SIAM J. COMPUT.
Vol. 42, No. 3, pp. 924–1029

GRAPH HOMOMORPHISMS WITH COMPLEX VALUES: A DICHOTOMY THEOREM*

JIN-YI CAI†, XI CHEN‡, AND PINYAN LU§

Abstract. Each symmetric matrix $\mathbf{A}$ over $\mathbb{C}$ defines a graph homomorphism function $Z_{\mathbf{A}}(\cdot)$ on undirected graphs. The function $Z_{\mathbf{A}}(\cdot)$ is also called the partition function from statistical physics, and can encode many interesting graph properties, including counting vertex covers and k-colorings. We study the computational complexity of $Z_{\mathbf{A}}(\cdot)$ for arbitrary symmetric matrices $\mathbf{A}$ with algebraic complex values. Building on work by Dyer and Greenhill [*Random Structures and Algorithms*, 17 (2000), pp. 260–289], Bulatov and Grohe [*Theoretical Computer Science*, 348 (2005), pp. 148–186], and especially the recent beautiful work by Goldberg et al. [*SIAM J. Comput.*, 39 (2010), pp. 3336–3402], we prove a complete dichotomy theorem for this problem. We show that $Z_{\mathbf{A}}(\cdot)$ is either computable in polynomial-time or #P-hard, depending explicitly on the matrix $\mathbf{A}$. We further prove that the tractability criterion on $\mathbf{A}$ is polynomial-time decidable.

Key words. computational complexity, counting complexity, graph homomorphisms, partition functions

AMS subject classifications. 68Q17, 68Q25, 68R05, 68R10, 05C31

DOI. 10.1137/110840194

1. Introduction.

Graph homomorphism has been studied intensely over the years [28, 23, 13, 18, 4, 12, 21]. Given two graphs G and H, a graph homomorphism from G to H is a map f from the vertex set $V(G)$ 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 [28] 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. Graph homomorphisms and the associated partition function defined below provide us an elegant and wide-ranging notion of *graph properties* [23].

In this paper, all graphs considered are undirected. We follow standard definitions: G is allowed to have multiple edges; H can have loops, multiple edges, and, more generally, edge weights. (The standard definition of graph homomorphism does not allow self-loops for G. However, our result is stronger: We prove polynomial-time tractability even for input graphs G with self-loops; at the same time, our hardness results hold for the more restricted case of G with no self-loops.) Formally, we use $\mathbf{A}$ to denote an $m \times m$ symmetric matrix with entries $(A_{i,j})$, $i, j \in [m] = \{1, 2, \ldots, m\}$. Given any undirected graph $G = (V, E)$, we define the graph homomorphism function

*Received by the editors July 11, 2011; accepted for publication (in revised form) February 21, 2013; published electronically May 21, 2013.
http://www.siam.org/journals/sicomp/42-3/84019.html
†Department of Computer Sciences, University of Wisconsin–Madison, Madison, WI 53706 (jyc@cs.wisc.edu). This work was supported by NSF CCF-0914969.
‡Department of Computer Science, Columbia University, New York, NY 10027 (xichen@cs.columbia.edu). This work was supported by NSF grants CCF-0832797 and DMS-0635607 when the author was a postdoc at the Institute for Advanced Study and Princeton University, by a USC Viterbi School of Engineering startup fund to Shang-Hua Teng, and by CCF-1149257 and a Sloan research fellowship.
§Microsoft Research Asia, Beijing 100080, China (pinyanl@microsoft.com).

$$Z_{\mathbf{A}}(G) = \sum_{\xi: V \to [m]} \prod_{(u,v) \in E} A_{\xi(u),\xi(v)}. \tag{1.1}$$

This is also called the *partition function* from statistical physics. It is clear from the definition that $Z_{\mathbf{A}}(G)$ is exactly the number of homomorphisms from G to H, when $\mathbf{A}$ is the adjacency matrix of H.

Graph homomorphism can express many natural graph properties. For example, if we take H to be the graph over two vertices $\{0,1\}$ with an edge $(0,1)$ and a loop at 1, then the set of vertices mapped to 1 in 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 over 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

$$\mathbf{H} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{1.2}$$

We index its rows and columns by $\{0,1\}$. In the sum $Z_{\mathbf{H}}(G)$, each term is either 1 or -1 and equals -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 of G with an odd number of edges. Also expressible as $Z_{\mathbf{A}}(\cdot)$ are S-flows, where S is a subset of a finite Abelian group closed under inversion [18], and a scaled version of the Tutte polynomial $\hat{T}(x,y)$, where $(x-1)(y-1)$ is a positive integer. In [18], Freedman, Lovász and Schrijver characterized the graph functions that can be expressed as $Z_{\mathbf{A}}(\cdot)$.

In this paper, we study the complexity of the partition function $Z_{\mathbf{A}}(\cdot)$, where $\mathbf{A}$ is an *arbitrary fixed symmetric matrix over the algebraic complex numbers*. Throughout the paper, we let $\mathbb{C}$ denote the set of algebraic complex numbers and refer to them simply as complex numbers when it is clear from the context. More discussion on the model of computation can be found in section 2.2.

The complexity question of $Z_{\mathbf{A}}(\cdot)$ has been intensely studied. Hell and Nešetřil first studied the H-coloring problem [22, 23] (i.e., given an undirected graph G, decide whether there exists a graph homomorphism from G to H) and proved that for any fixed undirected graph H, the problem is either in polynomial time or NP-complete. Results of this type are called *complexity dichotomy theorems*. Such theorems state that every member of the class of problems concerned is either tractable (i.e., solvable in P) or intractable (i.e., NP-hard or #P-hard depending on whether it is a decision or a counting problem). This includes the well-known Schaefer's dichotomy theorem [31]. The famous complexity dichotomy conjecture made by Feder and Vardi [16] on decision constraint satisfaction problems [11] motivated much of the subsequent work.

In [13], Dyer and Greenhill studied the counting version of the H-coloring problem. They proved that for any fixed symmetric $\{0,1\}$-matrix $\mathbf{A}$, $Z_{\mathbf{A}}(\cdot)$ is either computable in polynomial time or #P-hard. (In this paper, for a function computable in polynomial time we will simply say "in P.") Then in [4], Bulatov and Grohe gave a sweeping generalization of this theorem to all nonnegative symmetric matrices $\mathbf{A}$. (See Theorem 2.5 for the precise statement.) They obtained an elegant dichotomy theorem, which basically says that $Z_{\mathbf{A}}(\cdot)$ is computable in P if each *block* of $\mathbf{A}$ has rank at most one, and 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, $Z_{\mathbf{A}}(\cdot)$ is computable in P if every $Z_{\mathbf{A}_i}(\cdot)$ is and is #P-hard otherwise. For each nonbipartite graph H_i, the corresponding $Z_{\mathbf{A}_i}(\cdot)$

is computable in P if $\mathbf{A}_i$ has rank at most one and is #P-hard otherwise. For each bipartite H_i, the corresponding $Z_{\mathbf{A}_i}(\cdot)$ is in P if $\mathbf{A}_i$ has the form

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

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

The result of Bulatov and Grohe is both sweeping and enormously applicable. It completely solves the problem for all nonnegative symmetric matrices. However, when we are dealing with nonnegative matrices, there are no cancellations in the exponential sum $Z_{\mathbf{A}}(\cdot)$. These potential cancellations, when $\mathbf{A}$ is either a real or a complex matrix, may in fact be the source of surprisingly efficient algorithms for computing $Z_{\mathbf{A}}(\cdot)$. The occurrence of these cancellations, or the mere possibility of such occurrence, makes proving any complexity dichotomies more difficult. Such a proof must identify all polynomial-time decidable problems utilizing the potential cancellations, such as those found in holographic algorithms [36, 37, 8], and at the same time carve out exactly what is left. This situation is similar to *monotone* versus *nonmonotone* circuit complexity. It turns out that indeed there are more interesting tractable cases over the reals, and in particular, the 2×2 Hadamard matrix $\mathbf{H}$ in (1.2) turns out to be one such case. This is the starting point for the next great chapter on the complexity of $Z_{\mathbf{A}}(\cdot)$.

In a paper [21] comprising 67 pages of beautiful proofs of both exceptional depth and conceptual vision, Goldberg et al. proved a complexity dichotomy theorem for algebraic real-valued symmetric matrices $\mathbf{A}$. Their result is too intricate to give a short and accurate summary here. It states that the problem of computing $Z_{\mathbf{A}}(G)$ for any algebraic real $\mathbf{A}$ is either in P or #P-hard. Which case it is depends on the connected components of $\mathbf{A}$. The overall statement remains that $Z_{\mathbf{A}}(G)$ is tractable 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 $\mathbf{H} \otimes \cdots \otimes \mathbf{H}$ 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 nonbipartite 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 two matrices, and their arbitrary tensor products, all correspond to new tractable $Z_{\mathbf{A}}(\cdot)$. 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 [21] 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

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

where f_G is a quadratic polynomial over $\mathbb{Z}_2$. This sum is known to be computable in polynomial time in n [10] [27, Theorem 6.30], 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 viewpoint of [21].

While positive and negative real numbers provide the possibility of cancellations, there is a significantly richer variety of possible cancellations over the complex domain. We independently came to the tractability of $Z_{\mathbf{H}}(\cdot)$, with $\mathbf{H}$ being the 2×2

Hadamard matrix, from a slightly different angle. In [9], the authors studied a certain type of constraint satisfaction problem. 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 [35, 36]. Let us briefly describe this framework. A *signature grid* $\Omega = (G, \mathcal{F})$ is a tuple in which $G = (V, E)$ 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 set of incident edges of v. The counting problem on an input instance Ω is to compute

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

For example, if we take $\sigma\colon E \to \{0, 1\}$ and attach the exact-one function at every vertex $v \in V$, then Holant(Ω) is the number of perfect matchings of G. Incidentally, Freedman, Lovász, and Schrijver showed [18] that counting perfect matchings *cannot* be expressed as $Z_{\mathbf{A}}(\cdot)$ for any matrix $\mathbf{A}$ over $\mathbb{R}$. However, every function $Z_{\mathbf{A}}(\cdot)$ (vertex assignment) *can* be simulated by Holant$(\cdot)$ (edge assignment) as follows: $\mathbf{A}$ defines a function of arity 2 for every edge of G. Consider the bipartite vertex-edge incidence graph $G' = (V(G), E(G), E')$ of G, where $(v, e) \in E'$ if e is incident to v in G. Then attach the equality function at every $v \in V(G)$ and the function defined by $\mathbf{A}$ at every $e \in E(G)$. This defines a signature grid Ω with the underlying graph G'. Then $Z_{\mathbf{A}}(G) = \text{Holant}(\Omega)$.

Denote a symmetric function on n boolean variables by $[f_0, f_1, \ldots, f_n]$, where f_j is the value on inputs of Hamming weight j. For example, the exact-one function is $[0, 1, 0, \ldots, 0]$ and $\mathbf{H}$ is just $[1, 1, -1]$. The authors of [9] discovered that the three families of functions (listing the values of a function lexicographically as in a truth table on k boolean variables)

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

all give rise to tractable problems: Holant(Ω) for any $\Omega = (G, \mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3)$ can be solved in P. In particular, by taking $r = 1$, $k = 2$, and $\lambda = (1 + i)^{-1}$ in $\mathcal{F}_3$, we recover the binary function $[1, 1, -1]$ that corresponds to the Hadamard matrix $\mathbf{H}$ in (1.2). 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 $Z_{\mathbf{H}}(\cdot)$, as a special case, can be computed in P.

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

$$\sum_{x_1, x_2, \ldots, x_n \in \{0,1\}} i^{L_1 + L_2 + \cdots + L_s}, \tag{1.3}$$

where each L_j is an indicator function of an affine form of $x_1, x_2, \ldots, x_n$ over $\mathbb{Z}_2$ (and thus, the exponent of i in the equation above is a mod 4 sum of mod 2 sums). From here it is only natural to investigate the complexity of $Z_{\mathbf{A}}(\cdot)$ for symmetric complex

matrices, since it not only is a natural generalization but also can reveal the inner unity and some deeper structural properties. Interested readers can find more details in [9]. Also see Remark 12.10 at the end of section 12.

Our investigation of complex-valued graph homomorphisms is also motivated by the partition function in quantum physics. In classical statistical physics, the partition function is always real-valued. But in a generic quantum system, for which complex numbers are the right language, the partition function is in general complex-valued [17]. In particular, if the physics model is over a discrete graph and is nonorientable, then the edge weights are given by a symmetric complex matrix.

Our main result is the following complexity dichotomy theorem, though its criterion is too complicated to explain here.

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

Furthermore, under the model of computation described in section 2.2, we show that the following decision problem is solvable in polynomial time.

THEOREM 1.2 (polynomial-time decidability). *Given a symmetric and algebraic complex matrix* $\mathbf{A}$*, there is a polynomial-time algorithm that decides whether* $Z_{\mathbf{A}}(\cdot)$ *is in polynomial time or is #P-hard.*

Recent developments. In [34], Thurley announced a dichotomy theorem[1] for $Z_{\mathbf{A}}(\cdot)$, where $\mathbf{A}$ is a complex Hermitian matrix. The tractability result of the present paper (in section 12) was used in [34]. Cai and Chen proved a dichotomy theorem for $Z_{\mathbf{A}}(\cdot)$ for directed graph homomorphisms, where $\mathbf{A}$ is a nonnegative but not necessarily symmetric matrix [5]. A dichotomy theorem is also proved for the more general counting constraint satisfaction problem when the constraint functions take values in $\{0, 1\}$ [1, 2] (with an alternative proof given in [14] that also shows the decidability of the dichotomy criterion), when the functions take nonnegative and rational values [3], and when they are nonnegative and algebraic [7]. Finally, built on the methods and results of [1, 14, 21] and the present paper, Cai and Chen proved a dichotomy theorem for all algebraic complex-valued counting constraint satisfaction problems [6].

Organization. Due to the complexity of the proof of Theorem 1.1, both in terms of its overall structure and in terms of technical difficulty, we first give a high-level description of the proof for the bipartite case in section 3. We prove the first and second pinning lemmas in section 4. A more detailed outline of the proof for the two cases, bipartite and nonbipartite, is presented in sections 5 and 6, respectively, with formal definitions and theorems. We then prove all the lemmas and theorems used in sections 5 and 6, as well as Theorem 1.2, in the rest of the paper. An index of conditions and problem definitions is given in Figure 1.1.

2. Preliminaries. In the paper, we let $\mathbb{Q}$ denote the set of rational numbers and let $\mathbb{R}$ and $\mathbb{C}$ denote the set of algebraic real and algebraic complex numbers, respectively, for convenience (even though many of the supporting lemmas and theorems actually hold for general real or complex numbers, especially when computation or polynomial-time reduction is not concerned in the statement).

2.1. Notation. For a positive integer n, we use $[n]$ to denote the set $\{1, \ldots, n\}$ (when $n = 0$, $[0] = \emptyset$). We use $[m : n]$, where $m \leq n$, to denote $\{m, m+1, \ldots, n\}$. We

[1] However, the following is a counter example to Claim 3 on p. 50 of [34]: $D_{11}^{[c];1} = D_{22}^{[c];1} = 1$, $D_{11}^{[c];2} = i$ (the imaginary unit), and $D_{22}^{[c];2} = -i$. We believe that this minor deficiency in the proof probably can be overcome using the techniques in this paper, in particular those from section 8.4.

FIG. 1.1. *Index of conditions and problem definitions.*

use $\mathbf{1}_n$ to denote the all-one vector of dimension n. Sometimes we omit n when the dimension is clear from the context. For a positive integer N, we let $\omega_N = e^{2\pi i/N}$, a primitive Nth root of unity.

Let $\mathbf{x}, \mathbf{y}$ be two vectors in $\mathbb{C}^n$. Then we use $\langle \mathbf{x}, \mathbf{y} \rangle$ to denote their inner product,

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{n} x_i \cdot \overline{y_i},$$

and $\mathbf{x} \circ \mathbf{y} \in \mathbb{C}^n$ to denote their Hadamard product, $(\mathbf{x} \circ \mathbf{y})_i = x_i \cdot y_i$ 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 their tensor product: $\mathbf{C}$ is a $km \times \ell n$ matrix whose rows and columns are indexed by $[k] \times [m]$ and $[\ell] \times [n]$, respectively, such that

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

Given an $n \times n$ symmetric complex matrix $\mathbf{A}$, we use $G = (V, E)$ to denote the following undirected graph: $V = [n]$ and $ij \in E$ iff $A_{i,j} \neq 0$. 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 $|V_i| \times |V_i|$ submatrix of $\mathbf{A}$ restricted by $V_i \subseteq [n]$ for all $i \in [s]$. Moreover, we say $\mathbf{A}$ is *bipartite* if G is bipartite; otherwise, $\mathbf{A}$ is *nonbipartite*. Let Σ and Π be two permutations of $[n]$. Then we use $\mathbf{A}_{\Sigma,\Pi}$ to denote the $n \times n$ matrix whose (i,j)th entry is $A_{\Sigma(i),\Pi(j)}$, $i, j \in [n]$.

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

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

We usually use D_i to denote the (i,i)th entry of a diagonal matrix $\mathbf{D}$.

We say a problem is tractable if it can be solved in polynomial time. Given two problems $\mathcal{P}$ and $\mathcal{Q}$, we say $\mathcal{P}$ is polynomial-time reducible to $\mathcal{Q}$, or $\mathcal{P} \leq \mathcal{Q}$, if there is a polynomial-time algorithm that solves $\mathcal{P}$ using an oracle for $\mathcal{Q}$. These reductions are known as Cook reductions. We also say $\mathcal{P}$ is polynomial-time equivalent to $\mathcal{Q}$, or $\mathcal{P} \equiv \mathcal{Q}$, if $\mathcal{P} \leq \mathcal{Q}$ and $\mathcal{Q} \leq \mathcal{P}$.

2.2. Model of computation.[2] One technical issue is the *model of computation* with algebraic numbers. We adopt a standard model from [26] for computation in an algebraic number field. We start with some notation.

Let $\mathbf{A}$ be a fixed symmetric matrix where every entry $A_{i,j}$ is an algebraic number. We let $\mathscr{A}$ denote the finite set of algebraic numbers consisting of entries $A_{i,j}$ of $\mathbf{A}$. Then it is easy to see that $Z_{\mathbf{A}}(G)$, for any undirected graph G, is a number in $\mathbb{Q}(\mathscr{A})$, the algebraic extension of $\mathbb{Q}$ by $\mathscr{A}$. By the primitive element theorem [30], there exists an algebraic number $\alpha \in \mathbb{Q}(\mathscr{A})$ such that $\mathbb{Q}(\mathscr{A}) = \mathbb{Q}(\alpha)$. (Essentially, $\mathbb{Q}$ has characteristic 0, and therefore the field extension $\mathbb{Q}(\mathscr{A})$ is separable. We can take the normal closure of $\mathbb{Q}(\mathscr{A})$, which is a finite-dimensional separable and normal extension of $\mathbb{Q}$, and thus Galois [24]. By Galois correspondence, there are only a finite number of intermediate fields between $\mathbb{Q}$ and this Galois extension field and thus a fortiori only a finite number of intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\mathscr{A})$. Then Artin's theorem on primitive elements implies that $\mathbb{Q}(\mathscr{A})$ is a simple extension $\mathbb{Q}(\alpha)$.) In the proof of Theorem 1.1 when the complexity of a partition function $Z_{\mathbf{A}}(\cdot)$ is concerned, the matrix $\mathbf{A}$ is considered fixed. Thus, we may assume we are given, as part of the problem description, such a number α, encoded by a minimal polynomial $F(x) \in \mathbb{Q}[x]$ of α. In addition to F, we are given a sufficiently good rational approximation $\widehat{\alpha}$ of α which uniquely determines α as a root of $F(x)$.[3]

Let $d = \deg(F)$. Then every number c in $\mathbb{Q}(\mathscr{A})$, including the $A_{i,j}$'s and $Z_{\mathbf{A}}(G)$ for any G, has a unique representation as a polynomial of α:

$$c_0 + c_1 \cdot \alpha + \cdots + c_{d-1} \cdot \alpha^{d-1}, \qquad \text{where every } c_i \text{ is a rational number.}$$

We will refer to this polynomial as the *standard representation* of c. Given a number $c \in \mathbb{Q}(\mathscr{A})$ in the standard representation, its input size is the sum of the binary lengths of all the rational coefficients. It is easy to see that all the field operations over $\mathbb{Q}(\mathscr{A})$ in this representation can be computed in polynomial time in the input size.

We emphasize that when the complexity of $Z_{\mathbf{A}}(\cdot)$ is concerned in the proof of Theorem 1.1, all the following are considered as constants since they are part of the problem description and not part of the input: the size of $\mathbf{A}$, the minimal polynomial $F(x)$ of α, the approximation $\widehat{\alpha}$ of α, as well as the entries $A_{i,j}$ of $\mathbf{A}$ encoded in the standard representation. Given an undirected graph G, the problem is then to output $Z_{\mathbf{A}}(G) \in \mathbb{Q}(\mathscr{A})$ encoded in the standard representation. We remark that the same model applies to the problem of computing $Z_{\mathbf{C},\mathfrak{D}}(\cdot)$, to be defined in section 2.3.

However, for most of the proof of Theorem 1.1 this issue of computation model seems not to be central, because our proof starts with a preprocessing step using the purification lemma (see section 3 for a high-level description of the proof, and see section 7 for the purification lemma), after which the matrix concerned becomes a *pure* one, meaning that every entry is the product of a nonnegative integer and a root of unity. So throughout the proof, we let $\mathbb{C}$ denote the set of algebraic numbers and refer to them simply as complex numbers, except in the proof of the purification lemma in section 7, where we will be more careful about the model of computation.

[2] For readers who are not particularly concerned with details of the model of computation with complex numbers, this section can be skipped initially.

[3] This is a slight modification to the model of [26] and of [34, 33]. It will come in handy later in one step of the proof in section 7, in which it allows us to avoid certain technical subtleties.

After the proof of Theorem 1.1, we consider the decidability of the dichotomy theorem and prove Theorem 1.2. The input of the problem is the full description of $\mathbf{A}$, including the minimal polynomial $F(x)$ of α, the approximation $\widehat{\alpha}$ of α, as well as the standard representation of the entries $A_{i,j}$ of $\mathbf{A}$. We refer to the binary length of all the components above as the input size of $\mathbf{A}$. To prove Theorem 1.2, we give an algorithm that runs in polynomial time in the binary length of $\mathbf{A}$ and decides whether the problem of computing $Z_{\mathbf{A}}(\cdot)$ is in polynomial time or #P-hard.

2.3. 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 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

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

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

To study the complexity of $\mathsf{EVAL}(\mathbf{A})$, we introduce a much larger class of EVAL problems with not only edge weights but also vertex weights. Moreover, the vertex weights depend on the degrees of vertices of G, modulo some integer modulus. It is a generalization of the edge-vertex weight problems introduced in [21]. See also [29].

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

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

be a sequence of diagonal matrices in $\mathbb{C}^{m\times m}$ for some $N \geq 1$. We define the following problem $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$: Given an undirected graph $G = (V, E)$, compute

$$Z_{\mathbf{C},\mathfrak{D}}(G) = \sum_{\xi: V\to[m]} \mathrm{wt}_{\mathbf{C},\mathfrak{D}}(\xi), \tag{2.1}$$

where

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

and $\deg(v)$ *denotes the degree of v in G.*

Let G be an undirected graph with connected components $G_1, \ldots, G_s$.

Property 2.2. $Z_{\mathbf{C},\mathfrak{D}}(G) = Z_{\mathbf{C},\mathfrak{D}}(G_1) \times \cdots \times Z_{\mathbf{C},\mathfrak{D}}(G_s)$.

Property 2.2 implies that whether we need to design an algorithm for $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ or reduce $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ to another problem $\mathsf{EVAL}(\mathbf{C}', \mathfrak{D}')$, it suffices to consider connected input graphs. 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 an identity matrix, Property 2.2 and the remarks above apply to $\mathsf{EVAL}(\mathbf{A})$ as well.

Next, suppose $\mathbf{C}$ is the bipartization of an $m \times n$ $\mathbf{F}$, so $\mathbf{C}$ is $(m + n) \times (m + n)$. Given a graph G and a vertex u in G, we use Ξ_1 to denote the set of $\xi\colon V \to [m + n]$ with $\xi(u) \in [m]$ and Ξ_2 to denote the set of ξ with $\xi(u) \in [m + 1 : m + n]$. Then let

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

The next property follows from the definitions.

Property 2.3. $Z_{\mathbf{C},\mathfrak{D}}(G) = Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}(G, u) + Z^{\leftarrow}_{\mathbf{C},\mathfrak{D}}(G, u)$.

We introduce these two new functions because of the following lemma.

LEMMA 2.4. *For each $i \in \{0,1,2\}$, let $\mathbf{F}^{[i]}$ be an $m_i \times n_i$ complex matrix, where $m_0 = m_1 m_2$ and $n_0 = n_1 n_2$; let $\mathbf{C}^{[i]}$ be the bipartization of $\mathbf{F}^{[i]}$; and let*

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

be a sequence of $(m_i + n_i) \times (m_i + n_i)$ diagonal matrices for some $N \geq 1$, 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. Assume

$$\mathbf{F}^{[0]} = \mathbf{F}^{[1]} \otimes \mathbf{F}^{[2]}, \quad \mathbf{P}^{[0,r]} = \mathbf{P}^{[1,r]} \otimes \mathbf{P}^{[2,r]}, \quad \text{and} \quad \mathbf{Q}^{[0,r]} = \mathbf{Q}^{[1,r]} \otimes \mathbf{Q}^{[2,r]}$$

for all $r \in [0 : N-1]$. Then for any connected *graph G and any vertex u^* in G,*

$$Z^{\rightarrow}_{\mathbf{C}^{[0]},\mathfrak{D}^{[0]}}(G,u^*) = Z^{\rightarrow}_{\mathbf{C}^{[1]},\mathfrak{D}^{[1]}}(G,u^*) \cdot Z^{\rightarrow}_{\mathbf{C}^{[2]},\mathfrak{D}^{[2]}}(G,u^*) \quad \text{and} \tag{2.2}$$

$$Z^{\leftarrow}_{\mathbf{C}^{[0]},\mathfrak{D}^{[0]}}(G,u^*) = Z^{\leftarrow}_{\mathbf{C}^{[1]},\mathfrak{D}^{[1]}}(G,u^*) \cdot Z^{\leftarrow}_{\mathbf{C}^{[2]},\mathfrak{D}^{[2]}}(G,u^*). \tag{2.3}$$

Proof. We only prove (2.2) about $Z^{\rightarrow}$. The proof of (2.3) is similar. First, 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 (2.2) holds trivially.

Now assume $G = (U \cup V, E)$ 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

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

We define a map ρ from $\Xi_1 \times \Xi_2$ to Ξ_0 as follows: $\rho(\xi_1,\xi_2) = \xi_0$, 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 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. It is clear that ρ is a bijection, and

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

if $\rho(\xi_1,\xi_2) = \xi_0$. Equation (2.2) then follows, and the lemma is proved. ∎

2.4. Basic #P-hardness. We state the dichotomy of Bulatov and Grohe.

THEOREM 2.5 (Bulatov and Grohe [4]). *Let $\mathbf{A}$ be a symmetric and connected matrix with nonnegative algebraic entries. Then $\mathsf{EVAL}(\mathbf{A})$ is either in polynomial time or #P-hard. Moreover, we have the following two cases:*

1. *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-hard.*
2. *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-hard.*

Theorem 2.5 gives us the following useful corollary.

COROLLARY 2.6. *Let $\mathbf{A}$ be a symmetric and connected matrix with nonnegative algebraic entries. If $\mathbf{A}$ has a 2×2 submatrix $\mathbf{B}$ such that all four entries of $\mathbf{B}$ are nonzero and $\det(\mathbf{B}) \neq 0$, then the problem $\mathsf{EVAL}(\mathbf{A})$ is* #P-hard.

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 and matrices.

Let $\mathbf{A}$ be an $m \times m$ symmetric complex matrix. If G has connected components $\{G_i\}$, then $Z_{\mathbf{A}}(G) = \prod_i Z_{\mathbf{A}}(G_i)$; if G is connected and $\mathbf{A}$ has connected components $\{\mathbf{A}_j\}$, then $Z_{\mathbf{A}}(G) = \sum_j Z_{\mathbf{A}_j}(G)$. Thus, if every $Z_{\mathbf{A}_j}(\cdot)$ is computable in polynomial time, then so is $Z_{\mathbf{A}}(\cdot)$. The hardness direction is less obvious. Assume that $\mathsf{EVAL}(\mathbf{A}_j)$ is #P-hard for some j; we want to show that $\mathsf{EVAL}(\mathbf{A})$ is also #P-hard by giving a polynomial-time reduction from $\mathsf{EVAL}(\mathbf{A}_j)$ to $\mathsf{EVAL}(\mathbf{A})$.

Now let G be an undirected 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 just assume that G is connected. Define a *pinning* version of $Z_{\mathbf{A}}(\cdot)$ as follows. For any chosen vertex $w \in V(G)$ and any $k \in [m]$, we let

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

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 submatrix of $\mathbf{A}$ restricted by V_j, then for a connected graph G, we have

$$Z_{\mathbf{A}_j}(G) = \sum_{k \in V_j} Z_{\mathbf{A}}(G, w, k),$$

which gives us the desired polynomial-time reduction from $\mathsf{EVAL}(\mathbf{A}_j)$ to $\mathsf{EVAL}(\mathbf{A})$.

The proof of this pinning lemma (Lemma 4.1) is a standard adaptation to the complex numbers of the one proved in [21]. For technical reasons we indeed need a total of three pinning lemmas (Lemmas 4.1, 4.3, and 8.4), and the proofs of the other two are a bit more involved. We remark that all three pinning lemmas show only the *existence* of polynomial-time reductions between $Z_{\mathbf{A}}(\cdot)$ and $Z_{\mathbf{A}}(\cdot, \cdot, \cdot)$ but do not *constructively* produce such a reduction, given $\mathbf{A}$. The proof of the pinning lemma in [21] used a result by Lovász [29] for real matrices. It is possible to use a new result of Schrijver [32] in the complex case. However, we give direct and self-contained proofs of our three lemmas without using [29] or [32].

