements, then there is a polynomial-time algorithm to compute $Z_{\mathbf{C},\mathfrak{D}}(\cdot)$ and thus, the problem of computing $Z_{\mathbf{A}}(\cdot)$ is in P. As remarked earlier this tractability result may be of independent interest.

4 Pinning Lemmas and Preliminary Reductions

In this section, we prove two pinning lemmas, one for $\mathsf{EVAL}(\mathbf{A})$ and one for $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ where $(\mathbf{C},\mathfrak{D})$ satisfies certain conditions. The proof of the first lemma is very similar to [10], but the second one has some complications.

4.1 A Pinning Lemma for $\mathsf{EVAL}(\mathbf{A})$

Let $\mathbf{A}$ be an $m \times m$ symmetric complex matrix. We define $\mathsf{EVALP}(\mathbf{A})$ as follows: The input is a triple (G, w, i), where $G = (V, E)$ is an undirected graph, $w \in V$ is a vertex, and $i \in [m]$; The output is

$$Z_{\mathbf{A}}(G, w, i) = \sum_{\xi: V \to [m],\, \xi(w) = i} \mathrm{wt}_{\mathbf{A}}(\xi).$$

It is easy to see that $\mathsf{EVAL}(\mathbf{A}) \le \mathsf{EVALP}(\mathbf{A})$, but the following lemma shows that the reverse direction is also true.

Lemma 4.1 (First Pinning Lemma)**.** $\mathsf{EVALP}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{A})$.

We define the following equivalence relation over $[m]$ (Note that we do not know, given $\mathbf{A}$, how to compute this relation efficiently, but we know it exists. The lemma only proves, non-constructively, the existence of a polynomial-time reduction. Also see [17]):

$$i \sim j \;\text{ if for any undirected graph } G = (V, E) \text{ and } w \in V,\ Z_{\mathbf{A}}(G, w, i) = Z_{\mathbf{A}}(G, w, j).$$

This relation divides the set $[m]$ into s equivalence classes $\mathcal{A}_1, \ldots, \mathcal{A}_s$, for some positive integer s. For any $t \neq t' \in [s]$, there exists a pair $P_{t,t'} = (G, w)$, where G is an undirected graph and w is a vertex in G, such that (Again, we do not know how to find such a pair efficiently, but it always exists by the definition of the equivalence relation $\sim$.)

$$Z_{\mathbf{A}}(G, w, i) = Z_{\mathbf{A}}(G, w, j) \neq Z_{\mathbf{A}}(G, w, i') = Z_{\mathbf{A}}(G, w, j'), \quad \text{for all } i, j \in \mathcal{A}_t \text{ and } i', j' \in \mathcal{A}_{t'}.$$

Now for any subset $S \subseteq [s]$, we define a problem $\mathsf{EVAL}(\mathbf{A}, S)$ as follows: The input is a pair (G, w), where $G = (V, E)$ is an undirected graph and w is a vertex in G; The output is

$$Z_{\mathbf{A}}(G, w, S) = \sum_{\xi: V \to [m],\, \xi(w) \in \bigcup_{t \in S} \mathcal{A}_t} \mathrm{wt}_{\mathbf{A}}(\xi).$$

Clearly, if $S = [s]$, then $\mathsf{EVAL}(\mathbf{A}, S)$ is exactly $\mathsf{EVAL}(\mathbf{A})$. We prove the following claim:

Claim 4.1. *If $S \subseteq [s]$ and $|S| \ge 2$, then there exists a partition $\{S_1, \ldots, S_k\}$ of S for some $k > 1$ and*

$$\mathsf{EVAL}(\mathbf{A}, S_d) \le \mathsf{EVAL}(\mathbf{A}, S), \quad \textit{for all } d \in [k].$$

Before proving this claim, we use it to prove the First Pinning Lemma.

Proof of Lemma 4.1. Let (G, w, i) be an input of $\mathsf{EVALP}(\mathbf{A})$, and $i \in \mathcal{A}_t$ for some $t \in [s]$. We will use Claim 4.1 to prove that $\mathsf{EVAL}(\mathbf{A}, \{t\}) \le \mathsf{EVAL}(\mathbf{A})$. If this is true, then we are done because

$$Z_{\mathbf{A}}(G, w, i) = \frac{1}{|\mathcal{A}_t|} \cdot Z_{\mathbf{A}}(G, w, \{t\}).$$

To prove $\mathsf{EVAL}(\mathbf{A}, \{t\}) \le \mathsf{EVAL}(\mathbf{A})$, we apply Claim 4.1 above to $S = [s]$; if $s = 1$, then Lemma 4.1 is trivially true. By Claim 4.1, there exists a partition $\{S_1, \ldots, S_k\}$ of S, for some $k > 1$, such that

$$\mathsf{EVAL}(\mathbf{A}, S_d) \le \mathsf{EVAL}(\mathbf{A}, S) \equiv \mathsf{EVAL}(\mathbf{A}), \quad \text{for all } d \in [k].$$

Without loss of generality, assume $t \in S_1$. If $S_1 = \{t\}$, then we are done; otherwise we have $t \in S_1$ and $|S_1| \ge 2$. In this case, we just rename S_1 to be S and repeat the process above. Because $|S|$ is strictly monotonically decreasing after each iteration, this procedure will stop at some time, and we conclude that $\mathsf{EVAL}(\mathbf{A}, \{t\}) \le \mathsf{EVAL}(\mathbf{A})$. $\square$

Proof of Claim 4.1. Let $t \neq t'$ be two integers in S (as $|S| \geq 2$, such $t \neq t'$ exist). We let $P_{t,t'} = (G^*, w^*)$, where $G^* = (V^*, E^*)$. It defines the following equivalence relation $\sim^*$ over S: For $a, b \in S$,

$$a \sim^* b \ \text{ if } Z_{\mathbf{A}}(G^*, w^*, i) = Z_{\mathbf{A}}(G^*, w^*, j), \ \text{ where } i \in \mathcal{A}_a \text{ and } j \in \mathcal{A}_b.$$

This equivalence relation $\sim^*$ is clearly well-defined, being independent of our choices of $i \in \mathcal{A}_a, j \in \mathcal{A}_b$. It gives us equivalence classes $\{S_1, \ldots, S_k\}$, a partition of S. Because $(G^*, w^*) = P_{t,t'}$, by the definition of $\sim^*$, t and t' belong to different classes and thus, $k \geq 2$. For each $d \in [k]$, we let X_d denote

$$X_d = Z_{\mathbf{A}}(G^*.w^*, i), \quad \text{where } i \in \mathcal{A}_a \text{ and } a \in S_d.$$

This X_d is well-defined, being independent of the choices of $a \in S_d$ and $i \in \mathcal{A}_a$. The definition of the equivalence relation $\sim^*$ implies that $X_d \neq X_{d'}$ for all $d \neq d' \in [k]$.

Next, let G be an undirected graph and w be a vertex. We show that, by querying $\mathsf{EVAL}(\mathbf{A}, S)$ as an oracle, one can compute $Z_{\mathbf{A}}(G, w, S_d)$ efficiently for all d.

For each $p \in [0 : k-1]$ we construct a graph $G^{[p]} = (V^{[p]}, E^{[p]})$ as follows. Graph $G^{[p]}$ is the disjoint union of G and p independent copies of G^*, except that the w in G and the w^*'s in all copies of G^* are identified as one single vertex $w' \in V^{[p]}$ (thus $|V^{[p]}| = |V| + p \cdot |V^*| - p$). In particular, $G^{[0]} = G$.

We have the following collection of equations: For every $p \in [0 : k-1]$,

$$Z_{\mathbf{A}}(G^{[p]}, w', S) = \sum_{d \in [k]} (X_d)^p \cdot Z_{\mathbf{A}}(G, w, S_d).$$

Because $X_d \neq X_{d'}$ for all $d \neq d'$, this is a Vandermonde system and we can solve it to get $Z_{\mathbf{A}}(G, w, S_d)$ for all $d \in [k]$. As both k and the size of the graph G^* are constants that are independent of G, this gives us a polynomial-time reduction from $\mathsf{EVAL}(\mathbf{A}, S_d)$ to $\mathsf{EVAL}(\mathbf{A}, S)$, for every $d \in [k]$. ☐

4.2 A Pinning Lemma for $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$

Let $\mathbf{C}$ be the bipartisation of $\mathbf{F} \in \mathbb{C}^{m \times m}$ (so $\mathbf{C}$ is $2m \times 2m$). Let $\mathfrak{D} = \{\mathbf{D}^{[0]}, \ldots, \mathbf{D}^{[N-1]}\}$ be a sequence of N $2m \times 2m$ diagonal matrices. We define $\mathsf{EVALP}(\mathbf{C}, \mathfrak{D})$ as follows: The input is a triple (G, w, i), where $G = (V, E)$ is an undirected graph, $w \in V$ is a vertex, and i is an integer in $[2m]$; The output is

$$Z_{\mathbf{C},\mathfrak{D}}(G, w, i) = \sum_{\xi: V \to [2m],\, \xi(w) = i} \mathrm{wt}_{\mathbf{C},\mathfrak{D}}(\xi).$$

It is easy to see that $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D}) \leq \mathsf{EVALP}(\mathbf{C}, \mathfrak{D})$. However, unlike problems $\mathsf{EVALP}(\mathbf{A})$ and $\mathsf{EVAL}(\mathbf{A})$ we can only prove the reverse direction when $(\mathbf{C}, \mathfrak{D})$ satisfies the following condition:

($\mathcal{P}$*inning*) Every entry of $\mathbf{F}$ is a power of ω_N, for some positive integer N; $\frac{1}{\sqrt{m}} \cdot \mathbf{F}$ is a unitary matrix; and $\mathbf{D}^{[0]}$ is the $2m \times 2m$ identity matrix.

Lemma 4.2 (Second Pinning Lemma)**.** *If* $(\mathbf{C}, \mathfrak{D})$ *satisfies* ($\mathcal{P}$*inning*)*, then* $\mathsf{EVALP}(\mathbf{C}, \mathfrak{D}) \equiv \mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$.

Corollary 4.1. *If* $(\mathbf{C}, \mathfrak{D})$ *satisfies* ($\mathcal{P}$*inning*)*, then the problem of computing function* $Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}$ *(or function* $Z^{\leftarrow}_{\mathbf{C},\mathfrak{D}}$*) is polynomial time reducible to* $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$.

We define the following equivalence relation over $[2m]$:

$$i \sim j \ \text{ if for any undirected graph } G = (V, E) \text{ and } w \in V,\ Z_{\mathbf{C},\mathfrak{D}}(G, w, i) = Z_{\mathbf{C},\mathfrak{D}}(G, w, j).$$

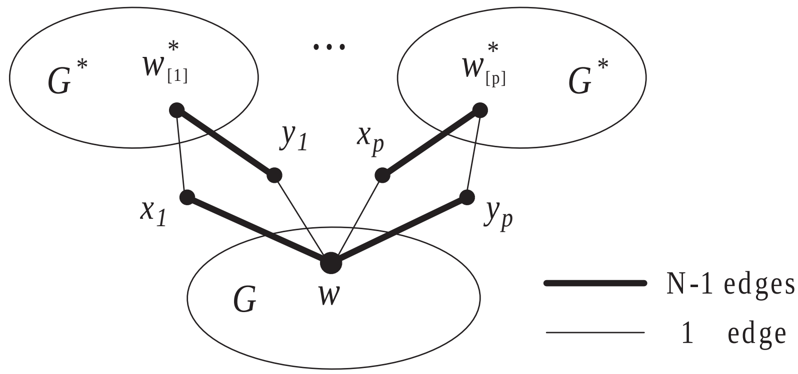

Figure 1: Graph $G^{[p]}$, $p \in [0 : k-1]$.

This relation divides $[2m]$ into s equivalence classes $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_s$, for some positive integer s. For any $t \neq t' \in [s]$ there exists a $P_{t,t'} = (G, w)$, where G is an undirected graph and w is a vertex, such that

$$Z_{\mathbf{C},\mathfrak{D}}(G,w,i) = Z_{\mathbf{C},\mathfrak{D}}(G,w,j) \neq Z_{\mathbf{C},\mathfrak{D}}(G,w,i') = Z_{\mathbf{C},\mathfrak{D}}(G,w,j'), \quad \text{for all } i,j \in \mathcal{A}_t \text{ and } i',j' \in \mathcal{A}_{t'}.$$

Now for any subset $S \subseteq [s]$, we define $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D}, S)$ as follows: The input is a pair (G, w), where $G = (V, E)$ is an undirected graph and w is a vertex in G; The output is

$$Z_{\mathbf{C},\mathfrak{D}}(G,w,S) = \sum_{\xi:V\rightarrow[2m],\, \xi(w)\in\bigcup_{t\in S}\mathcal{A}_t} \text{wt}_{\mathbf{C},\mathfrak{D}}(\xi).$$

Clearly, when $S = [s]$, $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D}, S)$ is exactly $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$. We prove the following claim:

Claim 4.2. *If $S \subseteq [s]$ and $|S| \geq 2$, then there exists a partition $\{S_1, \ldots, S_k\}$ of S for some $k > 1$, such that*

$$\mathsf{EVAL}(\mathbf{C}, \mathfrak{D}, S_d) \leq \mathsf{EVAL}(\mathbf{C}, \mathfrak{D}, S), \quad \textit{for all } d \in [k].$$

Lemma 4.2 then follows from Claim 4.2. Its proof is exactly the same as the one of Lemma 4.1 using Claim 4.1, so we omit it here.

Proof of Claim 4.2. Let $t \neq t'$ be two integers in S (as $|S| \geq 2$, such $t \neq t'$ exist). We let $P_{t,t'} = (G^*, w^*)$, where $G^* = (V^*, E^*)$. It defines the following equivalence relation over S: For $a, b \in S$,

$$a \sim^* b \ \text{ if } Z_{\mathbf{C},\mathfrak{D}}(G^*, w^*, i) = Z_{\mathbf{C},\mathfrak{D}}(G^*, w^*, j), \ \text{ where } i \in \mathcal{A}_a \text{ and } j \in \mathcal{A}_b.$$

This gives us equivalence classes $\{S_1, \ldots, S_k\}$, a partition of S. Since $(G^*, w^*) = P_{t,t'}$, t and t' belong to different classes and thus, $k \geq 2$. For each $d \in [k]$, we let Y_d denote

$$Y_d = Z_{\mathbf{C},\mathfrak{D}}(G^*, w^*, i), \quad \text{where } i \in \mathcal{A}_a \text{ and } a \in S_d.$$

The definition of the equivalence relation implies that $Y_d \neq Y_{d'}$ for all $d \neq d' \in [k]$.

Now let G be an undirected graph and w be a vertex. We show that, by querying $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D}, S)$ as an oracle, one can compute $Z_{\mathbf{C},\mathfrak{D}}(G, w, S_d)$ efficiently for all $d \in [k]$.

For every integer $p \in [0 : k-1]$, we build a graph $G^{[p]} = (V^{[p]}, E^{[p]})$ as follows: $G^{[p]}$ contains G and p independent copies of G^*. The vertex w in G is then *connected appropriately* to the w^* of each G^* (see Figure 1). More precisely, we have $V^{[p]}$ as a disjoint union:

$$V^{[p]} = V \cup \Big(\bigcup_{i=1}^{p} \{ v_{[i]} \,\big|\, v \in V^* \} \Big) \cup \{x_1, \ldots, x_p, y_1, \ldots, y_p\},$$

where $x_1, \ldots, x_p, y_1, \ldots, y_p$ are new vertices, and $E^{[p]}$ contains precisely the following edges:

1. If $uv \in E$, then $uv \in E^{[p]}$; If $uv \in E^*$, then $u_{[i]}v_{[i]} \in E^{[p]}$ for all $i \in [p]$;
2. One edge between $(w^*_{[i]}, x_i)$ and (y_i, w) for each $i \in [p]$; and
3. $N - 1$ edges between (x_i, w) and $(w^*_{[i]}, y_i)$ for each $i \in [p]$.

In particular, we have $G^{[0]} = G$.

We have the following collection of equations: For $p \in [0 : k-1]$, $Z_{\mathbf{C},\mathfrak{D}}(G^{[p]}, w, S)$ is equal to

$$\sum_{\substack{i \in \cup_{a \in S} \mathcal{A}_a \\ i_1, \ldots, i_p \in [2m]}} Z_{\mathbf{C},\mathfrak{D}}(G, w, i) \left(\prod_{j=1}^{p} Z_{\mathbf{C},\mathfrak{D}}(G^*, w^*, i_j) \right) \prod_{j=1}^{p} \left(\sum_{x \in [2m]} C_{i_j,x} \overline{C_{i,x}} \sum_{y \in [2m]} \overline{C_{i_j,y}} C_{i,y} \right).$$

By condition (*Pinning*), $\sum_{x \in [2m]} C_{i_j,x} \overline{C_{i,x}} = \langle \mathbf{F}_{i_j,*}, \mathbf{F}_{i,x} \rangle$ is 0 unless $i = i_j$. Therefore, we have

$$Z_{\mathbf{C},\mathfrak{D}}(G^{[p]}, w, S) = m^{2p} \cdot \sum_{i \in \cup_{a \in S} \mathcal{A}_a} Z_{\mathbf{C},\mathfrak{D}}(G, w, i) \big(Z_{\mathbf{C},\mathfrak{D}}(G^*, w^*, i) \big)^p = m^{2p} \cdot \sum_{d \in [k]} (Y_d)^p \cdot Z_{\mathbf{C},\mathfrak{D}}(G, w, S_d).$$

Since $Y_d \neq Y_{d'}$ for all $d \neq d'$, this is a Vandermonde system, and we can solve it to get $Z_{\mathbf{C},\mathfrak{D}}(G, w, S_d)$ for all d. As both k and the size of the graph G^* are constants that are independent of G, this gives us a polynomial-time reduction from $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D}, S_d)$ to $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D}, S)$ for every $d \in [k]$. □

4.3 Reduction to Connected Matrices

The following lemma allows us to focus on the connected components of $\mathbf{A}$:

Lemma 4.3. *Let $\mathbf{A} \in \mathbb{C}^{m \times m}$ be a symmetric matrix with components $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_s$. Then*

- *If $\mathsf{EVAL}(\mathbf{A}_i)$ is #P-hard for some $i \in [s]$, then $\mathsf{EVAL}(\mathbf{A})$ is #P-hard;*
- *If $\mathsf{EVAL}(\mathbf{A}_i)$ is polynomial-time computable for every $i \in [s]$, then so is $\mathsf{EVAL}(\mathbf{A})$.*

Proof. Lemma 4.3 follows directly from the First Pinning Lemma (Lemma 4.1). □

The main Dichotomy Theorem 1.1 will be proved by showing that for every connected $\mathbf{A} \in \mathbb{C}^{m \times m}$, the problem $\mathsf{EVAL}(\mathbf{A})$ is either solvable in polynomial-time, or #P-hard.

5 Proof Outline of the Case: A is Bipartite

We now give an overview of the proof of Theorem 1.1 for the case when $\mathbf{A}$ is connected and bipartite. The proof consists of two parts: a hardness part and a tractability part. The hardness part is further divided into three major steps in which we gradually "simplify" the problem being considered. In each of the three steps, we consider an EVAL problem passed down by the previous step (Step 1 starts with $\mathsf{EVAL}(\mathbf{A})$ 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.

One can view the three steps as three filters which remove #P-hard $\mathsf{EVAL}(\mathbf{A})$ problems using different arguments. Finally in the tractability part, we show that all the EVAL problems that survive the three filters are indeed polynomial-time solvable.

5.1 Step 1: Purification of Matrix A

We start with $\mathsf{EVAL}(\mathbf{A})$, in which $\mathbf{A} \in \mathbb{C}^{m\times m}$ is symmetric, connected, and bipartite. It is easy to see that if $m = 1$, then $\mathsf{EVAL}(\mathbf{A})$ is tractable. So in the discussion below, we assume $m > 1$.

In this step, we show that $\mathsf{EVAL}(\mathbf{A})$ is either #P-hard or polynomial-time equivalent to $\mathsf{EVAL}(\mathbf{A}')$, in which $\mathbf{A}'$ is also an $m \times m$ matrix but has a very nice structure.

Definition 5.1. *Let $\mathbf{A} \in \mathbb{C}^{m\times m}$ be a symmetric, connected and bipartite matrix. We say it is a* purified bipartite matrix *if there exist positive rational numbers $\mu_1, \ldots, \mu_m$ and an integer $1 \le k < m$ such that*

– *$A_{i,j} = 0$ for all $i, j \in [k]$; $A_{i,j} = 0$ for all $i, j \in [k+1 : m]$; and*

– *$A_{i,j}/(\mu_i\mu_j) = A_{j,i}/(\mu_i\mu_j)$ is a root of unity for all $i \in [k]$ and $j \in [k+1 : m]$.*

In other words, there exists a $k \times (m-k)$ matrix $\mathbf{B}$ of the form

$$\mathbf{B} = \begin{pmatrix} \mu_1 & & & \\ & \mu_2 & & \\ & & \ddots & \\ & & & \mu_k \end{pmatrix} \begin{pmatrix} \zeta_{1,1} & \zeta_{1,2} & \cdots & \zeta_{1,m-k} \\ \zeta_{2,1} & \zeta_{2,2} & \cdots & \zeta_{2,m-k} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_{k,1} & \zeta_{k,2} & \cdots & \zeta_{k,m-k} \end{pmatrix} \begin{pmatrix} \mu_{k+1} & & & \\ & \mu_{k+2} & & \\ & & \ddots & \\ & & & \mu_m \end{pmatrix},$$

where every $\mu_i > 0$ and every $\zeta_{i,j}$ is a root of unity, and $\mathbf{A}$ is the bipartisation of $\mathbf{B}$.

Theorem 5.1. *Let $\mathbf{A} \in \mathbb{C}^{m\times m}$ be a symmetric, connected and bipartite matrix, for some $m > 1$, then either $\mathsf{EVAL}(\mathbf{A})$ is #P-hard or there exists an $m \times m$ purified bipartite matrix $\mathbf{A}'$ such that*

$$\mathsf{EVAL}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{A}').$$

(By Definition 5.1, $\mathbf{A}'$ is symmetric and thus, $\mathsf{EVAL}(\mathbf{A}')$ is well defined.)

5.2 Step 2: Reduction to Discrete Unitary Matrix

Now let $\mathbf{A} \in \mathbb{C}^{m\times m}$ denote a purified bipartite matrix. We prove that $\mathsf{EVAL}(\mathbf{A})$ is either #P-hard or polynomial-time equivalent to $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ for some $\mathbf{C}$ and $\mathfrak{D}$, where the matrix $\mathbf{C}$ is the bipartisation of a discrete unitary matrix, which is to be defined in the next definition.

Definition 5.2. *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 $F_{i,j}$ of $\mathbf{F}$ is a root of unity, and $M = \text{lcm}\big\{\text{the order of } F_{i,j} : i, j \in [m]\big\}$;*

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

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

Some simplest examples of discrete unitary matrices are as follows:

$$\mathbf{H_2} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \ \mathbf{H_4} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, \ \boldsymbol{\mathcal{F}}_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \eta & \eta^2 \\ 1 & \eta^2 & \eta \end{pmatrix}, \ \boldsymbol{\mathcal{F}}_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \zeta & \zeta^{-1} & \zeta^2 & \zeta^{-2} \\ 1 & \zeta^2 & \zeta^{-2} & \zeta^{-1} & \zeta \\ 1 & \zeta^{-1} & \zeta & \zeta^{-2} & \zeta^2 \\ 1 & \zeta^{-2} & \zeta^2 & \zeta & \zeta^{-1} \end{pmatrix},$$

where $\eta = e^{2\pi i/3} = \omega_3$ is a third root of unity, and $\zeta = e^{2\pi i/5} = \omega_5$ is a fifth root of unity. Note that the tensor product of any two discrete unitary matrices is also a discrete unitary matrix.

Theorem 5.2. *Let $\mathbf{A} \in \mathbb{C}^{m\times m}$ be a purified bipartite matrix. Then either* 1). $\mathsf{EVAL}(\mathbf{A})$ *is tractable; or* 2). $\mathsf{EVAL}(\mathbf{A})$ *is #P-hard; or* 3). *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 conditions $(\mathcal{U}_1)$-$(\mathcal{U}_4)$:*

$(\mathcal{U}_1)$ *M and N are positive integers that satisfy $2\,|\,N$ and $M\,|\,N$. $\mathbf{C} \in \mathbb{C}^{2n\times 2n}$ for some $n \ge 1$, and*

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

is a sequence of N $2n \times 2n$ diagonal matrices over $\mathbb{C}$;

$(\mathcal{U}_2)$ *$\mathbf{C}$ is the bipartisation of an M-*discrete unitary matrix *$\mathbf{F} \in \mathbb{C}^{n\times n}$. (Note that matrices $\mathbf{C}$ and $\mathbf{F}$ uniquely determine each other);*

$(\mathcal{U}_3)$ *For all $i \in [2n]$, $D^{[0]}_i = 1$. For all $r \in [N-1]$, we have*

$$\exists i \in [n],\ D^{[r]}_i \neq 0 \implies \exists i' \in [n],\ D^{[r]}_{i'} = 1, \qquad \textit{and}$$
$$\exists i \in [n+1:2n],\ D^{[r]}_i \neq 0 \implies \exists i' \in [n+1:2n],\ D^{[r]}_{i'} = 1;$$

$(\mathcal{U}_4)$ *For all $r \in [N-1]$ and all $i \in [2n]$, $D^{[r]}_i \in \mathbb{Q}(\omega_N)$ and $\big|D^{[r]}_i\big| \in \{0,1\}$.*

5.3 Step 3: Canonical Form of C, F and $\mathfrak{D}$

After the first two steps, the original problem $\mathsf{EVAL}(\mathbf{A})$ is shown to be either tractable; or #P-hard; or polynomial-time equivalent to a new problem $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$. We also know there exist positive integers M and N such that $((M,N),\mathbf{C},\mathfrak{D})$ satisfies conditions $(\mathcal{U}_1)$-$(\mathcal{U}_4)$.

For convenience, we still use $2m$ to denote the number of rows of $\mathbf{C}$ and $\mathbf{D}^{[r]}$, though it should be noted that this new m is indeed the n in Theorem 5.2, which is different from the m used in the first two steps. We also denote the upper-right $m \times m$ block of $\mathbf{C}$ by $\mathbf{F}$.

In this step, we adopt the following convention: Given an $n \times n$ matrix, we use $[0:n-1]$, instead of $[n]$, to index its rows and columns. For example, we index the rows of $\mathbf{F}$ using $[0:m-1]$ and index the rows of $\mathbf{C}$ using $[0:2m-1]$.

We start with the special case when $M = 1$. Because $\mathbf{F}$ is M-discrete unitary, we must have $m = 1$. In this case, it is easy to check that $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ is tractable: $\mathbf{C}$ is a 2 by 2 matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};$$

$Z_{\mathbf{C},\mathfrak{D}}(G)$ is 0 unless G is bipartite; For connected and bipartite G, there are at most two assignments $\xi : V \to \{0,1\}$ which could yield non-zero values; Finally, for graph G with connected components G_i, $Z_{\mathbf{C},\mathfrak{D}}(G)$ is the product of $Z_{\mathbf{C},\mathfrak{D}}(G_i)$'s.

For the general case when parameter $M > 1$, we further study the structures of matrix $\mathbf{F}$ and the diagonal matrices in $\mathfrak{D}$, and derive several necessary conditions on them for the problem $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ to be *not #P-hard*. In the tractability part, we prove that these conditions are actually sufficient for it being polynomial-time computable.

5.3.1 Step 3.1: Entries of $\mathbf{D}^{[r]}$ are either 0 or Powers of ω_N

Suppose $((M,N),\mathbf{C},\mathfrak{D})$ satisfies conditions $(\mathcal{U}_1)$-$(\mathcal{U}_4)$ and $M > 1$. In the first step, we show that either $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ is #P-hard or every entry of $\mathbf{D}^{[r]}$ (in $\mathfrak{D}$), $r \in [N-1]$, is either 0 or a power of ω_N.

Theorem 5.3. *Suppose $((M,N),\mathbf{C},\mathfrak{D})$ satisfies $(\mathcal{U}_1)$-$(\mathcal{U}_4)$ and integer $M > 1$, then either the problem $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ is #P-hard or $((M,N),\mathbf{C},\mathfrak{D})$ satisfies the following additional condition $(\mathcal{U}_5)$:*

$(\mathcal{U}_5)$ *For all $r \in [N-1]$ and $i \in [0:2m-1]$, $D_i^{[r]}$ is either 0 or a power of ω_N.*

5.3.2 Step 3.2: Fourier Decomposition

Second, we show that either problem $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ is #P-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*, to be defined in the next definition.

Definition 5.3. *Let $q > 1$ be a prime power, and $k \ge 1$ be an integer such that $\gcd(k,q) = 1$. We call the following $q \times q$ matrix $\boldsymbol{\mathcal{F}}_{q,k}$ a (q,k)-*Fourier matrix*: The $(x,y)^{th}$ entry, where $x,y \in [0:q-1]$, is*

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

In particular, when $k = 1$, we use $\boldsymbol{\mathcal{F}}_q$ to denote $\boldsymbol{\mathcal{F}}_{q,1}$ for short.

Theorem 5.4. *Suppose $((M,N),\mathbf{C},\mathfrak{D})$ satisfies conditions $(\mathcal{U}_1)$-$(\mathcal{U}_5)$, and integer $M > 1$. 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 $q_1, q_2, \ldots, q_d$ of d prime powers, for some $d \ge 1$,*

such that

$$\mathbf{F}_{\Sigma,\Pi} = \bigotimes_{i\in[d]} \boldsymbol{\mathcal{F}}_{q_i}. \tag{4}$$

Suppose there do exist permutations Σ, Π and prime powers $q_1, \ldots, q_d$ such that $\mathbf{F}_{\Sigma,\Pi}$ satisfies (4), 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 r^{th} matrix is

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

It is clear that permuting the rows and columns of matrices $\mathbf{C}$ and every $\mathbf{D}^{[r]}$ by the same permutation pair (Σ, Π) does not affect the complexity of $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$, so $\mathsf{EVAL}(\mathbf{C}_{\Sigma,\Pi}, \mathfrak{D}_{\Sigma,\Pi}) \equiv \mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$. From now on, we let $\mathbf{F}$, $\mathbf{C}$ and $\mathfrak{D}$ denote $\mathbf{F}_{\Sigma,\Pi}$, $\mathbf{C}_{\Sigma,\Pi}$ and $\mathfrak{D}_{\Sigma,\Pi}$, respectively. By (4), the new $\mathbf{F}$ satisfies

$$\mathbf{F} = \bigotimes_{i \in [d]} \boldsymbol{\mathcal{F}}_{q_i}. \tag{5}$$

Before moving forward, we rearrange the prime powers $q_1, q_2, \ldots, q_d$ and divide them into groups according to different primes. We need the following notation.

Let $\mathbf{p} = (p_1, \ldots, p_s)$ be a sequence of primes such that $p_1 < p_2 < \ldots < p_s$ and $\mathbf{t} = (t_1, \ldots, t_s)$ be a sequence of positive integers. Let $\mathcal{Q} = \{\mathbf{q}_i \mid i \in [s]\}$ be a collection of s sequences in which each $\mathbf{q}_i$ is a sequence $(q_{i,1}, \ldots, q_{i,t_i})$ of powers of p_i such that $q_{i,1} \geq \ldots \geq q_{i,t_i}$. We let q_i denote $q_{i,1}$ for all $i \in [s]$,

$$\mathbb{Z}_{\mathbf{q}_i} \equiv \prod_{j \in [t_i]} \mathbb{Z}_{q_{i,j}} = \mathbb{Z}_{q_{i,1}} \times \cdots \times \mathbb{Z}_{q_{i,t_i}}, \quad \text{for all } i \in [s],$$

and

$$\begin{aligned}\mathbb{Z}_{\mathcal{Q}} \equiv \prod_{i \in [s], j \in [t_i]} \mathbb{Z}_{q_{i,j}} \equiv \prod_{i \in [s]} \mathbb{Z}_{\mathbf{q}_i} \quad \equiv \quad & \mathbb{Z}_{q_{1,1}} \times \cdots \times \mathbb{Z}_{q_{1,t_1}} \times \\ & \mathbb{Z}_{q_{2,1}} \times \cdots \times \mathbb{Z}_{q_{2,t_2}} \times \\ & \qquad \vdots \\ & \mathbb{Z}_{q_{s,1}} \times \cdots \times \mathbb{Z}_{q_{s,t_s}}\end{aligned}$$

be the Cartesian products of the respective finite Abelian groups. Both $\mathbb{Z}_{\mathcal{Q}}$ and $\mathbb{Z}_{\mathbf{q}_i}$ are finite Abelian groups, under component-wise operations. This implies that both $\mathbb{Z}_{\mathcal{Q}}$ and $\mathbb{Z}_{\mathbf{q}_i}$ are $\mathbb{Z}$-modules and thus $k\mathbf{x}$ is well defined for all $k \in \mathbb{Z}$ and $\mathbf{x}$ in $\mathbb{Z}_{\mathcal{Q}}$ or $\mathbb{Z}_{\mathbf{q}_i}$. As $\mathbb{Z}$-modules, we can also refer to their members as "vectors". When we use $\mathbf{x}$ to denote a vector in $\mathbb{Z}_{\mathcal{Q}}$, we denote its $(i,j)^{th}$ entry by $x_{i,j} \in \mathbb{Z}_{q_{i,j}}$. We also use $\mathbf{x}_i$ to denote $(x_{i,j} : j \in [t_i]) \in \mathbb{Z}_{\mathbf{q}_i}$, so $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_s)$. Given $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_{\mathcal{Q}}$, we let $\mathbf{x} \pm \mathbf{y}$ denote the vector in $\mathbb{Z}_{\mathcal{Q}}$ whose $(i,j)^{th}$ entry is $x_{i,j} \pm y_{i,j} \pmod{q_{i,j}}$. Similarly, for each $i \in [s]$, we can define $\mathbf{x} \pm \mathbf{y}$ for vectors $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_{\mathbf{q}_i}$.

By (5), there exist $\mathbf{p}, \mathbf{t}, \mathcal{Q}$ such that $((M,N), \mathbf{C}, \mathfrak{D}, (\mathbf{p}, \mathbf{t}, \mathcal{Q}))$ satisfies the following condition $(\mathcal{R})$:

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

($\mathcal{R}_2$) $\mathbf{C} \in \mathbb{C}^{2m \times 2m}$ is the bipartisation of $\mathbf{F} \in \mathbb{C}^{m \times m}$, and $((M,N), \mathbf{C}, \mathfrak{D})$ satisfies $(\mathcal{U}_1)$-$(\mathcal{U}_5)$;

($\mathcal{R}_3$) There is a bijection ρ from $[0 : m-1]$ to $\mathbb{Z}_{\mathcal{Q}}$ (so $m = \prod_{i \in [s], j \in [t_i]} q_{i,j}$) such that

$$F_{a,b} = \prod_{i \in [s], j \in [t_i]} \omega_{q_{i,j}}^{x_{i,j} y_{i,j}}, \quad \text{for all } a, b \in [0 : m-1], \tag{6}$$

where $(x_{i,j} : i \in [s], j \in [t_i]) = \mathbf{x} = \rho(a)$ and $(y_{i,j} : i \in [s], j \in [t_i]) = \mathbf{y} = \rho(b)$. Note that (6) above also gives us an expression of M using $\mathcal{Q}$. It is the product of the largest prime powers $q_i = q_{i,1}$ for each distinct prime p_i: $M = \prod_{i \in [s]} q_i$.

For convenience, we will from now on directly use $\mathbf{x} \in \mathbb{Z}_{\mathcal{Q}}$ to index the rows and columns of $\mathbf{F}$:

$$F_{\mathbf{x},\mathbf{y}} \equiv F_{\rho^{-1}(\mathbf{x}), \rho^{-1}(\mathbf{y})} = \prod_{i \in [s], j \in [t_i]} \omega_{q_{i,j}}^{x_{i,j} y_{i,j}}, \quad \text{for all } \mathbf{x}, \mathbf{y} \in \mathbb{Z}_{\mathcal{Q}}, \tag{7}$$

whenever we have a tuple $((M,N),\mathbf{C},\mathfrak{D},(\mathbf{p},\mathbf{t},\mathcal{Q}))$ which is known to satisfy condition $(\mathcal{R})$. We assume that $\mathbf{F}$ is indexed by $(\mathbf{x},\mathbf{y})\in\mathbb{Z}_{\mathcal{Q}}\times\mathbb{Z}_{\mathcal{Q}}$ rather than $(a,b)\in[0:m-1]\times[0:m-1]$, and $(\mathcal{R}_3)$ refers to (7). Correspondingly, to index the entries of matrices $\mathbf{C}$ and $\mathbf{D}^{[r]}$, we use $\{0,1\}\times\mathbb{Z}_{\mathcal{Q}}$: $(0,\mathbf{x})$ refers to the $\rho^{-1}(\mathbf{x})^{th}$ row (or column), and $(1,\mathbf{x})$ refers to the $(m+\rho^{-1}(\mathbf{x}))^{th}$ row (or column).

5.3.3 Step 3.3: Affine Support for $\mathfrak{D}$

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

For every $r\in[N-1]$, we define $\Lambda_r\subseteq\mathbb{Z}_{\mathcal{Q}}$ and $\Delta_r\subseteq\mathbb{Z}_{\mathcal{Q}}$ as

$$\Lambda_r=\big\{\mathbf{x}\in\mathbb{Z}_{\mathcal{Q}}\,\big|\,D^{[r]}_{(0,\mathbf{x})}\neq 0\big\}\quad\text{and}\quad\Delta_r=\big\{\mathbf{x}\in\mathbb{Z}_{\mathcal{Q}}\,\big|\,D^{[r]}_{(1,\mathbf{x})}\neq 0\big\}.$$

We let $\mathcal{S}$ denote the set of $r\in[N-1]$ such that $\Lambda_r\neq\emptyset$ and $\mathcal{T}$ denote the set of $r\in[N-1]$ such that $\Delta_r\neq\emptyset$. We recall the following standard definition of a coset of a group, specialized to our situation.

Definition 5.4. *Let Φ be a nonempty subset of $\mathbb{Z}_{\mathcal{Q}}$ (or $\mathbb{Z}_{\mathbf{q}_i}$ for some $i\in[s]$). We say Φ is a* coset *in $\mathbb{Z}_{\mathcal{Q}}$ (or $\mathbb{Z}_{\mathbf{q}_i}$) if there exists a vector $\mathbf{x}_0\in\Phi$ such that $\{\mathbf{x}-\mathbf{x}_0\,|\,\mathbf{x}\in\Phi\}$ is a subgroup of $\mathbb{Z}_{\mathcal{Q}}$ (or $\mathbb{Z}_{\mathbf{q}_i}$).*

Given a coset Φ (in $\mathbb{Z}_{\mathcal{Q}}$ or $\mathbb{Z}_{\mathbf{q}_i}$), we let Φ^{lin} denote its corresponding subgroup $\{\mathbf{x}-\mathbf{x}'\,|\,\mathbf{x},\mathbf{x}'\in\Phi\}$. Being a subgroup, clearly $\Phi^{\text{lin}}=\{\mathbf{x}-\mathbf{x}'\,|\,\mathbf{x},\mathbf{x}'\in\Phi\}=\{\mathbf{x}-\mathbf{x}_0\,|\,\mathbf{x}\in\Phi\}$, for any $\mathbf{x}_0\in\Phi$.

Theorem 5.5. *Let $((M,N),\mathbf{C},\mathfrak{D},(\mathbf{p},\mathbf{t},\mathcal{Q}))$ be a 4-tuple that satisfies $(\mathcal{R})$. Then either $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ is #P-hard or sets $\Lambda_r\subseteq\mathbb{Z}_{\mathcal{Q}}$ and $\Delta_r\subseteq\mathbb{Z}_{\mathcal{Q}}$ 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 $r\in\mathcal{T}$, $\Delta_r=\prod_{i=1}^s\Delta_{r,i}$, where for every $i\in[s]$, $\Delta_{r,i}$ is a coset in $\mathbb{Z}_{\mathbf{q}_i}$.*

Suppose $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ is not #P-hard, then by Theorem 5.5, tuple $((M,N),\mathbf{C},\mathfrak{D},(\mathbf{p},\mathbf{t},\mathcal{Q}))$ satisfies not only condition $(\mathcal{R})$ but also condition $(\mathcal{L})$. Actually, by condition $(\mathcal{U}_3)$, $\mathfrak{D}$ satisfies the following additional property:

$(\mathcal{L}_3)$ For every $r\in\mathcal{S}$, $\exists\,\mathfrak{a}^{[r]}\in\Lambda_r$ such that $D^{[r]}_{(0,\mathfrak{a}^{[r]})}=1$; for every $r\in\mathcal{T}$, $\exists\,\mathfrak{b}^{[r]}\in\Delta_r$, $D^{[r]}_{(1,\mathfrak{b}^{[r]})}=1$.

From now on, when we say condition $(\mathcal{L})$, we mean all three conditions $(\mathcal{L}_1)$-$(\mathcal{L}_3)$.

5.3.4 Step 3.4: Quadratic Structure

In this final step within Step 3, we prove that, for every $r\in[N-1]$, the nonzero entries of $\mathbf{D}^{[r]}$ must have a quadratic structure, otherwise $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ is #P-hard.

Given a vector $\mathbf{x}$ in $\mathbb{Z}_{\mathbf{q}_i}$ for some $i\in[s]$, we use $\mathbf{ext}_r(\mathbf{x})$, where $r\in\mathcal{S}$, to denote the vector $\mathbf{x}'\in\mathbb{Z}_{\mathcal{Q}}$ such that in the expression $\mathbf{x}'=(\mathbf{x}'_1,\ldots,\mathbf{x}'_s)\in\mathbb{Z}_{\mathcal{Q}}=\prod_{i\in[s]}\mathbb{Z}_{\mathbf{q}_i}$, its i^{th} component $\mathbf{x}'_i=\mathbf{x}$, the vector given in $\mathbb{Z}_{\mathbf{q}_i}$, and

$$\mathbf{x}'_j=\mathfrak{a}^{[r]}_j,\quad\text{for all } j\neq i.$$

Recall that $\mathfrak{a}^{[r]}$ is a vector we picked from Λ_r in condition $(\mathcal{L}_3)$. Similarly we let $\mathbf{ext}'_r(\mathbf{x})$, where $r\in\mathcal{T}$, denote the vector $\mathbf{x}'\in\mathbb{Z}_{\mathcal{Q}}$ such that $\mathbf{x}'_i=\mathbf{x}$ and

$$\mathbf{x}'_j=\mathfrak{b}^{[r]}_j,\quad\text{for all } j\neq i.$$

Let $\mathbf{a}$ be a vector in $\mathbb{Z}_{\mathbf{q}_i}$ for some $i \in [s]$, then we use $\widetilde{\mathbf{a}}$ to denote the vector $\mathbf{b} \in \mathbb{Z}_{\mathcal{Q}}$ such that $\mathbf{b}_i = \mathbf{a}$ and $\mathbf{b}_j = \mathbf{0}$ for all other $j \neq i$. Also recall that we use q_k, where $k \in [s]$, to denote $q_{k,1}$.

Theorem 5.6. *Let $((M,N), \mathbf{C}, \mathfrak{D}, (\mathbf{p}, \mathbf{t}, \mathcal{Q}))$ be a tuple that satisfies both $(\mathcal{R})$ and $(\mathcal{L})$ (including $(\mathcal{L}_3)$), then either* $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ *is #P-hard or $\mathfrak{D}$ satisfies the following condition $(\mathcal{D})$:*

$(\mathcal{D}_1)$ *For every $r \in \mathcal{S}$, we have*

$$D^{[r]}_{(0,\mathbf{x})} = D^{[r]}_{(0,\mathbf{ext}_r(\mathbf{x}_1))} D^{[r]}_{(0,\mathbf{ext}_r(\mathbf{x}_2))} \cdots D^{[r]}_{(0,\mathbf{ext}_r(\mathbf{x}_s))}, \quad \textit{for all } \mathbf{x} \in \Lambda_r. \tag{8}$$

$(\mathcal{D}_2)$ *For every $r \in \mathcal{T}$, we have*

$$D^{[r]}_{(1,\mathbf{x})} = D^{[r]}_{(1,\mathbf{ext}'_r(\mathbf{x}_1))} D^{[r]}_{(1,\mathbf{ext}'_r(\mathbf{x}_2))} \cdots D^{[r]}_{(1,\mathbf{ext}'_r(\mathbf{x}_s))}, \quad \textit{for all } \mathbf{x} \in \Delta_r. \tag{9}$$

$(\mathcal{D}_3)$ *For all $r \in \mathcal{S}$, $k \in [s]$ and $\mathbf{a} \in \Lambda^{\text{lin}}_{r,k} \subseteq \mathbb{Z}_{\mathbf{q}_k}$, there exist $\mathbf{b} \in \mathbb{Z}_{\mathbf{q}_k}$ and $\alpha \in \mathbb{Z}_N$ such that*

$$\omega_N^{\alpha} \cdot F_{\mathbf{x},\widetilde{\mathbf{b}}} = D^{[r]}_{(0,\mathbf{x}+\widetilde{\mathbf{a}})} \cdot \overline{D^{[r]}_{(0,\mathbf{x})}}, \quad \textit{for all } \mathbf{x} \in \Lambda_r; \tag{10}$$

$(\mathcal{D}_4)$ *For all $r \in \mathcal{T}$, $k \in [s]$ and $\mathbf{a} \in \Delta^{\text{lin}}_{r,k} \subseteq \mathbb{Z}_{\mathbf{q}_k}$, there exist $\mathbf{b} \in \mathbb{Z}_{\mathbf{q}_k}$ and $\alpha \in \mathbb{Z}_N$ such that*

$$\omega_N^{\alpha} \cdot F_{\widetilde{\mathbf{b}},\mathbf{x}} = D^{[r]}_{(1,\mathbf{x}+\widetilde{\mathbf{a}})} \cdot \overline{D^{[r]}_{(1,\mathbf{x})}}, \quad \textit{for all } \mathbf{x} \in \Delta_r; \tag{11}$$

Note that in $(\mathcal{D}_3)$ and $(\mathcal{D}_4)$, the expressions on the left-hand-side do not depend on all other components of $\mathbf{x}$ except the k^{th} component $\mathbf{x}_k$, because all other components of $\widetilde{\mathbf{b}}$ are $\mathbf{0}$.

The statements in conditions $(\mathcal{D}_3)$-$(\mathcal{D}_4)$ are a technically precise way to express the idea that there is a quadratic structure on the support of each matrix $\mathbf{D}^{[r]}$. We express it in terms of an exponential difference equation.

5.4 Tractability

Theorem 5.7. *Let $((M,N), \mathbf{C}, \mathfrak{D}, (\mathbf{p}, \mathbf{t}, \mathcal{Q}))$ be a 4-tuple that satisfies all three conditions $(\mathcal{R}), (\mathcal{L})$ and $(\mathcal{D})$, then problem* $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ *can be solved in polynomial time.*

6 Proof Outline of the Case: A is not Bipartite

The definitions and theorems of the case when matrix $\mathbf{A}$ is not bipartite are similar to, but also have significant differences with, those of the bipartite case. We will list these theorems.

6.1 Step 1: Purification of Matrix A

We start with $\mathsf{EVAL}(\mathbf{A})$, in which $\mathbf{A} \in \mathbb{C}^{m \times m}$ is symmetric, connected and non-bipartite. It is easy to see that if $m = 1$, then $\mathsf{EVAL}(\mathbf{A})$ is tractable. So in the discussion below, we assume $m > 1$.

Definition 6.1. *Let $\mathbf{A} \in \mathbb{C}^{m \times m}$ be a symmetric, connected, and non-bipartite matrix. We say $\mathbf{A}$ is a* purified non-bipartite matrix *if there exist positive rational numbers $\mu_1, \ldots, \mu_m$ such that $A_{i,j}/(\mu_i \mu_j)$ is a root of unity for all $i, j \in [m]$.*

In other words, $\mathbf{A}$ has the form

$$\mathbf{A} = \begin{pmatrix} \mu_1 & & & \\ & \mu_2 & & \\ & & \ddots & \\ & & & \mu_m \end{pmatrix} \begin{pmatrix} \zeta_{1,1} & \zeta_{1,2} & \cdots & \zeta_{1,m} \\ \zeta_{2,1} & \zeta_{2,2} & \cdots & \zeta_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_{m,1} & \zeta_{m,2} & \cdots & \zeta_{m,m} \end{pmatrix} \begin{pmatrix} \mu_1 & & & \\ & \mu_2 & & \\ & & \ddots & \\ & & & \mu_m \end{pmatrix},$$

where $\zeta_{i,j} = \zeta_{j,i}$ are all roots of unity. We prove the following theorem:

Theorem 6.1. *Let $\mathbf{A} \in \mathbb{C}^{m\times m}$ be a symmetric, connected, and non-bipartite matrix, for some $m > 1$. Then either $\mathsf{EVAL}(\mathbf{A})$ is #P-hard or there exists a purified non-bipartite matrix $\mathbf{A}' \in \mathbb{C}^{m\times m}$ such that*

$$\mathsf{EVAL}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{A}').$$

6.2 Step 2: Reduction to Discrete Unitary Matrix

In this step, we prove the following theorem:

Theorem 6.2. *Let $\mathbf{A} \in \mathbb{C}^{m\times m}$ be a purified non-bipartite matrix. Then either* 1). $\mathsf{EVAL}(\mathbf{A})$ *is tractable; or* 2). $\mathsf{EVAL}(\mathbf{A})$ *is #P-hard; or* 3). *there exists a triple $((M,N),\mathbf{F},\mathfrak{D})$ such that*

$$\mathsf{EVAL}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{F},\mathfrak{D})$$

and $((M,N),\mathbf{F},\mathfrak{D})$ satisfies the following conditions $(\mathcal{U}_1')$-$(\mathcal{U}_4')$:

- $(\mathcal{U}_1')$ *M and N are positive integers that satisfy $2|N$ and $M|N$. $\mathbf{F}$ is an $n\times n$ complex matrix for some $n \ge 1$, and $\mathfrak{D} = \{\mathbf{D}^{[0]},\ldots,\mathbf{D}^{[N-1]}\}$ is a sequence of N $n\times n$ diagonal matrices;*
- $(\mathcal{U}_2')$ *$\mathbf{F}$ is a symmetric M-discrete unitary matrix;*
- $(\mathcal{U}_3')$ *For all $i \in [n]$, $D_i^{[0]} = 1$. For all $r \in [N-1]$, we have $\mathbf{D}^{[r]} \neq \mathbf{0} \implies \exists\, i \in [n]$, $D_i^{[r]} = 1$;*
- $(\mathcal{U}_4')$ *For all $r \in [N-1]$ and all $i \in [n]$, $D_i^{[r]} \in \mathbb{Q}(\omega_N)$ and $\left|D_i^{[r]}\right| \in \{0,1\}$.*

6.3 Step 3: Canonical Form of F and $\mathfrak{D}$

Now suppose we have a tuple $((M,N),\mathbf{F},\mathfrak{D})$ that satisfies $(\mathcal{U}_1')$-$(\mathcal{U}_4')$. For convenience we still use m to denote the number of rows and columns of $\mathbf{F}$ and each $\mathbf{D}^{[r]}$ in $\mathfrak{D}$, though it should be noted that this new m is indeed the n in Theorem 6.2, which is different from the m used in the first two steps.

As in the bipartite case, we adopt the following convention in this section: Given any $n\times n$ matrix, we use $[0:n-1]$, instead of $[n]$, to index its rows and columns.

We start with the special case when $M = 1$. Since $\mathbf{F}$ is M-discrete unitary, we must have $m = 1$ and $\mathbf{F} = (1)$. In this case, the problem $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ is clearly tractable. So in the rest of this section, we always assume $M > 1$.

6.3.1 Step 3.1: Entries of $\mathbf{D}^{[r]}$ are either 0 or Powers of ω_N

Theorem 6.3. *Suppose $((M,N),\mathbf{F},\mathfrak{D})$ satisfies $(\mathcal{U}_1')$-$(\mathcal{U}_4')$ and integer $M > 1$. Then either $\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$ is #P-hard or $((M,N),\mathbf{F},\mathfrak{D})$ satisfies the following additional condition $(\mathcal{U}_5')$:*

- $(\mathcal{U}_5')$ *For all $r \in [N-1]$ and $i \in [0:m-1]$, $D_i^{[r]}$ is either zero or a power of ω_N.*

6.3.2 Step 3.2: Fourier Decomposition

Let q be a prime power. We say $\mathbf{W}$ is a *non-degenerate* matrix in $\mathbb{Z}_q^{2\times 2}$ if $\mathbf{W}\mathbf{x} \neq \mathbf{0}$ for all $\mathbf{x} \neq \mathbf{0} \in \mathbb{Z}_q^2$. The following lemma gives some equivalent characterizations of $\mathbf{W}$ being non-degenerate. The proof is elementary, so we omit it here.

Lemma 6.1. *Let q be a prime power and $\mathbf{W} \in \mathbb{Z}_q^{2\times 2}$. Then the following statements are equivalent:*

1. $\mathbf{W}$ *is non-degenerate;*
2. $\mathbf{x} \mapsto \mathbf{W}\mathbf{x}$ *is a bijection from $\mathbb{Z}_q^2$ to $\mathbb{Z}_q^2$; and*
3. $\det(\mathbf{W})$ *is invertible in $\mathbb{Z}_q$.*

Definition 6.2 (Generalized Fourier Matrix)**.** *Let q be a prime power and $\mathbf{W} = (W_{ij})$ be a symmetric non-degenerate matrix in $\mathbb{Z}_q^{2\times 2}$. $\boldsymbol{\mathcal{F}}_{q,\mathbf{W}}$ is called a* $(q,\mathbf{W})$-generalized Fourier matrix*, if it is a $q^2 \times q^2$ matrix and there is a one-to-one correspondence ρ from $[0:q^2-1]$ to $[0:q-1]^2$, such that*

$$(\boldsymbol{\mathcal{F}}_{q,\mathbf{W}})_{i,j} = \omega_q^{W_{11}x_1y_1+W_{12}x_1y_2+W_{21}x_2y_1+W_{22}x_2y_2}, \quad \textit{for all } i,j \in [0:q^2-1],$$

where $\mathbf{x} = (x_1,x_2) = \rho(i)$ and $\mathbf{y} = (y_1,y_2) = \rho(j)$.

Theorem 6.4. *Suppose $((M,N),\mathbf{F},\mathfrak{D})$ satisfies $(\mathcal{U}_1')$-$(\mathcal{U}_5')$, then either $\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$ is #P-hard or there exist a permutation Σ from $[0:m-1]$ to $[0:m-1]$ and*

1. *two sequences $\mathbf{d} = (d_1,\ldots,d_g)$ and $\mathcal{W} = (\mathbf{W}^{[1]},\ldots,\mathbf{W}^{[g]})$, for some non-negative g (Note that the g here could be 0, in which case both $\mathbf{d}$ and $\mathcal{W}$ are empty): For every $i \in [g]$, $d_i > 1$ is a power of 2, and $\mathbf{W}^{[i]}$ is a 2×2 symmetric non-degenerate matrix over $\mathbb{Z}_{d_i}$; and*
2. *two sequences $\mathbf{q} = (q_1,\ldots,q_\ell)$ and $\mathbf{k} = (k_1,\ldots,k_\ell)$ (Again ℓ could be 0, in which case both $\mathbf{q}$ and $\mathbf{k}$ are empty), in which for every $i \in [\ell]$, q_i is a prime power, $k_i \in \mathbb{Z}_{q_i}$, and $\gcd(q_i,k_i) = 1$,*

such that

$$\mathbf{F}_{\Sigma,\Sigma} = \left(\bigotimes_{i=1}^{g} \boldsymbol{\mathcal{F}}_{d_i,\mathbf{W}^{[i]}}\right) \bigotimes \left(\bigotimes_{i=1}^{\ell} \boldsymbol{\mathcal{F}}_{q_i,k_i}\right).$$

Suppose there does exist a permutation Σ (together with $\mathbf{d},\mathcal{W},\mathbf{q}$, and $\mathbf{k}$) such that $\mathbf{F}_{\Sigma,\Sigma}$ satisfies the equation above (otherwise, $\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$ is #P-hard). Then we apply Σ to $\mathbf{D}^{[r]}$, $r \in [0:N-1]$, to get a new sequence $\mathfrak{D}_\Sigma$ of N diagonal matrices in which the r^{th} matrix is

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

It is clear that permuting the rows and columns of $\mathbf{F}$ and $\mathbf{D}^{[r]}$ in $\mathfrak{D}$ by the same permutation Σ does not affect the complexity of $\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$, so $\mathsf{EVAL}(\mathbf{F}_{\Sigma,\Sigma},\mathfrak{D}_\Sigma) \equiv \mathsf{EVAL}(\mathbf{F},\mathfrak{D})$. From now on, we simply let $\mathbf{F}$ and $\mathfrak{D}$ denote $\mathbf{F}_{\Sigma,\Sigma}$ and $\mathfrak{D}_\Sigma$, respectively. Thus we have

$$\mathbf{F} = \left(\bigotimes_{i=1}^{g} \boldsymbol{\mathcal{F}}_{d_i,\mathbf{W}^{[i]}}\right) \bigotimes \left(\bigotimes_{i=1}^{\ell} \boldsymbol{\mathcal{F}}_{q_i,k_i}\right). \tag{12}$$

Before moving forward to Step 3.3, we rearrange the prime powers in $\mathbf{d}$ and $\mathbf{q}$ and divide them into groups according to different primes.

By (12), there exist $\mathbf{d}$, $\mathcal{W}$, $\mathbf{p}$, $\mathbf{t}$, $\mathcal{Q}$ and $\mathcal{K}$ such that tuple $((M,N),\mathbf{F},\mathfrak{D},(\mathbf{d},\mathcal{W},\mathbf{p},\mathbf{t},\mathcal{Q},\mathcal{K}))$ satisfies the following condition $(\mathcal{R}')$:

$(\mathcal{R}_1')$ $\mathbf{d}=(d_1,\ldots,d_g)$ is a sequence of powers of 2 for some non-negative integer g, such that if $g>0$, then $d_1\ge\ldots\ge d_g$; $\mathcal{W}=(\mathbf{W}^{[1]},\ldots,\mathbf{W}^{[g]})$ is a sequence of matrices. Every $\mathbf{W}^{[i]}$ is a symmetric non-degenerate 2×2 matrix over $\mathbb{Z}_{d_i}$ (Note that $\mathbf{d}$ and $\mathcal{W}$ could be empty);

$\mathbf{p}=(p_1,\ldots,p_s)$ is a sequence of s primes, for some $s\ge 1$, such that $2=p_1<\ldots<p_s$; $\mathbf{t}=(t_1,\ldots,t_s)$ is a sequence of integers: $t_1\ge 0$ and $t_i\ge 1$ for all $i>1$; $\mathcal{Q}=\{\mathbf{q}_i\,|\,i\in[s]\}$ is a collection of sequences in which $\mathbf{q}_i=(q_{i,1},\ldots,q_{i,t_i})$ is a sequence of powers of p_i such that $q_{i,1}\ge\ldots\ge q_{i,t_i}$ (Only $\mathbf{q}_1$ could be empty. We always fix p_1 to be 2 even when no powers of 2 occur in $\mathcal{Q}$);

$\mathcal{K}=\{\mathbf{k}_i\,|\,i\in[s]\}$ is a collection of s sequences in which each $\mathbf{k}_i=(k_{i,1},\ldots,k_{i,t_i})$ is a sequence of length t_i. For all $i\in[s]$ and $j\in[t_i]$, $k_{i,j}\in[0:q_{i,j}-1]$ and $\gcd(k_{i,j},q_{i,j})=\gcd(k_{i,j},p_i)=1$;

$(\mathcal{R}_2')$ $((M,N),\mathbf{F},\mathfrak{D})$ satisfies condition $(\mathcal{U}_1')$-$(\mathcal{U}_5')$, and

$$m=\prod_{i\in[g]}(d_i)^2\times\prod_{i\in[s],j\in[t_i]}q_{i,j}\,;$$

$(\mathcal{R}_3')$ There is a one-to-one correspondence ρ from $[0:m-1]$ to $\mathbb{Z}^2_{\mathbf{d}}\times\mathbb{Z}_{\mathcal{Q}}$, where

$$\mathbb{Z}^2_{\mathbf{d}}=\prod_{i\in[g]}(\mathbb{Z}_{d_i})^2\quad\text{and}\quad\mathbb{Z}_{\mathcal{Q}}=\prod_{i\in[s],j\in[t_i]}\mathbb{Z}_{q_{i,j}},$$

such that (For every $a\in[0:m-1]$, we use

$$\big(x_{0,i,j}:i\in[g],j\in\{1,2\}\big)\in\mathbb{Z}^2_{\mathbf{d}}\qquad\text{and}\qquad\big(x_{1,i,j}:i\in[s],j\in[t_i]\big)\in\mathbb{Z}_{\mathcal{Q}}$$

to denote the components of $\mathbf{x}=\rho(a)\in\mathbb{Z}^2_{\mathbf{d}}\times\mathbb{Z}_{\mathcal{Q}}$, where $x_{0,i,j}\in\mathbb{Z}_{d_i}$ and $x_{1,i,j}\in\mathbb{Z}_{q_{i,j}}$)

$$F_{a,b}=\prod_{i\in[g]}\omega_{d_i}^{(x_{0,i,1}\ x_{0,i,2})\cdot\mathbf{W}^{[i]}\cdot(y_{0,i,1}\ y_{0,i,2})^T}\prod_{i\in[s],j\in[t_i]}\omega_{q_{i,j}}^{k_{i,j}\cdot x_{1,i,j}y_{1,i,j}},\quad\text{for all } a,b\in[0:m-1],$$

where $((x_{0,i,j}),(x_{1,i,j}))=\mathbf{x}=\rho(a)$ and $((y_{0,i,j}),(y_{1,i,j}))=\mathbf{y}=\rho(b)$.

For convenience, we will from now on directly use $\mathbf{x}\in\mathbb{Z}^2_{\mathbf{d}}\times\mathbb{Z}_{\mathcal{Q}}$ to index the rows and columns of $\mathbf{F}$:

$$F_{\mathbf{x},\mathbf{y}}\equiv F_{\rho^{-1}(\mathbf{x}),\rho^{-1}(\mathbf{y})}=\prod_{i\in[g]}\omega_{d_i}^{(x_{0,i,1}\ x_{0,i,2})\cdot\mathbf{W}^{[i]}\cdot(y_{0,i,1}\ y_{0,i,2})^T}\prod_{i\in[s],j\in[t_i]}\omega_{q_{i,j}}^{k_{i,j}\cdot x_{1,i,j}y_{1,i,j}},\quad\text{for all }\mathbf{x},\mathbf{y},\tag{13}$$

whenever we have a tuple $((M,N),\mathbf{F},\mathfrak{D},(\mathbf{d},\mathcal{W},\mathbf{p},\mathbf{t},\mathcal{Q},\mathcal{K}))$ that is known to satisfy condition $(\mathcal{R}')$. We assume the matrix $\mathbf{F}$ is indexed by $(\mathbf{x},\mathbf{y})$ rather than $(a,b)\in[0:m-1]^2$, and $(\mathcal{R}_3')$ refers to (13).

6.3.3 Step 3.3: Affine Support for $\mathfrak{D}$

Now we have a tuple $((M,N),\mathbf{F},\mathfrak{D},(\mathbf{d},\mathcal{W},\mathbf{p},\mathbf{t},\mathcal{Q},\mathcal{K}))$ that satisfies condition $(\mathcal{R}')$. In the next step we show for every $r\in[N-1]$ (for $r=0$, we already know $\mathbf{D}^{[0]}$ is the identity matrix), the non-zero entries of the r^{th} diagonal matrix $\mathbf{D}^{[r]}$ (in $\mathfrak{D}$) must have a very nice coset structure, otherwise $\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$ is #P-hard.

For every $r\in[N-1]$, we use $\Gamma_r\subseteq\mathbb{Z}_{\mathbf{d}}^2\times\mathbb{Z}_{\mathcal{Q}}$ to denote the set of $\mathbf{x}$ such that $D_{\mathbf{x}}^{[r]}\neq 0$. We also use $\mathcal{Z}$ to denote the set of $r\in[N-1]$ such that $\Gamma_r\neq\emptyset$.