After this preliminary step, we restrict to *connected* and symmetric $\mathbf{A}$. As indicated, for our work the two most influential predecessor papers are those by Bulatov and Grohe [4] and Goldberg et al. [21]. In both papers, the polynomial-time algorithms for the tractable cases are relatively straightforward or are previously known. The difficult part of the proof is to show that, in all other cases, the problem is #P-hard. Our proof follows a conceptual framework similar to that of Goldberg et al. [21]. However, over the complex numbers, new difficulties arise in both the tractability and the hardness part of the proof. Therefore, both the overall organization and the substantive part of the proof have to be done separately.

First, the complex numbers afford a richer variety of cancellations, which could lead to surprisingly efficient algorithms for $\mathsf{EVAL}(\mathbf{A})$ when the complex matrix $\mathbf{A}$ satisfies certain nice conditions. This turns out to be the case, and we obtain additional nontrivial tractable cases. These boil down to the following class of problems called $\mathsf{EVAL}(q)$. Let q be a fixed prime power. The input of $\mathsf{EVAL}(q)$ is a quadratic polynomial $f(x_1, x_2, \ldots, x_n)$ with integer coefficients; the output is

$$Z_q(f) = \sum_{x_1, x_2, \ldots, x_n \in \mathbb{Z}_q} \omega_q^{f(x_1, x_2, \ldots, x_n)}.$$

We show that for any fixed prime power q, $\mathsf{EVAL}(q)$ is in polynomial time. In the algorithm (see section 12), Gauss sums play a crucial role. The tractability part of our dichotomy theorem is then done by reducing $\mathsf{EVAL}(\mathbf{A})$, assuming $\mathbf{A}$ satisfies a set of nice structural conditions (to be described in the rest of this section) imposed by the hardness part, to $\mathsf{EVAL}(q)$ for some appropriate prime power q. While the corresponding sums for finite fields (when q is a prime) are known to be in polynomial time [10, 15], [27, Theorem 6.30] and, in particular, this includes the special case of $\mathbb{Z}_2$ used in [21], our algorithm over rings $\mathbb{Z}_q$ is new and should be of independent interest.

Next we briefly describe the proof structure of the hardness part of the dichotomy theorem. Let $\mathbf{A}$ be a connected and symmetric matrix. The difficulty starts with the most basic proof technique, called gadget constructions. With a graph gadget, one can take any input undirected graph G and produce a modified graph G^* by replacing each edge of G with the gadget. Moreover, one can define a suitable modified matrix $\mathbf{A}^*$ from the fixed matrix $\mathbf{A}$ and the gadget such that $Z_{\mathbf{A}^*}(G) = Z_{\mathbf{A}}(G^*)$ for all undirected graphs G.

A simple example of this maneuver is called *thickening*, where one replaces each edge in the input G by t parallel edges to get G^*. It is easy to see that if $\mathbf{A}^*$ is obtained from $\mathbf{A}$ by replacing each entry $A_{i,j}$ by its tth power $(A_{i,j})^t$, then the equation above holds and we get a reduction from $\mathsf{EVAL}(\mathbf{A}^*)$ to $\mathsf{EVAL}(\mathbf{A})$. In particular, if $\mathbf{A}$ is real (as in the case of [21]) and t is even, this produces a nonnegative matrix $\mathbf{A}^*$, to which one may apply the Bulatov–Grohe result:

1. If $\mathbf{A}^*$, as a symmetric and nonnegative matrix, does not satisfy the tractability criteria of Bulatov and Grohe as described in Theorem 2.5, then both $\mathsf{EVAL}(\mathbf{A}^*)$ and $\mathsf{EVAL}(\mathbf{A})$ are #P-hard and we are done.
2. Otherwise, $\mathbf{A}^*$ satisfies the Bulatov–Grohe tractability criteria, from which $\mathbf{A}$ must satisfy certain necessary structural properties since $\mathbf{A}^*$ is derived from $\mathbf{A}$.

The big picture of the proof of the dichotomy theorem is then to design various graph gadgets to show that, assuming $\mathsf{EVAL}(\mathbf{A})$ is not #P-hard, the matrix $\mathbf{A}$ must satisfy a collection of strong necessary conditions over its complex entries $A_{i,j}$. (The exact proof structure, however, is different from this very-high-level description, which will become clear in the rest of this section.) To finish the proof, we show that for every $\mathbf{A}$ that satisfies all these structural conditions, one can reduce $\mathsf{EVAL}(\mathbf{A})$ to $\mathsf{EVAL}(q)$ for some appropriate prime power q (which depends only on $\mathbf{A}$), and thus $\mathsf{EVAL}(\mathbf{A})$ is tractable.

For complex matrices $\mathbf{A}$, we immediately encountered the following difficulty. Any graph gadget 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 nonnegative quantity, as was done in [21], no obvious arithmetic operations on the complex numbers have this property. Pointedly, *conjugation* is not an arithmetic operation. However, it is clear that for roots of unity, one *can* produce conjugation by multiplication.

Thus, our proof starts with a process of replacing an arbitrary complex matrix by a *purified* complex matrix with a special form. It turns out that we must separate out the cases where $\mathbf{A}$ is bipartite or nonbipartite. A purified bipartite (and symmetric, connected) matrix is the bipartization of a matrix $\mathbf{B}$, 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 μ_i is a positive rational number 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 $\mathsf{EVAL}(\mathbf{A})$ or there exists a purified bipartite matrix $\mathbf{A}' \in \mathbb{C}^{m\times m}$ such that $\mathsf{EVAL}(\mathbf{A}')$ is polynomial-time equivalent to $\mathsf{EVAL}(\mathbf{A})$ (Theorem 5.2). For nonbipartite matrices $\mathbf{A}$, a corresponding statement holds (Theorem 6.2). For convenience, we only consider the bipartite case in the discussion below.

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*. To carry out this process, we need to use the more general problem $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ defined earlier in section 2.3. 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 (not necessarily symmetric) matrix with entries $(F_{i,j})$. We call $\mathbf{F}$ 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 $F_{1,i} = F_{i,1} = 1$ for all $i \in [m]$.*
2. *M is the least common multiple (lcm) of orders of all the entries $F_{i,j}$ of $\mathbf{F}$.*
3. *For all $i \ne j \in [m]$, we have $\langle \mathbf{F}_{i,*}, \mathbf{F}_{j,*} \rangle = 0$ and $\langle \mathbf{F}_{*,i}, \mathbf{F}_{*,j} \rangle = 0$.*

Some of the simplest examples of discrete unitary matrices are as follows:

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \zeta & \zeta^{-1} & \zeta^2 & \zeta^{-2} \\ 1 & \zeta^2 & \zeta^{-2} & \zeta^{-1} & \zeta \\ 1 & \zeta^{-1} & \zeta & \zeta^{-2} & \zeta^2 \\ 1 & \zeta^{-2} & \zeta^2 & \zeta & \zeta^{-1} \end{pmatrix},$$

where $\omega = e^{2\pi i/3}$ and $\zeta = e^{2\pi i/5}$. Tensor products of discrete unitary matrices are also discrete unitary matrices. These matrices play a major role in our proof.

Now we come back to the proof outline. We show that $\mathsf{EVAL}(\mathbf{A}')$ is either #P-hard or polynomial-time equivalent to $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ for some matrix $\mathbf{C} \in \mathbb{C}^{2n\times 2n}$ and some $\mathfrak{D}$ of diagonal matrices from $\mathbb{C}^{2n\times 2n}$, where $n \le m$ and $\mathbf{C}$ is the bipartization of a discrete unitary matrix, denoted by $\mathbf{F}$. In addition, there are further stringent requirements for $\mathfrak{D}$; otherwise $\mathsf{EVAL}(\mathbf{A}')$ is #P-hard. The detailed statements can be found in Theorems 5.3 and 5.4, 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 $\mathfrak{D}$, each entry of $\mathbf{D}^{[r]}$ is either zero or a root of unity. We call these conditions, with some abuse of terminology, the discrete unitary requirements. The proof that these requirements are necessary is demanding and among the most difficult in the paper.

Next, assume that we have a problem $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ satisfying the discrete unitary requirements with $\mathbf{C}$ being the bipartization of $\mathbf{F}$. Recall that $\omega_q = e^{2\pi i/q}$.

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

We show that either $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is #P-hard or, after a permutation of rows and columns, $\mathbf{F}$ becomes the *tensor product* of a collection of suitable Fourier matrices:

$$\boldsymbol{\mathcal{F}}_{q_1} \otimes \boldsymbol{\mathcal{F}}_{q_2} \otimes \cdots \otimes \boldsymbol{\mathcal{F}}_{q_d}, \qquad \text{where } d \ge 1 \text{ and every } q_i \text{ is a prime power.}$$

Basically, we show that even with the stringent conditions imposed on the pair $(\mathbf{C}, \mathfrak{D})$ by the discrete unitary requirements, most of $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ are still #P-hard, unless

$\mathbf{F}$ is the tensor product of Fourier matrices. On the other hand, the tensor product decomposition into Fourier matrices finally brings in group theory and Gauss sums. It gives us a canonical way of writing the entries of $\mathbf{F}$ in a closed form. More exactly, we index the rows and columns of $\mathbf{F}$ using $\mathbf{x} = (x_1, \ldots, x_d) \in \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_d}$ so that

$$F_{\mathbf{x},\mathbf{y}} = \prod_{i \in [d]} \omega_{q_i}^{x_i y_i} \quad \text{for any } \mathbf{x}, \mathbf{y} \in \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_d}.$$

Assume $q_1, \ldots, q_d$ are powers of $s \leq d$ distinct primes $p_1, \ldots, p_s$. We can also view the set of indices as $\mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_d} = G_1 \times \cdots \times G_s$, where G_i is the finite Abelian group which is the product of all the groups $\mathbb{Z}_{q_j}$ with q_j being a power of p_i.

This canonical tensor product decomposition of $\mathbf{F}$ gives us a natural way to index the rows and columns of $\mathbf{C}$ and the diagonal matrices in $\mathfrak{D}$ using $\mathbf{x}$. More exactly, we index the first half of the rows and columns of $\mathbf{C}$ and every $\mathbf{D}^{[r]}$ in $\mathfrak{D}$ using $(0, \mathbf{x})$ and index the second half of the rows and columns using $(1, \mathbf{x})$, $\mathbf{x} \in \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_d}$.

With this canonical expression of $\mathbf{F}$ and $\mathbf{C}$, we further inquire into the structure of $\mathfrak{D}$. Here one more substantial difficulty awaits us. There are two more properties that we must demand of those diagonal matrices in $\mathfrak{D}$. If $\mathfrak{D}$ does not satisfy these additional properties, then $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ 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 (here we follow the convention of using D_i to denote the (i,i)th entry of a diagonal matrix $\mathbf{D}$):

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

We let $\mathcal{S}$ denote the set of subscripts r such that $\Lambda_r \neq \emptyset$ and let $\mathcal{T}$ denote the set of r such that $\Delta_r \neq \emptyset$. We can prove that for each $r \in \mathcal{S}$, $\Lambda_r = \prod_{i=1}^{s} \Lambda_{r,i}$ must be a direct product of cosets $\Lambda_{r,i}$ in the Abelian groups G_i, where $i = 1, \ldots, s$ correspond to the constituent prime powers of the group, and for each $r \in \mathcal{T}$, $\Delta_r = \prod_{i=1}^{s} \Delta_{r,i}$ is a direct product of cosets in the same Abelian groups. Otherwise, $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ 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 the quadratic structure as *a set of exponential difference equations* over bases which are appropriate roots of unity of orders equal to various prime powers. The constructions used in this part of the proof are the most demanding in the paper.

After all these necessary conditions, we finally show that if $\mathbf{C}$ and $\mathfrak{D}$ satisfy all these requirements, there is a polynomial-time algorithm for $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ and thus, $\mathsf{EVAL}(\mathbf{A})$ is also in polynomial time. To this end, we reduce $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ to $\mathsf{EVAL}(q)$ for some appropriate prime power q (which depends only on $\mathbf{C}$ and $\mathfrak{D}$). As noted earlier, the tractability of $\mathsf{EVAL}(q)$ is new and is of independent interest.

4. Pinning lemmas and preliminary reductions. We prove two pinning lemmas in this section, one for $\mathsf{EVAL}(\mathbf{A})$ and one for $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$. The proof of the first lemma is very similar to that of the pinning lemma from [21], but the second one has some complications. We will prove a third pinning lemma in section 8.1.

4.1. A pinning lemma for $\mathsf{EVAL}(\mathbf{A})$. Let $\mathbf{A}$ be an $m \times m$ symmetric complex matrix. We define a new problem $\mathsf{EVALP}(\mathbf{A})$: 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

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

It is easy to see that $\mathsf{EVAL}(\mathbf{A}) \le \mathsf{EVALP}(\mathbf{A})$. The other direction also holds.

LEMMA 4.1 (first pinning lemma). $\mathsf{EVALP}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{A})$.

Proof. We define an equivalence relation $\sim$ over $[m]$: $i \sim j$ if for any undirected graph $G=(V,E)$ and $w \in V$, $Z_{\mathbf{A}}(G,w,i) = Z_{\mathbf{A}}(G,w,j)$. Note that we do not know, given $\mathbf{A}$, how to compute $\sim$ efficiently, although this is possible using the new results of Schrijver [32]. Instead, the lemma only proves, nonconstructively, the existence of a polynomial-time reduction, which is sufficient for our purposes.

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

$$Z_{\mathbf{A}}(G,w,i) = Z_{\mathbf{A}}(G,w,j) \neq Z_{\mathbf{A}}(G,w,i') = Z_{\mathbf{A}}(G,w,j')$$

for all $i,j \in \mathcal{A}_t$ and $i',j' \in \mathcal{A}_{t'}$. Again, we do not know how to compute such a pair efficiently, but it always exists by the definition of the equivalence relation $\sim$.

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

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

When $S=[s]$, $\mathsf{EVAL}(\mathbf{A},S)$ is exactly $\mathsf{EVAL}(\mathbf{A})$. We make the following claim.

CLAIM 4.2. *If $S \subseteq [s]$ and $|S| \ge 2$, then there exists a partition $\{S_1,\dots,S_k\}$ of S for some $k>1$ such that $\mathsf{EVAL}(\mathbf{A},S_d) \le \mathsf{EVAL}(\mathbf{A},S)$ for all $d \in [k]$.*

We use Claim 4.2 to prove Lemma 4.1. Let (G,w,i) be an input of $\mathsf{EVALP}(\mathbf{A})$, and let $i \in \mathcal{A}_t$ for some $t \in [s]$. We will use Claim 4.2 to prove that $\mathsf{EVAL}(\mathbf{A},\{t\}) \le \mathsf{EVAL}(\mathbf{A})$. If this is the case, then we are done because

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

Finally we show that $\mathsf{EVAL}(\mathbf{A},\{t\}) \le \mathsf{EVAL}(\mathbf{A})$. It is trivially true when $s=1$. When $s \ge 2$, by Claim 4.2 there exists a partition $\{S_1,\dots,S_k\}$ of S for some $k>1$, such that $\mathsf{EVAL}(\mathbf{A},S_d) \le \mathsf{EVAL}(\mathbf{A},S) \equiv \mathsf{EVAL}(\mathbf{A})$, for all $d \in [k]$. Without loss of generality, assume $t \in S_1$. If $S_1 = \{t\}$, then we are done; otherwise, $|S_1| \ge 2$, and we just rename S_1 to be S and repeat the process above. As $|S|$ is strictly decreasing after each iteration, this procedure will stop at some time. The lemma is proved. ∎

Proof of Claim 4.2. Let t,t' be two distinct integers in S. We let $P_{t,t'} = (G^*,w^*)$, where $G^* = (V^*,E^*)$. It defines the following equivalence relation $\sim^*$ over S: For $a,b \in S$, $a \sim^* b$ if $Z_{\mathbf{A}}(G^*,w^*,i) = Z_{\mathbf{A}}(G^*,w^*,j)$, where $i \in \mathcal{A}_a$ and $j \in \mathcal{A}_b$.

This equivalence relation $\sim^*$ is well-defined, being independent of our choices of $i \in \mathcal{A}_a, j \in \mathcal{A}_b$. It gives us equivalence classes $\{S_1,\dots,S_k\}$, a partition of S. Because $(G^*,w^*) = P_{t,t'}$, by the definition of $\sim^*$, t and t' belong to different classes and thus $k \ge 2$. For each $d \in [k]$, we let $X_d = Z_{\mathbf{A}}(G^*,w^*,i)$, where $i \in \mathcal{A}_a$ and $a \in S_d$. This number X_d is well-defined and is independent of the choices of $a \in S_d$ and $i \in \mathcal{A}_a$. Moreover, the definition of $\sim^*$ 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. To this end, for each $p \in [0 : k-1]$ we construct a graph $G^{[p]} = (V^{[p]}, E^{[p]})$ as follows. $G^{[p]}$ 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, we have $|V^{[p]}| = |V| + p \cdot |V^*| - p$. In particular, $G^{[0]} = G$.

From the construction of these graphs, we get the following equations:

$$Z_{\mathbf{A}}(G^{[p]}, w', S) = \sum_{d \in [k]} (X_d)^p \cdot Z_{\mathbf{A}}(G, w, S_d) \quad \text{for every } p \in [0 : k-1].$$

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

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

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

Clearly, $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D}) \leq \mathsf{EVALP}(\mathbf{C}, \mathfrak{D})$. However, unlike $\mathsf{EVALP}(\mathbf{A})$ and $\mathsf{EVAL}(\mathbf{A})$, we can prove the other direction only when $(\mathbf{C}, \mathfrak{D})$ satisfies the following condition:

(*Pinning*) Every entry of $\mathbf{F}$ is a power of ω_N, where N denotes the number of matrices in $\mathfrak{D}$; $\mathbf{F}/\sqrt{m}$ is a unitary matrix, and $\mathbf{D}^{[0]}$ is the $2m \times 2m$ identity matrix.

LEMMA 4.3 (second pinning lemma). *If $(\mathbf{C}, \mathfrak{D})$ satisfies the condition* (*Pinning*) *above, then* $\mathsf{EVALP}(\mathbf{C}, \mathfrak{D}) \equiv \mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$.

COROLLARY 4.4. *If $(\mathbf{C}, \mathfrak{D})$ satisfies the condition* (*Pinning*)*, then the problem of computing $Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}$ as well as $Z^{\leftarrow}_{\mathbf{C},\mathfrak{D}}$ is polynomial-time reducible to* $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$.

Proof of Lemma 4.3. The proof structure is similar to that of Lemma 4.1. We start by introducing the following equivalence relation over $[2m]$: $i \sim j$ if for any undirected $G = (V, E)$ and $w \in V$, $Z_{\mathbf{C},\mathfrak{D}}(G, w, i) = Z_{\mathbf{C},\mathfrak{D}}(G, w, j)$. It partitions $[2m]$ into s equivalence classes $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_s$ for some $s \geq 1$. For any distinct $t, t' \in [s]$, there exists a pair $P_{t,t'} = (G, w)$, where G is an undirected graph and w is a vertex, such that for all $i, j \in \mathcal{A}_t$ and $i', j' \in \mathcal{A}_{t'}$,

$$Z_{\mathbf{C},\mathfrak{D}}(G, w, i) = Z_{\mathbf{C},\mathfrak{D}}(G, w, j) \neq Z_{\mathbf{C},\mathfrak{D}}(G, w, i') = Z_{\mathbf{C},\mathfrak{D}}(G, w, j').$$

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

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

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

CLAIM 4.5. *If $S \subseteq [s]$ and $|S| \geq 2$, there exists a partition $\{S_1, \ldots, S_k\}$ of S for some $k > 1$ such that $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D}, S_d) \leq \mathsf{EVAL}(\mathbf{C}, \mathfrak{D}, S)$ for all $d \in [k]$.*

Lemma 4.3 then follows from Claim 4.5. The rest of the proof is exactly the same as that of Lemma 4.1 using Claim 4.2, so we omit it here. □

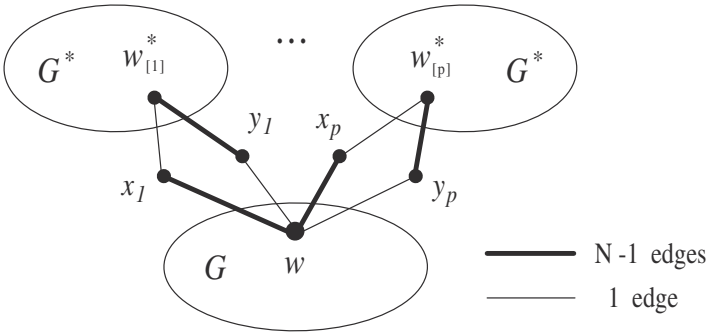

FIG. 4.1. *Graph* $G^{[p]}$, $p \in [0 : k-1]$.

Proof of Claim 4.5. Let t, t' be two distinct integers in S (as $|S| \geq 2$). Let $P_{t,t'} = (G^*, w^*)$, where $G^* = (V^*, E^*)$. It defines the following equivalence relation. For $a, b \in S$, $a \sim^* b$ if $Z_{\mathbf{C},\mathfrak{D}}(G^*, w^*, i) = Z_{\mathbf{C},\mathfrak{D}}(G^*, w^*, j)$, where $i \in \mathcal{A}_a$ and $j \in \mathcal{A}_b$.

This partitions S into equivalence classes $\{S_1, \ldots, S_k\}$. Because $(G^*, w^*) = P_{t,t'}$, t and t' must belong to different classes and thus we have $k \geq 2$. For each $d \in [k]$, we let $Y_d = Z_{\mathbf{C},\mathfrak{D}}(G^*, w^*, i)$, where $i \in \mathcal{A}_a$ and $a \in S_d$. The definition of the equivalence relation implies that $Y_d \neq Y_{d'}$ for all distinct $d, d' \in [k]$.

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. To this end, for each integer $p \in [0 : k-1]$, we construct 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 4.1). More precisely,

$$V^{[p]} = V \cup \{v_i : i \in [p] \text{ and } v \in V^*\} \cup \{x_1, \ldots, x_p, y_1, \ldots, y_p\},$$

where $x_1, \ldots, x_p, y_1, \ldots, y_p$ are new vertices, and $E^{[p]}$ contains 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 get the following equations. For $p \in [0 : k-1]$, $Z_{\mathbf{C},\mathfrak{D}}(G^{[p]}, w, S)$ is equal to

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

Note that $\deg(x_i) = \deg(y_i) = N$ and the changes to the degrees of w and w_i^* are all multiples of N. By (*Pinning*), there are no new vertex weight contributions from $\mathfrak{D}$.

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

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

Because $Y_d \neq Y_{d'}$ 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 G^* are constants independent of G, this gives a reduction from $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D}, S_d)$ to $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D}, S)$ for every d. ∎

4.3. Reduction to connected matrices. The following lemma allows us to focus on the connected components of $\mathbf{A}$.

LEMMA 4.6. *Let $\mathbf{A} \in \mathbb{C}^{m\times m}$ be a symmetric matrix with components $\{\mathbf{A}_i\}$.*

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

Proof. Lemma 4.6 follows from the first pinning lemma (Lemma 4.1). ∎

The main dichotomy, Theorem 1.1, will be proved by showing that for every connected $\mathbf{A} \in \mathbb{C}^{m\times m}$, $\mathsf{EVAL}(\mathbf{A})$ 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

1. either the problem is #P-hard, or
2. the matrix that defines the problem satisfies certain structural properties, or
3. 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 these three steps as three filters that remove #P-hard $\mathsf{EVAL}(\mathbf{A})$ 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 $\mathsf{EVAL}(\mathbf{A})$, where $\mathbf{A} \in \mathbb{C}^{m\times m}$ is a fixed symmetric, connected, and bipartite matrix with *algebraic* entries. It is easy to see that if $m = 1$, then $\mathsf{EVAL}(\mathbf{A})$ is tractable. So in the discussion below, we always 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 $1 \leq k < m$ such that*

1. *$A_{i,j} = 0$ for all $i, j \in [k]$; $A_{i,j} = 0$ for all $i, j \in [k+1 : m]$; and*
2. *$A_{i,j}/(\mu_i\mu_j) = A_{j,i}/(\mu_i\mu_j)$ is a root of unity for all $i \in [k]$, $j \in [k+1 : m]$.*

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 μ_i is a positive rational number and every $\zeta_{i,j}$ is a root of unity, and $\mathbf{A}$ is the bipartization of $\mathbf{B}$.

THEOREM 5.2. *Let $\mathbf{A} \in \mathbb{C}^{m\times m}$ be a symmetric, connected, and bipartite matrix with algebraic entries. 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. Note that we renamed the $\mathbf{A}'$ passed down from Step 1 to $\mathbf{A}$ for convenience. We show 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 bipartization of a discrete unitary matrix. (See section 3 for the definition.) Also note that the tensor product of two discrete unitary matrices is also discrete unitary.

THEOREM 5.3. *Given a purified bipartite matrix $\mathbf{A} \in \mathbb{C}^{m\times m}$, 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:*

($\mathcal{U}_1$) *$\mathbf{C} \in \mathbb{C}^{2n\times 2n}$ for some $n \geq 1$, and*

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

is a sequence of N $2n \times 2n$ diagonal matrices over $\mathbb{C}$ for some even *$N > 1$.*

($\mathcal{U}_2$) *$\mathbf{C}$ is the bipartization of an M-*discrete unitary matrix *$\mathbf{F} \in \mathbb{C}^{n\times n}$, where $M \geq 1$ and $M \mid N$. (Note that $\mathbf{C}$ and $\mathbf{F}$ uniquely determine each other.)*

($\mathcal{U}_3$) *$\mathbf{D}^{[0]}$ is the $2n \times 2n$ identity matrix, and for every $r \in [N-1]$ we have*

$$\exists i \in [n],\ D_i^{[r]} \neq 0 \implies \exists i' \in [n],\ D_{i'}^{[r]} = 1, \qquad \text{and}$$

$$\exists i \in [n+1:2n],\ D_i^{[r]} \neq 0 \implies \exists i' \in [n+1:2n],\ D_{i'}^{[r]} = 1.$$

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

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 $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$. There are also 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 5.3, 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 $M = 1$. As $\mathbf{F}$ is M-discrete unitary, we must have $m = 1$. It is easy to check that $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is tractable: $\mathbf{C}$ is a 2×2 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 $\xi\colon V \to \{0, 1\}$ which could yield nonzero values; finally, for a 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 the parameter $M > 1$ we further investigate the structure of $\mathbf{F}$ as well as the diagonal matrices in $\mathfrak{D}$ and derive three necessary conditions on them for $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ to not be #P-hard. In the tractability part, we prove that these conditions are actually sufficient for it to be polynomial-time computable.

5.3.1. Step 3.1: Entries of $\mathbf{D}^{[r]}$ are either 0 or powers of ω_N. In the first step, we prove the following theorem.

THEOREM 5.4. *Suppose $((M, N), \mathbf{C}, \mathfrak{D})$ satisfies ($\mathcal{U}_1$)–($\mathcal{U}_4$) with $M > 1$. Then either $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is #P-hard or $((M, N), \mathbf{C}, \mathfrak{D})$ satisfies the following condition ($\mathcal{U}_5$):*

($\mathcal{U}_5$) *For all $r \in [N-1]$ and $i \in [0 : 2n-1]$, $D_i^{[r]}$ 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* defined below.

DEFINITION 5.5. *Let $q > 1$ be a prime power, and $k \geq 1$ 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 of $\boldsymbol{\mathcal{F}}_{q,k}$, 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 5.6. *Assume $((M, N), \mathbf{C}, \mathfrak{D})$ satisfies conditions $(\mathcal{U}_1)$–$(\mathcal{U}_5)$ and $M > 1$. Then either $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is #P-hard or there exist permutations Σ and Π of $[0 : m-1]$ and a sequence $q_1, q_2, \ldots, q_d$ of d prime powers, for some $d \geq 1$, such that*

$$\mathbf{F}_{\Sigma,\Pi} = \bigotimes_{i \in [d]} \boldsymbol{\mathcal{F}}_{q_i}. \tag{5.1}$$

Suppose there do exist permutations Σ, Π and prime powers $q_1, \ldots, q_d$ such that $\mathbf{F}_{\Sigma,\Pi}$ satisfies (5.1). Then we let $\mathbf{C}_{\Sigma,\Pi}$ denote the bipartization of $\mathbf{F}_{\Sigma,\Pi}$ and let $\mathfrak{D}_{\Sigma,\Pi}$ denote a sequence of N $2m \times 2m$ diagonal matrices in which the rth matrix is

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

Since permuting the rows and columns of $\mathbf{C}$ and $\mathbf{D}^{[r]}$ by the same permutation pair does not affect the complexity of $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$, $\mathsf{EVAL}(\mathbf{C}_{\Sigma,\Pi}, \mathfrak{D}_{\Sigma,\Pi}) \equiv \mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$. 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, with

$$\mathbf{F} = \bigotimes_{i \in [d]} \boldsymbol{\mathcal{F}}_{q_i}. \tag{5.2}$$

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 strictly increasing sequence of primes and $\mathbf{t} = (t_1, \ldots, t_s)$ be a sequence of positive integers. Let $\mathcal{Q} = \{\mathbf{q}_i : i \in [s]\}$ be a set of s sequences in which each $\mathbf{q}_i$ is a nonincreasing sequence $(q_{i,1}, \ldots, q_{i,t_i})$ of powers of p_i. We let q_i denote $q_{i,1}$ for all $i \in [s]$, let

$$\mathbb{Z}_{\mathbf{q}_i} = \prod_{j \in [t_i]} \mathbb{Z}_{q_{i,j}} = \mathbb{Z}_{q_{i,1}} \times \cdots \times \mathbb{Z}_{q_{i,t_i}}$$

for all $i \in [s]$, and let

$$\mathbb{Z}_{\mathcal{Q}} = \prod_{i \in [s], j \in [t_i]} \mathbb{Z}_{q_{i,j}} = \prod_{i \in [s]} \mathbb{Z}_{\mathbf{q}_i} = \mathbb{Z}_{q_{1,1}} \times \cdots \times \mathbb{Z}_{q_{1,t_1}} \times \cdots \times \mathbb{Z}_{q_{s,1}} \times \cdots \times \mathbb{Z}_{q_{s,t_s}}$$

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 componentwise 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 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 $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_{\mathbf{q}_i}$.

From (5.2), 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 three conditions $(\mathcal{R}_1)$–$(\mathcal{R}_3)$, which we refer to combined as $(\mathcal{R})$.

$(\mathcal{R}_1)$ $\mathbf{p} = (p_1, \ldots, p_s)$ is a strictly increasing sequence of primes; $\mathbf{t} = (t_1, \ldots, t_s)$ is a sequence of positive integers; $\mathcal{Q} = \{\mathbf{q}_i : i \in [s]\}$ is a collection of s sequences, in which each $\mathbf{q}_i = (q_{i,1}, \ldots, q_{i,t_i})$ is a nonincreasing sequence of powers of p_i.

$(\mathcal{R}_2)$ $\mathbf{C}$ is the bipartization 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 $\rho\colon [0 : m-1] \to \mathbb{Z}_{\mathcal{Q}}$ (so $m = \prod_{i,j} q_{i,j}$) such that

$$F_{a,b} = \prod_{i \in [s], j \in [t_i]} \omega_{q_{i,j}}^{x_{i,j}\, y_{i,j}} \quad \text{for all } a, b \in [0 : m-1], \tag{5.3}$$

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 (5.3) 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: $M = q_1 q_2 \cdots q_s$.

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

$$F_{\mathbf{x},\mathbf{y}} = F_{\rho^{-1}(\mathbf{x}),\rho^{-1}(\mathbf{y})} = \prod_{i \in [s], j \in [t_i]} \omega_{q_{i,j}}^{x_{i,j}\, y_{i,j}} \quad \text{for all } \mathbf{x}, \mathbf{y} \in \mathbb{Z}_{\mathcal{Q}}, \tag{5.4}$$

whenever we have a tuple $((M,N), \mathbf{C}, \mathfrak{D}, (\mathbf{p}, \mathbf{t}, \mathcal{Q}))$ that is known to satisfy condition $(\mathcal{R})$. We assume that $\mathbf{F}$ is indexed by $(\mathbf{x}, \mathbf{y}) \in \mathbb{Z}_{\mathcal{Q}}^2$ rather than $(a,b) \in [0 : m-1]^2$ and that $(\mathcal{R}_3)$ refers to (5.4). Correspondingly, we use $\{0,1\} \times \mathbb{Z}_{\mathcal{Q}}$ to index the entries of matrices $\mathbf{C}$ and $\mathbf{D}^{[r]}$: $(0, \mathbf{x})$ 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 $(\mathcal{R})$. 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 rth 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

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

We use $\mathcal{S}$ to denote the set of $r \in [N-1]$ such that $\Lambda_r \neq \emptyset$ and $\mathcal{T}$ to 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 5.7. *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 is 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 use Φ^{lin} to denote its corresponding subgroup $\{\mathbf{x} - \mathbf{x}' \,|\, \mathbf{x}, \mathbf{x}' \in \Phi\}$.*

THEOREM 5.8. *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 $\Lambda_r, \Delta_r \subseteq \mathbb{Z}_{\mathcal{Q}}$ 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 $\Lambda_{r,i}$ is a coset in $\mathbb{Z}_{\mathbf{q}_i}$, $i \in [s]$.*

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

Suppose $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is not #P-hard. By Theorem 5.8, $((M,N), \mathbf{C}, \mathfrak{D}, (\mathbf{p}, \mathbf{t}, \mathcal{Q}))$ satisfies not only $(\mathcal{R})$ but also $(\mathcal{L})$. Actually, by $(\mathcal{U}_3)$, $\mathfrak{D}$ also satisfies the following:

$(\mathcal{L}_3)$ There exists an $\mathfrak{a}^{[r]} \in \Lambda_r$ for each $r \in \mathcal{S}$, a $\mathfrak{b}^{[r]} \in \Delta_r$ for each $r \in \mathcal{T}$ such that

$$D^{[r]}_{(0,\mathfrak{a}^{[r]})} = D^{[r]}_{(1,\mathfrak{b}^{[r]})} = 1.$$

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. We start with some notation.

Given $\mathbf{x}$ in $\mathbb{Z}_{\mathbf{q}_i}$ for some $i \in [s]$, we use $\mathbf{ext}_r(\mathbf{x})$ (extension of $\mathbf{x}$ for short), where $r \in \mathcal{S}$, to denote the following unique vector:

$$\left(\mathfrak{a}^{[r]}_1, \ldots, \mathfrak{a}^{[r]}_{i-1}, \mathbf{x}, \mathfrak{a}^{[r]}_{i+1}, \ldots, \mathfrak{a}^{[r]}_s\right) \in \mathbb{Z}_{\mathcal{Q}}.$$

Similarly we let $\mathbf{ext}'_r(\mathbf{x})$, where $r \in \mathcal{T}$, denote the following unique vector:

$$\left(\mathfrak{b}^{[r]}_1, \ldots, \mathfrak{b}^{[r]}_{i-1}, \mathbf{x}, \mathfrak{b}^{[r]}_{i+1}, \ldots, \mathfrak{b}^{[r]}_s\right) \in \mathbb{Z}_{\mathcal{Q}}.$$

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 $q_k = q_{k,1}$.

THEOREM 5.9. *Let $((M,N), \mathbf{C}, \mathfrak{D}, (\mathbf{p}, \mathbf{t}, \mathcal{Q}))$ be a tuple that satisfies both $(\mathcal{R})$ and $(\mathcal{L})$. Then either $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is #P-hard, or $\mathfrak{D}$ satisfies the following condition $(\mathcal{D})$:*

$(\mathcal{D}_1)$ *For all $r \in \mathcal{S}$ and $\mathbf{x} \in \Lambda_r$, we have*

$$D^{[r]}_{(0,\mathbf{x})} = D^{[r]}_{(0,\mathbf{ext}_r(\mathbf{x}_1))} D^{[r]}_{(0,\mathbf{ext}_r(\mathbf{x}_2))} \cdots D^{[r]}_{(0,\mathbf{ext}_r(\mathbf{x}_s))}. \tag{5.5}$$

$(\mathcal{D}_2)$ *For all $r \in \mathcal{T}$ and $\mathbf{x} \in \Delta_r$, we have*

$$D^{[r]}_{(1,\mathbf{x})} = D^{[r]}_{(1,\mathbf{ext}'_r(\mathbf{x}_1))} D^{[r]}_{(1,\mathbf{ext}'_r(\mathbf{x}_2))} \cdots D^{[r]}_{(1,\mathbf{ext}'_r(\mathbf{x}_s))}. \tag{5.6}$$

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

$$\omega_N^{\alpha} \cdot F_{\mathbf{x},\widetilde{\mathbf{b}}} = D^{[r]}_{(0,\mathbf{x}+\widetilde{\mathbf{a}})} \cdot \overline{D^{[r]}_{(0,\mathbf{x})}} \quad \text{for all } \mathbf{x} \in \Lambda_r. \tag{5.7}$$

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

$$\omega_N^{\alpha} \cdot F_{\widetilde{\mathbf{b}},\mathbf{x}} = D^{[r]}_{(1,\mathbf{x}+\widetilde{\mathbf{a}})} \cdot \overline{D^{[r]}_{(1,\mathbf{x})}} \quad \text{for all } \mathbf{x} \in \Delta_r. \tag{5.8}$$

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 kth component $\mathbf{x}_k$, since 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 diagonal matrix $\mathbf{D}^{[r]}$. We express it in terms of an exponential difference equation.

5.4. Tractability. Now we can state a theorem of tractability.

THEOREM 5.10. *Suppose that $((M,N), \mathbf{C}, \mathfrak{D}, (\mathbf{p}, \mathbf{t}, \mathcal{Q}))$ satisfies $(\mathcal{R}), (\mathcal{L})$, and $(\mathcal{D})$. Then the problem $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ can be solved in polynomial time.*

6. Proof outline of the case: A is not bipartite. Both the definitions and the theorems of the case when the fixed matrix $\mathbf{A}$ is not bipartite are similar to, but also have significant differences from, those of the bipartite case.

6.1. Step 1: Purification of matrix A. We start with $\mathbf{A} \in \mathbb{C}^{m\times m}$, a symmetric, connected, and nonbipartite matrix with algebraic entries. In the discussion below, we assume $m > 1$; $\mathsf{EVAL}(\mathbf{A})$ is clearly tractable if $m = 1$.

DEFINITION 6.1. *Let $\mathbf{A} \in \mathbb{C}^{m\times m}$ be a symmetric matrix. We say $\mathbf{A}$ is a* purified *nonbipartite matrix if there exist positive rational numbers $\mu_1, \mu_2, \ldots, \mu_m$ 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 6.2. *Let $\mathbf{A} \in \mathbb{C}^{m\times m}$ be a symmetric, connected, and nonbipartite matrix, where $m > 1$. Then either $\mathsf{EVAL}(\mathbf{A})$ is #P-hard or there exists a purified nonbipartite 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.

THEOREM 6.3. *Let $\mathbf{A} \in \mathbb{C}^{m\times m}$ be a purified nonbipartite 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 $(\mathcal{U}'_1)$–$(\mathcal{U}'_4)$:*

$(\mathcal{U}'_1)$ $\mathbf{F} \in \mathbb{C}^{n\times n}$ for some $n \geq 1$, and $\mathfrak{D} = (\mathbf{D}^{[0]}, \ldots, \mathbf{D}^{[N-1]})$ is a sequence of N $n \times n$ diagonal matrices for some even *$N > 1$.*

$(\mathcal{U}'_2)$ $\mathbf{F}$ is a symmetric M-discrete unitary matrix, where $M \geq 1$ and $M \,|\, N$.

$(\mathcal{U}'_3)$ $\mathbf{D}^{[0]}$ is the identity matrix. For each $r \in [N-1]$, either $\mathbf{D}^{[r]} = \mathbf{0}$ or $\mathbf{D}^{[r]}$ has an entry equal to 1*.*

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

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 6.3, which is different from the m used in the first two steps. Similar to the bipartite case, we adopt the following convention in this step: given an $n \times n$ 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, it is clear that the problem $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is tractable. So in the rest of this section, we always assume that $M > 1$.

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

THEOREM 6.4. *Suppose $((M, N), \mathbf{F}, \mathfrak{D})$ satisfies $(\mathcal{U}'_1)$–$(\mathcal{U}'_4)$ and $M > 1$. Then either $\mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ is #P-hard or $((M, N), \mathbf{F}, \mathfrak{D})$ satisfies the following condition $(\mathcal{U}'_5)$:*

$(\mathcal{U}'_5)$ For all $r \in [N-1]$, entries of $\mathbf{D}^{[r]}$ are either zero or powers of ω_N.

6.3.2. Step 3.2: Fourier decomposition. Let q be a prime power. We say $\mathbf{W}$ is a *nondegenerate* 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 nondegenerate matrices. The proof is elementary, so we omit it here.

LEMMA 6.5. *Let q be a prime power and $\mathbf{W} \in \mathbb{Z}_q^{2\times 2}$. The following statements are equivalent:* (1) $\mathbf{W}$ *is nondegenerate;* (2) $\mathbf{x} \mapsto \mathbf{W}\mathbf{x}$ *is a bijection from $\mathbb{Z}_q^2$ to itself; and* (3) $\det(\mathbf{W})$ *is invertible in $\mathbb{Z}_q$.*

DEFINITION 6.6 (generalized Fourier matrix). *Let q be a prime power and $\mathbf{W} = (W_{ij})$ be a symmetric nondegenerate matrix in $\mathbb{Z}_q^{2\times 2}$. We say a $q^2 \times q^2$ matrix $\boldsymbol{\mathcal{F}}_{q,\mathbf{W}}$ is a $(q, \mathbf{W})$*-generalized Fourier matrix *if there exists a bijection ρ from $[0 : q^2 - 1]$ to $[0 : q - 1]^2$ such that*

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

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

THEOREM 6.7. *Suppose $((M, N), \mathbf{F}, \mathfrak{D})$ satisfies conditions $(\mathcal{U}_1')$–$(\mathcal{U}_5')$. Then either $\mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ is #P-hard or there exists a permutation Σ of $[0 : m - 1]$ such that*

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

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

Assume there does exist a permutation Σ, together with the four sequences, 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 rth matrix of $\mathfrak{D}_\Sigma$ is

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

It is clear that $\mathsf{EVAL}(\mathbf{F}_{\Sigma,\Sigma}, \mathfrak{D}_\Sigma) \equiv \mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$. From now on, we simply let $\mathbf{F}$ and $\mathfrak{D}$ denote $\mathbf{F}_{\Sigma,\Sigma}$ and $\mathfrak{D}_\Sigma$, respectively. Thus, we have

$$\mathbf{F} = \left(\bigotimes_{i=1}^{g} \boldsymbol{\mathcal{F}}_{d_i,\mathbf{W}^{[i]}}\right) \otimes \left(\bigotimes_{i=1}^{\ell} \boldsymbol{\mathcal{F}}_{q_i,k_i}\right). \tag{6.1}$$

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 (6.1), 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 nonincreasing sequence of powers of 2 for some $g \geq 0$; $\mathcal{W} = (\mathbf{W}^{[1]}, \ldots, \mathbf{W}^{[g]})$ is a sequence of symmetric nondegenerate 2×2 matrices over $\mathbb{Z}_{d_i}$ (note that $\mathbf{d}$ and $\mathcal{W}$ can be empty); $\mathbf{p} = (p_1, \ldots, p_s)$ is a strictly increasing sequence of s primes for some $s \geq 1$, starting with $p_1 = 2$; $\mathbf{t} = (t_1, \ldots, t_s)$ is a sequence of integers with $t_1 \geq 0$ and $t_i \geq 1$ for all $i > 1$; $\mathcal{Q} = \{\mathbf{q}_i : i \in [s]\}$ is a collection of

sequences in which each $\mathbf{q}_i = (q_{i,1}, \ldots, q_{i,t_i})$ is a nonincreasing sequence of powers of p_i (only $\mathbf{q}_1$ can be empty as we always fix $p_1 = 2$ even when no powers of 2 occur in $\mathcal{Q}$); $\mathcal{K} = \{\mathbf{k}_i : i \in [s]\}$ is a collection of sequences in which each $\mathbf{k}_i = (k_{i,1}, \ldots, k_{i,t_i})$ is a sequence of length t_i. Finally, for all $i \in [s]$ and $j \in [t_i]$, $k_{i,j} \in [0 : q_{i,j} - 1]$ and satisfies $\gcd(k_{i,j}, q_{i,j}) = \gcd(k_{i,j}, p_i) = 1$.

$(\mathcal{R}'_2)$ $((M, N), \mathbf{F}, \mathfrak{D})$ satisfies conditions $(\mathcal{U}'_1)$–$(\mathcal{U}'_5)$, 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 bijection 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 each $a \in [0 : m-1]$, we use

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

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

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

for all $a, b \in [0 : m-1]$, where $((x_{0,i,j}), (x_{1,i,j})) = \mathbf{x} = \rho(a)$ and $\mathbf{y} = \rho(b)$.

For convenience, from now on we will directly use $\mathbf{x} \in \mathbb{Z}^2_{\mathbf{d}} \times \mathbb{Z}_{\mathcal{Q}}$ to index the rows and columns of $\mathbf{F}$, i.e., $F_{\mathbf{x},\mathbf{y}} \equiv F_{\rho^{-1}(\mathbf{x}),\rho^{-1}(\mathbf{y})}$.

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 $(\mathcal{R}')$. In the next step, we show for every $r \in [N-1]$ ($\mathbf{D}^{[0]}$ is already known to be the identity matrix) the nonzero entries of $\mathbf{D}^{[r]}$ (in $\mathfrak{D}$) must have a coset structure; otherwise $\mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ is #P-hard.

For each $r \in [N-1]$, let $\Gamma_r \subseteq \mathbb{Z}^2_{\mathbf{d}} \times \mathbb{Z}_{\mathcal{Q}}$ denote the set of $\mathbf{x}$ such that the entry of $\mathbf{D}^{[r]}$ indexed by $\mathbf{x}$ is nonzero. We also use $\mathcal{Z}$ to denote the set of $r \in [N-1]$ such that $\Gamma_r \neq \emptyset$. For convenience, we let $\tilde{\mathbb{Z}}_{\mathbf{q}_i}$, $i \in [s]$, denote the following set (or group):

$$\tilde{\mathbb{Z}}_{\mathbf{q}_i} = \begin{cases} \mathbb{Z}_{\mathbf{q}_i} & \text{if } i > 1, \\ \mathbb{Z}^2_{\mathbf{d}} \times \mathbb{Z}_{\mathbf{q}_1} & \text{if } i = 1. \end{cases}$$

This gives us a new way to denote the components of

$$\mathbf{x} \in \mathbb{Z}^2_{\mathbf{d}} \times \mathbb{Z}_{\mathcal{Q}} = \tilde{\mathbb{Z}}_{\mathbf{q}_1} \times \tilde{\mathbb{Z}}_{\mathbf{q}_2} \times \cdots \times \tilde{\mathbb{Z}}_{\mathbf{q}_s},$$

i.e., $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_s)$, where $\mathbf{x}_i \in \tilde{\mathbb{Z}}_{\mathbf{q}_i}$ for each $i \in [s]$.

THEOREM 6.8. *Assume that* $((M, N), \mathbf{F}, \mathfrak{D}, (\mathbf{d}, \mathcal{W}, \mathbf{p}, \mathbf{t}, \mathcal{Q}, \mathcal{K}))$ *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* $r \in \mathcal{Z}$, $\Gamma_r = \prod_{i=1}^{s} \Gamma_{r,i}$, *where* $\Gamma_{r,i}$ *is a coset in* $\tilde{\mathbb{Z}}_{\mathbf{q}_i}$ *for all* $i \in [s]$.

Suppose $\mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ is not #P-hard. Then by Theorem 6.8, 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 $(\mathcal{U}'_3)$, $\mathfrak{D}$ also satisfies the following:

$(\mathcal{L}'_2)$ For every $r \in \mathcal{Z}$, there exists an $\mathfrak{a}^{[r]} \in \Gamma_r \subseteq \mathbb{Z}^2_{\mathbf{d}} \times \mathbb{Z}_{\mathcal{Q}}$ such that the entry of $\mathbf{D}^{[r]}$ indexed by $\mathfrak{a}^{[r]}$ is equal to 1.

From now on, we refer to conditions $(\mathcal{L}'_1)$ and $(\mathcal{L}'_2)$ as condition $(\mathcal{L}')$.

6.3.4. Step 3.4: Quadratic structure. In this final step within Step 3 for the nonbipartite case, we show that for any index $r \in [N-1]$, the nonzero 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 $\tilde{\mathbb{Z}}_{\mathbf{q}_i}$ for some $i \in [s]$, we let $\mathbf{ext}_r(\mathbf{x})$, where $r \in \mathcal{Z}$, denote the following unique vector:

$$\left(\mathfrak{a}_1^{[r]}, \ldots, \mathfrak{a}_{i-1}^{[r]}, \mathbf{x}, \mathfrak{a}_{i+1}^{[r]}, \ldots, \mathfrak{a}_s^{[r]}\right) \in \prod_{j \in [s]} \tilde{\mathbb{Z}}_{\mathbf{q}_j}.$$

Given $\mathbf{a} \in \tilde{\mathbb{Z}}_{\mathbf{q}_i}$ for some $i \in [s]$, we let $\widetilde{\mathbf{a}} = (\widetilde{\mathbf{a}}_1, \ldots, \widetilde{\mathbf{a}}_s) \in \prod_{j \in [s]} \tilde{\mathbb{Z}}_{\mathbf{q}_j}$ such that $\widetilde{\mathbf{a}}_i = \mathbf{a}$ and all other components are $\mathbf{0}$.

THEOREM 6.9. *Suppose* $((M,N), \mathbf{F}, \mathfrak{D}, (\mathbf{d}, \mathcal{W}, \mathbf{p}, \mathbf{t}, \mathcal{Q}, \mathcal{K}))$ *satisfies* $(\mathcal{R}')$ *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 all* $r \in \mathcal{Z}$ *and* $\mathbf{x} \in \Gamma_r$*, we have*

$$D^{[r]}_{\mathbf{x}} = D^{[r]}_{\mathbf{ext}_r(\mathbf{x}_1)} D^{[r]}_{\mathbf{ext}_r(\mathbf{x}_2)} \cdots D^{[r]}_{\mathbf{ext}_r(\mathbf{x}_s)}. \tag{6.2}$$

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

$$\omega_N^{\alpha} \cdot F_{\widetilde{\mathbf{b}},\mathbf{x}} = D^{[r]}_{\mathbf{x}+\widetilde{\mathbf{a}}} \cdot \overline{D^{[r]}_{\mathbf{x}}} \quad \text{for all } \mathbf{x} \in \Gamma_r. \tag{6.3}$$

Note that in (6.3), the expression on the left-hand side does not depend on other components of $\mathbf{x}$ except the kth component $\mathbf{x}_k \in \tilde{\mathbb{Z}}_{\mathbf{q}_k}$.

6.4. Tractability.

THEOREM 6.10. *Let* $((M,N), \mathbf{F}, \mathfrak{D}, (\mathbf{d}, \mathcal{W}, \mathbf{p}, \mathbf{t}, \mathcal{Q}, \mathcal{K}))$ *be a tuple that satisfies all conditions* $(\mathcal{R}'), (\mathcal{L}')$*, and* $(\mathcal{D}')$*. Then* $\mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ *can be solved in polynomial time.*

7. Proofs of Theorems 5.2 and 6.2. In this section, we prove Theorems 5.2 and 6.2. Let $\mathbf{A} = (A_{i.j})$ denote a connected, symmetric $m \times m$ algebraic matrix. (At this moment, we do not make any assumptions about whether $\mathbf{A}$ is bipartite.) We also let $\mathscr{A} = \{A_{i,j} : i, j \in [m]\}$ denote the finite set of algebraic numbers from the entries of $\mathbf{A}$. 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 connected and symmetric (so that $\mathsf{EVAL}(\mathbf{B})$ is well-defined);
2. $\mathsf{EVAL}(\mathbf{B}) \equiv \mathsf{EVAL}(\mathbf{A})$; and
3. each entry of $\mathbf{B}$ is the product of a nonnegative integer and a root of unity.

We let $\mathbf{B}'$ be the nonnegative matrix such that $B'_{i,j} = |B_{i,j}|$. In the second step, we show that $\mathsf{EVAL}(\mathbf{B}') \leq \mathsf{EVAL}(\mathbf{B})$. Because $\mathbf{B}'$ is a connected, symmetric, and nonnegative (integer) matrix, we can apply the dichotomy of Bulatov and Grohe [4] (see Theorem 2.5) to $\mathbf{B}'$ and show that either $\mathsf{EVAL}(\mathbf{B}')$ is #P-hard or $\mathbf{B}$ is a (bipartite or nonbipartite, depending on $\mathbf{A}$) *purified* matrix. When $\mathsf{EVAL}(\mathbf{B}')$ is #P-hard, we have $\mathsf{EVAL}(\mathbf{B}') \leq \mathsf{EVAL}(\mathbf{B}) \equiv \mathsf{EVAL}(\mathbf{A})$ and thus $\mathsf{EVAL}(\mathbf{A})$ is #P-hard as well. This proves both Theorems 5.2 and 6.2.

7.1. Equivalence between $\mathsf{EVAL}(\mathbf{A})$ and $\mathsf{COUNT}(\mathbf{A})$. Before the construction of $\mathbf{B}$, we define a class of counting problems closely related to $\mathsf{EVAL}(\mathbf{A})$. It has been used in previous work [21] for establishing polynomial-time reductions between different EVAL problems.

Let $\mathbf{A} \in \mathbb{C}^{m \times m}$ be any fixed symmetric matrix with algebraic entries. The input of the problem $\mathsf{COUNT}(\mathbf{A})$ is a pair (G, x), where $G = (V, E)$ is an undirected graph and $x \in \mathbb{Q}(\mathscr{A})$. The output is

$$\#_{\mathbf{A}}(G,x) = \left|\left\{\text{assignment } \xi : V \to [m] \;\middle|\; \mathrm{wt}_{\mathbf{A}}(\xi) = x\right\}\right|,$$

a nonnegative integer. We prove the following lemma.

LEMMA 7.1. $\mathsf{EVAL}(\mathbf{A}) \equiv \mathsf{COUNT}(\mathbf{A})$.

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

$$X = \left\{ \prod_{i,j\in[m]} A_{i,j}^{k_{i,j}} \;\middle|\; \text{integers } k_{i,j} \geq 0 \text{ and } \sum_{i,j\in[m]} k_{i,j} = n \right\}. \tag{7.1}$$

It is clear that $|X|$ is polynomial in n, being $\binom{n+m^2-1}{m^2-1}$ counting multiplicity, and X can be enumerated in polynomial time (in n). It follows from the expression in the definition of $\mathrm{wt}_{\mathbf{A}}(\xi)$ that for any $x \notin X$, $\#_{\mathbf{A}}(G,x) = 0$. This implies that

$$Z_{\mathbf{A}}(G) = \sum_{x\in X} x \cdot \#_{\mathbf{A}}(G,x)$$

for any undirected graph G and thus $\mathsf{EVAL}(\mathbf{A}) \leq \mathsf{COUNT}(\mathbf{A})$.

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 any assignment ξ that has weight x over G has weight x^p over $G^{[p]}$. This gives us the following collection of equations: For every $p \in [|X|]$,

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

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 nonzero $x \in X$. We can also derive $\#_{\mathbf{A}}(G,0)$, if $0 \in X$, using the fact that the $\#_{\mathbf{A}}(G,x)$'s sum to $m^{|V|}$. ∎

7.2. Step 1.1. We now construct the desired matrix $\mathbf{B}$ from $\mathbf{A}$. We need the following notion of a *generating set*.

DEFINITION 7.2. *Let $\mathscr{A} = \{a_1, \ldots, a_n\}$ be a set of n nonzero algebraic numbers for some $n \geq 1$. We say $\{g_1, \ldots, g_d\}$ for some $d \geq 0$ is a* generating set *of $\mathscr{A}$ if*

1. *every g_i is a nonzero algebraic number in $\mathbb{Q}(\mathscr{A})$, and*
2. *for every $a \in \mathscr{A}$, there exists a* unique *tuple $(k_1, \ldots, k_d) \in \mathbb{Z}^d$ 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. It can also be derived from the definition that $g_1^{k_1} \cdots g_d^{k_d}$ of any nonzero $(k_1, \ldots, k_d) \in \mathbb{Z}^d$ cannot be a root of unity. We prove the following lemma.

LEMMA 7.3. *Every set $\mathscr{A}$ of nonzero algebraic numbers has a generating set.*

Lemma 7.3 follows directly from Theorem 17.1. Actually the statement of Theorem 17.1 is stronger: A generating set $\{g_1, g_2, \ldots, g_d\}$ can be computed from $\mathscr{A}$ in polynomial time. More precisely, following the model of computation discussed in section 2.2, we let α be a primitive element of $\mathbb{Q}(\mathscr{A})$ so that $\mathbb{Q}(\mathscr{A}) = \mathbb{Q}(\alpha)$ and let $F(x)$ be a minimal polynomial of α. Then Theorem 17.1 shows that given the

standard representation of the a_j's, one can compute the standard representation of $g_1 \ldots, g_d \in \mathbb{Q}(\alpha)$ in polynomial time in the input size of the a_j's with $\{g_1, \ldots, g_d\}$ being a generating set of $\mathscr{A}$. Moreover, for each element $a \in \mathscr{A}$ one can also compute in polynomial time the unique tuple of integers $(k_1, \ldots, k_d)$ such that $a/(g_1^{k_1} \cdots g_d^{k_d})$ is a root of unity. In addition, if we are given an approximation $\hat{\alpha}$ of α that uniquely determines α as a root of $F(x)$, then we can use it to determine which root of unity it is in polynomial time. Note that in Lemma 7.3 we only need the existence of a generating set $\{g_1, \ldots, g_d\}$. But later in section 17, the polynomial-time computability of a generating set will be critical to the proof of Theorem 1.2, the polynomial-time decidability of the dichotomy criterion.

Now we return to the construction of $\mathbf{B}$. Letting $\mathscr{A}$ denote the set of nonzero entries of $\mathbf{A}$, by Lemma 7.3, $\mathscr{A}$ has a generating set $\mathscr{G} = \{g_1, \ldots, g_d\}$. The matrix $\mathbf{B} = (B_{i,j})$ is constructed as follows. Let $p_1 < \cdots < p_d$ denote the d smallest primes. For every $i, j \in [m]$, $B_{i,j} = 0$ if $A_{i,j} = 0$. Suppose $A_{i,j} \neq 0$. Since $\mathscr{G}$ is a generating set, we know there exists a unique tuple of integers $(k_1, \ldots, k_d)$ such that

$$\zeta_{i,j} = \frac{A_{i,j}}{g_1^{k_1} \cdots g_d^{k_d}}$$

is a root of unity. Then we set $B_{i,j} = p_1^{k_1} \cdots p_d^{k_d} \cdot \zeta_{i,j}$.

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

LEMMA 7.4. *Let $\mathbf{A} \in \mathbb{C}^{m \times m}$ be a symmetric and connected matrix with algebraic entries and let $\mathbf{B}$ be the $m \times m$ matrix constructed above. Then* $\mathsf{EVAL}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{B})$.