For convenience, we let $\hat{\mathbb{Z}}_{\mathbf{q}_i}$, $i\in[s]$, denote the following set (or group, more exactly): When $i>1$, $\hat{\mathbb{Z}}_{\mathbf{q}_i}=\mathbb{Z}_{\mathbf{q}_i}$; and when $i=1$, $\hat{\mathbb{Z}}_{\mathbf{q}_1}=\mathbb{Z}_{\mathbf{d}}^2\times\mathbb{Z}_{\mathbf{q}_1}$. This gives us a new way to denote the components of

$$\mathbf{x}\in\mathbb{Z}_{\mathbf{d}}^2\times\mathbb{Z}_{\mathcal{Q}}=\prod_{i\in[s]}\hat{\mathbb{Z}}_{\mathbf{q}_i}\text{: }\mathbf{x}=(\mathbf{x}_1,...,\mathbf{x}_s)\text{, where }\mathbf{x}_i\in\hat{\mathbb{Z}}_{\mathbf{q}_i}.$$

Theorem 6.5. *Let* $((M,N),\mathbf{F},\mathfrak{D},(\mathbf{d},\mathcal{W},\mathbf{p},\mathbf{t},\mathcal{Q},\mathcal{K}))$ *be a tuple that satisfies condition* $(\mathcal{R}')$*, then either* $\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$ *is #P-hard; or* $\mathfrak{D}$ *satisfies the following condition* $(\mathcal{L}_1')$*: For every* $r\in\mathcal{Z}$*,*

($\mathcal{L}_1'$) $\Gamma_r=\prod_{i=1}^s\Gamma_{r,i}$*, where* $\Gamma_{r,i}$ *is a coset in* $\hat{\mathbb{Z}}_{\mathbf{q}_i}$*, for all* $i\in[s]$*.*

Suppose $\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$ is not #P-hard, then by Theorem 6.5, tuple $((M,N),\mathbf{F},\mathfrak{D},(\mathbf{d},\mathcal{W},\mathbf{p},\mathbf{t},\mathcal{Q},\mathcal{K}))$ satisfies not only $(\mathcal{R}')$ but also $(\mathcal{L}_1')$. By condition $(\mathcal{U}_3')$, $\mathfrak{D}$ satisfies the following additional property:

($\mathcal{L}_2'$) For every $r\in\mathcal{Z}$, there exists an $\mathfrak{a}^{[r]}\in\Gamma_r\subseteq\mathbb{Z}_{\mathbf{d}}^2\times\mathbb{Z}_{\mathcal{Q}}=\prod_{i\in[s]}\hat{\mathbb{Z}}_{\mathbf{q}_i}$ such that $D_{\mathfrak{a}^{[r]}}^{[r]}=1$.

From now on, when we say condition $(\mathcal{L}')$, we mean both conditions $(\mathcal{L}_1')$ and $(\mathcal{L}_2')$.

6.3.4 Step 3.4: Quadratic Structure

In this final step within Step 3 for the non-bipartite case, we show that, for any index $r\in[N-1]$, the non-zero entries of $\mathbf{D}^{[r]}$ must have a quadratic structure, otherwise $\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$ is #P-hard.

We need the following notation: Given $\mathbf{x}$ in $\hat{\mathbb{Z}}_{\mathbf{q}_i}$ for some $i\in[s]$, we let $\mathbf{ext}_r(\mathbf{x})$, where $r\in\mathcal{Z}$, denote the vector $\mathbf{x}'\in\mathbb{Z}_{\mathbf{d}}^2\times\mathbb{Z}_{\mathcal{Q}}$ such that in the expression $\mathbf{x}'=(\mathbf{x}_1',\dots,\mathbf{x}_s')\in\prod_{j\in[s]}\hat{\mathbb{Z}}_{\mathbf{q}_j}$, its i^{th} component $\mathbf{x}_i'=\mathbf{x}$, the vector given in $\hat{\mathbb{Z}}_{\mathbf{q}_i}$, and

$$\mathbf{x}_j'=\mathfrak{a}_j^{[r]},\quad\text{for all } j\neq i.$$

Recall that $\mathfrak{a}^{[r]}$ is a vector we picked from Γ_r in condition $(\mathcal{L}_2')$.

Let $\mathbf{a}$ be a vector in $\hat{\mathbb{Z}}_{\mathbf{q}_i}$ for some $i\in[s]$. Then we use $\widetilde{\mathbf{a}}$ to denote the vector $\mathbf{b}\in\prod_{j\in[s]}\hat{\mathbb{Z}}_{\mathbf{q}_j}$ such that $\mathbf{b}_i=\mathbf{a}$ and $\mathbf{b}_j=\mathbf{0}$ for all other $j\neq i$.

Theorem 6.6. *Suppose* $((M,N),\mathbf{F},\mathfrak{D},(\mathbf{d},\mathcal{W},\mathbf{p},\mathbf{t},\mathcal{Q},\mathcal{K}))$ *satisfies conditions* $(\mathcal{R}')$ *and* $(\mathcal{L})$*. Then either* $\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$ *is #P-hard or* $\mathfrak{D}$ *satisfies the following condition* $(\mathcal{D}')$*:*

($\mathcal{D}_1'$) *For every* $r\in\mathcal{Z}$*, we have*

$$D_{\mathbf{x}}^{[r]}=D_{\mathbf{ext}_r(\mathbf{x}_1)}^{[r]}D_{\mathbf{ext}_r(\mathbf{x}_2)}^{[r]}\cdots D_{\mathbf{ext}_r(\mathbf{x}_s)}^{[r]},\quad\textit{for all }\mathbf{x}\in\Gamma_r.\tag{14}$$

($\mathcal{D}_2'$) *For all* $r\in\mathcal{Z}$*,* $k\in[s]$ *and* $\mathbf{a}\in\Gamma_{r,k}^{\text{lin}}\subseteq\hat{\mathbb{Z}}_{\mathbf{q}_k}$*, there exist* $\mathbf{b}\in\hat{\mathbb{Z}}_{\mathbf{q}_k}$ *and* $\alpha\in\mathbb{Z}_N$ *such that*

$$\omega_N^{\alpha}\cdot F_{\widetilde{\mathbf{b}},\mathbf{x}}=D_{\mathbf{x}+\widetilde{\mathbf{a}}}^{[r]}\cdot\overline{D_{\mathbf{x}}^{[r]}},\quad\textit{for all }\mathbf{x}\in\Gamma_r;\tag{15}$$

Note that in $(\mathcal{D}_2')$, the expressions on the left-hand-side do not depend on all other components of $\mathbf{x}$ except the k^{th} component $\mathbf{x}_k\in\hat{\mathbb{Z}}_{\mathbf{q}_k}$, because all other components of $\widetilde{\mathbf{b}}$ are $\mathbf{0}$.

6.4 Tractability

Theorem 6.7. *Let* $((M,N),\mathbf{F},\mathfrak{D},(\mathbf{d},\mathcal{W},\mathbf{p},\mathbf{t},\mathcal{Q},\mathcal{K}))$ *be a tuple that satisfies conditions* $(\mathcal{R}')$*,* $(\mathcal{L}')$*, and* $(\mathcal{D}')$*, then* $\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$ *can be solved in polynomial time.*

7 Proofs of Theorem 5.1 and Theorem 6.1

In this section, we prove Theorem 5.1 and Theorem 6.1.

Let $\mathbf{A}=(A_{i,j})$ denote a connected and symmetric $m\times m$ matrix (at this moment, we do not make any assumption on whether $\mathbf{A}$ is bipartite or not. $\mathbf{A}$ could be either bipartite or non-bipartite). In the first step, we construct a new $m\times m$ matrix $\mathbf{B}$ from $\mathbf{A}$, which satisfies the following conditions:

1. $\mathbf{B}$ is also a connected and symmetric $m\times m$ matrix (so $\mathsf{EVAL}(\mathbf{B})$ is well-defined);
2. $\mathsf{EVAL}(\mathbf{B})\equiv\mathsf{EVAL}(\mathbf{A})$;
3. Every entry of $\mathbf{B}$ can be expressed as the product of a non-negative integer and a root of unity.

We let $\mathbf{B}'$ be the non-negative matrix such that $B'_{i,j}=|B_{i,j}|$. Then in the second step, we show that,

$$\mathsf{EVAL}(\mathbf{B}')\le\mathsf{EVAL}(\mathbf{B}).$$

Since $\mathbf{B}'$ is a connected, symmetric and non-negative matrix, we can apply the dichotomy theorem of Bulatov and Grohe [2] to $\mathbf{B}'$ and show that either $\mathsf{EVAL}(\mathbf{B}')$ is #P-hard or $\mathbf{B}$ is a (either bipartite or non-bipartite, depending on $\mathbf{A}$) *purified* matrix. When $\mathsf{EVAL}(\mathbf{B}')$ is #P-hard, we have

$$\mathsf{EVAL}(\mathbf{B}')\le\mathsf{EVAL}(\mathbf{B})\equiv\mathsf{EVAL}(\mathbf{A}),$$

which implies that $\mathsf{EVAL}(\mathbf{A})$ is also #P-hard. This proves both Theorem 5.1 and Theorem 6.1.

7.1 Equivalence between $\mathsf{EVAL}(\mathbf{A})$ and $\mathsf{COUNT}(\mathbf{A})$

We start with the definition of a class of counting problems $\mathsf{COUNT}(\cdot)$, which is very closely related to problems $\mathsf{EVAL}(\mathbf{A})$. It has been used in previous work [10] for establishing polynomial-time reductions between different $\mathsf{EVAL}(\cdot)$ problems.

Let $\mathbf{A}\in\mathbb{C}^{m\times m}$ denote a symmetric matrix. Then the input of problem $\mathsf{COUNT}(\mathbf{A})$ is a pair (G,x), where $G=(V,E)$ is an undirected graph, and x is a complex number. The output is

$$\#_{\mathbf{A}}(G,x)\equiv\Big|\Big\{\text{assignment }\xi:V\rightarrow[m]\;\Big|\;\text{wt}_{\mathbf{A}}(\xi)=x\Big\}\Big|,$$

a non-negative integer. The following lemma shows that $\mathsf{EVAL}(\mathbf{A})\equiv\mathsf{COUNT}(\mathbf{A})$.

Lemma 7.1. *Let* $\mathbf{A}\in\mathbb{C}^{m\times m}$ *be a symmetric matrix, then* $\mathsf{EVAL}(\mathbf{A})\equiv\mathsf{COUNT}(\mathbf{A})$*.*

Proof. To prove $\mathsf{EVAL}(\mathbf{A})\le\mathsf{COUNT}(\mathbf{A})$, recall that the matrix $\mathbf{A}$ is considered fixed. Let $G=(V,E)$ and $n=|E|$. We use X to denote the following set of complex numbers:

$$X=\left\{\prod_{i,j\in[m]}A_{i,j}^{k_{i,j}}\;\middle|\;\text{integers }k_{i,j}\ge 0\text{ and }\sum_{i,j\in[m]}k_{i,j}=n\right\}.\tag{16}$$

It is easy to see that $|X|$ is polynomial in n, being $\binom{n+m^2-1}{m^2-1}$ counting multiplicity, (we note that m is a constant here), and the elements in X can be enumerated in polynomial time (in n). It then follows from the expression in the definition of $\text{wt}_{\mathbf{A}}(\xi)$ that for any $x \notin X$, $\#_{\mathbf{A}}(G, x) = 0$. This gives us the following relation:

$$Z_{\mathbf{A}}(G) = \sum_{x \in X} x \cdot \#_{\mathbf{A}}(G, x), \quad \text{for any undirected graph } G,$$

and thus, $\mathsf{EVAL}(\mathbf{A}) \le \mathsf{COUNT}(\mathbf{A})$.

For the other direction, we construct, for any $p \in [|X|]$ (Recall that $|X|$ is polynomial in n), a new undirected graph $G^{[p]}$ from G by replacing every edge uv of G with p parallel edges between u and v. It is easy to check that for any assignment ξ, if its weight over G is x, then its weight over $G^{[p]}$ must be x^p. This gives us the following collection of equations: For every $p \in [|X|]$,

$$Z_{\mathbf{A}}(G^{[p]}) = \sum_{x \in X} x^p \cdot \#_{\mathbf{A}}(G, x), \quad \text{for any undirected graph } G.$$

Note that this is a Vandermonde system. Since we can query $\mathsf{EVAL}(\mathbf{A})$ for the values of $Z_{\mathbf{A}}(G^{[p]})$, we can solve it and get $\#_{\mathbf{A}}(G, x)$ for every non-zero $x \in X$. To obtain $\#_{\mathbf{A}}(G, 0)$ (if $0 \in X$), we note that

$$\sum_{x \in X} \#_{\mathbf{A}}(G, x) = m^{|V|}.$$

This gives us a polynomial-time reduction and thus, $\mathsf{COUNT}(\mathbf{A}) \le \mathsf{EVAL}(\mathbf{A})$. □

7.2 Step 1.1

We now show how to build the desired $\mathbf{B}$ from $\mathbf{A}$. We need the following notion of a *generating set*.

Definition 7.1. *Let $\mathscr{A} = \{a_j\}_{j \in [n]}$ be a set of n non-zero complex numbers, for some $n \ge 1$. Then we say $\{g_i\}_{i \in [d]}$, for some integer $d \ge 0$, is a* generating set *of $\mathscr{A}$ if*

1. *Every g_i is a non-zero complex number;*
2. *For all $(k_1, \ldots, k_d) \in \mathbb{Z}^d$ such that $(k_1, \ldots, k_d) \ne \mathbf{0}$, we have*
$$g_1^{k_1} \cdots g_d^{k_d} \text{ is not a root of unity.}$$
3. *For every $a \in \mathscr{A}$, there exists a unique $(k_1, \ldots, k_d) \in \mathbb{Z}^d$ such that*
$$\frac{a}{g_1^{k_1} \cdots g_d^{k_d}} \text{ is a root of unity.}$$

Clearly $d = 0$ iff the set $\mathscr{A}$ consists of roots of unity only. The next lemma shows that every $\mathscr{A}$ has a generating set.

Lemma 7.2. *Let $\mathscr{A} = \{a_j\}_{j \in [n]}$ be a set of non-zero complex numbers, then it has a generating set.*

Proof. We construct a generating set $\mathscr{G}$ for $\mathscr{A}$, which consists of two parts: $\mathscr{G} = \mathscr{B} \cup \mathscr{C}$.

First, let $\alpha_j = \log_2 |a_j|$, for every $j \in [n]$. We let $\{\alpha_{j_1}, \ldots, \alpha_{j_s}\}$, for some $s \ge 0$, denote a maximal linearly independent subset of $\{\alpha_j\}_{j \in [n]}$ over $\mathbb{Q}$. By definition, for any $j \in [n]$, there exist $r_{j,1}, \ldots, r_{j,s}$ in $\mathbb{Q}$ such that

$$\alpha_j = \sum_{\ell=1}^{s} r_{j,\ell} \cdot \alpha_{j_\ell}.$$

For each $\ell \in [s]$, we use N_ℓ to denote the smallest positive integer such that $N_\ell \cdot r_{j,\ell}$ is an integer for all $j \in [n]$. Then we define $\mathscr{B}$ as $\{b_1, \ldots, b_s\}$ where $b_\ell = 2^{\alpha_{j_\ell}/N_\ell}$, for all $\ell \in [s]$.

Second, we let β_j, for every $j \in [n]$, denote the unique real number in $[0,1)$ such that

$$\frac{a_j}{|a_j|} = e^{2\pi i \cdot \beta_j} \qquad \text{(where } i^2 = -1\text{)}.$$

Consider the set $\{\beta_1, \ldots, \beta_n, 1\}$. Extend, from the set $\{1\}$ consisting of a single non-zero value 1, to a maximal linearly independent subset $\{\beta_{j'_1}, \ldots, \beta_{j'_t}, 1\}$ of $\{\beta_1, \ldots, \beta_n, 1\}$ over $\mathbb{Q}$. Here $t \geq 0$. It implies that for every $j \in [n]$, there exist rational numbers $r'_{j,1}, \ldots, r'_{j,t}, r'_{j,t+1} \in \mathbb{Q}$, such that

$$\beta_j = \sum_{\ell=1}^{t} r'_{j,\ell} \cdot \beta_{j'_\ell} + r'_{j,t+1}.$$

Similarly, for each $\ell \in [t]$, we let M_ℓ denote the smallest positive integer such that $M_\ell \cdot r'_{j,\ell}$ is an integer for all $j \in [n]$. Then we define $\mathscr{C}$ as $\{c_1, \ldots, c_t\}$ where

$$c_\ell = e^{2\pi i \cdot \beta_{j'_\ell} \big/ M_\ell}, \quad \text{for all } \ell \in [t].$$

It is easy to check that $\mathscr{G} = \mathscr{B} \cup \mathscr{C}$ is a generating set of $\mathscr{A}$. Briefly: (1) Being exponentials, clearly every member in $\mathscr{G}$ is non-zero. (2) If

$$\prod_{\ell=1}^{s} b_\ell^{k_\ell} \cdot \prod_{\ell=1}^{t} c_\ell^{k'_\ell}$$

is equal to some root of unity ω, then by taking norm, we get $\prod_{\ell=1}^{s} b_\ell^{k_\ell} = 1$. By linear independence of $\{\alpha_{j_\ell}\}_{\ell \in [s]}$ we get all $k_\ell = 0$. On the other hand, $\prod_{\ell=1}^{t} c_\ell^{k'_\ell} = \omega$ gives all $k'_\ell = 0$ by linear independence of $\{\beta_{j'_1}, \ldots, \beta_{j'_t}, 1\}$. (3) To express any $a_j \in \mathscr{A}$ as an integral power from $\mathscr{G}$ together with a root of unity, first we express $a_j/|a_j|$ as such from $\mathscr{C}$ together with a root of unity, and then express $|a_j|$ as an integral power from $\mathscr{B}$. The uniqueness of the expression follows from (2). ◻

Now we use $\mathscr{A}$ to denote the set of all non-zero entries $A_{i,j}$ in the matrix $\mathbf{A}$. By Lemma 7.2, we know that it has a generating set $\mathscr{G} = \{g_1, \ldots, g_d\}$.

The matrix $\mathbf{B} = (B_{i,j}) \in \mathbb{C}^{m \times m}$ is constructed as follows. Let $p_1 < \cdots < p_d$ denote the d smallest primes. For every $i, j \in [m]$, we define $B_{i,j}$. If $A_{i,j} = 0$, then $B_{i,j} = 0$. Suppose $A_{i,j} \neq 0$, since $\mathscr{G}$ is a generating set, we know there exists a unique $(k_1, \ldots, k_d) \in \mathbb{Z}^d$ such that

$$\frac{A_{i,j}}{g_1^{k_1} \cdots g_d^{k_d}} \quad \text{is a root of unity.}$$

Then we set $B_{i,j}$ to be

$$B_{i,j} = p_1^{k_1} \cdots p_d^{k_d} \cdot \frac{A_{i,j}}{g_1^{k_1} \cdots g_d^{k_d}}.$$

So what we did in constructing $\mathbf{B}$ is just replacing each g_i in $\mathscr{G}$ with a prime p_i. $B_{i,j}$ is well-defined by the uniqueness of $(k_1, \ldots, k_d) \in \mathbb{Z}^d$ and conversely by taking the prime factorization of $|B_{i,j}|$ we can recover $(k_1, \ldots, k_d)$ uniquely, and then recover $A_{i,j}$ by

$$A_{i,j} = g_1^{k_1} \cdots g_d^{k_d} \cdot \frac{B_{i,j}}{p_1^{k_1} \cdots p_d^{k_d}}.$$

The next lemma shows that such a replacement does not affect the complexity of $\mathsf{EVAL}(\mathbf{A})$.

Lemma 7.3. *Let* $\mathbf{A} \in \mathbb{C}^{m\times m}$ *be a symmetric and connected matrix, and* $\mathbf{B} \in \mathbb{C}^{m\times m}$ *be the matrix we built above, then* $\mathsf{EVAL}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{B})$.

Proof. By Lemma 7.1, it suffices to prove that $\mathsf{COUNT}(\mathbf{A}) \equiv \mathsf{COUNT}(\mathbf{B})$. Here we only prove one of the two directions: $\mathsf{COUNT}(\mathbf{A}) \le \mathsf{COUNT}(\mathbf{B})$. The other direction can be proved similarly.

Let (G, x) be an input of $\mathsf{COUNT}(\mathbf{A})$, where $G = (V, E)$ and $n = |E|$. We use X to denote the set of complex numbers defined earlier in (16). Recall that $|X|$ is polynomial in n (since m is a constant), and can be enumerated in polynomial time. Furthermore, if $x \notin X$, then $\#_{\mathbf{A}}(G, x)$ must be zero.

Now suppose $x \in X$, then we can find a particular sequence of non-negative integers $\{k^*_{i,j}\}_{i,j\in[m]}$ in polynomial time, such that $\sum_{i,j} k^*_{i,j} = n$ and

$$x = \prod_{i,j\in[m]} A_{i,j}^{k^*_{i,j}}. \tag{17}$$

This sequence $\{k^*_{i,j}\}_{i,j\in[m]}$ is in general *not unique* for the given x. Using $\{k^*_{i,j}\}$, we define y by

$$y = \prod_{i,j\in[m]} B_{i,j}^{k^*_{i,j}}. \tag{18}$$

It is clear that $x = 0$ iff $y = 0$. This happens precisely when some $k^*_{i,j} > 0$ for some entry $A_{i,j} = 0$.

The reduction $\mathsf{COUNT}(\mathbf{A}) \le \mathsf{COUNT}(\mathbf{B})$ then follows from the following claim

$$\#_{\mathbf{A}}(G, x) = \#_{\mathbf{B}}(G, y). \tag{19}$$

To prove this claim, we only need to show that, for any assignment $\xi : V \to [m]$,

$$\text{wt}_{\mathbf{A}}(\xi) = x \iff \text{wt}_{\mathbf{B}}(\xi) = y.$$

We only prove $\text{wt}_{\mathbf{A}}(\xi) = x \Rightarrow \text{wt}_{\mathbf{B}}(\xi) = y$ here. The other direction can be proved similarly.

Let $\xi : V \to [m]$ denote any assignment. For every $i, j \in [m]$, we use $k_{i,j}$ to denote the number of edges $uv \in E$ such that $(\xi(u), \xi(v)) = (i, j)$ or (j, i), then for both $\mathbf{A}$ and $\mathbf{B}$,

$$\text{wt}_{\mathbf{A}}(\xi) = \prod_{i,j\in[m]} A_{i,j}^{k_{i,j}} \quad \text{and} \quad \text{wt}_{\mathbf{B}}(\xi) = \prod_{i,j\in[m]} B_{i,j}^{k_{i,j}}. \tag{20}$$

For $x = 0$, we note that the weight $\text{wt}_{\mathbf{A}}(\xi)$ is 0 iff for some zero entry $A_{i,j} = 0$ we have $k_{i,j} > 0$. By the construction of $\mathbf{B}$, $A_{i,j} = 0$ iff $B_{i,j} = 0$, so $\text{wt}_{\mathbf{B}}(\xi)$ must also be 0.

In the following we assume both $x, y \ne 0$, and we only consider assignments $\xi : V \to [m]$ such that its $k_{i,j} = 0$ for any $A_{i,j} = 0$ (equivalently $k_{i,j} = 0$ for any $B_{i,j} = 0$). Thus we may consider the products in (20) are over non-zero entries $A_{i,j}$ and $B_{i,j}$, respectively.

Now we use the generating set $\mathscr{G} = \{g_1, \ldots, g_d\}$ chosen above for the set $\mathscr{A}$ of all non-zero entries $A_{i,j}$ in the matrix $\mathbf{A}$. There are integer exponents $e_{1,(ij)}$, $e_{2,(ij)}$, $\ldots$, $e_{d,(ij)}$, such that

$$A_{i,j} = \prod_{\ell=1}^{d} g_\ell^{e_{\ell,(ij)}} \cdot \omega_{i,j}, \quad \text{and} \quad B_{i,j} = \prod_{\ell=1}^{d} p_\ell^{e_{\ell,(ij)}} \cdot \omega_{i,j}, \quad \text{for all } i, j \text{ such that } A_{i,j} \ne 0,$$

where $\omega_{i,j}$ is a root of unity. The expression of $B_{i,j}$ follows from the construction. By (17) and (20),

$$\text{wt}_{\mathbf{A}}(\xi) = x \implies \prod_{\ell=1}^{d} g_\ell^{\sum_{i,j}(k_{i,j}-k^*_{i,j})e_{\ell,(ij)}} \text{ is a root of unity.}$$

Here the sum $\sum_{i,j}$ in the exponent is over all $i,j \in [m]$ where the corresponding $A_{i,j}$ is non-zero. This last equation is equivalent to (since $\mathscr{G}$ is a generating set)

$$\sum_{i,j}(k_{i,j} - k^*_{i,j}) \cdot e_{\ell,(ij)} = 0, \qquad \text{for all } \ell \in [d], \tag{21}$$

which in turn implies that

$$\prod_{i,j}(\omega_{i,j})^{k_{i,j}} = \prod_{i,j}(\omega_{i,j})^{k^*_{i,j}}. \tag{22}$$

It then follows from (18), (20), (21) and (22) that $\text{wt}_{\mathbf{B}}(\xi) = y$. □

7.3 Step 1.2

Now we let $\mathbf{B}'$ denote the $m \times m$ matrix such that $B'_{i,j} = |B_{i,j}|$ for all $i,j \in [m]$. We have (note that Lemma 7.4 holds for any symmetric matrix $\mathbf{B}$ and $\mathbf{B}'$, as long as $B'_{i,j} = |B_{i,j}|$ for all i,j)

Lemma 7.4. $\mathsf{EVAL}(\mathbf{B}') \le \mathsf{EVAL}(\mathbf{B})$.

Proof. By Lemma 7.1, we only need to show that $\mathsf{COUNT}(\mathbf{B}') \le \mathsf{COUNT}(\mathbf{B})$.

Let (G, x) be an input of $\mathsf{COUNT}(\mathbf{B}')$. Since $\mathbf{B}'$ is non-negative, we have $\#_{\mathbf{B}'}(G,x) = 0$ if x is not real or $x < 0$. Now suppose $x \ge 0$, $G = (V,E)$ and $n = |E|$. We let Y denote the following set

$$Y = \left\{ \prod_{i,j\in[m]} B_{i,j}^{k_{i,j}} \;\middle|\; \text{integers } k_{i,j} \ge 0 \text{ and } \sum_{i,j\in[m]} k_{i,j} = n \right\}.$$

Again, we know $|Y|$ is polynomial in n and can be enumerated in polynomial time in n. Once we have Y, we remove all elements in Y whose complex norm is not equal to x. We call the subset left Y_x.

The lemma then follows directly from the following statement:

$$\#_{\mathbf{B}'}(G,x) = \sum_{y\in Y_x} \#_{\mathbf{B}}(G,y).$$

This is because for every assignment $\xi : V \to [m]$, $\text{wt}_{\mathbf{B}'}(\xi) = x$ if and only if $|\text{wt}_{\mathbf{B}}(\xi)| = x$. This gives us a polynomial reduction since $Y_x \subseteq Y$, $|Y_x|$ is polynomially bounded in n, and Y_x can be enumerated in polynomial time. □

Finally we prove Theorem 5.1 and Theorem 6.1.

Proof of Theorem 5.1. Let $\mathbf{A} \in \mathbb{C}^{m\times m}$ be a symmetric, connected and bipartite matrix. We construct matrices $\mathbf{B}$ and $\mathbf{B}'$ as above. Since we assumed $\mathbf{A}$ to be connected and bipartite, both matrices $\mathbf{B}$ and $\mathbf{B}'$ are connected and bipartite. Therefore, we know there is a permutation Π from $[m]$ to itself such that $\mathbf{B}_{\Pi,\Pi}$ is the bipartisation of a $k \times (m-k)$ matrix $\mathbf{F}$, for some $1 \le k < m$:

$$\mathbf{B}_{\Pi,\Pi} = \begin{pmatrix} \mathbf{0} & \mathbf{F} \\ \mathbf{F}^T & \mathbf{0} \end{pmatrix},$$

and $\mathbf{B}'_{\Pi,\Pi}$ is the bipartisation of $\mathbf{F}'$, where $F'_{i,j} = |F_{i,j}|$ for all $i \in [k]$ and $j \in [m-k]$. Since permuting the rows and columns of $\mathbf{B}$ does not affect the complexity of $\mathsf{EVAL}(\mathbf{B})$, we have

$$\mathsf{EVAL}(\mathbf{B}'_{\Pi,\Pi}) \le \mathsf{EVAL}(\mathbf{B}_{\Pi,\Pi}) \equiv \mathsf{EVAL}(\mathbf{B}) \equiv \mathsf{EVAL}(\mathbf{A}). \tag{23}$$

We also know that $\mathbf{B}'_{\Pi,\Pi}$ is non-negative. By Bulatov and Grohe's theorem, we have the following cases:

– First, if $\mathsf{EVAL}(\mathbf{B}'_{\Pi,\Pi})$ is #P-hard, then by (23), $\mathsf{EVAL}(\mathbf{A})$ is also #P-hard.

– Second, if $\mathsf{EVAL}(\mathbf{B}'_{\Pi,\Pi})$ is not #P-hard then the rank of $\mathbf{F}'$ must be 1 (it cannot be 0 since $\mathbf{B}'_{\Pi,\Pi}$ is assumed to be connected and bipartite). Therefore, there exist non-negative rational numbers $\mu_1,\ldots,\mu_k,\ldots,\mu_m$ such that $F'_{i,j}=\mu_i\mu_{j+k}$, for all $i\in[k]$ and $j\in[m-k]$. Moreover, μ_i, for all $i\in[m]$, cannot be 0 since otherwise $\mathbf{B}'_{\Pi,\Pi}$ is not connected.

As every entry of $\mathbf{B}_{\Pi,\Pi}$ is the product of the corresponding entry of $\mathbf{B}'_{\Pi,\Pi}$ and some root of unity, $\mathbf{B}_{\Pi,\Pi}$ is a purified bipartite matrix. The theorem is proven since $\mathsf{EVAL}(\mathbf{B})\equiv\mathsf{EVAL}(\mathbf{A})$. □

Proof of Theorem 6.1. The proof is similar.

Let $\mathbf{A}\in\mathbb{C}^{m\times m}$ be a symmetric, connected and non-bipartite matrix. We construct $\mathbf{B}$ and $\mathbf{B}'$ as above. Since $\mathbf{A}$ is connected and non-bipartite, both $\mathbf{B}$ and $\mathbf{B}'$ are connected and non-bipartite. Also, $\mathbf{B}'$ is non-negative. We consider the following two cases. If $\mathbf{B}'$ is #P-hard, then $\mathsf{EVAL}(\mathbf{B}')\le\mathsf{EVAL}(\mathbf{B})$ $\equiv\mathsf{EVAL}(\mathbf{A})$ implies that $\mathsf{EVAL}(\mathbf{A})$ must also be #P-hard. If $\mathbf{B}'$ is not #P-hard then it follows from the dichotomy theorem of Bulatov and Grohe [2] that the rank of $\mathbf{B}$ is 1 (it cannot be 0 since we assumed $m>1$, and $\mathbf{B}$ is connected). Since $\mathbf{B}$ is symmetric, it is a purified non-bipartite matrix. The theorem then follows since $\mathsf{EVAL}(\mathbf{B})\equiv\mathsf{EVAL}(\mathbf{A})$. □

8 Proof of Theorem 5.2

We start by introducing a technique for establishing reductions between $\mathsf{EVAL}(\mathbf{A})$ and $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$. It is inspired by the Twin Reduction Lemma proved in [10].

8.1 Cyclotomic Reduction and Inverse Cyclotomic Reduction

Let $\mathbf{A}$ be an $m\times m$ symmetric complex matrix (Note that $\mathbf{A}$ is not necessarily bipartite). Let $(\mathbf{C},\mathfrak{D})$ be a pair that satisfies the following condition $(\mathcal{T})$:

$(\mathcal{T}_1)$ $\mathbf{C}$ is an $n\times n$ symmetric complex matrix;

$(\mathcal{T}_2)$ $\mathfrak{D}=\{\mathbf{D}^{[0]},\ldots,\mathbf{D}^{[N-1]}\}$ is a sequence of N $n\times n$ diagonal matrices for some positive integer N;

$(\mathcal{T}_3)$ Every diagonal entry $D^{[0]}_i$ in $\mathbf{D}^{[0]}$ is a positive integer. Furthermore, for every $i\in[n]$, there exist nonnegative integers $\alpha_{i,0},\ldots,\alpha_{i,N-1}$ such that

$$D^{[0]}_i=\sum_{j=0}^{N-1}\alpha_{i,j}\quad\text{and}\quad D^{[r]}_i=\sum_{j=0}^{N-1}\alpha_{i,j}\cdot\omega_N^{jr},\quad\text{for all } r\in[N-1].$$

In particular, we say tuple $(\alpha_{i,0},\ldots,\alpha_{i,N-1})$ generates the i^{th} entries of $\mathfrak{D}$.

We show that if $\mathbf{A}$ and $(\mathbf{C},\mathfrak{D})$ satisfy certain conditions, then $\mathsf{EVAL}(\mathbf{A})\equiv\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$.

Definition 8.1. *Let $\mathscr{R}=\{R_{1,0},R_{1,1},\ldots,R_{1,N-1},\ldots,R_{n,0},\ldots,R_{n,N-1}\}$ be a partition of $[m]$ (note that each $R_{a,b}$ here need not be nonempty). We say $\mathbf{A}$ can be generated by $\mathbf{C}$ using $\mathscr{R}$ if*

1. *$\mathscr{R}$ satisfies $\bigcup_{b\in[0:N-1]}R_{a,b}\neq\emptyset$ for all $a\in[n]$;*
2. *For all $i,j\in[m]$, suppose $i\in R_{a,b}$ and $j\in R_{a',b'}$, then*

$$A_{i,j}=C_{a,a'}\cdot\omega_N^{b+b'}.\tag{24}$$

Note that for any pair $(\mathbf{C}, \mathfrak{D})$ that satisfies $(\mathcal{T})$, one can build a matrix $\mathbf{A} \in \mathbb{C}^{m\times m}$ for some $m \geq n$, together with a partition $\mathscr{R}$ of $[m]$, such that, $\mathbf{A}$ can be generated by $\mathbf{C}$ using $\mathscr{R}$ and the a^{th} entries of $\mathfrak{D}$ can be generated by $(|R_{a,0}|, |R_{a,1}|, \ldots, |R_{a,N-1}|)$, for all $a \in [n]$. We prove the following lemma:

Lemma 8.1 (Cyclotomic Reduction Lemma)**.** *Suppose matrix* $\mathbf{A}$ *can be* generated *by* $\mathbf{C}$ *using partition* $\mathscr{R} = \{R_{a,b}\}$*, and for any* $a \in [n]$*, the* a^{th} *entries of* $\mathfrak{D}$ *can be* generated *by* $(|R_{a,0}|, \ldots, |R_{a,N-1}|)$*, then*

$$\mathsf{EVAL}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{C}, \mathfrak{D}).$$

Proof. It suffices to prove for any undirected graph $G = (V, E)$,

$$Z_{\mathbf{A}}(G) = \sum_{\xi:V\rightarrow[m]} \mathrm{wt}_{\mathbf{A}}(\xi) \quad \text{and} \quad Z_{\mathbf{C},\mathfrak{D}}(G) = \sum_{\eta:V\rightarrow[n]} \mathrm{wt}_{\mathbf{C},\mathfrak{D}}(\eta)$$

are exactly the same.

To prove this, we define a surjective map ρ from $\{\xi\}$, the set of all assignments from V to $[m]$, to $\{\eta\}$, the set of all assignments from V to $[n]$. Then we show for every $\eta : V \rightarrow [n]$,

$$\mathrm{wt}_{\mathbf{C},\mathfrak{D}}(\eta) = \sum_{\xi:\rho(\xi)=\eta} \mathrm{wt}_{\mathbf{A}}(\xi). \tag{25}$$

We define $\rho(\xi)$ as follows. Since $\mathscr{R}$ is a partition of $[m]$, for any $v \in V$, there exists a unique pair (a, b) such that $\xi(v) \in R_{a,b}$. Let $\xi_1(v) = a$ and $\xi_2(v) = b$, then we set $\rho(\xi) = \eta \equiv \xi_1$ from V to $[n]$. It is easy to check that ρ is surjective.

To prove (25), we write $\mathrm{wt}_{\mathbf{A}}(\xi)$ as

$$\mathrm{wt}_{\mathbf{A}}(\xi) = \prod_{uv\in E} A_{\xi(u),\xi(v)} = \prod_{uv\in E} C_{\eta(u),\eta(v)} \cdot \omega_N^{\xi_2(u)+\xi_2(v)} = \prod_{uv\in E} C_{\eta(u),\eta(v)} \cdot \omega_N^{\xi_2(u)} \cdot \omega_N^{\xi_2(v)}.$$

It follows that

$$\begin{aligned}
\sum_{\xi:\rho(\xi)=\eta} \mathrm{wt}_{\mathbf{A}}(\xi) &= \prod_{uv\in E} C_{\eta(u),\eta(v)} \times \sum_{\xi:\rho(\xi)=\eta} \left(\prod_{uv\in E} \omega_N^{\xi_2(u)} \cdot \omega_N^{\xi_2(v)} \right) \\
&= \prod_{uv\in E} C_{\eta(u),\eta(v)} \times \sum_{\xi:\rho(\xi)=\eta} \left(\prod_{v\in V} \omega_N^{\xi_2(v)\cdot\deg(v)} \right) \\
&= \prod_{uv\in E} C_{\eta(u),\eta(v)} \times \left(\prod_{v\in V} \left(\sum_{b=0}^{N-1} \left|R_{\eta(v),b}\right| \cdot \omega_N^{b\cdot\deg(v)} \right) \right) \\
&= \prod_{uv\in E} C_{\eta(u),\eta(v)} \times \left(\prod_{v\in V} D_{\eta(v)}^{[\deg(v) \bmod N]} \right) \; = \; \mathrm{wt}_{\mathbf{C},\mathfrak{D}}(\eta),
\end{aligned}$$

and the lemma follows. □

By combining Lemma 8.1, Lemma 7.4, and the dichotomy theorem of Bulatov and Grohe, we have the following handy corollary for dealing with $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$:

Corollary 8.1 (Inverse Cyclotomic Reduction Lemma)**.** *Let* $(\mathbf{C}, \mathfrak{D})$ *be a pair that satisfies condition* $(\mathcal{T})$*. If* $\mathbf{C}$ *has a* 2×2 *sub-matrix*

$$\begin{pmatrix} C_{i,k} & C_{i,\ell} \\ C_{j,k} & C_{j,\ell} \end{pmatrix}$$

such that all of its four entries are nonzero and

$$\left|C_{i,k}C_{j,\ell}\right| \neq \left|C_{i,\ell}C_{j,k}\right|,$$

then the problem $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ *is #P-hard.*

Proof. By the Cyclotomic Reduction Lemma, we know there exist a symmetric $m \times m$ matrix $\mathbf{A}$, for some positive integer m, and a partition $\mathscr{R}$ of $[m]$, where

$$\mathscr{R} = \Big\{ R_{a,b} \;\Big|\; a \in [n], b \in [0:N-1] \Big\} \quad \text{and} \quad \bigcup_{b\in[0:N-1]} R_{a,b} \neq \emptyset, \quad \text{for all } a \in [n], \tag{26}$$

such that $\mathsf{EVAL}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{C},\mathfrak{D})$. Moreover, matrices $\mathbf{A}$ and $\mathbf{C}$ satisfy (24).

Now suppose there exist $i \neq j, k \neq \ell \in [n]$ such that $|C_{i,k}|, |C_{i,\ell}|, |C_{j,k}|$ and $|C_{j,\ell}|$ are non-zero and $|C_{i,k}C_{j,\ell}| \neq |C_{i,\ell}C_{j,k}|$. We arbitrarily pick an integer i' from $\bigcup_b R_{i,b}$ (which is known to be nonempty), a j' from $\bigcup_b R_{j,b}$, a k' from $\bigcup_b R_{k,b}$, and an ℓ' from $\bigcup_b R_{\ell,b}$. Then by (24), we have

$$|A_{i',k'}| = |C_{i,k}|, \quad |A_{i',\ell'}| = |C_{i,\ell}|, \quad |A_{j',k'}| = |C_{j,k}|, \quad |A_{j',\ell'}| = |C_{j,\ell}|, \quad \text{and} \quad |A_{i',k'}A_{j',\ell'}| \neq |A_{i',\ell'}A_{j',k'}|.$$

Let $\mathbf{A}' = (|A_{i,j}|)$ for all $i,j \in [m]$, then $\mathbf{A}'$ has a 2 by 2 sub-matrix of rank 2 and all of its four entries are non-zero. By the dichotomy theorem of Bulatov and Grohe (Corollary 2.1), $\mathsf{EVAL}(\mathbf{A}')$ is #P-hard. It then follows that $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ is also #P-hard, since $\mathsf{EVAL}(\mathbf{C},\mathfrak{D}) \equiv \mathsf{EVAL}(\mathbf{A})$, and by Lemma 7.4, $\mathsf{EVAL}(\mathbf{A}') \leq \mathsf{EVAL}(\mathbf{A})$. □

By combining Lemma 8.1, Eq. (25), and the First Pinning Lemma (Lemma 4.1), we have

Corollary 8.2 (Third Pinning Lemma)**.** *Let* $(\mathbf{C},\mathfrak{D})$ *be a pair that satisfies* $(\mathcal{T})$*, then*

$$\mathsf{EVALP}(\mathbf{C},\mathfrak{D}) \equiv \mathsf{EVAL}(\mathbf{C},\mathfrak{D}).$$

In particular, the problem of computing $Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}$ *(or* $Z^{\leftarrow}_{\mathbf{C},\mathfrak{D}}$*) is polynomial-time reducible to* $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$*.*

Proof. We only need to prove that $\mathsf{EVALP}(\mathbf{C},\mathfrak{D}) \leq \mathsf{EVAL}(\mathbf{C},\mathfrak{D})$.

By the Cyclotomic Reduction Lemma, we know there exist a symmetric $m \times m$ matrix $\mathbf{A}$, for some $m \geq 1$, and a partition $\mathscr{R}$ of $[m]$, such that, $\mathscr{R}$ satisfies (26) and $\mathsf{EVAL}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{C},\mathfrak{D})$. $\mathbf{A}$, $\mathbf{C}$ and $\mathscr{R}$ also satisfy (24).

By the First Pinning Lemma, we have $\mathsf{EVALP}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{C},\mathfrak{D})$. So we only need to reduce $\mathsf{EVALP}(\mathbf{C},\mathfrak{D})$ to $\mathsf{EVALP}(\mathbf{A})$.

Now let (G,w,i) be an input of $\mathsf{EVALP}(\mathbf{C},\mathfrak{D})$, where G is an undirected graph, w is a vertex in G and $i \in [n]$. By (25), we have

$$Z_{\mathbf{C},\mathfrak{D}}(G,w,i) = \sum_{\eta:\eta(w)=i} \mathrm{wt}_{\mathbf{C},\mathfrak{D}}(\eta) = \sum_{\xi:\xi_1(w)=i} \mathrm{wt}_{\mathbf{A}}(\xi) = \sum_{j\in\cup_b R_{i,b}} Z_{\mathbf{A}}(G,w,j).$$

This gives us a polynomial-time reduction from $\mathsf{EVALP}(\mathbf{C},\mathfrak{D})$ to $\mathsf{EVALP}(\mathbf{A})$. □

Notice that, compared to the Second Pinning Lemma, the Third Pinning Lemma does not require the matrix $\mathbf{C}$ to be the bipartisation of a unitary matrix. It only requires $(\mathbf{C},\mathfrak{D})$ to satisfy $(\mathcal{T})$.

8.2 Step 2.1

Let $\mathbf{A}$ be a purified bipartite matrix. Then after collecting its entries of equal norm in decreasing order (by permuting the rows and columns of $\mathbf{A}$), there exist a positive integer N and four sequences $\boldsymbol{\mu}, \boldsymbol{\nu}, \mathbf{m}$ and $\mathbf{n}$ such that $(\mathbf{A}, (N, \boldsymbol{\mu}, \boldsymbol{\nu}, \mathbf{m}, \mathbf{n}))$ satisfies the following condition:

($\mathcal{S}_1$) Matrix $\mathbf{A}$ is the bipartisation of an $m \times n$ matrix $\mathbf{B}$ so $\mathbf{A}$ is $(m+n) \times (m+n)$. $\boldsymbol{\mu} = \{\mu_1, \ldots, \mu_s\}$ and $\boldsymbol{\nu} = \{\nu_1, \ldots, \nu_t\}$ are two sequences of positive rational numbers, of lengths $s \geq 1$ and $t \geq 1$, respectively. $\boldsymbol{\mu}$ and $\boldsymbol{\nu}$ satisfy $\mu_1 > \mu_2 > \ldots > \mu_s$ and $\nu_1 > \nu_2 > \ldots > \nu_t$. $\mathbf{m} = \{m_1, ..., m_s\}$ and $\mathbf{n} = \{n_1, ..., n_t\}$ are two sequences of positive integers such that, $m = \sum m_i$ and $n = \sum n_i$. The rows of $\mathbf{B}$ are indexed by $\mathbf{x} = (x_1, x_2)$ where $x_1 \in [s]$ and $x_2 \in [m_{x_1}]$, while the columns of $\mathbf{B}$ are indexed by $\mathbf{y} = (y_1, y_2)$ where $y_1 \in [t]$ and $y_2 \in [n_{y_1}]$. For all $\mathbf{x}, \mathbf{y}$, we have

$$B_{\mathbf{x},\mathbf{y}} = B_{(x_1,x_2),(y_1,y_2)} = \mu_{x_1} \nu_{y_1} S_{\mathbf{x},\mathbf{y}},$$

where $\mathbf{S} = \{S_{\mathbf{x},\mathbf{y}}\}$ is an $m \times n$ matrix in which every entry is a power of ω_N.

$$\mathbf{B} = \begin{pmatrix} \mu_1 \mathbf{I}_{m_1} & & & \\ & \mu_2 \mathbf{I}_{m_2} & & \\ & & \ddots & \\ & & & \mu_s \mathbf{I}_{m_s} \end{pmatrix} \begin{pmatrix} \mathbf{S}_{(1,*),(1,*)} & \mathbf{S}_{(1,*),(2,*)} & \ldots & \mathbf{S}_{(1,*),(t,*)} \\ \mathbf{S}_{(2,*),(1,*)} & \mathbf{S}_{(2,*),(2,*)} & \ldots & \mathbf{S}_{(2,*),(t,*)} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{S}_{(s,*),(1,*)} & \mathbf{S}_{(s,*),(2,*)} & \ldots & \mathbf{S}_{(s,*),(t,*)} \end{pmatrix} \begin{pmatrix} \nu_1 \mathbf{I}_{n_1} & & & \\ & \nu_2 \mathbf{I}_{n_2} & & \\ & & \ddots & \\ & & & \nu_t \mathbf{I}_{n_t} \end{pmatrix},$$

where $\mathbf{I}_k$ denotes the $k \times k$ identity matrix.

We let

$$I \equiv \bigcup_{i \in [s]} \{ (i,j) \mid j \in [m_i] \} \quad \text{and} \quad J \equiv \bigcup_{i \in [t]} \{ (i,j) \mid j \in [n_i] \},$$

respectively. We use $\{0\} \times I$ to index the first m rows (or columns) of $\mathbf{A}$, and $\{1\} \times J$ to index the last n rows (or columns) of $\mathbf{A}$. Given $\mathbf{x} \in I$ and $j \in [t]$, we let

$$\mathbf{S}_{\mathbf{x},(j,*)} = \left(S_{\mathbf{x},(j,1)}, \ldots, S_{\mathbf{x},(j,n_j)} \right) \in \mathbb{C}^{n_j}$$

denote the j^{th} block of the $\mathbf{x}^{th}$ row vector of $\mathbf{S}$. Similarly, given $\mathbf{y} \in J$ and $i \in [s]$, we let

$$\mathbf{S}_{(i,*),\mathbf{y}} = \left(S_{(i,1),\mathbf{y}}, \ldots, S_{(i,m_i),\mathbf{y}} \right) \in \mathbb{C}^{m_i}$$

denote the i^{th} block of the $\mathbf{y}^{th}$ column vector of $\mathbf{S}$.

Lemma 8.2. *Suppose* $(\mathbf{A}, (N, \boldsymbol{\mu}, \boldsymbol{\nu}, \mathbf{m}, \mathbf{n}))$ *satisfies* ($\mathcal{S}_1$), *then either* $\mathsf{EVAL}(\mathbf{A})$ *is #P-hard or* $(\mathbf{A}, (N, \boldsymbol{\mu}, \boldsymbol{\nu}, \mathbf{m}, \mathbf{n}))$ *satisfies the following two conditions:*

($\mathcal{S}_2$) *For all* $\mathbf{x}, \mathbf{x}' \in I$, *either there exists an integer k such that* $\mathbf{S}_{\mathbf{x},*} = \omega_N^k \cdot \mathbf{S}_{\mathbf{x}',*}$ *or for every* $j \in [t]$,

$$\left\langle \mathbf{S}_{\mathbf{x},(j,*)}, \mathbf{S}_{\mathbf{x}',(j,*)} \right\rangle = 0;$$

($\mathcal{S}_3$) *For all* $\mathbf{y}, \mathbf{y}' \in J$, *either there exists an integer k such that* $\mathbf{S}_{*,\mathbf{y}} = \omega_N^k \cdot \mathbf{S}_{*,\mathbf{y}'}$ *or for every* $i \in [s]$,

$$\left\langle \mathbf{S}_{(i,*),\mathbf{y}}, \mathbf{S}_{(i,*),\mathbf{y}'} \right\rangle = 0.$$

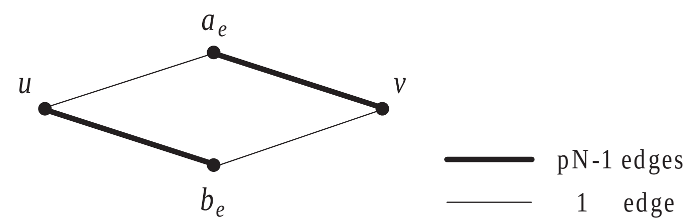

Figure 2: Gadget for constructing graph $G^{[p]}$, $p \geq 1$.

Proof. Assume $\mathsf{EVAL}(\mathbf{A})$ is not #P-hard. We only prove $(\mathcal{S}_2)$ here. $(\mathcal{S}_3)$ can be proved similarly.

Let $G = (V, E)$ be an undirected graph. For each $p \geq 1$, we construct a new graph $G^{[p]}$ by replacing every edge uv in E with a gadget which is shown in Figure 2.

More exactly, we define graph $G^{[p]} = (V^{[p]}, E^{[p]})$ as follows:

$$V^{[p]} = V \cup \big\{a_e, b_e \,\big|\, e \in E\big\}$$

and $E^{[p]}$ contains exactly the following edges: For each $e = uv \in E$,

1. one edge between (u, a_e) and (b_e, v);
2. $(pN - 1)$ edges between (a_e, v) and (u, b_e).

The construction of $G^{[p]}$, for each $p \geq 1$, gives us an $(m + n) \times (m + n)$ matrix $\mathbf{A}^{[p]}$ such that

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

Thus, we have $\mathsf{EVAL}(\mathbf{A}^{[p]}) \leq \mathsf{EVAL}(\mathbf{A})$, and $\mathsf{EVAL}(\mathbf{A}^{[p]})$ is also not #P-hard.

The entries of $\mathbf{A}^{[p]}$ are as follows. First,

$$A^{[p]}_{(0,\mathbf{u}),(1,\mathbf{v})} = A^{[p]}_{(1,\mathbf{v}),(0,\mathbf{u})} = 0, \quad \text{for all } \mathbf{u} \in I \text{ and } \mathbf{v} \in J.$$

So $\mathbf{A}^{[p]}$ is a block diagonal matrix with 2 blocks of $m \times m$ and $n \times n$, respectively. The entries in the upper-left $m \times m$ block are

$$\begin{aligned} A^{[p]}_{(0,\mathbf{u}),(0,\mathbf{v})} &= \left(\sum_{\mathbf{a} \in J} A_{(0,\mathbf{u}),(1,\mathbf{a})} (A_{(0,\mathbf{v}),(1,\mathbf{a})})^{pN-1}\right) \left(\sum_{\mathbf{b} \in J} (A_{(0,\mathbf{u}),(1,\mathbf{b})})^{pN-1} A_{(0,\mathbf{v}),(1,\mathbf{b})}\right) \\ &= \left(\sum_{\mathbf{a} \in J} B_{\mathbf{u},\mathbf{a}} (B_{\mathbf{v},\mathbf{a}})^{pN-1}\right) \left(\sum_{\mathbf{b} \in J} (B_{\mathbf{u},\mathbf{b}})^{pN-1} B_{\mathbf{v},\mathbf{b}}\right) \end{aligned}$$

for all $\mathbf{u}, \mathbf{v} \in I$. The first factor of the last expression is

$$\sum_{\mathbf{a} \in J} \mu_{u_1} \nu_{a_1} S_{\mathbf{u},\mathbf{a}} (\mu_{v_1} \nu_{a_1})^{pN-1} \overline{S_{\mathbf{v},\mathbf{a}}} = \mu_{u_1} \mu_{v_1}^{pN-1} \sum_{\mathbf{a} \in J} \nu_{a_1}^{pN} S_{\mathbf{u},\mathbf{a}} \overline{S_{\mathbf{v},\mathbf{a}}} = \mu_{u_1} \mu_{v_1}^{pN-1} \sum_{i \in [t]} \nu_i^{pN} \langle \mathbf{S}_{\mathbf{u},(i,*)}, \mathbf{S}_{\mathbf{v},(i,*)} \rangle.$$

Similarly, we have for the second factor

$$\sum_{\mathbf{b} \in J} (B_{\mathbf{u},\mathbf{b}})^{pN-1} B_{\mathbf{v},\mathbf{b}} = \mu_{u_1}^{pN-1} \mu_{v_1} \sum_{i \in [t]} \nu_i^{pN} \overline{\langle \mathbf{S}_{\mathbf{u},(i,*)}, \mathbf{S}_{\mathbf{v},(i,*)} \rangle}.$$

As a result,

$$A^{[p]}_{(0,\mathbf{u}),(0,\mathbf{v})} = (\mu_{u_1}\mu_{v_1})^{pN} \left| \sum_{i\in[t]} \nu_i^{pN} \langle \mathbf{S}_{\mathbf{u},(i,*)}, \mathbf{S}_{\mathbf{v},(i,*)} \rangle \right|^2 .$$

It is clear that the upper-left $m \times m$ block of $\mathbf{A}^{[p]}$ is a nonnegative real matrix. Similarly one can prove that the same holds for its lower-right $n \times n$ block, so $\mathbf{A}^{[p]}$ is a nonnegative real matrix.

Now let $\mathbf{u} \neq \mathbf{v}$ be two indices in I (note that if $|I| = 1$, then $(\mathcal{S}_2)$ is trivially true), then we have

$$A^{[p]}_{(0,\mathbf{u}),(0,\mathbf{u})} A^{[p]}_{(0,\mathbf{v}),(0,\mathbf{v})} = (\mu_{u_1}\mu_{v_1})^{2pN} \left(\sum_{i\in[t]} n_i \cdot \nu_i^{pN} \right)^4 ,$$

which is positive, and

$$A^{[p]}_{(0,\mathbf{u}),(0,\mathbf{v})} A^{[p]}_{(0,\mathbf{v}),(0,\mathbf{u})} = (\mu_{u_1}\mu_{v_1})^{2pN} \left| \sum_{i\in[t]} \nu_i^{pN} \langle \mathbf{S}_{\mathbf{u},(i,*)}, \mathbf{S}_{\mathbf{v},(i,*)} \rangle \right|^4 .$$

Since $\mathsf{EVAL}(\mathbf{A}^{[p]})$ is not #P-hard, by the dichotomy theorem of Bulatov and Grohe (Corollary 2.1),

$$\left| \sum_{i\in[t]} \nu_i^{pN} \langle \mathbf{S}_{\mathbf{u},(i,*)}, \mathbf{S}_{\mathbf{v},(i,*)} \rangle \right|$$

is either 0 or $\sum_{i\in[t]} n_i \cdot \nu_i^{pN}$.

Now suppose vectors $\mathbf{S}_{\mathbf{u},*}$ and $\mathbf{S}_{\mathbf{v},*}$ are linearly dependent, then because entries of $\mathbf{S}$ are all powers of ω_N, there must exist an integer $k \in [0 : N-1]$ such that $\mathbf{S}_{\mathbf{u},*} = \omega_N^k \cdot \mathbf{S}_{\mathbf{v},*}$, and we are done.

Otherwise, assuming $\mathbf{S}_{\mathbf{u},*}$ and $\mathbf{S}_{\mathbf{v},*}$ are linearly independent, we have

$$\left| \sum_{i\in[t]} \nu_i^{pN} \cdot \langle \mathbf{S}_{\mathbf{u},(i,*)}, \mathbf{S}_{\mathbf{v},(i,*)} \rangle \right| < \sum_{i\in[t]} n_i \cdot \nu_i^{pN}, \quad \text{for any } p \geq 1. \tag{27}$$

This is because, if the left-hand side is equal to the right-hand side, then $|\langle \mathbf{S}_{\mathbf{u},(i,*)}, \mathbf{S}_{\mathbf{v},(i,*)} \rangle| = n_i$ for all $i \in [t]$ and thus, $\mathbf{S}_{\mathbf{u},(i,*)} = \omega_N^{k_i} \cdot \mathbf{S}_{\mathbf{v},(i,*)}$ for some $k_i \in [0 : N-1]$. Moreover, these k_i's must be the same since we assumed (27) is an equality:

$$\left| \sum_{i\in[t]} \nu_i^{pN} n_i \cdot \omega_N^{k_i} \right| = \sum_{i\in[t]} n_i \cdot \nu_i^{pN}.$$

As a result, $\mathbf{S}_{\mathbf{u},*}$ and $\mathbf{S}_{\mathbf{v},*}$ are linearly dependent, which contradicts the assumption. By (27), we have

$$\sum_{i\in[t]} \nu_i^{pN} \langle \mathbf{S}_{\mathbf{u},(i,*)}, \mathbf{S}_{\mathbf{v},(i,*)} \rangle = 0, \quad \text{for all } p \geq 1.$$

Since $\nu_1 > \ldots > \nu_t$ is strictly decreasing, by using the Vandermonde matrix, we have

$$\langle \mathbf{S}_{\mathbf{u},(i,*)}, \mathbf{S}_{\mathbf{v},(i,*)} \rangle = 0, \quad \text{for all } i \in [t].$$

This finishes the proof of $(\mathcal{S}_2)$. □

We then have the following corollary:

Corollary 8.3. *For all $i \in [s]$ and $j \in [t]$, the rank of the $(i,j)^{th}$ block matrix $\mathbf{S}_{(i,*),(j,*)}$ of $\mathbf{S}$ has exactly the same rank as $\mathbf{S}$.*

Proof. Without loss of generality, we prove $\text{rank}(\mathbf{S}_{(1,*),(1,*)}) = \text{rank}(\mathbf{S})$.

First, we use Lemma 8.2 to show that

$$\text{rank}\begin{pmatrix} \mathbf{S}_{(1,*),(1,*)} \\ \mathbf{S}_{(2,*),(1,*)} \\ \vdots \\ \mathbf{S}_{(s,*),(1,*)} \end{pmatrix} = \text{rank}(\mathbf{S}).$$

To see this, we take any $h = \text{rank}(\mathbf{S})$ rows of $\mathbf{S}$ which are linearly independent. Since any two of them $\mathbf{S}_{\mathbf{x},(*,*)}$ and $\mathbf{S}_{\mathbf{y},(*,*)}$ are linearly independent, by condition $(\mathcal{S}_2)$, the two subvectors $\mathbf{S}_{\mathbf{x},(1,*)}$ and $\mathbf{S}_{\mathbf{y},(1,*)}$ are orthogonal. Therefore, the corresponding h rows of the matrix on the left-hand side are pairwise orthogonal, and the left-hand side is at least h. Of course it cannot be larger than h, so it is equal to h.

By using condition $(\mathcal{S}_3)$, we can similarly show that

$$\text{rank}(\mathbf{S}_{(1,*),(1,*)}) = \text{rank}\begin{pmatrix} \mathbf{S}_{(1,*),(1,*)} \\ \mathbf{S}_{(2,*),(1,*)} \\ \vdots \\ \mathbf{S}_{(s,*),(1,*)} \end{pmatrix}.$$

As a result, we have $\text{rank}(\mathbf{S}_{(1,*),(1,*)}) = \text{rank}(\mathbf{S})$. □

Now suppose $h = \text{rank}(\mathbf{S})$, then by Corollary 8.3, there must exist indices $1 \le i_1 < \ldots < i_h \le m_1$ and $1 \le j_1 < \ldots < j_h \le n_1$, such that, the $\{(1,i_1),\ldots,(1,i_h)\} \times \{(1,j_1),\ldots,(1,j_h)\}$ sub-matrix of $\mathbf{S}$ has full rank h. Without loss of generality (if this is not true, we can apply an appropriate permutation Π to the rows and columns of $\mathbf{A}$ so that the new $\mathbf{S}$ has this property) we assume $i_k = k$ and $j_k = k$ for all $k \in [h]$. We use $\mathbf{H}$ to denote this $h \times h$ matrix: $H_{i,j} = S_{(1,i),(1,j)}$.

By Corollary 8.3 and Lemma 8.2, for every index $\mathbf{x} \in I$, there exist two unique integers $j \in [h]$ and $k \in [0 : N-1]$ such that

$$\mathbf{S}_{\mathbf{x},*} = \omega_N^k \cdot \mathbf{S}_{(1,j),*}. \tag{28}$$

This gives us a partition of index set $\{0\} \times I$:

$$\mathscr{R}_0 = \left\{ R_{(0,i,j),k} \,\middle|\, i \in [s], j \in [h], k \in [0 : N-1] \right\},$$

as follows: For every $\mathbf{x} \in I$, $(0,\mathbf{x}) \in R_{(0,i,j),k}$ if $i = x_1$ and $\mathbf{x}, j, k$ satisfy (28). By Corollary 8.3, we have

$$\bigcup_{k \in [0:N-1]} R_{(0,i,j),k} \neq \emptyset, \quad \text{for all } i \in [s] \text{ and } j \in [h].$$

Similarly, for every $\mathbf{y} \in J$, there exist two unique integers $j \in [h]$ and $k \in [0 : N-1]$ such that

$$\mathbf{S}_{*,\mathbf{y}} = \omega_N^k \cdot \mathbf{S}_{*,(1,j)}, \tag{29}$$

and we partition $\{1\} \times J$ into

$$\mathscr{R}_1 = \left\{ R_{(1,i,j),k} \,\middle|\, i \in [t], j \in [h], k \in [0 : N-1] \right\},$$

as follows: For every $\mathbf{y} \in J$, $(1, \mathbf{y}) \in R_{(1,i,j),k}$ if $i = y_1$ and $\mathbf{y}, j, k$ satisfy (29). Again by Corollary 8.3,

$$\bigcup_{k \in [0:N-1]} R_{(1,i,j),k} \neq \emptyset, \quad \text{for all } i \in [t] \text{ and } j \in [h].$$

Now we define $(\mathbf{C}, \mathfrak{D})$ and use the Cyclotomic Reduction Lemma (Lemma 8.1) to show that

$$\mathsf{EVAL}(\mathbf{C}, \mathfrak{D}) \equiv \mathsf{EVAL}(\mathbf{A}).$$

First, $\mathbf{C}$ is an $(s+t)h \times (s+t)h$ matrix which is the bipartisation of an $sh \times th$ matrix $\mathbf{F}$. We use set $I' \equiv [s] \times [h]$ to index the rows of $\mathbf{F}$, and $J' \equiv [t] \times [h]$ to index the columns of $\mathbf{F}$. We have

$$F_{\mathbf{x},\mathbf{y}} = \mu_{x_1} \nu_{y_1} H_{x_2,y_2} = \mu_{x_1} \nu_{y_1} S_{(1,x_2),(1,y_2)}, \quad \text{for all } \mathbf{x} \in I', \, \mathbf{y} \in J',$$

or equivalently,

$$\mathbf{F} = \begin{pmatrix} \mu_1 \mathbf{I} & & & \\ & \mu_2 \mathbf{I} & & \\ & & \ddots & \\ & & & \mu_s \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{H} & \mathbf{H} & \ldots & \mathbf{H} \\ \mathbf{H} & \mathbf{H} & \ldots & \mathbf{H} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{H} & \mathbf{H} & \ldots & \mathbf{H} \end{pmatrix} \begin{pmatrix} \nu_1 \mathbf{I} & & & \\ & \nu_2 \mathbf{I} & & \\ & & \ddots & \\ & & & \nu_t \mathbf{I} \end{pmatrix},$$

where $\mathbf{I}$ is the $h \times h$ identity matrix. We use $(\{0\} \times I') \cup (\{1\} \times J')$ to index the rows/columns of $\mathbf{C}$.