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

Let (G, x) be an input pair of $\mathsf{COUNT}(\mathbf{A})$, where $G = (V, E)$ and $n = |E|$. We use X to denote the set of algebraic numbers defined earlier in (7.1). 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.

Suppose $x \in X$. Then we can find a particular sequence of nonnegative integers $(k^*_{i,j} : i, j \in [m])$ in polynomial time such that $\sum_{i,j} k^*_{i,j} = n$ and

$$x = \prod_{i,j \in [m]} A_{i,j}^{k^*_{i,j}}. \tag{7.2}$$

Note that $(k^*_{i,j})$ is in general *not unique* for the given x. Using $(k^*_{i,j})$, we define y by

$$y = \prod_{i,j \in [m]} B_{i,j}^{k^*_{i,j}}. \tag{7.3}$$

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:

$$\#_{\mathbf{A}}(G, x) = \#_{\mathbf{B}}(G, y). \tag{7.4}$$

To prove this claim, it suffices to show that for any assignment $\xi\colon V \to [m]$, $\mathrm{wt}_{\mathbf{A}}(\xi) = x$ iff $\mathrm{wt}_{\mathbf{B}}(\xi) = y$. Here we only show that $\mathrm{wt}_{\mathbf{A}}(\xi) = x$ implies $\mathrm{wt}_{\mathbf{B}}(\xi) = y$. The other direction can be proved similarly.

Let $\xi\colon V \to [m]$ denote an 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

$$\mathrm{wt}_{\mathbf{A}}(\xi) = \prod_{i,j\in[m]} A_{i,j}^{k_{i,j}} \quad \text{and} \quad \mathrm{wt}_{\mathbf{B}}(\xi) = \prod_{i,j\in[m]} B_{i,j}^{k_{i,j}}. \tag{7.5}$$

For $x = 0$, we note that the weight $\mathrm{wt}_{\mathbf{A}}(\xi)$ 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 $\mathrm{wt}_{\mathbf{B}}(\xi) = 0$.

In the following, we assume both $x, y \neq 0$. We only consider assignments ξ 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 (7.5) are over nonzero entries $A_{i,j}$ and $B_{i,j}$, respectively.

Now we use the generating set $\mathscr{G} = \{g_1, \dots, g_d\}$ chosen for $\mathscr{A}$. There are integer exponents $e_{1,i,j}, e_{2,i,j}, \dots, e_{d,i,j}$ and roots of unity $\zeta_{i,j}$ such that for all $A_{i,j} \neq 0$,

$$A_{i,j} = \prod_{\ell=1}^{d} g_\ell^{e_{\ell,i,j}} \cdot \zeta_{i,j} \quad \text{and} \quad B_{i,j} = \prod_{\ell=1}^{d} p_\ell^{e_{\ell,i,j}} \cdot \zeta_{i,j}.$$

The expression of $B_{i,j}$ here follows from the construction of $\mathbf{B}$. By (7.2) and (7.5),

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

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

$$\sum_{i,j} (k_{i,j} - k^*_{i,j}) \cdot e_{\ell,i,j} = 0 \quad \text{for all } \ell \in [d], \tag{7.6}$$

which in turn implies that

$$\prod_{i,j} \left(\zeta_{i,j}\right)^{k_{i,j}} = \prod_{i,j} \left(\zeta_{i,j}\right)^{k^*_{i,j}}. \tag{7.7}$$

It then follows from (7.3), (7.5), (7.6), and (7.7) that $\mathrm{wt}_{\mathbf{B}}(\xi) = y$. ∎

7.3. Step 1.2. The following lemma holds for any symmetric $\mathbf{B} \in \mathbb{C}^{m\times m}$.

LEMMA 7.5. *If $B'_{i,j} = |B_{i,j}|$ for all $i, j \in [m]$, then $\mathsf{EVAL}(\mathbf{B}') \le \mathsf{EVAL}(\mathbf{B})$.*

Proof. From Lemma 7.1, it suffices to show that $\mathsf{COUNT}(\mathbf{B}') \le \mathsf{COUNT}(\mathbf{B})$. Let (G, x) be an input of $\mathsf{COUNT}(\mathbf{B}')$. As $\mathbf{B}'$ is nonnegative, 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

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

We know that $|Y|$ is polynomial in n, and Y can be enumerated in polynomial time in n. Let Y_x denote the set of elements of Y whose complex norm is x.

The lemma then follows directly from the equation

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

because for every assignment $\xi\colon V \to [m]$, $\mathrm{wt}_{\mathbf{B}'}(\xi) = x$ iff $|\mathrm{wt}_{\mathbf{B}}(\xi)| = x$. 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 Theorems 5.2 and 6.2.

Proof of Theorem 5.2. 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. Thus, we know there is a permutation Π of $[m]$ such that $\mathbf{B}_{\Pi,\Pi}$ is the bipartization of a $k \times (m-k)$ matrix $\mathbf{F}$ for some $k \in [m-1]$, and $\mathbf{B}'_{\Pi,\Pi}$ is the bipartization 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

$$\mathsf{EVAL}(\mathbf{B}'_{\Pi,\Pi}) \le \mathsf{EVAL}(\mathbf{B}_{\Pi,\Pi}) \equiv \mathsf{EVAL}(\mathbf{B}) \equiv \mathsf{EVAL}(\mathbf{A}). \tag{7.8}$$

As $\mathbf{B}'_{\Pi,\Pi}$ is nonnegative, by Bulatov and Grohe we have the following cases:

1. If $\mathsf{EVAL}(\mathbf{B}'_{\Pi,\Pi})$ is #P-hard, then by (7.8), $\mathsf{EVAL}(\mathbf{A})$ is also #P-hard.
2. 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 $\mathbf{A}$ is assumed to be connected and bipartite.) Thus, there exist nonnegative rational numbers $\mu_1, \ldots, \mu_m$ such that $F'_{i,j} = \mu_i \mu_{j+k}$ for all $i \in [k]$ and $j \in [m-k]$. Moreover, $\mu_i \neq 0$ for all $i \in [m]$ 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 proved. □

Proof of Theorem 6.2. Let $\mathbf{A} \in \mathbb{C}^{m\times m}$ be a symmetric, connected, and nonbipartite matrix. We construct $\mathbf{B}$ and $\mathbf{B}'$ as above. Since $\mathbf{A}$ is connected and non-bipartite, $\mathbf{B}$ and $\mathbf{B}'$ are connected and nonbipartite. Also, $\mathbf{B}'$ is nonnegative. Consider the following 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 by Bulatov and Grohe, the rank of $\mathbf{B}$ is 1. (It cannot be 0 as we assumed $m > 1$, and $\mathbf{B}$ is connected.) Because $\mathbf{B}$ is symmetric, it is a purified nonbipartite matrix. The theorem follows. □

8. Proof of Theorem 5.3. We start the section by introducing a technique for establishing reductions between problems $\mathsf{EVAL}(\mathbf{A})$ and $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$. It was inspired by the twin reduction lemma proved in [21].

8.1. Cyclotomic reduction and inverse cyclotomic reduction. Let $\mathbf{A}$ be an $m \times m$ symmetric (but not necessarily bipartite) complex matrix, and 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 complex matrices for some $N \ge 1$.

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

$$D^{[0]}_a = \sum_{b=0}^{N-1} \alpha_{a,b} \quad \text{and} \quad D^{[r]}_a = \sum_{b=0}^{N-1} \alpha_{a,b} \cdot \omega_N^{br} \quad \text{for all } r \in [N-1].$$

In particular, we say that the tuple $(\alpha_{a,0},\dots,\alpha_{a,N-1})$ *generates* the ath entries of $\mathfrak{D}$.

We need the following definition.

DEFINITION 8.1. *Let $\mathscr{R}=\{R_{a,b}: a\in[n], b\in[0:N-1]\}$ be a partition of $[m]$ (note that any $R_{a,b}$ here may be empty) such that for every $a\in[n]$,*

$$\bigcup_{b=0}^{N-1} R_{a,b}\neq\emptyset.$$

We say $\mathbf{A}$ *can be* generated *by* $\mathbf{C}$ *using $\mathscr{R}$ if for all $i,j\in[m]$,*

$$A_{i,j}=C_{a,a'}\cdot\omega_N^{b+b'},\qquad \text{where } i\in R_{a,b} \text{ and } j\in R_{a',b'}. \tag{8.1}$$

Given any pair $(\mathbf{C},\mathfrak{D})$ that satisfies $(\mathcal{T})$, we prove the following lemma.

LEMMA 8.2 (cyclotomic reduction lemma). *Assume that $(\mathbf{C},\mathfrak{D})$ satisfies $(\mathcal{T})$ with nonnegative integers $\alpha_{a,b}$. Let $\mathscr{R}=\{R_{a,b}\}$ be a partition of $[m]$ satisfying*

$$|R_{a,b}|=\alpha_{a,b}\quad \text{and}\quad m=\sum_{a=1}^{n}\sum_{b=0}^{N-1}\alpha_{a,b}\geq n,$$

and let $\mathbf{A}$ denote the matrix generated by $\mathbf{C}$ using $\mathscr{R}$. Then $\mathsf{EVAL}(\mathbf{A})\equiv\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$.

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

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

are exactly the same. To this end, 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 that for every $\eta\colon V\to[n]$,

$$\mathrm{wt}_{\mathbf{C},\mathfrak{D}}(\eta)=\sum_{\xi:\rho(\xi)=\eta}\mathrm{wt}_{\mathbf{A}}(\xi). \tag{8.2}$$

We define $\rho(\xi)$ as follows. As $\mathscr{R}$ is a partition of $[m]$, for each $v\in V$ there exists a unique pair $(a(v),b(v))$ such that $\xi(v)\in R_{a(v),b(v)}$. Let $\eta(v)=a(v)$ for each v, and let $\rho(\xi)=\eta$. It is easy to check that ρ is surjective. To prove (8.2), we write $\mathrm{wt}_{\mathbf{A}}(\xi)$ as

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

It follows that

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

and the lemma follows. ∎

By combining Lemmas 8.2 and 7.5, as well as the dichotomy theorem of Bulatov and Grohe, we have the following handy corollary for dealing with $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$.

COROLLARY 8.3 (inverse cyclotomic reduction lemma). *Let $(\mathbf{C}, \mathfrak{D})$ be a pair that satisfies condition $(\mathcal{T})$. If $\mathbf{C}$ has a 2×2 submatrix*

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

such that all four entries are nonzero and $|C_{i,k}C_{j,\ell}| \neq |C_{i,\ell}C_{j,k}|$, then $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is #P-hard.

Proof. By the cyclotomic reduction lemma, there is a symmetric $m \times m$ matrix $\mathbf{A}$ for some positive integer m and a partition $\mathscr{R}$ of $[m]$, where

$$\mathscr{R} = \left\{ R_{a,b} \;\middle|\; a \in [n], b \in [0 : N-1] \right\} \quad \text{and} \quad \bigcup_{b=0}^{N-1} R_{a,b} \neq \emptyset \quad \text{for all } a \in [n], \tag{8.3}$$

such that $\mathsf{EVAL}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$. Moreover, $\mathbf{A}$ and $\mathbf{C}$ satisfy (8.1).

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 nonzero and $|C_{i,k}C_{j,\ell}| \neq |C_{i,\ell}C_{j,k}|$. We arbitrarily pick an i' from $\cup_b R_{i,b}$ (known to be nonempty), a j' from $\cup_b R_{j,b}$, a k' from $\cup_b R_{k,b}$, and an ℓ' from $\cup_b R_{\ell,b}$. Then from (8.1), we have $|A_{i',k'}| = |C_{i,k}|$, $|A_{i',\ell'}| = |C_{i,\ell}|$, $|A_{j',k'}| = |C_{j,k}|$, $|A_{j',\ell'}| = |C_{j,\ell}|$, and

$$|A_{i',k'}A_{j',\ell'}| \neq |A_{i',\ell'}A_{j',k'}|.$$

Let $\mathbf{A}' = (|A_{i,j}|)$ for all $i, j \in [m]$. Then $\mathbf{A}'$ has a 2×2 submatrix of rank 2 and all its four entries are nonzero. By the dichotomy of Bulatov and Grohe (Corollary 2.6), $\mathsf{EVAL}(\mathbf{A}')$ is #P-hard. It follows that $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is #P-hard, since $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D}) \equiv \mathsf{EVAL}(\mathbf{A})$ and by Lemma 7.5, $\mathsf{EVAL}(\mathbf{A}') \leq \mathsf{EVAL}(\mathbf{A})$. ∎

Combining Lemma 8.2, (8.2), and the first pinning lemma (Lemma 4.1), we get the following.

COROLLARY 8.4 (third pinning lemma). *Let $(\mathbf{C}, \mathfrak{D})$ be a pair that satisfies $(\mathcal{T})$. Then we have $\mathsf{EVALP}(\mathbf{C}, \mathfrak{D}) \equiv \mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$. 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. It suffices to show that $\mathsf{EVALP}(\mathbf{C}, \mathfrak{D}) \leq \mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$. By the cyclotomic reduction lemma, 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 (8.3) and $\mathsf{EVAL}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$. $\mathbf{A}, \mathbf{C}$, and $\mathscr{R}$ also satisfy (8.1). 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 (8.2), 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 $\mathsf{EVALP}(\mathbf{A})$. ∎

Note that compared to the second pinning lemma, the third pinning lemma does not require $\mathbf{C}$ to be the bipartization of a unitary matrix. It only requires $(\mathcal{T})$.

8.2. Step 2.1. Let $\mathbf{A}$ be a purified bipartite matrix. After collecting its entries of equal norm in decreasing order by permuting its rows and columns, 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:

($\mathcal{S}_1$) $\mathbf{A}$ is the bipartization 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 strictly decreasing sequences of positive rational numbers where $s \geq 1$ and $t \geq 1$. $\mathbf{m} = (m_1, \ldots, m_s)$ and $\mathbf{n} = (n_1, \ldots, n_t)$ 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 $x_2 \in [m_{x_1}]$; the columns of $\mathbf{B}$ are indexed by $\mathbf{y} = (y_1, y_2)$, where $y_1 \in [t]$ and $y_2 \in [n_{y_1}]$. We have, for all $\mathbf{x}, \mathbf{y}$,

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

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

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

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

We let

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

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

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

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

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

denotes the ith block of the $\mathbf{y}$th column vector of $\mathbf{S}$.

LEMMA 8.5. *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* $j \in [t]$, $\langle \mathbf{S}_{\mathbf{x},(j,*)}, \mathbf{S}_{\mathbf{x}',(j,*)} \rangle = 0$.

($\mathcal{S}_3$) *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* $i \in [s]$, $\langle \mathbf{S}_{(i,*),\mathbf{y}}, \mathbf{S}_{(i,*),\mathbf{y}'} \rangle = 0$.

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

Let $G = (V, E)$ be an undirected graph. We construct a new graph $G^{[p]}$ for each $p \geq 1$ by replacing every edge uv in E with a gadget shown in Figure 8.1. Formally we define graph $G^{[p]} = (V^{[p]}, E^{[p]})$ as

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

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

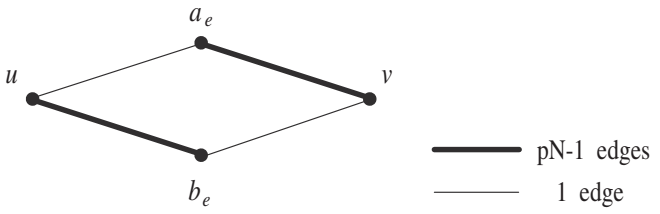

FIG. 8.1. *Gadget for constructing graph* $G^{[p]}$, $p \geq 1$.

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

The construction of $G^{[p]}$ 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 $\mathsf{EVAL}(\mathbf{A}^{[p]}) \le \mathsf{EVAL}(\mathbf{A})$, 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 two 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

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

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, we have

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

It is clear that the upper-left $m\times m$ block of $\mathbf{A}^{[p]}$ is nonnegative. This holds for its lower-right $n\times n$ block as well, so $\mathbf{A}^{[p]}$ is a nonnegative matrix.

Now let $\mathbf{u} \ne \mathbf{v}$ be two indices in I (if $|I| = 1$, $(\mathcal{S}_2)$ 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 Bulatov and Grohe (Corollary 2.6),

$$\left|\sum_{i\in[t]}\nu_i^{pN}\langle \mathbf{S}_{\mathbf{u},(i,*)}, \mathbf{S}_{\mathbf{v},(i,*)}\rangle\right| \in \left\{0, \sum_{i\in[t]} n_i\cdot\nu_i^{pN}\right\}. \tag{8.4}$$

On the other hand, the following inequality always holds: For any $p \geq 1$,

$$\left| \sum_{i \in [t]} \nu_i^{pN} \cdot \langle \mathbf{S}_{\mathbf{u},(i,*)}, \mathbf{S}_{\mathbf{v},(i,*)} \rangle \right| \leq \sum_{i \in [t]} n_i \cdot \nu_i^{pN}. \tag{8.5}$$

For the equality of (8.5) to hold, $\mathbf{S}$ must satisfy $|\langle \mathbf{S}_{\mathbf{u},(i,*)}, \mathbf{S}_{\mathbf{v},(i,*)} \rangle| = n_i$ for all $i \in [t]$ and thus $\mathbf{S}_{\mathbf{u},(i,*)} = (\omega_N)^{k_i} \cdot \mathbf{S}_{\mathbf{v},(i,*)}$ for some $k_i \in [0 : N-1]$. Furthermore, these k_i's must be the same. As a result, $\mathbf{S}_{\mathbf{u},*}$ and $\mathbf{S}_{\mathbf{v},*}$ are linearly dependent, which contradicts our assumption. It then follows from (8.4) that

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

As $\nu_1, \ldots, \nu_t$ is strictly decreasing, these equations form a Vandermonde system. It follows that $\langle \mathbf{S}_{\mathbf{u},(i,*)}, \mathbf{S}_{\mathbf{v},(i,*)} \rangle = 0$ for all $i \in [t]$. This finishes the proof of $(\mathcal{S}_2)$. ∎

We have the following corollary.

COROLLARY 8.6. *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 the same rank as $\mathbf{S}$.*

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

First, we use Lemma 8.5 to show that

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

To see this, we take any $h = \operatorname{rank}(\mathbf{S})$ 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

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

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

Now suppose $h = \operatorname{rank}(\mathbf{S})$. Then by Corollary 8.6, there must exist indices $1 \leq i_1 < \cdots < i_h \leq m_1$ and $1 \leq j_1 < \cdots < j_h \leq n_1$ such that the $\{(1,i_1), \ldots, (1,i_h)\} \times \{(1,j_1), \ldots, (1,j_h)\}$ submatrix 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 8.6 and Lemma 8.5, for every index $\mathbf{x} \in I$, there exists a unique pair of integers $j \in [h]$ and $k \in [0 : N-1]$ such that

$$\mathbf{S}_{\mathbf{x},*} = \omega_N^k \cdot \mathbf{S}_{(1,j),*}. \tag{8.6}$$

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

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

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 (8.6). By Corollary 8.6,

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

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

$$\mathbf{S}_{*,\mathbf{y}} = \omega_N^k \cdot \mathbf{S}_{*,(1,j)}, \tag{8.7}$$

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

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

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 (8.7). By Corollary 8.6,

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

Now we define $(\mathbf{C}, \mathfrak{D})$ and use the cyclotomic reduction lemma (Lemma 8.2) 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 bipartization of an $sh \times th$ matrix $\mathbf{F}$. We use the 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,

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

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

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

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

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

This finishes the construction of $(\mathbf{C}, \mathfrak{D})$, and we prove the following lemma.

LEMMA 8.7. $\mathsf{EVAL}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$.

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 bipartizations of $\mathbf{B}$ and $\mathbf{F}$, respectively. Therefore,

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

holds trivially. Clearly, this also holds 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'. By (8.6) and (8.7), we have

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

A similar equation also holds for the lower-left block. Thus, $\mathbf{A}$ can be generated from $\mathbf{C}$ using $\mathscr{R}_0 \cup \mathscr{R}_1$. Moreover, the construction of $\mathfrak{D}$ implies that $\mathfrak{D}$ can be generated from the partition $\mathscr{R}_0 \cup \mathscr{R}_1$. The lemma then follows directly from the cyclotomic reduction lemma. ∎

Before moving forward to the next step, we summarize our progress so far. We showed that $\mathsf{EVAL}(\mathbf{A})$ is either #P-hard or equivalent to $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$, where the pair $(\mathbf{C},\mathfrak{D})$ satisfies the following conditions ($Shape_1$)–($Shape_3$):

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

($Shape_2$) There are two strictly decreasing sequences $\boldsymbol{\mu} = (\mu_1,\dots,\mu_s)$ and $\boldsymbol{\nu} = (\nu_1,\dots,\nu_t)$ of positive rational numbers. There is also an $h \times h$ full-rank matrix $\mathbf{H}$ whose entries are all powers of ω_N for some positive integer N. Entries of $\mathbf{F}$ can be expressed using $\boldsymbol{\mu},\boldsymbol{\nu}$, and $\mathbf{H}$ explicitly as follows:

$$F_{\mathbf{x},\mathbf{y}} = \mu_{x_1}\nu_{y_1} H_{x_2,y_2} \quad \text{for all } \mathbf{x} \in I \text{ and } \mathbf{y} \in J.$$

($Shape_3$) $\mathfrak{D} = (\mathbf{D}^{[0]},\dots,\mathbf{D}^{[N-1]})$ is a sequence of $m \times m$ diagonal matrices. We use $(\{0\} \times I) \cup (\{1\} \times J)$ to index the rows and columns of matrices $\mathbf{C}$ and $\mathbf{D}^{[r]}$. $\mathfrak{D}$ satisfies ($\mathcal{T}_3$), so for all $r \in [N-1]$, $\mathbf{x} \in [s] \times [h]$, and $\mathbf{y} \in [t] \times [h]$,

$$D^{[r]}_{(0,\mathbf{x})} = \overline{D^{[N-r]}_{(0,\mathbf{x})}} \quad \text{and} \quad D^{[r]}_{(1,\mathbf{y})} = \overline{D^{[N-r]}_{(1,\mathbf{y})}}.$$

8.3. Step 2.2. In Step 2.2, we prove the following lemma.

LEMMA 8.8. *Either* $\mathsf{EVAL}(\mathbf{C},\mathfrak{D})$ *is #P-hard or* $\mathbf{H}$ *and* $\mathbf{D}^{[0]}$ *satisfy the following two conditions:*

($Shape_4$) $(1/\sqrt{h}) \cdot \mathbf{H}$ *is a unitary matrix, i.e.,*

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

($Shape_5$) $\mathbf{D}^{[0]}$ *satisfies, for all* $\mathbf{x} \in I$ *and for all* $\mathbf{y} \in J$,

$$D^{[0]}_{(0,\mathbf{x})} = D^{[0]}_{(0,(x_1,1))} \quad \textit{and} \quad D^{[0]}_{(1,\mathbf{y})} = D^{[0]}_{(1,(y_1,1))}.$$

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

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

and rearrange its entries indexed by $\{0\} \times I$ into an $s \times h$ matrix

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

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 8.9 that either $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is #P-hard or $\mathbf{H}, \mathbf{X}$, and $\mathbf{Y}$ must satisfy

$$\langle \mathbf{H}_{i,*} \circ \overline{\mathbf{H}_{j,*}}, \mathbf{X}_{k,*} \rangle = 0 \quad \text{for all } k \in [t] \text{ and } i \neq j \in [h] \quad \text{and} \tag{8.8}$$

$$\langle \mathbf{H}_{*,i} \circ \overline{\mathbf{H}_{*,j}}, \mathbf{Y}_{k,*} \rangle = 0 \quad \text{for all } k \in [s] \text{ and } i \neq j \in [h]. \tag{8.9}$$

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 $\mathbb{C}$.

Second, we show in Lemma 8.10 that, assuming (8.8) and (8.9), either

$$\langle \mathbf{H}_{i,*} \circ \overline{\mathbf{H}_{j,*}}, (\mathbf{X}_{k,*})^2 \rangle = 0 \quad \text{for all } k \in [t] \text{ and } i \neq j \in [h] \quad \text{and} \tag{8.10}$$

$$\langle \mathbf{H}_{*,i} \circ \overline{\mathbf{H}_{*,j}}, (\mathbf{Y}_{k,*})^2 \rangle = 0 \quad \text{for all } k \in [s] \text{ and } i \neq j \in [h], \tag{8.11}$$

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

Equations (8.8) and (8.10) 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 (8.8) and (8.9), 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 8.8. ∎

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

LEMMA 8.9. *Either* $\mathbf{H}, \mathbf{X}, \mathbf{Y}$ *satisfy* (8.8) *and* (8.9)*, or* $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ *is #P-hard.*

Proof. Suppose $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is not #P-hard; otherwise we are done.

We let $\mathfrak{D}^* = (\mathbf{D}^{[0]}, \ldots, \mathbf{D}^{[0]})$, a sequence of N $m \times m$ diagonal matrices in which every matrix is a copy of $\mathbf{D}^{[0]}$ (as in $\mathfrak{D}$). 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 8.5. This gives us an $m \times m$ matrix $\mathbf{C}^{[p]}$ such that $Z_{\mathbf{C}^{[p]}, \mathfrak{D}^*}(G) = Z_{\mathbf{C}, \mathfrak{D}}(G^{[p]})$ for all undirected graphs G. 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 with the same block 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

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

From ($Shape_2$) and the fact that all entries of $\mathbf{X}$ are positive integers, we can rewrite the first factor as

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

Similarly, we can rewrite the second factor as

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

Since $\nu_a>0$ for all a, we have

$$C^{[p]}_{(0,\mathbf{x}),(0,\mathbf{y})}=(\mu_{x_1}\mu_{y_1})^{pN}\left|\sum_{a\in[t]}(\nu_a)^{pN}\langle\mathbf{H}_{x_2,*}\circ\overline{\mathbf{H}_{y_2,*}},\mathbf{X}_{a,*}\rangle\right|^2, \tag{8.12}$$

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

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

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

which is positive, and for any $\mathbf{x}\neq\mathbf{y}\in I$, we have

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

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 8.3), we have either

$$\left(C^{[p]}_{(0,\mathbf{x}),(0,\mathbf{y})}\right)^2=C^{[p]}_{(0,\mathbf{x}),(0,\mathbf{x})}C^{[p]}_{(0,\mathbf{y}),(0,\mathbf{y})}\ \text{ or }\ C^{[p]}_{(0,\mathbf{x}),(0,\mathbf{y})}=0. \tag{8.13}$$

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

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

and the norm of $\langle\mathbf{H}_{x_2,*}\circ\overline{\mathbf{H}_{y_2,*}},\mathbf{X}_{a,*}\rangle$ must be $\sum_{b\in[h]}X_{a,b}$. The inner product, however, 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 $x_2=y_2$. Together with (8.13), we have

$$\sum_{a\in[t]}(\nu_a)^{pN}\langle\mathbf{H}_{x_2,*}\circ\overline{\mathbf{H}_{y_2,*}},\mathbf{X}_{a,*}\rangle=0\quad\text{for all } p\geq1 \text{ and all } x_2\neq y_2,$$

since the argument is independent of the value of p. These equations form a Vandermonde system, and we conclude that $\langle\mathbf{H}_{x_2,*}\circ\overline{\mathbf{H}_{y_2,*}},\mathbf{X}_{a,*}\rangle=0$ for all $a\in[t]$ and all $x_2\neq y_2$. This finishes the proof of (8.8). Equation (8.9) can be proved similarly. ∎

In the second stage, we prove the following lemma.

LEMMA 8.10. *Suppose matrices* $\mathbf{H}$, $\mathbf{X}$, *and* $\mathbf{Y}$ *satisfy both* (8.8) *and* (8.9). *Then either they also satisfy* (8.10) *and* (8.11) *or* $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ *is #P-hard.*

Proof. We will only prove (8.11). Equation (8.10) can be proved similarly.

Again, we let $\mathfrak{D}^*$ denote a sequence of N $m \times m$ diagonal matrices in which each matrix is a copy of $\mathbf{D}^{[0]}$ (so $\mathfrak{D}^*$ satisfies $(\mathcal{T}_3)$). Note that the matrix $\mathbf{C}^{[1]}$ we used in the proof of Lemma 8.9 satisfies the following property: When $x_2 = y_2$, by (8.12),

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

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

Additionally, because of (8.9), we have that $\mathbf{Y}_{k,*}$ and $\mathbf{Y}_{1,*}$ are linearly dependent for every k. Thus, for every $k \in [s]$, there exists a positive, rational λ_k such that

$$\mathbf{Y}_{k,*} = \lambda_k \cdot \mathbf{Y}_{1,*}. \tag{8.14}$$

Because of this, we only need to prove (8.11) for the case when $k = 1$.

Now we start the proof of (8.11). 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 that is shown in Figure 8.2. More exactly, we define $G^{(p)} = (V^{(p)}, E^{(p)})$ as

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

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

1. one edge $(u, a_e), (a'_e, v), (c_e, b_e), (d_e, a_e), (c'_e, b'_e)$, and (d'_e, a'_e);
2. $pN - 1$ parallel edges between (a_e, v) and (u, a'_e);
3. $N - 1$ parallel 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 $Z_{\mathbf{R}^{(p)},\mathfrak{D}^*}(G) = Z_{\mathbf{C},\mathfrak{D}}(G^{(p)})$ for all G. 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.

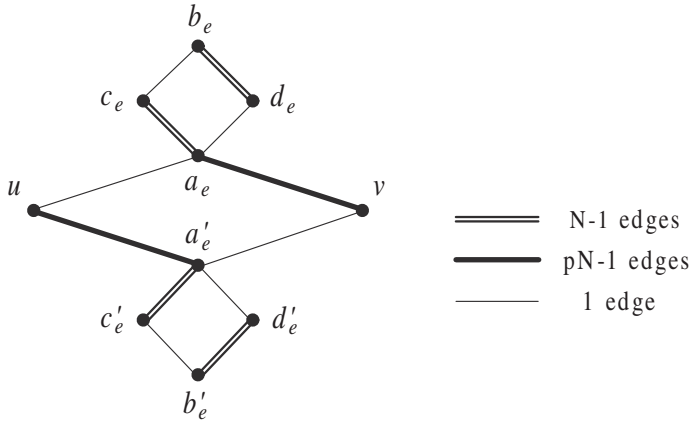

FIG. 8.2. *Gadget for constructing* $G^{(p)}$, $p \geq 1$.