Second, $\mathfrak{D} = \{\mathbf{D}^{[0]}, ..., \mathbf{D}^{[N-1]}\}$ is a sequence of N diagonal matrices of the same size as $\mathbf{C}$. We use $\{0\} \times I'$ to index the first sh diagonal entries, and $\{1\} \times J'$ to index the last th diagonal entries. Then the $(0, \mathbf{x})^{th}$ entries of $\mathfrak{D}$ are generated by $(|R_{(0,x_1,x_2),0}|, \ldots, |R_{(0,x_1,x_2),N-1}|)$ and the $(1, \mathbf{y})^{th}$ entries of $\mathfrak{D}$ are generated by $(|R_{(1,y_1,y_2),0}|, \ldots, |R_{(1,y_1,y_2),N-1}|)$:

$$D^{[r]}_{(0,\mathbf{x})} = \sum_{k=0}^{N-1} \left| R_{(0,x_1,x_2),k} \right| \cdot \omega_N^{kr} \quad \text{and} \quad D^{[r]}_{(1,\mathbf{y})} = \sum_{k=0}^{N-1} \left| R_{(1,y_1,y_2),k} \right| \cdot \omega_N^{kr},$$

for all $r \in [0 : N-1], \mathbf{x} = (x_1, x_2) \in I'$ and $\mathbf{y} = (y_1, y_2) \in J'$.

The following lemma is a direct application of the Cyclotomic Reduction Lemma (Lemma 8.1).

Lemma 8.3. $\mathsf{EVAL}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$.

Proof. First we show that $\mathbf{A}$ can be generated from $\mathbf{C}$ using $\mathscr{R}_0 \cup \mathscr{R}_1$.

Let $\mathbf{x}, \mathbf{x}' \in I$, $(0, \mathbf{x}) \in R_{(0,x_1,j),k}$ and $(0, \mathbf{x}') \in R_{(0,x'_1,j'),k'}$, then we have

$$A_{(0,\mathbf{x}),(0,\mathbf{x}')} = C_{(0,x_1,j),(0,x'_1,j')} = 0,$$

since $\mathbf{A}$ and $\mathbf{C}$ are the bipartisations of $\mathbf{B}$ and $\mathbf{F}$, respectively. As a result,

$$A_{(0,\mathbf{x}),(0,\mathbf{x}')} = C_{(0,x_1,j),(0,x'_1,j')} \cdot \omega_N^{k+k'}$$

holds trivially. Clearly, this is also true for the lower-right $n \times n$ block of $\mathbf{A}$.

Let $\mathbf{x} \in I$, $(0, \mathbf{x}) \in R_{(0,x_1,j),k}$, $\mathbf{y} \in J$, and $(1, \mathbf{y}) \in R_{(1,y_1,j'),k'}$ for some j, k, j', k', then by (28)-(29),

$$A_{(0,\mathbf{x}),(1,\mathbf{y})} = \mu_{x_1} \nu_{y_1} S_{\mathbf{x},\mathbf{y}} = \mu_{x_1} \nu_{y_1} S_{(1,j),\mathbf{y}} \cdot \omega_N^{k} = \mu_{x_1} \nu_{y_1} S_{(1,j),(1,j')} \cdot \omega_N^{k+k'} = C_{(0,x_1,j),(1,y_1,j')} \cdot \omega_N^{k+k'}.$$

A similar equation holds for the lower-left block of $\mathbf{A}$, so it can be generated from $\mathbf{C}$ using $\mathscr{R}_0 \cup \mathscr{R}_1$.

On the other hand, the construction of $\mathfrak{D}$ implies that $\mathfrak{D}$ can be generated from partition $\mathscr{R}_0 \cup \mathscr{R}_1$. The lemma then follows directly from the Cyclotomic Reduction Lemma. $\square$

8.3 Step 2.2

We first summarize what we proved in Step 2.1. We showed that problem $\mathsf{EVAL}(\mathbf{A})$ is either #P-hard or equivalent to $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$, where $(\mathbf{C},\mathfrak{D})$ satisfies the following condition (*Shape*):

($Shape_1$): $\mathbf{C}\in\mathbb{C}^{m\times m}$ (note that this m is different from the m used in Step 2.1) is the bipartisation of an $sh\times th$ matrix $\mathbf{F}$ (thus $m=(s+t)h$). $\mathbf{F}$ is an $s\times t$ block matrix and we use $I=[s]\times[h]$, $J=[t]\times[h]$ to index the rows and columns of $\mathbf{F}$, respectively.

($Shape_2$): There are two sequences $\boldsymbol{\mu}=\{\mu_1>\ldots>\mu_s>0\}$ and $\boldsymbol{\nu}=\{\nu_1>\ldots>\nu_t>0\}$ of rational numbers together with an $h\times h$ full-rank matrix $\mathbf{H}$ whose entries are all powers of ω_N, for some positive integer N. For all $\mathbf{x}\in I$ and $\mathbf{y}\in J$, we have

$$F_{\mathbf{x},\mathbf{y}}=\mu_{x_1}\nu_{y_1}H_{x_2,y_2}.$$

($Shape_3$): $\mathfrak{D}=\{\mathbf{D}^{[0]},\ldots,\mathbf{D}^{[N-1]}\}$ is a sequence of $m\times m$ diagonal matrices. $\mathfrak{D}$ satisfies $(\mathcal{T}_3)$, so

$$D^{[r]}_{(0,\mathbf{x})}=\overline{D^{[N-r]}_{(0,\mathbf{x})}}\ \text{ and }\ D^{[r]}_{(1,\mathbf{y})}=\overline{D^{[N-r]}_{(1,\mathbf{y})}},\quad\text{for all } r\in[N-1],\ \mathbf{x}\in[s]\times[h] \text{ and } \mathbf{y}\in[t]\times[h].$$

We use $(\{0\}\times I)\cup(\{1\}\times J)$ to index the rows and columns of matrices $\mathbf{C}$ and $\mathbf{D}^{[r]}$.

Now in Step 2.2, we prove the following lemma:

Lemma 8.4. *Either* $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ *is #P-hard, or* $\mathbf{H}$ *and* $\mathbf{D}^{[0]}$ *satisfy the following two conditions:*

($Shape_4$)*:* $\frac{1}{\sqrt{n}}\cdot\mathbf{H}$ is a unitary matrix: $\langle\mathbf{H}_{i,*},\mathbf{H}_{j,*}\rangle=\langle\mathbf{H}_{*,i},\mathbf{H}_{*,j}\rangle=0$ for all $i\neq j\in[h]$.

($Shape_5$)*:* $\mathbf{D}^{[0]}$ *satisfies* $D^{[0]}_{(0,\mathbf{x})}=D^{[0]}_{(0,(x_1,1))}$ *for all* $\mathbf{x}\in I$*, and* $D^{[0]}_{(1,\mathbf{y})}=D^{[0]}_{(1,(y_1,1))}$ *for all* $\mathbf{y}\in J$*.*

Proof. We rearrange the diagonal entries of $\mathbf{D}^{[0]}$ indexed by $\{1\}\times J$ into a $t\times h$ matrix $\mathbf{X}$:

$$X_{i,j}=D^{[0]}_{(1,(i,j))},\quad\text{for all } i\in[t] \text{ and } j\in[h],$$

and its diagonal entries indexed by $\{0\}\times I$ into an $s\times h$ matrix $\mathbf{Y}$:

$$Y_{i,j}=D^{[0]}_{(0,(i,j))},\quad\text{for all } i\in[s] \text{ and } j\in[h].$$

Note that by condition $(\mathcal{T}_3)$, all entries of $\mathbf{X}$ and $\mathbf{Y}$ are positive integers.

The proof has two stages: First, we show in Lemma 8.5 that, either $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ is #P-hard, or

$$\langle\mathbf{H}_{i,*}\circ\overline{\mathbf{H}_{j,*}},\mathbf{X}_{k,*}\rangle=0,\quad\text{for all } k\in[t] \text{ and } i\neq j\in[h],\quad\text{and}\tag{30}$$

$$\langle\mathbf{H}_{*,i}\circ\overline{\mathbf{H}_{*,j}},\mathbf{Y}_{k,*}\rangle=0,\quad\text{for all } k\in[s] \text{ and } i\neq j\in[h].\tag{31}$$

We use U to denote the set of h-dimensional vectors that are orthogonal to

$$\mathbf{H}_{1,*}\circ\overline{\mathbf{H}_{2,*}},\ \mathbf{H}_{1,*}\circ\overline{\mathbf{H}_{3,*}},\ \ldots,\ \mathbf{H}_{1,*}\circ\overline{\mathbf{H}_{h,*}}.$$

The above set of $h-1$ vectors is linearly independent. This is because

$$\sum_{i=2}^{h}a_i\big(\mathbf{H}_{1,*}\circ\overline{\mathbf{H}_{i,*}}\big)=\mathbf{H}_{1,*}\circ\left(\sum_{i=2}^{h}a_i\overline{\mathbf{H}_{i,*}}\right),$$

and if $\sum_{i=2}^{h} a_i(\mathbf{H}_{1,*} \circ \overline{\mathbf{H}_{i,*}}) = \mathbf{0}$, then $\sum_{i=2}^{h} a_i\overline{\mathbf{H}_{i,*}} = \mathbf{0}$ since all entries of $\mathbf{H}_{1,*}$ are nonzero. Because $\mathbf{H}$ has full rank, we have $a_i = 0$, $i = 2, \ldots, h$. As a result, U is a linear space of dimension 1 over $\mathbb{C}$.

In the second stage, we show in Lemma 8.6 that, assuming (30) and (31), either

$$\langle \mathbf{H}_{i,*} \circ \overline{\mathbf{H}_{j,*}}, (\mathbf{X}_{k,*})^2 \rangle = 0, \quad \text{for all } k \in [t] \text{ and } i \neq j \in [h], \quad \text{and} \tag{32}$$

$$\langle \mathbf{H}_{*,i} \circ \overline{\mathbf{H}_{*,j}}, (\mathbf{Y}_{k,*})^2 \rangle = 0, \quad \text{for all } k \in [s] \text{ and } i \neq j \in [h], \tag{33}$$

or $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is #P-hard. Here we use $(\mathbf{X}_{k,*})^2$ to denote $\mathbf{X}_{k,*} \circ \mathbf{X}_{k,*}$.

(30) and (32) then imply that both $\mathbf{X}_{k,*}$ and $(\mathbf{X}_{k,*})^2$ are in U and thus, they are linearly dependent (since the dimension of U is 1). On the other hand, by $(\mathcal{T}_3)$, every entry in $\mathbf{X}_{k,*}$ is a positive integer. Therefore, $\mathbf{X}_{k,*}$ must have the form $u \cdot \mathbf{1}$, for some positive integer u. The same argument works for $\mathbf{Y}_{k,*}$ and the latter must also have the form $u' \cdot \mathbf{1}$. By (30) and (31), this further implies that

$$\langle \mathbf{H}_{i,*}, \mathbf{H}_{j,*} \rangle = 0 \ \text{ and } \ \langle \mathbf{H}_{*,i}, \mathbf{H}_{*,j} \rangle = 0, \quad \text{for all } i \neq j \in [h].$$

This finishes the proof of Lemma 8.4. □

Now we proceed to the two stages of the proof. In the first stage, we prove the following lemma:

Lemma 8.5. *Either matrices* $\mathbf{H}$, $\mathbf{X}$ *and* $\mathbf{Y}$ *satisfy* (30) *and* (31), *or* $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ *is #P-hard.*

Proof. Suppose problem $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is not #P-hard, otherwise we are already done. We let $\mathfrak{D}^*$ denote a sequence of N $m \times m$ diagonal matrices in which every matrix is a copy of $\mathbf{D}^{[0]}$ (as in $\mathfrak{D}$):

$$\mathfrak{D}^* = \{\mathbf{D}^{[0]}, \ldots, \mathbf{D}^{[0]}\}.$$

It is easy to check that $\mathfrak{D}^*$ satisfies condition $(\mathcal{T}_3)$.

Let $G = (V, E)$ be an undirected graph. For each $p \geq 1$, we build a new graph $G^{[p]} = (V^{[p]}, E^{[p]})$ in the same way as we did in the proof of Lemma 8.2. This gives us an $m \times m$ matrix $\mathbf{C}^{[p]}$ such that

$$Z_{\mathbf{C}^{[p]}, \mathfrak{D}^*}(G) = Z_{\mathbf{C}, \mathfrak{D}}(G^{[p]}), \quad \text{for all undirected graphs } G,$$

and thus, $\mathsf{EVAL}(\mathbf{C}^{[p]}, \mathfrak{D}^*) \leq \mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$, and $\mathsf{EVAL}(\mathbf{C}^{[p]}, \mathfrak{D}^*)$ is also not #P-hard.

Matrix $\mathbf{C}^{[p]}$ is a block matrix which has the same block dimension structure as $\mathbf{C}$. The upper-right and lower-left blocks of $\mathbf{C}^{[p]}$ are zero matrices. For $\mathbf{x}, \mathbf{y} \in I$, we have

$$C^{[p]}_{(0,\mathbf{x}),(0,\mathbf{y})} = \left(\sum_{\mathbf{a} \in J} F_{\mathbf{x},\mathbf{a}} (F_{\mathbf{y},\mathbf{a}})^{pN-1} X_{a_1,a_2} \right) \left(\sum_{\mathbf{b} \in J} (F_{\mathbf{x},\mathbf{b}})^{pN-1} F_{\mathbf{y},\mathbf{b}} X_{b_1,b_2} \right).$$

By (*Shape*$_2$) and the fact that all entries of $\mathbf{X}$ are positive integers, we can rewrite the first factor as

$$\mu_{x_1} (\mu_{y_1})^{pN-1} \sum_{\mathbf{a} \in J} (\nu_{a_1})^{pN} H_{x_2,a_2} \overline{H_{y_2,a_2}} X_{a_1,a_2} = \mu_{x_1} (\mu_{y_1})^{pN-1} \sum_{a \in [t]} (\nu_a)^{pN} \langle \mathbf{H}_{x_2,*} \circ \overline{\mathbf{H}_{y_2,*}}, \mathbf{X}_{a,*} \rangle.$$

Similarly, we have

$$(\mu_{x_1})^{pN-1} \mu_{y_1} \sum_{a \in [t]} (\nu_a)^{pN} \overline{\langle \mathbf{H}_{x_2,*} \circ \overline{\mathbf{H}_{y_2,*}}, \mathbf{X}_{a,*} \rangle}$$

for the second factor. Since $\nu_a > 0$ for all a, we have

$$C^{[p]}_{(0,\mathbf{x}),(0,\mathbf{y})} = (\mu_{x_1} \mu_{y_1})^{pN} \left| \sum_{a \in [t]} (\nu_a)^{pN} \langle \mathbf{H}_{x_2,*} \circ \overline{\mathbf{H}_{y_2,*}}, \mathbf{X}_{a,*} \rangle \right|^2, \tag{34}$$

so the upper-left block of $\mathbf{C}^{[p]}$ is a nonnegative real matrix. Similarly one can show that the same holds for its lower-right block, so $\mathbf{C}^{[p]}$ is a nonnegative real matrix.

Now for any $\mathbf{x} \neq \mathbf{y} \in I$, we have

$$C^{[p]}_{(0,\mathbf{x}),(0,\mathbf{x})} = (\mu_{x_1})^{2pN} \left(\sum_{a\in[t]} (\nu_a)^{pN} \sum_{b\in[h]} X_{a,b} \right)^2 \text{ and } C^{[p]}_{(0,\mathbf{y}),(0,\mathbf{y})} = (\mu_{y_1})^{2pN} \left(\sum_{a\in[t]} (\nu_a)^{pN} \sum_{b\in[h]} X_{a,b} \right)^2,$$

which are positive, and

$$C^{[p]}_{(0,\mathbf{x}),(0,\mathbf{x})} C^{[p]}_{(0,\mathbf{y}),(0,\mathbf{y})} = (\mu_{x_1}\mu_{y_1})^{2pN} \left(\sum_{a\in[t]} (\nu_a)^{pN} \sum_{b\in[h]} X_{a,b} \right)^4 > 0.$$

Since $\mathsf{EVAL}(\mathbf{C}^{[p]}, \mathfrak{D}^*)$ is not #P-hard and $(\mathbf{C}^{[p]}, \mathfrak{D}^*)$ satisfies $(\mathcal{T})$, by the Inverse Cyclotomic Reduction Lemma (Corollary 8.1), we have

$$\text{either } \left(C^{[p]}_{(0,\mathbf{x}),(0,\mathbf{y})}\right)^2 = C^{[p]}_{(0,\mathbf{x}),(0,\mathbf{x})} C^{[p]}_{(0,\mathbf{y}),(0,\mathbf{y})} \text{ or } C^{[p]}_{(0,\mathbf{x}),(0,\mathbf{y})} = 0.$$

We claim that if the former is true, then we must have $x_2 = y_2$. This is because, in this case, we have

$$\left| \sum_{a\in[t]} (\nu_a)^{pN} \langle \mathbf{H}_{x_2,*} \circ \overline{\mathbf{H}_{y_2,*}}, \mathbf{X}_{a,*} \rangle \right| = \sum_{a\in[t]} (\nu_a)^{pN} \sum_{b\in[h]} X_{a,b},$$

and the norm of $\langle \mathbf{H}_{x_2,*} \circ \overline{\mathbf{H}_{y_2,*}}, \mathbf{X}_{a,*} \rangle$ must be $\sum_{b\in[h]} X_{a,b}$. However the inner product is a sum of $X_{a,b}$'s weighted by roots of unity, so the entries of $\mathbf{H}_{x_2,*} \circ \overline{\mathbf{H}_{y_2,*}}$ must be the same root of unity. Thus, $\mathbf{H}_{x_2,*}$ and $\mathbf{H}_{y_2,*}$ are linearly dependent. Since $\mathbf{H}$ is a matrix of full rank, we conclude that $x_2 = y_2$.

In other words, if $x_2 \neq y_2$, then we have $C^{[p]}_{(0,\mathbf{x}),(0,\mathbf{y})} = 0$ and thus,

$$\sum_{a\in[t]} (\nu_a)^{pN} \langle \mathbf{H}_{x_2,*} \circ \overline{\mathbf{H}_{y_2,*}}, \mathbf{X}_{a,*} \rangle = 0, \quad \text{for all } p \geq 1 \text{ and all } x_2 \neq y_2,$$

since the argument has nothing to do with p. By using the Vandermonde matrix, we have

$$\langle \mathbf{H}_{x_2,*} \circ \overline{\mathbf{H}_{y_2,*}}, \mathbf{X}_{a,*} \rangle = 0, \quad \text{for all } a \in [t] \text{ and all } x_2 \neq y_2.$$

This finishes the proof of (30). (31) can be proved similarly. □

In the second stage, we prove the following lemma:

Lemma 8.6. *Suppose matrices* $\mathbf{H}$, $\mathbf{X}$ *and* $\mathbf{Y}$ *satisfy both* (30) *and* (31)*. Then either they also satisfy* (32) *and* (33)*, or* $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ *is #P-hard.*

Proof. We will only prove (33). (32) can be proved similarly. Again, we let $\mathfrak{D}^*$ to denote a sequence of N $m \times m$ diagonal matrices in which every matrix is a copy of $\mathbf{D}^{[0]}$ ($\mathfrak{D}^*$ satisfies $(\mathcal{T}_3)$).

Before starting the proof we note the following property of the matrix $\mathbf{C}^{[1]}$ which we used in the proof of Lemma 8.5 since we need it to prove (33) here: When $x_2 = y_2$, by (34), we have

$$C^{[1]}_{(0,\mathbf{x}),(0,\mathbf{y})} = (\mu_{x_1}\mu_{y_1})^N \left(\sum_{a\in[t]} (\nu_a)^N \sum_{b\in[h]} X_{a,b} \right)^2,$$

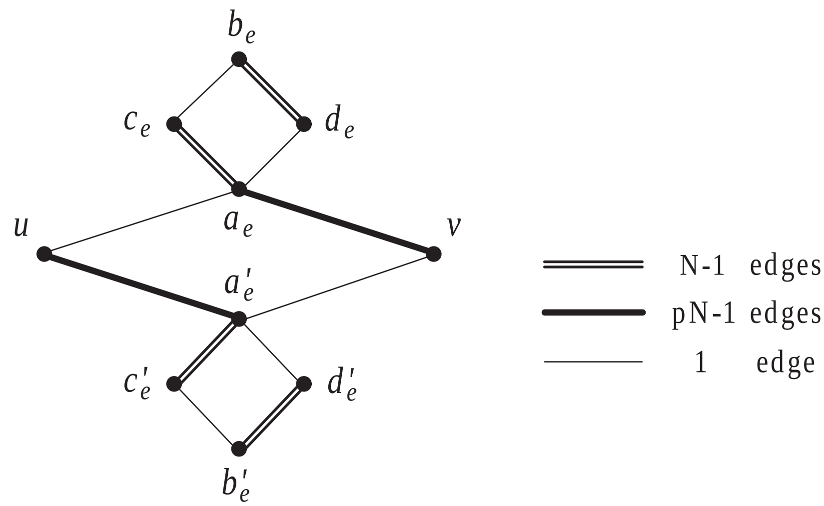

Figure 3: Gadget for constructing $G^{(p)}$, $p \geq 1$.

and is equal to 0 when $x_2 \neq y_2$. We use L to denote the second factor on the right-hand side, which is independent of $\mathbf{x}$ and $\mathbf{y}$, so the right-hand side becomes $(\mu_{x_1}\mu_{y_1})^N \cdot L$.

Additionally, because of (31), we have $\mathbf{Y}_{k,*}$ and $\mathbf{Y}_{1,*}$ are linearly dependent for every k. Thus there exists a positive rational number λ_k such that

$$\mathbf{Y}_{k,*} = \lambda_k \cdot \mathbf{Y}_{1,*}, \quad \text{for all } k \in [s]. \tag{35}$$

Because of this, we only need to prove (33) for the case when $k = 1$.

Now we start the proof of (33). Suppose $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is not #P-hard. We use $G = (V, E)$ to denote an undirected graph, then for each $p \geq 1$, we build a new graph $G^{(p)} = (V^{(p)}, E^{(p)})$ by replacing every edge $e = uv \in E$ with a gadget which is shown in Figure 3.

More exactly, we define $G^{(p)} = (V^{(p)}, E^{(p)})$ as follows:

$$V^{(p)} = V \cup \big\{ a_e, b_e, c_e, d_e, a'_e, b'_e, c'_e, d'_e \;\big|\; e \in E \big\},$$

and $E^{(p)}$ contains exactly the following edges: For every edge $e = uv \in E$,

1. One edge between $(u, a_e), (a'_e, v), (c_e, b_e), (d_e, a_e), (c'_e, b'_e)$ and (d'_e, a'_e);
2. $pN - 1$ edges between (a_e, v) and (u, a'_e);
3. $N - 1$ edges between $(a_e, c_e), (b_e, d_e), (a'_e, c'_e)$ and (b'_e, d'_e).

It is easy to check that the degree of every vertex in $G^{(p)}$ is a multiple of N.

Moreover, the construction of $G^{(p)}$ gives us a new $m \times m$ matrix $\mathbf{R}^{(p)}$ which is symmetric since the gadget is symmetric, such that

$$Z_{\mathbf{R}^{(p)}, \mathfrak{D}^*}(G) = Z_{\mathbf{C}, \mathfrak{D}}(G^{(p)}), \quad \text{for all undirected graphs } G$$

and thus, $\mathsf{EVAL}(\mathbf{R}^{(p)}, \mathfrak{D}^*) \leq \mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$, and $\mathsf{EVAL}(\mathbf{R}^{(p)}, \mathfrak{D}^*)$ is also not #P-hard.

The matrix $\mathbf{R}^{(p)}$ is a block matrix which has the same block dimension structure as $\mathbf{C}$. The upper-right and lower-left blocks of $\mathbf{R}^{(p)}$ are zero matrices. The entries in its lower-right block are as follows:

$$R^{(p)}_{(1,\mathbf{x}),(1,\mathbf{y})} = \left(\sum_{\mathbf{a},\mathbf{b}\in I} F_{\mathbf{a},\mathbf{x}}(F_{\mathbf{a},\mathbf{y}})^{pN-1} C^{[1]}_{(0,\mathbf{a}),(0,\mathbf{b})} Y_{a_1,a_2} Y_{b_1,b_2}\right)\left(\sum_{\mathbf{a},\mathbf{b}\in I} (F_{\mathbf{a},\mathbf{x}})^{pN-1} F_{\mathbf{a},\mathbf{y}} C^{[1]}_{(0,\mathbf{a}),(0,\mathbf{b})} Y_{a_1,a_2} Y_{b_1,b_2}\right)$$

for $\mathbf{x},\mathbf{y}\in J$. Firstly, by (35), we have $Y_{a_1,a_2}Y_{b_1,b_2} = \lambda_{a_1}\lambda_{b_1}Y_{1,a_2}Y_{1,b_2}$. Secondly, we have

$$C^{[1]}_{(0,\mathbf{a}),(0,\mathbf{b})} = 0, \quad \text{whenever } a_2 \neq b_2.$$

As a result, we can simplify the first factor to be

$$\begin{aligned}
&\nu_{x_1}(\nu_{y_1})^{pN-1} L \cdot \sum_{\mathbf{a},\mathbf{b}\in I, a_2=b_2} (\mu_{a_1})^{pN} H_{a_2,x_2}\overline{H_{a_2,y_2}} (\mu_{a_1}\mu_{b_1})^N \lambda_{a_1}\lambda_{b_1} Y_{1,a_2}Y_{1,b_2}\\
&= \nu_{x_1}(\nu_{y_1})^{pN-1} L \cdot \sum_{a_1,b_1\in[s]} (\mu_{a_1})^{(p+1)N}(\mu_{b_1})^N \lambda_{a_1}\lambda_{b_1} \sum_{a_2\in[h]} H_{a_2,x_2}\overline{H_{a_2,y_2}}(Y_{1,a_2})^2\\
&= \nu_{x_1}(\nu_{y_1})^{pN-1} L' \cdot \langle \mathbf{H}_{*,x_2}\circ \overline{\mathbf{H}_{*,y_2}}, (\mathbf{Y}_{1,*})^2\rangle,
\end{aligned}$$

where

$$L' = L \sum_{a_1,b_1\in[s]} (\mu_{a_1})^{(p+1)N}(\mu_{b_1})^N \lambda_{a_1}\lambda_{b_1}$$

is a positive number that is independent from $\mathbf{x},\mathbf{y}$. Similarly the second factor can be simplified to be

$$(\nu_{x_1})^{pN-1}\nu_{y_1} L' \cdot \overline{\langle \mathbf{H}_{*,x_2}\circ \overline{\mathbf{H}_{*,y_2}}, (\mathbf{Y}_{1,*})^2\rangle}.$$

As a result, we have

$$R^{(p)}_{(1,\mathbf{x}),(1,\mathbf{y})} = (L')^2 \cdot (\nu_{x_1}\nu_{y_1})^{pN} \cdot \left|\langle \mathbf{H}_{*,x_2}\circ \overline{\mathbf{H}_{*,y_2}}, (\mathbf{Y}_{1,*})^2\rangle\right|^2.$$

Thus the lower-right block of $\mathbf{R}^{(p)}$ is non-negative. Similarly one can prove that the same holds for its upper-left block, so $\mathbf{R}^{(p)}$ is non-negative.

We now apply Corollary 8.1 to $(\mathbf{R}^{(p)}, \mathfrak{D}^*)$. Since $\mathsf{EVAL}(\mathbf{R}^{(p)}, \mathfrak{D}^*)$ is not #P-hard, we have

$$\text{either } \left(R^{(p)}_{(1,\mathbf{x}),(1,\mathbf{y})}\right)^2 = R^{(p)}_{(1,\mathbf{x}),(1,\mathbf{x})} R^{(p)}_{(1,\mathbf{y}),(1,\mathbf{y})} \text{ or } R^{(p)}_{(1,\mathbf{x}),(1,\mathbf{y})} = 0, \quad \text{for any } \mathbf{x}\neq\mathbf{y}\in J.$$

We claim that if the former is true, then we must have $x_2 = y_2$. This is because, in this case,

$$\left|\langle \mathbf{H}_{*,x_2}\circ \overline{\mathbf{H}_{*,y_2}}, (\mathbf{Y}_{1,*})^2\rangle\right| = \sum_{i\in[h]} Y^2_{1,i}.$$

However, the left-hand side is a sum of $(Y_{1,i})^2$'s, which are positive integers, weighted by roots of unity. To sum to a number of norm $\sum_{i\in[h]} Y^2_{1,i}$ the entries of $\mathbf{H}_{*,x_2}\circ\overline{\mathbf{H}_{*,y_2}}$ must be the same root of unity. As a result, $\mathbf{H}_{*,x_2}$ and $\mathbf{H}_{*,y_2}$ are linearly dependent. Since $\mathbf{H}$ is of full rank, we conclude that $x_2 = y_2$. In other words, we have shown that

$$\langle \mathbf{H}_{*,x_2}\circ \overline{\mathbf{H}_{*,y_2}}, (\mathbf{Y}_{1,*})^2\rangle = 0, \quad \text{for all } x_2\neq y_2.$$

By combining it with (35), we have finished the proof of (33). ∎

8.4 Step 2.3

Now we have a pair $(\mathbf{C},\mathfrak{D})$ that satisfies conditions ($Shape_1$)-($Shape_5$) since otherwise, by Lemma 8.4, $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ is #P-hard and we are done.

In particular, by using ($Shape_5$) we define two diagonal matrices $\mathbf{K}^{[0]}$ and $\mathbf{L}^{[0]}$ as follows. $\mathbf{K}^{[0]}$ is an $(s+t)\times(s+t)$ diagonal matrix. We use $(0,i)$, where $i\in[s]$, to index the first s rows, and $(1,j)$, where $j\in[t]$, to index the last t rows of $\mathbf{K}^{[0]}$. The diagonal entries of $\mathbf{K}^{[0]}$ are

$$K^{[0]}_{(0,i)}=D^{[0]}_{(0,(i,1))}\quad\text{and}\quad K^{[0]}_{(1,j)}=D^{[0]}_{(1,(j,1))},\quad\text{for all } i\in[s] \text{ and } j\in[t].$$

The matrix $\mathbf{L}^{[0]}$ is the $2h\times 2h$ identity matrix. We use $(0,i)$, where $i\in[h]$, to index the first h rows, and $(1,j)$, where $j\in[h]$, to index the last h rows of $\mathbf{L}^{[0]}$. By ($Shape_5$), we have

$$D^{[0]}_{(0,\mathbf{x})}=K^{[0]}_{(0,x_1)}\cdot L^{[0]}_{(0,x_2)}\quad\text{and}\quad D^{[0]}_{(1,\mathbf{y})}=K^{[0]}_{(1,y_1)}\cdot L^{[0]}_{(1,y_2)},\quad\text{for all } \mathbf{x}\in I \text{ and } \mathbf{y}\in J. \tag{36}$$

or equivalently,

$$\mathbf{D}^{[0]}=\begin{pmatrix}\mathbf{D}^{[0]}_{(0,*)} & \\ & \mathbf{D}^{[0]}_{(1,*)}\end{pmatrix}=\begin{pmatrix}\mathbf{K}^{[0]}_{(0,*)}\otimes\mathbf{L}^{[0]}_{(0,*)} & \\ & \mathbf{K}^{[0]}_{(1,*)}\otimes\mathbf{L}^{[0]}_{(1,*)}\end{pmatrix}. \tag{37}$$

The main target of this step is to prove a similar statement for $\mathbf{D}^{[r]}$, $r\in[N-1]$. These equations will allow us to decompose, in Step 2.4, the problem $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ into two subproblems.

In the proof of Lemma 8.4, we crucially used the property (from ($\mathcal{T}_3$)) that all the diagonal entries of $\mathbf{D}^{[0]}$ are positive integers. However, for $r\ge 1$, ($\mathcal{T}_3$) only gives us some very weak properties about $\mathbf{D}^{[r]}$. For example, the entries are not guaranteed to be real numbers. So the proof that we are going to present here is, as one might expect, much more complicated. We prove the following lemma:

Lemma 8.7. *Let $(\mathbf{C},\mathfrak{D})$ be a pair that satisfies conditions ($Shape_1$)-($Shape_5$), then either the problem $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ is #P-hard, or it satisfies the following condition:*

($Shape_6$): There exist diagonal matrices $\mathbf{K}^{[0]}$ and $\mathbf{L}^{[0]}$ such that $\mathbf{D}^{[0]},\mathbf{K}^{[0]}$ and $\mathbf{L}^{[0]}$ satisfy (37). Every entry of $\mathbf{K}^{[0]}$ is a positive integer, and $\mathbf{L}^{[0]}$ is the $2h\times 2h$ identity matrix. For every $r\in[N-1]$, there exist two diagonal matrices: $\mathbf{K}^{[r]}$ and $\mathbf{L}^{[r]}$. $\mathbf{K}^{[r]}$ is an $(s+t)\times(s+t)$ matrix, and $\mathbf{L}^{[r]}$ is a $2h\times 2h$ matrix. We index $\mathbf{K}^{[r]}$ and $\mathbf{L}^{[r]}$ in the same way we index $\mathbf{K}^{[0]}$ and $\mathbf{L}^{[0]}$, respectively, and

$$\mathbf{D}^{[r]}=\begin{pmatrix}\mathbf{D}^{[r]}_{(0,*)} & \\ & \mathbf{D}^{[r]}_{(1,*)}\end{pmatrix}=\begin{pmatrix}\mathbf{K}^{[r]}_{(0,*)}\otimes\mathbf{L}^{[r]}_{(0,*)} & \\ & \mathbf{K}^{[r]}_{(1,*)}\otimes\mathbf{L}^{[r]}_{(1,*)}\end{pmatrix}.$$

Moreover, the norm of every diagonal entry in $\mathbf{L}^{[r]}$ is either 0 or 1, and for any $r\in[N-1]$,

$$\mathbf{K}^{[r]}_{(0,*)}=\mathbf{0}\iff\mathbf{L}^{[r]}_{(0,*)}=\mathbf{0}\quad\textit{and}\quad\mathbf{K}^{[r]}_{(1,*)}=\mathbf{0}\iff\mathbf{L}^{[r]}_{(1,*)}=\mathbf{0};$$
$$\mathbf{L}^{[r]}_{(0,*)}\ne\mathbf{0}\implies\exists i\in[h],\ L^{[r]}_{(0,i)}=1\quad\textit{and}\quad\mathbf{L}^{[r]}_{(1,*)}\ne\mathbf{0}\implies\exists i\in[h],\ L^{[r]}_{(1,i)}=1.$$

We now present the proof of Lemma 8.7. Fix an $r\in[N-1]$ to be any index. We use the following notation. Consider the diagonal matrix $\mathbf{D}^{[r]}$. This matrix has two parts:

$$\mathbf{D}^{[r]}_{(0,*)}\in\mathbb{C}^{sh\times sh}\quad\text{and}\quad\mathbf{D}^{[r]}_{(1,*)}\in\mathbb{C}^{th\times th}.$$

The first part has s blocks where each block is a diagonal matrix with h entries. We will rearrange the entries indexed by $(0,*)$ into another matrix which we will denote as $\mathbf{D}$ (just like what we did to $\mathbf{D}^{[0]}$

in the proof of Lemma 8.4), where its i-th row $\mathbf{D}_{i,*}$, for $i \in [s]$, denotes the values of the i-th block and the j-th entry of the i-th row $D_{i,j}$, for $j \in [h]$, denotes the j-th entry of that i-th block. More exactly,

$$D_{i,j} = D^{[r]}_{(0,(i,j))}, \quad \text{for all } i \in [s] \text{ and } j \in [h].$$

We prove the following lemma in Section 8.4.2. A similar statement can be proved for $\mathbf{D}^{[r]}_{(1,*)}$.

Lemma 8.8. *Either problem* $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ *is #P-hard; or*

– $\text{rank}(\mathbf{D})$ *is at most* 1*, and for any* $i, j, j' \in [h]$*, if* $D_{i,j} \neq 0$ *and* $D_{i,j'} \neq 0$*, then* $|D_{i,j}| = |D_{i,j'}|$.

We now use it to prove the first half of Lemma 8.7, that is, there exist $\mathbf{K}^{[r]}_{(0,*)}$ and $\mathbf{L}^{[r]}_{(0,*)}$ such that

$$\mathbf{D}^{[r]}_{(0,*)} = \mathbf{K}^{[r]}_{(0,*)} \otimes \mathbf{L}^{[r]}_{(0,*)}. \tag{38}$$

Assume $\mathbf{D}^{[r]}_{(0,*)}$ is non-zero (otherwise, the lemma is trivially true by setting $\mathbf{K}^{[r]}_{(0,*)}$ and $\mathbf{L}^{[r]}_{(0,*)}$ to be zero). Let a be an index in $[s]$ and b be an index in $[h]$ such that $D_{a,b} \neq 0$. By Lemma 8.8, we know the rank of $\mathbf{D}$ is 1, so $\mathbf{D}_{i,*} = (D_{i,b}/D_{a,b}) \cdot \mathbf{D}_{a,*}$, for any $i \in [s]$. Then it is clear that, by setting

$$K^{[r]}_{(0,i)} = D_{i,b}, \quad \text{and} \quad L^{[r]}_{(0,j)} = \frac{D_{a,j}}{D_{a,b}},$$

we have

$$D^{[r]}_{(0,(i,j))} = D_{i,j} = K^{[r]}_{(0,i)} \cdot L^{[r]}_{(0,j)}, \quad \text{for all } i \in [s] \text{ and } j \in [h],$$

and (38) follows. The existence of matrices $\mathbf{K}^{[r]}_{(1,*)}$ and $\mathbf{L}^{[r]}_{(1,*)}$ can be proved similarly.

One can also check that $\mathbf{K}^{[r]}$ and $\mathbf{L}^{[r]}$ satisfy all the properties stated in (Shape_6). This finishes the proof of Lemma 8.7 (assuming Lemma 8.8).

8.4.1 The Vanishing Lemma

We will use the following Vanishing Lemma in the proof of Lemma 8.8.

Lemma 8.9 (Vanishing Lemma)**.** *Let k be a positive integer and $\{x_{i,n}\}_{n\geq 1}$, for $1 \leq i \leq k$, be k infinite sequences of non-zero real numbers. For notational uniformity we also denote by $\{x_{0,n}\}_{n\geq 1}$ the sequence where $x_{0,n} = 1$ for all $n \geq 1$. Suppose*

$$\lim_{n\to\infty} \frac{x_{i+1,n}}{x_{i,n}} = 0, \quad \text{for } 0 \leq i < k.$$

Part A: *Let a_i and $b_i \in \mathbb{C}$, for $0 \leq i \leq k$. Suppose for some $1 \leq \ell \leq k$, $a_i = b_i$ for all $0 \leq i < \ell$ and $a_0 = b_0 = 1$. Also suppose $\text{Im}(a_\ell) = \text{Im}(b_\ell)$. If for infinitely many n,*

$$\left|\sum_{i=0}^{k} a_i x_{i,n}\right| = \left|\sum_{i=0}^{k} b_i x_{i,n}\right|,$$

then $a_\ell = b_\ell$.

Part B: *Let $a_i \in \mathbb{C}$, for $0 \leq i \leq k$. Suppose for infinitely many n,*

$$\left|\sum_{i=0}^{k} a_i x_{i,n}\right| = 0,$$

then $a_i = 0$ for all $0 \leq i \leq k$.

Proof. We first prove Part B, which is simpler. By taking $n \to \infty$ (Technically we take a subsequence of n approaching ∞ where the equality holds; same below), we get immediately $a_0 = 0$. Since $x_{1,n} \neq 0$, we can divide out $|x_{1,n}|$, and get for infinitely many n,

$$\left| \sum_{i=1}^{k} a_i x_{i,n} / x_{1,n} \right| = 0.$$

Now the result follows by induction.

Next we prove Part A. Multiplying by its conjugate, we get

$$\left(\sum_{i=0}^{k} a_i x_{i,n} \right) \left(\sum_{j=0}^{k} \overline{a_j} x_{j,n} \right) = \left(\sum_{i=0}^{k} b_i x_{i,n} \right) \left(\sum_{j=0}^{k} \overline{b_j} x_{j,n} \right).$$

Every term involves a product $x_{i,n}x_{j,n}$. If $\max\{i,j\} < \ell$, then the terms $a_i\overline{a_j}x_{i,n}x_{j,n} = b_i\overline{b_j}x_{i,n}x_{j,n}$ and they cancel (since $a_i = b_i$ and $a_j = b_j$). If $\max\{i,j\} > \ell$, then both terms $a_i\overline{a_j}x_{i,n}x_{j,n}$ and $b_i\overline{b_j}x_{i,n}x_{j,n}$ are $o(|x_{\ell,n}|)$ as $n \to \infty$. This is also true if $\max\{i,j\} = \ell$ and $\min\{i,j\} > 0$. The only remaining terms correspond to $\max\{i,j\} = \ell$ and $\min\{i,j\} = 0$. After canceling out identical terms, we get

$$(a_\ell + \overline{a_\ell})x_{\ell,n} + o(|x_{\ell,n}|) = (b_\ell + \overline{b_\ell})x_{\ell,n} + o(|x_{\ell,n}|),$$

as $n \to \infty$. Dividing out $x_{\ell,n}$, and then taking limit $n \to \infty$, we get the real part

$$\text{Re}(a_\ell) = \text{Re}(b_\ell).$$

It follows that $a_\ell = b_\ell$ since $\text{Im}(a_\ell) = \text{Im}(b_\ell)$. □

We remark that Part A of the Vanishing Lemma above cannot be extended to arbitrary sequences $\{a_i\}$ and $\{b_i\}$ without the condition that $\text{Im}(a_\ell) = \text{Im}(b_\ell)$, as shown by the following example: Let

$$a_1 = 3 + \sqrt{3}i, \quad a_2 = 3\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right), \quad \text{and} \quad b_1 = b_2 = 3.$$

Then the following is an identity for all real values x,

$$\left|1 + a_1x + a_2x^2\right| = \left|1 + b_1x + b_2x^2\right|.$$

In particular this holds when $x \to 0$. We note that $a_1 \neq b_1$.

8.4.2 Proof of Lemma 8.8

Without loss of generality, we assume $1 = \mu_1 > \ldots > \mu_s > 0$ and $1 = \nu_1 > \ldots > \nu_t > 0$ (otherwise, we can multiply $\mathbf{C}$ with an appropriate scalar so that the new $\mathbf{C}$ has this property. This operation clearly does not affect the complexity of $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$). We assume $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is not #P-hard.

Again, we let $\mathfrak{D}^*$ denote a sequence of N $m \times m$ diagonal matrices in which every matrix is a copy of the matrix $\mathbf{D}^{[0]}$ in $\mathfrak{D}$. It is clear that $\mathfrak{D}^*$ satisfies condition $(\mathcal{T}_3)$.

Recall that r is a fixed index in $[N-1]$, and the definition of the $s \times h$ matrix $\mathbf{D}$ from $\mathbf{D}^{[r]}$. Let $G = (V, E)$ be an undirected graph. For each $n \geq 1$, we construct a new graph $G^{[n]}$ by replacing every edge $uv \in E$ with a gadget which is shown in Figure 4.

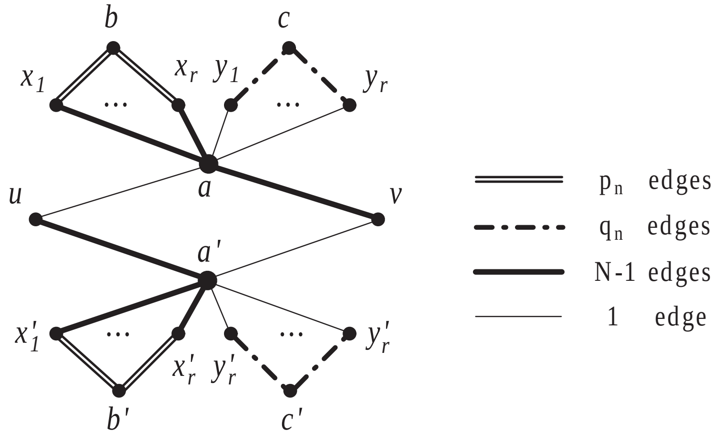

Figure 4: Gadget for constructing $G^{[n]}$, $n \geq 1$ (Note that the subscript e is suppressed).

More exactly, we define $G^{[n]}$ as follows. Let $p_n = n^2N + 1$ and $q_n = nN - 1$ (when $n \to \infty$, q_n will be arbitrarily large, and for a given q_n, p_n will be arbitrarily *larger*). Then

$$V^{[n]} = V \cup \big\{a_e, x_{e,i}, y_{e,i}, b_e, c_e, a'_e, x'_{e,i}, y'_{e,i}, b'_e, c'_e \,\big|\, e \in E, i \in [r]\big\},$$

and $E^{[n]}$ contains exactly the following edges: For every edge $e = uv \in E$,

1. One edge between $(u, a_e), (v, a'_e), (a_e, y_{e,i})$ and $(a'_e, y'_{e,i})$, for all $i \in [r]$;
2. $N - 1$ edges between $(v, a_e), (u, a'_e), (a_e, x_{e,i})$ and $(a'_e, x'_{e,i})$, for all $i \in [r]$;
3. p_n edges between $(b_e, x_{e,i})$ and $(b'_e, x'_{e,i})$, for all $i \in [r]$;
4. q_n edges between $(c_e, y_{e,i})$ and $(c'_e, y'_{e,i})$, for all $i \in [r]$.

It is easy to check that the degree of every vertex in graph $G^{[n]}$ is a multiple of N except for b_e and b'_e, which have degree $r \bmod N$, and c_e and c'_e, which have degree $N - r \bmod N$.

Since the gadget is symmetric with respect to vertices u and v, the construction of $G^{[n]}$ gives us a symmetric $m \times m$ matrix $\mathbf{R}^{[n]}$ (recall $m = (s + t) \times h$) such that

$$Z_{\mathbf{R}^{[n]},\mathfrak{D}^*}(G) = Z_{\mathbf{C},\mathfrak{D}}(G^{[n]}), \quad \text{for all undirected graphs } G.$$

As a result, $\mathsf{EVAL}(\mathbf{R}^{[n]}, \mathfrak{D}^*) \leq \mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$, and $\mathsf{EVAL}(\mathbf{R}^{[n]}, \mathfrak{D}^*)$ is also not #P-hard.

The entries of $\mathbf{R}^{[n]}$ are as follows: For all $\mathbf{u} \in I$ and $\mathbf{v} \in J$,

$$R^{[n]}_{(0,\mathbf{u}),(1,\mathbf{v})} = R^{[n]}_{(1,\mathbf{u}),(0,\mathbf{v})} = 0.$$

For $\mathbf{u}, \mathbf{v} \in J$, we have

$$R^{[n]}_{(1,\mathbf{u}),(1,\mathbf{v})} = \left(\sum_{\mathbf{a},\mathbf{b},\mathbf{c} \in I} \left(\sum_{\mathbf{x} \in J} F^{N-1}_{\mathbf{a},\mathbf{x}} F^{p_n}_{\mathbf{b},\mathbf{x}} D^{[0]}_{(1,\mathbf{x})} \right)^r \left(\sum_{\mathbf{y} \in J} F_{\mathbf{a},\mathbf{y}} F^{q_n}_{\mathbf{c},\mathbf{y}} D^{[0]}_{(1,\mathbf{y})} \right)^r F_{\mathbf{a},\mathbf{u}} F^{N-1}_{\mathbf{a},\mathbf{v}} D^{[0]}_{(0,\mathbf{a})} D^{[r]}_{(0,\mathbf{b})} D^{[N-r]}_{(0,\mathbf{c})} \right)$$

$$\times \left(\sum_{\mathbf{a},\mathbf{b},\mathbf{c} \in I} \left(\sum_{\mathbf{x} \in J} F^{N-1}_{\mathbf{a},\mathbf{x}} F^{p_n}_{\mathbf{b},\mathbf{x}} D^{[0]}_{(1,\mathbf{x})} \right)^r \left(\sum_{\mathbf{y} \in J} F_{\mathbf{a},\mathbf{y}} F^{q_n}_{\mathbf{c},\mathbf{y}} D^{[0]}_{(1,\mathbf{y})} \right)^r F^{N-1}_{\mathbf{a},\mathbf{u}} F_{\mathbf{a},\mathbf{v}} D^{[0]}_{(0,\mathbf{a})} D^{[r]}_{(0,\mathbf{b})} D^{[N-r]}_{(0,\mathbf{c})} \right).$$

Let us simplify the first factor. By using (*Shape*$_2$) and (*Shape*$_5$), we have

$$\sum_{\mathbf{x}\in J} F_{\mathbf{a},\mathbf{x}}^{N-1} F_{\mathbf{b},\mathbf{x}}^{p_n} D_{(1,\mathbf{x})}^{[0]} = \mu_{a_1}^{N-1}\mu_{b_1}^{p_n} \sum_{\mathbf{x}\in J} (\nu_{x_1})^{N-1+p_n} \overline{H_{a_2,x_2}} H_{b_2,x_2} D_{(1,(x_1,1))}^{[0]}$$
$$= \mu_{a_1}^{N-1}\mu_{b_1}^{p_n} \sum_{x_1\in[t]} (\nu_{x_1})^{N-1+p_n} D_{(1,(x_1,1))}^{[0]} \langle \mathbf{H}_{b_2,*}, \mathbf{H}_{a_2,*}\rangle. \tag{39}$$

We use L to denote the following positive number which is independent of $\mathbf{u},\mathbf{v},\mathbf{a},\mathbf{b}$ and $\mathbf{c}$:

$$L = h \cdot \sum_{x_1\in[t]} (\nu_{x_1})^{N-1+p_n} D_{(1,(x_1,1))}^{[0]}.$$

Then by (*Shape*$_4$), (39) is equal to $L\cdot \mu_{a_1}^{N-1}\mu_{b_1}^{p_n}$ if $a_2 = b_2$; and 0 otherwise. Similarly,

$$\sum_{\mathbf{y}\in J} F_{\mathbf{a},\mathbf{y}} F_{\mathbf{c},\mathbf{y}}^{q_n} D_{(1,\mathbf{y})}^{[0]} = L' \cdot \mu_{a_1}\mu_{c_1}^{q_n}, \quad \text{if } a_2 = c_2;$$

and 0 otherwise, where L' is a positive number that is independent of $\mathbf{u},\mathbf{v},\mathbf{a},\mathbf{b}$ and $\mathbf{c}$.

By (*Shape*$_3$), we have

$$D_{(0,\mathbf{c})}^{[N-r]} = \overline{D_{(0,\mathbf{c})}^{[r]}} = \overline{D_{c_1,c_2}}.$$

Combining these equations, the first factor of $R_{(1,\mathbf{u}),(1,\mathbf{v})}^{[n]}$ becomes

$$\nu_{u_1}\nu_{v_1}^{N-1} \sum_{\mathbf{a}\in I, b,c\in[s]} \left(L\cdot \mu_{a_1}^{N-1}\mu_b^{p_n}\right)^r \left(L'\cdot \mu_{a_1}\mu_c^{q_n}\right)^r \mu_{a_1}^N H_{a_2,u_2}\overline{H_{a_2,v_2}} D_{(0,(a_1,1))}^{[0]} D_{b,a_2}\overline{D_{c,a_2}}.$$

Let Z denote the following positive number that is independent of $\mathbf{u}$ and $\mathbf{v}$:

$$Z = \sum_{a_1\in[s]} \left(L\cdot \mu_{a_1}^{N-1}\right)^r \left(L'\cdot \mu_{a_1}\right)^r \mu_{a_1}^N D_{(0,(a_1,1))}^{[0]}.$$

Let $P_n = rp_n$ and $Q_n = rq_n$, then the first factor becomes

$$Z\cdot \nu_{u_1}\nu_{v_1}^{N-1} \sum_{b,c\in[s]} \mu_b^{P_n}\mu_c^{Q_n} \sum_{a\in[h]} D_{b,a}\overline{D_{c,a}} H_{a,u_2}\overline{H_{a,v_2}}.$$

We can also simplify the second factor so that $R_{(1,\mathbf{u}),(1,\mathbf{v})}^{[n]}$ is equal to

$$Z^2(\nu_{u_1}\nu_{v_1})^N \left(\sum_{b,c\in[s]} \mu_b^{P_n}\mu_c^{Q_n} \sum_{a\in[h]} D_{b,a}\overline{D_{c,a}} H_{a,u_2}\overline{H_{a,v_2}}\right) \left(\sum_{b',c'\in[s]} \mu_{b'}^{P_n}\mu_{c'}^{Q_n} \sum_{a\in[h]} D_{b',a}\overline{D_{c',a}H_{a,u_2}} H_{a,v_2}\right).$$

Since $\mathsf{EVAL}(\mathbf{R}^{[n]},\mathfrak{D}^*)$ is not #P-hard and $(\mathbf{R}^{[n]},\mathfrak{D}^*)$ satisfies $(\mathcal{T})$ for all $n\ge 1$, the necessary condition of the Inverse Cyclotomic Reduction Lemma (Corollary 8.1) applies to $\mathbf{R}^{[n]}$.

In the proof below, for notational convenience, we suppress the index $n\ge 1$ and use P,Q and $\mathbf{R}$ to represent sequences $\{P_n\},\{Q_n\}$ and $\{\mathbf{R}^{[n]}\}$, respectively. Whenever we state or prove a property about $\mathbf{R}$, we mean $\mathbf{R}^{[n]}$ has this property for any large enough n (sometimes it holds for all $n\ge 1$). Moreover, since we only use the entries of $\mathbf{R}^{[n]}$ indexed by $((1,\mathbf{u}),(1,\mathbf{v}))$ with $u_1 = v_1 = 1$, we let

$$R_{u,v} \equiv R_{(1,(1,u)),(1,(1,v))}, \quad \text{for all } u,v\in[h].$$

As a result, we have (note that $\nu_1 = 1$)

$$R_{u,v} = Z^2 \left(\sum_{b,c\in[s]} \mu_b^P \mu_c^Q \sum_{a\in[h]} D_{b,a}\overline{D_{c,a}} H_{a,u}\overline{H_{a,v}} \right) \left(\sum_{b',c'\in[s]} \mu_{b'}^P \mu_{c'}^Q \sum_{a\in[h]} D_{b',a}\overline{D_{c',a}H_{a,u}} H_{a,v} \right). \tag{40}$$

We will consider the above expression for $R_{u,v}$ *stratified* according to the order of magnitude of

$$\mu_b^P \mu_c^Q \mu_{b'}^P \mu_{c'}^Q = (\mu_b \mu_{b'})^P (\mu_c \mu_{c'})^Q.$$

Since $P = \Theta(n^2)$ and $Q = \Theta(n)$, when $n \to \infty$, Q is arbitrarily and sufficiently large, and P is further arbitrarily and sufficiently large compared to Q. Thus, the terms are ordered strictly first by $\mu_b \mu_{b'}$, and then by $\mu_c \mu_{c'}$.

Inspired by this observation, we define the following total order $\le_\mu$ over $\mathcal{T}$, where

$$\mathcal{T} = \left\{ \begin{pmatrix} b & c \\ b' & c' \end{pmatrix} \,\middle|\, b, b', c, c' \in [s] \right\}.$$

For T_1 and T_2 in $\mathcal{T}$, where

$$T_1 = \begin{pmatrix} b_1 & c_1 \\ b_1' & c_1' \end{pmatrix} \quad \text{and} \quad T_2 = \begin{pmatrix} b_2 & c_2 \\ b_2' & c_2' \end{pmatrix},$$

we have $T_1 \le_\mu T_2$ if either $\mu_{b_1}\mu_{b_1'} < \mu_{b_2}\mu_{b_2'}$; or $\mu_{b_1}\mu_{b_1'} = \mu_{b_2}\mu_{b_2'}$ and $\mu_{c_1}\mu_{c_1'} \le \mu_{c_2}\mu_{c_2'}$. For convenience, whenever we denote a 2×2 matrix in $\mathcal{T}$ by T_i or T, we denote its entries by

$$\begin{pmatrix} b_i & c_i \\ b_i' & c_i' \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} b & c \\ b' & c' \end{pmatrix}, \quad \text{respectively.}$$

Using $\le_\mu$, we can divide $\mathcal{T}$ into classes $\mathcal{T}_1, \mathcal{T}_2, \ldots, \mathcal{T}_d$ ordered from the largest to the smallest, for some positive integer d, such that

1. If $T_1, T_2 \in \mathcal{T}_i$, for some $i \in [d]$, then we have $\mu_{b_1}\mu_{b_1'} = \mu_{b_2}\mu_{b_2'}$ and $\mu_{c_1}\mu_{c_1'} = \mu_{c_2}\mu_{c_2'}$. Note that this is an equivalence relation which we denote by $=_\mu$;

2. If $T_1 \in \mathcal{T}_i$, $T_2 \in \mathcal{T}_j$ and $i < j$, then either $\mu_{b_1}\mu_{b_1'} > \mu_{b_2}\mu_{b_2'}$; or $\mu_{b_1}\mu_{b_1'} = \mu_{b_2}\mu_{b_2'}$ and $\mu_{c_1}\mu_{c_1'} > \mu_{c_2}\mu_{c_2'}$.

For each $i \in [d]$, we arbitrarily pick a $T \in \mathcal{T}_i$ and let U_i denote $\mu_b\mu_{b'}$ and W_i denote $\mu_c\mu_{c'}$ (note that U_i and W_i are independent of the choice of T). It is clear that there is exactly one matrix $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ in $\mathcal{T}_1$.

Now we can rewrite (40) as follows

$$R_{u,v} = Z^2 \sum_{i\in[d]} U_i^P W_i^Q \sum_{T\in\mathcal{T}_i} X_{u,v,T}, \tag{41}$$

where

$$X_{u,v,T} = \left(\sum_{a\in[h]} D_{b,a}\overline{D_{c,a}} H_{a,u}\overline{H_{a,v}} \right) \left(\sum_{a\in[h]} D_{b',a}\overline{D_{c',a}H_{a,u}} H_{a,v} \right), \quad \text{for } T = \begin{pmatrix} b & c \\ b' & c' \end{pmatrix}.$$

Clearly, the term with the maximum possible order in the sum (41) corresponds to the choice of $T = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right) \in \mathcal{T}_1$, since μ_1 is strictly maximum among all $\mu_1, \ldots, \mu_s$. This is true for every (u, v), and it will be the actual leading term of the sum, provided the coefficient of $U_1^P W_1^Q = \mu_1^{2P+2Q}$ is non-zero.

Consider the diagonal entries where $u = v$: First, we notice that, by (40), we have $R_{u,u} = R_{1,1}$ for all $u \in [h]$; Second, the coefficient of the leading term $U_1^P W_1^Q$ is

$$X_{u,u,\left(\begin{smallmatrix}1 & 1\\ 1 & 1\end{smallmatrix}\right)} = \left(\sum_{a\in[h]} |D_{1,a}|^2\right)^2 = \|\mathbf{D}_{1,*}\|^4,$$

which is, again, independent of u. Without loss of generality, we may assume $\mathbf{D}_{1,*}$ is not identically 0; otherwise, we can remove all terms involving μ_1 in Eq. (40) and μ_2 will take its place, and the proof is completed by induction. (If all $\mathbf{D}_{i,*} = \mathbf{0}$, then the statement that $\mathbf{D}$ has rank at most one is trivial.)

Assuming that $\mathbf{D}_{1,*} \neq \mathbf{0}$, we have $R_{u,u} = R_{1,1} \neq 0$, for all $u \in [h]$ (and sufficiently large n). This is because, ignoring the positive factor Z^2, the coefficient $\|\mathbf{D}_{1,*}\|^4$ of the leading term $U_1^P W_1^Q$ is positive. By using Corollary 8.1, we have

Property 8.1. *For all sufficiently large n, $|R_{1,1}| > 0$ and $|R_{u,v}| \in \{0, |R_{1,1}|\}$ for all $u, v \in [h]$.*

From now on, we focus on $u = 1$ and denote by $\boldsymbol{\mathcal{H}}_{*,v} = \mathbf{H}_{*,1} \circ \overline{\mathbf{H}_{*,v}}$. We note that $\{\boldsymbol{\mathcal{H}}_{*,v}\}_{v\in[h]}$ forms an orthogonal basis, with each $\|\boldsymbol{\mathcal{H}}_{*,v}\|^2 = h$. We also denote $X_{1,v,T}$ by $X_{v,T}$, so

$$X_{v,T} = \left(\sum_{a\in[h]} D_{b,a}\overline{D_{c,a}}\mathcal{H}_{a,v}\right)\left(\sum_{a\in[h]} D_{b',a}\overline{D_{c',a}\mathcal{H}_{a,v}}\right) \text{ for } T = \begin{pmatrix} b & c\\ b' & c'\end{pmatrix}. \tag{42}$$

We need to make two more definitions. Let $K = \{i \in [h] \mid D_{1,i} \neq 0\}$. By our assumption above, we have $K \neq \emptyset$. Define

$$A = \{v \in [h] \,\big|\, \forall\, i, j \in K, \mathcal{H}_{i,v} = \mathcal{H}_{j,v}\} \quad \text{and} \quad B = [h] - A.$$

Note that if $|K| = 1$ then $A = [h]$. The converse is also true which follows from the fact that $\{\boldsymbol{\mathcal{H}}_{*,v}\}_{v\in[h]}$ forms an orthogonal basis. Also since $\boldsymbol{\mathcal{H}}_{*,1}$ is the all-one vector, $1 \in A$ and A is non-empty. Moreover, if $K = [h]$, then $A = \{1\}$. This, again, follows from the fact that $\{\boldsymbol{\mathcal{H}}_{*,v}\}$ forms an orthogonal basis.

Now we consider the coefficient $X_{v,T}$ of $U_1^P W_1^Q$ in $R_{1,v}$, where $T = \left(\begin{smallmatrix}1 & 1\\ 1 & 1\end{smallmatrix}\right)$. For every $v \in A$, it has norm $\|\mathbf{D}_{1,*}\|^4 > 0$. It then follows from Property 8.1 and Part B of the Vanishing Lemma that

Property 8.2. *For any $v \in A$ and sufficiently large n, $|R_{1,v}| = |R_{1,1}|$.*

If $B \neq \emptyset$, then for any $v \in B$, the coefficient of $T = \left(\begin{smallmatrix}1 & 1\\ 1 & 1\end{smallmatrix}\right)$ in $R_{1,v}$ is

$$X_{v,T} = \left(\sum_{a\in K} |D_{1,a}|^2\mathcal{H}_{a,v}\right)\left(\sum_{a\in K} |D_{1,a}|^2\overline{\mathcal{H}_{a,v}}\right) = \left|\sum_{a\in K} |D_{1,a}|^2\mathcal{H}_{a,v}\right|^2 \in \mathbb{R}.$$

Since we assumed $v \in B$, $\sum_{a\in K} |D_{1,a}|^2\mathcal{H}_{a,v}$ is a sum of positive terms $|D_{1,a}|^2$ weighted by non-constant $\mathcal{H}_{a,v}$, for $a \in K$, each with complex norm 1. Thus its absolute value must be strictly less than $\|\mathbf{D}_{1,*}\|^2$, which is only achieved when all $\mathcal{H}_{a,v}$, for $a \in K$, are equal to a constant. It follows that $X_{v,T} < \|\mathbf{D}_{1,*}\|^4$. Therefore, for $v \in B$ (and n sufficiently large), we have $|R_{1,v}| < |R_{1,1}|$. By using Property 8.1 and Part B of the Vanishing Lemma, we have the following property:

Property 8.3. *If $v \in B$, then for all sufficiently large n, $R_{1,v} = 0$ and thus,*

$$\sum_{T\in\mathcal{T}_i} X_{v,T} = 0, \quad \textit{for all } i \in [d].$$

In particular, by applying Property 8.3 to $\mathcal{T}_1 = \{\left(\begin{smallmatrix}1 & 1\\ 1 & 1\end{smallmatrix}\right)\}$, we have

$$\sum_{a \in K} |D_{1,a}|^2 \mathcal{H}_{a,v} = \sum_{a \in K} |D_{1,a}|^2 \overline{\mathcal{H}_{a,v}} = \langle |\mathbf{D}_{1,*}|^2, \boldsymbol{\mathcal{H}}_{*,v} \rangle = 0, \quad \text{for every } v \in B,$$

since $|D_{1,a}|$ is real. Furthermore, because $\{\boldsymbol{\mathcal{H}}_{*,v}\}$ forms an orthogonal basis, $|\mathbf{D}_{1,*}|^2$ must be expressible as a linear combination of $\{\boldsymbol{\mathcal{H}}_{*,v} \,|\, v \in A\}$, over $\mathbb{C}$. From such an expression, we have $|D_{1,i}|^2 = |D_{1,j}|^2$ for all $i, j \in K$, by the definition of K. Since $\mathbf{D}_{1,*}$ is only non-zero on K, $|D_{1,i}|$ is a constant on K, and $D_{1,i} = 0$ for any $i \in [h] - K$. (The above proof does not actually assume $B \neq \emptyset$; if $B = \emptyset$, then $A = [h]$ and by $\{\boldsymbol{\mathcal{H}}_{*,v}\}$ being an orthogonal basis, $|K| = 1$. Then the above statement about $\mathbf{D}_{1,*}$ is still valid, namely $\mathbf{D}_{1,*}$ has a unique non-zero entry and zero elsewhere.)