Moreover, $\mathbf{R}^{(p)}$ is a block matrix which has the same block 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: For $\mathbf{x}, \mathbf{y} \in J$,

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

Recall that $C^{[1]}_{(0,\mathbf{a}),(0,\mathbf{b})} = 0$ when $a_2 \neq b_2$. From (8.14), $Y_{a_1,a_2} Y_{b_1,b_2} = \lambda_{a_1} \lambda_{b_1} Y_{1,a_2} Y_{1,b_2}$. As a result, we can simplify the first factor to be

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

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 positive and is independent of $\mathbf{x}, \mathbf{y}$. Similarly, the second factor becomes

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

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

We apply Corollary 8.3 to $(\mathbf{R}^{(p)}, \mathfrak{D}^*)$. As $\mathsf{EVAL}(\mathbf{R}^{(p)}, \mathfrak{D}^*)$ is not #P-hard, either

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

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

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

However, the left-hand side is a sum of $(Y_{1,i})^2$, which are positive integers, weighted by roots of unity. To sum to a number of norm $\sum_{i \in [h]} Y_{1,i}^2$ 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 (8.14), we have finished the proof of (8.11). ∎

8.4. Step 2.3. Now we get a pair $(\mathbf{C}, \mathfrak{D})$ that satisfies ($Shape_1$)–($Shape_5$) since otherwise, by Lemma 8.8, $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ 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 $(0, i)$, $i \in [s]$, to index its first s rows and $(1, j)$, $j \in [t]$, to index its last t rows. Its diagonal entries are

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

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

$$D^{[0]}_{(0,\mathbf{x})} = K^{[0]}_{(0,x_1)} \cdot L^{[0]}_{(0,x_2)} \quad \text{and} \quad D^{[0]}_{(1,\mathbf{y})} = K^{[0]}_{(1,y_1)} \cdot L^{[0]}_{(1,y_2)} \tag{8.15}$$

for all $\mathbf{x} \in I$ and $\mathbf{y} \in J$, or equivalently,

$$\mathbf{D}^{[0]} = \begin{pmatrix} \mathbf{D}^{[0]}_{(0,*)} & \\ & \mathbf{D}^{[0]}_{(1,*)} \end{pmatrix} = \begin{pmatrix} \mathbf{K}^{[0]}_{(0,*)} \otimes \mathbf{L}^{[0]}_{(0,*)} & \\ & \mathbf{K}^{[0]}_{(1,*)} \otimes \mathbf{L}^{[0]}_{(1,*)} \end{pmatrix}. \tag{8.16}$$

The goal of Step 2.3 is to prove a similar statement for $\mathbf{D}^{[r]}$, $r \in [N-1]$, and these equations will allow us in Step 2.4 to decompose $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ into two subproblems.

In the proof of Lemma 8.8, we crucially used the property (from $(\mathcal{T}_3)$) that all the diagonal entries of $\mathbf{D}^{[0]}$ are positive integers. However, for $r \geq 1$, $(\mathcal{T}_3)$ 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 more difficult. We prove the following lemma.

LEMMA 8.11. *Let $(\mathbf{C}, \mathfrak{D})$ be a pair that satisfies ($Shape_1$)–($Shape_5$). Then either $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is #P-hard or it satisfies the following additional 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* (8.16). *Every entry of $\mathbf{K}^{[0]}$ is a positive integer, and $\mathbf{L}^{[0]}$ is the $2h \times 2h$ identity matrix. For each $r \in [N-1]$, 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. Then*

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

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

$$\mathbf{K}^{[r]}_{(0,*)} = \mathbf{0} \iff \mathbf{L}^{[r]}_{(0,*)} = \mathbf{0} \quad \textit{and} \quad \mathbf{K}^{[r]}_{(1,*)} = \mathbf{0} \iff \mathbf{L}^{[r]}_{(1,*)} = \mathbf{0};$$

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

We now present the proof of Lemma 8.11. Fix an $r \in [N-1]$ to be any index. We use the following notation. Consider the diagonal matrix $\mathbf{D}^{[r]}$. It 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 $s \times h$ matrix, which we denote as $\mathbf{D}$ (just as we did with $\mathbf{D}^{[0]}$ in the proof of Lemma 8.8), where

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

We prove the following lemma in section 8.4.2.

LEMMA 8.12. *Either problem* $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ *is #P-hard, or we have* (1) $\operatorname{rank}(\mathbf{D}) \le 1$ *and* (2) *for each* $i \in [s]$, *all nonzero entries of* $\mathbf{D}_{i,*}$ *have the same norm.*

Proof of Lemma 8.11. We start with the first half, that is,

$$\mathbf{D}^{[r]}_{(0,*)} = \mathbf{K}^{[r]}_{(0,*)} \otimes \mathbf{L}^{[r]}_{(0,*)}. \tag{8.17}$$

Assume $\mathbf{D}^{[r]}_{(0,*)}$ is nonzero; otherwise the lemma is true by setting $\mathbf{K}^{[r]}_{(0,*)} = \mathbf{L}^{[r]}_{(0,*)} = \mathbf{0}$. As a result, we know that $\mathbf{D} \neq \mathbf{0}$.

Let $D_{a,b}$ be a nonzero entry of $\mathbf{D}$, where $a \in [s]$ and $b \in [h]$. From Lemma 8.12, the rank of $\mathbf{D}$ is 1, so $\mathbf{D}_{i,*} = (D_{i,b}/D_{a,b}) \cdot \mathbf{D}_{a,*}$ for any $i \in [s]$. 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 (8.17) follows. The second half 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 8.11 (assuming Lemma 8.12). ∎

8.4.1. The vanishing lemma. We need the following lemma in the proof of Lemma 8.12.

LEMMA 8.13 (vanishing lemma). *Let* k *be a positive integer and let* $(x_{i,n})_{n\ge 1}$, *for* $1 \le i \le k$, *be* k *infinite sequences of nonzero real numbers. For notational uniformity we also denote by* $(x_{0,n})_{n\ge 1}$ *the sequence where* $x_{0,n} = 1$ *for all* $n \ge 1$. *Suppose*

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

Part A. *Let* a_i *and* $b_i \in \mathbb{C}$ *for* $0 \le i \le k$. *Suppose for some* $\ell \in [k]$, $a_i = b_i$ *for all* $0 \le i < \ell$; $a_0 = b_0 = 1$; *and* $\operatorname{Im}(a_\ell) = \operatorname{Im}(b_\ell)$. *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 we have $a_\ell = b_\ell$.

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

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

then we have $a_i = 0$ *for all* $0 \le i \le k$.

Proof. We first prove Part B, which is simpler. Taking $n \to \infty$ (technically we take a subsequence of n approaching ∞ where the equality holds, and the same below), we get $a_0 = 0$. 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 $a_i\overline{a_j}x_{i,n}x_{j,n}$ 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 when $\max\{i,j\} = \ell$ and $\min\{i,j\} > 0$. The 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 $\mathrm{Re}(a_\ell) = \mathrm{Re}(b_\ell)$. It follows that $a_\ell = b_\ell$ since $\mathrm{Im}(a_\ell) = \mathrm{Im}(b_\ell)$. □

We also remark that Part A of the vanishing lemma above cannot be extended to arbitrary sequences $\{a_i\}$ and $\{b_i\}$ without the condition that $\mathrm{Im}(a_\ell) = \mathrm{Im}(b_\ell)$, 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 $|1+a_1x+a_2x^2| = |1+b_1x+b_2x^2|$ is an identity for all real values x. In particular this holds when $x \to 0$. We note that $a_1 \neq b_1$.

8.4.2. Proof of Lemma 8.12. Without loss of generality, we assume $1 = \mu_1 > \cdots > \mu_s > 0$ and $1 = \nu_1 > \cdots > \nu_t > 0$. (Otherwise, we can multiply $\mathbf{C}$ by 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 $\mathfrak{D}$ (so $\mathfrak{D}^*$ satisfies $(\mathcal{T}_3)$. Recall that r is a fixed index in $[N-1]$, and recall 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 build a new graph $G^{[n]}$ by replacing each edge $uv \in E$ with a gadget shown in Figure 8.3. 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

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

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

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

It is easy to check that the degree of every vertex in $G^{[n]}$ is a multiple of N except for b_e and b'_e, which have degree r mod N, and c_e and c'_e, which have degree $N-r$ mod 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 that $m = (s+t)h$) such that

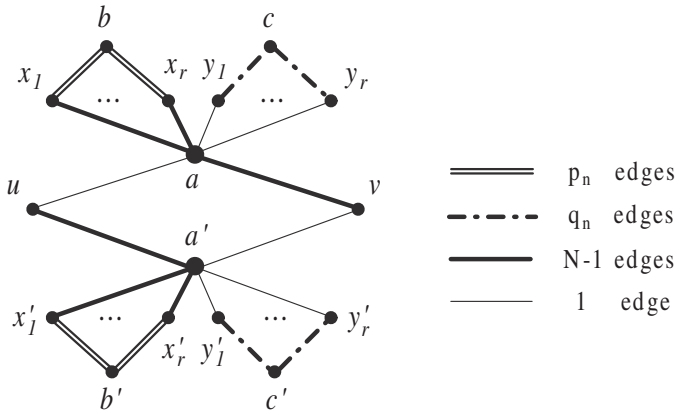

FIG. 8.3. *Gadget for constructing* $G^{[n]}$, $n \geq 1$. *(Note that the subscript e is suppressed.)*

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

The entries of $\mathbf{R}^{[n]}$ are as follows: For $\mathbf{u} \in I$ and $\mathbf{v} \in J$, the $((0,\mathbf{u}),(1,\mathbf{v}))$th and $((1,\mathbf{u}),(0,\mathbf{v}))$th entries of $\mathbf{R}^{[n]}$ are zero. For $\mathbf{u},\mathbf{v} \in J$, $R^{[n]}_{(1,\mathbf{u}),(1,\mathbf{v})}$ is the product of

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

and

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

We simplify the first sum. By using ($Shape_2$) and ($Shape_5$), we have

$$\begin{aligned}\sum_{\mathbf{x}\in J} F^{N-1}_{\mathbf{a},\mathbf{x}} F^{p_n}_{\mathbf{b},\mathbf{x}} D^{[0]}_{(1,\mathbf{x})} &= \mu^{N-1}_{a_1}\mu^{p_n}_{b_1} \sum_{\mathbf{x}\in J} (\nu_{x_1})^{N-1+p_n} \overline{H_{a_2,x_2}} H_{b_2,x_2} D^{[0]}_{(1,(x_1,1))} \\ &= \mu^{N-1}_{a_1}\mu^{p_n}_{b_1} \sum_{x_1\in[t]} (\nu_{x_1})^{N-1+p_n} D^{[0]}_{(1,(x_1,1))} \langle \mathbf{H}_{b_2,*}, \mathbf{H}_{a_2,*}\rangle. \end{aligned} \tag{8.18}$$

Let L denote the following positive number that is independent of $\mathbf{u},\mathbf{v},\mathbf{a},\mathbf{b}$, and $\mathbf{c}$:

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

By ($Shape_4$), (8.18) is equal to $L \cdot \mu^{N-1}_{a_1}\mu^{p_n}_{b_1}$ if $a_2 = b_2$ and 0 otherwise. Similarly,

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

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

By ($Shape_3$), we have

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

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

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

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

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

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

$$R^{[n]}_{(1,\mathbf{u}),(1,\mathbf{v})}=Z^2(\nu_{u_1}\nu_{v_1})^N\left(\sum_{b,c\in[s]}\mu_b^{P_n}\mu_c^{Q_n}\sum_{a\in[h]}D_{b,a}\overline{D_{c,a}}H_{a,u_2}\overline{H_{a,v_2}}\right)\times\left(\sum_{b',c'\in[s]}\mu_{b'}^{P_n}\mu_{c'}^{Q_n}\sum_{a\in[h]}D_{b',a}\overline{D_{c',a}H_{a,u_2}}H_{a,v_2}\right).$$

As $\mathsf{EVAL}(\mathbf{R}^{[n]},\mathfrak{D}^*)$ is not #P-hard and $(\mathbf{R}^{[n]},\mathfrak{D}^*)$ satisfies $(\mathcal{T})$ for all $n\geq 1$, the necessary condition of the inverse cyclotomic reduction lemma (Corollary 8.3) applies to $\mathbf{R}^{[n]}$.

In the proof below, for notational convenience we suppress the index $n\geq 1$ 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 $n\geq 1$). 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 $R_{u,v}\equiv R_{(1,(1,u)),(1,(1,v))}$ for all $u,v\in[h]$. As a result, we have (note that $\nu_1=1$)

(8.19)
$$R_{u,v}=Z^2\left(\sum_{b,c\in[s]}\mu_b^P\mu_c^Q\sum_{a\in[h]}D_{b,a}\overline{D_{c,a}}H_{a,u}\overline{H_{a,v}}\right)\left(\sum_{b',c'\in[s]}\mu_{b'}^P\mu_{c'}^Q\sum_{a\in[h]}D_{b',a}\overline{D_{c',a}H_{a,u}}H_{a,v}\right).$$

We will consider the above expression for $R_{u,v}$ *stratified* according to the order of magnitude of $\mu_b^P\mu_c^Q\mu_{b'}^P\mu_{c'}^Q=(\mu_b\mu_{b'})^P(\mu_c\mu_{c'})^Q$. Because $P=\Theta(n^2)$ 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, terms are ordered strictly first by $\mu_b\mu_{b'}$ and then by $\mu_c\mu_{c'}$. Inspired by this, we define the following total order $\leq_\mu$ over

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

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, we denote the entries of a 2×2 matrix T_i or T in $\mathcal{T}$ by

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

respectively. Using $\le_\mu$, we divide $\mathcal{T}$ into classes $\mathcal{T}_1, \mathcal{T}_2, \ldots, \mathcal{T}_d$ ordered from the largest to the smallest, for some $d \ge 1$, such that the following hold:

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

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 use U_i to denote $\mu_b\mu_{b'}$ and W_i to 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 (8.19) as follows:

$$R_{u,v} = Z^2 \sum_{i \in [d]} U_i^P W_i^Q \sum_{T \in \mathcal{T}_i} X_{u,v,T}, \tag{8.20}$$

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 (8.20) 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 nonzero.

Consider the diagonal entries where $u = v$. First notice that from (8.19), 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 $\mathbf{D}_{1,*} \neq \mathbf{0}$; otherwise, we can remove all terms involving μ_1 in (8.19) 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 8.3, we have the following.

PROPERTY 8.14. *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 let $\boldsymbol{\mathcal{H}}_{*,v} = \mathbf{H}_{*,1} \circ \overline{\mathbf{H}_{*,v}}$. $\{\boldsymbol{\mathcal{H}}_{*,v}\}_{v \in [h]}$ forms an orthogonal basis with each $\|\boldsymbol{\mathcal{H}}_{*,v}\|^2 = h$. We also denote $X_{1,v,T}$ by $X_{v,T}$, so

$$X_{v,T} = \left(\sum_{a \in [h]} D_{b,a} \overline{D_{c,a}} \mathcal{H}_{a,v} \right) \left(\sum_{a \in [h]} D_{b',a} \overline{D_{c',a} \mathcal{H}_{a,v}} \right) \quad \text{for } T = \begin{pmatrix} b & c \\ b' & c' \end{pmatrix}. \tag{8.21}$$

We make three more definitions. Let $K = \{i \in [h] : D_{1,i} \neq 0\}$. By our assumption $K \neq \emptyset$. Let $A = \{v \in [h] : \text{ for all } i, j \in K, \mathcal{H}_{i,v} = \mathcal{H}_{j,v}\}$ and $B = [h] - A$. 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 nonempty. 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 $\|\mathbf{D}_{1,*}\|^4 > 0$. Then from Property 8.14 and Part B of the vanishing lemma the next property follows.

PROPERTY 8.15. *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 nonconstant $\mathcal{H}_{a,v}$, 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 8.14 and Part B of the vanishing lemma, we have the following property.

PROPERTY 8.16. *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 8.16 to $\mathcal{T}_1 = \{\left(\begin{smallmatrix}1 & 1\\ 1 & 1\end{smallmatrix}\right)\}$, we have

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

because $|D_{1,a}|$ is real. Here we use $|\mathbf{D}_{1,*}|^2$ to denote the vector $(|D_{1,1}|^2, |D_{1,2}|^2, \ldots)$. 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 nonzero 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 nonzero entry and is zero elsewhere.) We summarize as follows.

PROPERTY 8.17. *$|\mathbf{D}_{1,*}|^2 \perp \boldsymbol{\mathcal{H}}_{*,v}$ for all $v \in B$. $|\mathbf{D}_{1,*}|^2$ is 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 K, $\mathbf{D}_{2,*}$ is a constant multiple of $\mathbf{D}_{1,*}$. Clearly if $B = \emptyset$, then we have $|K| = 1$ 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 8.16, $\sum_{T\in\mathcal{T}_g} X_{v,T} = 0$ for every $v \in B$. So we focus on terms $X_{v,T}$, where $T \in \mathcal{T}_g$ (i.e., $T \equiv_\mu T_1$). Suppose $T \equiv_\mu T_1$; then $\mu_b\mu_{b'} = \mu_1\mu_2$ and $\mu_c\mu_{c'} = \mu_1\mu_2$. Thus, $\{b, b'\} = \{c, c'\} = \{1, 2\}$, so

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

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 need one more definition: 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

$$X_{v,T} = \left| \sum_{a=1}^{h} D_{b,a} \overline{D_{c,a}} \mathcal{H}_{a,v} \right|^2 \geq 0.$$

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 nonnegative. Since $X_{v,T_1} + X_{v,T_2} = 0$, $X_{v,T_1} = X_{v,T_2} = 0$. This gives

$$\sum_{a \in [h]} \overline{D_{1,a}} D_{2,a} \overline{\mathcal{H}_{a,v}} = 0 \quad \text{for all } v \in B.$$

Hence $\overline{\mathbf{D}_{1,*}} \circ \mathbf{D}_{2,*} \perp \boldsymbol{\mathcal{H}}_{*,v}$ for all $v \in B$. It follows that $\overline{\mathbf{D}_{1,*}} \circ \mathbf{D}_{2,*}$ can be expressed 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 accomplishes our goal stated above, which we summarize as follows.

PROPERTY 8.18. *There exists some complex number λ, such that $D_{2,a} = \lambda D_{1,a}$, for all $a \in K$.*

Let $K_2 = \{i \in [h] : D_{2,i} \neq 0\}$. 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 is trivially true.

To this end, we consider the matrices in $\mathcal{T}_g$ 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

$$\sum_{T \in \mathcal{T}_g} X_{v,T} = \sum_{T \in \mathcal{T}_g} X_{1,T} \quad \text{for any } v \in A. \tag{8.22}$$

By Property 8.15, $|R_{1,v}| = |R_{1,1}|$ for any sufficiently large n. To apply the vanishing lemma, we first show that terms that have a higher order of magnitude satisfy

$$\sum_{T \in \mathcal{T}_{g'}} X_{v,T} = \sum_{T \in \mathcal{T}_{g'}} X_{1,T} \quad \text{for all } 1 \leq g' < g \text{ and } v \in A. \tag{8.23}$$

We also need to show that

$$\text{Im}\left(\sum_{T\in\mathcal{T}_g} X_{v,T}\right) = \text{Im}\left(\sum_{T\in\mathcal{T}_g} X_{1,T}\right). \tag{8.24}$$

By definition, every $T \geq_\mu T_1$ satisfies $\mu_b\mu_{b'} \geq \mu_1\mu_2$. Thus, the first column of T is either $(1\ 1)^{\mathrm{T}}, (1\ 2)^{\mathrm{T}}$, or $(2\ 1)^{\mathrm{T}}$.

First, consider those matrices $T \geq_\mu T_1$ where each row of T has at least one 1. For every $v \in A$, the two inner product factors in (8.21), namely,

$$\sum_{a=1}^{h} D_{b,a}\overline{D_{c,a}}\mathcal{H}_{a,v} \quad \text{and} \quad \sum_{a=1}^{h} D_{b',a}\overline{D_{c',a}}\,\overline{\mathcal{H}_{a,v}}$$

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 $v_0 = 1 \in A$. So for all such T, their contributions to $R_{1,v}$ and to $R_{1,1}$ are the same for any $v \in A$.

Such $T \geq_\mu T_1$ with at least one 1 in each row include any matrix of the form

$$\begin{pmatrix} 1 & c \\ 1 & c' \end{pmatrix}, \ \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}, \ \text{or} \ \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

These exhaust all $T >_\mu T_1$, and (8.23) follows.

Such $T \geq_\mu T_1$ 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

$$\left(\sum_{a\in K} |D_{1,a}|^2\mathcal{H}_{a,v}\right)\left(\sum_{a=1}^{h} |D_{2,a}|^2\overline{\mathcal{H}_{a,v}}\right) + \left(\sum_{a=1}^{h} |D_{2,a}|^2\mathcal{H}_{a,v}\right)\left(\sum_{a\in K} |D_{1,a}|^2\overline{\mathcal{H}_{a,v}}\right), \tag{8.25}$$

which is a real number. Equation (8.24) then follows.

Now we can apply Part A of the vanishing lemma, which gives us (8.22). Since $X_{v,T_1} = X_{1,T_1}$ 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 (8.25). (By our assumption, $\|\mathbf{D}_{1,*}\|^2\|\mathbf{D}_{2,*}\|^2 > 0$.) The only way the sum in (8.25) can achieve 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 pair of complex numbers α_v and β_v of norm 1. Moreover, by (8.25) we have $\alpha_v\overline{\beta_v} + \overline{\alpha_v}\beta_v = 2$. It follows that $\alpha_v = \beta_v$. Therefore, $\mathcal{H}_{a,v}$ is constant on $a \in K \cup K_2$ for each $v \in A$. We summarize it as follows.

PROPERTY 8.19. *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 vacuously 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 8.16, 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 $\mu_b \mu_{b'} = \mu_2^2$. 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 $(2\ 2)^{\mathrm{T}}$, $(s\ 1)^{\mathrm{T}}$, or $(1\ s)^{\mathrm{T}}$. Let's examine such a matrix T 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 of the following: The presence of $\mathbf{D}_{1,*}$ restricts the sum to $a \in K$. By Property 8.17, we know that for every $v \in B$, $|\mathbf{D}_{1,*}|^2 \perp \boldsymbol{\mathcal{H}}_{*,v}$. Moreover, on set K, we know from Property 8.18 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) and 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). 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 nonnegative. It follows that all three sums are 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 $\{\boldsymbol{\mathcal{H}}_{*,v} : v \in A\}$. 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 Property 8.19.

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 nonzero. 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 $\{\boldsymbol{\mathcal{H}}_{*,v} : v \in A\}$.

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, we denote by χ_{K_2} the characteristic vector for K_2. Both vectors χ_K and χ_{K_2} are in the linear span of $\{\boldsymbol{\mathcal{H}}_{*,v} : v \in A\}$. 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 Property 8.19. 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 $|K_2| = h/|A|$. Hence $|K| = |K_2|$ and $K = K_2$. At this point the statement in Property 8.18 can be strengthened to the following.

PROPERTY 8.20. *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 $\ell \geq 2$, the $(\ell - 1)$ rows $\mathbf{D}_{1,*}, \ldots, \mathbf{D}_{\ell-1,*}$ satisfy that $\mathbf{D}_{i,*} = \lambda_i \cdot \mathbf{D}_{1,*}$ for some λ_i and $1 \leq i < \ell$.

The proof mainly follow that of 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 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, consider the 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 8.16, we have for every $v \in B$, $\sum_{T \in \mathcal{T}_g} X_{v,T} = 0$. We only need to examine those $T \in \mathcal{T}_g$ 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 of T must have entries $\{1, \ell\}$ or have both entries $< \ell$. 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 product

$$X_{v,T} = \left(\sum_{a=1}^{h} D_{b,a} \overline{D_{c,a}} \mathcal{H}_{a,v} \right) \left(\sum_{a=1}^{h} D_{b',a} \overline{D_{c',a}}\, \overline{\mathcal{H}_{a,v}} \right)$$

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 Property 8.17 for all $v \in B$.

In Case 2, it is easy to check that to have the same order $\mu_1 \mu_\ell$, T can only be T_1 or T_2. Now observe that both T_1 and T_2 have the conjugate-pair form. Thus, their contributions X_{v,T_1} and X_{v,T_2} are both nonnegative. 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 $\overline{\mathbf{D}_{1,*}} \circ \mathbf{D}_{\ell,*} \perp \boldsymbol{\mathcal{H}}_{*,v}$ for all $v \in B$. It follows that the vector $\overline{\mathbf{D}_{1,*}} \circ \mathbf{D}_{\ell,*}$ belongs to the linear span of $\{\boldsymbol{\mathcal{H}}_{*,v} : v \in A\}$. From 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.

PROPERTY 8.21. *There exists some complex number λ_ℓ such that $D_{\ell,a} = \lambda_\ell D_{1,a}$ for all $a \in K$.*

Let $K_\ell = \{i \in [r] : D_{\ell,i} \neq 0\}$. 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

$$\sum_{T \in \mathcal{T}_g} X_{v,T} = \sum_{T \in \mathcal{T}_g} X_{1,T} \quad \text{for any } v \in A. \tag{8.26}$$

For this purpose, we need to compare the respective terms of the sum (8.20) for an arbitrary $v \in A$ and for the particular $v_0 = 1 \in A$. More exactly, we will show that

$$\sum_{T \in \mathcal{T}_{g'}} X_{v,T} = \sum_{T \in \mathcal{T}_{g'}} X_{1,T} \quad \text{and} \quad \operatorname{Im}\left(\sum_{T \in \mathcal{T}_g} X_{v,T}\right) = \operatorname{Im}\left(\sum_{T \in \mathcal{T}_g} X_{1,T}\right) \tag{8.27}$$

for all $v \in A$ and $g' < g$. Then (8.26) follows from Part A of the vanishing lemma.

To this end, we first consider matrices T that have an order of magnitude strictly larger than that of T_3 and T_4. We have either $\mu_b \mu_{b'} > \mu_1 \mu_\ell$ or $\mu_b \mu_{b'} = \mu_1 \mu_\ell$ and $\mu_c \mu_{c'} > \mu_1 \mu_\ell$. The first alternative implies $b, b' < \ell$. The second implies $c, c' < \ell$.

In both cases, each row of T has at least one entry $< \ell$. By the inductive hypothesis, both inner products in (8.21), namely,

$$\sum_{a=1}^{h} D_{b,a} \overline{D_{c,a}} \mathcal{H}_{a,v} \quad \text{and} \quad \sum_{a=1}^{h} D_{b',a} \overline{D_{c',a}}\, \overline{\mathcal{H}_{a,v}}$$

must be 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 is

$$X_{v,T} = \left(\sum_{a \in K} D_{b,a} \overline{D_{c,a}}\right)\left(\sum_{a \in K} D_{b',a} \overline{D_{c',a}}\right),$$

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 $T \equiv_\mu T_3 \in \mathcal{T}_g$), and the first part of (8.27) 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

$$\sum_{T \in \mathcal{T}_g} X_{v,T} - \sum_{T \in \mathcal{T}_g} X_{1,T} = X_{v,T_3} + X_{v,T_4} - (X_{1,T_3} + X_{1,T_4}) \quad \text{for any } v \in A.$$

Now to the matrices T_3, T_4 themselves. We note that the sum of their coefficients $X_{v,T_3} + X_{v,T_4}$, at any $v \in A$, is

(8.28)
$$\left(\sum_{a \in K} |D_{1,a}|^2 \mathcal{H}_{a,v}\right)\left(\sum_{a=1}^{h} |D_{\ell,a}|^2 \overline{\mathcal{H}_{a,v}}\right) + \left(\sum_{a=1}^{h} |D_{\ell,a}|^2 \mathcal{H}_{a,v}\right)\left(\sum_{a \in K} |D_{1,a}|^2 \overline{\mathcal{H}_{a,v}}\right).$$

This is a real number, and the second part of (8.27) 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 (8.28). By assumption, $\|\mathbf{D}_{1,*}\|^2 \|\mathbf{D}_{\ell,*}\|^2 > 0$. The only way the sum in (8.28) 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 (8.28), 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 the next property.

PROPERTY 8.22. *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 prove that $|\mathbf{D}_{\ell,*}|^2 \perp \boldsymbol{\mathcal{H}}_{*,v}$ for all $v \in B$. Of course, if $B = \emptyset$, then this is trivially true. We assume $B \neq \emptyset$. For this purpose, we examine T^*, the matrix with all four entries being ℓ, and the class $\mathcal{T}_g$ it belongs to. By Property 8.16, 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 $T \equiv_\mu T^* \in \mathcal{T}_g$.