We summarize the above as follows:

Claim 8.1. *$|\mathbf{D}_{1,*}|^2 \perp \boldsymbol{\mathcal{H}}_{*,v}$ for all $v \in B$, and $|\mathbf{D}_{1,*}|^2$ is a constant on K and 0 elsewhere. In particular the vector χ_K, which is 1 on K and 0 elsewhere, is in the span of $\{\boldsymbol{\mathcal{H}}_{*,v} \,|\, v \in A\}$, and is orthogonal to all $\{\boldsymbol{\mathcal{H}}_{*,v} \,|\, v \in B\}$.*

Our next goal is to show that on set K, $\mathbf{D}_{2,*}$ is a constant multiple of $\mathbf{D}_{1,*}$. Clearly if $B = \emptyset$, then $|K| = 1$ as noted above and thus, it is trivially true that $\mathbf{D}_{2,*}$ is a constant multiple of $\mathbf{D}_{1,*}$ on K. So we assume $B \neq \emptyset$. We now consider

$$T_1 = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \quad \text{and} \quad T_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

T_1 and T_2 belong to the same $\mathcal{T}_g$, for some $g \in [d]$. By Property 8.3, we have $\sum_{T \in \mathcal{T}_g} X_{v,T} = 0$ for every $v \in B$. So we focus on terms $X_{v,T}$, where $T \in \mathcal{T}_g$ (i.e., $T =_\mu T_1$). Suppose $T =_\mu T_1$, then by definition, we have $\mu_b \mu_{b'} = \mu_1 \mu_2$ and $\mu_c \mu_{c'} = \mu_1 \mu_2$. Thus, $\{b, b'\} = \{c, c'\} = \{1, 2\}$. As a result,

$$\mathcal{T}_g = \left\{ T_1, T_2, T_3 = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}, T_4 = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix} \right\}.$$

However, due to the presence of a row (1 1), the sum $\sum_{a=1}^{h} |D_{1,a}|^2 \mathcal{H}_{a,v} = \sum_{a=1}^{h} |D_{1,a}|^2 \overline{\mathcal{H}_{a,v}} = 0$ for any $v \in B$ as shown above. Therefore, the coefficients X_{v,T_3}, X_{v,T_4} corresponding to T_3 and T_4 are both 0.

We make one more observation:

Observation: We say a matrix $T \in \mathcal{T}$ is of a *Conjugate-Pair* form if it is of the form

$$T = \begin{pmatrix} b & c \\ c & b \end{pmatrix}.$$

For a matrix T in Conjugate-Pair form, the corresponding coefficient $X_{v,T}$ is of the form

$$X_{v,T} = \left| \sum_{a=1}^{h} D_{b,a} \overline{D_{c,a}} \mathcal{H}_{a,v} \right|^2,$$

which is always non-negative.

Now the remaining two matrices T_1 and T_2 in $\mathcal{T}_g$ both have this form, so both X_{v,T_1} and X_{v,T_2} are non-negative. Since $X_{v,T_1} + X_{v,T_2} = 0$, both X_{v,T_1} and X_{v,T_2} must be zero. This gives us

$$\sum_{a \in [h]} \overline{D_{1,a}} D_{2,a} \overline{\mathcal{H}_{a,v}} = 0, \quad \text{for all } v \in B.$$

Hence the vector $\overline{\mathbf{D}_{1,*}} \circ \mathbf{D}_{2,*} \perp \boldsymbol{\mathcal{H}}_{*,v}$ for all $v \in B$. It follows that the vector $\overline{\mathbf{D}_{1,*}} \circ \mathbf{D}_{2,*}$ is expressible as a linear combination of $\boldsymbol{\mathcal{H}}_{*,v}$ over $v \in A$. By the definition of A, this expression has a constant value on entries indexed by $a \in K$, where $|D_{1,a}|$ is a positive constant. Therefore, over K, $\mathbf{D}_{2,*}$ is a constant multiple of $\mathbf{D}_{1,*}$. This accomplished our goal stated above, which we summarize as

Claim 8.2. *There exists some complex number λ, such that $D_{2,a} = \lambda D_{1,a}$, for all $a \in K$.*

Let $K_2 = \{i \in [h] \mid D_{2,i} \neq 0\}$. Note that the λ above could be 0 so it is possible that $K \not\subset K_2$. Our next goal is to show that for every $v \in A$, $\boldsymbol{\mathcal{H}}_{*,v}$ takes a constant value on K_2. This means that for all $v \in A$, $\mathcal{H}_{i,v} = \mathcal{H}_{j,v}$, for all $i, j \in K_2$. Without loss of generality, we assume $\mathbf{D}_{2,*} \neq \mathbf{0}$ since otherwise $K_2 = \emptyset$ and everything below regarding $\mathbf{D}_{2,*}$ and regarding $\boldsymbol{\mathcal{H}}_{*,v}$ on K_2 are trivially true.

Toward this end, we will consider the class

$$\mathcal{T}_g = \left\{ T_1 = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, T_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, T_3 = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}, T_4 = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix} \right\}$$

and their corresponding coefficients X_{v,T_i} for any $v \in A$. We will apply the more delicate Part A of the Vanishing Lemma on $R_{1,v}$ and $R_{1,1}$, for an arbitrary $v \in A$. Our target is to show that

$$\sum_{T \in \mathcal{T}_g} X_{v,T} = \sum_{T \in \mathcal{T}_g} X_{1,T}, \quad \text{for any } v \in A. \tag{43}$$

By Property 8.2, we already know that $|R_{1,v}| = |R_{1,1}|$ for any sufficiently large n. So in order to apply the Vanishing Lemma, we need first to show that terms which have a higher order of magnitude satisfy

$$\sum_{T \in \mathcal{T}_{g'}} X_{v,T} = \sum_{T \in \mathcal{T}_{g'}} X_{1,T}, \quad \text{for all } 1 \le g' < g \text{ and } v \in A. \tag{44}$$

We also need to show that

$$\operatorname{Im}\left(\sum_{T \in \mathcal{T}_g} X_{v,T} \right) = \operatorname{Im}\left(\sum_{T \in \mathcal{T}_g} X_{1,T} \right). \tag{45}$$

By definition, any $T \ge_\mu T_1$ must satisfy $\mu_b \mu_{b'} \ge \mu_1 \mu_2$. Thus the first column of T is

$$\text{either } \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix} \text{ or } \begin{pmatrix} 2 \\ 1 \end{pmatrix}.$$

Firstly, consider those matrices $T \ge_\mu T_1$ where each row of T has at least one 1's. For every $v \in A$, the two inner product factors in (42), namely, $\sum_{a=1}^{h} D_{b,a} \overline{D_{c,a}} \mathcal{H}_{a,v}$, and $\sum_{a=1}^{h} D_{b',a} \overline{D_{c',a}}\, \overline{\mathcal{H}_{a,v}}$, must be actually a sum over $a \in K$, since $\mathbf{D}_{1,*}$ is zero elsewhere. But for $a \in K$, $\mathcal{H}_{a,v}$ is just a constant α_v of norm 1 (a root of unity), independent of $a \in K$. Thus

$$\sum_{a=1}^{h} D_{b,a} \overline{D_{c,a}} \mathcal{H}_{a,v} = \alpha_v \sum_{a \in K} D_{b,a} \overline{D_{c,a}} \quad \text{and} \quad \sum_{a=1}^{h} D_{b',a} \overline{D_{c',a}}\ \overline{\mathcal{H}_{a,v}} = \overline{\alpha_v} \sum_{a \in K} D_{b',a} \overline{D_{c',a}}.$$

Since $\alpha_v \overline{\alpha_v} = |\alpha_v|^2 = 1$, it follows that their product is

$$\left(\sum_{a=1}^{h} D_{b,a} \overline{D_{c,a}} \mathcal{H}_{a,v} \right) \left(\sum_{a=1}^{h} D_{b',a} \overline{D_{c',a} \mathcal{H}_{a,v}} \right) = \left(\sum_{a \in K} D_{b,a} \overline{D_{c,a}} \right) \left(\sum_{a \in K} D_{b',a} \overline{D_{c',a}} \right),$$

which is the same as the coefficient $X_{1,T}$ corresponding to T for $v_0 = 1 \in A$. Thus for all such T, their respective contributions to $R_{1,v}$ and to $R_{1,1}$ are the same, for any $v \in A$.

Such matrices $T \geq_\mu T_1$ with at least one 1's in each row include any matrix of the form

$$\begin{pmatrix} 1 & c \\ 1 & c' \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

These exhaust all $T >_\mu T_1$, and (44) follows.

Such matrices $T \geq_\mu T_1$ also include T_1 and T_2 in $\mathcal{T}_g$. So $X_{v,T_1} = X_{1,T_1}$ and $X_{v,T_2} = X_{1,T_2}$, for any $v \in A$. Now we deal with matrices T_3 and T_4. We note that the *sum* of X_{v,T_3} and X_{v,T_4}, at any v, is

$$\left(\sum_{a\in K} |D_{1,a}|^2 \mathcal{H}_{a,v}\right)\left(\sum_{a=1}^{h} |D_{2,a}|^2 \overline{\mathcal{H}_{a,v}}\right) + \left(\sum_{a=1}^{h} |D_{2,a}|^2 \mathcal{H}_{a,v}\right)\left(\sum_{a\in K} |D_{1,a}|^2 \overline{\mathcal{H}_{a,v}}\right), \tag{46}$$

which is a real number. (45) then follows.

Now we can apply Part A of the Vanishing Lemma which gives us (43). Because $X_{v,T_1} = X_{1,T_1}$ and $X_{v,T_2} = X_{1,T_2}$, we have

$$X_{v,T_3} + X_{v,T_4} = X_{1,T_3} + X_{1,T_4} = 2 \cdot \|\mathbf{D}_{1,*}\|^2 \|\mathbf{D}_{2,*}\|^2.$$

However this is clearly the maximum possible value of (46) (By our assumption, $\|\mathbf{D}_{1,*}\|^2\|\mathbf{D}_{2,*}\|^2 > 0$). The only way the sum in (46) also achieves this maximum at $v \in A$ is for $\mathcal{H}_{a,v}$ to take a constant value β_v for all $a \in K_2$, and $\mathcal{H}_{a,v}$ to take a constant value α_v for all $a \in K$, for some two complex numbers α_v and β_v of norm 1. Moreover, by (46), we have

$$\alpha_v \overline{\beta_v} + \overline{\alpha_v} \beta_v = 2.$$

It follows that $\alpha_v = \beta_v$. Thus, $\mathcal{H}_{a,v}$ is a constant on $a \in K \cup K_2$ for each $v \in A$.

We summarize it as follows:

Claim 8.3. *For every $v \in A$, there exists a complex number α_v of norm 1, such that $\mathcal{H}_{a,v} = \alpha_v$ for all a in $K \cup K_2$.*

We eventually want to prove $K_2 = K$. Our next goal is to prove that $|\mathbf{D}_{2,*}|^2 \perp \boldsymbol{\mathcal{H}}_{*,v}$, for all $v \in B$. Of course if $B = \emptyset$ then this is vacously true. We assume $B \neq \emptyset$.

For this purpose we will examine

$$T^* = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix},$$

and the class $\mathcal{T}_g$ it belongs to. By Property 8.3, we have

$$\sum_{T\in\mathcal{T}_g} X_{v,T} = 0, \quad \text{for any } v \in B.$$

Thus we will examine $T \in \mathcal{T}_g$, namely, $\mu_b\mu_{b'} = \mu_c\mu_{c'} = \mu_2^2$.

Now there might be some other pair $(b, b') \neq (2, 2)$ such that $\mu_b\mu_{b'} = \mu_2\mu_2$. If such a pair exists, it is essentially unique, and is of the form $(1, s)$ or $(s, 1)$, where $s > 2$. Then $\mathcal{T}_g$ consists of precisely the following matrices, namely each column must be either

$$\begin{pmatrix} 2 \\ 2 \end{pmatrix} \text{ or } \begin{pmatrix} s \\ 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 \\ s \end{pmatrix}. \tag{47}$$

Let's examine such a matrix $T = \begin{pmatrix} b & c \\ b' & c' \end{pmatrix}$ in more detail. Suppose $T \in \mathcal{T}_g$ has a row that is either (1 1) or (1 2) or (2 1). Then,

$$X_{v,T} = \left(\sum_{a=1}^{h} D_{b,a}\overline{D_{c,a}}\mathcal{H}_{a,v}\right)\left(\sum_{a=1}^{h} D_{b',a}\overline{D_{c',a}}\,\overline{\mathcal{H}_{a,v}}\right) = 0, \quad \text{for any } v \in B.$$

This is because the following: The presence of $\mathbf{D}_{1,*}$ restricts the sum to $a \in K$. By Claim 8.1 we know that for every $v \in B$, $|\mathbf{D}_{1,*}|^2 \perp \boldsymbol{\mathcal{H}}_{*,v}$. Moreover, on set K, we know from Claim 8.2, that both vectors $\overline{\mathbf{D}_{1,*}} \circ \mathbf{D}_{2,*}$ and $\mathbf{D}_{1,*} \circ \overline{\mathbf{D}_{2,*}}$ can be replaced by a constant multiple of the vector $|\mathbf{D}_{1,*}|^2$ (the constant could be 0), thus also perpendicular to $\boldsymbol{\mathcal{H}}_{*,v}$ (and to $\overline{\boldsymbol{\mathcal{H}}_{*,v}}$).

Now suppose T is a matrix in $\mathcal{T}_g$, and yet it does not have a row which is either (1 1) or (1 2) or (2 1). By (47), it is easy to check that the only cases are

$$T^* = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}, \quad T_1 = \begin{pmatrix} 1 & s \\ s & 1 \end{pmatrix} \quad \text{and} \quad T_2 = \begin{pmatrix} s & 1 \\ 1 & s \end{pmatrix}.$$

Thus $X_{v,T^*} + X_{v,T_1} + X_{v,T_2} = 0$ for all $v \in B$. However, as noted above, all three matrices T^*, T_1 and T_2 have the Conjugate-Pair form, so their contributions

$$\left|\sum_{a=1}^{h} D_{2,a}\overline{D_{2,a}}\mathcal{H}_{a,v}\right|^2, \quad \left|\sum_{a=1}^{h} D_{1,a}\overline{D_{s,a}}\mathcal{H}_{a,v}\right|^2 \quad \text{and} \quad \left|\sum_{a=1}^{h} D_{s,a}\overline{D_{1,a}}\mathcal{H}_{a,v}\right|^2$$

are all non-negative. It follows that all three sums are simultaneously zero. In particular, from X_{v,T^*}, we get $|\mathbf{D}_{2,*}|^2 \perp \boldsymbol{\mathcal{H}}_{*,v}$ for all $v \in B$.

It follows that the vector $|\mathbf{D}_{2,*}|^2$ is in the span of $\{\boldsymbol{\mathcal{H}}_{*,v} \mid v \in A\}$. This linear combination produces a constant value at any entry $|D_{2,a}|^2$, for $a \in K \cup K_2$. This is because each vector $\boldsymbol{\mathcal{H}}_{*,v}$ for $v \in A$ has this property by Claim 8.3.

As we assumed $\mathbf{D}_{2,*} \neq 0$, and $\mathbf{D}_{2,*}$ is 0 outside of K_2 (by the definition of K_2), this constant value produced at each entry $|D_{2,a}|^2$ for $a \in K \cup K_2$ must be non-zero. In particular, $D_{2,a} \neq 0$ at $a \in K$. It follows that $K \subseteq K_2$. It also implies that the vector, which is 1 on $K \cup K_2 = K_2$ and 0 elsewhere, is in the span of $\{\boldsymbol{\mathcal{H}}_{*,v} \mid v \in A\}$.

Next we prove that $K = K_2$, by showing that $|K| = |K_2|$ (since we already know $K \subseteq K_2$). Let χ_K denote the h-dimensional characteristic vector for K, which is 1 for any index $a \in K$ and 0 elsewhere. Similarly denote by χ_{K_2} the characteristic vector for K_2. We know that both vectors χ_K and χ_{K_2} are in the linear span of $\{\boldsymbol{\mathcal{H}}_{*,v} \mid v \in A\}$. Write $\chi_K = \sum_{v \in A} x_v \boldsymbol{\mathcal{H}}_{*,v}$, where $x_v \in \mathbb{C}$, then

$$x_v \|\boldsymbol{\mathcal{H}}_{*,v}\|^2 = \langle \chi_K, \boldsymbol{\mathcal{H}}_{*,v} \rangle = \sum_{a=1}^{h} \chi_K(a)\overline{\mathcal{H}_{a,v}} = \sum_{a \in K} \overline{\mathcal{H}_{a,v}} = |K|\overline{\alpha_v},$$

by Claim 8.3. It follows that $|x_v|h = |K|$ for each $v \in A$. Thus

$$|K| = \|\chi_K\|^2 = \sum_{v \in A} |x_v|^2 \cdot \|\boldsymbol{\mathcal{H}}_{*,v}\|^2 = |A| \left(\frac{|K|}{h}\right)^2 h = \frac{|A||K|^2}{h},$$

and it follows that $|K| = h/|A|$. Exactly the same argument gives also $|K_2| = h/|A|$. Hence $|K| = |K_2|$, and $K = K_2$. At this point the statement in Claim 8.2 can be strengthened to

Claim 8.4. *There exists some complex number λ, such that $\mathbf{D}_{2,*} = \lambda \mathbf{D}_{1,*}$.*

Our final goal is to generalize this proof to all $\mathbf{D}_{\ell,*}$, for $\ell = 1, 2, \ldots, s$. We prove this by induction.

Inductive Hypothesis: For some $\ell \geq 2$, all rows $\mathbf{D}_{1,*}, \ldots, \mathbf{D}_{\ell-1,*}$ are linearly dependent:

$$\mathbf{D}_{i,*} = \lambda_i \cdot \mathbf{D}_{1,*},$$

for some λ_i, and $1 \leq i < \ell$.

The proof below will mainly follow the proof for the case $\ell = 2$ above, except for one crucial argument at the end. We presented the special case $\ell = 2$ alone for ease of understanding.

We now prove that $\mathbf{D}_{\ell,*} = \lambda_\ell \cdot \mathbf{D}_{1,*}$ for some λ_ℓ. Clearly we may assume $\mathbf{D}_{\ell,*} \neq \mathbf{0}$, for otherwise the inductive step is trivial. To start with, we consider the following two matrices

$$T_1 = \begin{pmatrix} \ell & 1 \\ 1 & \ell \end{pmatrix} \quad \text{and} \quad T_2 = \begin{pmatrix} 1 & \ell \\ \ell & 1 \end{pmatrix},$$

and the corresponding class $\mathcal{T}_g$ they belong to. By Property 8.3, we have for every $v \in B$,

$$\sum_{T \in \mathcal{T}_g} X_{v,T} = 0.$$

We only need to examine each $T \in \mathcal{T}_g$ with exactly the same order as that of T_1, T_2: $\mu_b \mu_{b'} = \mu_c \mu_{c'} = \mu_1 \mu_\ell$. To satisfy this condition, both columns $\binom{b}{b'}$ and $\binom{c}{c'}$ of T must have entries $\{1, \ell\}$ or have both entries $< \ell$. Clearly, no entry in $\{b, b', c, c'\}$ can be $> \ell$. There are two cases now: Case 1: There is a row $(b\ c)$ or $(b'\ c')$ (or both) which has both entries $< \ell$; Case 2: Both rows have an entry $= \ell$.

In Case 1, at least one of the inner product sums in the following product

$$X_{v,T} = \left(\sum_{a=1}^{h} D_{b,a} \overline{D_{c,a}} \mathcal{H}_{a,v} \right) \left(\sum_{a=1}^{h} D_{b',a} \overline{D_{c',a}}\, \overline{\mathcal{H}_{a,v}} \right)$$

actually takes place over $a \in K$. This follows from the Inductive Hypothesis. In fact that inner product is a constant multiple of $\sum_{a \in K} |D_{1,a}|^2 \mathcal{H}_{a,v}$ or its conjugate $\sum_{a \in K} |D_{1,a}|^2 \overline{\mathcal{H}_{a,v}}$ which are 0 according to Claim 8.1, for all $v \in B$.

In Case 2, it is easy to verify that to have the same order $\mu_1 \mu_l$, T must be equal to either T_1 or T_2. Now observe that both T_1 and T_2 have the Conjugate-Pair form. Therefore, their contributions X_{v,T_1} and X_{v,T_2} are both non-negative. Since $X_{v,T_1} + X_{v,T_2} = 0$, both of them have to vanish:

$$\sum_{a \in [h]} \overline{D_{1,a}} D_{\ell,a} \overline{\mathcal{H}_{a,v}} = 0, \quad \text{and} \quad \sum_{a \in [h]} D_{1,a} \overline{D_{\ell,a}}\, \overline{\mathcal{H}_{a,v}} = 0, \quad \text{for all } v \in B.$$

Hence the vector $\overline{\mathbf{D}_{1,*}} \circ \mathbf{D}_{\ell,*} \perp \boldsymbol{\mathcal{H}}_{*,v}$, for all $v \in B$. It follows that the vector $\overline{\mathbf{D}_{1,*}} \circ \mathbf{D}_{\ell,*}$ belongs to the linear span of $\{\boldsymbol{\mathcal{H}}_{*,v} \mid v \in A\}$. By the definition of A, this expression has a constant value on entries indexed by $a \in K$. Therefore, on K, $\mathbf{D}_{\ell,*}$ is a constant multiple of $\mathbf{D}_{1,*}$. We summarize this as follows

Claim 8.5. *There exists some complex number λ_ℓ, such that $D_{\ell,a} = \lambda_\ell \cdot D_{1,a}$, for all $a \in K$.*

Let $K_\ell = \{i \in [r] \mid D_{\ell,i} \neq 0\}$. Next, we prove that for every $v \in A$, $\boldsymbol{\mathcal{H}}_{*,v}$ takes a constant value on K_ℓ, i.e., $\mathcal{H}_{i,v} = \mathcal{H}_{j,v}$, for all indices $i, j \in K_\ell$. We had assumed $\mathbf{D}_{\ell,*} \neq 0$, since otherwise the induction is completed for ℓ. Then $K_\ell \neq \emptyset$.

To show that $\boldsymbol{\mathcal{H}}_{*,v}$ is a constant on K_ℓ, we consider

$$T_3 = \begin{pmatrix} \ell & \ell \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad T_4 = \begin{pmatrix} 1 & 1 \\ \ell & \ell \end{pmatrix},$$

and the class $\mathcal{T}_g$ they belong to. We want to apply Part A of the Vanishing Lemma to show that

$$\sum_{T \in \mathcal{T}_g} X_{v,T} = \sum_{T \in \mathcal{T}_g} X_{1,T}, \quad \text{for any } v \in A. \tag{48}$$

For this purpose, we need to compare the respective terms of the sum (41), for an arbitrary $v \in A$ and for the particular $v_0 = 1 \in A$. More exactly, we will show that

$$\sum_{T \in \mathcal{T}_{g'}} X_{v,T} = \sum_{T \in \mathcal{T}_{g'}} X_{1,T}, \quad \text{and} \quad \mathrm{Im}\left(\sum_{T \in \mathcal{T}_g} X_{v,T}\right) = \mathrm{Im}\left(\sum_{T \in \mathcal{T}_g} X_{1,T}\right), \tag{49}$$

for all $v \in A$ and $g' < g$. Then (48) follows from Part A of the Vanishing Lemma.

To this end, we first consider any matrix T which has an order of magnitude strictly larger than that of T_3 and T_4. We have

$$\text{either } \mu_b \mu_{b'} > \mu_1 \mu_\ell, \quad \text{or } \left[\mu_b \mu_{b'} = \mu_1 \mu_\ell \text{ and } \mu_c \mu_{c'} > \mu_1 \mu_\ell\right].$$

The first alternative implies that both b and $b' < \ell$. The second alternative implies that c and $c' < \ell$.

In both cases, each row of T has at least one entry $< \ell$. By the Inductive Hypothesis, both inner products in (42), namely, $\sum_{a=1}^h D_{b,a}\overline{D_{c,a}}\mathcal{H}_{a,v}$ and $\sum_{a=1}^h D_{b',a}\overline{D_{c',a}}\,\overline{\mathcal{H}_{a,v}}$, must be actually a sum over K since $\mathbf{D}_{1,*}$ is zero elsewhere. However for any $a \in K$, $\mathcal{H}_{a,v}$ is a constant α_v of norm 1 (a root of unity), independent of $a \in K$. Thus

$$\sum_{a \in [h]} D_{b,a}\overline{D_{c,a}}\mathcal{H}_{a,v} = \alpha_v \sum_{a \in K} D_{b,a}\overline{D_{c,a}} \quad \text{and} \quad \sum_{a \in [h]} D_{b',a}\overline{D_{c',a}}\,\overline{\mathcal{H}_{a,v}} = \overline{\alpha_v} \sum_{a \in K} D_{b',a}\overline{D_{c',a}}.$$

Since $\alpha_v \overline{\alpha_v} = |\alpha_v|^2 = 1$, it follows that their product

$$X_{v,T} = \left(\sum_{a \in K} D_{b,a}\overline{D_{c,a}}\right)\left(\sum_{a \in K} D_{b',a}\overline{D_{c',a}}\right),$$

which is exactly the same as the coefficient $X_{1,T}$ for $v_0 = 1 \in A$. Thus for any T, where each row has at least one entry $< \ell$, $X_{v,T} = X_{1,T}$, for any $v \in A$. This includes *all* matrices $T >_\mu T_3$ (as well as *some* matrices $T =_\mu T_3 \in \mathcal{T}_g$), and the first part of (49) follows.

Now we consider any matrix $T \in \mathcal{T}_g$. If each row of T has at least one entry $< \ell$, then by the proof above, we know $X_{v,T} = X_{1,T}$ for any $v \in A$. Suppose $T \in \mathcal{T}_g$ does not have this property. Then each column of such a matrix must consist of $\{1, \ell\}$. We have four such matrices: T_1, T_2, T_3 and T_4. But the former two matrices already belong to the case covered above. So we have

$$\sum_{T \in \mathcal{T}_g} X_{v,T} - \sum_{T \in \mathcal{T}_g} X_{1,T} = X_{v,T_3} + X_{v,T_4} - \left(X_{1,T_3} + X_{1,T_4}\right), \quad \text{for any } v \in A.$$

Now to the matrices T_3, T_4 themselves. We note that the *sum* of their coefficients $X_{v,T_3} + X_{v,T_4}$ is

$$\left(\sum_{a \in K} |D_{1,a}|^2 \mathcal{H}_{a,v}\right)\left(\sum_{a=1}^h |D_{\ell,a}|^2 \overline{\mathcal{H}_{a,v}}\right) + \left(\sum_{a=1}^h |D_{\ell,a}|^2 \mathcal{H}_{a,v}\right)\left(\sum_{a \in K} |D_{1,a}|^2 \overline{\mathcal{H}_{a,v}}\right), \quad \text{at any } v \in A. \tag{50}$$

This is a real number, and the second part of (49) follows.

Now we can apply Part A of the Vanishing Lemma to conclude that

$$X_{v,T_3} + X_{v,T_4} = X_{1,T_3} + X_{1,T_4} = 2 \cdot \|\mathbf{D}_{1,*}\|^2 \|\mathbf{D}_{\ell,*}\|^2, \quad \text{for any } v \in A.$$

This is the maximum possible value of (50). By our assumption $\|\mathbf{D}_{1,*}\|^2 \|\mathbf{D}_{\ell,*}\|^2 > 0$. The only way the sum in (50) also achieves this maximum at $v \in A$ is for $\mathcal{H}_{a,v}$ to take a constant value γ_v for all $a \in K_\ell$, (and we already know that $\mathcal{H}_{a,v}$ takes a constant value α_v for all $a \in K$), where α_v and γ_v are of norm 1. Moreover, by (50), we have

$$\alpha_v \overline{\gamma_v} + \overline{\alpha_v} \gamma_v = 2.$$

It follows that $\alpha_v = \gamma_v$. Thus $\boldsymbol{\mathcal{H}}_{*,v}$ is a constant on $K \cup K_\ell$ for each $v \in A$. We summarize it as

Claim 8.6. *For every $v \in A$, there exists a complex number α_v of norm 1, such that $\mathcal{H}_{v,a} = \alpha_v$ for all $a \in K \cup K_\ell$.*

Our next goal is to show that $|\mathbf{D}_{\ell,*}|^2 \perp \boldsymbol{\mathcal{H}}_{*,v}$ for all $v \in B$. Of course if $B = \emptyset$ then this is vacously true. We assume $B \neq \emptyset$. For this purpose, we examine

$$T^* = \begin{pmatrix} \ell & \ell \\ \ell & \ell \end{pmatrix},$$

and the class $\mathcal{T}_g$ it belongs to. By Property 8.3, we have $\sum_{T \in \mathcal{T}_g} X_{v,T} = 0$ for any $v \in B$, and our target is to show that $X_{v,T^*} = 0$. To prove this, we need to examine terms $X_{v,T}$ for all $T =_\mu T^* \in \mathcal{T}_g$.

It is now possible to have a number of pairs, $(a_1, b_1), (a_2, b_2), \ldots, (a_k, b_k)$, for some $k \geq 0$, such that $\mu_{a_i} \mu_{b_i} = \mu_\ell^2$, for $1 \leq i \leq k$. (When $\ell = 2$, such a pair, if it exists, is essentially unique, but for $\ell > 2$ there could be many such pairs. This is a complication for $\ell > 2$). For every matrix $T \in \mathcal{T}_g$, it must have each column chosen from either $\binom{\ell}{\ell}$ or one of the pairs $\binom{a_i}{b_i}$ or $\binom{b_i}{a_i}$. Note that if such pairs do not exist, i.e., $k = 0$, then $\mathcal{T}_g = \{T^*\}$ and we have

$$X_{v,T^*} = \left(\sum_{a=1}^{h} |D_{\ell,a}|^2 \mathcal{H}_{a,v} \right) \left(\sum_{a=1}^{h} |D_{\ell,a}|^2 \overline{\mathcal{H}_{a,v}} \right) = 0, \quad \text{at any } v \in B.$$

The following proof is to show that even when such pairs exist ($k \geq 1$), we still have $X_{v,T^*} = 0$. For this purpose, we show that $\sum_{T \in \mathcal{T}_g, T \neq T^*} X_{v,T} \geq 0$.

Suppose $k \geq 1$. We may assume $a_i < \ell < b_i$, for all $i \in [k]$. Let's examine all the matrices $T \in \mathcal{T}_g$ other than T^*. If T has at least one row, say $(b \ \ c)$, with $\max\{b, c\} \leq \ell$ and $\min\{b, c\} < \ell$, then by the Inductive Hypothesis and Claim 8.5, the corresponding inner product actually takes place over K. In fact, the inner product is a constant multiple of the projection of $|\mathbf{D}_{1,*}|^2$ on either $\boldsymbol{\mathcal{H}}_{*,v}$ or $\overline{\boldsymbol{\mathcal{H}}_{*,v}}$. But we already know that this projection is zero for all $v \in B$.

For the remaining T where both rows satisfy $[\max\{b, c\} > \ell$ or $\min\{b, c\} \geq \ell]$, if $T \neq T^*$ then one of its two columns $\neq \binom{\ell}{\ell}$, and one entry of this column is $a_i < \ell$, for some $i \in [k]$. It then follows that the other entry in the same row as a_i must be $b_j > \ell$, for some $j \in [k]$. As a result, the only matrices remaining are of the form

$$\begin{pmatrix} a_i & b_j \\ b_i & a_j \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} b_i & a_j \\ a_i & b_j \end{pmatrix}, \quad \text{for some } 1 \leq i, j \leq k.$$

We consider the first type $\begin{pmatrix} a_i & b_j \\ b_i & a_j \end{pmatrix}$. The total contribution of these matrices is

$$\begin{aligned}
&\sum_{i,j=1}^{k}\left(\sum_{a=1}^{h} D_{a_i,a}\overline{D_{b_j,a}}\mathcal{H}_{a,v}\right)\left(\sum_{a'=1}^{h} D_{b_i,a'}\overline{D_{a_j,a'}}\,\overline{\mathcal{H}_{a',v}}\right)\\
=\;&\sum_{i,j=1}^{k}\left(\sum_{a=1}^{h} \lambda_{a_i} D_{1,a}\overline{D_{b_j,a}}\mathcal{H}_{a,v}\right)\left(\sum_{a'=1}^{h} D_{b_i,a'}\overline{\lambda_{a_j}}\,\overline{D_{1,a'}}\,\overline{\mathcal{H}_{a',v}}\right)\\
=\;&\sum_{i,j=1}^{k}\sum_{a,a'=1}^{h} \overline{\lambda_{a_j}} D_{1,a}\overline{D_{b_j,a}}\mathcal{H}_{a,v}\cdot\lambda_{a_i} D_{b_i,a'}\overline{D_{1,a'}}\,\overline{\mathcal{H}_{a',v}}\\
=\;&\left[\sum_{a=1}^{h} D_{1,a}\mathcal{H}_{a,v}\left(\sum_{j=1}^{k}\overline{\lambda_{a_j}}\,\overline{D_{b_j,a}}\right)\right]\cdot\left[\sum_{a'=1}^{h}\overline{D_{1,a'}}\,\overline{\mathcal{H}_{a',v}}\left(\sum_{i=1}^{k}\lambda_{a_i} D_{b_i,a'}\right)\right]\\
=\;&\left|\sum_{a=1}^{h} D_{1,a}\mathcal{H}_{a,v}\left(\sum_{j=1}^{k}\overline{\lambda_{a_j}}\,\overline{D_{b_j,a}}\right)\right|^2 \ge 0.
\end{aligned}$$

Here in the first equality we used the Inductive Hypothesis for $a_i, a_j < \ell$.

The argument for the second type of matrices is symmetric.

Note also that the matrix T^* has the Conjugate-Pair form, and therefore its contribution X_{v,T^*} at any $v \in B$ is also non-genative. Then it follows from $\sum_{T\in\mathcal{T}_g} X_{v,T} = 0$ (Property 8.3) that X_{v,T^*} must be zero. Hence

$$\left|\sum_{a=1}^{h} |D_{\ell,a}|^2\overline{\mathcal{H}_{a,v}}\right|^2 = 0, \quad \text{for all } v \in B.$$

This means that $|\mathbf{D}_{\ell,*}|^2 \perp \boldsymbol{\mathcal{H}}_{*,v}$ for all $v \in B$ and thus, $|\mathbf{D}_{\ell,*}|^2$ is in the linear span of $\{\boldsymbol{\mathcal{H}}_{*,v} \mid v \in A\}$.

Now by exactly the same argument as for $\ell = 2$ we obtain $K = K_\ell$. We summarize as follows

Claim 8.7. *There exists some complex number λ_ℓ, such that $\mathbf{D}_{\ell,*} = \lambda_\ell \cdot \mathbf{D}_{1,*}$.*

This completes the proof by induction that $\mathbf{D}$ has rank at most one.

8.5 Step 2.4

After Step 2.3, we get a pair $(\mathbf{C}, \mathfrak{D})$ that satisfies conditions ($Shape_1$)-($Shape_6$). By ($Shape_2$), we have

$$\mathbf{C} = \begin{pmatrix} \mathbf{0} & \mathbf{F} \\ \mathbf{F}^T & \mathbf{0} \end{pmatrix} = \begin{pmatrix} \mathbf{0} & \mathbf{M}\otimes\mathbf{H} \\ (\mathbf{M}\otimes\mathbf{H})^T & \mathbf{0} \end{pmatrix},$$

where $\mathbf{M}$ is an $s \times t$ matrix of rank 1: $M_{i,j} = \mu_i\nu_j$, and $\mathbf{H}$ is the $h \times h$ matrix defined in ($Shape_2$). By ($Shape_5$) and ($Shape_6$), we have

$$\mathbf{D}^{[r]} = \begin{pmatrix} \mathbf{D}^{[r]}_{(0,*)} & \\ & \mathbf{D}^{[r]}_{(1,*)} \end{pmatrix} = \begin{pmatrix} \mathbf{K}^{[r]}_{(0,*)} \otimes \mathbf{L}^{[r]}_{(0,*)} & \\ & \mathbf{K}^{[r]}_{(1,*)} \otimes \mathbf{L}^{[r]}_{(1,*)} \end{pmatrix}, \quad \text{for every } r \in [0 : N-1],$$

where $\mathbf{K}^{[r]}_{(0,*)}$, $\mathbf{K}^{[r]}_{(1,*)}$, $\mathbf{L}^{[r]}_{(0,*)}$ and $\mathbf{L}^{[r]}_{(1,*)}$ are all diagonal matrices.

Moreover, every entry in $\mathbf{L}^{[r]}$ either is 0 or has norm 1, and $\mathbf{L}^{[0]}$ is the $2h \times 2h$ identity matrix.

Using these matrices, we define two new pairs $(\mathbf{C}', \mathfrak{K})$ and $(\mathbf{C}'', \mathfrak{L})$, which give rise to two problems $\mathsf{EVAL}(\mathbf{C}', \mathfrak{K})$ and $\mathsf{EVAL}(\mathbf{C}'', \mathfrak{L})$: First, $\mathbf{C}'$ is the bipartisation of $\mathbf{M}$, so it is $(s+t)\times(s+t)$; and $\mathfrak{K}$ is a sequence of N diagonal matrices of the same size: $\{\mathbf{K}^{[0]}, \ldots, \mathbf{K}^{[N-1]}\}$. Second, $\mathbf{C}''$ is the bipartisation of $\mathbf{H}$, so it is $2h \times 2h$; and $\mathfrak{L}$ is a sequence of N diagonal matrices: $\{\mathbf{L}^{[0]}, \ldots, \mathbf{L}^{[N-1]}\}$. The following lemma shows that $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ has the same complexity as $\mathsf{EVAL}(\mathbf{C}'', \mathfrak{L})$.

Lemma 8.10. $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D}) \equiv \mathsf{EVAL}(\mathbf{C}'', \mathfrak{L})$.

Proof. Let G be a connected undirected graph and u^* be one of its vertices, then by Lemma 2.2 and Lemma 2.3, we have $Z_{\mathbf{C},\mathfrak{D}}(G) = Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}(G, u^*) + Z^{\leftarrow}_{\mathbf{C},\mathfrak{D}}(G, u^*)$,

$$Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}(G, u^*) = Z^{\rightarrow}_{\mathbf{C}',\mathfrak{K}}(G, u^*) \cdot Z^{\rightarrow}_{\mathbf{C}'',\mathfrak{L}}(G, u^*), \quad \text{and} \quad Z^{\leftarrow}_{\mathbf{C},\mathfrak{D}}(G, u^*) = Z^{\leftarrow}_{\mathbf{C}',\mathfrak{K}}(G, u^*) \cdot Z^{\leftarrow}_{\mathbf{C}'',\mathfrak{L}}(G, u^*).$$

Because $\mathbf{M}$ is of rank 1, both $Z^{\rightarrow}_{\mathbf{C}',\mathfrak{K}}$ and $Z^{\leftarrow}_{\mathbf{C}',\mathfrak{K}}$ can be computed in polynomial time. We only prove for $Z^{\rightarrow}_{\mathbf{C}',\mathfrak{K}}$ here: If G is not bipartite, then $Z^{\rightarrow}_{\mathbf{C}',\mathfrak{K}}(G, u^*)$ is trivially 0; Otherwise let $U \cup V$ be the vertex set of G, $u^* \in U$, and every edge $uv \in E$ has one vertex u from U and one vertex v from V. We use Ξ to denote the set of assignments ξ which maps U to $[s]$ and V to $[t]$. Then we have (note that we use $\mathbf{K}^{[r]}$ to denote $\mathbf{K}^{[r \bmod N]}$, for any $r \ge N$)

$$\begin{aligned} Z^{\rightarrow}_{\mathbf{C}',\mathfrak{K}}(G, u^*) &= \sum_{\xi \in \Xi} \left(\prod_{uv \in E} \mu_{\xi(u)} \cdot \nu_{\xi(v)} \right) \left(\prod_{u \in U} K^{[\deg(u)]}_{(0,\xi(u))} \right) \left(\prod_{v \in V} K^{[\deg(v)]}_{(1,\xi(v))} \right) \\ &= \prod_{u \in U} \left(\sum_{i \in [s]} (\mu_i)^{\deg(u)} \cdot K^{[\deg(u)]}_{(0,i)} \right) \times \prod_{v \in V} \left(\sum_{j \in [t]} (\nu_j)^{\deg(v)} \cdot K^{[\deg(v)]}_{(1,j)} \right), \end{aligned}$$

which can be computed in polynomial time.

Moreover, because pair $(\mathbf{C}'', \mathfrak{L})$ satisfies (*Pinning*), by the Second Pinning Lemma (Lemma 4.2), the problem of computing $Z^{\rightarrow}_{\mathbf{C}'',\mathfrak{L}}$ and $Z^{\leftarrow}_{\mathbf{C}'',\mathfrak{L}}$ is reducible to $\mathsf{EVAL}(\mathbf{C}'', \mathfrak{L})$. It then follows that

$$\mathsf{EVAL}(\mathbf{C}, \mathfrak{D}) \le \mathsf{EVAL}(\mathbf{C}'', \mathfrak{L}).$$

We now prove the reverse direction. First note that, by the Third Pinning Lemma (Corollary 8.2), computing $Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}$ and $Z^{\leftarrow}_{\mathbf{C},\mathfrak{D}}$ is reducible to $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$. However, this does not finish the proof since $Z^{\rightarrow}_{\mathbf{C}',\mathfrak{K}}$ (or $Z^{\leftarrow}_{\mathbf{C}',\mathfrak{K}}$) could be 0 at (G, u^*). To deal with this case, we prove the following claim:

Claim 8.8. *Given any connected bipartite graph $G = (U \cup V, E)$ and $u^* \in U$, either we can construct a new connected bipartite graph $G' = (U' \cup V', E')$ in polynomial time such that $u^* \in U \subset U'$,*

$$Z^{\rightarrow}_{\mathbf{C}'',\mathfrak{L}}(G', u^*) = h^{|U \cup V|} \cdot Z^{\rightarrow}_{\mathbf{C}'',\mathfrak{L}}(G, u^*), \tag{51}$$

and $Z^{\rightarrow}_{\mathbf{C}',\mathfrak{K}}(G', u^*) \neq 0$; or we can show that $Z^{\rightarrow}_{\mathbf{C}'',\mathfrak{L}}(G, u^*) = 0$.

It is clear that Claim 8.8 gives us a polynomial-time reduction from $Z^{\rightarrow}_{\mathbf{C}'',\mathfrak{L}}$ to $Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}$. One can prove a similar claim for $Z^{\leftarrow}$, and Lemma 8.10 follows. We now prove Claim 8.8.

For every $u \in U$ (and $v \in V$), we let r_u (and r_v) denote its degree in graph G. To construct G', we need an integer $\ell_u \in [s]$ for every $u \in U$, and an integer $\ell_v \in [t]$ for every $v \in V$, such that

$$\sum_{i \in [s]} \mu_i^{\ell_u N + r_u} \cdot K^{[r_u]}_{(0,i)} \neq 0, \quad \text{and} \quad \sum_{i \in [t]} \nu_i^{\ell_v N + r_v} \cdot K^{[r_v]}_{(1,i)} \neq 0. \tag{52}$$

Assume there exists a $u \in U$ such that no $\ell_u \in [s]$ satisfies (52). In this case, note that the s equations for $\ell_u = 1, \ldots, s$ form a Vandermonde system since $\mu_1 > \ldots > \mu_s > 0$. As a result, we have

$$\mathbf{K}^{[r_u]}_{(0,*)} = \mathbf{0} \implies \mathbf{L}^{[r_u]}_{(0,*)} = \mathbf{0},$$

by (Shape_6). It follows that $Z_{\overrightarrow{\mathbf{C}''},\mathfrak{L}}(G, u^*) = 0$, and we are done. Similarly, we have $Z_{\overrightarrow{\mathbf{C}''},\mathfrak{L}}(G, u^*) = 0$ if there exists a $v \in V$ such that no $\ell_v \in [t]$ satisfies (52).

Otherwise, suppose there exist an $\ell_u \in [s]$ for every $u \in U$, and an $\ell_v \in [t]$ for every $v \in V$, which satisfy (52). We construct a bipartite graph $G' = (U' \cup V', E')$ as follows: First,

$$U' = U \cup \widehat{V}, \quad \text{and} \quad V' = V \cup \widehat{U}, \quad \text{where} \;\; \widehat{V} = \big\{\widehat{v} \,|\, v \in V\big\} \;\; \text{and} \;\; \widehat{U} = \big\{\widehat{u} \,|\, u \in U\big\}.$$

Edge set E' contains E over $U \cup V$, and the following edges: $\ell_u N$ parallel edges between u and $\widehat{u}$, for every $u \in U$; and $\ell_v N$ parallel edges between v and $\widehat{v}$, for every $v \in V$.

It is clear that G' is a connected and bipartite graph. The degree of $u \in U$ (or $v \in V$) is $r_u + \ell_u N$ (or $r_v + \ell_v N$), and the degree of $\widehat{u}$ (or $\widehat{v}$) is $\ell_u N$ (or $\ell_v N$). We now use G' to prove Claim 8.8.

First, $Z_{\overrightarrow{\mathbf{C}'},\mathfrak{K}}(G', u^*)$ is equal to (the summation is over all ξ that maps U' to $[s]$ and V' to $[t]$)

$$\sum_{\xi} \left(\prod_{uv \in E} M_{\xi(u),\xi(v)} \prod_{u \in U} M^{\ell_u N}_{\xi(u),\xi(\widehat{u})} \prod_{v \in V} M^{\ell_v N}_{\xi(\widehat{v}),\xi(v)} \right) \left(\prod_{u \in U} K^{[r_u]}_{(0,\xi(u))} K^{[0]}_{(1,\xi(\widehat{u}))} \right) \left(\prod_{v \in V} K^{[r_v]}_{(1,\xi(v))} K^{[0]}_{(0,\xi(\widehat{v}))} \right)$$

$$= \prod_{u \in U} \left(\sum_{i \in [s]} \mu_i^{\ell_u N + r_u} \cdot K^{[r_u]}_{(0,i)} \right) \prod_{v \in V} \left(\sum_{i \in [t]} \nu_i^{\ell_v N + r_v} \cdot K^{[r_v]}_{(1,i)} \right) \prod_{\widehat{u} \in \widehat{U}} \left(\sum_{i \in [t]} \nu_i^{\ell_u N} \cdot K^{[0]}_{(1,i)} \right) \prod_{\widehat{v} \in \widehat{V}} \left(\sum_{i \in [s]} \mu_i^{\ell_v N} \cdot K^{[0]}_{(0,i)} \right).$$

It is non-zero: the first two factors are non-zero because of the way we picked ℓ_u and ℓ_v; the latter two factors are non-zero because $\mu_i, \nu_i > 0$, and by (Shape_6), every entry of $\mathbf{K}^{[0]}$ is a positive integer.

The only thing left is to prove (51). We let η be any assignment over $U \cup V$, which maps U to $[s]$ and V to $[t]$. Given η, we let Ξ denote the set of assignments ξ over $U' \cup V'$ which map U' to $[s]$, V' to $[t]$, and satisfies $\xi(u) = \eta(u)$, $\xi(v) = \eta(v)$ for all $u \in U$ and $v \in V$. We have

$$\begin{aligned} \sum_{\xi \in \Xi} \mathrm{wt}_{\mathbf{C}'',\mathfrak{L}}(\xi) \;&=\; \sum_{\xi \in \Xi} \left(\prod_{uv \in E} H_{\eta(u),\eta(v)} \prod_{u \in U} \big(H_{\eta(u),\xi(\widehat{u})}\big)^{\ell_u N} \prod_{v \in V} \big(H_{\xi(\widehat{v}),\eta(v)}\big)^{\ell_v N} \right) \\ &\qquad \times \left(\prod_{u \in U} L^{[r_u]}_{(0,\eta(u))} L^{[0]}_{(1,\xi(\widehat{u}))} \right) \left(\prod_{v \in V} L^{[r_v]}_{(1,\eta(v))} L^{[0]}_{(0,\xi(\widehat{v}))} \right) \\ &=\; \sum_{\xi \in \Xi} \mathrm{wt}_{\mathbf{C}'',\mathfrak{L}}(\eta) \;=\; h^{|\widehat{U} \cup \widehat{V}|} \cdot \mathrm{wt}_{\mathbf{C}'',\mathfrak{L}}(\eta). \end{aligned}$$

The second equation uses the fact that every entry of $\mathbf{H}$ is a power of ω_N (thus $(H_{i,j})^N = 1$) and $\mathbf{L}^{[0]}$ is the identity matrix. (51) then follows. ∎

8.6 Step 2.5

We are almost done with Step 2. The only conditions $(\mathcal{U}_i)$'s that are possibly violated by $(\mathbf{C}'', \mathfrak{L})$ are $(\mathcal{U}_1)$ (N might be odd), and $(\mathcal{U}_2)$ ($H_{i,1}$ and $H_{1,j}$ might not be 1). We deal with $(\mathcal{U}_2)$ first.

What we will do below is to normalize $\mathbf{H}$ (in $\mathbf{C}''$) so that it becomes a discrete unitary matrix for some positive integer M that divides N, while not changing the complexity of $\mathsf{EVAL}(\mathbf{C}'', \mathfrak{L})$.

First, without loss of generality, we may assume $\mathbf{H}$ satisfies $H_{1,1} = 1$ since otherwise, we can divide $\mathbf{H}$ with $H_{1,1}$, which does not affect the complexity of $\mathsf{EVAL}(\mathbf{C}'', \mathfrak{L})$. Second, we construct the following pair $(\mathbf{X}, \mathfrak{Y})$: $\mathbf{X}$ is the bipartisation of an $h \times h$ matrix over $\mathbb{C}$, whose $(i,j)^{th}$ entry is

$$H_{i,j} \cdot \overline{H_{1,j} H_{i,1}}, \quad \text{for all } i,j \in [h];$$

and $\mathfrak{Y} = \{\mathbf{Y}^{[0]}, ..., \mathbf{Y}^{[N-1]}\}$ is a sequence of $2h \times 2h$ diagonal matrices: $\mathbf{Y}^{[0]}$ is the identity matrix; Let

$$\mathcal{S} = \{r \in [0 : N-1] \,\big|\, \mathbf{L}^{[r]}_{(0,*)} \neq \mathbf{0}\} \quad \text{and} \quad \mathcal{T} = \{r \in [0 : N-1] \,\big|\, \mathbf{L}^{[r]}_{(1,*)} \neq \mathbf{0}\},$$

then

$$\mathbf{Y}^{[r]}_{(0,*)} = \mathbf{0}, \ \text{ for all } r \notin \mathcal{S}; \quad \text{and} \quad \mathbf{Y}^{[r]}_{(1,*)} = \mathbf{0}, \ \text{ for all } r \notin \mathcal{T}.$$

For every $r \in \mathcal{S}$ (and $r \in \mathcal{T}$), by (Shape_6), there must exist an $a_r \in [h]$ (and $b_r \in [h]$, resp.) such that

$$L^{[r]}_{(0,a_r)} = 1 \qquad \Big(\text{and } L^{[r]}_{(1,b_r)} = 1, \text{ resp.}\Big).$$

Set

$$Y^{[r]}_{(0,i)} = L^{[r]}_{(0,i)} \cdot \left(\frac{H_{i,1}}{H_{a_r,1}}\right)^r, \ \text{ for all } i \in [h]; \ \ Y^{[r]}_{(1,j)} = L^{[r]}_{(1,j)} \cdot \left(\frac{H_{1,j}}{H_{1,b_r}}\right)^r, \ \text{ for all } j \in [h].$$

We show that $\mathsf{EVAL}(\mathbf{C}'', \mathfrak{L}) \equiv \mathsf{EVAL}(\mathbf{X}, \mathfrak{Y})$.

First, we prove that $\mathsf{EVAL}(\mathbf{X}, \mathfrak{Y}) \le \mathsf{EVAL}(\mathbf{C}'', \mathfrak{L})$. Let $G = (U \cup V, E)$ be a connected undirected graph and u^* be a vertex in U. For every $r \in \mathcal{S}$ (and $r \in \mathcal{T}$), we use $U_r \subseteq U$ (and $V_r \subseteq V$, resp.) to denote the subset of vertices with degree $r \bmod N$. It is clear that if $U_r \neq \emptyset$ for some $r \notin \mathcal{S}$ or if $V_r \neq \emptyset$ for some $r \notin \mathcal{T}$, both $Z^{\rightarrow}_{\mathbf{C}'',\mathfrak{L}}(G, u^*)$ and $Z^{\rightarrow}_{\mathbf{X},\mathfrak{Y}}(G, u^*)$ are trivially zero. Otherwise, we have

$$Z^{\rightarrow}_{\mathbf{C}'',\mathfrak{L}}(G, u^*) = \left(\prod_{r \in \mathcal{S}} (H_{a_r,1})^{r|U_r|}\right) \left(\prod_{r \in \mathcal{T}} (H_{1,b_r})^{r|V_r|}\right) \cdot Z^{\rightarrow}_{\mathbf{X},\mathfrak{Y}}(G, u^*). \tag{53}$$

So the problem of computing $Z^{\rightarrow}_{\mathbf{X},\mathfrak{Y}}$ is reducible to computing $Z^{\rightarrow}_{\mathbf{C}'',\mathfrak{L}}$. By combining it with the Second Pinning Lemma (Lemma 4.2), we know that computing $Z^{\rightarrow}_{\mathbf{X},\mathfrak{Y}}$ is reducible to $\mathsf{EVAL}(\mathbf{C}'', \mathfrak{L})$. A similar statement can be proved for $Z^{\leftarrow}_{\mathbf{X},\mathfrak{Y}}$, and it follows that

$$\mathsf{EVAL}(\mathbf{X}, \mathfrak{Y}) \le \mathsf{EVAL}(\mathbf{C}'', \mathfrak{L}).$$

The other direction, $\mathsf{EVAL}(\mathbf{C}'', \mathfrak{L}) \le \mathsf{EVAL}(\mathbf{X}, \mathfrak{Y})$, can be proved similarly.

One can check that $(\mathbf{X}, \mathfrak{Y})$ satisfies ($\mathcal{U}_1$)-($\mathcal{U}_4$) except that N might be odd. In particular the upper-right $h \times h$ block of $\mathbf{X}$ is an M-discrete unitary matrix for some positive integer $M \,|\, N$; and $\mathfrak{Y}$ satisfies both ($\mathcal{U}_3$) and ($\mathcal{U}_4$) (which follow from the fact that every entry of $\mathbf{H}$ is a power of ω_N).

If N is even then we are done with Step 2; otherwise we extend $\mathfrak{Y}$ to be

$$\mathfrak{Y}' = \{\mathbf{Y}^{[0]}, \ldots, \mathbf{Y}^{[N-1]}, \mathbf{Y}^{[N]}, \ldots, \mathbf{Y}^{[2N-1]}\},$$

where $\mathbf{Y}^{[r]} = \mathbf{Y}^{[r-N]}$, for all $r \in [N : 2N-1]$. We have $\mathsf{EVAL}(\mathbf{X}, \mathfrak{Y}) \equiv \mathsf{EVAL}(\mathbf{X}, \mathfrak{Y}')$, since

$$Z_{\mathbf{X},\mathfrak{Y}}(G) = Z_{\mathbf{X},\mathfrak{Y}'}(G), \quad \text{for all undirected graphs } G,$$

and the new tuple $((M, 2N), \mathbf{X}, \mathfrak{Y}')$ now satisfies conditions ($\mathcal{U}_1$)-($\mathcal{U}_4$).

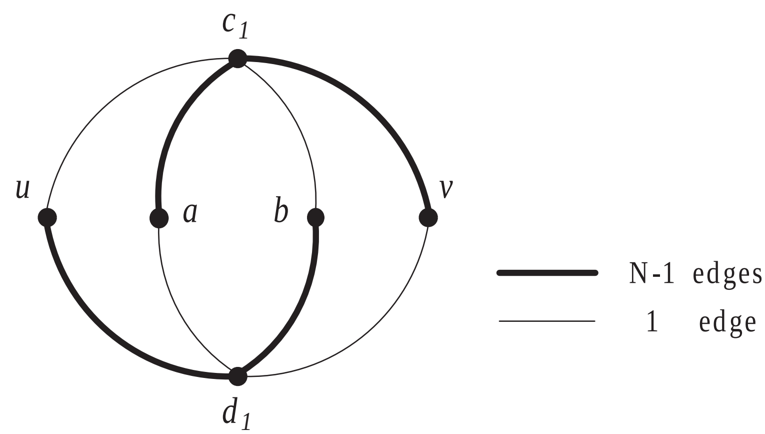

Figure 5: The gadget for $p = 1$ (Note that the subscript e is suppressed).

9 Proofs of Theorem 5.3 and Theorem 5.4

Let $((M, N), \mathbf{C}, \mathfrak{D})$ be a tuple that satisfies $(\mathcal{U}_1)$-$(\mathcal{U}_4)$ and $\mathbf{F} \in \mathbb{C}^{m\times m}$ be the upper-right block of $\mathbf{C}$. In this section, we index the rows and columns of an $n \times n$ matrix with $[0 : n - 1]$.

9.1 The Group Condition

We first prove that either $\mathbf{F}$ satisfies the following condition or $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is #P-hard:

Lemma 9.1. *Let $((M, N), \mathbf{C}, \mathfrak{D})$ be a tuple that satisfies $(\mathcal{U}_1)$-$(\mathcal{U}_4)$, then either $\mathbf{F}$ satisfies the following group condition $(\mathcal{GC})$:*

1. (row-$\mathcal{GC}$)*: $\forall\, i, j \in [0 : m - 1]$, $\exists\, k \in [0 : m - 1]$ such that $\mathbf{F}_{k,*} = \mathbf{F}_{i,*} \circ \mathbf{F}_{j,*}$;*
2. (column-$\mathcal{GC}$)*: $\forall\, i, j \in [0 : m - 1]$, $\exists\, k \in [0 : m - 1]$ such that $\mathbf{F}_{*,k} = \mathbf{F}_{*,i} \circ \mathbf{F}_{*,j}$,*

or $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is #P-hard.

Proof. Suppose $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is not #P-hard.

Let $G = (V, E)$ be an undirected graph. For every integer $p \ge 1$, we construct a new graph $G^{[p]}$ by replacing every edge $uv \in E$ with a gadget. The gadget for $p = 1$ is shown in Figure 5.

More exactly, we define $G^{[p]} = (V^{[p]}, E^{[p]})$ as

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

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

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

It is easy to check that the degree of every vertex in $G^{[p]}$ is a multiple of N, so

$$Z_{\mathbf{C},\mathfrak{D}}(G^{[p]}) = Z_{\mathbf{C}}(G^{[p]}),$$

since $\mathfrak{D}$ satisfies $(\mathcal{U}_3)$. On the other hand, the way we build $G^{[p]}$ gives us, for every $p \ge 1$, a symmetric matrix $\mathbf{A}^{[p]} \in \mathbb{C}^{2m\times 2m}$ which only depends on $\mathbf{C}$, such that

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

As a result, we have $\mathsf{EVAL}(\mathbf{A}^{[p]}) \le \mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ and thus, $\mathsf{EVAL}(\mathbf{A}^{[p]})$ is not #P-hard for all $p \ge 1$.

The $(i,j)^{th}$ entry of $\mathbf{A}^{[p]}$, where $i,j \in [0:2m-1]$, is

$$\begin{aligned} A^{[p]}_{i,j} &= \sum_{a=0}^{2m-1}\sum_{b=0}^{2m-1}\left(\sum_{c=0}^{2m-1} C_{i,c}\overline{C_{a,c}}C_{b,c}\overline{C_{j,c}}\right)^p \left(\sum_{d=0}^{2m-1} \overline{C_{i,d}}C_{a,d}\overline{C_{b,d}}C_{j,d}\right)^p. \\ &= \sum_{a=0}^{2m-1}\sum_{b=0}^{2m-1}\left|\sum_{c=0}^{2m-1} C_{i,c}\overline{C_{a,c}}C_{b,c}\overline{C_{j,c}}\right|^{2p}. \end{aligned}$$

To derive the first equation, we use the fact that $M\,|\,N$ and thus, e.g., $(C_{a,c})^{N-1} = \overline{C_{a,c}}$ since $C_{a,c}$ is a power of ω_M. Note that $\mathbf{A}^{[p]}$ is a symmetric non-negative matrix. Furthermore, it is easy to check that

$$A^{[p]}_{i,j} = 0, \quad \forall\, i \in [0:m-1], \forall j \in [m, 2m-1]; \qquad \text{and} \quad A^{[p]}_{i,j} = 0, \quad \forall\, i \in [m,2m-1], \forall j \in [0:m-1].$$

For $i,j \in [0:m-1]$, we have

$$\begin{aligned} A^{[p]}_{i,j} &= \sum_{a=0}^{m-1}\sum_{b=0}^{m-1} \left|\langle \mathbf{F}_{i,*}\circ\overline{\mathbf{F}_{j,*}}, \mathbf{F}_{a,*}\circ\overline{\mathbf{F}_{b,*}}\rangle\right|^{2p}, \quad \text{and} \\ A^{[p]}_{i+m,j+m} &= \sum_{a=0}^{m-1}\sum_{b=0}^{m-1} \left|\langle \mathbf{F}_{*,i}\circ\overline{\mathbf{F}_{*,j}}, \mathbf{F}_{*,a}\circ\overline{\mathbf{F}_{*,b}}\rangle\right|^{2p}. \end{aligned} \tag{54}$$

It is clear that all these entries are positive real numbers (by taking $a=i$ and $b=j$). Now let us focus on the upper-left $m\times m$ block of $\mathbf{A}^{[p]}$. Since it is a non-negative symmetric matrix, we can apply the dichotomy theorem of Bulatov and Grohe.

On the one hand, for the special case when $j = i \in [0:m-1]$, we have

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

As $\mathbf{F}$ is a discrete unitary matrix, we have $A^{[p]}_{i,i} = m\cdot m^{2p}$. On the other hand, assuming $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ is not #P-hard, then by using Bulatov and Grohe's dichotomy theorem (Corollary 2.1), we have

$$A^{[p]}_{i,i}\cdot A^{[p]}_{j,j} = A^{[p]}_{i,j}\cdot A^{[p]}_{j,i} = (A^{[p]}_{i,j})^2, \quad \text{for all } i \ne j \in [0:m-1],$$

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

Now we use this condition to show that $\mathbf{F}$ satisfies (row-$\mathcal{GC}$). We introduce the following notation: For $i,j \in [0:m-1]$, let

$$X_{i,j} = \left\{ \left|\langle \mathbf{F}_{i,*}\circ\overline{\mathbf{F}_{j,*}}, \mathbf{F}_{a,*}\circ\overline{\mathbf{F}_{b,*}}\rangle\right| \;\Big|\; a,b \in [0:m-1]\right\}.$$

Clearly set $X_{i,j}$ is finite for all i,j, with cardinality $|X_{i,j}| \le m^2$. Each $x \in X_{i,j}$ satisfies $0 \le x \le m$. For each $x \in X_{i,j}$, we let $s_{i,j}(x)$ denote the number of pairs $(a,b) \in [0:m-1]\times[0:m-1]$ such that

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

We can now rewrite $A_{i,j}^{[p]}$ as

$$A_{i,j}^{[p]} = \sum_{x \in X_{i,j}} s_{i,j}(x) \cdot x^{2p}, \tag{55}$$

and is equal to m^{2p+1} for all $p \geq 1$. Also note that $s_{i,j}(x)$, for all $x \in X_{i,j}$, do not depend on p, and

$$\sum_{x \in X_{i,j}} s_{i,j}(x) = m^2. \tag{56}$$

We can view (55) and (56) as a linear system of equations in the unknowns $s_{i,j}(x)$. Fix i, j, then there are $|X_{i,j}|$ many variables $s_{i,j}(x)$, one for each distinct value $x \in X_{i,j}$. Equations in (55) are indexed by $p \geq 1$. If we choose (56) and (55) for $p = 1, \ldots, |X_{i,j}| - 1$, this linear system has an $|X_{i,j}| \times |X_{i,j}|$ Vandermonde matrix $((x^2)^p)$, with row index p and column index $x \in X_{i,j}$. It has full rank. Note that by setting $(a, b) = (i, j)$ and (i', j), where $i' \neq i$, respectively, we get $m \in X_{i,j}$ and $0 \in X_{i,j}$, respectively. Moreover, $s_{i,j}(0) = m^2 - m$, $s_{i,j}(m) = m$, and all other $s_{i,j}(x) = 0$ is a solution to the linear system. Therefore this must be the unique solution. As a result, we have $X_{i,j} = \{0, m\}$,

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

This implies that for all $i, j, a, b \in [0 : m-1]$, $|\langle \mathbf{F}_{i,*} \circ \overline{\mathbf{F}_{j,*}}, \mathbf{F}_{a,*} \circ \overline{\mathbf{F}_{b,*}} \rangle|$ is either m or 0.

Finally, we prove (row-$\mathcal{GC}$). Set $j = 0$. Because $\mathbf{F}_{0,*} = \mathbf{1}$, the all-1 vector, we have

$$|\langle \mathbf{F}_{i,*} \circ \mathbf{1}, \mathbf{F}_{a,*} \circ \overline{\mathbf{F}_{b,*}} \rangle| = |\langle \mathbf{F}_{i,*} \circ \mathbf{F}_{b,*}, \mathbf{F}_{a,*} \rangle| \in \{0, m\}, \quad \text{for all } i, a, b \in [0 : m-1].$$

As $\{\mathbf{F}_{a,*}, a \in [0 : m-1]\}$ is an orthogonal basis, where each $\|\mathbf{F}_{a,*}\|^2 = m$, by Parseval, we have

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

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

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

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

By property $(\mathcal{U}_2)$, every entry of $\mathbf{F}_{i,*}$, $\mathbf{F}_{b,*}$, and $\mathbf{F}_{a,*}$ is a root of unity. The inner product $\langle \mathbf{F}_{i,*} \circ \mathbf{F}_{b,*}, \mathbf{F}_{a,*} \rangle$ is a sum of m terms each of complex norm 1. To sum to a complex number of norm m, each term must be a complex number of unit norm with the *same* argument, i.e., they are the same complex number $e^{i\theta}$. Thus, $\mathbf{F}_{i,*} \circ \mathbf{F}_{b,*} = e^{i\theta} \cdot \mathbf{F}_{a,*}$. We assert that in fact $e^{i\theta} = 1$, and $\mathbf{F}_{i,*} \circ \mathbf{F}_{b,*} = \mathbf{F}_{a,*}$. This is because $\mathbf{F}_{i,1} = \mathbf{F}_{a,1} = \mathbf{F}_{b,1} = 1$. This proves the group condition (row-$\mathcal{GC}$).

One can prove (column-$\mathcal{GC}$) similarly using (54) and the lower-right $m \times m$ block of $\mathbf{A}^{[p]}$. $\square$

We prove the following property concerning discrete unitary matrices that satisfy $(\mathcal{GC})$: (Given an $n \times n$ matrix $\mathbf{A}$, we let A^R denote the set of its row vectors $\{\mathbf{A}_{i,*}\}$, and A^C denote the set of its column vectors $\{\mathbf{A}_{*,j}\}$. For general matrices, it is possible that $|A^R|, |A^C| < n$, since $\mathbf{A}$ might have duplicate rows or columns. However, if $\mathbf{A}$ is M-discrete unitary, then it is clear that $|A^R| = |A^C| = n$.)

Property 9.1. *Let $\mathbf{A} \in \mathbb{C}^{n \times n}$ be an M-discrete unitary matrix that satisfies $(\mathcal{GC})$. Then both A^R and A^C are finite Abelian groups (of order n) under the Hadamard product.*

Proof. The Hadamard product $\circ$ gives a binary operation on both A^R and A^C. The group condition $(\mathcal{GC})$ states that both sets A^R and A^C are closed under this operation, and it is clearly associative and commutative. Being discrete unitary, the all-1 vector $\mathbf{1}$ belongs to both A^R and A^C, and serves as the identity element. This operation also satisfies the cancelation law: if $x \circ y = x \circ z$ then $y = z$. From general group theory, a finite set with these properties already forms a group. But here we can be more specific about the inverse of an element. For each $\mathbf{A}_{i,*}$, the inverse should clearly be $\overline{\mathbf{A}_{i,*}}$. By $(\mathcal{GC})$, there exists a $k \in [0 : m-1]$ such that $\mathbf{A}_{k,*} = (\mathbf{A}_{i,*})^{M-1} = \overline{\mathbf{A}_{i,*}}$. The second equation is because $A_{i,j}$, for all j, is a power of ω_M. □

9.2 Proof of Theorem 5.3

In this section, we prove Theorem 5.3. Suppose $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ is not #P-hard (otherwise we are already done), then by Lemma 9.1, $((M,N),\mathbf{C},\mathfrak{D})$ satisfies not only $(\mathcal{U}_1)$-$(\mathcal{U}_4)$, but also $(\mathcal{GC})$. Let us fix r to be any index in $[N-1]$. We will prove $(\mathcal{U}_5)$ for $D_i^{[r]}$ where $i \in [m : 2m-1]$. The proof for the first half of $\mathbf{D}^{[r]}$ is similar. For simplicity, we let $\mathbf{D}$ be the m-dimensional vector such that

$$D_i = D_{m+i}^{[r]}, \quad \text{for all } i \in [0 : m-1].$$

We also need the following notation: Let $K = \{i \in [0 : m-1] \mid D_i \neq 0\}$.

If $|K| = 0$, then there is nothing to prove; If $|K| = 1$, then by $(\mathcal{U}_3)$, the only non-zero entry in $\mathbf{D}$ must be 1. So we assume $|K| \geq 2$.

We claim that D_i, for every $i \in K$, must be a root of unity otherwise problem $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ is #P-hard, which contradicts the assumption. Actually, the lemma below shows that, such a claim is all we need to prove Theorem 5.3:

Lemma 9.2. *If $D \in \mathbb{Q}(\omega_N)$ is a root of unity, then D must be a power of ω_N.*

We delay the proof to the end of the section. Now we use it to show that every D_i, $i \in K$, is a root of unity. Suppose for a contradiction that this is not true. We start by proving the following lemma about $\mathbf{Z} = (Z_0, \ldots, Z_{m-1})$, where $Z_i = (D_i)^N$ for all i:

Lemma 9.3. *Assume there exists some $k \in K$ such that Z_k is not a root of unity, then there exists an infinite integer sequence $\{P_n\}$ such that, when $n \to \infty$, the vector sequence $((Z_k)^{P_n} : k \in K)$ approaches to, but never equals to, the all-one vector of dimension $|K|$.*

Proof. Since Z_k, for $k \in K$, has norm 1, there exists a real number $\theta_k \in [0,1)$ such that, $Z_k = e^{2\pi i \theta_k}$. We will treat θ_k as a number in the $\mathbb{Z}$-module $\mathbb{R}_{\text{ mod } 1}$, i.e., real numbers modulo 1. By the assumption we know that at least one of the θ_k's, $k \in K$, is irrational.

This lemma follows from the well-known Dirichlet's Box Principle. For completeness, we include a proof here. Clearly, for any positive integer P, $((Z_k)^P : k \in K)$ does not equal to the all-one vector of dimension $|K|$; Otherwise, every θ_k is rational, contradicting the assumption.

Let $n^* = n^{|K|} + 1$, for some positive integer $n > 1$. We consider $(L \cdot \theta_k : k \in K)$ for all $L \in [n^*]$. We divide the unit cube $[0,1)^{|K|}$ into $n^* - 1$ sub-cubes of the following form

$$\left[\frac{a_1}{n}, \frac{a_1+1}{n}\right) \times \cdots \times \left[\frac{a_{|K|}}{n}, \frac{a_{|K|}+1}{n}\right),$$

where $a_k \in \{0, \ldots, n-1\}$ for all $k \in |K|$. By cardinality, there exist $L \neq L' \in [n^*]$ such that

$$\big(L \cdot \theta_k \bmod 1 : k \in K\big) \quad \text{and} \quad \big(L' \cdot \theta_k \bmod 1 : k \in K\big)$$

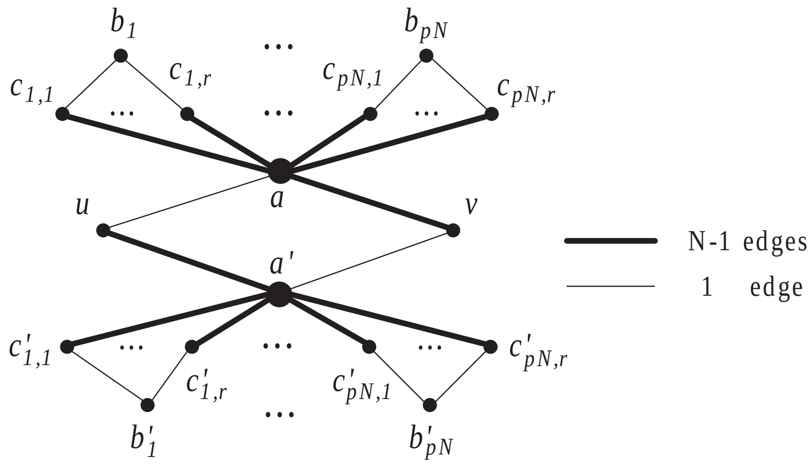

Figure 6: The gadget for $p = 1$ (Note that the subscript e is suppressed).

fall in the same sub-cube. Assume $L > L'$, then by setting $P_n = L - L' \geq 1$, we have

$$\left|P_n \cdot \theta_k \bmod 1\right| = \left|(L - L') \cdot \theta_k \bmod 1\right| \leq \frac{1}{n}, \quad \text{for all } k \in K.$$

It is clear that by repeating the procedure for every n, we get an infinite sequence $\{P_n\}$ such that

$$\Big((Z_k)^{P_n} = e^{2\pi i(P_n \cdot \theta_k)} : k \in K\Big)$$

approaches to, but never equals to, the all-one vector of dimension $|K|$. □

Let $G = (V, E)$ be an undirected graph. Then for each $p \geq 1$, we build a graph $G^{[p]}$ by replacing every edge $e = uv \in E$ with a gadget which is shown in Figure 6. Recall that $r \in [N - 1]$ is fixed.

More exactly, we define $G^{[p]} = (V^{[p]}, E^{[p]})$ as follows:

$$V^{[p]} = V \cup \big\{a_e, b_{e,i}, c_{e,i,j}, a'_e, b'_{e,i}, c'_{e,i,j} \;\big|\; e \in E, i \in [pN], j \in [r]\big\},$$

and $E^{[p]}$ contains the following edges: For each edge $e = uv \in E$,

1. One edge between (u, a_e) and (v, a'_e);
2. $N - 1$ edges between (a_e, v) and (u, a'_e);
3. One edge between $(c_{e,i,j}, b_{e,i})$ and $(c'_{e,i,j}, b'_{e,i})$, for all $i \in [pN]$ and $j \in [r]$;
4. $N - 1$ edges between $(a_e, c_{e,i,j})$ and $(a'_e, c'_{e,i,j})$, for all $i \in [pN]$ and $j \in [r]$.

It is easy to check that the degree of every vertex in $G^{[p]}$ is a multiple of N except $b_{e,i}$ and $b'_{e,i}$, which have degree $r \bmod N$.

As the gadget is symmetric, the construction gives us a symmetric $2m \times 2m$ matrix $\mathbf{A}^{[p]}$ such that

$$Z_{\mathbf{A}^{[p]}}(G) = Z_{\mathbf{C},\mathfrak{D}}(G^{[p]}), \quad \text{for any undirected graph } G,$$

and thus, $\mathsf{EVAL}(\mathbf{A}^{[p]}) \leq \mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$, and $\mathsf{EVAL}(\mathbf{A}^{[p]})$ is also not #P-hard.

The entries of $\mathbf{A}^{[p]}$ are as follows: First, for all $u, v \in [0 : m-1]$,

$$A^{[p]}_{u,m+v} = A^{[p]}_{m+u,v} = 0.$$

The entries in the upper-left $m \times m$ block of $\mathbf{A}^{[p]}$ are

$$\begin{aligned} A^{[p]}_{u,v} \;=\; & \left(\sum_{a\in[0:m-1]} F_{u,a}\overline{F_{v,a}} \left(\sum_{b\in[0:m-1]} D^{[r]}_{m+b} \left(\sum_{c\in[0:m-1]} F_{c,b}\overline{F_{c,a}} \right)^{r} \right)^{pN} \right) \\ & \times \left(\sum_{a\in[0:m-1]} \overline{F_{u,a}}F_{v,a} \left(\sum_{b\in[0:m-1]} D^{[r]}_{m+b} \left(\sum_{c\in[0:m-1]} F_{c,b}\overline{F_{c,a}} \right)^{r} \right)^{pN} \right), \end{aligned}$$

for all $u, v \in [0 : m-1]$. Since $\mathbf{F}$ is discrete unitary,

$$\sum_{c\in[0:m-1]} F_{c,b}\overline{F_{c,a}} = \langle \mathbf{F}_{*,b}, \mathbf{F}_{*,a} \rangle = 0,$$

unless $a = b$. As a result, the equation can be simplified to be

$$A^{[p]}_{u,v} = L_p \cdot \left(\sum_{k\in K} (D_k)^{pN} F_{u,k}\overline{F_{v,k}} \right) \left(\sum_{k\in K} (D_k)^{pN} \overline{F_{u,k}} F_{v,k} \right), \quad \text{for all } u, v \in [0 : m-1].$$

where L_p is a positive constant that is independent of u and v.

Assume for a contradiction that not all the D_k's, $k \in K$, are roots of unity, then by Lemma 9.3 we know there exists a sequence $\{P_n\}$ such that $((D_k)^{NP_n} : k \in K)$ approaches to, but never equals to, the all-1 vector of dimension $|K|$, when $n \to \infty$. Besides, by $(\mathcal{U}_3)$ we know there exists an $i \in K$ such that $D_i = 1$. Now consider $G^{[P_n]}$ with parameter $p = P_n$ from this sequence. We have

$$A^{[P_n]}_{u,u} = L_{P_n} \cdot \left(\sum_{k\in K} (D_k)^{NP_n} \right)^2, \quad \text{for any } u \in [0 : m-1].$$

We let T_n denote the second factor on the right-hand side, then $|T_n|$ could be arbitrarily close to $|K|^2$ if we choose n large enough. By using the dichotomy theorem of Bulatov and Grhoe (and Lemma 7.4) together with the assumption that problem $\mathsf{EVAL}(\mathbf{A}^{[P_n]})$ is not #P-hard, we know the norm of every entry of $\mathbf{A}^{[P_n]}$ in its upper-left block is either 0 or $L_{P_n} \cdot |T_n|$.

Now we focus on the first row by fixing $u = 0$. Since $\mathbf{F}_{0,*} = \mathbf{1}$, we have

$$A^{[P_n]}_{0,v} = L_{P_n} \cdot \left(\sum_{k\in K} (D_k)^{NP_n} \overline{F_{v,k}} \right) \left(\sum_{k\in K} (D_k)^{NP_n} F_{v,k} \right), \quad \text{for any } v \in [0 : m-1].$$

By Property 9.1, $F^R = \{\mathbf{F}_{v,*}\}$ is a group under the Hadamard product. We let

$$S = \{ v \in [0 : m-1] \,\big|\, \forall\, i, j \in K, F_{v,i} = F_{v,j} \},$$

and denote $\{\mathbf{F}_{v,*} : v \in S\}$ by F^S, Then it is clear that F^S is a subgroup of F^R. Also note that, $0 \in S$ since $\mathbf{F}_{0,*}$ is the all-one vector of dimension m.

For any $v \notin S$, when n is sufficiently large, we have $|A^{[P_n]}_{0,v}| < |A^{[P_n]}_{1,1}|$. This is because when $n \to \infty$,

$$T_n \to |K|^2 \quad \text{but} \quad \left(\sum_{k\in K}(D_k)^{NP_n}\overline{F_{v,k}}\right)\left(\sum_{k\in K}(D_k)^{NP_n}F_{v,k}\right) \to \left(\sum_{k\in K}\overline{F_{v,k}}\right)\left(\sum_{k\in K}F_{v,k}\right),$$

which has norm strictly smaller than $|K|^2$ (since $v \notin S$). So when n is sufficiently large, $A^{[P_n]}_{0,v}$ must be 0 for all $v \notin S$. We denote $((D_k)^{NP_n} : k \in [0 : m-1])$ by $\mathbf{D}^n$, then for $v \notin S$ and sufficiently large n,

$$\text{either} \quad \langle \mathbf{D}^n, \mathbf{F}_{v,*}\rangle = 0 \quad \text{or} \quad \langle \mathbf{D}^n, \overline{\mathbf{F}_{v,*}}\rangle = 0. \tag{57}$$

Next, we focus on the characteristic vector $\boldsymbol{\chi}$ (of dimension m) of K: $\chi_k = 1$ if $k \in K$ and $\chi_k = 0$ elsewhere. By (57) and the definition of S, we have

$$\langle \boldsymbol{\chi}, \mathbf{F}_{v,*}\rangle = 0, \quad \text{for all } v \notin S \quad \text{and} \quad |\langle \boldsymbol{\chi}, \mathbf{F}_{v,*}\rangle| = |K|, \quad \text{for all } v \in S. \tag{58}$$

To prove the first equation, we note that by Eq. (57), either there is an infinite subsequence $\{\mathbf{D}^n\}$ that satisfies $\langle \mathbf{D}^n, \mathbf{F}_{v,*}\rangle = 0$ or there is an infinite subsequence that satisfies $\langle \mathbf{D}^n, \overline{\mathbf{F}_{v,*}}\rangle = 0$. Since $\mathbf{D}^n \to \boldsymbol{\chi}$ when $n \to \infty$, we have either $\langle \boldsymbol{\chi}, \mathbf{F}_{v,*}\rangle$ or $\langle \boldsymbol{\chi}, \overline{\mathbf{F}_{v,*}}\rangle$. The second case still gives us $\langle \boldsymbol{\chi}, \mathbf{F}_{v,*}\rangle = 0$ since $\boldsymbol{\chi}$ is real. The second equation in (58) follows directly from the definition of S. As a result, we have

$$\boldsymbol{\chi} = \frac{1}{m}\sum_{v\in S}\langle \boldsymbol{\chi}, \mathbf{F}_{v,*}\rangle \cdot \mathbf{F}_{v,*}.$$

Now we assume the expression of vector $\mathbf{D}^n$, under the orthogonal basis $\{\mathbf{F}_{v,*}\}$, is

$$\mathbf{D}^n = \sum_{i=0}^{m-1} x_{i,n}\mathbf{F}_{i,*}, \quad \text{where} \quad x_{i,n} = \frac{1}{m}\langle \mathbf{D}^n, \mathbf{F}_{i,*}\rangle.$$

If for some n we have $x_{i,n} = 0$ for all $i \notin S$, then we are done because by the definition of S, every $\mathbf{F}_{i,*}$, $i \in S$, is a constant over K and thus, the vector $\mathbf{D}^n$ is a constant over K. Since we know there exists an $i \in K$ such that $D_i = 1$, every D_j, $j \in K$, must be a root of unity.

Suppose this is not the case. Then (here consider those sufficiently large n so that (57) holds)

$$\boldsymbol{\chi} = \mathbf{D}^n \circ \overline{\mathbf{D}^n} = \left(\sum_i x_{i,n}\mathbf{F}_{i,*}\right) \circ \left(\sum_j \overline{x_{j,n}}\,\overline{\mathbf{F}_{j,*}}\right) = \sum_v y_{v,n}\mathbf{F}_{v,*}, \quad \text{where} \quad y_{v,n} = \sum_{\mathbf{F}_{i,*}\circ\overline{\mathbf{F}_{j,*}}=\mathbf{F}_{v,*}} x_{i,n}\overline{x_{j,n}}.$$

The last equation uses the fact that F^R is a group under the Hadamard product (so for any i, j there exists a unique v such that $\mathbf{F}_{v,*} = \mathbf{F}_{i,*} \circ \overline{\mathbf{F}_{j,*}}$).

Since the Fourier expansion of $\boldsymbol{\chi}$ under $\{\mathbf{F}_{v,*}\}$ is unique, we have $y_{v,n} = 0$, for any $v \notin S$. Because $\mathbf{D}^n \to \boldsymbol{\chi}$, by (58), we know that when $n \to \infty$, $x_{i,n}$, for any $i \notin S$, can be arbitrarily close to 0, while $|x_{i,n}|$ can be arbitrarily close to $|K|/m$, for any $i \in S$. So there exists a sufficiently large n such that

$$|x_{i,n}| < \frac{4|K||S|}{5m^2}, \quad \text{for all } i \notin S, \quad \text{and} \quad |x_{i,n}| > \frac{4|K|}{5m}, \quad \text{for all } i \in S.$$

We pick such an n and will use it to reach a contradiction. Since we assumed that for any n (which is of course also true for this particular n we picked here), there exists at least one index $i \notin S$ such that $x_{i,n} \neq 0$, we can choose a $w \notin S$ that maximizes $|x_{i,n}|$ among all $i \notin S$. Clearly, $|x_{w,n}|$ is positive.

We consider the expression of $y_{w,n}$ using $x_{i,n}$. We divide the summation into two parts: the *main* terms $x_{i,n}\overline{x_{j,n}}$ in which either $i \in S$ or $j \in S$ and the remaining terms in which $i,j \notin S$ (note that if $\mathbf{F}_{w,*} = \mathbf{F}_{i,*} \circ \overline{\mathbf{F}_{j,*}}$, then i and j cannot be both in S. Otherwise, since F^S is a subgroup, we have $w \in S$ which contradicts the assumption that $w \in S$.)

$$\text{The main terms of } y_{w,n} = \frac{1}{m^2}\sum_{j\in S}\langle \mathbf{D}^n, \mathbf{F}_{w,*} \circ \mathbf{F}_{j,*}\rangle\overline{\langle \mathbf{D}^n, \mathbf{F}_{j,*}\rangle} + \frac{1}{m^2}\sum_{i\in S}\langle \mathbf{D}^n, \mathbf{F}_{i,*}\rangle\overline{\langle \mathbf{D}^n, \mathbf{F}_{i,*} \circ \overline{\mathbf{F}_{w,*}}\rangle}$$

Note that $x_{0,n} = (1/m)\langle \mathbf{D}^n, \mathbf{F}_{0,*}\rangle$ and $\mathbf{F}_{0,*} = \mathbf{1}$. Also note that (by the definition of S), when $j \in S$, $F_{j,k} = \alpha_j$ for all $k \in K$, for some complex number α_j of norm 1. Since $\mathbf{D}^n$ is only non-zero on K,

$$\langle \mathbf{D}^n, \mathbf{F}_{w,*} \circ \mathbf{F}_{j,*}\rangle\overline{\langle \mathbf{D}^n, \mathbf{F}_{j,*}\rangle} = \langle \mathbf{D}^n, \alpha_j \mathbf{F}_{w,*}\rangle\overline{\langle \mathbf{D}^n, \alpha_j \mathbf{1}\rangle} = m\overline{x_{0,n}} \cdot \langle \mathbf{D}^n, \mathbf{F}_{w,*}\rangle.$$

Similarly, we can simplify the other sum so that

$$\text{The main terms of } y_{w,n} = \frac{|S|}{m}\Big(\overline{x_{0,n}}\langle \mathbf{D}^n, \mathbf{F}_{w,*}\rangle + x_{0,n}\langle \overline{\mathbf{D}^n}, \mathbf{F}_{w,*}\rangle\Big).$$

By (57) we have either $\langle \mathbf{D}^n, \mathbf{F}_{w,*}\rangle$ or $\langle \overline{\mathbf{D}^n}, \mathbf{F}_{w,*}\rangle$ is 0. But since we assumed that $x_{w,n} = \langle \mathbf{D}^n, \mathbf{F}_{w,*}\rangle \neq 0$, the latter has to be 0. Therefore, the main terms of $y_{w,n}$ equal to $\overline{x_{0,n}}x_{w,n}|S|$. Since $0 \in S$, we have

$$\Big|\overline{x_{0,n}}x_{w,n}|S|\Big| \geq \frac{4|K||S|}{5m}|x_{w,n}|.$$

Now we consider the remaining terms. Below we show that the sum of all these terms cannot have a norm as large as $|\overline{x_{0,n}}x_{w,n}|S||$ and thus, $y_{w,n}$ is non-zero and we get a contradiction. To prove this, it is easy to check that the number of remaining terms is at most m, and the norm of each of them is

$$|x_{i,n}\overline{x_{j,n}}| \leq |x_{w,n}|^2 < \frac{4|K||S|}{5m^2}|x_{w,n}|,$$

since $i,j \notin S$. So the norm of their sum is $< \frac{4|K||S|}{5m}|x_{w,n}|$. This finishes the proof of Theorem 5.3.

Proof of Lemma 9.2. Assume $D = \omega_M^k$, for some positive integers k and M with $\gcd(k,M) = 1$. Since $D \in \mathbb{Q}(\omega_N)$, we have $\omega_M^k \in \mathbb{Q}(\omega_N)$. By $\gcd(k,M) = 1$, we have $\omega_M \in \mathbb{Q}(\omega_N)$ and

$$\mathbb{Q}(\omega_N) = \mathbb{Q}(\omega_N, \omega_M) = \mathbb{Q}(\omega_{\text{lcm}(M,N)}).$$

The field degree extension is $[\mathbb{Q}(\omega_N) : \mathbb{Q}] = \phi(N)$, the Euler function [14].

When $N \,|\, N'$, and $\phi(N) = \phi(N')$, by expanding according to the prime factorization for ϕ, we can get (and indeed this is all there is to be had) that if N is even, then $N' = N$; if N is odd, then $N' = N$ or $N' = 2N$. Since by $(\mathcal{U}_1)$ N is even, we have $\text{lcm}(M,N) = N$, $M \,|\, N$, and D is a power of ω_N. □

9.3 Decomposing F into Fourier Matrices

Assume that $((M,N), \mathbf{C}, \mathfrak{D})$ satisfies not only conditions $(\mathcal{U}_1)$-$(\mathcal{U}_5)$ but also the group condition $(\mathcal{GC})$; since otherwise $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is #P-hard.

To prove a decomposition for $\mathbf{F}$ (recall that $\mathbf{F}$ is the upper-right $m \times m$ block matrix of $\mathbf{C}$) we first show that if $M = pq$ and $\gcd(p,q) = 1$, then up to a permutation of rows and columns, $\mathbf{F}$ must be the tensor product of two smaller matrices, both of which are discrete unitary and satisfy $(\mathcal{GC})$. Note that p,q here are not necessarily primes or prime powers.

Lemma 9.4. *Let $\mathbf{F} \in \mathbb{C}^{m \times m}$ be an M-discrete unitary matrix that satisfies $(\mathcal{GC})$. Moreover, $M = pq$, $p, q > 1$ and $\gcd(p, q) = 1$. Then there exist two permutations $\Pi, \Sigma : [0 : m-1] \to [0 : m-1]$ such that*

$$\mathbf{F}_{\Pi,\Sigma} = \mathbf{F}' \otimes \mathbf{F}'',$$

where $\mathbf{F}'$ is p-discrete unitary, $\mathbf{F}''$ is q-discrete unitary, and both of them satisfy $(\mathcal{GC})$.

Proof. By Property 9.1, both F^R and F^C are finite Abelian groups. Since $\mathbf{F}$ is M-discrete unitary, the order of any vector in F^R and F^C is a divisor of M.

By the fundamental theorem of Abelian groups, there is a group isomorphism

$$\rho : F^R \to \mathbb{Z}_{g_1} \times \cdots \times \mathbb{Z}_{g_h} \equiv \mathbb{Z}_{\mathbf{g}},$$

where $g_1, \ldots, g_h$ are prime powers, and $g_i \,|\, M$ for all i. As $\gcd(p, q) = 1$, without loss of generality, we may assume there exists an integer h' such that $g_i \,|\, p$ for all $i \in [h']$ and $g_i \,|\, q$ for all other i.

We use ρ^{-1} to define the following two subsets of F^R:

$$S^p = \big\{\rho^{-1}(\mathbf{x}) \;\big|\; \mathbf{x} \in \mathbb{Z}_{\mathbf{g}},\, x_i = 0 \text{ for all } i > h'\big\} \quad\text{and}\quad S^q = \big\{\rho^{-1}(\mathbf{x}) \;\big|\; \mathbf{x} \in \mathbb{Z}_{\mathbf{g}},\, x_i = 0 \text{ for all } i \le h'\big\}.$$

Then it is easy to show the following four properties:

1. Both S^p and S^q are subgroups of F^R;
2. $S^p = \{\mathbf{u} \in F^R \,|\, (\mathbf{u})^p = \mathbf{1}\}$ and $S^q = \{\mathbf{v} \in F^R \,|\, (\mathbf{v})^q = \mathbf{1}\}$;
3. Let $m' = |S^p|$, $m'' = |S^q|$, then $m = m' \cdot m''$, $\gcd(m', q) = 1$, $\gcd(m'', p) = 1$, $\gcd(m', m'') = 1$;
4. $(\mathbf{u}, \mathbf{v}) \mapsto \mathbf{u} \circ \mathbf{v}$ is a group isomorphism from $S^p \oplus S^q$ onto F^R.

Let $S^p = \{\mathbf{u}_0 = \mathbf{1}, \mathbf{u}_1, \ldots, \mathbf{u}_{m'-1}\}$ and $S^q = \{\mathbf{v}_0 = \mathbf{1}, \mathbf{v}_1, \ldots, \mathbf{v}_{m''-1}\}$. Then by 4) there is a one-to-one correspondence $f : i \mapsto (f_1(i), f_2(i))$ from $[0 : m-1]$ to $[0 : m'-1] \times [0 : m''-1]$ such that

$$\mathbf{F}_{i,*} = \mathbf{u}_{f_1(i)} \circ \mathbf{v}_{f_2(i)}, \quad \text{for all } i \in [0 : m-1]. \tag{59}$$

Next we apply the fundamental theorem to F^C. We use the group isomorphism, in the same way, to define two subgroups T^p and T^q with four corresponding properties:

1. Both T^p and T^q are subgroups of F^C;
2. $T^p = \{\mathbf{w} \in F^C \,|\, (\mathbf{w})^p = \mathbf{1}\}$ and $T^q = \{\mathbf{r} \in F^C \,|\, (\mathbf{r})^q = \mathbf{1}\}$;
3. $m = |T^p| \cdot |T^q|$, $\gcd(|T^p|, q) = 1$, $\gcd(|T^q|, p) = 1$, and $\gcd(|T^p|, |T^q|) = 1$;
4. $(\mathbf{w}, \mathbf{r}) \mapsto \mathbf{w} \circ \mathbf{r}$ is a group isomorphism from $T^p \oplus T^q$ onto F^C.

By comparing item 3) in both lists, we have $|T^p| = |S^p| = m'$ and $|T^q| = |S^q| = m''$.

Let $T^p = \{\mathbf{w}_0 = \mathbf{1}, \mathbf{w}_1, \ldots, \mathbf{w}_{m'-1}\}$ and $T^q = \{\mathbf{r}_0 = \mathbf{1}, \mathbf{r}_1, \ldots, \mathbf{r}_{m''-1}\}$. Then by item 4), we have a one-to-one correspondence g from $[0 : m-1]$ to $[0 : m'-1] \times [0 : m''-1]$ and

$$\mathbf{F}_{*,j} = \mathbf{w}_{g_1(j)} \circ \mathbf{r}_{g_2(j)}, \quad \text{for all } j \in [0 : m-1]. \tag{60}$$

Now we are ready to permute the rows and columns of $\mathbf{F}$ to get a new matrix $\mathbf{G}$ that is the tensor product of two smaller matrices. We use (x_1, x_2), where $x_1 \in [0 : m'-1], x_2 \in [0 : m''-1]$, to index the rows and columns of $\mathbf{G}$. We use $\Pi(x_1, x_2) = f^{-1}(x_1, x_2)$, from $[0 : m'-1] \times [0 : m''-1]$ to $[0 : m-1]$, to permute the rows of $\mathbf{F}$ and $\Sigma(y_1, y_2) = g^{-1}(y_1, y_2)$ to permute the columns of $\mathbf{F}$, respectively. As a result, we get $\mathbf{G} = \mathbf{F}_{\Pi,\Sigma}$ where

$$G_{(x_1,x_2),(y_1,y_2)} = F_{\Pi(x_1,x_2),\Sigma(y_1,y_2)}, \quad \text{for all } x_1, y_1 \in [0 : m'-1] \text{ and } x_2, y_2 \in [0 : m''-1].$$

By (59), and using the fact that $\mathbf{u}_0 = \mathbf{1}$ and $\mathbf{v}_0 = \mathbf{1}$, we have

$$\mathbf{G}_{(x_1,x_2),*} = \mathbf{G}_{(x_1,0),*} \circ \mathbf{G}_{(0,x_2),*}, \quad \text{for all } x_1 \in [0 : m'-1] \text{ and } x_2 \in [0 : m''-1].$$

Similarly by (60) and $\mathbf{w}_0 = \mathbf{1}$ and $\mathbf{r}_0 = \mathbf{1}$, we have

$$\mathbf{G}_{*,(y_1,y_2)} = \mathbf{G}_{*,(y_1,0)} \circ \mathbf{G}_{*,(0,y_2)}, \quad \text{for all } y_1 \in [0 : m'-1] \text{ and } y_2 \in [0 : m''-1].$$

Therefore, applying both relations, we have

$$G_{(x_1,x_2),(y_1,y_2)} = G_{(x_1,0),(y_1,0)} \cdot G_{(x_1,0),(0,y_2)} \cdot G_{(0,x_2),(y_1,0)} \cdot G_{(0,x_2),(0,y_2)}.$$

We claim

$$G_{(x_1,0),(0,y_2)} = 1 \quad \text{and} \quad G_{(0,x_2),(y_1,0)} = 1. \tag{61}$$

Then we have

$$G_{(x_1,x_2),(y_1,y_2)} = G_{(x_1,0),(y_1,0)} \cdot G_{(0,x_2),(0,y_2)}. \tag{62}$$

To prove the first equation in (61), we realize that it appears as an entry in both $\mathbf{u}_{x_1}$ and $\mathbf{r}_{y_2}$. Then by item 2) for S^p and T^q, both of its pth and qth powers are 1. Thus it has to be 1. The other equation in (61) can be proved the same way.

As a result, we have obtained our tensor product decomposition $\mathbf{G} = \mathbf{F}' \otimes \mathbf{F}''$, where

$$\mathbf{F}' = \Big(F'_{x,y} \equiv G_{(x,0),(y,0)}\Big) \text{ and } \mathbf{F}'' = \Big(F''_{x,y} \equiv G_{(0,x),(0,y)}\Big).$$

The only thing left is to show that $\mathbf{F}'$ and $\mathbf{F}''$ are discrete unitary, and satisfy $(\mathcal{GC})$. Here we only prove it for $\mathbf{F}'$. The proof for $\mathbf{F}''$ is the same. To see $\mathbf{F}'$ is discrete unitary, for all $x \neq y \in [0 : m'-1]$,

$$\begin{aligned} 0 &= \langle \mathbf{G}_{(x,0),*}, \mathbf{G}_{(y,0),*} \rangle = \sum_{z_1,z_2} G_{(x,0),(z_1,z_2)} \overline{G_{(y,0),(z_1,z_2)}} \\ &= \sum_{z_1,z_2} G_{(x,0),(z_1,0)} G_{(0,0),(0,z_2)} \overline{G_{(y,0),(z_1,0)} G_{(0,0),(0,z_2)}} \\ &= m'' \cdot \langle \mathbf{F}'_{x,*}, \mathbf{F}'_{y,*} \rangle. \end{aligned}$$

Here we used the factorization (62) and $\mathbf{u}_0 = \mathbf{1}$ and $\mathbf{v}_0 = \mathbf{1}$. Similarly, we can prove that $\mathbf{F}'_{*,x}$ and $\mathbf{F}'_{*,y}$ are orthogonal for $x \neq y$. $\mathbf{F}'$ also satisfies $(\mathcal{GC})$ because both S^p and T^p are groups and thus, closed under the Hadamard product. Finally, $\mathbf{F}'$ is exactly p-discrete unitary: First, by definition, we have

$$pq = M = \text{lcm}\Big\{\text{order of } G_{(x_1,x_2),(y_1,y_2)} : \mathbf{x}, \mathbf{y}\Big\} = \text{lcm}\Big\{\text{order of } G_{(x_1,0),(y_1,0)} \cdot G_{(x_2,0),(y_2,0)} : \mathbf{x}, \mathbf{y}\Big\};$$

Second, the order of $G_{(x_1,0),(y_1,0)}$ divides p and the order of $G_{(x_2,0),(y_2,0)}$ divides q. As a result, we have

$$p = \text{lcm}\big\{\text{order of } G_{(x,0),(y,0)} : x, y\big\}$$

and by definition, $\mathbf{F}'$ is a p-discrete unitary matrix. $\square$

Next we prove Lemma 9.5 which deals with the case when M is a prime power.

Property 9.2. *Let* $\mathbf{A}$ *be an* M*-discrete unitary matrix that satisfies the group condition* ($\mathcal{GC}$). *If* M *is a prime power, then one of its entries is equal to* ω_M.

Lemma 9.5. *Let* $\mathbf{F} \in \mathbb{C}^{m\times m}$ *be an* M*-discrete unitary matrix that satisfies* ($\mathcal{GC}$). *Moreover,* $M = p^k$ *is a prime power for some* $k \geq 1$. *Then there exist two permutations* Π *and* Σ *such that*

$$\mathbf{F}_{\Pi,\Sigma} = \boldsymbol{\mathcal{F}}_M \otimes \mathbf{F}',$$

where $\mathbf{F}'$ *is an* M'*-discrete unitary matrix,* $M' = p^{k'}$ *for some* $k' \leq k$*, and* $\mathbf{F}'$ *satisfies* ($\mathcal{GC}$).

Proof. By Property 9.2, there exist a and b such that $F_{a,b} = \omega_M$. Thus both the order of $\mathbf{F}_{a,*}$ (in F^R) and the order of $\mathbf{F}_{*,b}$ (in F^C) are M. Let

$$S_1 = \big\{\mathbf{1}, \mathbf{F}_{a,*}, (\mathbf{F}_{a,*})^2, \ldots, (\mathbf{F}_{a,*})^{M-1}\big\}$$

denote the subgroup of F^R generated by $\mathbf{F}_{a,*}$. Since the order of $\mathbf{F}_{a,*}$ is M, we have $|S_1| = M$.

Let S_2 denote the subset of F^R such that $\mathbf{u} \in S_2$ iff its b^{th} entry $u_b = 1$. It is easy to see that S_2 is a subgroup of F^R. Moreover, one can show that $(\mathbf{w}_1, \mathbf{w}_2) \mapsto \mathbf{w}_1 \circ \mathbf{w}_2$ is a group isomorphism from $S_1 \oplus S_2$ onto F^R. As a result, $|S_2| = m/M$ which we denote by n.

Let $S_2 = \{\mathbf{u}_0 = \mathbf{1}, \mathbf{u}_1, \ldots, \mathbf{u}_{n-1}\}$, then there exists a one-to-one correspondence f from $[0 : m-1]$ to $[0 : M-1] \times [0 : n-1]$, where $i \mapsto f(i) = (f_1(i), f_2(i))$, such that

$$\mathbf{F}_{i,*} = (\mathbf{F}_{a,*})^{f_1(i)} \circ \mathbf{u}_{f_2(i)}, \quad \text{for all } i \in [0 : m-1]. \tag{63}$$

In particular, we have $f(a) = (1, 0)$.

Similarly, we use T_1 to denote the subgroup of F^C generated by $\mathbf{F}_{*,b}$ ($|T_1| = M$), and T_2 to denote the subgroup of F^C that contains all the $\mathbf{v} \in F^C$ such that $v_a = 1$. $(\mathbf{w}_1, \mathbf{w}_2) \mapsto \mathbf{w}_1 \circ \mathbf{w}_2$ also gives us a natural group isomorphism from $T_1 \oplus T_2$ onto F^C, so $|T_2| = m/M = n$

Let $T_2 = \{\mathbf{v}_0 = \mathbf{1}, \mathbf{v}_1, \ldots, \mathbf{v}_{n-1}\}$, then there exists a one-to-one correspondence g from $[0 : m-1]$ to $[0 : M-1] \times [0 : n-1]$, where $j \mapsto g(j) = (g_1(j), g_2(j))$, such that

$$\mathbf{F}_{*,j} = (\mathbf{F}_{*,b})^{g_1(j)} \circ \mathbf{v}_{g_2(j)}, \quad \text{for all } j \in [0 : m-1]. \tag{64}$$

In particular, we have $g(b) = (1, 0)$.

Now we are ready to permute the rows and columns of $\mathbf{F}$ to get a new $m \times m$ matrix $\mathbf{G}$. Again we use (x_1, x_2), where $x_1 \in [0 : M-1]$ and $x_2 \in [0 : n-1]$, to index the rows and columns of matrix $\mathbf{G}$. We use $\Pi(x_1, x_2) = f^{-1}(x_1, x_2)$, from $[0 : M-1] \times [0 : n-1]$ to $[0 : m-1]$, to permute the rows and $\Sigma(y_1, y_2) = g^{-1}(y_1, y_2)$ to permute the columns of $\mathbf{F}$, respectively. As a result, we get $\mathbf{G} = \mathbf{F}_{\Pi,\Sigma}$.

By equations (63) and (64), and $\mathbf{u}_0 = \mathbf{1}$ and $\mathbf{v}_0 = \mathbf{1}$, we have

$$\mathbf{G}_{(x_1,x_2),*} = (\mathbf{G}_{(1,0),*})^{x_1} \circ \mathbf{G}_{(0,x_2),*} \quad \text{and} \quad \mathbf{G}_{*,(y_1,y_2)} = (\mathbf{G}_{*,(1,0)})^{y_1} \circ \mathbf{G}_{*,(0,y_2)}.$$

Applying them in succession, we get

$$G_{(x_1,x_2),(y_1,y_2)} = (G_{(1,0),(y_1,y_2)})^{x_1} G_{(0,x_2),(y_1,y_2)} = (G_{(1,0),(1,0)})^{x_1 y_1} (G_{(1,0),(0,y_2)})^{x_1} (G_{(0,x_2),(1,0)})^{y_1} G_{(0,x_2),(0,y_2)}.$$

We can check that $G_{(1,0),(1,0)} = F_{a,b} = \omega_M$. Indeed, by $f(a) = (1,0)$ and $g(b) = (1,0)$, we have

$$G_{(1,0),(1,0)} = F_{\Pi(1,0),\Sigma(1,0)} = F_{f^{-1}(1,0),g^{-1}(1,0)} = F_{a,b} = \omega_M.$$

By (64), and a similar reasoning, we have

$$G_{(1,0),(0,y_2)} = F_{a,g^{-1}(0,y_2)} = (F_{a,b})^0 \cdot v_{y_2,a} = v_{y_2,a} = 1,$$

where $v_{y_2,a}$ denotes the a^{th} entry of $\mathbf{v}_{y_2}$, which is 1 by the definition of T_2. By (63), we also have

$$G_{(0,x_2),(1,0)} = F_{f^{-1}(0,x_2),b} = (F_{a,b})^0 \cdot u_{x_2,b} = u_{x_2,b} = 1,$$

where $u_{x_2,b}$ denotes the b^{th} entry of $\mathbf{u}_{x_2}$, which is 1 by the definition of S_2.

Combining all these equations, we have

$$G_{(x_1,x_2),(y_1,y_2)} = \omega_M^{x_1 y_1} \cdot G_{(0,x_2),(0,y_2)}. \tag{65}$$

As a result, $\mathbf{G} = \boldsymbol{\mathcal{F}}_M \otimes \mathbf{F}'$, where $\mathbf{F}' = (F'_{x,y} \equiv G_{(0,x),(0,y)})$ is an $n \times n$ matrix.

To see $\mathbf{F}'$ is discrete unitary, by (65), we have

$$0 = \langle \mathbf{G}_{(0,x),*}, \mathbf{G}_{(0,y),*} \rangle = M \cdot \langle \mathbf{F}'_{x,*}, \mathbf{F}'_{y,*} \rangle, \quad \text{for any } x \neq y \in [0 : n-1].$$

Similarly we can prove that $\mathbf{F}'_{*,x}$ and $\mathbf{F}'_{*,y}$ are orthogonal for $x \neq y$. $\mathbf{F}'$ also satisfies the group condition because both S_2 and T_2 are groups and thus, closed under the Hadamard product. More precisely, for (row-$\mathcal{GC}$), suppose $\mathbf{F}'_{x,*}$ and $\mathbf{F}'_{y,*}$ are two rows of $\mathbf{F}'$. The corresponding two rows $\mathbf{G}_{(0,x),*}$ and $\mathbf{G}_{(0,y),*}$ in $\mathbf{G}$ are permuted versions of $\mathbf{u}_x$ and $\mathbf{u}_y$, respectively. We have, by (59),

$$F'_{x,z} = F_{f^{-1}(0,x),g^{-1}(0,z)} = u_{x,g^{-1}(0,z)} \quad \text{and} \quad F'_{y,z} = F_{f^{-1}(0,y),g^{-1}(0,z)} = u_{y,g^{-1}(0,z)}.$$

Since S_2 is a group, we have some $w \in [0 : n-1]$ such that $\mathbf{u}_x \circ \mathbf{u}_y = \mathbf{u}_w$, and thus

$$F'_{x,z} \cdot F'_{y,z} = u_{w,g^{-1}(0,z)} = F'_{w,z}.$$

The verification of (column-$\mathcal{GC}$) is similar. Finally, it is also easy to see that $\mathbf{F}'$ is $p^{k'}$-discrete unitary, for some integer $k' \leq k$. □

Theorem 5.4 then follows from Lemma 9.4 and Lemma 9.5.

10 Proof of Theorem 5.5

Let $((M,N), \mathbf{C}, \mathfrak{D}, (\mathbf{q}, \mathbf{t}, \mathcal{Q}))$ be a 4-tuple that satisfies condition $(\mathcal{R})$. Also assume that $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is not #P-hard (since otherwise, we are done). For every r in $\mathcal{T}$ (recall that $\mathcal{T}$ is the set of $r \in [N-1]$ such $\Delta_r \neq \emptyset$), we show that Δ_r must be a coset in $\mathbb{Z}_{\mathcal{Q}}$. Condition $(\mathcal{L}_2)$ then follows from the following lemma which we will prove at the end of this section. Condition $(\mathcal{L}_1)$ about Λ_r can be proved similarly.

Lemma 10.1. *Let Φ be a coset in $G_1 \oplus G_2$, where G_1 and G_2 are finite Abelian groups such that*

$$\gcd\big(|G_1|, |G_2|\big) = 1.$$

Then for both $i = 1, 2$, there exists a coset Φ_i in G_i such that $\Phi = \Phi_1 \times \Phi_2$.

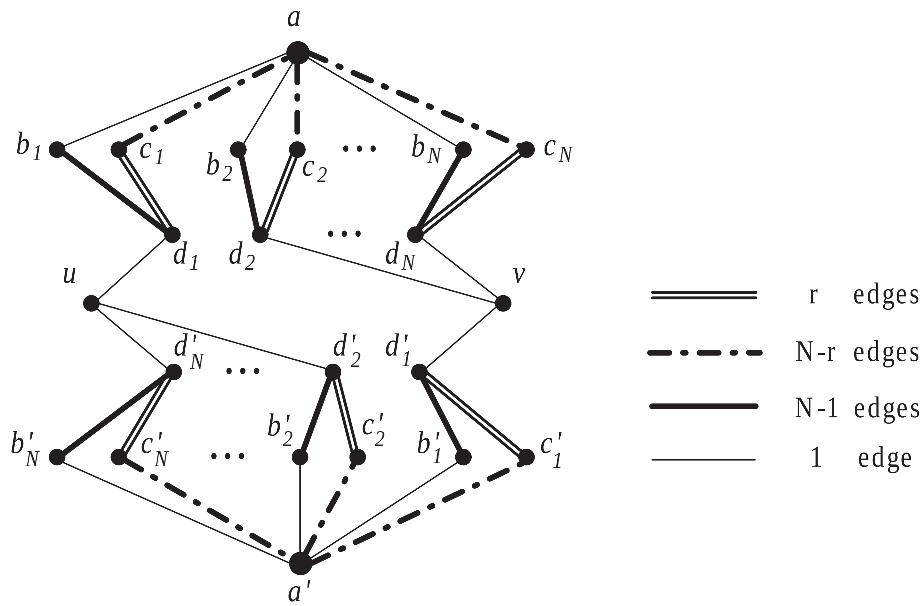

Figure 7: The gadget for constructing graph G' (Note that the subscript e is suppressed).

Let $G = (V, E)$ be an undirected graph. We build a new graph G' by replacing every $e = uv \in E$ with the gadget as shown in Figure 7. More exactly, we define $G' = (V', E')$ as

$$V' = V \cup \left\{a_e, b_{e,i}, c_{e,i}, d_{e,i}, a'_e, b'_{e,i}, c'_{e,i}, d'_{e,i} \,\middle|\, e \in E \text{ and } i \in [N]\right\}$$

and E' contains exactly the following edges: For each $e = uv \in E$,

1. One edge between $(u, d_{e,1})$, $(v, d'_{e,1})$, $(u, d'_{e,i})$ and $(v, d_{e,i})$ for all $i \in [2 : N]$;
2. For every $i \in [N]$, one edge between $(a_e, b_{e,i})$, $N - 1$ edges between $(b_{e,i}, d_{e,i})$;
3. For every $i \in [N]$, $N - r$ edges between $(a_e, c_{e,i})$, r edges between $(c_{e,i}, d_{e,i})$;
4. For every $i \in [N]$, one edge between $(a'_e, b'_{e,i})$, $N - 1$ edges between $(b'_{e,i}, d'_{e,i})$;
5. For every $i \in [N]$, $N - r$ edges between $(a'_e, c'_{e,i})$, r edges between $(c'_{e,i}, d'_{e,i})$.

It is easy to check that the degree of $d_{e,i}$ and $d'_{e,i}$, for all $e \in E, i \in [N]$, is exactly $r \pmod N$ while all other vertices in V' have degree $0 \pmod N$. It is also noted that the graph fragment which defines the gadget is bipartite, with all $u, v, b_{e,i}, c_{e,i}, b'_{e,i}, c'_{e,i}$ on one side and all $a_e, a'_e, d_{e,i}, d'_{e,i}$ on the other side.

The way we construct G' gives us a $2m \times 2m$ matrix $\mathbf{A}$ such that

$$Z_{\mathbf{A}}(G) = Z_{\mathbf{C},\mathfrak{D}}(G'), \quad \text{for all } G,$$

and thus, $\mathsf{EVAL}(\mathbf{A}) \le \mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$, and $\mathsf{EVAL}(\mathbf{A})$ is also not #P-hard. We use $\{0,1\} \times \mathbb{Z}_{\mathcal{Q}}$ to index the rows and columns of $\mathbf{A}$. Then for all $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_{\mathcal{Q}}$, we have

$$A_{(0,\mathbf{u}),(1,\mathbf{v})} = A_{(1,\mathbf{u}),(0,\mathbf{v})} = 0.$$

This follows from the bipartiteness of the gadget.

We now analyze the upper-left $m \times m$ block of $\mathbf{A}$. For $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_\mathcal{Q}$, we have

$$A_{(0,\mathbf{u}),(0,\mathbf{v})} = \left(\sum_{\mathbf{a},\mathbf{d}_1,\ldots,\mathbf{d}_N \in \mathbb{Z}_\mathcal{Q}} F_{\mathbf{u},\mathbf{d}_1} \prod_{i=2}^N F_{\mathbf{v},\mathbf{d}_i} \left(\prod_{i=1}^N \left(\sum_{\mathbf{b}_i \in \mathbb{Z}_\mathcal{Q}} F_{\mathbf{b}_i,\mathbf{a}} \overline{F_{\mathbf{b}_i,\mathbf{d}_i}} \right) \left(\sum_{\mathbf{c}_i \in \mathbb{Z}_\mathcal{Q}} F^{N-r}_{\mathbf{c}_i,\mathbf{a}} F^{r}_{\mathbf{c}_i,\mathbf{d}_i} \right) \right) \prod_{i=1}^N D^{[r]}_{(1,\mathbf{d}_i)} \right)$$
$$\times \left(\sum_{\mathbf{a},\mathbf{d}_1,\ldots,\mathbf{d}_N \in \mathbb{Z}_\mathcal{Q}} F_{\mathbf{v},\mathbf{d}_1} \prod_{i=2}^N F_{\mathbf{u},\mathbf{d}_i} \left(\prod_{i=1}^N \left(\sum_{\mathbf{b}_i \in \mathbb{Z}_\mathcal{Q}} F_{\mathbf{b}_i,\mathbf{a}} \overline{F_{\mathbf{b}_i,\mathbf{d}_i}} \right) \left(\sum_{\mathbf{c}_i \in \mathbb{Z}_\mathcal{Q}} F^{N-r}_{\mathbf{c}_i,\mathbf{a}} F^{r}_{\mathbf{c}_i,\mathbf{d}_i} \right) \right) \prod_{i=1}^N D^{[r]}_{(1,\mathbf{d}_i)} \right).$$

Note that in deriving this equation, we used the fact that $M \,|\, N$ and entries of $\mathbf{F}$ are all powers of ω_M.

Since $\mathbf{F}$ is discrete unitary,

$$\sum_{\mathbf{b}_i \in \mathbb{Z}_\mathcal{Q}} F_{\mathbf{b}_i,\mathbf{a}} \overline{F_{\mathbf{b}_i,\mathbf{d}_i}} = \langle \mathbf{F}_{*,\mathbf{a}}, \mathbf{F}_{*,\mathbf{d}_i} \rangle$$

is 0 unless $\mathbf{d}_i = \mathbf{a}$. When $\mathbf{d}_i = \mathbf{a}$ for every $i \in [N]$, the inner product $\langle \mathbf{F}_{*,\mathbf{a}}, \mathbf{F}_{*,\mathbf{d}_i} \rangle = m$, and likewise so are the sums over $\mathbf{c}_i$. Also the product

$$\prod_{i \in [N]} D^{[r]}_{(1,\mathbf{d}_i)} = \left(D^{[r]}_{(1,\mathbf{a})} \right)^N = 1,$$

when each $\mathbf{d}_i = \mathbf{a} \in \Delta_r$, and 0 otherwise. This is because by $(\mathcal{U}_5)$, $D^{[r]}_{(1,\mathbf{a})}$ is a power of ω_N when $\mathbf{a} \in \Delta_r$, and 0 otherwise.

As a result, we have

$$A_{(0,\mathbf{u}),(0,\mathbf{v})} = \left(\sum_{\mathbf{a} \in \Delta_r} F_{\mathbf{u},\mathbf{a}} \overline{F_{\mathbf{v},\mathbf{a}}} \cdot m^{2N} \right) \times \left(\sum_{\mathbf{a} \in \Delta_r} F_{\mathbf{v},\mathbf{a}} \overline{F_{\mathbf{u},\mathbf{a}}} \cdot m^{2N} \right) = m^{4N} \left| \sum_{\mathbf{a} \in \Delta_r} F_{\mathbf{u},\mathbf{a}} \overline{F_{\mathbf{v},\mathbf{a}}} \right|^2. \tag{66}$$

By using condition $(\mathcal{R}_3)$, we can further simplify (66) to be

$$A_{(0,\mathbf{u}),(0,\mathbf{v})} = m^{4N} \left| \sum_{\mathbf{a} \in \Delta_r} F_{\mathbf{u}-\mathbf{v},\mathbf{a}} \right|^2 = m^{4N} \Big| \langle \chi, \mathbf{F}_{\mathbf{u}-\mathbf{v},*} \rangle \Big|^2, \tag{67}$$

where χ is a 0-1 characteristic vector such that $\chi_\mathbf{a} = 0$ if $\mathbf{a} \notin \Delta_r$ and $\chi_\mathbf{a} = 1$ if $\mathbf{a} \in \Delta_r$, for all $\mathbf{a} \in \mathbb{Z}_\mathcal{Q}$.

Since $\mathbf{F}$ is discrete unitary, it is easy to show that

$$0 \le A_{(0,\mathbf{u}),(0,\mathbf{v})} \le m^{4N} |\Delta_r|^2 \quad \text{and} \quad A_{(0,\mathbf{u}),(0,\mathbf{u})} = m^{4N} |\Delta_r|^2, \quad \text{for all } \mathbf{u}, \mathbf{v} \in \mathbb{Z}_\mathcal{Q}.$$

As $r \in \mathcal{T}$, we have $|\Delta_r| \ge 1$ and let n denote $|\Delta_r|$. Using the dichotomy theorem of Bulatov and Grohe (Corollary 11.1) together with the assumption that $\mathsf{EVAL}(\mathbf{A})$ is not #P-hard, we have

$$A_{(0,\mathbf{u}),(0,\mathbf{v})} \in \{0, m^{4N} n^2\}, \quad \text{for all } \mathbf{u}, \mathbf{v} \in \mathbb{Z}_\mathcal{Q}.$$

As a result, we have for all $\mathbf{u} \in \mathbb{Z}_\mathcal{Q}$,

$$\Big| \langle \chi, \mathbf{F}_{\mathbf{u},*} \rangle \Big| \in \{0, n\}. \tag{68}$$

The inner product $\langle \chi, \mathbf{F}_{\mathbf{u},*} \rangle$ is a sum of n terms, each term a power of ω_M. To sum to a complex number of norm n, each term must have exactly the same argument; any misalignment will result in a complex number of norm $< n$, which is the maximum possible. This implies that

$$\langle \chi, \mathbf{F}_{\mathbf{u},*} \rangle \in \big\{0, n, n\omega_M, n\omega_M^2, \ldots, n\omega_M^{M-1}\big\}. \tag{69}$$

Next, let $\mathfrak{a}$ denote a vector in Δ_r. We use Φ to denote $\mathfrak{a} + \langle \Delta_r - \mathfrak{a} \rangle$, where

$$\Delta_r - \mathfrak{a} \equiv \{\mathbf{x} - \mathfrak{a} \,|\, \mathbf{x} \in \Delta_r\}$$

and $\langle \Delta_r - \mathfrak{a} \rangle$ is the subgroup generated by $\Delta_r - \mathfrak{a}$. Clearly $\Delta_r \subseteq \Phi$. We want to prove that Δ_r is equal to Φ, which by definition is a coset in $\mathbb{Z}_\mathcal{Q}$. This statement, together with Lemma 10.1, will finish the proof of Theorem 5.5.

To this end we use κ to denote the characteristic vector of Φ: $\kappa_\mathbf{x} = 0$ if $\mathbf{x} \notin \Phi$ and $\kappa_\mathbf{x} = 1$ if $\mathbf{x} \in \Phi$. We will show for every $\mathbf{u} \in \mathbb{Z}_\mathcal{Q}$,

$$\langle \kappa, \mathbf{F}_{\mathbf{u},*} \rangle = \frac{|\Phi|}{|\Delta_r|} \langle \chi, \mathbf{F}_{\mathbf{u},*} \rangle. \tag{70}$$

Since $\mathbf{F}$ is discrete unitary, $\{\mathbf{F}_{\mathbf{u},*}, \mathbf{u} \in \mathbb{Z}_\mathcal{Q}\}$ is an orthogonal basis. From (70) we have

$$\kappa = \frac{|\Phi|}{|\Delta_r|} \chi,$$

which implies $\kappa = \chi$ (since both of them are 0-1 vectors) and thus, $\Delta_r = \Phi$ is a coset in $\mathbb{Z}_\mathcal{Q}$.

We now prove (70). We make the following observations:

1. If $|\langle \chi, \mathbf{F}_{\mathbf{u},*} \rangle| = n$, then there exists an $\alpha \in \mathbb{Z}_M$ such that $F_{\mathbf{u},\mathbf{x}} = \omega_M^\alpha$ for all $\mathbf{x} \in \Delta_r$;
2. Otherwise, (which is equivalent to $\langle \chi, \mathbf{F}_{\mathbf{u},*} \rangle = 0$ from (68)), there exist $\mathbf{y}$ and $\mathbf{z}$ in Δ_r such that $F_{\mathbf{u},\mathbf{y}} \neq F_{\mathbf{u},\mathbf{z}}$.

Observation 1) has already been noted when we proved (69). Observation 2) is obvious since if $F_{\mathbf{u},\mathbf{y}} = F_{\mathbf{u},\mathbf{z}}$ for all $\mathbf{y}, \mathbf{z} \in \Delta_r$, then clearly $\langle \chi, \mathbf{F}_{\mathbf{u},*} \rangle \neq 0$.

Equation (70) then follows from the following two lemmas.

Lemma 10.2. *If there exists an α such that $F_{\mathbf{u},\mathbf{x}} = \omega_M^\alpha$ for all $\mathbf{x} \in \Delta_r$, then $F_{\mathbf{u},\mathbf{x}} = \omega_M^\alpha$ for all $\mathbf{x} \in \Phi$.*

Proof. Let $\mathbf{x}$ be a vector in Φ, then there exist $\mathbf{x}_1, \ldots, \mathbf{x}_k \in \Delta_r$ and $h_1, \ldots, h_k \in \{\pm 1\}$ for some $k \geq 0$, such that $\mathbf{x} = \mathfrak{a} + \sum_{i=1}^k h_i(\mathbf{x}_i - \mathfrak{a})$. By using $(\mathcal{R}_3)$ together with the assumption that $F_{\mathbf{u},\mathfrak{a}} = F_{\mathbf{u},\mathbf{x}_i} = \omega_M^\alpha$,

$$F_{\mathbf{u},\mathbf{x}} = F_{\mathbf{u},\mathfrak{a}+\sum_i h_i(\mathbf{x}_i - \mathfrak{a})} = F_{\mathbf{u},\mathfrak{a}} \prod_i F_{\mathbf{u},h_i(\mathbf{x}_i - \mathfrak{a})} = F_{\mathbf{u},\mathfrak{a}} \prod_i \left(F_{\mathbf{u},\mathbf{x}_i} \overline{F_{\mathbf{u},\mathfrak{a}}}\right)^{h_i} = \omega_M^\alpha.$$

□

Lemma 10.3. *If there exist $\mathbf{y}, \mathbf{z} \in \Phi$ such that $F_{\mathbf{u},\mathbf{y}} \neq F_{\mathbf{u},\mathbf{z}}$, then $\sum_{\mathbf{x} \in \Phi} F_{\mathbf{u},\mathbf{x}} = 0$.*

Proof. Let l be the smallest positive integer such that $l(\mathbf{y} - \mathbf{z}) = \mathbf{0}$, then l exists because $\mathbb{Z}_\mathcal{Q}$ is a finite group, and $l > 1$ because $\mathbf{y} \neq \mathbf{z}$. We use c to denote $F_{\mathbf{u},\mathbf{y}} \overline{F_{\mathbf{u},\mathbf{z}}}$. By using condition $(\mathcal{R}_3)$ together with the assumption, we have $c^l = F_{\mathbf{u},l(\mathbf{y}-\mathbf{z})} = 1$ but $c \neq 1$.

We define the following equivalence relation over Φ: For $\mathbf{x}, \mathbf{x}' \in \Phi$,

$$\mathbf{x} \sim \mathbf{x}' \text{ if there exists an integer } k \text{ such that } \mathbf{x} - \mathbf{x}' = k(\mathbf{y} - \mathbf{z}).$$

For every $\mathbf{x} \in \Phi$, its equivalence class contains the following l vectors:

$$\mathbf{x},\ \mathbf{x} + (\mathbf{y} - \mathbf{z}),\ \ldots,\ \mathbf{x} + (l-1)(\mathbf{y} - \mathbf{z}),$$

as Φ is a coset in $\mathbb{Z}_\mathcal{Q}$. We conclude that $\sum_{\mathbf{x} \in \Phi} F_{\mathbf{u},\mathbf{x}} = 0$ since for every class, we have (by using $(\mathcal{R}_3)$)

$$\sum_{i=0}^{l-1} F_{\mathbf{u},\mathbf{x}+i(\mathbf{y}-\mathbf{z})} = F_{\mathbf{u},\mathbf{x}} \sum_{i=0}^{l-1} c^i = F_{\mathbf{u},\mathbf{x}} \frac{1 - c^l}{1 - c} = 0.$$

□

Now (70) can be proved as follows: If $|\langle \chi, \mathbf{F}_{\mathbf{u},*}\rangle| = n = |\Delta_r|$, then by 1) and Lemma 10.2

$$|\langle \kappa, \mathbf{F}_{\mathbf{u},*}\rangle| = |\Phi|.$$

If $|\langle \chi, \mathbf{F}_{\mathbf{u},*}\rangle| \neq |\Delta_r|$, then $\langle \chi, \mathbf{F}_{\mathbf{u},*}\rangle = 0$. By 2) and $\Delta_r \subseteq \Phi$, Lemma 10.3 implies

$$\langle \kappa, \mathbf{F}_{\mathbf{u},*}\rangle = 0.$$

This concludes that Δ_r is a coset in $\mathbb{Z}_\mathcal{Q}$. To get the decomposition $(\mathcal{L}_2)$ for $\Delta_r = \prod_{i=1}^{s} \Delta_{r,i}$, we use Lemma 10.1.

10.1 Proof of Lemma 10.1

First, we show that if $\mathbf{u} = (u_1, u_2) \in \Phi$ and $\mathbf{v} = (v_1, v_2) \in \Phi$, for $u_i, v_i \in G_i$, $i = 1, 2$, then $(u_1, v_2) \in \Phi$.