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 $\ell > 2$.) Every matrix $T \in \mathcal{T}_g$ must have each column chosen from either $(\ell\ \ell)^{\mathrm{T}}$ or one of the pairs $(a_i\ b_i)^{\mathrm{T}}$ or $(b_i\ a_i)^{\mathrm{T}}$. 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 $i \in [k]$. We examine all the $T \in \mathcal{T}_g$ 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 Property 8.21, 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 is not T^*, then one of its two columns is not $(\ell\ \ell)^{\mathrm{T}}$, and one entry of this column is $a_i < \ell$ for some $i \in [k]$. It 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 two types:

$$\begin{pmatrix} a_i & b_j \\ b_i & a_j \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} b_i & a_j \\ a_i & b_j \end{pmatrix} \quad \text{for some } 1 \leq i,j \leq k.$$

We consider the first type. The total contribution of these matrices is

$$\begin{aligned}
&\sum_{i,j=1}^{k} \left(\sum_{a=1}^{h} D_{a_i,a} \overline{D_{b_j,a}} \mathcal{H}_{a,v} \right) \left(\sum_{a'=1}^{h} D_{b_i,a'} \overline{D_{a_j,a'}}\, \overline{\mathcal{H}_{a',v}} \right) \\
&= \sum_{i,j=1}^{k} \left(\sum_{a=1}^{h} \lambda_{a_i} D_{1,a} \overline{D_{b_j,a}} \mathcal{H}_{a,v} \right) \left(\sum_{a'=1}^{h} D_{b_i,a'} \overline{\lambda_{a_j}}\, \overline{D_{1,a'}}\, \overline{\mathcal{H}_{a',v}} \right) \\
&= \sum_{i,j=1}^{k} \sum_{a,a'=1}^{h} \overline{\lambda_{a_j}} D_{1,a} \overline{D_{b_j,a}} \mathcal{H}_{a,v} \cdot \lambda_{a_i} D_{b_i,a'} \overline{D_{1,a'}}\, \overline{\mathcal{H}_{a',v}} \\
&= \left[\sum_{a=1}^{h} D_{1,a} \mathcal{H}_{a,v} \left(\sum_{j=1}^{k} \overline{\lambda_{a_j}}\, \overline{D_{b_j,a}} \right) \right] \cdot \left[\sum_{a'=1}^{h} \overline{D_{1,a'}}\, \overline{\mathcal{H}_{a',v}} \left(\sum_{i=1}^{k} \lambda_{a_i} D_{b_i,a'} \right) \right] \\
&= \left| \sum_{a=1}^{h} D_{1,a} \mathcal{H}_{a,v} \left(\sum_{j=1}^{k} \overline{\lambda_{a_j}}\, \overline{D_{b_j,a}} \right) \right|^2 \geq 0.
\end{aligned}$$

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 T^* has the conjugate-pair form, and therefore its contribution X_{v,T^*} at any $v \in B$ is nonnegative. It follows from $\sum_{T \in \mathcal{T}_g} X_{v,T} = 0$ (Property 8.16) that $X_{v,T^*} = 0$ and

$$\left| \sum_{a=1}^{h} |D_{\ell,a}|^2 \overline{\mathcal{H}_{a,v}} \right|^2 = 0 \quad \text{for all } v \in B.$$

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 $\{\boldsymbol{\mathcal{H}}_{*,v} : v \in A\}$. Then by the same argument used for $\ell = 2$, we obtain $K = K_\ell$, and summarize as follows.

PROPERTY 8.23. *There exists a complex number λ_ℓ such that $\mathbf{D}_{\ell,*} = \lambda_\ell \mathbf{D}_{1,*}$.*

This completes the proof by induction that $\mathbf{D}$ has rank at most one.

8.5. Step 2.4. After Step 2.3, we obtain 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 for every $r \in [0 : N-1]$

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

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 bipartization of $\mathbf{M}$, so it is $(s+t) \times (s+t)$, and $\mathfrak{K}$ is a sequence of N diagonal matrices also of this size: $(\mathbf{K}^{[0]}, \ldots, \mathbf{K}^{[N-1]})$. Second, $\mathbf{C}''$ is the bipartization of $\mathbf{H}$, and it is $2h \times 2h$, and $\mathfrak{L}$ is the 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 8.24. $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D}) \equiv \mathsf{EVAL}(\mathbf{C}'', \mathfrak{L})$.

Proof. Let G be a connected undirected graph and let u^* be one of its vertices. Then by Lemmas 2.3 and 2.4, we have

$$\begin{aligned} Z_{\mathbf{C},\mathfrak{D}}(G) &= Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}(G, u^*) + Z^{\leftarrow}_{\mathbf{C},\mathfrak{D}}(G, u^*), \\ Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}(G, u^*) &= Z^{\rightarrow}_{\mathbf{C}',\mathfrak{K}}(G, u^*) \cdot Z^{\rightarrow}_{\mathbf{C}'',\mathfrak{L}}(G, u^*), \quad \text{and} \\ Z^{\leftarrow}_{\mathbf{C},\mathfrak{D}}(G, u^*) &= Z^{\leftarrow}_{\mathbf{C}',\mathfrak{K}}(G, u^*) \cdot Z^{\leftarrow}_{\mathbf{C}'',\mathfrak{L}}(G, u^*). \end{aligned}$$

As $\mathbf{M}$ 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, $Z^{\rightarrow}_{\mathbf{C}',\mathfrak{K}}(G, u^*)$ 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. Let Ξ denote the set of assignments ξ which map U to $[s]$ and V to $[t]$. Then (note that we use $\mathbf{K}^{[r]}$ to denote $\mathbf{K}^{[r \bmod N]}$ for any $r \geq N$)

$$\begin{aligned} Z^{\rightarrow}_{\mathbf{C}',\mathfrak{K}}(G, u^*) &= \sum_{\xi \in \Xi} \left(\prod_{uv \in E} \mu_{\xi(u)} \cdot \nu_{\xi(v)} \right) \left(\prod_{u \in U} K^{[\deg(u)]}_{(0,\xi(u))} \right) \left(\prod_{v \in V} K^{[\deg(v)]}_{(1,\xi(v))} \right) \\ &= \prod_{u \in U} \left(\sum_{i \in [s]} (\mu_i)^{\deg(u)} \cdot K^{[\deg(u)]}_{(0,i)} \right) \times \prod_{v \in V} \left(\sum_{j \in [t]} (\nu_j)^{\deg(v)} \cdot K^{[\deg(v)]}_{(1,j)} \right), \end{aligned}$$

which can be computed in polynomial time.

Moreover, since $(\mathbf{C}'', \mathfrak{L})$ satisfies (*Pinning*), by the second pinning lemma (Lemma 4.3), 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 $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D}) \leq \mathsf{EVAL}(\mathbf{C}'', \mathfrak{L})$.

We next prove the reverse direction. First note that by the third pinning lemma (Corollary 8.4), 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 because $Z^{\rightarrow}_{\mathbf{C}',\mathfrak{K}}$ (or $Z^{\leftarrow}_{\mathbf{C}',\mathfrak{K}}$) could be 0 at (G, u^*). To deal with this case, we prove the following claim.

CLAIM 8.25. *Given a connected, bipartite $G = (U \cup V, E)$ and vertex $u^* \in U$, either we can construct a new connected, bipartite $G' = (U' \cup V', E')$ in polynomial time such that $u^* \in U \subset U'$,*

$$Z^{\rightarrow}_{\mathbf{C}'',\mathfrak{L}}(G', u^*) = h^{|U \cup V|} \cdot Z^{\rightarrow}_{\mathbf{C}'',\mathfrak{L}}(G, u^*), \tag{8.29}$$

and $Z^{\rightarrow}_{\mathbf{C}',\mathfrak{K}}(G', u^*) \neq 0$, or we can show that $Z^{\rightarrow}_{\mathbf{C}'',\mathfrak{L}}(G, u^*) = 0$.

Claim 8.25 gives us a polynomial-time reduction from $Z^{\rightarrow}_{\mathbf{C}'',\mathfrak{L}}$ to $Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}$. A similar claim can be proved for $Z^{\leftarrow}$, and Lemma 8.24 follows. We now prove Claim 8.25.

For each $u \in U$ (and $v \in V$), we use r_u (and r_v) to denote its degree in G. To get G', we need an $\ell_u \in [s]$ for each $u \in U$ and an $\ell_v \in [t]$ for each $v \in V$ such that

$$\sum_{i \in [s]} \mu_i^{\ell_u N + r_u} \cdot K^{[r_u]}_{(0,i)} \neq 0 \quad \text{and} \quad \sum_{i \in [t]} \nu_i^{\ell_v N + r_v} \cdot K^{[r_v]}_{(1,i)} \neq 0. \tag{8.30}$$

Assume there exists a $u \in U$ such that no $\ell_u \in [s]$ satisfies (8.30). In this case, note that the s equations for $\ell_u = 1, \ldots, s$ form a Vandermonde system since $\mu_1 > \cdots > \mu_s > 0$. Therefore, the $(0,*)$-block of $\mathbf{K}^{[r_u]}$ is $\mathbf{0}$ and thus the $(0,*)$-block of $\mathbf{L}^{[r_u]}$ is also $\mathbf{0}$ by ($Shape_6$). It follows that $Z^{\rightarrow}_{\mathbf{C}'',\mathfrak{L}}(G,u^*) = 0$, and we are done. Similarly, we have $Z^{\rightarrow}_{\mathbf{C}'',\mathfrak{L}}(G,u^*) = 0$ if there exists a $v \in V$ such that no $\ell_v \in [t]$ satisfies (8.30).

Otherwise, suppose there do exist an $\ell_u \in [s]$ for each $u \in U$ and an $\ell_v \in [t]$ for each $v \in V$, which satisfy (8.30). We construct a bipartite $G' = (U' \cup V', E')$. First, $U' = U \cup \widehat{V}$ and $V' = V \cup \widehat{U}$, where $\widehat{V} = \{\widehat{v} : v \in V\}$ and $\widehat{U} = \{\widehat{u} : u \in U\}$. 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 $v \in V$.

Clearly, 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 8.25.

First, we have (the sum is over all ξ that map U' to $[s]$, V' to $[t]$)

$$\begin{aligned}
Z^{\rightarrow}_{\mathbf{C}',\mathfrak{K}}(G',u^*) &= \sum_{\xi} \left(\prod_{uv \in E} M_{\xi(u),\xi(v)} \prod_{u \in U} M^{\ell_u N}_{\xi(u),\xi(\widehat{u})} \prod_{v \in V} M^{\ell_v N}_{\xi(\widehat{v}),\xi(v)} \right) \\
&\quad \times \left(\prod_{u \in U} K^{[r_u]}_{(0,\xi(u))} K^{[0]}_{(1,\xi(\widehat{u}))} \right) \left(\prod_{v \in V} K^{[r_v]}_{(1,\xi(v))} K^{[0]}_{(0,\xi(\widehat{v}))} \right) \\
&= \prod_{u \in U} \left(\sum_{i \in [s]} \mu_i^{\ell_u N + r_u} \cdot K^{[r_u]}_{(0,i)} \right) \prod_{v \in V} \left(\sum_{i \in [t]} \nu_i^{\ell_v N + r_v} \cdot K^{[r_v]}_{(1,i)} \right) \\
&\quad \times \prod_{\widehat{u} \in \widehat{U}} \left(\sum_{i \in [t]} \nu_i^{\ell_u N} \cdot K^{[0]}_{(1,i)} \right) \prod_{\widehat{v} \in \widehat{V}} \left(\sum_{i \in [s]} \mu_i^{\ell_v N} \cdot K^{[0]}_{(0,i)} \right).
\end{aligned}$$

It is nonzero: The first two factors are nonzero because of the way we pick ℓ_u and ℓ_v; the latter two factors are nonzero because $\mu_i, \nu_i > 0$, and by ($Shape_6$), every entry of $\mathbf{K}^{[0]}$ is a positive integer.

It now suffices to prove (8.29). Let η be an assignment that maps U to $[s]$ and V to $[t]$. Given η, let Ξ denote the set of assignments ξ over $U' \cup V'$ that map U' to $[s]$ and V' to $[t]$ and that satisfy $\xi(u) = \eta(u)$, $\xi(v) = \eta(v)$ for all $u \in U$ and $v \in V$. We have

$$\begin{aligned}
\sum_{\xi \in \Xi} \mathrm{wt}_{\mathbf{C}'',\mathfrak{L}}(\xi) &= \sum_{\xi \in \Xi} \left(\prod_{uv \in E} H_{\eta(u),\eta(v)} \prod_{u \in U} (H_{\eta(u),\xi(\widehat{u})})^{\ell_u N} \prod_{v \in V} (H_{\xi(\widehat{v}),\eta(v)})^{\ell_v N} \right) \\
&\quad \times \left(\prod_{u \in U} L^{[r_u]}_{(0,\eta(u))} L^{[0]}_{(1,\xi(\widehat{u}))} \right) \left(\prod_{v \in V} L^{[r_v]}_{(1,\eta(v))} L^{[0]}_{(0,\xi(\widehat{v}))} \right) \\
&= \sum_{\xi \in \Xi} \mathrm{wt}_{\mathbf{C}'',\mathfrak{L}}(\eta) \;=\; h^{|\widehat{U} \cup \widehat{V}|} \cdot \mathrm{wt}_{\mathbf{C}'',\mathfrak{L}}(\eta).
\end{aligned}$$

The second equation uses the fact that entries of $\mathbf{H}$ are powers of ω_N (thus $(H_{i,j})^N = 1$) and $\mathbf{L}^{[0]}$ is the identity matrix. Equation (8.29) then follows. ∎

8.6. Step 2.5. We are almost done with Step 2. The only conditions $(\mathcal{U}_i)$ 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 $\mathbf{H}$ by $H_{1,1}$, which does not affect the complexity of $\mathsf{EVAL}(\mathbf{C}'', \mathfrak{L})$. Then we construct the following pair: $(\mathbf{X}, \mathfrak{Y})$. $\mathbf{X}$ is the bipartization of an $h \times h$ matrix over $\mathbb{C}$, whose (i,j)th entry is $H_{i,j}\overline{H_{1,j}H_{i,1}}$; $\mathfrak{Y}$ is a sequence $(\mathbf{Y}^{[0]}, \ldots, \mathbf{Y}^{[N-1]})$ of $2h \times 2h$ diagonal matrices; $\mathbf{Y}^{[0]}$ is the identity matrix. Let

$$\mathcal{S} = \{r \in [0 : N-1] : \mathbf{L}^{[r]}_{(0,*)} \neq \mathbf{0}\} \quad \text{and} \quad \mathcal{T} = \{r \in [0 : N-1] : \mathbf{L}^{[r]}_{(1,*)} \neq \mathbf{0}\};$$

then we have

$$\mathbf{Y}^{[r]}_{(0,*)} = \mathbf{0} \ \text{ for all } r \notin \mathcal{S} \quad \text{and} \quad \mathbf{Y}^{[r]}_{(1,*)} = \mathbf{0} \ \text{ for all } r \notin \mathcal{T}.$$

For each $r \in \mathcal{S}$ (or $r \in \mathcal{T}$), by $(Shape_6)$ there must be an $a_r \in [h]$ (or $b_r \in [h]$, resp.) such that the $(0, a_r)$th entry of $\mathbf{L}^{[r]}$ is 1 (or the $(1, b_r)$th entry of $\mathbf{L}^{[r]}$ is 1, resp.). Set

$$Y^{[r]}_{(0,i)} = L^{[r]}_{(0,i)} \left(\frac{H_{i,1}}{H_{a_r,1}}\right)^r \text{ for all } i \in [h]; \ \ Y^{[r]}_{(1,j)} = L^{[r]}_{(1,j)} \left(\frac{H_{1,j}}{H_{1,b_r}}\right)^r \text{ for all } j \in [h].$$

We show that $\mathsf{EVAL}(\mathbf{C}'', \mathfrak{L}) \equiv \mathsf{EVAL}(\mathbf{X}, \mathfrak{Y})$. For $\mathsf{EVAL}(\mathbf{X}, \mathfrak{Y}) \leq \mathsf{EVAL}(\mathbf{C}'', \mathfrak{L})$, we 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 set of vertices with degree r mod 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

$$Z^{\rightarrow}_{\mathbf{C}'',\mathfrak{L}}(G, u^*) = \left(\prod_{r \in \mathcal{S}} (H_{a_r,1})^{r|U_r|}\right) \left(\prod_{r \in \mathcal{T}} (H_{1,b_r})^{r|V_r|}\right) \cdot Z^{\rightarrow}_{\mathbf{X},\mathfrak{Y}}(G, u^*).$$

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 4.3), 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 $\mathsf{EVAL}(\mathbf{X}, \mathfrak{Y}) \leq \mathsf{EVAL}(\mathbf{C}'', \mathfrak{L})$. The other direction, $\mathsf{EVAL}(\mathbf{C}'', \mathfrak{L}) \leq \mathsf{EVAL}(\mathbf{X}, \mathfrak{Y})$, can be proved similarly.

One can verify 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 $M \mid N$, and $\mathfrak{Y}$ satisfies both $(\mathcal{U}_3)$ and $(\mathcal{U}_4)$ (which follows 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 $Z_{\mathbf{X},\mathfrak{Y}}(G) = Z_{\mathbf{X},\mathfrak{Y}'}(G)$, for all undirected G, and the new tuple $((M, 2N), \mathbf{X}, \mathfrak{Y}')$ now satisfies conditions $(\mathcal{U}_1)$–$(\mathcal{U}_4)$.

9. Proofs of Theorems 5.4 and 5.6. Let $((M, N), \mathbf{C}, \mathfrak{D})$ be a tuple that satisfies $(\mathcal{U}_1)$–$(\mathcal{U}_4)$ and let $\mathbf{F} \in \mathbb{C}^{m \times m}$ be the upper-right block of $\mathbf{C}$. In this section, we index the rows and columns of an $n \times n$ matrix with $[0 : n-1]$.

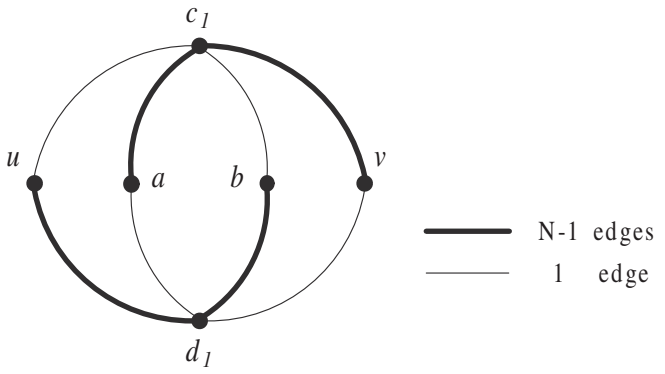

FIG. 9.1. *The gadget for $p = 1$. (Note that the subscript e is suppressed.)*

9.1. The group condition. We first show 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 group condition $(\mathcal{GC})$,*

(row-$\mathcal{GC}$) for all $i, j \in [0 : m-1]$, $\exists\, k \in [0 : m-1]$ such that $\mathbf{F}_{k,*} = \mathbf{F}_{i,*} \circ \mathbf{F}_{j,*}$;

(column-$\mathcal{GC}$) for all $i, j \in [0 : m-1]$, $\exists\, k \in [0 : m-1]$ 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 $p \geq 1$, 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 9.1. More exactly, we define $G^{[p]} = (V^{[p]}, E^{[p]})$ as

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

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

1. one edge $(u, c_{e,i})$, $(c_{e,i}, b_e)$, $(d_{e,i}, a_e)$, and $(d_{e,i}, v)$;
2. $N - 1$ parallel edges $(c_{e,i}, v)$, $(c_{e,i}, a_e)$, $(d_{e,i}, b_e)$, and $(d_{e,i}, u)$.

It is easy to verify that the degree of every vertex in $G^{[p]}$ is a multiple of N. Thus, we have $Z_{\mathbf{C},\mathfrak{D}}(G^{[p]}) = Z_{\mathbf{C}}(G^{[p]})$ because $\mathfrak{D}$ satisfies $(\mathcal{U}_3)$. On the other hand, the way we construct $G^{[p]}$ gives us, for each $p \geq 1$, a symmetric matrix $\mathbf{A}^{[p]} \in \mathbb{C}^{2m \times 2m}$ which only depends on $\mathbf{C}$, such that $Z_{\mathbf{A}^{[p]}}(G) = Z_{\mathbf{C}}(G^{[p]}) = Z_{\mathbf{C},\mathfrak{D}}(G^{[p]})$ for all G. It follows that $\mathsf{EVAL}(\mathbf{A}^{[p]}) \leq \mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ and thus $\mathsf{EVAL}(\mathbf{A}^{[p]})$ is not #P-hard for all $p \geq 1$.

The (i, j)th entry of $\mathbf{A}^{[p]}$, where $i, j \in [0 : 2m-1]$, is

$$\begin{aligned} A^{[p]}_{i,j} &= \sum_{a=0}^{2m-1} \sum_{b=0}^{2m-1} \left(\sum_{c=0}^{2m-1} C_{i,c} \overline{C_{a,c}} C_{b,c} \overline{C_{j,c}} \right)^p \left(\sum_{d=0}^{2m-1} \overline{C_{i,d}} C_{a,d} \overline{C_{b,d}} C_{j,d} \right)^p \\ &= \sum_{a=0}^{2m-1} \sum_{b=0}^{2m-1} \left| \sum_{c=0}^{2m-1} C_{i,c} \overline{C_{a,c}} C_{b,c} \overline{C_{j,c}} \right|^{2p}. \end{aligned}$$

For the first equality, we used the fact that $M \,|\, N$ and thus, e.g., $(C_{a,c})^{N-1} = \overline{C_{a,c}}$ as $C_{a,c}$ is a power of ω_M. Note that $\mathbf{A}^{[p]}$ is symmetric and nonnegative and satisfies

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

For $i, j \in [0 : m-1]$, we have

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

$$A^{[p]}_{i+m,j+m} = \sum_{a=0}^{m-1}\sum_{b=0}^{m-1} \left|\langle \mathbf{F}_{*,i} \circ \overline{\mathbf{F}_{*,j}}, \mathbf{F}_{*,a} \circ \overline{\mathbf{F}_{*,b}}\rangle\right|^{2p}. \tag{9.1}$$

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 nonnegative 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 discrete unitary, $A^{[p]}_{i,i} = m \cdot m^{2p}$. On the other hand, assuming $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is not #P-hard, by using the Bulatov–Grohe dichotomy theorem (Corollary 2.6),

$$A^{[p]}_{i,i} \cdot A^{[p]}_{j,j} = A^{[p]}_{i,j} \cdot A^{[p]}_{j,i} = (A^{[p]}_{i,j})^2 \quad \text{for all } i \neq j \in [0 : m-1],$$

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

Now we use this condition to prove that $\mathbf{F}$ satisfies (row-$\mathcal{GC}$). We introduce the following notation. For $i, j \in [0 : m-1]$, let

$$X_{i,j} = \left\{ |\langle \mathbf{F}_{i,*} \circ \overline{\mathbf{F}_{j,*}}, \mathbf{F}_{a,*} \circ \overline{\mathbf{F}_{b,*}}\rangle| \;\middle|\; a, b \in [0 : m-1] \right\}.$$

Clearly $X_{i,j}$ is finite for all i, j, with $|X_{i,j}| \leq m^2$. Each $x \in X_{i,j}$ satisfies $0 \leq x \leq m$. For each $x \in X_{i,j}$, let $s_{i,j}(x)$ denote the number of pairs $(a, b) \in [0 : m-1]^2$ such that

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

We can now rewrite $A^{[p]}_{i,j}$ as the sum

$$A^{[p]}_{i,j} = \sum_{x \in X_{i,j}} s_{i,j}(x) \cdot x^{2p}, \tag{9.2}$$

which is equal to m^{2p+1} for all $p \geq 1$. Note that $s_{i,j}(x)$ does not depend on p, and

$$\sum_{x \in X_{i,j}} s_{i,j}(x) = m^2. \tag{9.3}$$

We can view (9.2) and (9.3) 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 (9.2) are indexed by p. If we choose (9.3) and (9.2) for p from 1 up to $|X_{i,j}| - 1$, 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.

So $X_{i,j} = \{0, m\}$ and thus $|\langle \mathbf{F}_{i,*} \circ \overline{\mathbf{F}_{j,*}}, \mathbf{F}_{a,*} \circ \overline{\mathbf{F}_{b,*}} \rangle| \in \{0, m\}$ for all i, j, a, b.

Finally, we prove (row-$\mathcal{GC}$). Set $j = 0$. As $\mathbf{F}_{0,*} = \mathbf{1}$, 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 with $\|\mathbf{F}_{a,*}\|^2 = m$, by Parseval

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

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

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

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

From 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 norms 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 (9.1) and the lower-right $m \times m$ block of $\mathbf{A}^{[p]}$. □

Next we prove a property concerning discrete unitary matrices that satisfy ($\mathcal{GC}$). Given an $n \times n$ matrix $\mathbf{A}$, 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 $|A^{\mathrm{R}}|, |A^{\mathrm{C}}| < n$, since $\mathbf{A}$ may have duplicate rows or columns. But if $\mathbf{A}$ is M-discrete unitary, then it is clear that $|A^{\mathrm{R}}| = |A^{\mathrm{C}}| = n$.

PROPERTY 9.2. *If $\mathbf{A} \in \mathbb{C}^{n \times n}$ is an M-discrete unitary matrix that satisfies ($\mathcal{GC}$), then 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 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 cancellation 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 5.4. In this section, we prove Theorem 5.4 by showing that ($\mathcal{U}_1$)–($\mathcal{U}_4$) indeed imply ($\mathcal{U}_5$).

Suppose $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is not #P-hard; otherwise we are already done. By Lemma 9.1, $((M, N), \mathbf{C}, \mathfrak{D})$ satisfies ($\mathcal{GC}$). Fixing r to be any index in $[N-1]$, we will prove ($\mathcal{U}_5$) for the (i,i)th entries of $\mathbf{D}^{[r]}$, where $i \in [m : 2m-1]$. The proof for the first half of $\mathbf{D}^{[r]}$ is similar. For simplicity, let $\mathbf{D}$ be the m-dimensional vector such that

$$D_i = D^{[r]}_{m+i} \quad \text{for all } i \in [0 : m-1].$$

Also let $K = \{i \in [0 : m-1] : D_i \neq 0\}$. If $|K| = 0$, then there is nothing to prove; if $|K| = 1$, then by ($\mathcal{U}_3$), the only nonzero entry in $\mathbf{D}$ must be 1. So we assume $|K| \geq 2$.

We start with a useful lemma. It implies that to prove Theorem 5.4, i.e., $(\mathcal{U}_5)$, it suffices to prove that D_i is a root of unity for every $i \in K$.

LEMMA 9.3. *If $D \in \mathbb{Q}(\omega_N)$ is a root of unity, then D must be a power of ω_N.*

Proof. 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 $\gcd(k, M) = 1$, $\omega_M \in \mathbb{Q}(\omega_N)$ and

$$\mathbb{Q}(\omega_N) = \mathbb{Q}(\omega_N, \omega_M) = \mathbb{Q}(\omega_{\mathrm{lcm}(M,N)}).$$

The degree of the field extension is $[\mathbb{Q}(\omega_N) : \mathbb{Q}] = \phi(N)$, the Euler function [25].

When $N \mid N'$ and $\phi(N) = \phi(N')$, by expanding according to the prime factorization for N, we can get (and actually this is all there is to be had) that if N is even, then $N' = N$; if N is odd, then $N' = N$ or $N' = 2N$. As by $(\mathcal{U}_1)$ N is even, we have $\mathrm{lcm}(M, N) = N$, $M \mid N$, and D is a power of ω_N. ∎

Next we show that every D_i, $i \in K$, is a root of unity. Suppose for a contradiction that this is not true. We show the following lemma about $\mathbf{Z} = (Z_0, \ldots, Z_{m-1})$, where $Z_i = (D_i)^N$.

LEMMA 9.4. *Suppose there is a $k \in K$ 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, but never reaches, the all-one vector $\mathbf{1}_{|K|}$.*

Proof. As Z_k has norm 1, $Z_k = e^{2\pi i \theta_k}$ for some real number $\theta_k \in [0, 1)$. We will treat θ_k as a number in the $\mathbb{Z}$-module $\mathbb{R}_{\bmod 1}$, 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. First, for any positive integer P, $((Z_k)^P : k \in K) \neq \mathbf{1}$; otherwise, every θ_k is rational, contradicting the assumption.

Let $n^* = n^{|K|} + 1$ for some 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 $n^* - 1$ subcubes 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. By cardinality, there are $L \neq L' \in [n^*]$ such that

$$\big(L \cdot \theta_k \bmod 1 : k \in K\big) \quad \text{and} \quad \big(L' \cdot \theta_k \bmod 1 : k \in K\big)$$

fall in the same subcube. Assume $L > L'$; by setting $P_n = L - L' \geq 1$, we have

$$\big|P_n \cdot \theta_k \bmod 1\big| = |(L - L') \cdot \theta_k \bmod 1| < 1/n \quad \text{for all } k \in K.$$

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, but never reaches, 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 that is shown in Figure 9.2. Recall that $r \in [N - 1]$ is fixed. More exactly, we define $G^{[p]} = (V^{[p]}, E^{[p]})$ as follows:

$$V^{[p]} = V \cup \big\{a_e, b_{e,i}, c_{e,i,j}, a'_e, b'_{e,i}, c'_{e,i,j} : e \in E, i \in [pN], j \in [r]\big\},$$

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

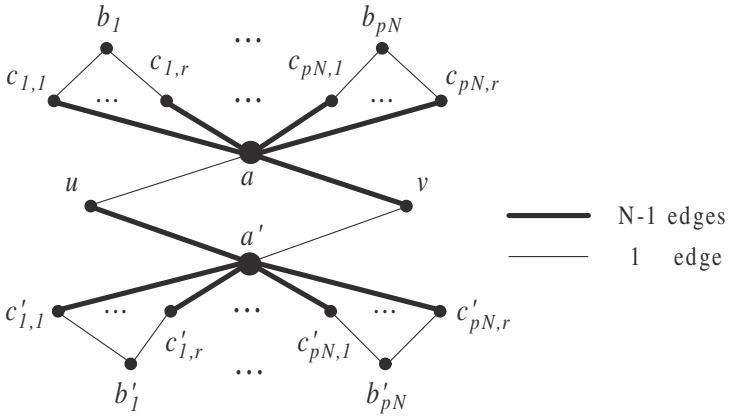

FIG. 9.2. *The gadget for $p = 1$. (Note that the subscript e is suppressed.)*

1. one edge (u, a_e) and (v, a'_e);
2. $N - 1$ parallel edges (a_e, v) and (u, a'_e);
3. one edge $(c_{e,i,j}, b_{e,i})$ and $(c'_{e,i,j}, b'_{e,i})$ for all $i \in [pN]$ and $j \in [r]$;
4. $N - 1$ parallel edges $(a_e, c_{e,i,j})$ and $(a'_e, c'_{e,i,j})$ for all $i \in [pN]$ and $j \in [r]$.