On the one hand, since $\gcd(|G_1|, |G_2|) = 1$, there exists an integer k such that $|G_1| \,\big|\, k$ and $k \equiv 1 \pmod{|G_2|}$. On the other hand, since Φ is a coset, we have $\mathbf{u} + k(\mathbf{v} - \mathbf{u}) \in \Phi$. Since

$$u_1 + k(v_1 - u_1) = u_1 \quad\text{and}\quad u_2 + k(v_2 - u_2) = v_2,$$

we conclude that $(u_1, v_2) \in \Phi$.

This implies the existence of subsets $\Phi_1 \subseteq G_1$ and $\Phi_2 \subseteq G_2$ such that $\Phi = \Phi_1 \times \Phi_2$. Namely we let $\Phi_1 = \{x \in G_1 \,|\, \exists y \in G_2, (x, y) \in \Phi\}$, and $\Phi_2 = \{y \in G_2 \,|\, \exists x \in G_1, (x, y) \in \Phi\}$. It is easy to check that both Φ_1 and Φ_2 are cosets (in G_1 and G_2, respectively), and $\Phi = \Phi_1 \times \Phi_2$.

10.2 Some Corollaries of Theorem 5.5

Now that we have proved Theorem 5.5, we know that unless the problem is #P-hard, we may assume that condition $(\mathcal{L})$ holds. Thus Λ_r and Δ_r are cosets.

Lemma 10.4. *Let* $\mathbf{H}$ *be the* $m \times |\Delta_r|$ *submatrix obtained from* $\mathbf{F}$ *by restricting to the columns indexed by* Δ_r*. Then for any two rows* $\mathbf{H}_{\mathbf{u},*}$ *and* $\mathbf{H}_{\mathbf{v},*}$*, where* $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_\mathcal{Q}$*, either there exists some* $\alpha \in \mathbb{Z}_M$ *such that* $\mathbf{H}_{\mathbf{u},*} = \omega_M^\alpha \cdot \mathbf{H}_{\mathbf{v},*}$*, or* $\langle \mathbf{H}_{\mathbf{u},*}, \mathbf{H}_{\mathbf{v},*}\rangle = 0$*.*

Similarly we denote by $\mathbf{G}$ *the* $|\Lambda_r| \times m$ *submatrix obtained from* $\mathbf{F}$ *by restricting to the rows indexed by* Λ_r*. Then for any two columns* $\mathbf{G}_{*,\mathbf{u}}$ *and* $\mathbf{G}_{*,\mathbf{v}}$*, where* $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_\mathcal{Q}$*, either there exists an* $\alpha \in \mathbb{Z}_M$ *such that* $\mathbf{G}_{*,\mathbf{u}} = \omega_M^\alpha \cdot \mathbf{G}_{*,\mathbf{v}}$*, or* $\langle \mathbf{G}_{*,\mathbf{u}}, \mathbf{G}_{*,\mathbf{v}}\rangle = 0$*.*

Proof. The rows of $\mathbf{H}$ are restrictions of $\mathbf{F}$. Any two rows $\mathbf{H}_{\mathbf{u},*}, \mathbf{H}_{\mathbf{v},*}$ satisfy

$$\mathbf{H}_{\mathbf{u},*} \circ \overline{\mathbf{H}_{\mathbf{v},*}} = \mathbf{F}_{\mathbf{u}-\mathbf{v},*}|_{\Delta_r} = \mathbf{H}_{\mathbf{u}-\mathbf{v},*},$$

which is a row in $\mathbf{H}$. If this $\mathbf{H}_{\mathbf{u}-\mathbf{v},*}$ is a constant, namely ω_M^α for some $\alpha \in \mathbb{Z}_M$, then $\mathbf{H}_{\mathbf{u},*} = \omega_M^\alpha \mathbf{H}_{\mathbf{v},*}$ holds. Otherwise, Lemma 10.3 says $\langle \mathbf{H}_{\mathbf{u},*}, \mathbf{H}_{\mathbf{v},*}\rangle = 0$.

The proof for $\mathbf{G}$ is exactly the same. □

As part of a discrete unitary matrix $\mathbf{F}$, all columns $\{\mathbf{H}_{*,\mathbf{u}} \,|\, \mathbf{u} \in \Delta_r\}$ of $\mathbf{H}$ must be orthogonal and thus $\text{rank}(\mathbf{H}) = |\Delta_r|$. We denote by n the cardinality $|\Delta_r|$. There must be n linearly independent rows in $\mathbf{H}$. We may start with $\mathfrak{b}_0 = \mathbf{0}$, and assume the following n vectors $\mathfrak{b}_0 = \mathbf{0}, \mathfrak{b}_1, \ldots, \mathfrak{b}_{n-1} \in \mathbb{Z}_\mathcal{Q}$ are the indices of a set of linearly independent rows. By Lemma 10.4, these must be orthogonal as row vectors (over $\mathbb{C}$). Since the rank of the matrix $\mathbf{H}$ is exactly n, it is clear that all other rows must be a multiple of these rows, since the only alternative is to be orthogonal to them all, by Lemma 10.4 again, which is absurd. A symmetric statement for $\mathbf{G}$ also holds.

11 Proof of Theorem 5.6

Let $((M, N), \mathbf{C}, \mathfrak{D}, (\mathbf{p}, \mathbf{t}, \mathcal{Q}))$ be a tuple that satisfies both conditions $(\mathcal{R})$ and $(\mathcal{L})$ (including $(\mathcal{L}_3)$). We also assume that $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is not #P-hard. By $(\mathcal{L})$, we have

$$\Lambda_r = \prod_{i=1}^{s} \Lambda_{r,i} \quad \text{for every } r \in \mathcal{S}, \quad \text{and} \quad \Delta_r = \prod_{i=1}^{s} \Delta_{r,i} \quad \text{for every } r \in \mathcal{T},$$

where both $\Lambda_{r,i}$ and $\Delta_{r,i}$ are cosets in $\mathbb{Z}_{\mathbf{q}_i}$.

Let r be an integer in $\mathcal{S}$. Below we will prove $(\mathcal{D}_1)$ and $(\mathcal{D}_3)$ for Λ_r. The other parts of the theorem, that is, $(\mathcal{D}_2)$ and $(\mathcal{D}_4)$, can be proved similarly.

Let $\mathbf{G}$ denote the $|\Lambda_r| \times m$ submatrix of $\mathbf{F}$ whose row set is $\Lambda_r \subseteq \mathbb{Z}_{\mathcal{Q}}$. We start with the following simple lemma about $\mathbf{G}$. In this section we denote by n the cardinality $|\Lambda_r| \geq 1$. A symmetric statement also holds for the $m \times |\Delta_r|$ submatrix of $\mathbf{F}$ whose column set is Δ_r, where we replace $n = |\Lambda_r|$ by $|\Delta_r|$, which could be different.

Lemma 11.1. *There exist vectors $\mathfrak{b}_0 = \mathbf{0}, \mathfrak{b}_1, \ldots, \mathfrak{b}_{n-1} \in \mathbb{Z}_{\mathcal{Q}}$ such that*

1. *$\{\mathbf{G}_{*,\mathfrak{b}_i} \,\big|\, i \in [0 : n-1]\}$ forms an orthogonal basis;*
2. *For all $\mathbf{b} \in \mathbb{Z}_{\mathcal{Q}}$, there exist $i \in [0 : n-1]$ and $\alpha \in \mathbb{Z}_M$ such that $\mathbf{G}_{*,\mathbf{b}} = \omega_M^{\alpha} \cdot \mathbf{G}_{*,\mathfrak{b}_i}$; and*
3. *Let A_i denote the set of $\mathbf{b} \in \mathbb{Z}_{\mathcal{Q}}$ such that $\mathbf{G}_{*,\mathbf{b}}$ is linearly dependent with $\mathbf{G}_{*,\mathfrak{b}_i}$, then*

$$|A_0| = |A_1| = \ldots = |A_{n-1}| = \frac{m}{n}.$$

Proof. By Lemma 10.4, and the discussion following Lemma 10.4 (the symmetric statements regarding Λ_r and $\mathbf{G}$), there exist vectors $\mathfrak{b}_0 = \mathbf{0}, \mathfrak{b}_1, \ldots, \mathfrak{b}_{n-1} \in \mathbb{Z}_{\mathcal{Q}}$ such that Properties 1) and 2) hold.

We now prove property 3). By condition $(\mathcal{R}_3)$, fixing $\mathfrak{b}_i$, for any i, there is a one-to-one correspondence between A_i and A_0, by $\mathbf{b} \mapsto \mathbf{b} - \mathfrak{b}_i$. This is clear from $\mathbf{G}_{\mathbf{b}-\mathfrak{b}_i,*} = \mathbf{G}_{\mathbf{b},*} \circ \overline{\mathbf{G}_{\mathfrak{b}_i,*}}$. Hence we have $A_0 = \{\mathbf{b} - \mathfrak{b}_i \mid \mathbf{b} \in A_i\}$ for all sets A_i. It then follows that $|A_0| = |A_1| = \ldots = |A_{n-1}| = m/n$. $\square$

Now let $G = (V, E)$ be an undirected graph. For every positive integer p, we can build a new graph $G^{[p]}$ from G by replacing every edge $e = uv \in E$ with a gadget. We will need $G^{[2]}$ in the proof. But it is more convenient to describe $G^{[1]}$ first and illustrate it only with the case $p = 1$. (The picture for $G^{[2]}$ will be too cumbersome to draw.) The gadget for $G^{[1]}$ is shown in Figure 8.

More exactly, we have $G^{[1]} = (V^{[1]}, E^{[1]})$ where

$$V^{[1]} = V \cup \big\{x_e, y_e, a_{e,i}, a'_{e,i}, b_e, b'_e, c_{e,i}, c'_{e,i}, d_{e,j}, d'_{e,j}, w_e, w'_e, z_e, z'_e \,\big|\, e \in E, i \in [N-1], j \in [r+1]\big\},$$

and $E^{[1]}$ contains exactly the following edges: For every edge $e = uv \in E$,

1. one edge between $(u, d_{e,j})$ for all $j \in [r+1] - \{2\}$;
2. $N-1$ edges between $(v, d_{e,j})$ for all $j \in [r+1] - \{1\}$;
3. one edge between $(d_{e,1}, w_e)$, $(d_{e,2}, z_e)$, (w_e, y_e) and (z_e, x_e);
4. $N-1$ edges between $(d_{e,1}, z_e)$, $(d_{e,2}, w_e)$, (w_e, x_e) and (z_e, y_e);
5. one edge between $(a_{e,i}, d_{e,j})$ for all $i \in [N-1]$ and $j \in [r+1] - \{2\}$;
6. one edge between $(b_e, d_{e,j})$ for all $j \in [r+1] - \{1\}$;

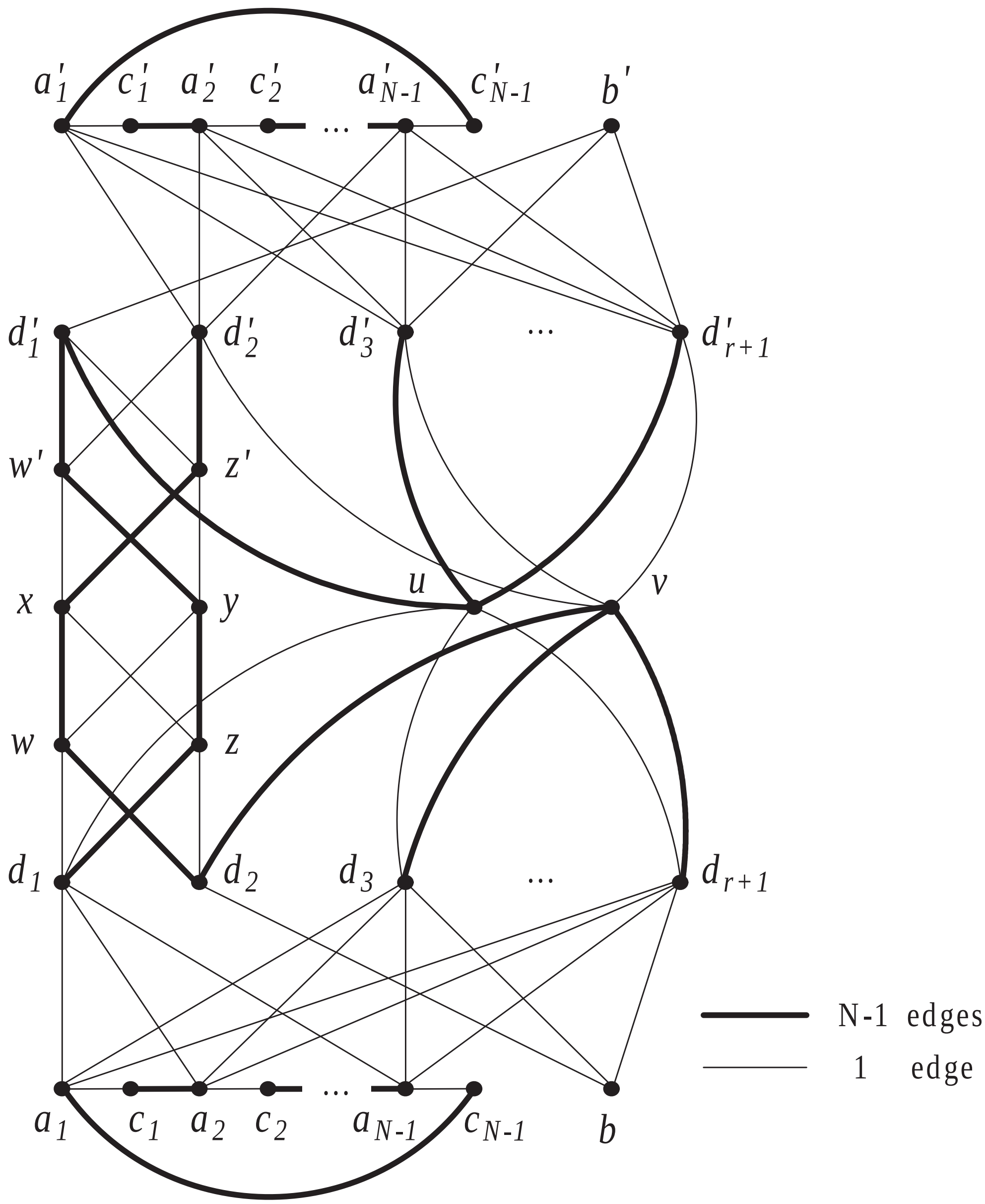

Figure 8: The gadget for constructing $G^{[1]}$ (Note that the subscript e is suppressed).

7. $N-1$ edges between $(c_{e,N-1}, a_{e,1})$ and $(c_{e,i}, a_{e,i+1})$ for all $i \in [N-2]$;
8. one edge between $(a_{e,i}, c_{e,i})$ for all $i \in [N-1]$;
9. $N-1$ edges between $(u, d'_{e,j})$ for all $j \in [r+1] - \{2\}$;
10. one edge between $(v, d'_{e,j})$ for all $j \in [r+1] - \{1\}$;
11. one edge between $(d'_{e,1}, z'_e)$, $(d'_{e,2}, w'_e)$, (w'_e, x_e) and (z'_e, y_e);
12. $N-1$ edges between $(d'_{e,1}, w'_e)$, $(d'_{e,2}, z'_e)$, (w'_e, y_e) and (z'_e, x_e);
13. one edge between $(a'_{e,i}, d'_{e,j})$ for all $i \in [N-1]$ and $j \in [r+1] - \{1\}$;
14. one edges between $(b'_e, d'_{e,j})$ for all $j \in [r+1] - \{2\}$;
15. $N-1$ edges between $(c'_{e,N-1}, a'_{e,1})$ and $(c'_{e,i}, a'_{e,i+1})$ for all $i \in [N-2]$;
16. one edge between $(a'_{e,i}, c'_{e,i})$ for all $i \in [N-1]$.

As indicated earlier, the graph we really need in the proof is $G^{[2]}$. The gadget for $G^{[2]}$ can be built from the one for $G^{[1]}$ in Figure 8 as follows: First, we make a new copy of the subgraph spanned by vertices

$$\{u, v, x, y, w, z, d_j, a_i, c_i, b \mid i \in [N-1], j \in [r+1]\}.$$

All vertices are new except x, y, u and v. Second, make a new copy of the subgraph spanned by

$$\{u, v, x, y, w', z', d'_j, a'_i, c'_i, b' \mid i \in [N-1], j \in [r+1]\}.$$

Again all vertices are new except x, y, u and v. In this way, we get a new gadget and we use it to build $G^{[2]}$ by replacing every edge $e = uv \in E$ with this gadget.

It is easy to verify that the degree of every vertex in $G^{[2]}$ is a $0 \pmod N$ except both copies of $a_{e,i}$, $a'_{e,i}, b_e$ and b'_e whose degree is $r \pmod N$. The construction gives us a $2m \times 2m$ matrix $\mathbf{A}$ such that

$$Z_{\mathbf{A}}(G) = Z_{\mathbf{C},\mathfrak{D}}(G^{[2]}), \quad \text{for any undirected graph } G,$$

and thus, $\mathsf{EVAL}(\mathbf{A})$ ($\le \mathsf{EVAL}(\mathbf{C},\mathfrak{D})$) (right now it is not clear whether $\mathbf{A}$ is a symmetric matrix, which we will prove later) is not #P-hard. We index the rows (columns) of $\mathbf{A}$ in the same way as we do for $\mathbf{C}$: The first m rows (columns) are indexed by $\{0\} \times \mathbb{Z}_\mathcal{Q}$ and the last m rows (columns) are indexed by $\{1\} \times \mathbb{Z}_\mathcal{Q}$. Since $\mathbf{C}$ is the bipartisation of $\mathbf{F}$, we have $A_{(0,\mathbf{u}),(1,\mathbf{v})} = A_{(1,\mathbf{u}),(0,\mathbf{v})} = 0$, for all $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_\mathcal{Q}$.

We now analyze the upper-left $m \times m$ block of $\mathbf{A}$. For $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_\mathcal{Q}$, we have

$$A_{(0,\mathbf{u}),(0,\mathbf{v})} = \sum_{\mathbf{x},\mathbf{y} \in \mathbb{Z}_\mathcal{Q}} A^2_{\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}} B^2_{\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}},$$

where

$$\begin{aligned} A_{\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}} \;=\; & \sum_{\mathbf{a}_1,\ldots,\mathbf{a}_{N-1},\mathbf{b} \in \Lambda_r, \mathbf{d}_1,\mathbf{d}_2 \in \mathbb{Z}_\mathcal{Q}} D^{[r]}_{(0,\mathbf{b})} \prod_{i=1}^{N-1} D^{[r]}_{(0,\mathbf{a}_i)} \left(\sum_{\mathbf{w} \in \mathbb{Z}_\mathcal{Q}} F_{\mathbf{w},\mathbf{d}_1} F_{\mathbf{w},\mathbf{y}} \overline{F_{\mathbf{w},\mathbf{d}_2} F_{\mathbf{w},\mathbf{x}}} \right) \\ & \times \left(\sum_{\mathbf{z} \in \mathbb{Z}_\mathcal{Q}} F_{\mathbf{z},\mathbf{d}_2} F_{\mathbf{z},\mathbf{x}} \overline{F_{\mathbf{z},\mathbf{d}_1} F_{\mathbf{z},\mathbf{y}}} \right) \left(\prod_{i=1}^{N-2} \sum_{\mathbf{c}_i \in \mathbb{Z}_\mathcal{Q}} F_{\mathbf{a}_i,\mathbf{c}_i} \overline{F_{\mathbf{a}_{i+1},\mathbf{c}_i}} \right) \left(\sum_{\mathbf{c}_{N-1} \in \mathbb{Z}_\mathcal{Q}} F_{\mathbf{a}_{N-1},\mathbf{c}_{N-1}} \overline{F_{\mathbf{a}_1,\mathbf{c}_{N-1}}} \right) \\ & \times \left(\prod_{i=3}^{r+1} \sum_{\mathbf{d}_i \in \mathbb{Z}_\mathcal{Q}} F_{\mathbf{u},\mathbf{d}_i} F_{\mathbf{b},\mathbf{d}_i} \overline{F_{\mathbf{v},\mathbf{d}_i}} \prod_{j=1}^{N-1} F_{\mathbf{a}_j,\mathbf{d}_i} \right) F_{\mathbf{u},\mathbf{d}_1} \left(\prod_{j=1}^{N-1} F_{\mathbf{a}_j,\mathbf{d}_1} \right) \overline{F_{\mathbf{v},\mathbf{d}_2}} F_{\mathbf{b},\mathbf{d}_2}, \quad \text{and} \end{aligned}$$

$$B_{\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}} = \sum_{\mathbf{a}_1,\ldots,\mathbf{a}_{N-1},\mathbf{b}\in\Lambda_r,\mathbf{d}_1,\mathbf{d}_2\in\mathbb{Z}_\mathcal{Q}} D^{[r]}_{(0,\mathbf{b})} \prod_{i=1}^{N-1} D^{[r]}_{(0,\mathbf{a}_i)} \left(\sum_{\mathbf{w}\in\mathbb{Z}_\mathcal{Q}} F_{\mathbf{w},\mathbf{d}_2} F_{\mathbf{w},\mathbf{x}} \overline{F_{\mathbf{w},\mathbf{d}_1} F_{\mathbf{w},\mathbf{y}}}\right)$$
$$\times \left(\sum_{\mathbf{z}\in\mathbb{Z}_\mathcal{Q}} F_{\mathbf{z},\mathbf{d}_1} F_{\mathbf{z},\mathbf{y}} \overline{F_{\mathbf{z},\mathbf{d}_2} F_{\mathbf{z},\mathbf{x}}}\right) \left(\prod_{i=1}^{N-2} \sum_{\mathbf{c}_i\in\mathbb{Z}_\mathcal{Q}} F_{\mathbf{a}_i,\mathbf{c}_i} \overline{F_{\mathbf{a}_{i+1},\mathbf{c}_i}}\right) \left(\sum_{\mathbf{c}_{N-1}\in\mathbb{Z}_\mathcal{Q}} F_{\mathbf{a}_{N-1},\mathbf{c}_{N-1}} \overline{F_{\mathbf{a}_1,\mathbf{c}_{N-1}}}\right)$$
$$\times \left(\prod_{i=3}^{r+1} \sum_{\mathbf{d}_i\in\mathbb{Z}_\mathcal{Q}} F_{\mathbf{v},\mathbf{d}_i} F_{\mathbf{b},\mathbf{d}_i} \overline{F_{\mathbf{u},\mathbf{d}_i}} \prod_{j=1}^{N-1} F_{\mathbf{a}_j,\mathbf{d}_i}\right) F_{\mathbf{v},\mathbf{d}_2} \left(\prod_{j=1}^{N-1} F_{\mathbf{a}_j,\mathbf{d}_2}\right) \overline{F_{\mathbf{u},\mathbf{d}_1}} F_{\mathbf{b},\mathbf{d}_1}.$$

We simplify $A_{\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}}$ first. Since $\mathbf{F}$ is discrete unitary and satisfies $(\mathcal{R}_3)$, we have

$$\sum_{\mathbf{w}\in\mathbb{Z}_\mathcal{Q}} F_{\mathbf{w},\mathbf{d}_1} F_{\mathbf{w},\mathbf{y}} \overline{F_{\mathbf{w},\mathbf{d}_2} F_{\mathbf{w},\mathbf{x}}} = \langle \mathbf{F}_{*,\mathbf{d}_1+\mathbf{y}}, \mathbf{F}_{*,\mathbf{d}_2+\mathbf{x}}\rangle$$

is zero unless $\mathbf{d}_1 - \mathbf{d}_2 = \mathbf{x} - \mathbf{y}$. When this equation holds, the inner product $\langle \mathbf{F}_{*,\mathbf{d}_1+\mathbf{y}}, \mathbf{F}_{*,\mathbf{d}_2+\mathbf{x}}\rangle = m$. Also when $\mathbf{d}_1 - \mathbf{d}_2 = \mathbf{x} - \mathbf{y}$ the sum $\sum_{\mathbf{z}\in\mathbb{Z}_\mathcal{Q}} F_{\mathbf{z},\mathbf{d}_2} F_{\mathbf{z},\mathbf{x}} \overline{F_{\mathbf{z},\mathbf{d}_1} F_{\mathbf{z},\mathbf{y}}} = m$ as well. Similarly,

$$\sum_{\mathbf{c}_i\in\mathbb{Z}_\mathcal{Q}} F_{\mathbf{a}_i,\mathbf{c}_i} \overline{F_{\mathbf{a}_{i+1},\mathbf{c}_i}} = \langle \mathbf{F}_{\mathbf{a}_i,*}, \mathbf{F}_{\mathbf{a}_{i+1},*}\rangle$$

is zero unless $\mathbf{a}_i = \mathbf{a}_{i+1}$, for $i = 1, \ldots, N-2$. Also, we have

$$\sum_{\mathbf{c}_{N-1}\in\mathbb{Z}_\mathcal{Q}} F_{\mathbf{a}_{N-1},\mathbf{c}_{N-1}} \overline{F_{\mathbf{a}_1,\mathbf{c}_{N-1}}} = \langle \mathbf{F}_{\mathbf{a}_{N-1},*}, \mathbf{F}_{\mathbf{a}_1,*}\rangle$$

is zero unless $\mathbf{a}_{N-1} = \mathbf{a}_1$. When $\mathbf{a}_1 = \ldots = \mathbf{a}_{N-1}$, all these inner products are equal to m. So now we may assume $\mathbf{d}_1 - \mathbf{d}_2 = \mathbf{x} - \mathbf{y}$ and all $\mathbf{a}_i$'s are equal, call it $\mathbf{a}$, in the sum for $A_{\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}}$.

Let $\mathbf{x} - \mathbf{y} = \mathbf{o}$, then $A_{\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}}$ is equal to

$$m^{N+1} \sum_{\mathbf{a},\mathbf{b}\in\Lambda_r,\mathbf{d}_2\in\mathbb{Z}_\mathcal{Q}} D^{[r]}_{(0,\mathbf{b})} \overline{D^{[r]}_{(0,\mathbf{a})}} \left(\prod_{i=3}^{r+1} \sum_{\mathbf{d}_i\in\mathbb{Z}_\mathcal{Q}} F_{\mathbf{u},\mathbf{d}_i} F_{\mathbf{b},\mathbf{d}_i} \overline{F_{\mathbf{v},\mathbf{d}_i} F_{\mathbf{a},\mathbf{d}_i}}\right) F_{\mathbf{u},\mathbf{d}_2+\mathbf{o}} F_{\mathbf{b},\mathbf{d}_2} \overline{F_{\mathbf{v},\mathbf{d}_2} F_{\mathbf{a},\mathbf{d}_2+\mathbf{o}}}. \qquad (71)$$

Again,

$$\sum_{\mathbf{d}_i\in\mathbb{Z}_\mathcal{Q}} F_{\mathbf{u},\mathbf{d}_i} F_{\mathbf{b},\mathbf{d}_i} \overline{F_{\mathbf{v},\mathbf{d}_i} F_{\mathbf{a},\mathbf{d}_i}} = \langle \mathbf{F}_{\mathbf{u}+\mathbf{b},*}, \mathbf{F}_{\mathbf{v}+\mathbf{a},*}\rangle = 0$$

unless $\mathbf{u} + \mathbf{b} = \mathbf{v} + \mathbf{a}$. When $\mathbf{u} + \mathbf{b} = \mathbf{v} + \mathbf{a}$, the inner product $\langle \mathbf{F}_{\mathbf{u}+\mathbf{b},*}, \mathbf{F}_{\mathbf{v}+\mathbf{a},*}\rangle = m$. As a result, if

$$\mathbf{v} - \mathbf{u} \notin \Lambda_r^{\text{lin}} \equiv \{\mathbf{x} - \mathbf{x}' \mid \mathbf{x}, \mathbf{x}' \in \Lambda_r\},$$

then $A_{\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}} = 0$ since $\mathbf{a}, \mathbf{b} \in \Lambda_r$ and $\mathbf{b} - \mathbf{a} \in \Lambda_r^{\text{lin}}$.

For every vector $\mathbf{h} \in \Lambda_r^{\text{lin}}$ (e.g., $\mathbf{h} = \mathbf{v} - \mathbf{u}$), we define a $|\Lambda_r|$-dimensional vector $\mathbf{T}^{[\mathbf{h}]}$ as follows:

$$T^{[\mathbf{h}]}_{\mathbf{x}} = D^{[r]}_{(0,\mathbf{x}+\mathbf{h})} \overline{D^{[r]}_{(0,\mathbf{x})}}, \quad \text{for all } \mathbf{x} \in \Lambda_r.$$

By $(\mathcal{L})$, Λ_r is a coset in $\mathbb{Z}_\mathcal{Q}$, so for any $\mathbf{x} \in \Lambda_r$, we also have $\mathbf{x} + \mathbf{h} \in \Lambda_r$. Therefore every entry of $\mathbf{T}^{[\mathbf{h}]}$ is non-zero and is a power of ω_N.

Now we use $\mathbf{T}^{[\mathbf{v}-\mathbf{u}]}$ to express $A_{\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}}$. Suppose $\mathbf{v}-\mathbf{u}\in\Lambda_r^{\text{lin}}$, then

$$\begin{aligned} A_{\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}} &= m^{N+r}\sum_{\mathbf{a}\in\Lambda_r,\mathbf{d}_2\in\mathbb{Z}_\mathcal{Q},\mathbf{b}=\mathbf{a}+\mathbf{v}-\mathbf{u}} D^{[r]}_{(0,\mathbf{b})}\overline{D^{[r]}_{(0,\mathbf{a})}}F_{\mathbf{u},\mathbf{d}_2+\mathbf{o}}F_{\mathbf{b},\mathbf{d}_2}\overline{F_{\mathbf{v},\mathbf{d}_2}F_{\mathbf{a},\mathbf{d}_2+\mathbf{o}}} \\ &= m^{N+r+1}\sum_{\mathbf{a}\in\Lambda_r} D^{[r]}_{(0,\mathbf{a}+\mathbf{v}-\mathbf{u})}\overline{D^{[r]}_{(0,\mathbf{a})}}F_{\mathbf{u},\mathbf{o}}\overline{F_{\mathbf{a},\mathbf{o}}} \;=\; m^{N+r+1}F_{\mathbf{u},\mathbf{x}-\mathbf{y}}\langle\mathbf{T}^{[\mathbf{v}-\mathbf{u}]},\mathbf{G}_{*,\mathbf{x}-\mathbf{y}}\rangle. \end{aligned}$$

Here we used $(\mathcal{R}_3)$ in the second equality, and we recall the definition of $\mathbf{o}=\mathbf{x}-\mathbf{y}$.

Similarly, when $\mathbf{v}-\mathbf{u}\notin\Lambda_r^{\text{lin}}$, we have $B_{\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}}=0$; and when $\mathbf{v}-\mathbf{u}\in\Lambda_r^{\text{lin}}$,

$$\begin{aligned} B_{\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}} &= m^{N+r}\sum_{\mathbf{b}\in\Lambda_r,\mathbf{d}_2\in\mathbb{Z}_\mathcal{Q},\mathbf{a}=\mathbf{b}+\mathbf{v}-\mathbf{u}} D^{[r]}_{(0,\mathbf{b})}\overline{D^{[r]}_{(0,\mathbf{a})}}F_{\mathbf{v},\mathbf{d}_2}F_{\mathbf{b},\mathbf{d}_2+\mathbf{x}-\mathbf{y}}\overline{F_{\mathbf{a},\mathbf{d}_2}F_{\mathbf{u},\mathbf{d}_2+\mathbf{x}-\mathbf{y}}} \\ &= m^{N+r}\sum_{\mathbf{b}\in\Lambda_r,\mathbf{d}_2\in\mathbb{Z}_\mathcal{Q}} D^{[r]}_{(0,\mathbf{b})}\overline{D^{[r]}_{(0,\mathbf{b}+\mathbf{v}-\mathbf{u})}}F_{\mathbf{b},\mathbf{x}-\mathbf{y}}\overline{F_{\mathbf{u},\mathbf{x}-\mathbf{y}}} \;=\; m^{N+r+1}\overline{F_{\mathbf{u},\mathbf{x}-\mathbf{y}}\langle\mathbf{T}^{[\mathbf{v}-\mathbf{u}]},\mathbf{G}_{*,\mathbf{x}-\mathbf{y}}\rangle}. \end{aligned}$$

To summarize, when $\mathbf{v}-\mathbf{u}\notin\Lambda_r^{\text{lin}}$, $A_{(0,\mathbf{u}),(0,\mathbf{v})}=0$; and when $\mathbf{v}-\mathbf{u}\in\Lambda_r^{\text{lin}}$,

$$A_{(0,\mathbf{u}),(0,\mathbf{v})}=m^{4(N+r+1)}\sum_{\mathbf{x},\mathbf{y}\in\mathbb{Z}_\mathcal{Q}}\left|\langle\mathbf{T}^{[\mathbf{v}-\mathbf{u}]},\mathbf{G}_{*,\mathbf{x}-\mathbf{y}}\rangle\right|^4=m^{4N+4r+5}\sum_{\mathbf{b}\in\mathbb{Z}_\mathcal{Q}}\left|\langle\mathbf{T}^{[\mathbf{v}-\mathbf{u}]},\mathbf{G}_{*,\mathbf{b}}\rangle\right|^4. \tag{72}$$

We now show that $\mathbf{A}$ is a symmetric non-negative matrix. Let $\mathbf{a}=\mathbf{v}-\mathbf{u}\in\Lambda_r^{\text{lin}}$. Then by $(\mathcal{R}_3)$, we have for every $\mathbf{b}\in\mathbb{Z}_\mathcal{Q}$,

$$\begin{aligned} \left|\langle\mathbf{T}^{[-\mathbf{a}]},\mathbf{G}_{*,-\mathbf{b}}\rangle\right| &= \left|\sum_{\mathbf{x}\in\Lambda_r}D^{[r]}_{\mathbf{x}-\mathbf{a}}\overline{D^{[r]}_{\mathbf{x}}G_{\mathbf{x},-\mathbf{b}}}\right| = \left|\sum_{\mathbf{x}\in\Lambda_r}D^{[r]}_{\mathbf{x}}\overline{D^{[r]}_{\mathbf{x}-\mathbf{a}}G_{\mathbf{x},\mathbf{b}}}\right| \\ &= \left|\sum_{\mathbf{y}\in\Lambda_r}D^{[r]}_{\mathbf{y}+\mathbf{a}}\overline{D^{[r]}_{\mathbf{y}}G_{\mathbf{y},\mathbf{b}}F_{\mathbf{a},\mathbf{b}}}\right| = \left|\sum_{\mathbf{y}\in\Lambda_r}D^{[r]}_{\mathbf{y}+\mathbf{a}}\overline{D^{[r]}_{\mathbf{y}}G_{\mathbf{y},\mathbf{b}}}\right| = \left|\langle\mathbf{T}^{[\mathbf{a}]},\mathbf{G}_{*,\mathbf{b}}\rangle\right|, \end{aligned}$$

where the second equation is by conjugation, the third equation is by the substitution $\mathbf{x}=\mathbf{y}+\mathbf{a}$ and the fourth equation is because $F_{\mathbf{a},\mathbf{b}}$ is a root of unity. It then follows that $A_{(0,\mathbf{u}),(0,\mathbf{v})}=A_{(0,\mathbf{v}),(0,\mathbf{u})}$. The lower-right block can be proved similarly. Hence $\mathbf{A}$ is symmetric.

Next, we further simplify (72) using Lemma 11.1:

$$A_{(0,\mathbf{u}),(0,\mathbf{v})}=\frac{m^{4N+4r+6}}{n}\cdot\sum_{i=0}^{n-1}\left|\langle\mathbf{T}^{[\mathbf{v}-\mathbf{u}]},\mathbf{G}_{*,\mathfrak{b}_i}\rangle\right|^4. \tag{73}$$

For the special case when $\mathbf{u}=\mathbf{v}$, we know exactly what $A_{(0,\mathbf{u}),(0,\mathbf{u})}$ is: Since $\mathbf{T}^{[\mathbf{0}]}=\mathbf{1}=\mathbf{G}_{*,\mathfrak{b}_0}$, we have

$$\langle\mathbf{T}^{[\mathbf{0}]},\mathbf{G}_{*,\mathfrak{b}_0}\rangle=n;$$

By Lemma 11.1, $\{\mathbf{G}_{*,\mathfrak{b}_0},\ldots,\mathbf{G}_{*,\mathfrak{b}_{n-1}}\}$ is an orthogonal basis, hence

$$\sum_{i=0}^{n-1}\left|\langle\mathbf{T}^{[\mathbf{0}]},\mathbf{G}_{*,\mathfrak{b}_i}\rangle\right|^4=n^4\quad\text{and}\quad A_{(0,\mathbf{u}),(0,\mathbf{u})}=L\cdot n^4,\quad\text{where } L\equiv m^{4N+4r+6}/n.$$

Our next goal is to prove (75). Note that if $|\Lambda_r^{\text{lin}}| = 1$ then (75) is trivially true. So below we assume $|\Lambda_r^{\text{lin}}| > 1$. Because $\mathbf{A}$ is symmetric and non-negative, we can apply the dichotomy theorem of Bulatov and Grohe. For any pair $\mathbf{u} \neq \mathbf{v}$ such that $\mathbf{u} - \mathbf{v} \in \Lambda_r^{\text{lin}}$, we consider the following 2×2 submatrix

$$\begin{pmatrix} A_{(0,\mathbf{u}),(0,\mathbf{u})} & A_{(0,\mathbf{u}),(0,\mathbf{v})} \\ A_{(0,\mathbf{v}),(0,\mathbf{u})} & A_{(0,\mathbf{v}),(0,\mathbf{v})} \end{pmatrix}$$

of $\mathbf{A}$. Since $\mathsf{EVAL}(\mathbf{A})$ is assumed to be not #P-hard, by Corollary 2.1, we have

$$A_{(0,\mathbf{u}),(0,\mathbf{v})} = A_{(0,\mathbf{v}),(0,\mathbf{u})} \in \{0, L \cdot n^4\},$$

and thus from (73), we get

$$\sum_{i=0}^{n-1} \left| \langle \mathbf{T}^{[\mathbf{v}-\mathbf{u}]}, \mathbf{G}_{*,\mathfrak{b}_i} \rangle \right|^4 \in \{0, n^4\}, \quad \text{for all } \mathbf{u}, \mathbf{v} \text{ such that } \mathbf{u} - \mathbf{v} \in \Lambda_r^{\text{lin}}. \tag{74}$$

However, the sum in (74) cannot be zero. This is because the following: By Lemma 11.1, $\{\mathbf{G}_{*,\mathfrak{b}_i} \mid i \in [0:n-1]\}$ is an orthogonal basis, with each $\|\mathbf{G}_{*,\mathfrak{b}_i}\|^2 = n$. Then by Parseval,

$$\sum_{i=0}^{n-1} \left| \langle \mathbf{T}^{[\mathbf{v}-\mathbf{u}]}, \frac{\mathbf{G}_{*,\mathfrak{b}_i}}{\|\mathbf{G}_{*,\mathfrak{b}_i}\|} \rangle \right|^2 = \|\mathbf{T}^{[\mathbf{v}-\mathbf{u}]}\|^2 = n,$$

since each entry of $\mathbf{T}^{[\mathbf{v}-\mathbf{u}]}$ is a root of unity. Hence, $\sum_{i=0}^{n-1} |\langle \mathbf{T}^{[\mathbf{v}-\mathbf{u}]}, \mathbf{G}_{*,\mathfrak{b}_i} \rangle|^2 = n^2$. This shows that for some $0 \leq i < n$, $|\langle \mathbf{T}^{[\mathbf{v}-\mathbf{u}]}, \mathbf{G}_{*,\mathfrak{b}_i} \rangle| \neq 0$, and therefore, the sum in (74) is non-zero, and thus in fact

$$\sum_{i=0}^{n-1} \left| \langle \mathbf{T}^{[\mathbf{v}-\mathbf{u}]}, \mathbf{G}_{*,\mathfrak{b}_i} \rangle \right|^4 = n^4, \quad \text{for all } \mathbf{u}, \mathbf{v} \text{ such that } \mathbf{u} - \mathbf{v} \in \Lambda_r^{\text{lin}}.$$

If we temporarily denote $x_i = |\langle \mathbf{T}^{[\mathbf{v}-\mathbf{u}]}, \mathbf{G}_{*,\mathfrak{b}_i} \rangle|$, for $0 \leq i < n$, then each $x_i \geq 0$. We have both

$$\sum_{i=0}^{n-1} x_i^2 = n^2 \quad \text{and} \quad \sum_{i=0}^{n-1} x_i^4 = n^4.$$

By taking the square, we have

$$n^4 = \left(\sum_{i=0}^{n-1} x_i^2 \right)^2 = \sum_{i=0}^{n-1} x_i^4 + \text{non-negative cross terms}.$$

It follows that all cross terms must be zero. Thus, there exists a unique term $x_i \neq 0$. Moreover, this x_i must equal to n while all other $x_j = 0$. We conclude that, for all $\mathbf{u}$ and $\mathbf{v} \in \mathbb{Z}_\mathcal{Q}$ such that $\mathbf{u} - \mathbf{v} \in \Lambda_r^{\text{lin}}$, there exists a unique $i \in [0:n-1]$ such that

$$\left| \langle \mathbf{T}^{[\mathbf{v}-\mathbf{u}]}, \mathbf{G}_{*,\mathfrak{b}_i} \rangle \right| = n.$$

Again apply the argument that $\langle \mathbf{T}^{[\mathbf{v}-\mathbf{u}]}, \mathbf{G}_{*,\mathfrak{b}_i} \rangle$ is a sum of n terms, each of which is a root of unity, we can conclude the following: For all $\mathbf{a} \in \Lambda_r^{\text{lin}}$, there exist $\mathbf{b} \in \mathbb{Z}_\mathcal{Q}$ and $\alpha \in \mathbb{Z}_N$ such that

$$\mathbf{T}^{[\mathbf{a}]} = \omega_N^\alpha \cdot \mathbf{G}_{*,\mathbf{b}}. \tag{75}$$

Below we use (75) to prove ($\mathcal{D}_3$). Note that, if $s = 1$, then ($\mathcal{D}_3$) follows directly from (75). So below we assume $s > 1$. First, (75) implies the following useful lemma:

Lemma 11.2. *Let* $\mathbf{a}$ *be a vector in* $\Lambda_{r,k}^{\text{lin}}$ *for some* $k \in [s]$*. Then for every* $\mathbf{c} \in \Lambda_{r,\ell}^{\text{lin}}$*, where* $\ell \neq k$*,*

$$T_{\mathbf{x}+\widetilde{\mathbf{c}}}^{[\widetilde{\mathbf{a}}]} \Big/ T_{\mathbf{x}}^{[\widetilde{\mathbf{a}}]} \quad \textit{for all } \mathbf{x} \in \Lambda_r,$$

is a power of ω_{q_ℓ}*. (Recall we use* q_ℓ *to denote* $q_{\ell,1}$*. Also note that for every* $\mathbf{x} \in \Lambda_r$*, the translated point* $\mathbf{x} + \widetilde{\mathbf{c}}$ *is in* Λ_r*, so* $\mathbf{T}^{[\widetilde{\mathbf{a}}]}$ *is defined at both* $\mathbf{x}$ *and* $\mathbf{x} + \widetilde{\mathbf{c}}$*. Since they are roots of unity, one can divide one by the other.)*

Proof. By (75), there exists a vector $\mathbf{b} \in \mathbb{Z}_{\mathcal{Q}}$ such that

$$T_{\mathbf{x}+\widetilde{\mathbf{c}}}^{[\widetilde{\mathbf{a}}]} \Big/ T_{\mathbf{x}}^{[\widetilde{\mathbf{a}}]} = G_{\mathbf{x}+\widetilde{\mathbf{c}},\mathbf{b}} \Big/ G_{\mathbf{x},\mathbf{b}} = F_{\widetilde{\mathbf{c}},\mathbf{b}},$$

which, by $(\mathcal{R}_3)$, must be a power of ω_{q_ℓ}. □

Let $\mathbf{a}$ still denote an arbitrary vector in $\Lambda_{r,k}^{\text{lin}}$, and $\mathbf{c} \in \Lambda_{r,\ell}^{\text{lin}}$, where $\ell \neq k$ and $\ell, k \in [s]$. By writing out the definition of $T_{\mathbf{x}}^{[\mathbf{h}]}$ in term of $D_*^{[r]}$, we have

$$T_{\mathbf{x}+\widetilde{\mathbf{a}}}^{[\widetilde{\mathbf{c}}]} \cdot T_{\mathbf{x}}^{[\widetilde{\mathbf{a}}]} = T_{\mathbf{x}}^{[\widetilde{\mathbf{a}}+\widetilde{\mathbf{c}}]} = T_{\mathbf{x}+\widetilde{\mathbf{c}}}^{[\widetilde{\mathbf{a}}]} \cdot T_{\mathbf{x}}^{[\widetilde{\mathbf{c}}]},$$

and thus,

$$T_{\mathbf{x}+\widetilde{\mathbf{a}}}^{[\widetilde{\mathbf{c}}]} \Big/ T_{\mathbf{x}}^{[\widetilde{\mathbf{c}}]} = T_{\mathbf{x}+\widetilde{\mathbf{c}}}^{[\widetilde{\mathbf{a}}]} \Big/ T_{\mathbf{x}}^{[\widetilde{\mathbf{a}}]}.$$

By Lemma 11.2, the left hand side of the equation is a power of ω_{q_k}, while the right hand side of the equation is a power of ω_{q_ℓ}. Since $k \neq \ell$, $\gcd(q_k, q_\ell) = 1$, we have

$$T_{\mathbf{x}+\widetilde{\mathbf{c}}}^{[\widetilde{\mathbf{a}}]} \Big/ T_{\mathbf{x}}^{[\widetilde{\mathbf{a}}]} = 1, \quad \text{for all } \mathbf{c} \in \Lambda_{r,\ell}^{\text{lin}} \text{ such that } \ell \neq k. \tag{76}$$

This implies that $T_{\mathbf{x}}^{[\widetilde{\mathbf{a}}]}$, as a function of $\mathbf{x}$, only depends on $\mathbf{x}_k \in \Lambda_{r,k}$. It then follows from (75) that

$$T_{\mathbf{x}}^{[\widetilde{\mathbf{a}}]} = T_{\mathbf{ext}_r(\mathbf{x}_k)}^{[\widetilde{\mathbf{a}}]} = \omega_N^{\alpha} \cdot G_{\mathbf{ext}_r(\mathbf{x}_k),\mathbf{b}} = \omega_N^{\alpha+\beta} \cdot F_{\widetilde{\mathbf{x}_k},\widetilde{\mathbf{b}_k}} = \omega_N^{\alpha+\beta} \cdot F_{\mathbf{x},\widetilde{\mathbf{b}_k}}, \quad \text{for any } \mathbf{x} \in \Lambda_r,$$

and for some constants $\alpha, \beta \in \mathbb{Z}_N$ and $\mathbf{b}_k \in \mathbb{Z}_{\mathbf{q}_k}$ that are independent of $\mathbf{x}$. This proves condition $(\mathcal{D}_3)$.

Finally we prove $(\mathcal{D}_1)$ from $(\mathcal{D}_3)$.

Recall that, in condition $(\mathcal{L}_3)$, we have $D_{(0,\mathfrak{a}^{[r]})}^{[r]} = 1$. Let $\mathfrak{a}^{[r]} = (\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_s) \in \Lambda_r$, then

$$\begin{aligned}
D_{(0,\mathbf{x})}^{[r]} &= D_{(0,(\mathbf{x}_1,\mathbf{x}_2,\ldots,\mathbf{x}_s))}^{[r]} \overline{D_{(0,(\mathbf{a}_1,\mathbf{a}_2,\ldots,\mathbf{a}_s))}^{[r]}} \\
&= \left(D_{(0,(\mathbf{x}_1,\mathbf{x}_2,\ldots,\mathbf{x}_{s-1},\mathbf{x}_s))}^{[r]} \overline{D_{(0,(\mathbf{x}_1,\mathbf{x}_2,\ldots,\mathbf{x}_{s-1},\mathbf{a}_s))}^{[r]}} \right) \\
&\quad \times \left(D_{(0,(\mathbf{x}_1,\mathbf{x}_2,\ldots,\mathbf{x}_{s-1},\mathbf{a}_s))}^{[r]} \overline{D_{(0,(\mathbf{x}_1,\ldots,\mathbf{x}_{s-2},\mathbf{a}_{s-1},\mathbf{a}_s))}^{[r]}} \right) \\
&\qquad \vdots \\
&\quad \times \left(D_{(0,(\mathbf{x}_1,\mathbf{a}_2,\ldots,\mathbf{a}_s))}^{[r]} \overline{D_{(0,(\mathbf{a}_1,\mathbf{a}_2,\ldots,\mathbf{a}_s))}^{[r]}} \right), \quad \text{for any } \mathbf{x} \in \Lambda_r.
\end{aligned}$$

We consider the k^{th} factor

$$D_{(0,(\mathbf{x}_1,\ldots,\mathbf{x}_{k-1},\mathbf{x}_k,\mathbf{a}_{k+1},\ldots,\mathbf{a}_s))}^{[r]} \overline{D_{(0,(\mathbf{x}_1,\ldots,\mathbf{x}_{k-1},\mathbf{a}_k,\mathbf{a}_{k+1},\ldots,\mathbf{a}_s))}^{[r]}}.$$

By (76) this factor is independent of all other components in the starting point $(\mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{a}_k, \mathbf{a}_{k+1}, \ldots, \mathbf{a}_s)$ *except* the k^{th} component $\mathbf{a}_k$. In particular we can replace all other components, as long as we stay within Λ_r. We choose to replace the first $k-1$ components $\mathbf{x}_i$ by $\mathbf{a}_i$, then

$$D^{[r]}_{(0,(\mathbf{x}_1,\ldots,\mathbf{x}_{k-1},\mathbf{x}_k,\mathbf{a}_{k+1},\ldots,\mathbf{a}_s))}\overline{D^{[r]}_{(0,(\mathbf{x}_1,\ldots,\mathbf{x}_{k-1},\mathbf{a}_k,\mathbf{a}_{k+1},\ldots,\mathbf{a}_s))}}$$

$$= D^{[r]}_{(0,(\mathbf{a}_1,\ldots,\mathbf{a}_{k-1},\mathbf{x}_k,\mathbf{a}_{k+1},\ldots,\mathbf{a}_s))}\overline{D^{[r]}_{(0,(\mathbf{a}_1,\ldots,\mathbf{a}_{k-1},\mathbf{a}_k,\mathbf{a}_{k+1},\ldots,\mathbf{a}_s))}} = D^{[r]}_{(0,\mathbf{ext}_r(\mathbf{x}_k))}\overline{D^{[r]}_{(0,\mathfrak{a}^{[r]})}} = D^{[r]}_{(0,\mathbf{ext}_r(\mathbf{x}_k))}.$$

$(\mathcal{D}_1)$ is proved.

12 Tractability: Proof of Theorem 5.7

Let $((M,N),\mathbf{C},\mathfrak{D},(\mathbf{p},\mathbf{t},\mathcal{Q}))$ be a tuple that satisfies all the three conditions $(\mathcal{R}), (\mathcal{L})$ and $(\mathcal{D})$. In this section, we reduce $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ to the following problem:

> $\mathsf{EVAL}(q)$: Let $q = p^k$ be a prime power for some prime p and positive integer k. The input of $\mathsf{EVAL}(q)$ is a quadratic polynomial $f(x_1, x_2, \ldots, x_n) = \sum_{i,j\in[n]} a_{i,j}x_ix_j$, where $a_{i,j} \in \mathbb{Z}_q$ for all i, j; and the output is
>
> $$Z_q(f) = \sum_{x_1,\ldots,x_n\in\mathbb{Z}_q} \omega_q^{f(x_1,\ldots,x_n)}.$$

We postpone the proof of the following theorem to the end of this section.

Theorem 12.1. *Problem* $\mathsf{EVAL}(q)$ *can be solved in polynomial time (in n: the number of variables).*

The reduction goes as follows: First, we use conditions $(\mathcal{R})$, $(\mathcal{L})$, and $(\mathcal{D})$ to show that $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ can be decomposed into s smaller problems (recall s is the number of primes in the sequence $\mathbf{p}$):

$$\mathsf{EVAL}(\mathbf{C}^{[1]},\mathfrak{D}^{[1]}), \ldots, \mathsf{EVAL}(\mathbf{C}^{[s]},\mathfrak{D}^{[s]}).$$

If every $\mathsf{EVAL}(\mathbf{C}^{[i]},\mathfrak{D}^{[i]})$ is tractable, then so is $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$. Second, for each problem $\mathsf{EVAL}(\mathbf{C}^{[i]},\mathfrak{D}^{[i]})$ where $i \in [s]$, we reduce it to $\mathsf{EVAL}(q)$ for some prime power q which will become clear later, and thus, by Theorem 12.1, all $\mathsf{EVAL}(\mathbf{C}^{[i]},\mathfrak{D}^{[i]})$'s can be solved in polynomial time.

12.1 Step 1

For every integer $i \in [s]$, we define a $2m_i \times 2m_i$ matrix $\mathbf{C}^{[i]}$ where $m_i = |\mathbb{Z}_{\mathbf{q}_i}|$: $\mathbf{C}^{[i]}$ is the bipartisation of the following $m_i \times m_i$ matrix $\mathbf{F}^{[i]}$, where (we index the rows and columns of $\mathbf{F}^{[i]}$ using $\mathbf{x} \in \mathbb{Z}_{\mathbf{q}_i}$ and index the rows and columns of $\mathbf{C}^{[i]}$ using $\{0,1\} \times \mathbb{Z}_{\mathbf{q}_i}$)

$$F^{[i]}_{\mathbf{x},\mathbf{y}} = \prod_{j\in[t_i]} \omega_{q_{i,j}}^{x_jy_j}, \quad \text{for all } \mathbf{x} = (x_1, \ldots, x_{t_i}), \mathbf{y} = (y_1, \ldots, y_{t_i}) \in \mathbb{Z}_{\mathbf{q}_i}. \tag{77}$$

Here we use x_j, where $j \in [t_i]$, to denote the j^{th} entry of $\mathbf{x}$ in $\mathbb{Z}_{q_{i,j}}$. It then follows from $(\mathcal{R}_3)$ that

$$F_{\mathbf{x},\mathbf{y}} = F^{[1]}_{\mathbf{x}_1,\mathbf{y}_1} \cdot F^{[2]}_{\mathbf{x}_2,\mathbf{y}_2} \cdots F^{[s]}_{\mathbf{x}_s,\mathbf{y}_s}, \quad \text{for all } \mathbf{x},\mathbf{y} \in \mathbb{Z}_{\mathcal{Q}}. \tag{78}$$

On the other hand, for each integer $i \in [s]$, we define a sequence of N $2m_i \times 2m_i$ diagonal matrices

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

$\mathbf{D}^{[i,0]}$ is the $2m_i \times 2m_i$ identity matrix; and for every $r \in [N-1]$, we set

$$\mathbf{D}^{[i,r]}_{(0,*)} = \mathbf{0},\ \text{if } r \notin \mathcal{S}, \quad \text{and} \quad D^{[i,r]}_{(0,\mathbf{x})} = D^{[r]}_{(0,\mathbf{ext}_r(\mathbf{x}))} \text{ for all } \mathbf{x} \in \mathbb{Z}_{\mathbf{q}_i},\ \text{if } r \in \mathcal{S}; \quad \text{and}$$

$$\mathbf{D}^{[i,r]}_{(1,*)} = \mathbf{0},\ \text{if } r \notin \mathcal{T}, \quad \text{and} \quad D^{[i,r]}_{(1,\mathbf{x})} = D^{[r]}_{(1,\mathbf{ext}'_r(\mathbf{x}))} \text{ for all } \mathbf{x} \in \mathbb{Z}_{\mathbf{q}_i},\ \text{if } r \in \mathcal{T}.$$

By conditions $(\mathcal{D}_1)$ and $(\mathcal{D}_2)$, we have

$$D^{[r]}_{(b,\mathbf{x})} = D^{[1,r]}_{(b,\mathbf{x}_1)} \cdots D^{[s,r]}_{(b,\mathbf{x}_s)}, \quad \text{for all } b \in \{0,1\} \text{ and } \mathbf{x} \in \mathbb{Z}_{\mathcal{Q}}. \tag{79}$$

Eq. (79) is valid for all $\mathbf{x} \in \mathbb{Z}_{\mathcal{Q}}$: For example for $b=0$ and $\mathbf{x} \in \mathbb{Z}_{\mathcal{Q}} - \Lambda_r$, the left-hand side is 0 because $\mathbf{x} \notin \Lambda_r$. The right-hand side is also 0, since there exists an index $i \in [s]$ such that $\mathbf{x}_i \notin \Lambda_{r,i}$ and thus, $\mathbf{ext}_r(\mathbf{x}_i) \notin \Lambda_r$, and $D^{[i,r]}_{(0,\mathbf{x}_i)} = 0$. It then follows from (77), (79) and the following lemma that

$$\mathsf{EVAL}(\mathbf{C}^{[i]}, \mathfrak{D}^{[i]}) \text{ is in polynomial time for all } i \in [s] \implies \mathsf{EVAL}(\mathbf{C}, \mathfrak{D}) \text{ is in polynomial time.}$$

Lemma 12.1. *For each $i \in \{0,1,2\}$, $\mathbf{F}^{[i]}$ is an $m_i \times m_i$ complex matrix, for some positive integers m_i; $\mathbf{C}^{[i]}$ is the bipartisation of $\mathbf{F}^{[i]}$; and $\mathfrak{D}^{[i]} = \{\mathbf{D}^{[i,0]}, \ldots, \mathbf{D}^{[i,N-1]}\}$ is a sequence of N $2m_i \times 2m_i$ diagonal matrices for some positive integer N, where*

$$\mathbf{D}^{[i,r]} = \begin{pmatrix} \mathbf{P}^{[i,r]} & \\ & \mathbf{Q}^{[i,r]} \end{pmatrix}$$

and both $\mathbf{P}^{[i,r]}$ and $\mathbf{Q}^{[i,r]}$ are $m_i \times m_i$ diagonal matrices.

For each $i \in \{0,1,2\}$, $(\mathbf{C}^{[i]}, \mathfrak{D}^{[i]})$ satisfies (Pinning). Moreover, $m_0 = m_1 \cdot m_2$,

$$\mathbf{F}^{[0]} = \mathbf{F}^{[1]} \otimes \mathbf{F}^{[2]}, \quad \mathbf{P}^{[0,r]} = \mathbf{P}^{[1,r]} \otimes \mathbf{P}^{[2,r]}, \quad \mathbf{Q}^{[0,r]} = \mathbf{Q}^{[1,r]} \otimes \mathbf{Q}^{[2,r]}, \quad \textit{for all } r \in [0:N-1].$$

Then if both $\mathsf{EVAL}(\mathbf{C}^{[1]}, \mathfrak{D}^{[1]})$ and $\mathsf{EVAL}(\mathbf{C}^{[2]}, \mathfrak{D}^{[2]})$ are tractable, $\mathsf{EVAL}(\mathbf{C}^{[0]}, \mathfrak{D}^{[0]})$ is also tractable.

Proof. By the Second Pinning Lemma (Lemma 4.2), we can compute $Z^{\rightarrow}_{\mathbf{C}^{[i]},\mathfrak{D}^{[i]}}$ and $Z^{\leftarrow}_{\mathbf{C}^{[i]},\mathfrak{D}^{[i]}}$, for both $i=1$ and 2, in polynomial time. The lemma then follows from Lemma 2.3. □

We now use condition $(\mathcal{D}_4)$ to prove the following lemma about $\mathbf{D}^{[i,r]}_{(1,*)}$, where $r \in \mathcal{T}$.

Lemma 12.2. *For any $r \in \mathcal{T}$, $i \in [s]$ and $\mathbf{a} \in \Delta^{\text{lin}}_{r,i}$, there exist $\mathbf{b} \in \mathbb{Z}_{\mathbf{q}_i}$ and $\alpha \in \mathbb{Z}_N$ such that*

$$D^{[i,r]}_{(1,\mathbf{x}+\mathbf{a})} \cdot \overline{D^{[i,r]}_{(1,\mathbf{x})}} = \omega_N^{\alpha} \cdot F^{[i]}_{\mathbf{b},\mathbf{x}}, \quad \textit{for all } \mathbf{x} \in \Delta_{r,i}.$$

Proof. By the definition of $\mathbf{D}^{[i,r]}$, we have

$$D^{[i,r]}_{(1,\mathbf{x}+\mathbf{a})} \cdot \overline{D^{[i,r]}_{(1,\mathbf{x})}} = D^{[r]}_{(1,\mathbf{ext}'_r(\mathbf{x}+\mathbf{a}))} \cdot \overline{D^{[r]}_{(1,\mathbf{ext}'_r(\mathbf{x}))}} = D^{[r]}_{(1,\mathbf{ext}'_r(\mathbf{x})+\widetilde{\mathbf{a}})} \cdot \overline{D^{[r]}_{(1,\mathbf{ext}'_r(\mathbf{x}))}}.$$

Recall that we use $\widetilde{\mathbf{a}}$ to denote the vector $\mathbf{x} \in \mathbb{Z}_{\mathcal{Q}}$ such that $\mathbf{x}_i = \mathbf{a}$ and $\mathbf{x}_j = 0$ for all other $j \neq i$.

Then by condition $(\mathcal{D}_4)$, we know there exist $\mathbf{b} \in \mathbb{Z}_{\mathbf{q}_i}$ and $\alpha \in \mathbb{Z}_N$ such that

$$D^{[i,r]}_{(1,\mathbf{x}+\mathbf{a})} \cdot \overline{D^{[i,r]}_{(1,\mathbf{x})}} = \omega_N^{\alpha} \cdot F_{\widetilde{\mathbf{b}},\mathbf{ext}'_r(\mathbf{x})} = \omega_N^{\alpha} \cdot F^{[i]}_{\mathbf{b},\mathbf{x}}, \quad \text{for all } \mathbf{x} \in \Delta_{r,i},$$

and the lemma is proven. □

One can also prove a similar lemma for $\mathbf{D}^{[i,r]}_{(0,*)}$, $r \in \mathcal{S}$, using condition $(\mathcal{D}_3)$.

12.2 Step 2

For convenience, in this subsection we abuse the notation slightly and use $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ to denote one of the subproblems we defined in the last step: $\mathsf{EVAL}(\mathbf{C}^{[i]},\mathfrak{D}^{[i]})$, $i \in [s]$. Then by using conditions $(\mathcal{R}),(\mathcal{L})$ and $(\mathcal{D})$, we summarize the properties of this new $(\mathbf{C},\mathfrak{D})$ that we need in the reduction as follows:

$(\mathcal{F}_1)$ There exist a prime p and a sequence $\boldsymbol{\pi} = \{\pi_1 \ge \pi_2 \ge \ldots \ge \pi_h\}$ of powers of the same p. $\mathbf{F}$ is an $m \times m$ complex matrix, where $m = \pi_1\pi_2\ldots\pi_h$, and $\mathbf{C}$ is the bipartisation of $\mathbf{F}$. We let π denote π_1. We use $\mathbb{Z}_{\boldsymbol{\pi}} \equiv \mathbb{Z}_{\pi_1} \times \cdots \times \mathbb{Z}_{\pi_h}$ to index the rows and columns of $\mathbf{F}$, then

$$F_{\mathbf{x},\mathbf{y}} = \prod_{i\in[h]} \omega_{\pi_i}^{x_i y_i}, \quad \text{for all } \mathbf{x} = (x_1,\ldots,x_h) \text{ and } \mathbf{y} = (y_1,\ldots,y_h) \in \mathbb{Z}_{\boldsymbol{\pi}},$$

where we use x_i to denote the i^{th} entry of $\mathbf{x}$ in $\mathbb{Z}_{\pi_i}$, $i \in [h]$.

$(\mathcal{F}_2)$ $\mathfrak{D} = \{\mathbf{D}^{[0]},\ldots,\mathbf{D}^{[N-1]}\}$ is a sequence of N $2m \times 2m$ diagonal matrices, for some positive integer N with $\pi \,|\, N$. $\mathbf{D}^{[0]}$ is the identity matrix, and every diagonal entry of $\mathbf{D}^{[r]}$, $r \in [N-1]$, is either 0 or a power of ω_N. We use $\{0,1\} \times \mathbb{Z}_{\boldsymbol{\pi}}$ to index the rows and columns of matrices $\mathbf{C}$ and $\mathbf{D}^{[r]}$. (The condition $\pi \,|\, N$ is from the condition $M \,|\, N$ in $(\mathcal{U}_1)$, and the expression of M in terms of the prime powers, stated after $(\mathcal{R}_3)$. The π here is one of the $q_i = q_{i,1}$ there.)