It is easy to verify 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 a symmetric $2m \times 2m$ matrix $\mathbf{A}^{[p]}$ such that $Z_{\mathbf{A}^{[p]}}(G) = Z_{\mathbf{C},\mathfrak{D}}(G^{[p]})$ for all G and thus $\mathsf{EVAL}(\mathbf{A}^{[p]}) \le \mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$, and $\mathsf{EVAL}(\mathbf{A}^{[p]})$ is also not #P-hard.

The entries of $\mathbf{A}^{[p]}$ are as follows. First, for all $u, v \in [0 : m-1]$, the $(u, m+v)$th and $(m+u, v)$th entries of $\mathbf{A}^{[p]}$ are zero. The entries in the upper-left block are

$$A^{[p]}_{u,v} = \left(\sum_{a \in [0:m-1]} F_{u,a} \overline{F_{v,a}} \left(\sum_{b \in [0:m-1]} D^{[r]}_{m+b} \left(\sum_{c \in [0:m-1]} F_{c,b} \overline{F_{c,a}} \right)^r \right)^{pN} \right) \times \left(\sum_{a \in [0:m-1]} \overline{F_{u,a}} F_{v,a} \left(\sum_{b \in [0:m-1]} D^{[r]}_{m+b} \left(\sum_{c \in [0:m-1]} F_{c,b} \overline{F_{c,a}} \right)^r \right)^{pN} \right)$$

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

$$A^{[p]}_{u,v} = L_p \cdot \left(\sum_{k \in K} (D_k)^{pN} F_{u,k} \overline{F_{v,k}} \right) \left(\sum_{k \in K} (D_k)^{pN} \overline{F_{u,k}} F_{v,k} \right)$$

for $u, v \in [0 : m-1]$, where L_p is a positive constant that is independent of u and v.

Assume for a contradiction that some D_k, $k \in K$, is not a root of unity. Then by Lemma 9.4 we know there exists a sequence $\{P_n\}$ such that $((D_k)^{NP_n} : k \in K)$

approaches, but never equals, the all-one vector, when $n \to \infty$. Also 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 Grohe and Lemma 7.5 together with the assumption that $\mathsf{EVAL}(\mathbf{A}^{[P_n]})$ 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 $L_{P_n}|T_n|$.

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 9.2, $F^{\mathrm{R}} = \{\mathbf{F}_{v,*}\}$ is a group under the Hadamard product. We let

$$S = \{v \in [0 : m-1] : \text{ for all } i, j \in K, F_{v,i} = F_{v,j}\}$$

and denote $\{\mathbf{F}_{v,*} : v \in S\}$ by F^S. F^S is a subgroup of F^{R}, and $0 \in S$ as $\mathbf{F}_{0,*} = \mathbf{1}$.

For any $v \notin S$, when n is sufficiently large, we have

$$\left| A^{[P_n]}_{0,v} \right| < \left| A^{[P_n]}_{0,0} \right|.$$

This is because when $n \to \infty$, $T_n \to |K|^2$ but

$$\left(\sum_{k \in K} (D_k)^{NP_n} \overline{F_{v,k}} \right) \left(\sum_{k \in K} (D_k)^{NP_n} F_{v,k} \right) \to \left(\sum_{k \in K} \overline{F_{v,k}} \right) \left(\sum_{k \in K} F_{v,k} \right),$$

which has norm $< |K|^2$ since $v \notin S$. So when n is sufficiently large, $A^{[P_n]}_{0,v} = 0$ for all $v \notin S$. Denote $((D_k)^{NP_n} : k \in [0 : m-1])$ by $\mathbf{D}^n$; for $v \notin S$ and sufficiently large n,

$$\text{either } \langle \mathbf{D}^n, \mathbf{F}_{v,*} \rangle = 0 \quad \text{or } \langle \mathbf{D}^n, \overline{\mathbf{F}_{v,*}} \rangle = 0. \tag{9.4}$$

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 (9.4) and the definition of S, we have

$$\langle \boldsymbol{\chi}, \mathbf{F}_{v,*} \rangle = 0 \text{ for all } v \notin S \quad \text{and} \quad |\langle \boldsymbol{\chi}, \mathbf{F}_{v,*} \rangle| = |K| \text{ for all } v \in S. \tag{9.5}$$

To prove the first equation, note that by (9.4), 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 $n \to \infty$, either $\langle \boldsymbol{\chi}, \mathbf{F}_{v,*} \rangle = 0$ or $\langle \boldsymbol{\chi}, \overline{\mathbf{F}_{v,*}} \rangle = 0$. The second case still gives us $\langle \boldsymbol{\chi}, \mathbf{F}_{v,*} \rangle = 0$ since $\boldsymbol{\chi}$ is real. The second equation in (9.5) 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 $\mathbf{D}^n$, under the orthogonal basis $\{\mathbf{F}_{v,*}\}$, is

$$\mathbf{D}^n = \sum_{i=0}^{m-1} x_{i,n}\mathbf{F}_{i,*}, \quad \text{where } \; x_{i,n} = \frac{1}{m}\langle \mathbf{D}^n, \mathbf{F}_{i,*}\rangle.$$

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.

Assume this is not the case. Then (here consider those sufficiently large n so that (9.4) holds),

$$\boldsymbol{\chi} = \mathbf{D}^n \circ \overline{\mathbf{D}^n} = \left(\sum_i x_{i,n}\mathbf{F}_{i,*}\right) \circ \left(\sum_j \overline{x_{j,n}}\,\overline{\mathbf{F}_{j,*}}\right) = \sum_v y_{v,n}\mathbf{F}_{v,*},$$

where

$$y_{v,n} = \sum_{\mathbf{F}_{i,*}\circ\overline{\mathbf{F}_{j,*}}=\mathbf{F}_{v,*}} x_{i,n}\overline{x_{j,n}}.$$

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 must have $y_{v,n} = 0$ for any $v \notin S$. Because $\mathbf{D}^n \to \boldsymbol{\chi}$, by (9.5), 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 $x_{i,n} \neq 0$, and 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 both be in S; otherwise, since F^S is a subgroup, we have $w \in S$, which contradicts the assumption that $w \notin S$.) The main terms of $y_{w,n}$ are given by

$$\frac{1}{m^2}\sum_{j\in S}\langle \mathbf{D}^n, \mathbf{F}_{w,*} \circ \mathbf{F}_{j,*}\rangle\overline{\langle \mathbf{D}^n, \mathbf{F}_{j,*}\rangle} + \frac{1}{m^2}\sum_{i\in S}\langle \mathbf{D}^n, \mathbf{F}_{i,*}\rangle\overline{\langle \mathbf{D}^n, \mathbf{F}_{i,*} \circ \overline{\mathbf{F}_{w,*}}\rangle}.$$

Note that $x_{0,n} = \langle \mathbf{D}^n, \mathbf{F}_{0,*}\rangle/m$ 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 nonzero on K, we have

$$\langle \mathbf{D}^n, \mathbf{F}_{w,*} \circ \mathbf{F}_{j,*}\rangle\overline{\langle \mathbf{D}^n, \mathbf{F}_{j,*}\rangle} = \langle \mathbf{D}^n, \alpha_j\mathbf{F}_{w,*}\rangle\overline{\langle \mathbf{D}^n, \alpha_j\mathbf{1}\rangle} = m\overline{x_{0,n}} \cdot \langle \mathbf{D}^n, \mathbf{F}_{w,*}\rangle.$$

Similarly, we can simplify the other sum so that the main terms of $y_{w,n}$ are given by

$$\frac{|S|}{m} \cdot \left(\overline{x_{0,n}}\langle \mathbf{D}^n, \mathbf{F}_{w,*}\rangle + x_{0,n}\langle \overline{\mathbf{D}^n}, \mathbf{F}_{w,*}\rangle\right).$$

By (9.4) we have either $\langle \mathbf{D}^n, \mathbf{F}_{w,*} \rangle$ or $\langle \overline{\mathbf{D}^n}, \mathbf{F}_{w,*} \rangle$ is 0. Since we assumed that $x_{w,n} = \langle \mathbf{D}^n, \mathbf{F}_{w,*} \rangle / m \neq 0$, the latter has to be 0. Therefore, the sum of the main terms of $y_{w,n}$ is equal to $\overline{x_{0,n}} x_{w,n} |S|$. As $0 \in S$, we have

$$\left| \overline{x_{0,n}} x_{w,n} |S| \right| \geq \frac{4|K||S|}{5m} |x_{w,n}|.$$

Consider the remaining terms. Below we prove 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 nonzero and we get a contradiction. To see 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 $< |\overline{x_{0,n}} x_{w,n} |S||$. Theorem 5.4 is proved.

9.3. Decomposing F into Fourier matrices. Suppose $((M, N), \mathbf{C}, \mathfrak{D})$ satisfies $(\mathcal{U}_1)$–$(\mathcal{U}_5)$ and $(\mathcal{GC})$; otherwise $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is #P-hard. We prove Theorem 5.6. To decompose $\mathbf{F}$ into Fourier matrices (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, $\mathbf{F}$ is the tensor product of two smaller matrices, both of which are discrete unitary and satisfy $(\mathcal{GC})$. Note that p and q here are not necessarily primes or prime powers.

LEMMA 9.5. *Let $\mathbf{F} \in \mathbb{C}^{m \times m}$ be an M-discrete unitary matrix that satisfies $(\mathcal{GC})$, where $M = pq$, $p, q > 1$, and $\gcd(p, q) = 1$. Then there exist two permutations Π and Σ over $[0 : m-1]$ such that $\mathbf{F}_{\Pi,\Sigma} = \mathbf{F}' \otimes \mathbf{F}''$, where $\mathbf{F}'$ is a p-discrete unitary matrix, $\mathbf{F}''$ is a q-discrete unitary matrix, and both of them satisfy $(\mathcal{GC})$.*

Proof. Using Property 9.2, 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} or F^{C} is a divisor of M.

By the fundamental theorem of Abelian groups, there is a group isomorphism

$$\rho : F^{\mathrm{R}} \to \mathbb{Z}_{g_1} \times \cdots \times \mathbb{Z}_{g_h} \equiv \mathbb{Z}_{\mathbf{g}},$$

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}:

$$S^p = \{\rho^{-1}(\mathbf{x}) : \mathbf{x} \in \mathbb{Z}_{\mathbf{g}},\ x_i = 0 \text{ for all } i > h'\} \quad \text{and}$$
$$S^q = \{\rho^{-1}(\mathbf{x}) : \mathbf{x} \in \mathbb{Z}_{\mathbf{g}},\ x_i = 0 \text{ for all } i \leq h'\}.$$

It is easy to show the following four properties: Letting $m' = |S^p|$ and $m'' = |S^q|$,

1. both S^p and S^q are subgroups of F^{R};
2. $S^p = \{\mathbf{u} \in F^{\mathrm{R}} : (\mathbf{u})^p = \mathbf{1}\}$ and $S^q = \{\mathbf{v} \in F^{\mathrm{R}} : (\mathbf{v})^q = \mathbf{1}\}$;
3. $m = m' \cdot m''$, $\gcd(m', q) = 1$, $\gcd(m'', p) = 1$, $\gcd(m', m'') = 1$;
4. $(\mathbf{u}, \mathbf{v}) \mapsto \mathbf{u} \circ \mathbf{v}$ is a group isomorphism from $S^p \times S^q$ onto F^{R}.

Let $S^p = \{\mathbf{u}_0 = \mathbf{1}, \mathbf{u}_1, \ldots, \mathbf{u}_{m'-1}\}$ and $S^q = \{\mathbf{v}_0 = \mathbf{1}, \mathbf{v}_1, \ldots, \mathbf{v}_{m''-1}\}$. By 4, there is a bijection $f : i \mapsto (f_1(i), f_2(i))$ from $[0 : m-1]$ to $[0 : m'-1] \times [0 : m''-1]$ such that

$$\mathbf{F}_{i,*} = \mathbf{u}_{f_1(i)} \circ \mathbf{v}_{f_2(i)} \quad \text{for all } i \in [0 : m-1]. \tag{9.6}$$

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. $T^p = \{\mathbf{w} \in F^{\mathrm{C}} : (\mathbf{w})^p = \mathbf{1}\}$ and $T^q = \{\mathbf{r} \in F^{\mathrm{C}} : (\mathbf{r})^q = \mathbf{1}\}$;
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 $T^p \times T^q$ 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 bijection g from $[0 : m-1]$ to $[0 : m'-1] \times [0 : m''-1]$ and

$$\mathbf{F}_{*,j} = \mathbf{w}_{g_1(j)} \circ \mathbf{r}_{g_2(j)} \quad \text{for all } j \in [0 : m-1]. \tag{9.7}$$

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 $\mathbf{F}$. We get $\mathbf{G} = \mathbf{F}_{\Pi,\Sigma}$, where

$$G_{(x_1,x_2),(y_1,y_2)} = F_{\Pi(x_1,x_2),\Sigma(y_1,y_2)} \quad \text{for all } x_1, y_1 \in [0 : m'-1], x_2, y_2 \in [0 : m''-1].$$

By (9.6), and using the fact that $\mathbf{u}_0 = \mathbf{1}$ and $\mathbf{v}_0 = \mathbf{1}$, we have

$$\mathbf{G}_{(x_1,x_2),*} = \mathbf{G}_{(x_1,0),*} \circ \mathbf{G}_{(0,x_2),*}.$$

Similarly by (9.7) and $\mathbf{w}_0 = \mathbf{1}$ and $\mathbf{r}_0 = \mathbf{1}$, we have

$$\mathbf{G}_{*,(y_1,y_2)} = \mathbf{G}_{*,(y_1,0)} \circ \mathbf{G}_{*,(0,y_2)}.$$

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

$$G_{(x_1,0),(0,y_2)} = 1 \quad \text{and} \quad G_{(0,x_2),(y_1,0)} = 1. \tag{9.8}$$

Then we have

$$G_{(x_1,x_2),(y_1,y_2)} = G_{(x_1,0),(y_1,0)} \cdot G_{(0,x_2),(0,y_2)}. \tag{9.9}$$

To prove the first equation in (9.8), 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 its pth and qth powers are 1. Thus it has to be 1. The other equation in (9.8) can be proved the same way.

As a result, we have obtained our tensor product decomposition $\mathbf{G} = \mathbf{F}' \otimes \mathbf{F}''$:

$$\mathbf{F}' = \left(F'_{x,y} \equiv G_{(x,0),(y,0)}\right) \quad \text{and} \quad \mathbf{F}'' = \left(F''_{x,y} \equiv G_{(0,x),(0,y)}\right).$$

The only thing left is to show that $\mathbf{F}', \mathbf{F}''$ are both discrete unitary and satisfy $(\mathcal{GC})$. Here we only prove it for $\mathbf{F}'$. The proof for $\mathbf{F}''$ is the same. For all $x \neq y$,

$$\begin{aligned} 0 = \langle \mathbf{G}_{(x,0),*}, \mathbf{G}_{(y,0),*} \rangle &= \sum_{z_1,z_2} G_{(x,0),(z_1,z_2)} \overline{G_{(y,0),(z_1,z_2)}} \\ &= \sum_{z_1,z_2} G_{(x,0),(z_1,0)} G_{(0,0),(0,z_2)} \overline{G_{(y,0),(z_1,0)} G_{(0,0),(0,z_2)}} = m'' \cdot \langle \mathbf{F}'_{x,*}, \mathbf{F}'_{y,*} \rangle. \end{aligned}$$

Here we used the factorization (9.9) 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 all $x \neq y$. $\mathbf{F}'$ 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 the definition of M and (9.9), we have

$$pq = M = \operatorname{lcm}\{\text{order of } G_{(x_1,0),(y_1,0)} \cdot G_{(x_2,0),(y_2,0)} : \mathbf{x}, \mathbf{y}\}.$$

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, p is the least common multiple of orders of entries of $\mathbf{F}'$ and thus $\mathbf{F}'$ is p-discrete unitary. □

Next we prove Lemma 9.7, which deals with the case when M is a prime power.

PROPERTY 9.6. *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.*

Proof. Since M is a prime power, some entry of $\mathbf{A}$ has order exactly M as a root of unity. Hence it has the form ω_M^k for some k relatively prime to M. Then by the group condition $(\mathcal{GC})$ all powers of ω_M^k appear as entries of $\mathbf{A}$, in particular ω_M. □

LEMMA 9.7. *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 9.6, 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

$$S_1 = \left\{\mathbf{1}, \mathbf{F}_{a,*}, (\mathbf{F}_{a,*})^2, \ldots, (\mathbf{F}_{a,*})^{M-1}\right\}$$

denote the subgroup of F^{R} generated by $\mathbf{F}_{a,*}$. As the order of $\mathbf{F}_{a,*}$ is M, $|S_1| = M$.

Let S_2 denote the subset of F^{R} such that $\mathbf{u} \in S_2$ iff $u_b = 1$. Then it is clear that S_2 is a subgroup of F^{R}. Moreover, $(\mathbf{w}_1, \mathbf{w}_2) \mapsto \mathbf{w}_1 \circ \mathbf{w}_2$ is a group isomorphism from $S_1 \times S_2$ 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 bijection 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

$$\mathbf{F}_{i,*} = (\mathbf{F}_{a,*})^{f_1(i)} \circ \mathbf{u}_{f_2(i)} \quad \text{for all } i \in [0 : m-1]. \tag{9.10}$$

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 $\mathbf{v} \in F^{\mathrm{C}}$ such that $v_a = 1$. $(\mathbf{w}_1, \mathbf{w}_2) \mapsto \mathbf{w}_1 \circ \mathbf{w}_2$ is an isomorphism from $T_1 \times T_2$ 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 bijection 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

$$\mathbf{F}_{*,j} = (\mathbf{F}_{*,b})^{g_1(j)} \circ \mathbf{v}_{g_2(j)} \quad \text{for all } j \in [0 : m-1]. \tag{9.11}$$

In particular, we have $g(b) = (1, 0)$.

We are ready to permute the rows and columns of $\mathbf{F}$ to get a new $m \times m$ matrix $\mathbf{G}$. 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 (9.10) and (9.11), 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

$$\begin{aligned} G_{(x_1,x_2),(y_1,y_2)} &= (G_{(1,0),(y_1,y_2)})^{x_1} G_{(0,x_2),(y_1,y_2)} \\ &= (G_{(1,0),(1,0)})^{x_1 y_1} (G_{(1,0),(0,y_2)})^{x_1} (G_{(0,x_2),(1,0)})^{y_1} G_{(0,x_2),(0,y_2)}. \end{aligned}$$

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 (9.11), and 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 ath entry of $\mathbf{v}_{y_2}$, which is 1 by the definition of T_2. By (9.10),

$$G_{(0,x_2),(1,0)} = F_{f^{-1}(0,x_2),b} = (F_{a,b})^0 \cdot u_{x_2,b} = u_{x_2,b} = 1,$$

where $u_{x_2,b}$ denotes the bth entry of $\mathbf{u}_{x_2}$, which is 1 by the definition of S_2.

Combining all these equations, we have

$$G_{(x_1,x_2),(y_1,y_2)} = \omega_M^{x_1 y_1} \cdot G_{(0,x_2),(0,y_2)}. \tag{9.12}$$

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 (9.12), 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 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 (9.6),

$$F'_{x,z} = F_{f^{-1}(0,x),g^{-1}(0,z)} = u_{x,g^{-1}(0,z)} \quad \text{and} \quad F'_{y,z} = F_{f^{-1}(0,y),g^{-1}(0,z)} = u_{y,g^{-1}(0,z)}.$$

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 proof of (column-$\mathcal{GC}$) is similar. $\mathbf{F}'$ is also $p^{k'}$-discrete unitary for some $k' \leq k$. ∎

Theorem 5.6 then follows from Lemmas 9.5 and 9.7.

10. Proof of Theorem 5.8. 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; otherwise, we are done. For every r in $\mathcal{T}$ (recall that $\mathcal{T}$ is the set of $r \in [N-1]$ such that $\Delta_r \neq \emptyset$), we show that Δ_r must be a coset in $\mathbb{Z}_{\mathcal{Q}}$. Condition $(\mathcal{L}_2)$ then follows from the following lemma. Condition $(\mathcal{L}_1)$ about Λ_r can be proved similarly.

LEMMA 10.1. *Let Φ be a coset in $G_1 \times G_2$, where G_1 and G_2 are finite Abelian groups such that* $\gcd(|G_1|, |G_2|) = 1$. *Then for both $i = 1, 2$, there exists a coset Φ_i in G_i such that $\Phi = \Phi_1 \times \Phi_2$.*

Proof. First, we show that if $\mathbf{u} = (u_1, u_2), \mathbf{v} = (v_1, v_2) \in \Phi$, where $u_i, v_i \in G_i$, then $(u_1, v_2) \in \Phi$.

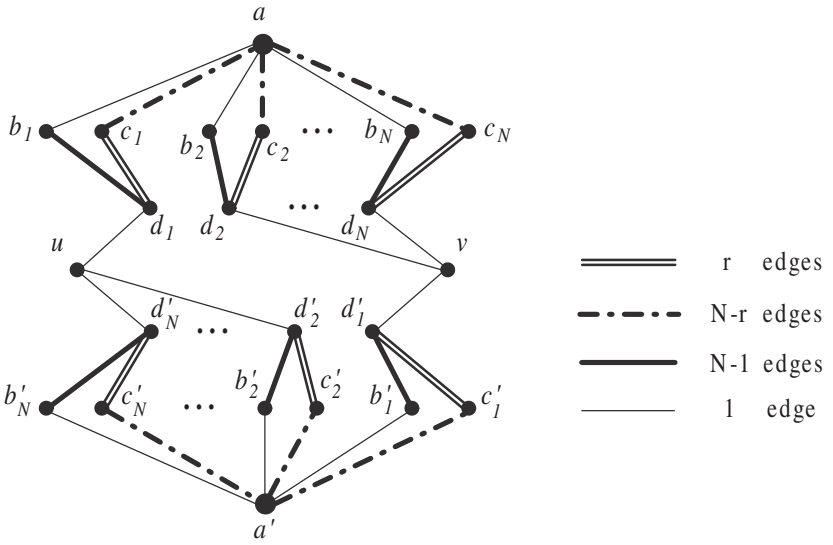

FIG. 10.1. *The gadget for constructing graph G'. (Note that the subscript e is suppressed.)*

Since $\gcd(|G_1|, |G_2|) = 1$, we can pick an integer k such that $|G_1| \,|\, k$ and $k \equiv 1 \pmod{|G_2|}$. As Φ is a coset, we have $\mathbf{u} + k(\mathbf{v} - \mathbf{u}) \in \Phi$. From $u_1 + k(v_1 - u_1) = u_1$ and $u_2 + k(v_2 - u_2) = v_2$, we conclude that $(u_1, v_2) \in \Phi$.

This implies the existence of $\Phi_1 \subseteq G_1$ and $\Phi_2 \subseteq G_2$ such that $\Phi = \Phi_1 \times \Phi_2$: Let

$$\Phi_1 = \big\{x \in G_1 : \exists\, y \in G_2, (x, y) \in \Phi\big\} \quad \text{and} \quad \Phi_2 = \big\{y \in G_2 : \exists\, x \in G_1, (x, y) \in \Phi\big\}.$$

Then both Φ_1 and Φ_2 are cosets (in G_1 and G_2, respectively), and $\Phi = \Phi_1 \times \Phi_2$. □

To prove Theorem 5.8, we need the following construction. Given an undirected graph $G = (V, E)$, we build a new graph G' by replacing every edge $e = uv \in E$ with the gadget shown in Figure 10.1. More exactly, we define $G' = (V', E')$ as

$$V' = V \cup \big\{a_e, b_{e,i}, c_{e,i}, d_{e,i}, a'_e, b'_{e,i}, c'_{e,i}, d'_{e,i} : e \in E \text{ and } i \in [N]\big\}$$

and E' contains exactly the following edges: For each $e = uv \in E$, add

1. one edge $(u, d_{e,1})$, $(v, d'_{e,1})$, $(u, d'_{e,i})$ and $(v, d_{e,i})$ for all $i \in [2 : N]$;
2. one edge $(a_e, b_{e,i})$ and $N - 1$ parallel edges $(b_{e,i}, d_{e,i})$ for all $i \in [N]$;
3. $N - r$ parallel edges $(a_e, c_{e,i})$ and r parallel edges $(c_{e,i}, d_{e,i})$ for all $i \in [N]$;
4. one edge $(a'_e, b'_{e,i})$ and $N - 1$ parallel edges $(b'_{e,i}, d'_{e,i})$ for all $i \in [N]$;
5. $N - r$ parallel edges $(a'_e, c'_{e,i})$ and r parallel edges $(c'_{e,i}, d'_{e,i})$ for all $i \in [N]$.

The degree of $d_{e,i}$ and $d'_{e,i}$ for all $e \in E, i \in [N]$, is $r \pmod N$. All other vertices in V' have degree $0 \pmod N$. It is also noted that the graph fragment that defines the gadget is bipartite, with $u, v, b_{e,i}, c_{e,i}, b'_{e,i}, c'_{e,i}$ on one side and $a_e, a'_e, d_{e,i}, d'_{e,i}$ on the other side. The way we construct G' gives us a $2m \times 2m$ matrix $\mathbf{A}$ such that $Z_{\mathbf{A}}(G) = Z_{\mathbf{C},\mathfrak{D}}(G')$ for all G, and thus $\mathsf{EVAL}(\mathbf{A}) \leq \mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$, 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 $\mathbb{Z}_{\mathcal{Q}}$, $A_{(0,\mathbf{u}),(1,\mathbf{v})} = A_{(1,\mathbf{u}),(0,\mathbf{v})} = 0$, which follows from the gadget being bipartite.

We now analyze the upper-left $m \times m$ block of $\mathbf{A}$. For $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_{\mathcal{Q}}$, $A_{(0,\mathbf{u}),(0,\mathbf{v})}$ is the product of the following two sums:

$$\sum_{\mathbf{a},\mathbf{d}_1,\ldots,\mathbf{d}_N\in\mathbb{Z}_{\mathcal{Q}}} F_{\mathbf{u},\mathbf{d}_1}\prod_{i=2}^{N}F_{\mathbf{v},\mathbf{d}_i}\left(\prod_{i=1}^{N}\left(\sum_{\mathbf{b}_i\in\mathbb{Z}_{\mathcal{Q}}}F_{\mathbf{b}_i,\mathbf{a}}\overline{F_{\mathbf{b}_i,\mathbf{d}_i}}\right)\left(\sum_{\mathbf{c}_i\in\mathbb{Z}_{\mathcal{Q}}}F_{\mathbf{c}_i,\mathbf{a}}^{N-r}F_{\mathbf{c}_i,\mathbf{d}_i}^{r}\right)\right)\prod_{i=1}^{N}D_{(1,\mathbf{d}_i)}^{[r]}$$

and

$$\sum_{\mathbf{a},\mathbf{d}_1,\ldots,\mathbf{d}_N\in\mathbb{Z}_{\mathcal{Q}}} F_{\mathbf{v},\mathbf{d}_1}\prod_{i=2}^{N}F_{\mathbf{u},\mathbf{d}_i}\left(\prod_{i=1}^{N}\left(\sum_{\mathbf{b}_i\in\mathbb{Z}_{\mathcal{Q}}}F_{\mathbf{b}_i,\mathbf{a}}\overline{F_{\mathbf{b}_i,\mathbf{d}_i}}\right)\left(\sum_{\mathbf{c}_i\in\mathbb{Z}_{\mathcal{Q}}}F_{\mathbf{c}_i,\mathbf{a}}^{N-r}F_{\mathbf{c}_i,\mathbf{d}_i}^{r}\right)\right)\prod_{i=1}^{N}D_{(1,\mathbf{d}_i)}^{[r]}.$$

Note that in deriving these sums, we used the fact that $M\,|\,N$ and entries of $\mathbf{F}$ are all powers of ω_M. Next, 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 m when $\mathbf{d}_i=\mathbf{a}$ and is 0 otherwise. The same thing can be said about those sums over $\mathbf{c}_i$. Assuming $\mathbf{d}_i=\mathbf{a}$ for all i, by $(\mathcal{U}_5)$, we have that

$$\prod_{i\in[N]}D_{(1,\mathbf{d}_i)}^{[r]}=\left(D_{(1,\mathbf{a})}^{[r]}\right)^N$$

is 1 when $\mathbf{a}\in\Delta_r$ and 0 otherwise. As a result, we have

(10.1)
$$A_{(0,\mathbf{u}),(0,\mathbf{v})}=\left(\sum_{\mathbf{a}\in\Delta_r}F_{\mathbf{u},\mathbf{a}}\overline{F_{\mathbf{v},\mathbf{a}}}m^{2N}\right)\left(\sum_{\mathbf{a}\in\Delta_r}F_{\mathbf{v},\mathbf{a}}\overline{F_{\mathbf{u},\mathbf{a}}}m^{2N}\right)=m^{4N}\left|\sum_{\mathbf{a}\in\Delta_r}F_{\mathbf{u},\mathbf{a}}\overline{F_{\mathbf{v},\mathbf{a}}}\right|^2.$$

By using condition $(\mathcal{R}_3)$, we can further simplify (10.1) to be

$$A_{(0,\mathbf{u}),(0,\mathbf{v})}=m^{4N}\left|\sum_{\mathbf{a}\in\Delta_r}F_{\mathbf{u}-\mathbf{v},\mathbf{a}}\right|^2=m^{4N}\left|\langle\chi,\mathbf{F}_{\mathbf{u}-\mathbf{v},*}\rangle\right|^2, \tag{10.2}$$

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

$$0\le A_{(0,\mathbf{u}),(0,\mathbf{v})}\le m^{4N}|\Delta_r|^2\ \text{ and }\ A_{(0,\mathbf{u}),(0,\mathbf{u})}=m^{4N}|\Delta_r|^2\quad\text{for all }\mathbf{u},\mathbf{v}\in\mathbb{Z}_{\mathcal{Q}}.$$

As $r\in\mathcal{T}$, we have $|\Delta_r|\ge 1$, and let n denote $|\Delta_r|$. Using the dichotomy of Bulatov and Grohe (Corollary 11.1) and the assumption that $\mathsf{EVAL}(\mathbf{A})$ is not #P-hard,

$$A_{(0,\mathbf{u}),(0,\mathbf{v})}\in\left\{0,m^{4N}n^2\right\}\ \text{ for all }\mathbf{u},\mathbf{v}\in\mathbb{Z}_{\mathcal{Q}}.$$

As a result, we have for all $\mathbf{u}\in\mathbb{Z}_{\mathcal{Q}}$,

$$\left|\langle\chi,\mathbf{F}_{\mathbf{u},*}\rangle\right|\in\{0,n\}. \tag{10.3}$$

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

$$\langle\chi,\mathbf{F}_{\mathbf{u},*}\rangle\in\left\{0,n,n\omega_M,n\omega_M^2,\ldots,n\omega_M^{M-1}\right\}. \tag{10.4}$$

Next, let $\mathfrak{a}$ denote a vector in Δ_r. We use Φ to denote $\mathfrak{a} + \langle \Delta_r - \mathfrak{a} \rangle$, where

$$\Delta_r - \mathfrak{a} \equiv \left\{ \mathbf{x} - \mathfrak{a} \,\middle|\, \mathbf{x} \in \Delta_r \right\}$$

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 $\Delta_r = \Phi$, which by definition is a coset in $\mathbb{Z}_{\mathcal{Q}}$. This, combined with Lemma 10.1, will finish the proof of Theorem 5.8.