$(\mathcal{F}_3)$ For each $r \in [0:N-1]$, we let Λ_r and Δ_r denote

$$\Lambda_r = \{\mathbf{x} \in \mathbb{Z}_{\boldsymbol{\pi}} \,|\, D^{[r]}_{(0,\mathbf{x})} \ne 0\} \quad \text{and} \quad \Delta_r = \{\mathbf{x} \in \mathbb{Z}_{\boldsymbol{\pi}} \,|\, D^{[r]}_{(1,\mathbf{x})} \ne 0\}.$$

We let $\mathcal{S}$ denote the set of r such that $\Lambda_r \ne \emptyset$, and $\mathcal{T}$ denote the set of r such that $\Delta_r \ne \emptyset$. Then for every $r \in \mathcal{S}$, Λ_r is a coset in $\mathbb{Z}_{\boldsymbol{\pi}}$; and for every $r \in \mathcal{T}$, Δ_r is a coset in $\mathbb{Z}_{\boldsymbol{\pi}}$. Moreover, for every $r \in \mathcal{S}$ (and $r \in \mathcal{T}$, resp.), there exists a vector $\mathfrak{a}^{[r]} \in \Lambda_r$ (and $\mathfrak{b}^{[r]} \in \Delta_r$, resp.) such that

$$D^{[r]}_{(0,\mathfrak{a}^{[r]})} = 1 \quad \Big(\text{and } D^{[r]}_{(1,\mathfrak{b}^{[r]})} = 1, \text{ resp.}\Big).$$

$(\mathcal{F}_4)$ For all $r \in \mathcal{S}$ and $\mathbf{a} \in \Lambda_r^{\text{lin}}$, there exist $\mathbf{b} \in \mathbb{Z}_{\boldsymbol{\pi}}$ and $\alpha \in \mathbb{Z}_N$ such that

$$D^{[r]}_{(0,\mathbf{x}+\mathbf{a})}\overline{D^{[r]}_{(0,\mathbf{x})}} = \omega_N^{\alpha} \cdot \mathbf{F}_{\mathbf{x},\mathbf{b}}, \quad \text{for all } \mathbf{x} \in \Lambda_r;$$

For all $r \in \mathcal{T}$ and $\mathbf{a} \in \Delta_r^{\text{lin}}$, there exist $\mathbf{b} \in \mathbb{Z}_{\boldsymbol{\pi}}$ and $\alpha \in \mathbb{Z}_N$ such that

$$D^{[r]}_{(1,\mathbf{x}+\mathbf{a})}\overline{D^{[r]}_{(1,\mathbf{x})}} = \omega_N^{\alpha} \cdot \mathbf{F}_{\mathbf{b},\mathbf{x}}, \quad \text{for all } \mathbf{x} \in \Delta_r.$$

Now let G be a connected graph. Below we will reduce the computation of $Z_{\mathbf{C},\mathfrak{D}}(G)$ to $\mathsf{EVAL}(\widehat{\pi})$,

$$\text{where } \widehat{\pi} = \pi \text{ if } p \ne 2; \quad \text{and } \widehat{\pi} = 2\pi \text{ if } p = 2.$$

Given $a \in \mathbb{Z}_{\pi_i}$ for some $i \in [h]$, we let $\widehat{a}$ denote an element in $\mathbb{Z}_{\widehat{\pi}}$ such that $\widehat{a} \equiv a \pmod{\pi_i}$. As $\pi_h \,|\, \pi_{h-1} \,|\, \ldots \,|\, \pi_1 = \pi \,|\, \widehat{\pi}$, this lifting of a is certainly feasible. For definiteness, we can choose a itself if we consider a to be an integer between 0 and $\pi_i - 1$.

First, if G is not bipartite, then $Z_{\mathbf{C},\mathfrak{D}}(G)$ is trivially 0. So from now on in this section, we assume $G = (U \cup V, E)$ to be bipartite: every edge $uv \in E$ has one vertex in U and one vertex in V.

Let u^* be a vertex in U, then we can decompose $Z_{\mathbf{C},\mathfrak{D}}(G)$ into

$$Z_{\mathbf{C},\mathfrak{D}}(G) = Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}(G,u^*) + Z^{\leftarrow}_{\mathbf{C},\mathfrak{D}}(G,u^*).$$

We will give a reduction from the computation of $Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}(G, u^*)$ to $\mathsf{EVAL}(\widehat{\pi})$. The other part concerning $Z^{\leftarrow}$ can be proved similarly.

We use U_r, where $r \in [0 : N-1]$, to denote the set of vertices in U whose degree is $r \pmod N$, and V_ρ to denote the set of vertices in V whose degree is $\rho \pmod N$. We further decompose E into $\bigcup_{i,j} E_{i,j}$ where $E_{i,j}$ contains the edges between U_i and V_j.

It is clear that if $U_r \neq \emptyset$ for some $r \notin \mathcal{S}$ or if $V_\rho \neq \emptyset$ for some $\rho \notin \mathcal{T}$, then $Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}(G) = 0$. Therefore we assume $U_r = \emptyset$ for all $r \notin \mathcal{S}$ and $V_\rho = \emptyset$ for all $\rho \notin \mathcal{T}$. In this case, we have

$$Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}(G, u^*) = \sum_{(f,g)} \left[\prod_{r\in\mathcal{S}} \left(\prod_{u\in U_r} D^{[r]}_{(0,\mathbf{x}_u)}\right) \cdot \prod_{\rho\in\mathcal{T}} \left(\prod_{v\in V_\rho} D^{[r]}_{(1,\mathbf{y}_v)}\right)\right] \cdot \left[\prod_{(r,\rho)\in\mathcal{S}\times\mathcal{T}} \prod_{uv\in E_{r,\rho}} F_{\mathbf{x}_u,\mathbf{y}_v}\right]. \tag{80}$$

Here the sum ranges over all pairs (f, g), where

$$f = (f_r; r \in \mathcal{S}) \in \prod_{r\in\mathcal{S}} (U_r \to \Lambda_r) \quad \text{and} \quad g = (g_\rho; \rho \in \mathcal{T}) \in \prod_{\rho\in\mathcal{T}} (V_\rho \to \Delta_\rho),$$

such that $f(u) = \mathbf{x}_u$ and $g(v) = \mathbf{y}_v$.

The following lemma gives us a convenient way to do summation over a coset.

Lemma 12.3. *Let Φ be a coset in $\mathbb{Z}_{\boldsymbol{\pi}}$ and $\mathbf{c} = (c_1, \ldots, c_h)$ be a vector in Φ, then there exist a positive integer s and an $s \times h$ matrix $\mathbf{A}$ over $\mathbb{Z}_{\widehat{\pi}}$ such that the following map $\tau : (\mathbb{Z}_{\widehat{\pi}})^s \to \mathbb{Z}_{\pi_1} \times \cdots \times \mathbb{Z}_{\pi_h}$*

$$\tau(\mathbf{x}) = \big(\tau_1(\mathbf{x}), \ldots, \tau_h(\mathbf{x})\big), \text{ where } \tau_j(\mathbf{x}) = \big(\mathbf{x}\mathbf{A}_{*,j} + \widehat{c}_j \pmod{\pi_j}\big) \in \mathbb{Z}_{\pi_j} \text{ for all } j \in [h], \tag{81}$$

is a uniform *map from $\mathbb{Z}^s_{\widehat{\pi}}$ onto Φ. This uniformity means that for all $\mathbf{b}, \mathbf{b}' \in \Phi$, the number of $\mathbf{x} \in \mathbb{Z}^s_{\widehat{\pi}}$ such that $\tau(\mathbf{x}) = \mathbf{b}$ is the same as the number of $\mathbf{x}$ such that $\tau(\mathbf{x}) = \mathbf{b}'$.*

Proof. By the fundamental theorem of finite Abelian groups, there is a group isomorphism f from $\mathbb{Z}_{\mathbf{g}}$ onto Φ^{lin}, where $\mathbf{g} = (g_1, \ldots, g_s)$ is a sequence of powers of p and satisfies $\widehat{\pi} \geq \pi = \pi_1 \geq g_1 \geq \ldots \geq g_s$, for some $s \geq 1$. $\mathbb{Z}_{\mathbf{g}} \equiv \mathbb{Z}_{g_1} \times \ldots \times \mathbb{Z}_{g_s}$ is a $\mathbb{Z}_{\widehat{\pi}}$-module. This is clear, since as a $\mathbb{Z}$-module, any multiple of $\widehat{\pi}$ annihilates $\mathbb{Z}_{\mathbf{g}}$. Thus f is also a $\mathbb{Z}_{\widehat{\pi}}$-module isomorphism.

Let $\mathbf{a}_i = f(\mathbf{e}_i) \in \Phi^{\text{lin}}$, for each $i \in [s]$, where $\mathbf{e}_i \in \mathbb{Z}_{\mathbf{g}}$ is the vector whose i^{th} entry is 1 and all other entries are 0. Let $\mathbf{a}_i = (a_{i,1}, \ldots, a_{i,h}) \in \mathbb{Z}_{\boldsymbol{\pi}}$ where $a_{i,j} \in \mathbb{Z}_{\pi_j}$, $i \in [s]$, $j \in [h]$. Let $\widehat{\mathbf{a}}_i = (\widehat{a}_{i,1}, \ldots, \widehat{a}_{i,h}) \in (\mathbb{Z}_{\widehat{\pi}})^h$ be a lifting of $\mathbf{a}_i$ component-wise. Similarly let $\widehat{\mathbf{c}}$ be a lifting of $\mathbf{c}$ component-wise. Then we claim that $\mathbf{A} = (\widehat{a}_{i,j})$ and $\widehat{\mathbf{c}}$ together give us a *uniform* map τ from $\mathbb{Z}^s_{\widehat{\pi}}$ to Φ defined in (81).

To prove that τ is uniform, we consider the linear part of the map $\tau' : \mathbb{Z}^s_{\widehat{\pi}} \to \Phi^{\text{lin}}$,

$$\tau'(\mathbf{x}) = (\tau'_1(\mathbf{x}), \ldots, \tau'_h(\mathbf{x})), \quad \text{where } \tau'_j(\mathbf{x}) = (\mathbf{x}\mathbf{A}_{*,j} \pmod{\pi_j}) \in \mathbb{Z}_{\pi_j}, \text{ for all } j \in [h].$$

Clearly we only need to show that τ' is a uniform map.

Let σ be the natural projection from $\mathbb{Z}^s_{\widehat{\pi}}$ to $\mathbb{Z}_{\mathbf{g}}$:

$$\mathbf{x} = (x_1, \ldots, x_s) \mapsto \big(x_1 \pmod{g_1}, \ldots, x_s \pmod{g_s}\big).$$

σ is certainly a uniform map, being a surjective homomorphism. Thus every vector $\mathbf{b} \in \mathbb{Z}_{\mathbf{g}}$ has exactly $|\ker\sigma| = \widehat{\pi}^s/(g_1 \cdots g_s)$ many preimages. We show that the map τ' factors through σ and f: $\tau' = f \circ \sigma$. Since f is an isomorphism, this implies that τ' is also a uniform map.

Since $g_i\mathbf{e}_i = \mathbf{0}$ in $\mathbb{Z}_{\mathbf{g}}$, the following is a valid expression in the $\mathbb{Z}_{\widehat{\pi}}$-module for $\sigma(\mathbf{x})$

$$\big(x_1 \pmod{g_1}, \ldots, x_s \pmod{g_s}\big) = \textstyle\sum_{i=1}^s x_i\mathbf{e}_i.$$

Apply f as a $\mathbb{Z}_{\widehat{\pi}}$-module homomorphism

$$f(\sigma(\mathbf{x})) = \sum_{i=1}^{s} x_i f(\mathbf{e}_i),$$

which has its j^{th} entry $\sum_{i=1}^{s} x_i a_{i,j}$. This is an expression in the $\mathbb{Z}_{\widehat{\pi}}$-module $\mathbb{Z}_{\pi_j}$, which is the same as

$$\sum_{i=1}^{s} \big(x_i \pmod{\pi_j}\big) \cdot a_{i,j} = \sum_{i=1}^{s} x_i \widehat{a}_{i,j} \pmod{\pi_j} = \tau'_j(\mathbf{x}).$$

□

By applying Lemma 12.3 to coset Λ_r, we know for every $r \in \mathcal{S}$, there exist a positive integer s_r and an $s_r \times h$ matrix $\mathbf{A}^{[r]}$ over $\mathbb{Z}_{\widehat{\pi}}$ which give us a uniform map $\lambda^{[r]}(\mathbf{x})$ from $\mathbb{Z}_{\widehat{\pi}}^{s_r}$ to Λ_r, where

$$\lambda^{[r]}_i(\mathbf{x}) = \big(\mathbf{x}\mathbf{A}^{[r]}_{*,i} + \widehat{\mathfrak{a}}^{[r]}_i \pmod{\pi_i}\big), \quad \text{for all } i \in [h] \text{ and } \mathbf{x} \in \mathbb{Z}_{\widehat{\pi}}^{s_r}. \tag{82}$$

Similarly for every $r \in \mathcal{T}$, there exist a positive integer t_r and an $t_r \times h$ matrix $\mathbf{B}^{[r]}$ over $\mathbb{Z}_{\widehat{\pi}}$ which give us a uniform map $\delta^{[r]}$ from $\mathbb{Z}_{\widehat{\pi}}^{t_r}$ to Δ_r, where

$$\delta^{[r]}_i(\mathbf{y}) = \big(\mathbf{y}\mathbf{B}^{[r]}_{*,i} + \widehat{\mathfrak{b}}^{[r]}_i \pmod{\pi_i}\big), \quad \text{for all } i \in [h] \text{ and } \mathbf{y} \in \mathbb{Z}_{\widehat{\pi}}^{t_r}. \tag{83}$$

Using $(\mathcal{F}_3)$, we have

$$D^{[r]}_{(0,\lambda^{[r]}(\mathbf{0}))} = 1, \text{ when } r \in \mathcal{S}; \text{ and } D^{[r]}_{(1,\delta^{[r]}(\mathbf{0}))} = 1, \text{ when } r \in \mathcal{T}. \tag{84}$$

Because both $\lambda^{[r]}$ and $\delta^{[r]}$ are uniform, and we know the multiplicity of each map (cardinality of inverse images), to compute (80), it suffices to compute the following

$$\sum_{(\mathbf{x}_u),(\mathbf{y}_v)} \prod_{r\in\mathcal{S}} \left(\prod_{u\in U_r} D^{[r]}_{(0,\lambda^{[r]}(\mathbf{x}_u))}\right) \prod_{r\in\mathcal{T}} \left(\prod_{v\in V_r} D^{[r]}_{(1,\delta^{[r]}(\mathbf{y}_v))}\right) \prod_{r_1\in\mathcal{S},r_2\in\mathcal{T}} \left(\prod_{uv\in E_{r_1,r_2}} F_{\lambda^{[r_1]}(\mathbf{x}_u),\delta^{[r_2]}(\mathbf{y}_v)}\right), \tag{85}$$

where the sum is over pairs of sequences

$$\Big(\mathbf{x}_u; u \in \bigcup_{r\in\mathcal{S}} U_r\Big) \in \prod_{r\in\mathcal{S}} \big(\mathbb{Z}_{\widehat{\pi}}^{s_r}\big)^{|U_r|} \quad \text{and} \quad \Big(\mathbf{y}_v; v \in \bigcup_{r\in\mathcal{T}} V_r\Big) \in \prod_{r\in\mathcal{T}} \big(\mathbb{Z}_{\widehat{\pi}}^{t_r}\big)^{|V_r|}.$$

If we can show for all $r \in \mathcal{S}$, there is a quadratic polynomial $f^{[r]}$ over $\mathbb{Z}_{\widehat{\pi}}$ such that

$$D^{[r]}_{(0,\lambda^{[r]}(\mathbf{x}))} = \omega_{\widehat{\pi}}^{f^{[r]}(\mathbf{x})}, \quad \text{for all } \mathbf{x} \in \mathbb{Z}_{\widehat{\pi}}^{s_r}; \tag{86}$$

and for all $r \in \mathcal{T}$, there is a quadratic polynomial $g^{[r]}$ over $\mathbb{Z}_{\widehat{\pi}}$ such that

$$D^{[r]}_{(1,\delta^{[r]}(\mathbf{y}))} = \omega_{\widehat{\pi}}^{g^{[r]}(\mathbf{y})}, \quad \text{for all } \mathbf{y} \in \mathbb{Z}_{\widehat{\pi}}^{t_r}; \tag{87}$$

and for all $r_1 \in \mathcal{S}$ and $r_2 \in \mathcal{T}$, there is a quadratic polynomial $f^{[r_1,r_2]}$ over $\mathbb{Z}_{\widehat{\pi}}$ such that

$$F_{\lambda^{[r_1]}(\mathbf{x}),\delta^{[r_2]}(\mathbf{y})} = \omega_{\widehat{\pi}}^{f^{[r_1,r_2]}(\mathbf{x},\mathbf{y})}, \quad \text{for all } \mathbf{x} \in \mathbb{Z}_{\widehat{\pi}}^{s_{r_1}} \text{ and } \mathbf{y} \in \mathbb{Z}_{\widehat{\pi}}^{t_{r_2}}, \tag{88}$$

then we can reduce the computation of the summation in (85) to problem $\mathsf{EVAL}(\widehat{\pi})$.

We start by proving the existence of the quadratic polynomial $f^{[r_1,r_2]}$. Let $r_1 \in \mathcal{S}$ and $r_2 \in \mathcal{T}$ then by $(\mathcal{F}_1)$, the following map $f^{[r_1,r_2]}$ satisfies (88):

$$f^{[r_1,r_2]}(\mathbf{x},\mathbf{y}) = \sum_{i\in[h]} \left(\frac{\widehat{\pi}}{\pi_i}\right) \cdot \lambda_i^{[r_1]}(\mathbf{x}) \cdot \delta_i^{[r_2]}(\mathbf{y}) = \sum_{i\in[h]} \left(\frac{\widehat{\pi}}{\pi_i}\right) \left(\mathbf{x}\mathbf{A}^{[r_1]}_{*,i} + \widehat{\mathfrak{a}}^{[r_1]}_i\right) \left(\mathbf{y}\mathbf{B}^{[r_2]}_{*,i} + \widehat{\mathfrak{b}}^{[r_2]}_i\right).$$

Note that the presence of the integer $\widehat{\pi}/\pi_i$ is crucial to be able to substitute the mod π_i expressions for $\lambda_i^{[r_1]}(\mathbf{x})$ in (82) and $\delta_i^{[r_2]}(\mathbf{y})$ in (83) respectively, as if they were mod $\widehat{\pi}$ expressions. Now it is clear that $f^{[r_1,r_2]}$ is indeed a quadratic polynomial over $\mathbb{Z}_{\widehat{\pi}}$.

Next, we prove the existence of a quadratic polynomial $f^{[r]}$ for Λ_r, $r \in \mathcal{S}$, in (86), which is a little more complicated. One can prove the same result for (87) similarly.

Let $r \in S$ and $\mathbf{e}_i$ denote the vector in $\mathbb{Z}_{\widehat{\pi}}^{s_r}$ whose i^{th} entry is 1 and all other entries are 0. Then by $(\mathcal{F}_4)$, for each $i \in [s_r]$, there exist $\alpha_i \in \mathbb{Z}_N$ and $\mathbf{b}_i = (b_{i,1},\ldots,b_{i,h}) \in \mathbb{Z}_{\boldsymbol{\pi}}$, where $b_{i,j} \in \mathbb{Z}_{\pi_j}$, such that

$$D^{[r]}_{(0,\lambda^{[r]}(\mathbf{x}+\mathbf{e}_i))}\overline{D^{[r]}_{(0,\lambda^{[r]}(\mathbf{x}))}} = \omega_N^{\alpha_i} \prod_{j\in[h]} \omega_{\pi_j}^{b_{i,j}\cdot\lambda_j^{[r]}(\mathbf{x})}, \quad \text{for all } \mathbf{x} \in \mathbb{Z}_{\widehat{\pi}}^{s_r}. \tag{89}$$

We have this equation because $\lambda^{[r]}(\mathbf{x}+\mathbf{e}_i) - \lambda^{[r]}(\mathbf{x})$ is indeed a vector in $\mathbb{Z}_{\boldsymbol{\pi}}$ that is independent of $\mathbf{x}$. To see this, its j^{th} entry in $\lambda^{[r]}(\mathbf{x}+\mathbf{e}_i) - \lambda^{[r]}(\mathbf{x})$ is

$$\mathbf{e}_i\mathbf{A}^{[r]}_{*,j} = A^{[r]}_{i,j} \pmod{\pi_j},$$

and thus the displacement vector $\lambda^{[r]}(\mathbf{x}+\mathbf{e}_i) - \lambda^{[r]}(\mathbf{x})$ is independent of $\mathbf{x}$, and is in Λ_r^{lin} by definition. This is the $\mathbf{a} \in \Lambda_r^{\text{lin}}$ in the statement of $(\mathcal{F}_4)$ which we applied.

Before moving forward, we show that $\omega_N^{\alpha_i}$ must be a power of $\omega_{\widehat{\pi}}$. This is because

$$1 = \prod_{j=0}^{\widehat{\pi}-1} D^{[r]}_{(0,\lambda^{[r]}((j+1)\mathbf{e}_i))}\overline{D^{[r]}_{(0,\lambda^{[r]}(j\mathbf{e}_i))}} = (\omega_N^{\alpha_i})^{\widehat{\pi}} \prod_{k\in[h]} \omega_{\pi_k}^{b_{i,k}\cdot[\lambda_k^{[r]}(0\mathbf{e}_i)+\ldots+\lambda_k^{[r]}((\widehat{\pi}-1)\mathbf{e}_i)]}. \tag{90}$$

For each $k \in [h]$, the exponent of ω_{π_k} is $b_{i,k}Q_k \in \mathbb{Z}_{\pi_k}$ where Q_k is the following summation:

$$\sum_{j=0}^{\widehat{\pi}-1} \lambda_k^{[r]}(j\mathbf{e}_i) = \sum_{j=0}^{\widehat{\pi}-1} \Big((j\mathbf{e}_i)\mathbf{A}^{[r]}_{*,k} + \widehat{\mathfrak{a}}^{[r]}_k \pmod{\pi_k}\Big) = \left(\sum_{j=1}^{\widehat{\pi}-1} j\mathbf{e}_i\right) \mathbf{A}^{[r]}_{*,k} \pmod{\pi_k} = 0. \tag{91}$$

The last equality comes from $J \equiv \sum_{j=1}^{\widehat{\pi}-1} j = 0 \pmod{\pi_k}$, and this is due to our definition of $\widehat{\pi}$. When p is odd, J is a multiple of $\widehat{\pi}$ and $\pi_k \,|\, \widehat{\pi}$; When $p = 2$, J is a multiple of $\widehat{\pi}/2$. However in this case, we have $\widehat{\pi}/2 = \pi_1$ and $\pi_k \,|\, \pi_1$.

As a result, $(\omega_N^{\alpha_i})^{\widehat{\pi}} = 1$ and $\omega_N^{\alpha_i}$ is a power of $\omega_{\widehat{\pi}}$. So there exists $\beta_i \in \mathbb{Z}_{\widehat{\pi}}$ for each $i \in [s_r]$ such that

$$D^{[r]}_{(0,\lambda^{[r]}(\mathbf{x}+\mathbf{e}_i))}\overline{D^{[r]}_{(0,\lambda^{[r]}(\mathbf{x}))}} = \omega_{\widehat{\pi}}^{\beta_i} \prod_{j\in[h]} \omega_{\pi_j}^{b_{i,j}\cdot\lambda_j^{[r]}(\mathbf{x})}, \quad \text{for all } \mathbf{x} \in \mathbb{Z}_{\widehat{\pi}}^{s_r}. \tag{92}$$

It follows that every non-zero entry of $\mathbf{D}^{[r]}$ is a power of $\omega_{\widehat{\pi}}$. This uses $(\mathcal{F}_3)$: the $(0,\mathfrak{a}^{[r]})^{th}$ entry of $\mathbf{D}^{[r]}$ is 1, and the fact that $\lambda^{[r]}$ is surjective to Λ_r: any point in Λ_r is connected to the normalizing point $\mathfrak{a}^{[r]}$ by a sequence of moves $\lambda^{[r]}(\mathbf{x}) \to \lambda^{[r]}(\mathbf{x}+\mathbf{e}_i)$, for $i \in [s_r]$.

Now we know there is a function $f^{[r]}\colon \mathbb{Z}_{\widehat{\pi}}^{s_r} \to \mathbb{Z}_{\widehat{\pi}}$ satisfying (86). We want to show that we can take a quadratic polynomial $f^{[r]}$ for this purpose. To see this, by (92), we have for every $i \in [s_r]$,

$$f^{[r]}(\mathbf{x}+\mathbf{e}_i)-f^{[r]}(\mathbf{x})=\beta_i+\sum_{j\in[h]}\left(\left(\frac{\widehat{\pi}}{\pi_j}\right)b_{i,j}\right)\cdot\lambda_j^{[r]}(\mathbf{x})=\beta_i+\sum_{j\in[h]}\left(\frac{\widehat{\pi}}{\pi_j}\right)\widehat{b}_{i,j}\cdot\big(\mathbf{x}\mathbf{A}_{*,j}^{[r]}+\widehat{\mathfrak{a}}_j^{[r]}\big). \tag{93}$$

We should remark that, originally $b_{i,j}$ is in $\mathbb{Z}_{\pi_j}$; however with the integer multiplier $(\widehat{\pi}/\pi_j)$, the quantity $(\widehat{\pi}/\pi_j)\cdot b_{i,j}$ is now considered in $\mathbb{Z}_{\widehat{\pi}}$. Furthermore,

$$\widehat{b}_{i,j}\equiv b_{i,j}\pmod{\pi_j}\quad\text{implies that}\quad\left(\frac{\widehat{\pi}}{\pi_j}\right)\widehat{b}_{i,j}\equiv\left(\frac{\widehat{\pi}}{\pi_j}\right)b_{i,j}\pmod{\widehat{\pi}}.$$

Thus the expression in (93) happens in $\mathbb{Z}_{\widehat{\pi}}$. It means for any $i\in[s_r]$, there exist $c_{i,0},c_{i,1},\ldots,c_{i,s_r}\in\mathbb{Z}_{\widehat{\pi}}$,

$$f^{[r]}(\mathbf{x}+\mathbf{e}_i)-f^{[r]}(\mathbf{x})=c_{i,0}+\sum_{j\in[s_r]}c_{i,j}x_j. \tag{94}$$

Since $D^{[r]}_{(0,\lambda^{[r]}(\mathbf{0}))}=1$, $f^{[r]}(\mathbf{0})$ is 0. The case when the prime p is odd follows from the lemma below.

Lemma 12.4. *Let f be a map from $\mathbb{Z}_\pi^s$, for some positive integer $s\geq 1$, to $\mathbb{Z}_\pi$, and π is a power of an odd prime. Suppose for every $i\in[s]$, there exist $c_{i,0},c_{i,1},\ldots,c_{i,s}\in\mathbb{Z}_\pi$ such that*

$$f(\mathbf{x}+\mathbf{e}_i)-f(\mathbf{x})=c_{i,0}+\sum_{j\in[s]}c_{i,j}x_j,\quad\text{for all }\mathbf{x}\in\mathbb{Z}_\pi^s,$$

and $f(\mathbf{0})=0$. Then there exist $a_{i,j},a_i\in\mathbb{Z}_\pi$ such that

$$f(\mathbf{x})=\sum_{i\leq j\in[s]}a_{i,j}x_ix_j+\sum_{i\in[s]}a_ix_i,\quad\text{for all }\mathbf{x}\in\mathbb{Z}_\pi^s.$$

Proof. First note that f is uniquely determined by the conditions on $f(\mathbf{x}+\mathbf{e}_i)-f(\mathbf{x})$ and $f(\mathbf{0})$. Second we show that $c_{i,j}=c_{j,i}$ for all $i,j\in[s]$; otherwise f does not exist, contradicting the assumption.

On the one hand, we have

$$f(\mathbf{e}_i+\mathbf{e}_j)=f(\mathbf{e}_i+\mathbf{e}_j)-f(\mathbf{e}_j)+f(\mathbf{e}_j)-f(\mathbf{0})=c_{i,0}+c_{i,j}+c_{j,0}.$$

On the other hand,

$$f(\mathbf{e}_i+\mathbf{e}_j)=f(\mathbf{e}_i+\mathbf{e}_j)-f(\mathbf{e}_i)+f(\mathbf{e}_i)-f(\mathbf{0})=c_{j,0}+c_{j,i}+c_{i,0}.$$

As a result, we have $c_{i,j}=c_{j,i}$.

Finally, we set $a_{i,j}=c_{i,j}$ for all $i<j\in[s]$;

$$a_{i,i}=c_{i,i}/2,\quad\text{for all }i\in[s];$$

(Here $c_{i,i}/2$ is well defined because π is odd) and $a_i=c_{i,0}-a_{i,i}$ for all $i\in[s]$. We now claim that

$$g(\mathbf{x})=\sum_{i\leq j\in[s]}a_{i,j}x_ix_j+\sum_{i\in[s]}a_ix_i$$

satisfies both conditions and thus, $f=g$. To see this, we check the case when $i=1$ and the other cases are similar:

$$g(\mathbf{x}+\mathbf{e}_1)-g(\mathbf{x})=2a_{1,1}x_1+\sum_{j>1}a_{1,j}x_j+(a_{1,1}+a_1)=c_{1,1}x_1+\sum_{j>1}c_{1,j}x_j+c_{1,0}.$$

□

The case when $p = 2$ is a little more complicated. We first claim for every $i \in [s]$, the constant $c_{i,i}$ in (94) must be even. This is because

$$0 = f^{[r]}(\widehat{\pi}\mathbf{e}_i) - f^{[r]}((\widehat{\pi}-1)\mathbf{e}_i) + \ldots + f^{[r]}(\mathbf{e}_i) - f^{[r]}(\mathbf{0}) = \widehat{\pi}\cdot c_{i,0} + c_{i,i}(\widehat{\pi}-1+\widehat{\pi}-2+\ldots+1+0).$$

This equality happens in $\mathbb{Z}_{\widehat{\pi}}$. So

$$c_{i,i}\frac{\widehat{\pi}}{2}(\widehat{\pi}-1) = 0 \pmod{\widehat{\pi}}.$$

When $\widehat{\pi}-1$ is odd we have $2\,|\,c_{i,i}$. It follows from the lemma below that $f^{[r]}$ is a quadratic polynomial.

Lemma 12.5. *Let π be a power of 2 and f be a map from $\mathbb{Z}_\pi^s$ to $\mathbb{Z}_\pi$, for some positive integer $s \geq 1$. Suppose for every $i \in [s]$, there exist $c_{i,0}, c_{i,1}, \ldots, c_{i,s} \in \mathbb{Z}_\pi$, where $2\,|\,c_{i,i}$, such that*

$$f(\mathbf{x}+\mathbf{e}_i) - f(\mathbf{x}) = c_{i,0} + \sum_{j\in[s]} c_{i,j}x_j, \quad \textit{for all } \mathbf{x}\in\mathbb{Z}_\pi^s,$$

and $f(\mathbf{0}) = 0$. Then there exist $a_{i,j}, a_i \in \mathbb{Z}_\pi$ such that

$$f(\mathbf{x}) = \sum_{i\leq j\in[s]} a_{i,j}x_ix_j + \sum_{i\in[s]} a_ix_i, \quad \textit{for all } \mathbf{x}\in\mathbb{Z}_\pi^s.$$

Proof. The proof of Lemma 12.5 is essentially the same as in Lemma 12.4. The only thing to notice is that, because $2\,|\,c_{i,i}$, $a_{i,i} = c_{i,i}/2$ is well defined (in particular, when $c_{i,i} = 0$, we set $a_{i,i} = 0$). □

12.3 Proof of Theorem 12.1

Now we turn to the proof of Theorem 12.1: $\mathsf{EVAL}(q)$ is tractable for any prime power q.

Actually, there is a well-known polynomial-time algorithm for $\mathsf{EVAL}(q)$ when q is a prime (see [15]. The algorithm works for any finite field). In this section we present a polynomial-time algorithm that works for any prime power q. We start with the easier case when q is odd.

Lemma 12.6. *Let p be an odd prime, and $q = p^k$ for some positive integer k. Let $f \in \mathbb{Z}_q[x_1, \ldots, x_n]$ be a quadratic polynomial over n variables $x_1, \ldots, x_n$. Then the following sum*

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

can be evaluated in polynomial time (in n). Here by a quadratic polynomial over n variables we mean a polynomial where every monomial term has degree at most 2.

Proof. In the proof, we assume $f(x_1, x_2, \ldots, x_n)$ has the following form:

$$f(x_1,\ldots,x_n) = \sum_{i\leq j\in[n]} c_{i,j}x_ix_j + \sum_{i\in[n]} c_ix_i + c_0. \tag{95}$$

where all the $c_{i,j}$ and c_i are elements in $\mathbb{Z}_q$.

First, as a warm up, we give an algorithm and prove its correctness for the case $k = 1$. In this case $q = p$ is an odd prime. Note that if f is an affine linear function, then the evaluation can be trivially done in polynomial time. In fact the sum simply decouples into a product of n sums

$$\sum_{x_1,x_2,\ldots,x_n\in\mathbb{Z}_q} \omega_q^{f(x_1,x_2,\ldots,x_n)} = \sum_{x_1,x_2,\ldots,x_n\in\mathbb{Z}_q} \omega_q^{\sum_{i=1}^n c_ix_i+c_0} = \omega_q^{c_0} \times \prod_{i=1}^n \sum_{x_i\in\mathbb{Z}_q} \omega_q^{c_ix_i}.$$

This sum is equal to 0 if any $c_i \in \mathbb{Z}_q$ is non-zero, and is equal to $q^n \omega_q^{c_0}$ otherwise.

Now assume $f(x_1, \ldots, x_n)$ is not affine linear. Then in each round (which we will describe below), the algorithm will decrease the number of variables by at least one, in polynomial time.

Assume f contains some quadratic terms. There are two cases: f has at least one square term; or f does not have any square term. In the first case, without loss of generality, we assume that $c_{1,1} \in \mathbb{Z}_q$ is non-zero. Then there exist an affine linear function $g \in \mathbb{Z}_q[x_2, x_3, \ldots, x_n]$, and a quadratic polynomial $f' \in \mathbb{Z}_q[x_2, x_3, \ldots, x_n]$, both over $n-1$ variables $x_2, x_3, \ldots, x_n$, such that

$$f(x_1, x_2, \ldots, x_n) = c_{1,1}\big(x_1 + g(x_2, x_3, \ldots, x_n)\big)^2 + f'(x_2, x_3, \ldots, x_n).$$

Here we used the fact that both 2 and $c_{1,1} \in \mathbb{Z}_q$ are invertible in the field $\mathbb{Z}_q$ (Recall we assumed that $q = p$ is an odd prime). Thus we can factor out a coefficient $2c_{1,1}$ from the cross term $x_1 x_i$, for every $i > 1$, and from the linear term x_1, to get the expression $c_{1,1}(x_1 + g(x_2, \ldots, x_n))^2$.

For any fixed $x_2, \ldots, x_n \in \mathbb{Z}_q$, when x_1 goes over $\mathbb{Z}_q$, $x_1 + g(x_2, \ldots, x_n)$ also goes over $\mathbb{Z}_q$. Thus,

$$\sum_{x_1, x_2, \ldots, x_n \in \mathbb{Z}_q} \omega_q^{f(x_1, x_2, \ldots, x_n)} = \sum_{x_2, \ldots, x_n \in \mathbb{Z}_q} \omega_q^{f'(x_2, \ldots, x_n)} \sum_{x_1 \in \mathbb{Z}_q} \omega_q^{c_{1,1}(x_1 + g(x_2, \ldots, x_n))^2} = \sum_{x \in \mathbb{Z}_q} \omega_q^{c_{1,1} x^2} \cdot Z_q(f').$$

The first factor can be evaluated in constant time (which is independent of n) and the computation of $Z_q(f)$ is reduced to the computation of $Z_q(f')$ in which f' has at most $n-1$ variables.

> **Remark**: The claim of $\sum_x \omega_q^{cx^2}$ being "computable in constant time" is a trivial statement, since we consider $q = p$ to be a fixed constant. However, for a general prime p, we remark that the sum is the famous Gauss quadratic sum, and has the closed formula
>
> $$\sum_{x \in \mathbb{Z}_p} \omega_p^{cx^2} = p, \text{ if } c = 0, \text{ and it is } \left(\frac{c}{p}\right) \cdot G, \text{ if } c \neq 0, \text{ where } G = \sum_{x \in \mathbb{Z}_p} \left(\frac{x}{p}\right) \omega^x.$$
>
> Here $\left(\frac{c}{p}\right)$ is the Legendre symbol, which can be computed in polynomial time in the binary length of c and p, and G has the closed form $G = +\sqrt{p}$ if $p \equiv 1 \bmod 4$ and $G = +i\sqrt{p}$ if $p \equiv 3 \bmod 4$ [1].

The second case is that all the quadratic terms in f are cross terms (in particular this implies that $n \geq 2$). In this case we assume, without loss of generality, that $c_{1,2}$ is non-zero. We apply the following transformation: $x_1 = x_1' + x_2'$ and $x_2 = x_1' - x_2'$. As 2 is invertible in $\mathbb{Z}_q$, when x_1' and x_2' go over $\mathbb{Z}_q^2$, x_1 and x_2 also go over $\mathbb{Z}_q^2$. Therefore, we have

$$\sum_{x_1, x_2, \ldots, x_n \in \mathbb{Z}_q} \omega_q^{f(x_1, x_2, \ldots, x_n)} = \sum_{x_1', x_2', \ldots, x_n \in \mathbb{Z}_q} \omega_q^{f(x_1' + x_2', x_1' - x_2', \ldots, x_n)}.$$

If we view $f(x_1' + x_2', x_1' - x_2', \ldots, x_n)$ as a new quadratic polynomial f' of $x_1', x_2', \ldots, x_n$, its coefficient of $x_1'^2$ is exactly $c_{1,2} \neq 0$, so f' contains at least one square term. This reduces our problem back to the first case, and we can use the method above to reduce the number of variables.

By repeating this process, we get a polynomial-time algorithm for computing $Z_q(f)$ when $q = p$ is an odd prime. Now we consider the case when $q = p^k$.

[1] It had been known to Gauss since 1801 that $G^2 = \left(\frac{-1}{p}\right) p$. Thus $G = \pm\sqrt{p}$ if $p \equiv 1 \pmod 4$ and $G = \pm i\sqrt{p}$ if $p \equiv 3 \pmod 4$. The fact that G always takes the sign $+$ was conjectured by Gauss in his diary in May 1801. Four years later, on Sept 3, 1805, he wrote, ... Seldom had a week passed for four years that he 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 ...").

For any non-zero $a \in \mathbb{Z}_q$, we can write it as $a = p^t a'$, where t is a unique non-negative integer, such that $p \nmid a'$. We call t the order of a (with respect to p). Again, if f is an affine linear function, $Z_q(f)$ is easy to compute, as the sum factors into n sums as before. Now we assume f has non-zero quadratic terms. Let t_0 be the smallest order of all the non-zero quadratic coefficients $c_{i,j}$ of f. We consider the following two cases: there exists at least one square term with coefficient of order t_0 or not.

In the first case, without loss of generality, we assume $c_{1,1} = p^{t_0} c$ and $p \nmid c$ (so c is invertible in $\mathbb{Z}_q$). Then by the minimality of t_0, every non-zero coefficient of a quadratic term has a factor p^{t_0}. Now we factor out $c_{1,1}$ from every quadratic term involving x_1, namely from $x_1^2, x_1x_2, \ldots, x_1x_n$ (clearly it does not matter if the coefficient of a term x_1x_i, $i \neq 1$, is 0). We can write

$$f(x_1, x_2, \ldots, x_n) = c_{1,1}\big(x_1 + g(x_2, \ldots, x_n)\big)^2 + c_1x_1 + \textit{a qurdratic polynomial in } (x_2, \ldots, x_n),$$

where g is a linear form over $x_2, \ldots, x_n$. By adding and then subtracting $c_1 g(x_2, \ldots, x_n)$, we get

$$f(x_1, x_2, \ldots, x_n) = c_{1,1}\big(x_1 + g(x_2, \ldots, x_n)\big)^2 + c_1\big(x_1 + g(x_2, \ldots, x_n)\big) + f'(x_2, \ldots, x_n),$$

where $f'(x_2, \ldots, x_n) \in \mathbb{Z}_q[x_2, \ldots, x_n]$ is a quadratic polynomial over $x_2, \ldots x_n$.

For any fixed $x_2, \ldots, x_n \in \mathbb{Z}_q$, when x_1 goes over $\mathbb{Z}_q$, $x_1 + g(x_2, \ldots, x_n)$ also goes over $\mathbb{Z}_q$. Thus,

$$\sum_{x_1, \ldots, x_n \in \mathbb{Z}_q} \omega_q^{f(x_1, \ldots, x_n)} = \left(\sum_{x \in \mathbb{Z}_q} \omega_q^{c_{1,1}x^2 + c_1 x}\right)\left(\sum_{x_2, \ldots, x_n \in \mathbb{Z}_q} \omega_q^{f'(x_2, \ldots, x_n)}\right) = \sum_{x \in \mathbb{Z}_q} \omega_q^{c_{1,1}x^2 + c_1 x} \cdot Z_q(f').$$

The first term can be evaluated in constant time and the problem is reduced to $Z_q(f')$ in which f' has at most $n-1$ variables.

In the second case, all the square terms of f are either 0 or have orders larger than t_0. Then we assume, without loss of generality, that $c_{1,2} = p^{t_0} c$ and $p \nmid c$. We apply the following transformation: $x_1 = x_1' + x_2'$ and $x_2 = x_1' - x_2'$. Since 2 is invertible in $\mathbb{Z}_q$, when x_1' and x_2' go over $\mathbb{Z}_q^2$, x_1 and x_2 also go over $\mathbb{Z}_q^2$. After the transformation, we get a new quadratic polynomial over $x_1', x_2', x_3, \ldots, x_n$ such that $Z_q(f') = Z_q(f)$. It is easy to check that t_0 is still the smallest order of all the quadratic terms of f': The terms x_1^2 and x_2^2 (in f) produce terms with coefficients divisible by p^{t_0+1}, the term x_1x_2 (in f) produces terms ${x_1'}^2$ and ${x_2'}^2$ with coefficients of order exactly t_0, and terms x_1x_i or x_2x_i, for $i \neq 1, 2$, produce terms $x_1'x_i$ and $x_2'x_i$ with coefficients divisible by p^{t_0}. In particular, the coefficient of $(x_1')^2$ in f' has order exactly t_0, so we can reduce the problem to the first case.

To sum up, we have a polynomial-time algorithm for every $q = p^k$, when $p \neq 2$. □

Now we deal with the more difficult case when $q = 2^k$ is a power of 2, for some $k \geq 1$. We note that the property of an element $c \in \mathbb{Z}_{2^k}$ being even or odd is well-defined. We will use the following simple but important observation, the proof of which is straightforward:

Lemma 12.7. *For any integer x and integer $k > 1$, $(x + 2^{k-1})^2 \equiv x^2 \pmod{2^k}$.*

Lemma 12.8. *Let $q = 2^k$ for some positive integer k. Let $f \in \mathbb{Z}_q[x_1, \ldots, x_n]$ be a quadratic polynomial over n variables $x_1, \ldots, x_n$. Then $Z_q(f)$ can be evaluated in polynomial time (in n).*

Proof. If $k = 1$, $Z_q(f)$ is computable in polynomial time according to [15] so we assume $k > 1$. We also assume f has the form as in (95).

The algorithm goes as follows: For each round, we can, in polynomial time, either

1. output the correct value of $Z_q(f)$; or

2. construct a new quadratic polynomial $g \in \mathbb{Z}_{q/2}[x_1, \ldots, x_n]$ and reduce the computation of $Z_q(f)$ to the computation of $Z_{q/2}(g)$; or

3. construct a new quadratic polynomial $g \in \mathbb{Z}_q[x_1, \ldots, x_{n-1}]$, and reduce the computation of $Z_q(f)$ to the computation of $Z_q(g)$.

This gives us a polynomial-time algorithm for $\mathsf{EVAL}(q)$ since we know how to solve the two base cases when $k = 1$ or $n = 1$ efficiently.

Suppose we have a quadratic polynomial $f \in \mathbb{Z}_q[x_1, \ldots, x_n]$. Our first step is to transform f so that all the coefficients of its cross terms ($c_{i,j}$, where $i \neq j$) and linear terms (c_i) are divisible by 2. Assume f does not yet have this property. We let t be the smallest index in $[n]$ such that one of $\{c_t, c_{t,j} : j > t\}$ is not divisible by 2. By separating out the terms involving x_t, we rewrite f as follows

$$f = c_{t,t} \cdot x_t^2 + x_t \cdot f_1(x_1, \ldots, \widehat{x_t}, \ldots, x_n) + f_2(x_1, \ldots, \widehat{x_t}, \ldots, x_n), \tag{96}$$

where f_1 is an affine linear function and f_2 is a quadratic polynomial. Both f_1 and f_2 are over variables $\{x_1, \ldots, x_n\} - \{x_t\}$. Here the notation $\widehat{x_t}$ means that x_t does not appear in the polynomial. Moreover,

$$f_1(x_1, \ldots, \widehat{x_t}, \ldots, x_n) = \sum_{i<t} c_{i,t} x_i + \sum_{j>t} c_{t,j} x_j + c_t. \tag{97}$$

By the minimality of t, $c_{i,t}$ is even for all $i < t$, and at least one of $\{c_{t,j}, c_t : j > t\}$ is odd.

We claim that

$$Z_q(f) = \sum_{x_1,\ldots,x_n \in \mathbb{Z}_q} \omega_q^{f(x_1,\ldots,x_n)} = \sum_{\substack{x_1,\ldots,x_n \in \mathbb{Z}_q \\ f_1(x_1,\ldots,\widehat{x_t},\ldots,x_n) \equiv 0 \bmod 2}} \omega_q^{f(x_1,\ldots,x_n)}. \tag{98}$$

This is because

$$\sum_{\substack{x_1,\ldots,x_n \in \mathbb{Z}_q \\ f_1 \equiv 1 \bmod 2}} \omega_q^{f(x_1,\ldots,x_n)} = \sum_{\substack{x_1,\ldots,\widehat{x_t},\ldots,x_n \in \mathbb{Z}_q \\ f_1 \equiv 1 \bmod 2}} \sum_{x_t \in \mathbb{Z}_q} \omega_{2^k}^{c_{t,t} x_t^2 + x_t f_1 + f_2}.$$

However, for any fixed $x_1, \ldots, \widehat{x_t}, \ldots, x_n$, $\sum_{x_t \in \mathbb{Z}_q} \omega_{2^k}^{c_{t,t} x_t^2 + x_t f_1 + f_2}$ is equal to $\omega_{2^k}^{f_2}$ times

$$\sum_{x_t \in [0:2^{k-1}-1]} \omega_{2^k}^{c_{t,t} x_t^2 + x_t f_1} + \omega_{2^k}^{c_{t,t}(x_t + 2^{k-1})^2 + (x_t + 2^{k-1}) f_1} = \Big(1 + (-1)^{f_1}\Big) \sum_{x_t \in [0:2^{k-1}-1]} \omega_{2^k}^{c_{t,t} x_t^2 + x_t f_1} = 0,$$

since $f_1 \equiv 1 \bmod 2$, and $1 + (-1)^{f_1} = 0$. Note that we used Lemma 12.7 in the first equation.

Recall f_1 (see (97)) is an affine linear form of $\{x_1, \ldots, \widehat{x_t}, \ldots, x_n\}$. Also note that $c_{i,t}$ is even for all $i < t$, and one of $\{c_{t,j}, c_t : j > t\}$ is odd. We consider the following two cases.

In the first case, $c_{t,j}$ is even for all $j > t$ and c_t is odd. Then for any assignment $(x_1, \ldots, \widehat{x_t}, \ldots, x_n)$ in $\mathbb{Z}_q^{n-1}$, f_1 is odd. As a result, by (98), $Z_q(f)$ is trivially zero.

In the second case, there exists at least one $j > t$ such that $c_{t,j}$ is odd. Let $\ell > t$ be the smallest of such $j's$. Then we substitute the variable x_ℓ in f with a new variable x'_ℓ over $\mathbb{Z}_q$, where (since $c_{t,\ell}$ is odd, $c_{t,\ell}$ is invertible in $\mathbb{Z}_q$)

$$x_\ell = c_{t,\ell}^{-1} \left(2x'_\ell - \left(\sum_{i<t} c_{i,t} x_i + \sum_{j>t, j \neq \ell} c_{t,j} x_j + c_t \right) \right). \tag{99}$$

and let f' denote the new quadratic polynomial in $\mathbb{Z}_q[x_1, \ldots, x'_\ell, \ldots, x_n]$.

We claim that

$$Z_q(f') = 2 \cdot Z_q(f) = 2 \cdot \sum_{\substack{x_1,\ldots,x_n \in \mathbb{Z}_q \\ f_1 \equiv 0 \bmod 2}} \omega_q^{f(x_1,\ldots,x_n)}.$$

To see this, we define the following map from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q^n$:

$$(x_1, \ldots, x'_\ell, \ldots, x_n) \mapsto (x_1, \ldots, x_\ell, \ldots, x_n),$$

where x_ℓ satisfies (99). It is easy to show that the range of the map is the set of $(x_1, \ldots, x_\ell, \ldots, x_n)$ in $\mathbb{Z}_q^n$ such that f_1 is even. Moreover, for every such tuple $(x_1, \ldots, x_\ell, \ldots, x_n)$ the number of its preimages in $\mathbb{Z}_q^n$ is exactly two. The claim then follows.

So to compute $Z_q(f)$, we only need to compute $Z_q(f')$. The advantage of $f' \in \mathbb{Z}_q[x_1, \ldots, x'_\ell, \ldots, x_n]$ over f is the following property that we are going to prove:

(*Even*): For every cross term and linear term that involves $x_1, \ldots, x_t$, its coefficient in f' is even.

To prove this, we divide the terms of f' (that we are interested in) into three groups: Cross and linear terms that involve x_t; linear terms x_s, $s < t$; and cross terms of the form $x_s x_{s'}$, where $s < s', s < t$.

Firstly, we consider the expression (96) of f after the substitution. The first term $c_{t,t}x_t^2$ remains the same; The second term $x_t f_1$ becomes $2x_t x'_\ell$ by (99); and x_t does not appear in the third term, even after the substitution. Therefore, condition (*Even*) holds for x_t.

Secondly, we consider the coefficient c'_s of the linear term x_s in f', where $s < t$. Only the following terms in f can possibly contribute to c'_s:

$$c_s x_s,\ c_{\ell,\ell} x_\ell^2,\ c_{s,\ell} x_s x_\ell, \text{ and } c_\ell x_\ell.$$

By the minimality of t, both c_s and $c_{s,\ell}$ are even. For $c_{\ell,\ell}x_\ell^2$ and $c_\ell x_\ell$, although we do not know whether $c_{\ell,\ell}$ and c_ℓ are even or odd, we know that the coefficient $-c_{t,\ell}^{-1} c_{s,t}$ of x_s in (99) is even since $c_{s,t}$ is even. As a result, for every term in the list above, its contribution to c'_s is even and thus, c'_s is even.

Finally, we consider the coefficient $c'_{s,s'}$ of the term $x_s x_{s'}$ in f', where $s < s'$ and $s < t$. Similarly, only the following terms in f can possibly contribute to $c'_{s,s'}$ (Here we consider the general case when $s' \neq \ell$. The special case when $s' = \ell$ is easier)

$$c_{s,s'} x_s x_{s'},\ c_{\ell,\ell} x_\ell^2,\ c_{s,\ell} x_s x_\ell, \text{ and } c_{\ell,s'} x_\ell x_{s'} \text{ (or } c_{s',\ell} x_{s'} x_\ell).$$

Again, by the minimality of t, $c_{s,s'}$ and $c_{s,\ell}$ are even. Moreover, the coefficient $-c_{t,\ell}^{-1} c_{s,t}$ of x_s in (99) is even. As a result, for every term listed above, its contribution to $c'_{s,s'}$ is even and thus, $c'_{s,s'}$ is even.

To summarize, after substituting x_ℓ with x'_ℓ using (99), we get a new quadratic polynomial f' such that $Z_q(f') = 2 \cdot Z_q(f)$, and for every cross term and linear term that involves $x_1, \ldots, x_t$, its coefficient in f' is even. We can repeat this substitution procedure on f': Either we show that $Z_q(f')$ is trivially 0, or we get a quadratic polynomial f'' such that $Z_q(f'') = 2 \cdot Z_q(f')$ and the parameter t increases by at least one. As a result, given any quadratic polynomial f, we can, in polynomial time, either show that $Z_q(f)$ is zero, or construct a new quadratic polynomial $g \in \mathbb{Z}_q[x_1, \ldots, x_n]$ such that $Z_q(f) = 2^k \cdot Z_q(g)$, for some known integer $k \in [0:n]$, and every cross term and linear term has an even coefficient in g.

Now we only need to compute $Z_q(g)$. We will show that, given such a polynomial g in n variables, we can reduce it to either $\mathsf{EVAL}(2^{k-1}) = \mathsf{EVAL}(q/2)$, or to the computation of $Z_q(g')$, in which g' is a quadratic polynomial in $n-1$ variables.

Let

$$g = \sum_{i \le j \in [n]} a_{i,j} x_i x_j + \sum_{i \in [n]} a_i x_i + a,$$

then we consider the following two cases: $a_{i,i}$ is even for all $i \in [n]$; or at least one of the $a_{i,i}$'s is odd.

In the first case, we know $a_{i,j}$ and a_i are even for all $i \le j \in [n]$. We let $a'_{i,j}$ and a'_i denote integers in $[0 : 2^{k-1} - 1]$ such that $a_{i,j} \equiv 2a'_{i,j} \pmod q$ and $a_i \equiv 2a'_i \pmod q$, respectively. Then,

$$Z_q(g) = \omega_q^a \cdot \sum_{x_1,\ldots,x_n \in \mathbb{Z}_q} \omega_q^{2\left(\sum_{i \le j \in [n]} a'_{i,j} x_i x_j + \sum_{i \in [n]} a'_i x_i\right)} = 2^n \cdot \omega_q^a \cdot Z_{2^{k-1}}(g'),$$

where

$$g' = \sum_{i \le j \in [n]} a'_{i,j} x_i x_j + \sum_{i \in [n]} a'_i x_i$$

is a quadratic polynomial over $\mathbb{Z}_{q/2} = \mathbb{Z}_{2^{k-1}}$. This reduces the computation of $Z_q(g)$ to $Z_{q/2}(g')$.

In the second case, without loss of generality, we assume $a_{1,1}$ is odd. Then we have

$$f = a_{1,1}(x_1^2 + 2x_1 g_1) + g_2 = a_{1,1}(x_1 + g_1)^2 + g',$$

where g_1 is an affine linear form, and g_2, g' are quadratic polynomials, all of which are over $x_2, \ldots, x_n$. We are able to do this because $a_{1,j}$ and a_1, for all $j \ge 2$, are even. Now we have

$$Z_q(g) = \sum_{x_1,\ldots,x_n \in \mathbb{Z}_q} \omega_q^{a_{1,1}(x_1+g_1)^2 + g'} = \sum_{x_2,\ldots,x_n \in \mathbb{Z}_q} \omega_q^{g'} \cdot \sum_{x_1 \in \mathbb{Z}_q} \omega_q^{a_{1,1}(x_1+g_1)^2} = \left(\sum_{x \in \mathbb{Z}_q} \omega_q^{a_{1,1}x^2}\right) \cdot Z_q(g').$$

The last equation is because the sum over $x_1 \in \mathbb{Z}_q$ is independent of the value of g_1. This reduces the computation of $Z_q(g)$ to $Z_q(g')$ in which g' is a quadratic polynomial in $n-1$ variables.

To sum up, given any quadratic polynomial f, we can, in polynomial time, either output the correct value of $Z_q(f)$; or reduce one of the two parameters, k or n, by at lease one. This gives us a polynomial time algorithm to evaluate $Z_q(f)$. $\square$

13 Proof of Theorem 6.2

Let $\mathbf{A}$ be a symmetric, non-bipartite and purified matrix. After collecting its entries of equal norm in decreasing order (by permuting the rows and columns of $\mathbf{A}$), there exist a positive integer N, and two sequences $\boldsymbol{\kappa}$ and $\mathbf{m}$ such that $(\mathbf{A}, (N, \boldsymbol{\kappa}, \mathbf{m}))$ satisfies the following condition:

($\mathcal{S}'_1$) Matrix $\mathbf{A}$ is an $m \times m$ symmetric matrix. $\boldsymbol{\kappa} = \{\kappa_1, \kappa_2, \ldots, \kappa_s\}$ is a sequence of positive rational numbers of length $s \ge 1$ such that $\kappa_1 > \kappa_2 > \ldots > \kappa_s > 0$. $\mathbf{m} = \{m_1, \ldots, m_s\}$ is a sequence of positive integers such that $m = \sum m_i$. The rows (and columns) of $\mathbf{A}$ are indexed by $\mathbf{x} = (x_1, x_2)$ where $x_1 \in [s]$ and $x_2 \in [m_{x_1}]$. For all $\mathbf{x}, \mathbf{y}$, we have

$$A_{\mathbf{x},\mathbf{y}} = A_{(x_1,x_2),(y_1,y_2)} = \kappa_{x_1} \kappa_{y_1} S_{\mathbf{x},\mathbf{y}},$$

where $\mathbf{S} = \{S_{\mathbf{x},\mathbf{y}}\}$ is an $m \times m$ symmetric matrix in which every entry is a power of ω_N:

$$\mathbf{A} = \begin{pmatrix} \kappa_1 \mathbf{I}_{m_1} & & & \\ & \kappa_2 \mathbf{I}_{m_2} & & \\ & & \ddots & \\ & & & \kappa_s \mathbf{I}_{m_s} \end{pmatrix} \begin{pmatrix} \mathbf{S}_{(1,*),(1,*)} & \mathbf{S}_{(1,*),(2,*)} & \ldots & \mathbf{S}_{(1,*),(s,*)} \\ \mathbf{S}_{(2,*),(1,*)} & \mathbf{S}_{(2,*),(2,*)} & \ldots & \mathbf{S}_{(2,*),(s,*)} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{S}_{(s,*),(1,*)} & \mathbf{S}_{(s,*),(2,*)} & \ldots & \mathbf{S}_{(s,*),(s,*)} \end{pmatrix} \begin{pmatrix} \kappa_1 \mathbf{I}_{m_1} & & & \\ & \kappa_2 \mathbf{I}_{m_2} & & \\ & & \ddots & \\ & & & \kappa_s \mathbf{I}_{m_s} \end{pmatrix},$$

where $\mathbf{I}_{m_i}$ is the $m_i \times m_i$ identity matrix.

We use I to denote

$$I = \{(i,j) \mid i \in [s], j \in [m_i]\}.$$

The proof of Theorem 6.2, just like the one of Theorem 5.2, consists of five steps. All the proofs, as one will see, use the following strategy: We construct, from the $m \times m$ matrix $\mathbf{A}$, its bipartisation $\mathbf{A}'$ (which is a $2m \times 2m$ symmetric matrix). Then we just apply the lemmas for the bipartite case to $\mathbf{A}'$, and show that $\mathbf{A}'$ is either #P-hard or has certain properties. Finally, we use these properties of $\mathbf{A}'$ to derive properties of $\mathbf{A}$.

We need the following lemma:

Lemma 13.1. *Let $\mathbf{A}$ be a symmetric matrix, and $\mathbf{A}'$ be its bipartisation, then $\mathsf{EVAL}(\mathbf{A}') \le \mathsf{EVAL}(\mathbf{A})$.*

Proof. Suppose $\mathbf{A}$ is an $m \times m$ matrix. Let G be a connected undirected graph. If G is not bipartite, then $Z_{\mathbf{A}'}(G)$ is trivially 0, since $\mathbf{A}'$ is the bipartisation of $\mathbf{A}$. Otherwise, we assume $G = (U \cup V, E)$ to be a bipartite and connected graph, and u^* be a vertex in U. It is easy to show that

$$Z_{\mathbf{A}}(G, u^*, i) = Z_{\mathbf{A}'}(G, u^*, i) = Z_{\mathbf{A}'}(G, u^*, m+i), \quad \text{for any } i \in [m].$$

It then follows that $Z_{\mathbf{A}'}(G) = 2 \cdot Z_{\mathbf{A}}(G)$, and $\mathsf{EVAL}(\mathbf{A}') \le \mathsf{EVAL}(\mathbf{A})$. □

13.1 Step 2.1

Lemma 13.2. *Suppose $(\mathbf{A}, (N, \boldsymbol{\kappa}, \mathbf{m}))$ satisfies $(\mathcal{S}_1')$, then either $\mathsf{EVAL}(\mathbf{A})$ is #P-hard or $(\mathbf{A}, (N, \boldsymbol{\kappa}, \mathbf{m}))$ satisfies the following condition:*

$(\mathcal{S}_2')$ For all $\mathbf{x}, \mathbf{x}' \in I$, either there exists an integer k such that $\mathbf{S}_{\mathbf{x},*} = \omega_N^k \cdot \mathbf{S}_{\mathbf{x}',*}$; or for every $j \in [s]$,

$$\langle \mathbf{S}_{\mathbf{x},(j,*)}, \mathbf{S}_{\mathbf{x}',(j,*)} \rangle = 0.$$

Proof. Suppose $\mathsf{EVAL}(\mathbf{A})$ is not #P-hard.

Let $\mathbf{A}'$ denote the bipartisation of $\mathbf{A}$. Then by Lemma 13.1, $\mathsf{EVAL}(\mathbf{A}') \le \mathsf{EVAL}(\mathbf{A})$, and $\mathsf{EVAL}(\mathbf{A}')$ is also not #P-hard. It is easy to check that $(\mathbf{A}', (N, \boldsymbol{\kappa}, \boldsymbol{\kappa}, \mathbf{m}, \mathbf{m})$ satisfies condition $(\mathcal{S}_1)$, so by Lemma 8.2 together with the assumption that $\mathbf{A}'$ is not #P-hard (also note that the $\mathbf{S}$ matrix in Lemma 8.2 is exactly the same $\mathbf{S}$ we have here), $\mathbf{S}$ satisfies $(\mathcal{S}_2)$ which is exactly the same as $(\mathcal{S}_2')$ here (note that in Lemma 8.2, $\mathbf{S}$ also need to satisfy $(\mathcal{S}_3)$, but since $\mathbf{S}$ is symmetric here, $(\mathcal{S}_3)$ is the same as $(\mathcal{S}_2)$). □

We also have the following corollary. The proof is exactly the same as the one of Corollary 8.3.

Corollary 13.1. *For all $i, j \in [s]$, the $(i,j)^{th}$ block matrix $\mathbf{S}_{(i,*),(j,*)}$ has the same rank as $\mathbf{S}$.*

Next, we apply the Cyclotomic Reduction Lemma on $\mathbf{A}$ to build a pair $(\mathbf{F}, \mathfrak{D})$ such that

$$\mathsf{EVAL}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{F}, \mathfrak{D}).$$

Let $h = \text{rank}(\mathbf{S})$. By Corollary 13.1, it can be easily proved that there exist $1 \le i_1 < \ldots < i_h \le m_1$ such that, the $\{(1, i_1), \ldots, (1, i_h)\} \times \{(1, i_1), \ldots, (1, i_h)\}$ submatrix of $\mathbf{S}$ has full rank h (using the fact that $\mathbf{S}$ is symmetric). Without loss of generality (if this is not the case, we can apply an appropriate permutation Π to the rows and columns of $\mathbf{A}$ so that the new $\mathbf{S}$ has this property), we assume $i_k = k$ for all $k \in [h]$. We use $\mathbf{H}$ to denote this $h \times h$ symmetric matrix: $H_{i,j} = S_{(1,i),(1,j)}$.

By Corollary 13.1 and Lemma 13.2, for any index $\mathbf{x} \in I$, there exist two unique integers $j \in [h]$ and $k \in [0 : N-1]$ such that

$$\mathbf{S}_{\mathbf{x},*} = \omega_N^k \cdot \mathbf{S}_{(1,j),*} \quad \text{and} \quad \mathbf{S}_{*,\mathbf{x}} = \omega_N^k \cdot \mathbf{S}_{*,(1,j)}. \tag{100}$$

This gives us a partition of the index set I

$$\mathscr{R} = \big\{R_{(i,j),k} \,\big|\, i \in [s], j \in [h], k \in [0:N-1]\big\},$$

as follows: For every $\mathbf{x} \in I$, $\mathbf{x} \in R_{(i,j),k}$ iff $i = x_1$ and $\mathbf{x}, j, k$ satisfy (100). By Corollary 13.1, we have

$$\bigcup_{k \in [0:N-1]} R_{(i,j),k} \neq \emptyset, \quad \text{for all } i \in [s] \text{ and } j \in [h].$$

Now we define $(\mathbf{F}, \mathfrak{D})$ and use the Cyclotomic Reduction Lemma together with $\mathscr{R}$ to show that

$$\mathsf{EVAL}(\mathbf{F}, \mathfrak{D}) \equiv \mathsf{EVAL}(\mathbf{A}).$$

First, $\mathbf{F}$ is an $sh \times sh$ matrix. We use $I' \equiv [s] \times [h]$ to index the rows and columns of $\mathbf{F}$. Then

$$F_{\mathbf{x},\mathbf{y}} = \kappa_{x_1}\kappa_{y_1} H_{x_2,y_2} = \kappa_{x_1}\kappa_{y_1} S_{(1,x_2),(1,y_2)}, \quad \text{for all } \mathbf{x}, \mathbf{y} \in I'.$$

or equivalently,

$$\mathbf{F} = \begin{pmatrix} \kappa_1 \mathbf{I} & & & \\ & \kappa_2 \mathbf{I} & & \\ & & \ddots & \\ & & & \kappa_s \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{H} & \mathbf{H} & \dots & \mathbf{H} \\ \mathbf{H} & \mathbf{H} & \dots & \mathbf{H} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{H} & \mathbf{H} & \dots & \mathbf{H} \end{pmatrix} \begin{pmatrix} \kappa_1 \mathbf{I} & & & \\ & \kappa_2 \mathbf{I} & & \\ & & \ddots & \\ & & & \kappa_s \mathbf{I} \end{pmatrix},$$

where $\mathbf{I}$ is the $h \times h$ identity matrix.

Second, $\mathfrak{D} = \{\mathbf{D}^{[0]}, \ldots, \mathbf{D}^{[N-1]}\}$ is a sequence of N diagonal matrices of the same size as $\mathbf{F}$. We use I' to index its diagonal entries. The $\mathbf{x}^{th}$ entries of $\mathfrak{D}$ are generated by $(|R_{(x_1,x_2),0}|, \ldots, |R_{(x_1,x_2),N-1}|)$:

$$D^{[r]}_{\mathbf{x}} = \sum_{k=0}^{N-1} \big|R_{(x_1,x_2),k}\big| \cdot \omega_N^{kr}, \quad \text{for all } r \in [0:N-1], \mathbf{x} \in I'.$$

The following lemma is a direct application of the Cyclotomic Reduction Lemma (Lemma 8.1).

Lemma 13.3. $\mathsf{EVAL}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$.

Proof. First we show that matrix $\mathbf{A}$ can be generated from $\mathbf{F}$ using $\mathscr{R}$. Let $\mathbf{x}, \mathbf{y} \in I$, $\mathbf{x} \in R_{(x_1,j),k}$ and $\mathbf{y} \in R_{(y_1,j'),k'}$ for some j, k, j', k', then by (100),

$$A_{\mathbf{x},\mathbf{y}} = \kappa_{x_1}\kappa_{y_1} S_{\mathbf{x},\mathbf{y}} = \kappa_{x_1}\kappa_{y_1} S_{(1,j),\mathbf{y}} \cdot \omega_N^k = \kappa_{x_1}\kappa_{y_1} S_{(1,j),(1,j')} \cdot \omega_N^{k+k'} = F_{(x_1,j),(y_1,j')} \cdot \omega_N^{k+k'}.$$

On the other hand, the construction of $\mathfrak{D}$ implies that $\mathfrak{D}$ can be generated from the partition $\mathscr{R}$. The lemma then follows directly from the Cyclotomic Reduction Lemma. □

13.2 Steps 2.2 and 2.3

Now we get a pair $(\mathbf{F}, \mathfrak{D})$ that satisfies the following condition (*Shape'*):

($Shape'_1$): $\mathbf{F} \in \mathbb{C}^{m \times m}$ (note that this m is different from the m used in Step 2.1) is an symmetric $s \times s$ block matrix and we use $I = [s] \times [h]$ to index its rows and columns.

($Shape'_2$): There is a sequence $\boldsymbol{\kappa} = \{\kappa_1 > \ldots > \kappa_s > 0\}$ of rational numbers together with an $h \times h$ matrix $\mathbf{H}$ of full rank, whose entries are all powers of ω_N, for some positive integer N. We have

$$F_{\mathbf{x},\mathbf{y}} = \kappa_{x_1}\kappa_{y_1} H_{x_2,y_2}, \quad \text{for all } \mathbf{x}, \mathbf{y} \in I.$$

(Shape'_3): $\mathfrak{D} = \{\mathbf{D}^{[0]}, \ldots, \mathbf{D}^{[N-1]}\}$ is a sequence of N $m \times m$ diagonal matrices. $\mathfrak{D}$ satisfies ($\mathcal{T}_3$), so

$$D^{[r]}_{\mathbf{x}} = \overline{D^{[N-r]}_{\mathbf{x}}}, \quad \text{for all } r \in [N-1], \text{ and } \mathbf{x} \in I.$$

Now suppose $\mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ is not #P-hard.

We build the following pair $(\mathbf{C}, \hat{\mathfrak{D}})$: $\mathbf{C}$ is the bipartisation of $\mathbf{F}$ and $\hat{\mathfrak{D}} = \{\hat{\mathbf{D}}^{[0]}, \ldots, \hat{\mathbf{D}}^{[N-1]}\}$, where

$$\hat{\mathbf{D}}^{[r]} = \begin{pmatrix} \mathbf{D}^{[r]} & \\ & \mathbf{D}^{[r]} \end{pmatrix}, \quad \text{for all } r \in [0 : N-1].$$

The proof of the following lemma is the same as the one of Lemma 13.1.

Lemma 13.4. $\mathsf{EVAL}(\mathbf{C}, \hat{\mathfrak{D}}) \le \mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$.

By Lemma 13.4 above, we have $\mathsf{EVAL}(\mathbf{C}, \hat{\mathfrak{D}}) \le \mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$, and $\mathsf{EVAL}(\mathbf{C}, \hat{\mathfrak{D}})$ is also not #P-hard. Using (Shape'_1)-(Shape'_3), one can check that $(\mathbf{C}, \hat{\mathfrak{D}})$ satisfies (Shape_1)-(Shape_3). Therefore, by Lemma 8.4 and Lemma 8.7, $(\mathbf{C}, \hat{\mathfrak{D}})$ must also satisfy (Shape_4)-(Shape_6). Since $(\mathbf{C}, \hat{\mathfrak{D}})$ is built from $(\mathbf{F}, \mathfrak{D})$, we have the latter must satisfy the following conditions:

(Shape'_4): $\frac{1}{\sqrt{n}} \cdot \mathbf{H}$ *is unitary:* $\langle \mathbf{H}_{i,*}, \mathbf{H}_{j,*} \rangle = \langle \mathbf{H}_{*,i}, \mathbf{H}_{*,j} \rangle = 0$ *for all* $i \neq j \in [h]$*;*

(Shape'_5): $D^{[0]}_{\mathbf{x}} = D^{[0]}_{(x_1,1)}$ for all $\mathbf{x} \in I$;

(Shape'_6): For every $r \in [N-1]$, there exist two diagonal matrices: $\mathbf{K}^{[r]} \in \mathbb{C}^{s \times s}$ and $\mathbf{L}^{[r]} \in \mathbb{C}^{h \times h}$. The norm of every diagonal entry in $\mathbf{L}^{[r]}$ is either 0 or 1. We have

$$\mathbf{D}^{[r]} = \mathbf{K}^{[r]} \otimes \mathbf{L}^{[r]}, \quad \text{for any } r \in [N-1].$$

Moreover, for any $r \in [N-1]$,

$$\mathbf{K}^{[r]} = \mathbf{0} \iff \mathbf{L}^{[r]} = \mathbf{0} \quad \text{and} \quad \mathbf{L}^{[r]} \neq \mathbf{0} \implies \exists i \in [h],\ L^{[r]}_i = 1.$$

In particular, (Shape'_5) means by setting

$$K^{[0]}_i = D^{[0]}_{(i,1)} \quad \text{and} \quad L^{[0]}_j = 1, \quad \text{for all } i \in [s] \text{ and } j \in [h].$$

we have $\mathbf{D}^{[0]} = \mathbf{K}^{[0]} \otimes \mathbf{L}^{[0]}$, where $\mathbf{L}^{[0]}$ is the $h \times h$ identity matrix. By ($\mathcal{T}_3$) in (Shape'_3), every entry of $\mathbf{K}^{[0]}$ is a positive integer.

13.3 Step 2.4

Suppose $(\mathbf{F}, \mathfrak{D})$ satisfies conditions (Shape'_1)-(Shape'_6). By (Shape'_2), we have $\mathbf{F} = \mathbf{M} \otimes \mathbf{H}$, where $\mathbf{M}$ is the $s \times s$ matrix of rank 1: $M_{i,j} = \kappa_i \kappa_j$ for all $i, j \in [s]$.

We now decompose $\mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ into two problems $\mathsf{EVAL}(\mathbf{M}, \mathfrak{K})$ and $\mathsf{EVAL}(\mathbf{H}, \mathfrak{L})$, where

$$\mathfrak{K} = \{\mathbf{K}^{[0]}, \ldots, \mathbf{K}^{[N-1]}\}, \quad \text{and} \quad \mathfrak{L} = \{\mathbf{L}^{[0]}, \ldots, \mathbf{L}^{[N-1]}\}.$$

The proof of the following lemma is essentially the same as the one of Lemma 8.10:

Lemma 13.5. $\mathsf{EVAL}(\mathbf{F}, \mathfrak{D}) \equiv \mathsf{EVAL}(\mathbf{H}, \mathcal{L})$.

13.4 Step 2.5

We normalize the matrix $\mathbf{H}$, in the same way we did for the bipartite case, to obtain a new pair that 1). satisfies conditions $(\mathcal{U}_1')$-$(\mathcal{U}_4')$; and 2). is polynomial-time equivalent to $\mathsf{EVAL}(\mathbf{H},\mathcal{L})$.

14 Proofs of Theorem 6.3 and Theorem 6.4

Let $((M,N),\mathbf{F},\mathfrak{D})$ be a triple that satisfies $(\mathcal{U}_1')$-$(\mathcal{U}_4')$. We prove Theorem 6.3 and 6.4 in this section.

We first prove that, if $\mathbf{F}$ does not satisfy the group condition $(\mathcal{GC})$, then $\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$ is #P-hard. This is done by applying Lemma 9.1 (for the bipartite case) to the bipartisation $\mathbf{C}$ of $\mathbf{F}$:

Lemma 14.1. *Let $((M,N),\mathbf{F},\mathfrak{D})$ be a triple that satisfies conditions $(\mathcal{U}_1')$-$(\mathcal{U}_4')$, then either the matrix $\mathbf{F}$ satisfies the group condition $(\mathcal{GC})$, or $\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$ is #P-hard.*

Proof. Suppose $\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$ is not #P-hard.

Let $\mathbf{C}$ and $\mathfrak{E}=\{\mathbf{E}^{[0]},\ldots,\mathbf{E}^{[N-1]}\}$ denote the bipartisations of $\mathbf{F}$ and $\mathfrak{D}$, respectively:

$$\mathbf{C}=\begin{pmatrix}\mathbf{0} & \mathbf{F}\\ \mathbf{F} & \mathbf{0}\end{pmatrix}, \quad \text{and} \quad \mathbf{E}^{[r]}=\begin{pmatrix}\mathbf{D}^{[r]} & \mathbf{0}\\ \mathbf{0} & \mathbf{D}^{[r]}\end{pmatrix}, \quad \text{for all } r\in[0:N-1].$$

By using $(\mathcal{U}_1')$-$(\mathcal{U}_4')$, one can show that $((M,N),\mathbf{C},\mathfrak{E})$ satisfies $(\mathcal{U}_1)$-$(\mathcal{U}_4)$. Furthermore, by Lemma 13.4, we have $\mathsf{EVAL}(\mathbf{C},\mathfrak{E})\le\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$ and thus, $\mathsf{EVAL}(\mathbf{C},\mathfrak{E})$ is also not #P-hard. It then follows from Lemma 9.1 that $\mathbf{F}$ satisfies the group condition $(\mathcal{GC})$. □

14.1 Proof of Theorem 6.3

We prove Theorem 6.3, again, by using $\mathbf{C}$ and $\mathfrak{E}$: the bipartisations of $\mathbf{F}$ and $\mathfrak{D}$, respectively.

Suppose $\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$ is not #P-hard. On the one hand, $\mathsf{EVAL}(\mathbf{C},\mathfrak{E})\le\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$ and $\mathsf{EVAL}(\mathbf{C},\mathfrak{E})$ is also not #P-hard. On the other hand, $((M,N),\mathbf{C},\mathfrak{E})$ satisfies conditions $(\mathcal{U}_1)$-$(\mathcal{U}_4)$. As a result, by Theorem 5.3, $\mathfrak{E}$ must satisfy $(\mathcal{U}_5)$: Every entry of $\mathbf{E}^{[r]}$, $r\in[N-1]$, is either 0 or a power of ω_N. It then follows directly that every entry of $\mathbf{D}^{[r]}$, $r\in[N-1]$, is either 0 or a power of ω_N.

14.2 Proof of Theorem 6.4

In this section, we prove Theorem 6.4.

However, we can not simply reduce it, using pair $(\mathbf{C},\mathfrak{E})$, to the bipartite case (Theorem 5.4). The reason is because, in Theorem 6.4, we are only allowed to permute the rows and columns symmetrically, while in Theorem 5.4, one can use two different permutations to permute the rows and columns. But as we will see below, for most of the lemmas we need here, their proofs are exactly the same as those for the bipartite case. The only exception is the counterpart of Lemma 9.5, in which we have to bring in the generalized Fourier matrices (see Section 4.3 for the definition).

Suppose $\mathbf{F}$ satisfies $(\mathcal{GC})$ (otherwise we already know that $\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$ is #P-hard).

We let F^R denote the set of row vectors $\{\mathbf{F}_{i,*}\}$ of $\mathbf{F}$ and F^C denote the set of column vectors $\{\mathbf{F}_{*,j}\}$ of $\mathbf{F}$. Since $\mathbf{F}$ satisfies $(\mathcal{GC})$, by Property 9.1, both F^R and F^C are finite Abelian groups of order m, under the Hadamard product.

We start the proof by proving a symmetric version of Lemma 9.4, stating that when $M=pq$ and $\gcd(p,q)=1$ (note that p and q are not necessarily primes), $\mathbf{F}$ (after an appropriate permutation) is the tensor product of two smaller discrete unitary matrices, both of which satisfy the group condition.

Lemma 14.2. *Let* $\mathbf{F} \in \mathbb{C}^{m\times m}$ *be a symmetric* M*-discrete unitary matrix that satisfies* $(\mathcal{GC})$*. Moreover,* $M = pq$*,* $p, q > 1$ *and* $\gcd(p,q) = 1$*. Then there is a permutation* $\Pi : [0 : m-1] \to [0 : m-1]$ *such that*

$$\mathbf{F}_{\Pi,\Pi} = \mathbf{F}' \otimes \mathbf{F}'',$$

where $\mathbf{F}'$ *is a symmetric* p*-discrete unitary matrix,* $\mathbf{F}''$ *is a symmetric* q*-discrete unitary matrix, and both of them satisfy* $(\mathcal{GC})$*.*

Proof. The proof is almost the same as the one of Lemma 9.4. The only thing to notice is that, as $\mathbf{F}$ is symmetric, the two correspondences f, g that we defined in the proof of Lemma 9.4, from $[0 : m-1]$ to $[0 : m'-1] \times [0 : m''-1]$, are exactly the same. As a result, the row permutation Π and the column permutation Σ that we apply on $\mathbf{F}$ are the same. ◻

As a result, we only need to deal with the case when $M = p^\beta$ is a prime power.

Lemma 14.3. *Let* $\mathbf{F} \in \mathbb{C}^{m\times m}$ *be a symmetric* M*-discrete unitary matrix that satisfies* $(\mathcal{GC})$*. Moreover* $M = p^\beta$ *is a prime power,* $p \neq 2$*, and* $\beta \geq 1$*. Then there must exist an integer* $k \in [0 : m-1]$ *such that* $F_{k,k} = \omega_M^{\alpha_{k,k}}$ *and* $p \nmid \alpha_{k,k}$*.*

Proof. For $i, j \in [0 : m-1]$, we let $\alpha_{i,j}$ denote the integer in $[0 : M-1]$ such that $F_{i,j} = \omega_M^{\alpha_{i,j}}$.

Assume the lemma is not true, that is, $p \,|\, \alpha_{k,k}$ for all k. Since $\mathbf{F}$ is M-discrete unitary, there must exist $i \neq j \in [0 : m-1]$ such that $p \nmid \alpha_{i,j}$. Without loss of generality, we assume $p \nmid \alpha_{2,1} = \alpha_{1,2}$.

As $\mathbf{F}$ satisfies $(\mathcal{GC})$, there must exist a $k \in [0 : m-1]$ such that $\mathbf{F}_{k,*} = \mathbf{F}_{1,*} \circ \mathbf{F}_{2,*}$. However,

$$\omega_M^{\alpha_{k,k}} = F_{k,k} = F_{1,k}F_{2,k} = F_{k,1}F_{k,2} = F_{1,1}F_{2,1}F_{1,2}F_{2,2} = \omega_M^{\alpha_{1,1}+\alpha_{2,2}+2\alpha_{1,2}},$$

and $\alpha_{k,k} \equiv \alpha_{1,1} + \alpha_{2,2} + 2\alpha_{1,2} \pmod{M}$ implies that $0 \equiv 0 + 0 + 2\alpha_{1,2} \pmod{p}$. Since $p \neq 2$ and $p \nmid \alpha_{1,2}$ we get a contradiction. ◻

The next lemma is the symmetric version of Lemma 9.5 showing that when there exists a diagonal entry $F_{k,k}$ such that $p \nmid \alpha_{k,k}$, then $\mathbf{F}$ is the tensor product of a Fourier matrix and a discrete unitary matrix. Note that this lemma also applies to the case when $p = 2$. So the only case left is when $p = 2$ but $2 \,|\, \alpha_{i,i}$ for all $i \in [0 : m-1]$.

Lemma 14.4. *Let* $\mathbf{F} \in \mathbb{C}^{m\times m}$ *be a symmetric* M*-discrete unitary matrix that satisfies* $(\mathcal{GC})$*. Moreover,* $M = p^\beta$ *is a prime power. If there exists a* $k \in [0 : m-1]$ *such that* $F_{k,k} = \omega_M^\alpha$ *and* $p \nmid \alpha$*, then one can find a permutation* Π *such that*

$$\mathbf{F}_{\Pi,\Pi} = \boldsymbol{\mathcal{F}}_{M,\alpha} \otimes \mathbf{F}',$$

where $\mathbf{F}'$ *is a symmetric* M'*-discrete unitary matrix,* $M' = p^{\beta'}$ *for some* $\beta' \leq \beta$*, and* $\mathbf{F}'$ *satisfies* $(\mathcal{GC})$*.*

Proof. The proof is exactly the same as the one of Lemma 9.5 by setting $a = k$ and $b = k$. The only thing to notice is that, as $\mathbf{F}$ is symmetric, the two correspondences f and g that we defined in the proof of Lemma 9.5 are the same. As a result, the row permutation Π and the column permutation Σ that we apply on $\mathbf{F}$ are the same. Also note that, since $F_{k,k} = \omega_M^\alpha$, (65) becomes

$$G_{(x_1,x_2),(y_1,y_2)} = \omega_M^{\alpha x_1 y_1} \cdot G_{(0,x_2),(0,y_2)}.$$

This explains why we need to use Fourier matrix $\boldsymbol{\mathcal{F}}_{M,\alpha}$ here. ◻

Finally, we deal with the case when $p = 2$ and $2 \,|\, \alpha_{i,i}$ for all $i \in [0 : m-1]$.

Lemma 14.5. *Let* $\mathbf{F} \in \mathbb{C}^{m\times m}$ *be a symmetric* M*-discrete unitary matrix that satisfies condition* $(\mathcal{GC})$*. Moreover,* $M = 2^\beta$ *and* $2\,|\,\alpha_{i,i}$ *for all* $i \in [0 : m-1]$*. Then one can find a permutation* Π *together with a symmetric non-degenerate matrix* $\mathbf{W}$ *in* $\mathbb{Z}_M^{2\times 2}$ (see Section 4.3 for definition) *such that*

$$\mathbf{F}_{\Pi,\Pi} = \boldsymbol{\mathcal{F}}_{M,\mathbf{W}} \otimes \mathbf{F}',$$

where $\mathbf{F}'$ *is a symmetric* M'*-discrete unitary matrix,* $M' = 2^{\beta'}$ *for some* $\beta' \le \beta$*, and* $\mathbf{F}'$ *satisfies* $(\mathcal{GC})$*.*

Proof. By Property 9.2, there exist two integers $a \ne b$ such that $F_{a,b} = F_{b,a} = \omega_M$. Let $F_{a,a} = \omega^{\alpha_a}$ and $F_{b,b} = \omega^{\alpha_b}$. The assumption of the lemma implies that $2\,|\,\alpha_a, \alpha_b$.

We let $S^{a,b}$ denote the following subset of F^R:

$$S^{a,b} = \{\mathbf{u} \in F^R \,\big|\, u_a = u_b = 1\}.$$

It is easy to see that $S^{a,b}$ is a subgroup of F^R. On the other hand, let S^a denote the subgroup of F^R that is generated by $\mathbf{F}_{a,*}$, and S^b denote the subgroup generated by $\mathbf{F}_{b,*}$:

$$S^a = \{(\mathbf{F}_{a,*})^0, (\mathbf{F}_{a,*})^1, \ldots, (\mathbf{F}_{a,*})^{M-1}\} \quad \text{and} \quad S^b = \{(\mathbf{F}_{b,*})^0, (\mathbf{F}_{b,*})^1, \ldots, (\mathbf{F}_{b,*})^{M-1}\}.$$

We have $|S^a| = |S^b| = M$, because $F_{a,b} = \omega_M$. It is clear that $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3) \mapsto \mathbf{u}_1 \circ \mathbf{u}_2 \circ \mathbf{u}_3$ is a group homomorphism from $S^a \oplus S^b \oplus S^{a,b}$ to F^R. We now prove that it is a surjective group isomorphism.

Toward this end, we first note that the matrix $\mathbf{W}$, where

$$\mathbf{W} = \begin{pmatrix} \alpha_a & 1 \\ 1 & \alpha_b \end{pmatrix},$$

is non-degenerate. This follows from Lemma 6.1, since $\det(\mathbf{W}) = \alpha_a\alpha_b - 1$ is odd.

First, we show that $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3) \mapsto \mathbf{u}_1 \circ \mathbf{u}_2 \circ \mathbf{u}_3$ is surjective. This is because for any $\mathbf{u} \in F^R$, there exist integers k_1 and k_2 such that (since $\mathbf{W}$ is non-degenerate, by Lemma 6.1, $\mathbf{x} \mapsto \mathbf{W}\mathbf{x}$ is a bijection)

$$u_a = F_{a,a}^{k_1} \cdot F_{b,a}^{k_2} = \omega_M^{\alpha_a k_1 + k_2} \quad \text{and} \quad u_b = F_{a,b}^{k_1} \cdot F_{b,b}^{k_2} = \omega_M^{k_1 + \alpha_b k_2},$$

and thus, $\mathbf{u} \circ \overline{\mathbf{F}_{a,*}^{k_1}} \circ \overline{\mathbf{F}_{b,*}^{k_2}} \in S^{a,b}$. It then follows that $\mathbf{u} = \mathbf{F}_{a,*}^{k_1} \circ \mathbf{F}_{b,*}^{k_2} \circ \mathbf{u}_3$ for some $\mathbf{u}_3 \in S^{a,b}$.

Second, we show that it is injective. Suppose this is not true. Then there exist $k_1, k_2, k_1', k_2' \in \mathbb{Z}_M$, and $\mathbf{u}, \mathbf{u}' \in S^{a,b}$ such that $(k_1, k_2, \mathbf{u}) \ne (k_1', k_2', \mathbf{u}')$ but

$$(\mathbf{F}_{a,*})^{k_1} \circ (\mathbf{F}_{b,*})^{k_2} \circ \mathbf{u} = (\mathbf{F}_{a,*})^{k_1'} \circ (\mathbf{F}_{b,*})^{k_2'} \circ \mathbf{u}'.$$

If $k_1 = k_1'$ and $k_2 = k_2'$, then $\mathbf{u} = \mathbf{u}'$, which contradicts with our assumption. Therefore, we may assume that $\boldsymbol{\ell} = (\ell_1, \ell_2) = (k_1 - k_1', k_2 - k_2')^T \ne \mathbf{0}$. By restricting on the a^{th} and b^{th} entries, we get $\mathbf{W}\boldsymbol{\ell} = \mathbf{0}$. This contradicts with the fact that $\mathbf{W}$ is non-degenerate.

Now we know that $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3) \mapsto \mathbf{u}_1 \circ \mathbf{u}_2 \circ \mathbf{u}_3$ is a group isomorphism from $S^a \oplus S^b \oplus S^{a,b}$ to F^R. As a result, $|S^{a,b}| = m/M^2$ which we denote by n. Let $S^{a,b} = \{\mathbf{v}_0 = \mathbf{1}, \mathbf{v}_1, \ldots, \mathbf{v}_{n-1}\}$, then there exists a one-to-one correspondence f from $[0 : m-1]$ to $[0 : M-1] \times [0 : M-1] \times [0 : n-1]$, $f(i) = (f_1(i), f_2(i), f_3(i))$, such that

$$\mathbf{F}_{i,*} = (\mathbf{F}_{a,*})^{f_1(i)} \circ (\mathbf{F}_{b,*})^{f_2(i)} \circ \mathbf{v}_{f_3(i)}, \quad \text{for all } i \in [0 : m-1]. \tag{101}$$

Since $\mathbf{F}$ is symmetric, this also implies that

$$\mathbf{F}_{*,j} = (\mathbf{F}_{*,a})^{f_1(j)} \circ (\mathbf{F}_{*,b})^{f_2(j)} \circ \mathbf{v}_{f_3(j)}, \quad \text{for all } j \in [0 : m-1]. \tag{102}$$

Note that $f(a) = (1,0,0)$ and $f(b) = (0,1,0)$.

Finally we permute the rows and columns of $\mathbf{F}$ to obtain a new matrix $\mathbf{G}$. For convenience, we use (x_1, x_2, x_3) and (y_1, y_2, y_3), where $x_1, x_2, y_1, y_2 \in [0 : M-1]$ and $x_3, y_3 \in [0 : n-1]$, to index the rows and columns of $\mathbf{G}$, respectively. We permute $\mathbf{F}$ using $\Pi(x_1, x_2, x_3) = f^{-1}(x_1, x_2, x_3)$:

$$G_{(x_1,x_2,x_3),(y_1,y_2,y_3)} = F_{\Pi(x_1,x_2,x_3),\Pi(y_1,y_2,y_3)}. \tag{103}$$

Then by (101) and (102),

$$\mathbf{G}_{(x_1,x_2,x_3),*} = (\mathbf{G}_{(1,0,0),*})^{x_1} \circ (\mathbf{G}_{(0,1,0),*})^{x_2} \circ \mathbf{G}_{(0,0,x_3),*} \qquad \text{and}$$
$$\mathbf{G}_{*,(y_1,y_2,y_3)} = (\mathbf{G}_{*,(1,0,0)})^{y_1} \circ (\mathbf{G}_{*,(0,1,0)})^{y_2} \circ \mathbf{G}_{*,(0,0,y_3)}.$$

As a result,

$$G_{(x_1,x_2,x_3),(y_1,y_2,y_3)} = (G_{(1,0,0),(y_1,y_2,y_3)})^{x_1} \cdot (G_{(0,1,0),(y_1,y_2,y_3)})^{x_2} \cdot G_{(0,0,x_3),(y_1,y_2,y_3)}.$$

We analyze the three factors. First, we have $G_{(1,0,0),(y_1,y_2,y_3)}$ is equal to

$$(G_{(1,0,0),(1,0,0)})^{y_1} \cdot (G_{(1,0,0),(0,1,0)})^{y_2} \cdot G_{(1,0,0),(0,0,y_3)} = F_{a,a}^{y_1} \cdot F_{a,b}^{y_2} \cdot v_{y_3,a} = \omega_M^{\alpha_a y_1 + y_2},$$

where $v_{y_3,a}$ denotes the a^{th} entry of $\mathbf{v}_{y_3}$. Similarly, $G_{(0,1,0),(y_1,y_2,y_3)} = \omega_M^{y_1+\alpha_b y_2}$. Second,

$$G_{(0,0,x_3),(y_1,y_2,y_3)} = (G_{(0,0,x_3),(1,0,0)})^{y_1} \cdot (G_{(0,0,x_3),(0,1,0)})^{y_2} \cdot G_{(0,0,x_3),(0,0,y_3)}.$$

By (103) and (102) we have

$$G_{(0,0,x),(1,0,0)} = F_{\Pi(0,0,x),\Pi(1,0,0)} = F_{\Pi(0,0,x),a}\,.$$

Then by (101), $F_{\Pi(0,0,x),a} = v_{x,a} = 1$. Similarly, we have $G_{(0,0,x),(0,1,0)} = v_{x,b} = 1$. Therefore,

$$G_{(x_1,x_2,x_3),(y_1,y_2,y_3)} = \omega_M^{\alpha_a x_1 y_1 + x_1 y_2 + x_2 y_1 + \alpha_b x_2 y_2} \cdot G_{(0,0,x_3),(0,0,y_3)}.$$

In other words, we have

$$\mathbf{G} = \boldsymbol{\mathcal{F}}_{M,\mathbf{W}} \otimes \mathbf{F}', \text{ where } \mathbf{W} \text{ is non-degenerate and } \mathbf{F}' \equiv \big(F'_{i,j} = G_{(0,0,i),(0,0,j)}\big) \text{ is symmetric.}$$

The only thing left is to show $\mathbf{F}'$ is discrete unitary and satisfies $(\mathcal{GC})$. $\mathbf{F}'$ satisfies $(\mathcal{GC})$ because $S^{a,b}$ is a group and thus, closed under the Hadamard product. To see $\mathbf{F}'$ is discrete unitary, we have

$$0 = \langle \mathbf{G}_{(0,0,i),*}, \mathbf{G}_{(0,0,j),*} \rangle = M^2 \cdot \langle \mathbf{F}'_{i,*}, \mathbf{F}'_{j,*} \rangle, \quad \text{for any } i \neq j \in [0 : n-1].$$

Since $\mathbf{F}'$ is symmetric, columns $\mathbf{F}'_{*,i}$ and $\mathbf{F}'_{*,j}$ are also orthogonal. □

Theorem 6.4 then follows from Lemma 14.3, Lemma 14.4, and Lemma 14.5.

15 Proofs of Theorem 6.5 and Theorem 6.6

Suppose $((M,N), \mathbf{F}, \mathfrak{D}, (\mathbf{d}, \mathcal{W}, \mathbf{p}, \mathbf{t}, \mathcal{Q}, \mathcal{K}))$ satisfies $(\mathcal{R}')$. We first prove Theorem 6.5: either $\mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ is #P-hard or $\mathfrak{D}$ satisfies conditions $(\mathcal{L}_1')$ and $(\mathcal{L}_2')$.

Suppose $\mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ is not #P-hard. We use $(\mathbf{C}, \mathfrak{E})$ to denote the bipartisation of $(\mathbf{F}, \mathfrak{D})$. The plan is to show that $(\mathbf{C}, \mathfrak{E})$ (together with appropriate $\mathbf{p}', \mathbf{t}'$ and $\mathcal{Q}'$) satisfies condition $(\mathcal{R})$.

To see this is the case we permute $\mathbf{C}$ and $\mathfrak{E}$ using the following permutation Σ. We index the rows (and columns) of $\mathbf{C}$ and $\mathbf{E}^{[r]}$ using $\{0,1\}\times\mathbb{Z}_{\mathbf{d}}^2\times\mathbb{Z}_{\mathcal{Q}}$. We set $\Sigma(1,\mathbf{y})=(1,\mathbf{y})$ for all $\mathbf{y}\in\mathbb{Z}_{\mathbf{d}}^2\times\mathbb{Z}_{\mathcal{Q}}$ (that is, Σ fixes pointwise the second half of the rows and columns), and $\Sigma(0,\mathbf{x})=(0,\mathbf{x}')$, where $\mathbf{x}'$ satisfies

$$x_{0,i,1}=W_{1,1}^{[i]}x'_{0,i,1}+W_{2,1}^{[i]}x'_{0,i,2},\quad x_{0,i,2}=W_{1,2}^{[i]}x'_{0,i,1}+W_{2,2}^{[i]}x'_{0,i,2},\quad \text{for all } i\in[g],$$

and

$$x_{1,i,j}=k_{i,j}\cdot x'_{1,i,j},\quad \text{for all } i\in[s] \text{ and } j\in[t_i].$$

See $(\mathcal{R}')$ for definition of these symbols.

Before proving properties of $\mathbf{C}_{\Sigma,\Sigma}$ and $\mathfrak{E}_\Sigma$, we need to verify that Σ is indeed a permutation. This follows from the fact that $\mathbf{W}^{[i]}$, for every $i\in[g]$, is non-degenerate over $\mathbb{Z}_{d_i}$, and $k_{i,j}$, for all $i\in[s]$ and $j\in[t_i]$, satisfies $\gcd(k_{i,j},q_{i,j})=1$ (so the $\mathbf{x}'$ above is unique). We use Σ_0 to denote the $(0,*)$-part of Σ and I to denote the identity map:

$$\Sigma(0,\mathbf{x})=(0,\Sigma_0(\mathbf{x}))=(0,\mathbf{x}'),\quad \text{for all } \mathbf{x}\in\mathbb{Z}_{\mathbf{d}}^2\times\mathbb{Z}_{\mathcal{Q}}.$$

Now can write $\mathbf{C}_{\Sigma,\Sigma}$ and $\mathfrak{E}_\Sigma=\{\mathbf{E}_\Sigma^{[0]},\ldots,\mathbf{E}_\Sigma^{[N-1]}\}$ as

$$\mathbf{C}_{\Sigma,\Sigma}=\begin{pmatrix}\mathbf{0} & \mathbf{F}_{\Sigma_0,I}\\ \mathbf{F}_{I,\Sigma_0} & \mathbf{0}\end{pmatrix}\quad\text{and}\quad \mathbf{E}_\Sigma^{[r]}=\begin{pmatrix}\mathbf{D}_{\Sigma_0}^{[r]} & \mathbf{0}\\ \mathbf{0} & \mathbf{D}^{[r]}\end{pmatrix},\quad \text{for all } r\in[0:N-1]. \tag{104}$$

We make the following observations:

Observation 1: $\mathsf{EVAL}(\mathbf{C}_{\Sigma,\Sigma},\mathfrak{E}_\Sigma)\equiv\mathsf{EVAL}(\mathbf{C},\mathfrak{E})\le\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$, thus $\mathsf{EVAL}(\mathbf{C}_{\Sigma,\Sigma},\mathfrak{E}_\Sigma)$ is not #P-hard;

Observation 2: $\mathbf{F}_{\Sigma_0,I}$ satisfies (letting $\mathbf{x}'=\Sigma_0(\mathbf{x})$)

$$\begin{aligned}\big(\mathbf{F}_{\Sigma_0,I}\big)_{\mathbf{x},\mathbf{y}}=F_{\Sigma_0(\mathbf{x}),\mathbf{y}}=F_{\mathbf{x}',\mathbf{y}} &= \prod_{i\in[g]}\omega_{d_i}^{(x'_{0,i,1}\ x'_{0,i,2})\cdot\mathbf{W}^{[i]}\cdot(y_{0,i,1}\ y_{0,i,2})^T}\prod_{i\in[s],j\in[t_i]}\omega_{q_{i,j}}^{k_{i,j}\cdot x'_{1,i,j}y_{1,i,j}}\\ &= \prod_{i\in[g]}\omega_{d_i}^{x_{0,i,1}y_{0,i,1}+x_{0,i,2}y_{0,i,2}}\prod_{i\in[s],j\in[t_i]}\omega_{q_{i,j}}^{x_{1,i,j}y_{1,i,j}}.\end{aligned}$$

By Observation 2, it is easy to show that $\mathbf{C}_{\Sigma,\Sigma}$ and $\mathfrak{E}_\Sigma$ (together with appropriate $\mathbf{q}',\mathbf{t}',\mathcal{Q}'$) satisfy condition $(\mathcal{R})$. Since $\mathsf{EVAL}(\mathbf{C}_{\Sigma,\Sigma},\mathfrak{E}_\Sigma)$, by Observation 1, is not #P-hard, it follows from Theorem 5.5 and (104) that $\mathbf{D}^{[r]}$, for all r, satisfy conditions $(\mathcal{L}_2)$ and $(\mathcal{L}_3)$. This proves Theorem 6.5 since $(\mathcal{L}'_1)$ and $(\mathcal{L}'_2)$ follow directly from $(\mathcal{L}_2)$ and $(\mathcal{L}_3)$, respectively.

We continue to prove Theorem 6.6. Suppose $\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$ is not #P-hard, then the argument above shows that $(\mathbf{C}_{\Sigma,\Sigma},\mathfrak{E}_\Sigma)$ (with appropriate $\mathbf{p}',\mathbf{t}',\mathcal{Q}'$) satisfies both $(\mathcal{R})$ and $(\mathcal{L})$. Since by Observation 1, $\mathsf{EVAL}(\mathbf{C}_{\Sigma,\Sigma},\mathfrak{E}_\Sigma)$ is not #P-hard, by Theorem 5.6 and (104), $\mathbf{D}^{[r]}$ satisfies $(\mathcal{D}_2)$ and $(\mathcal{D}_4)$ for all $r\in\mathcal{Z}$.

Condition $(\mathcal{D}'_1)$ follows directly from $(\mathcal{D}_2)$. To prove $(\mathcal{D}'_2)$, we let $\mathbf{F}'$ denote $\mathbf{F}_{\Sigma_0,I}$.

By $(\mathcal{D}_4)$, for any $r\in\mathcal{Z}$, $k\in[s]$ and $\mathbf{a}\in\Gamma_{r,k}^{\text{lin}}$, there exist $\mathbf{b}\in\hat{\mathbb{Z}}_{\mathbf{q}_k}$ and $\alpha\in\mathbb{Z}_N$ such that

$$\omega_N^\alpha\cdot F'_{\widetilde{\mathbf{b}},\mathbf{x}}=D_{\mathbf{x}+\widetilde{\mathbf{a}}}^{[r]}\cdot\overline{D_{\mathbf{x}}^{[r]}},\quad \text{for all } \mathbf{x}\in\Gamma_r,\ \text{where}\quad \mathbf{F}'_{\widetilde{\mathbf{b}},*}=\mathbf{F}_{\Sigma_0(\widetilde{\mathbf{b}}),*}.$$

Also note that Σ_0 works within each prime factor, so there exists a $\mathbf{b}'\in\hat{\mathbb{Z}}_{\mathbf{q}_k}$ such that $\Sigma_0(\widetilde{\mathbf{b}})=\widetilde{\mathbf{b}'}$, and $(\mathcal{D}'_2)$ follows.

16 Tractability: Proof of Theorem 6.7

In this section, we prove Theorem 6.7. The proof is almost the same as the one of Theorem 5.7 for the bipartite case.

Let $((M,N),\mathbf{F},\mathfrak{D},(\mathbf{d},\mathcal{W},\mathbf{p},\mathbf{t},\mathcal{Q},\mathcal{K}))$ be a tuple that satisfies $(\mathcal{R}')$,$(\mathcal{L}')$ and $(\mathcal{D}')$. The proof has the following two steps. In the first step, we use $(\mathcal{R}')$, $(\mathcal{L}')$ and $(\mathcal{D}')$ to decompose the problem $\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$ into a collection of s subproblems (Recall s is the length of the sequence $\mathbf{p}$):

$$\mathsf{EVAL}(\mathbf{F}^{[1]},\mathfrak{D}^{[1]}),\ldots,\mathsf{EVAL}(\mathbf{F}^{[s]},\mathfrak{D}^{[s]}),$$

such that, if every $\mathsf{EVAL}(\mathbf{F}^{[i]},\mathfrak{D}^{[i]})$, $i\in[s]$, is tractable, then $\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$ is also tractable. In the second step, we reduce $\mathsf{EVAL}(\mathbf{F}^{[i]},\mathfrak{D}^{[i]})$, for every $i\in[s]$, to problem $\mathsf{EVAL}(\pi)$ for some prime power π. Recall that $\mathsf{EVAL}(\pi)$ is the following problem: Given a quadratic polynomial $f(x_1,\ldots,x_n)$ over $\mathbb{Z}_\pi$, compute

$$Z_\pi(f)=\sum_{x_1,\ldots,x_n\in\mathbb{Z}_\pi}\omega_\pi^{f(x_1,\ldots,x_n)}.$$

By Theorem 12.1, we have for any prime power π, problem $\mathsf{EVAL}(\pi)$ can be solved in polynomial time. As a result, $\mathsf{EVAL}(\mathbf{F}^{[i]},\mathfrak{D}^{[i]})$ is tractable for all $i\in[s]$, and so is $\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$.

16.1 Step 1

Fix i to be any index in $[s]$. We start by defining $\mathbf{F}^{[i]}$ and $\mathfrak{D}^{[i]}$.

For any $\mathbf{x}\in\hat{\mathbb{Z}}_{\mathbf{q}_i}$, we use $\widetilde{\mathbf{x}}$ to denote the vector $\mathbf{y}\in\mathbb{Z}_{\mathbf{d}}^2\times\mathbb{Z}_{\mathcal{Q}}=\prod_{j=1}^s\hat{\mathbb{Z}}_{\mathbf{q}_j}$ such that

$$\mathbf{y}_i=\mathbf{x}\text{ and }\mathbf{y}_j=\mathbf{0}\text{ for all }j\neq i,\quad\text{where }\mathbf{y}=(\mathbf{y}_1,\ldots,\mathbf{y}_s)\text{ and }\mathbf{y}_j\in\hat{\mathbb{Z}}_{\mathbf{q}_j}.$$

First, we define $\mathbf{F}^{[i]}$. $\mathbf{F}^{[i]}$ is an $m_i\times m_i$ symmetric matrix, where $m_i=|\hat{\mathbb{Z}}_{\mathbf{q}_i}|$. We use $\hat{\mathbb{Z}}_{\mathbf{q}_i}$ to index the rows and columns of $\mathbf{F}^{[i]}$. Then

$$F^{[i]}_{\mathbf{x},\mathbf{y}}=F_{\widetilde{\mathbf{x}},\widetilde{\mathbf{y}}},\quad\text{for all }\mathbf{x},\mathbf{y}\in\hat{\mathbb{Z}}_{\mathbf{q}_i}.$$

By condition $(\mathcal{R}_3')$, it is easy to see that $\mathbf{F},\mathbf{F}^{[1]},\ldots,\mathbf{F}^{[s]}$ satisfy

$$\mathbf{F}=\mathbf{F}^{[1]}\otimes\ldots\otimes\mathbf{F}^{[s]}.\tag{105}$$

Next, we define $\mathfrak{D}^{[i]}$. $\mathfrak{D}^{[i]}=\{\mathbf{D}^{[i,0]},\ldots,\mathbf{D}^{[i,N-1]}\}$ is a sequence of $m_i\times m_i$ diagonal matrices: $\mathbf{D}^{[i,0]}$ is the $m_i\times m_i$ identity matrix; and for every $r\in[N-1]$, the $\mathbf{x}^{th}$ entry, where $\mathbf{x}\in\hat{\mathbb{Z}}_{\mathbf{q}_i}$, of $\mathbf{D}^{[i,r]}$ is

$$D^{[i,r]}_{\mathbf{x}}=D^{[r]}_{\mathbf{ext}_r(\mathbf{x})}.$$

By condition $(\mathcal{D}_1')$, we have

$$\mathbf{D}^{[r]}=\mathbf{D}^{[1,r]}\otimes\ldots\otimes\mathbf{D}^{[s,r]},\quad\text{for all }r\in[0:N-1].\tag{106}$$

It then follows from (105) and (106) that

$$Z_{\mathbf{F},\mathfrak{D}}(G)=Z_{\mathbf{F}^{[1]},\mathfrak{D}^{[1]}}(G)\times\ldots\times Z_{\mathbf{F}^{[s]},\mathfrak{D}^{[s]}}(G),\quad\text{for all undirected graphs }G.$$

As a result, we have the following lemma:

Lemma 16.1. *If $\mathsf{EVAL}(\mathbf{F}^{[i]},\mathfrak{D}^{[i]})$ is tractable for all $i\in[s]$, then $\mathsf{EVAL}(\mathbf{F},\mathfrak{D})$ is also tractable.*

We can use condition $(\mathcal{D}_2')$ to prove the following lemma about the matrix $\mathbf{D}^{[i,r]}$ (recall $\mathcal{Z}$ is the set of $r \in [N-1]$ such that $\mathbf{D}^{[r]} \neq \mathbf{0}$, and $\Gamma_{r,i}$ is a coset in $\hat{\mathbb{Z}}_{\mathbf{q}_i}$ for every $i \in [s]$, such that, $\Gamma_r = \prod_{i\in[s]} \Gamma_{r,i}$):

Lemma 16.2. *Let $r \in \mathcal{Z}$. Then for any $i \in [s]$, $\mathbf{a} \in \Gamma_{r,i}^{\text{lin}}$, there exist $\mathbf{b} \in \hat{\mathbb{Z}}_{\mathbf{q}_i}$ and $\alpha \in \mathbb{Z}_N$ such that*

$$D^{[i,r]}_{\mathbf{x}+\mathbf{a}} \cdot \overline{D^{[i,r]}_{\mathbf{x}}} = \omega_N^{\alpha} \cdot F^{[i]}_{\mathbf{b},\mathbf{x}}, \quad \textit{for all } \mathbf{x} \in \Gamma_{r,i}.$$

Proof. By the definition of $\mathbf{D}^{[i,r]}$, we have

$$D^{[i,r]}_{\mathbf{x}+\mathbf{a}} \cdot \overline{D^{[i,r]}_{\mathbf{x}}} = D^{[r]}_{\mathbf{ext}_r(\mathbf{x}+\mathbf{a})} \cdot \overline{D^{[r]}_{\mathbf{ext}_r(\mathbf{x})}} = D^{[r]}_{\mathbf{ext}_r(\mathbf{x})+\widetilde{\mathbf{a}}} \cdot \overline{D^{[r]}_{\mathbf{ext}_r(\mathbf{x})}}.$$

Then by condition $(\mathcal{D}_2')$, we know there exist $\mathbf{b} \in \hat{\mathbb{Z}}_{\mathbf{q}_i}$ and $\alpha \in \mathbb{Z}_N$ such that

$$D^{[i,r]}_{\mathbf{x}+\mathbf{a}} \cdot \overline{D^{[i,r]}_{\mathbf{x}}} = \omega_N^{\alpha} \cdot F_{\widetilde{\mathbf{b}},\mathbf{ext}_r(\mathbf{x})} = \omega_N^{\alpha} \cdot F^{[i]}_{\mathbf{b},\mathbf{x}}, \quad \text{for all } \mathbf{x} \in \Gamma_{r,i},$$

and the lemma is proven. □

16.2 Step 2

Now we let $\mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ denote one of the subproblems $\mathsf{EVAL}(\mathbf{F}^{[i]}, \mathfrak{D}^{[i]})$ we defined in the last step. By conditions $(\mathcal{R}')$, $(\mathcal{L}')$, $(\mathcal{D}')$ and Lemma 16.2, we summarize the properties of $(\mathbf{F}, \mathfrak{D})$ as follows. We will use these properties to show that $\mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ is tractable.

$(\mathcal{F}_1')$ There exist a prime p and a sequence $\boldsymbol{\pi} = (\pi_1 \geq \pi_2 \geq \ldots \geq \pi_h)$ of powers of p. $\mathbf{F}$ is an $m \times m$ symmetric matrix, where $m = \pi_1\pi_2\ldots\pi_h$. We let π denote π_1 and use $\mathbb{Z}_{\boldsymbol{\pi}} \equiv \mathbb{Z}_{\pi_1} \times \ldots \times \mathbb{Z}_{\pi_h}$ to index the rows and columns of $\mathbf{F}$. We also let $\mathcal{T}$ denote the set of pairs $(i,j) \in [h] \times [h]$ such that $\pi_i = \pi_j$. Then there exist $c_{i,j} \in \mathbb{Z}_{\pi_i} = \mathbb{Z}_{\pi_j}$ for all $(i,j) \in \mathcal{T}$ such that $c_{i,j} = c_{j,i}$ and

$$F_{\mathbf{x},\mathbf{y}} = \prod_{(i,j)\in\mathcal{T}} \omega_{\pi_i}^{c_{i,j}x_iy_j}, \qquad \text{for all } \mathbf{x} = (x_1, \ldots, x_h), \mathbf{y} = (y_1, \ldots, y_h) \in \mathbb{Z}_{\boldsymbol{\pi}},$$

where we use $x_i \in \mathbb{Z}_{\pi_i}$ to denote the i^{th} entry of $\mathbf{x}$ (The reason we express $\mathbf{F}$ in this very general form is to unify the proofs for the two slightly different cases: $(\mathbf{F}^{[1]}, \mathfrak{D}^{[1]})$ and $(\mathbf{F}^{[i]}, \mathfrak{D}^{[i]})$, $i \geq 2$);

$(\mathcal{F}_2')$ $\mathfrak{D} = \{\mathbf{D}^{[0]}, \ldots, \mathbf{D}^{[N-1]}\}$ is a sequence of N $m \times m$ diagonal matrices, for some positive integer N with $\pi \mid N$. $\mathbf{D}^{[0]}$ is the identity matrix; and every diagonal entry of $\mathbf{D}^{[r]}$, $r \in [N-1]$, is either 0 or a power of ω_N. We also use $\mathbb{Z}_{\boldsymbol{\pi}}$ to index the diagonal entries of $\mathbf{D}^{[r]}$;

$(\mathcal{F}_3')$ For every $r \in [0 : N-1]$, we let Γ_r denote the set of $\mathbf{x} \in \mathbb{Z}_{\boldsymbol{\pi}}$ such that $D^{[r]}_{\mathbf{x}} \neq 0$, and let $\mathcal{Z}$ denote the set of r such that $\Gamma_r \neq \emptyset$. For every $r \in \mathcal{Z}$, Γ_r is a coset in $\mathbb{Z}_{\boldsymbol{\pi}}$. Moreover, for every $r \in \mathcal{Z}$, there exists a vector $\mathfrak{a}^{[r]} \in \Gamma_r$ such that $D^{[r]}_{\mathfrak{a}^{[r]}} = 1$;

$(\mathcal{F}_4')$ For all $r \in \mathcal{Z}$ and $\mathbf{a} \in \Gamma_r^{\text{lin}}$, there exist $\mathbf{b} \in \mathbb{Z}_{\boldsymbol{\pi}}$ and $\alpha \in \mathbb{Z}_N$ such that

$$D^{[r]}_{\mathbf{x}+\mathbf{a}} \cdot \overline{D^{[r]}_{\mathbf{x}}} = \omega_N^{\alpha} \cdot F_{\mathbf{b},\mathbf{x}}, \quad \text{for all } \mathbf{x} \in \Gamma_r.$$

Now let G be an undirected graph. Below we will reduce the computation of $Z_{\mathbf{F},\mathfrak{D}}(G)$ to $\mathsf{EVAL}(\widehat{\pi})$,

$$\text{where } \widehat{\pi} = \pi \text{ if } p \neq 2, \ \text{ and } \widehat{\pi} = 2\pi \text{ if } p = 2.$$

Given $a \in \mathbb{Z}_{\pi_i}$ for some $i \in [h]$, we use $\widehat{a}$ to denote an element in $\mathbb{Z}_{\widehat{\pi}}$ such that $\widehat{a} \equiv a \pmod{\pi_i}$. For definiteness we can choose a itself if we consider a to be an integer between 0 and $\pi_i - 1$.

Let $G = (V, E)$. We let V_r, $r \in [0 : N-1]$, denote the set of vertices in V whose degree is r mod N. We further decompose E into $\cup_{i \le j \in [0:N-1]} E_{i,j}$, where $E_{i,j}$ contains the edges between V_i and V_j.

It is clear that if $V_r \neq \emptyset$ for some $r \notin \mathcal{Z}$, then $Z_{\mathbf{F},\mathfrak{D}}(G)$ is trivially 0. As a result, we assume $V_r = \emptyset$ for all $r \notin \mathcal{Z}$. In this case, we have

$$Z_{\mathbf{F},\mathfrak{D}}(G) = \sum_{\xi} \left[\prod_{r \in \mathcal{Z}} \left(\prod_{v \in V_r} D^{[r]}_{\mathbf{x}_v} \right) \right] \left[\prod_{r \le r' \in \mathcal{Z}} \left(\prod_{uv \in E_{r,r'}} F_{\mathbf{x}_u, \mathbf{x}_v} \right) \right],$$

where the sum ranges over all assignments $\xi = (\xi_r : V_r \to \Gamma_r \mid r \in \mathcal{Z})$ such that $\xi(v) = \mathbf{x}_v$.

Next by using Lemma 12.3, we know for every $r \in \mathcal{Z}$, there exist a positive integer s_r and an $s_r \times h$ matrix $\mathbf{A}^{[r]}$ over $\mathbb{Z}_{\widehat{\pi}}$ which gives us a *uniform* map $\gamma^{[r]}$ (see Lemma 12.3 for definition) from $\mathbb{Z}_{\widehat{\pi}}^{s_r}$ to Γ_r:

$$\gamma_i^{[r]}(\mathbf{x}) = \left(\mathbf{x} \mathbf{A}^{[r]}_{*,i} + \widehat{\mathfrak{a}}^{[r]}_i \pmod{\pi_i} \right), \quad \text{for all } i \in [h].$$

Recall that for every $r \in \mathcal{Z}$, $\mathfrak{a}^{[r]}$ is a vector in Γ_r such that $D^{[r]}_{\mathfrak{a}^{[r]}} = 1$. Thus, $D^{[r]}_{\gamma^{[r]}(\mathbf{0})} = 1$. Because $\gamma^{[r]}$ is uniform, to compute $Z_{\mathbf{F},\mathfrak{D}}(G)$, it suffices to compute

$$\sum_{(\mathbf{x}_v)} \left[\prod_{r \in \mathcal{Z}} \left(\prod_{v \in V_r} D^{[r]}_{\gamma^{[r]}(\mathbf{x}_v)} \right) \right] \left[\prod_{r \le r' \in \mathcal{Z}} \left(\prod_{uv \in E_{r,r'}} F_{\gamma^{[r]}(\mathbf{x}_u), \gamma^{[r']}(\mathbf{x}_v)} \right) \right],$$

where the sum is over

$$\left(\mathbf{x}_v \in \mathbb{Z}_{\widehat{\pi}}^{s_r} : v \in V_r, r \in \mathcal{Z} \right) = \prod_{r \in \mathcal{Z}} (\mathbb{Z}_{\widehat{\pi}}^{s_r})^{|V_r|}.$$

If we can show for every $r \in \mathcal{Z}$, there is a quadratic polynomial $f^{[r]}$ over $\mathbb{Z}_{\widehat{\pi}}$, such that,

$$D^{[r]}_{\gamma^{[r]}(\mathbf{x})} = \omega_{\widehat{\pi}}^{f^{[r]}(\mathbf{x})}, \quad \text{for all } \mathbf{x} \in \mathbb{Z}_{\widehat{\pi}}^{s_r}, \tag{107}$$

and for all $r \le r' \in \mathcal{Z}$, there is a quadratic polynomial $f^{[r,r']}$ over $\mathbb{Z}_{\widehat{\pi}}$, such that,

$$F_{\gamma^{[r]}(\mathbf{x}), \gamma^{[r']}(\mathbf{y})} = \omega_{\widehat{\pi}}^{f^{[r,r']}(\mathbf{x},\mathbf{y})}, \quad \text{for all } \mathbf{x} \in \mathbb{Z}_{\widehat{\pi}}^{s_r} \text{ and } \mathbf{y} \in \mathbb{Z}_{\widehat{\pi}}^{s_{r'}}, \tag{108}$$

then we can reduce the computation of $Z_{\mathbf{F},\mathfrak{D}}(G)$ to $\mathsf{EVAL}(\widehat{\pi})$ and finish the proof.

First, we prove the existence of the quadratic polynomial $f^{[r,r']}$. By condition $(\mathcal{F}_1')$, the following function $f^{[r,r']}$ satisfies (108):

$$f^{[r,r']}(\mathbf{x},\mathbf{y}) = \sum_{(i,j) \in \mathcal{T}} \left(\frac{\widehat{\pi}}{\pi_i} \right) \cdot c_{i,j} \cdot \gamma_i^{[r]}(\mathbf{x}) \cdot \gamma_j^{[r']}(\mathbf{y}) = \sum_{(i,j) \in \mathcal{T}} \widehat{c}_{i,j} \left(\frac{\widehat{\pi}}{\pi_i} \right) \left(\mathbf{x} \mathbf{A}^{[r]}_{*,i} + \widehat{\mathfrak{a}}^{[r]}_i \right) \left(\mathbf{y} \mathbf{A}^{[r']}_{*,j} + \widehat{\mathfrak{a}}^{[r']}_j \right).$$

Note that $(i,j) \in \mathcal{T}$ implies that $\pi_i = \pi_j$ and thus,

$$\gamma_i^{[r]}(\mathbf{x}),\ \gamma_j^{[r']}(\mathbf{y}) \in \mathbb{Z}_{\pi_i} = \mathbb{Z}_{\pi_j}.$$

The presence of $\widehat{\pi}/\pi_i$ is crucial to be able to substitute the $\bmod \pi_i$ expressions for $\gamma_i^{[r]}(\mathbf{x})$ and $\gamma_j^{[r']}(\mathbf{y})$, as if they were $\bmod \widehat{\pi}$ expressions. It is clear that $f^{[r,r']}$ is a quadratic polynomial over $\mathbb{Z}_{\widehat{\pi}}$.

Next we prove the existence of the quadratic polynomial $f^{[r]}$. Let us fix r to be an index in $\mathcal{Z}$. We use $\mathbf{e}_i$, $i \in [s_r]$, to denote the vector in $\mathbb{Z}_{\widehat{\pi}}^{s_r}$ whose i^{th} entry is 1 and all other entries are 0. By $(\mathcal{F}_4')$, we know for every $i \in [s_r]$, there exist $\alpha_i \in \mathbb{Z}_N$ and $\mathbf{b}_i = (b_{i,1}, ..., b_{i,h}) \in \mathbb{Z}_{\boldsymbol{\pi}}$, where $b_{i,j} \in \mathbb{Z}_{\pi_j}$, such that

$$D^{[r]}_{\gamma^{[r]}(\mathbf{x}+\mathbf{e}_i)} \cdot \overline{D^{[r]}_{\gamma^{[r]}(\mathbf{x})}} = \omega_N^{\alpha_i} \cdot \prod_{j\in[h]} \omega_{\pi_j}^{b_{i,j}\cdot\gamma_j^{[r]}(\mathbf{x})}, \quad \text{for all } \mathbf{x} \in \mathbb{Z}_{\widehat{\pi}}^{s_r}.$$

We have this equation because $\gamma^{[r]}(\mathbf{x}+\mathbf{e}_i) - \gamma^{[r]}(\mathbf{x})$ is a vector in $\mathbb{Z}_{\boldsymbol{\pi}}$ that is independent of $\mathbf{x}$.

By the same argument we used in the proof of Theorem 5.7 ((90) and (91), more exactly), one can show that $\omega_N^{\alpha_i}$ must be a power of $\omega_{\widehat{\pi}}$, for all $i \in [s_r]$. As a result, there exists $\beta_i \in \mathbb{Z}_{\widehat{\pi}}$ such that

$$D^{[r]}_{\gamma^{[r]}(\mathbf{x}+\mathbf{e}_i)} \cdot \overline{D^{[r]}_{\gamma^{[r]}(\mathbf{x})}} = \omega_{\widehat{\pi}}^{\beta_i} \cdot \prod_{j\in[h]} \omega_{\pi_j}^{b_{i,j}\cdot\gamma_j^{[r]}(\mathbf{x})}, \quad \text{for all } \mathbf{x} \in \mathbb{Z}_{\widehat{\pi}}^{s_r}. \tag{109}$$

Again, by the argument we used in the proof of Theorem 5.7, every non-zero entry of $\mathbf{D}^{[r]}$ must be a power of $\omega_{\widehat{\pi}}$. Therefore, there does exist a function $f^{[r]}$ from $\mathbb{Z}_{\widehat{\pi}}^{s_r}$ to $\mathbb{Z}_{\widehat{\pi}}$ that satisfies (107). To see $f^{[r]}$ is a quadratic polynomial, by (109), we have for every $i \in [s_r]$,

$$f^{[r]}(\mathbf{x}+\mathbf{e}_i) - f^{[r]}(\mathbf{x}) = \beta_i + \sum_{j\in[h]} \left(\widehat{b}_{i,j} \cdot \left(\frac{\widehat{\pi}}{\pi_j}\right) \left(\mathbf{x}\mathbf{A}^{[r]}_{*,j} + \widehat{\mathfrak{a}}_j^{[r]}\right)\right), \quad \text{for all } i \in [s_r] \text{ and } \mathbf{x} \in \mathbb{Z}_{\widehat{\pi}}^{s_r},$$

which is an affine linear form of $\mathbf{x}$ with all coefficients from $\mathbb{Z}_{\widehat{\pi}}$.

By using Lemma 12.4 and Lemma 12.5, we can prove that $f^{[r]}$ is a quadratic polynomial over $\mathbb{Z}_{\widehat{\pi}}$, and this finishes the reduction from $\mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ to $\mathsf{EVAL}(\widehat{\pi})$.

References

[1] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation*. Springer-Verlag New York, 1998.

[2] A. Bulatov and M. Grohe. The complexity of partition functions. *Theoretical Computer Science*, 348(2):148–186, 2005.

[3] J.-Y. Cai, P. Lu, and M. Xia. Holant problems and counting CSP. In *Proceedings of the 41st ACM Symposium on Theory of Computing*, to appear.

[4] N. Creignou, S. Khanna, and M. Sudan. *Complexity classifications of boolean constraint satisfaction problems*. SIAM Monographs on Discrete Mathematics and Applications, 2001.

[5] M.E. Dyer, L.A. Goldberg, and M. Paterson. On counting homomorphisms to directed acyclic graphs. *Journal of the ACM*, 54(6): Article 27, 2007.

[6] M.E. Dyer and C. Greenhill. The complexity of counting graph homomorphisms. In *Proceedings of the 9th International Conference on Random Structures and Algorithms*, pages 260–289, 2000.

[7] T. Feder and M. Vardi. The computational structure of monotone monadic SNP and constraint satisfaction: A study through Datalog and group theory. *SIAM Journal on Computing*, 28(1):57–104, 1999.

[8] R. Feynman, R. Leighton, and M. Sands. *The Feynman Lectures on Physics*. Addison-Wesley, 1970.

[9] M. Freedman, L. Lovász, and A. Schrijver. Reflection positivity, rank connectivity, and homomorphism of graphs. *Journal of the American Mathematical Society*, 20:37–51, 2007.

[10] L. A. Goldberg, M. Grohe, M. Jerrum, and M. Thurley. A complexity dichotomy for partition functions with mixed signs. In *Proceedings of the 26th International Symposium on Theoretical Aspects of Computer Science*, pages 493–504, 2009.

[11] P. Hell and J. Nešetřil. On the complexity of H-coloring. *Journal of Combinatorial Theory, Series B*, 48(1):92–110, 1990.

[12] P. Hell and J. Nešetřil. *Graphs and Homomorphisms*. Oxford University Press, 2004.

[13] K. Ko. *Complexity Theory of Real Functions*. Birkhauser Boston, 1991.

[14] S. Lang. *Algebra*. Springer-Verlag, 3rd edition, 2002.

[15] R. Lidl and H. Niederreiter. *Finite fields*. volume 20 of Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, 1997.

[16] L. Lovász. Operations with structures. *Acta Mathematica Hungarica*, 18:321–328, 1967.

[17] L. Lovász. The rank of connection matrices and the dimension of graph algebras. *European Journal of Combinatorics*, 27(6):962–970, 2006.

[18] T. J. Schaefer. The complexity of satisfiability problems. In *Proceedings of the tenth annual ACM symposium on Theory of computing*, pages 216–226, 1978.

[19] L. G. Valiant. Holographic algorithms (extended abstract). In *Proceedings of the 45th annual IEEE Symposium on Foundations of Computer Science*, pages 306–315, 2004.

[20] L. G. Valiant. Accidental algorthims. In *Proceedings of the 47th annual IEEE Symposium on Foundations of Computer Science*, pages 509–517, 2006.