To this end, we use $\boldsymbol{\kappa}$ 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 that for every $\mathbf{u} \in \mathbb{Z}_{\mathcal{Q}}$,

$$\langle \boldsymbol{\kappa}, \mathbf{F}_{\mathbf{u},*} \rangle = \frac{|\Phi|}{|\Delta_r|} \langle \chi, \mathbf{F}_{\mathbf{u},*} \rangle. \tag{10.5}$$

Since $\mathbf{F}$ is discrete unitary, $\{\mathbf{F}_{\mathbf{u},*} : \mathbf{u} \in \mathbb{Z}_{\mathcal{Q}}\}$ is an orthogonal basis. From (10.5),

$$\boldsymbol{\kappa} = \frac{|\Phi|}{|\Delta_r|} \chi,$$

which implies $\boldsymbol{\kappa} = \chi$ (since both are 0-1 vectors) and thus, $\Delta_r = \Phi$ is a coset in $\mathbb{Z}_{\mathcal{Q}}$.

We now prove (10.5). We make the following observations: (1) If $|\langle \chi, \mathbf{F}_{\mathbf{u},*} \rangle| = n$, then there is 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 (10.3)), 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 (10.4). 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 (10.5) 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 we have $F_{\mathbf{u},\mathbf{x}} = \omega_M^{\alpha}$ 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 $F_{\mathbf{u},\mathfrak{a}} = F_{\mathbf{u},\mathbf{x}_i} = \omega_M^{\alpha}$, we have

$$F_{\mathbf{u},\mathbf{x}} = F_{\mathbf{u},\mathfrak{a}+\sum_i h_i(\mathbf{x}_i-\mathfrak{a})} = F_{\mathbf{u},\mathfrak{a}} \prod_i F_{\mathbf{u},h_i(\mathbf{x}_i-\mathfrak{a})} = F_{\mathbf{u},\mathfrak{a}} \prod_i \left(F_{\mathbf{u},\mathbf{x}_i} \overline{F_{\mathbf{u},\mathfrak{a}}}\right)^{h_i} = \omega_M^{\alpha},$$

and the lemma is proved. ∎

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 $\ell(\mathbf{y} - \mathbf{z}) = \mathbf{0}$; then ℓ exists because $\mathbb{Z}_{\mathcal{Q}}$ is a finite group and $\ell > 1$ because $\mathbf{y} \neq \mathbf{z}$. We use c to denote $F_{\mathbf{u},\mathbf{y}} \overline{F_{\mathbf{u},\mathbf{z}}}$. By $(\mathcal{R}_3)$ together with the assumption, we have $c^{\ell} = F_{\mathbf{u},\ell(\mathbf{y}-\mathbf{z})} = 1$ but $c \neq 1$.

We define the following equivalence relation $\sim$ over Φ. For $\mathbf{x}, \mathbf{x}' \in \Phi$, $\mathbf{x} \sim \mathbf{x}'$ iff there exists an integer k such that $\mathbf{x} - \mathbf{x}' = k(\mathbf{y} - \mathbf{z})$. For each $\mathbf{x} \in \Phi$, 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, by using $(\mathcal{R}_3)$,

$$\sum_{i=0}^{l-1} F_{\mathbf{u},\mathbf{x}+i(\mathbf{y}-\mathbf{z})} = F_{\mathbf{u},\mathbf{x}} \sum_{i=0}^{l-1} c^i = F_{\mathbf{u},\mathbf{x}} \frac{1 - c^l}{1 - c} = 0,$$

and the lemma is proved. ∎

Now (10.5) can be proved as follows. If $|\langle \chi, \mathbf{F}_{\mathbf{u},*} \rangle| = n\ (= |\Delta_r|)$, then by observation (1) and Lemma 10.2, $|\langle \boldsymbol{\kappa}, \mathbf{F}_{\mathbf{u},*} \rangle| = |\Phi|$. If $|\langle \chi, \mathbf{F}_{\mathbf{u},*} \rangle| \neq n$, then $\langle \chi, \mathbf{F}_{\mathbf{u},*} \rangle = 0$. By observation (2) and $\Delta_r \subseteq \Phi$, Lemma 10.3 implies $\langle \boldsymbol{\kappa}, \mathbf{F}_{\mathbf{u},*} \rangle = 0$. Therefore, 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. A Corollary of Theorem 5.8. Now that we have proved Theorem 5.8, we know that unless the problem is #P-hard, we may assume that $(\mathcal{L})$ holds. Thus, Λ_r and Δ_r are cosets.

COROLLARY 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 $\mathbf{H}_{\mathbf{u},*} = \omega_M^{\alpha} \mathbf{H}_{\mathbf{v},*}$; otherwise, Lemma 10.3 says that $\langle \mathbf{H}_{\mathbf{u},*}, \mathbf{H}_{\mathbf{v},*} \rangle = 0$.

The proof for $\mathbf{G}$ is exactly the same. ∎

As part of a discrete unitary matrix $\mathbf{F}$, all columns $\{\mathbf{H}_{*,\mathbf{u}} \mid \mathbf{u} \in \Delta_r\}$ of $\mathbf{H}$ must be orthogonal and thus $\operatorname{rank}(\mathbf{H}) = |\Delta_r|$. 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 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 Corollary 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 Corollary 10.4 again, which is absurd. A symmetric statement for $\mathbf{G}$ also holds.

11. Proof of Theorem 5.9. Let $((M, N), \mathbf{C}, \mathfrak{D}, (\mathbf{p}, \mathbf{t}, \mathcal{Q}))$ be a tuple that satisfies $(\mathcal{R})$ 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 $\Lambda_r = \prod_{i=1}^{s} \Lambda_{r,i}$ for every $r \in \mathcal{S}$ and $\Delta_r = \prod_{i=1}^{s} \Delta_{r,i}$ 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 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 let $n = |\Lambda_r| \geq 1$. 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. $\{\mathbf{G}_{*,\mathfrak{b}_i} : i \in [0 : n-1]\}$ *forms an orthogonal basis;*
2. *for all* $\mathbf{b} \in \mathbb{Z}_{\mathcal{Q}}$, $\exists\, i \in [0 : n-1]$ *and* $\alpha \in \mathbb{Z}_M$ *such that* $\mathbf{G}_{*,\mathbf{b}} = \omega_M^{\alpha} \cdot \mathbf{G}_{*,\mathfrak{b}_i}$;
3. *let* A_i *be the set of* $\mathbf{b} \in \mathbb{Z}_{\mathcal{Q}}$ *s.t.* $\mathbf{G}_{*,\mathbf{b}}$ *is linearly dependent on* $\mathbf{G}_{*,\mathfrak{b}_i}$; *then*

$$|A_0| = |A_1| = \cdots = |A_{n-1}| = m/n.$$

Proof. By Corollary 10.4, and the discussion following Corollary 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 $(\mathcal{R}_3)$, fixing $\mathfrak{b}_i$ for any i, there is a bijection 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 $|A_0| = |A_1| = \cdots = |A_{n-1}| = m/n$. ∎

Now let $G = (V, E)$ be an undirected graph. For each positive integer p we build a new graph $G^{[p]}$ from G by replacing every edge $e = uv \in E$ with a gadget. We 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.)

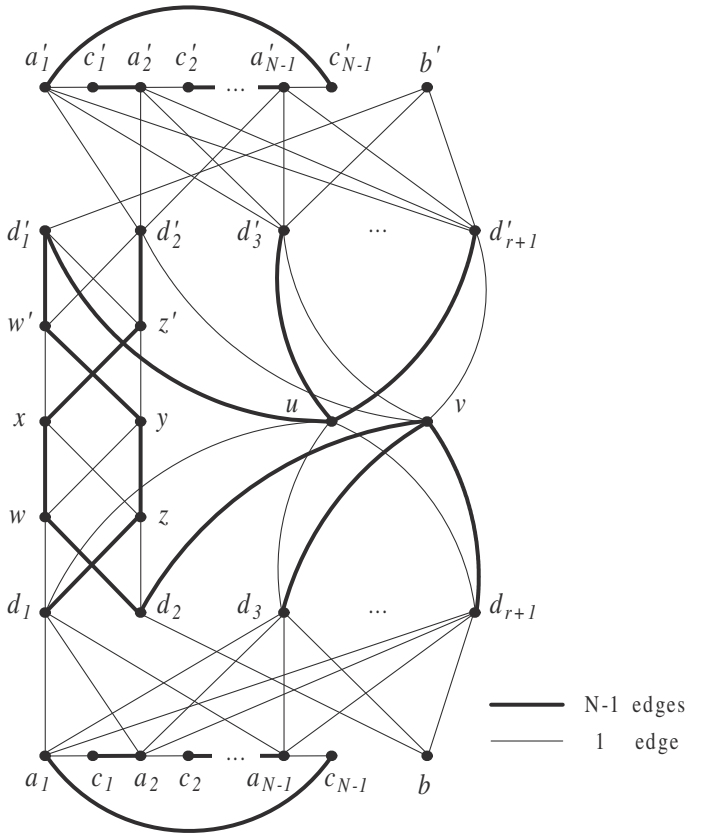

FIG. 11.1. *The gadget for constructing $G^{[1]}$. (Note that the subscript e is suppressed.)*

The gadget for $G^{[1]}$ is shown in Figure 11.1. Here $G^{[1]} = (V^{[1]}, E^{[1]})$, where

$$V^{[1]} = V \cup \big\{ x_e, y_e, a_{e,i}, a'_{e,i}, b_e, b'_e, c_{e,i}, c'_{e,i}, d_{e,j}, d'_{e,j}, w_e, w'_e, z_e, z'_e : e \in E, i \in [N-1], j \in [r+1] \big\},$$

and $E^{[1]}$ contains exactly the following edges: For every edge $e = uv \in E$, add

1. one edge $(u, d_{e,j})$ for all $j \in [r+1] - \{2\}$;
2. $N-1$ parallel edges $(v, d_{e,j})$ for all $j \in [r+1] - \{1\}$;
3. one edge $(d_{e,1}, w_e)$, $(d_{e,2}, z_e)$, (w_e, y_e), and (z_e, x_e);
4. $N-1$ parallel edges $(d_{e,1}, z_e)$, $(d_{e,2}, w_e)$, (w_e, x_e), and (z_e, y_e);
5. one edge $(a_{e,i}, d_{e,j})$ for all $i \in [N-1]$ and $j \in [r+1] - \{2\}$;
6. one edge $(b_e, d_{e,j})$ for all $j \in [r+1] - \{1\}$;
7. $N-1$ parallel edges $(c_{e,N-1}, a_{e,1})$ and $(c_{e,i}, a_{e,i+1})$ for all $i \in [N-2]$;
8. one edge $(a_{e,i}, c_{e,i})$ for all $i \in [N-1]$;
9. $N-1$ parallel edges $(u, d'_{e,j})$ for all $j \in [r+1] - \{2\}$;
10. one edge $(v, d'_{e,j})$ for all $j \in [r+1] - \{1\}$;
11. one edge $(d'_{e,1}, z'_e)$, $(d'_{e,2}, w'_e)$, (w'_e, x_e), and (z'_e, y_e);
12. $N-1$ parallel edges $(d'_{e,1}, w'_e)$, $(d'_{e,2}, z'_e)$, (w'_e, y_e), and (z'_e, x_e);
13. one edge $(a'_{e,i}, d'_{e,j})$ for all $i \in [N-1]$ and $j \in [r+1] - \{1\}$;
14. one edges $(b'_e, d'_{e,j})$ for all $j \in [r+1] - \{2\}$;

15. $N-1$ parallel edges $(c'_{e,N-1}, a'_{e,1})$ and $(c'_{e,i}, a'_{e,i+1})$ for all $i \in [N-2]$;
16. one edge $(a'_{e,i}, c'_{e,i})$ for all $i \in [N-1]$.

As indicated earlier, the graph we really need in the proof is $G^{[2]}$. The gadget for $G^{[2]}$ consists of two disjoint copies of the gadget for $G^{[1]}$, with the respective copies of the vertices u, v, x, and y in the two copies identified. Given $G = (V, E)$, we use this new gadget to build $G^{[2]}$ by replacing each $e = uv \in E$ with this gadget. The degree of every vertex in $G^{[2]}$ is a 0 (mod N) except both copies of $a_{e,i}, a'_{e,i}, b_e$, and b'_e whose degree is r (mod N).

The construction gives us a $2m \times 2m$ matrix $\mathbf{A}$ such that $Z_{\mathbf{A}}(G) = Z_{\mathbf{C},\mathfrak{D}}(G^{[2]})$ for all G and thus $\mathsf{EVAL}(\mathbf{A})$ $(\leq \mathsf{EVAL}(\mathbf{C}, \mathfrak{D}))$ (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 and columns of $\mathbf{A}$ in the same way as we do for $\mathbf{C}$: The first m rows and columns are indexed by $\{0\} \times \mathbb{Z}_{\mathcal{Q}}$ and the last m rows and columns are indexed by $\{1\} \times \mathbb{Z}_{\mathcal{Q}}$. Since $\mathbf{C}$ is the bipartization of $\mathbf{F}$, we have $A_{(0,\mathbf{u}),(1,\mathbf{v})} = A_{(1,\mathbf{u}),(0,\mathbf{v})} = 0$ for all $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_{\mathcal{Q}}$.

Next we analyze the upper-left $m \times m$ block of $\mathbf{A}$. Given $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_{\mathcal{Q}}$, let $A_{\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}}$ denote the following sum:

$$\sum_{\substack{\mathbf{a}_1,\ldots,\mathbf{a}_{N-1},\mathbf{b}\in\Lambda_r,\\ \mathbf{d}_1,\mathbf{d}_2\in\mathbb{Z}_{\mathcal{Q}}}} D^{[r]}_{(0,\mathbf{b})} \prod_{i=1}^{N-1} D^{[r]}_{(0,\mathbf{a}_i)} \left(\sum_{\mathbf{w}\in\mathbb{Z}_{\mathcal{Q}}} F_{\mathbf{w},\mathbf{d}_1} F_{\mathbf{w},\mathbf{y}} \overline{F_{\mathbf{w},\mathbf{d}_2} F_{\mathbf{w},\mathbf{x}}} \right) \left(\sum_{\mathbf{z}\in\mathbb{Z}_{\mathcal{Q}}} F_{\mathbf{z},\mathbf{d}_2} F_{\mathbf{z},\mathbf{x}} \overline{F_{\mathbf{z},\mathbf{d}_1} F_{\mathbf{z},\mathbf{y}}} \right)$$
$$\times \left(\prod_{i=1}^{N-2} \sum_{\mathbf{c}_i\in\mathbb{Z}_{\mathcal{Q}}} F_{\mathbf{a}_i,\mathbf{c}_i} \overline{F_{\mathbf{a}_{i+1},\mathbf{c}_i}} \right) \left(\sum_{\mathbf{c}_{N-1}\in\mathbb{Z}_{\mathcal{Q}}} F_{\mathbf{a}_{N-1},\mathbf{c}_{N-1}} \overline{F_{\mathbf{a}_1,\mathbf{c}_{N-1}}} \right)$$
$$\times \left(\prod_{i=3}^{r+1} \sum_{\mathbf{d}_i\in\mathbb{Z}_{\mathcal{Q}}} F_{\mathbf{u},\mathbf{d}_i} F_{\mathbf{b},\mathbf{d}_i} \overline{F_{\mathbf{v},\mathbf{d}_i}} \prod_{j=1}^{N-1} F_{\mathbf{a}_j,\mathbf{d}_i} \right) F_{\mathbf{u},\mathbf{d}_1} \left(\prod_{j=1}^{N-1} F_{\mathbf{a}_j,\mathbf{d}_1} \right) \overline{F_{\mathbf{v},\mathbf{d}_2}} F_{\mathbf{b},\mathbf{d}_2};$$

let $B_{\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}}$ denote the following sum:

$$\sum_{\substack{\mathbf{a}_1,\ldots,\mathbf{a}_{N-1},\mathbf{b}\in\Lambda_r,\\ \mathbf{d}_1,\mathbf{d}_2\in\mathbb{Z}_{\mathcal{Q}}}} D^{[r]}_{(0,\mathbf{b})} \prod_{i=1}^{N-1} D^{[r]}_{(0,\mathbf{a}_i)} \left(\sum_{\mathbf{w}\in\mathbb{Z}_{\mathcal{Q}}} F_{\mathbf{w},\mathbf{d}_2} F_{\mathbf{w},\mathbf{x}} \overline{F_{\mathbf{w},\mathbf{d}_1} F_{\mathbf{w},\mathbf{y}}} \right) \left(\sum_{\mathbf{z}\in\mathbb{Z}_{\mathcal{Q}}} F_{\mathbf{z},\mathbf{d}_1} F_{\mathbf{z},\mathbf{y}} \overline{F_{\mathbf{z},\mathbf{d}_2} F_{\mathbf{z},\mathbf{x}}} \right)$$
$$\times \left(\prod_{i=1}^{N-2} \sum_{\mathbf{c}_i\in\mathbb{Z}_{\mathcal{Q}}} F_{\mathbf{a}_i,\mathbf{c}_i} \overline{F_{\mathbf{a}_{i+1},\mathbf{c}_i}} \right) \left(\sum_{\mathbf{c}_{N-1}\in\mathbb{Z}_{\mathcal{Q}}} F_{\mathbf{a}_{N-1},\mathbf{c}_{N-1}} \overline{F_{\mathbf{a}_1,\mathbf{c}_{N-1}}} \right)$$
$$\times \left(\prod_{i=3}^{r+1} \sum_{\mathbf{d}_i\in\mathbb{Z}_{\mathcal{Q}}} F_{\mathbf{v},\mathbf{d}_i} F_{\mathbf{b},\mathbf{d}_i} \overline{F_{\mathbf{u},\mathbf{d}_i}} \prod_{j=1}^{N-1} F_{\mathbf{a}_j,\mathbf{d}_i} \right) F_{\mathbf{v},\mathbf{d}_2} \left(\prod_{j=1}^{N-1} F_{\mathbf{a}_j,\mathbf{d}_2} \right) \overline{F_{\mathbf{u},\mathbf{d}_1}} F_{\mathbf{b},\mathbf{d}_1}.$$

Then we have

$$A_{(0,\mathbf{u}),(0,\mathbf{v})} = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{Z}_{\mathcal{Q}}} A^2_{\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}} B^2_{\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}}.$$

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

$$\sum_{\mathbf{w}\in\mathbb{Z}_{\mathcal{Q}}} F_{\mathbf{w},\mathbf{d}_1} F_{\mathbf{w},\mathbf{y}} \overline{F_{\mathbf{w},\mathbf{d}_2} F_{\mathbf{w},\mathbf{x}}} = \langle \mathbf{F}_{*,\mathbf{d}_1+\mathbf{y}}, \mathbf{F}_{*,\mathbf{d}_2+\mathbf{x}} \rangle = \begin{cases} m & \text{if } \mathbf{d}_1 - \mathbf{d}_2 = \mathbf{x} - \mathbf{y}, \\ 0 & \text{otherwise.} \end{cases}$$

Also when $\mathbf{d}_1 - \mathbf{d}_2 = \mathbf{x} - \mathbf{y}$, we have $\sum_{\mathbf{z}\in\mathbb{Z}_\mathcal{Q}} F_{\mathbf{z},\mathbf{d}_2} F_{\mathbf{z},\mathbf{x}} \overline{F_{\mathbf{z},\mathbf{d}_1} F_{\mathbf{z},\mathbf{y}}} = m$. 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 $i = 1, \ldots, N-2$, and

$$\sum_{\mathbf{c}_{N-1}\in\mathbb{Z}_\mathcal{Q}} F_{\mathbf{a}_{N-1},\mathbf{c}_{N-1}} \overline{F_{\mathbf{a}_1,\mathbf{c}_{N-1}}} = \langle \mathbf{F}_{\mathbf{a}_{N-1},*}, \mathbf{F}_{\mathbf{a}_1,*} \rangle$$

is zero unless $\mathbf{a}_{N-1} = \mathbf{a}_1$. When $\mathbf{a}_1 = \cdots = \mathbf{a}_{N-1}$, all these inner products are equal to m. So now we may assume that $\mathbf{d}_1 - \mathbf{d}_2 = \mathbf{x} - \mathbf{y}$ 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 $\mathbf{x} - \mathbf{y} = \mathbf{s}$. Then $A_{\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}}$ is equal to

(11.1)

$$m^{N+1} \sum_{\substack{\mathbf{a},\mathbf{b}\in\Lambda_r \\ \mathbf{d}_2\in\mathbb{Z}_\mathcal{Q}}} D^{[r]}_{(0,\mathbf{b})} \overline{D^{[r]}_{(0,\mathbf{a})}} \left(\prod_{i=3}^{r+1} \sum_{\mathbf{d}_i\in\mathbb{Z}_\mathcal{Q}} F_{\mathbf{u},\mathbf{d}_i} F_{\mathbf{b},\mathbf{d}_i} \overline{F_{\mathbf{v},\mathbf{d}_i} F_{\mathbf{a},\mathbf{d}_i}} \right) F_{\mathbf{u},\mathbf{d}_2+\mathbf{s}} F_{\mathbf{b},\mathbf{d}_2} \overline{F_{\mathbf{v},\mathbf{d}_2} F_{\mathbf{a},\mathbf{d}_2+\mathbf{s}}}.$$

Again we have

$$\sum_{\mathbf{d}_i\in\mathbb{Z}_\mathcal{Q}} F_{\mathbf{u},\mathbf{d}_i} F_{\mathbf{b},\mathbf{d}_i} \overline{F_{\mathbf{v},\mathbf{d}_i} F_{\mathbf{a},\mathbf{d}_i}} = \langle \mathbf{F}_{\mathbf{u}+\mathbf{b},*}, \mathbf{F}_{\mathbf{v}+\mathbf{a},*} \rangle = \begin{cases} m & \text{if } \mathbf{u}+\mathbf{b} = \mathbf{v}+\mathbf{a}, \\ 0 & \text{otherwise.} \end{cases}$$

If $\mathbf{v} - \mathbf{u} \notin \Lambda_r^{\mathrm{lin}} \equiv \{\mathbf{x} - \mathbf{x}' : \mathbf{x}, \mathbf{x}' \in \Lambda_r\}$, then $A_{\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}} = 0$ as $\mathbf{a}, \mathbf{b} \in \Lambda_r$, $\mathbf{b} - \mathbf{a} \in \Lambda_r^{\mathrm{lin}}$.

For every $\mathbf{h} \in \Lambda_r^{\mathrm{lin}}$ (e.g., $\mathbf{h} = \mathbf{v} - \mathbf{u}$), we define a $|\Lambda_r|$-dimensional vector $\mathbf{T}^{[\mathbf{h}]}$:

$$T^{[\mathbf{h}]}_{\mathbf{x}} = D^{[r]}_{(0,\mathbf{x}+\mathbf{h})} \overline{D^{[r]}_{(0,\mathbf{x})}} \quad \text{for all } \mathbf{x} \in \Lambda_r.$$

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 nonzero 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 $\mathbf{v} - \mathbf{u} \in \Lambda_r^{\mathrm{lin}}$; then

$$\begin{aligned} A_{\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}} &= m^{N+r} \sum_{\substack{\mathbf{a}\in\Lambda_r, \mathbf{d}_2\in\mathbb{Z}_\mathcal{Q} \\ \mathbf{b}=\mathbf{a}+\mathbf{v}-\mathbf{u}}} D^{[r]}_{(0,\mathbf{b})} \overline{D^{[r]}_{(0,\mathbf{a})}} F_{\mathbf{u},\mathbf{d}_2+\mathbf{s}} F_{\mathbf{b},\mathbf{d}_2} \overline{F_{\mathbf{v},\mathbf{d}_2} F_{\mathbf{a},\mathbf{d}_2+\mathbf{s}}} \\ &= m^{N+r+1} \sum_{\mathbf{a}\in\Lambda_r} D^{[r]}_{(0,\mathbf{a}+\mathbf{v}-\mathbf{u})} \overline{D^{[r]}_{(0,\mathbf{a})}} F_{\mathbf{u},\mathbf{s}} \overline{F_{\mathbf{a},\mathbf{s}}} \\ &= m^{N+r+1} \cdot F_{\mathbf{u},\mathbf{x}-\mathbf{y}} \langle \mathbf{T}^{[\mathbf{v}-\mathbf{u}]}, \mathbf{G}_{*,\mathbf{x}-\mathbf{y}} \rangle. \end{aligned}$$

Here we used $(\mathcal{R}_3)$ in the second equality, and we recall the definition of $\mathbf{s} = \mathbf{x} - \mathbf{y}$.

Similarly, when $\mathbf{v} - \mathbf{u} \notin \Lambda_r^{\mathrm{lin}}$, we have $B_{\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}} = 0$, and when $\mathbf{v} - \mathbf{u} \in \Lambda_r^{\mathrm{lin}}$,

$$\begin{aligned} B_{\mathbf{u},\mathbf{v},\mathbf{x},\mathbf{y}} &= m^{N+r} \sum_{\substack{\mathbf{b}\in\Lambda_r, \mathbf{d}_2\in\mathbb{Z}_\mathcal{Q} \\ \mathbf{a}=\mathbf{b}+\mathbf{v}-\mathbf{u}}} D^{[r]}_{(0,\mathbf{b})} \overline{D^{[r]}_{(0,\mathbf{a})}} F_{\mathbf{v},\mathbf{d}_2} F_{\mathbf{b},\mathbf{d}_2+\mathbf{x}-\mathbf{y}} \overline{F_{\mathbf{a},\mathbf{d}_2} F_{\mathbf{u},\mathbf{d}_2+\mathbf{x}-\mathbf{y}}} \\ &= m^{N+r+1} \cdot \overline{F_{\mathbf{u},\mathbf{x}-\mathbf{y}} \langle \mathbf{T}^{[\mathbf{v}-\mathbf{u}]}, \mathbf{G}_{*,\mathbf{x}-\mathbf{y}} \rangle}. \end{aligned}$$

To summarize, when $\mathbf{v} - \mathbf{u} \notin \Lambda_r^{\mathrm{lin}}$, $A_{(0,\mathbf{u}),(0,\mathbf{v})} = 0$, and when $\mathbf{v} - \mathbf{u} \in \Lambda_r^{\mathrm{lin}}$,

(11.2)

$$A_{(0,\mathbf{u}),(0,\mathbf{v})} = m^{4(N+r+1)} \sum_{\mathbf{x},\mathbf{y}\in\mathbb{Z}_\mathcal{Q}} \left| \langle \mathbf{T}^{[\mathbf{v}-\mathbf{u}]}, \mathbf{G}_{*,\mathbf{x}-\mathbf{y}} \rangle \right|^4 = m^{4N+4r+5} \sum_{\mathbf{b}\in\mathbb{Z}_\mathcal{Q}} \left| \langle \mathbf{T}^{[\mathbf{v}-\mathbf{u}]}, \mathbf{G}_{*,\mathbf{b}} \rangle \right|^4.$$

We now show that $\mathbf{A}$ is symmetric. Let $\mathbf{a} = \mathbf{v} - \mathbf{u} \in \Lambda_r^{\mathrm{lin}}$. By $(\mathcal{R}_3)$, for $\mathbf{b} \in \mathbb{Z}_{\mathcal{Q}}$,

$$\left|\langle \mathbf{T}^{[-\mathbf{a}]}, \mathbf{G}_{*,-\mathbf{b}}\rangle\right| = \left|\sum_{\mathbf{x}\in\Lambda_r} D^{[r]}_{(0,\mathbf{x}-\mathbf{a})}\overline{D^{[r]}_{(0,\mathbf{x})}G_{\mathbf{x},-\mathbf{b}}}\right| = \left|\sum_{\mathbf{x}\in\Lambda_r} D^{[r]}_{(0,\mathbf{x})}\overline{D^{[r]}_{(0,\mathbf{x}-\mathbf{a})}G_{\mathbf{x},\mathbf{b}}}\right|$$

$$= \left|\sum_{\mathbf{y}\in\Lambda_r} D^{[r]}_{(0,\mathbf{y}+\mathbf{a})}\overline{D^{[r]}_{(0,\mathbf{y})}G_{\mathbf{y},\mathbf{b}}F_{\mathbf{a},\mathbf{b}}}\right| = \left|\sum_{\mathbf{y}\in\Lambda_r} D^{[r]}_{(0,\mathbf{y}+\mathbf{a})}\overline{D^{[r]}_{(0,\mathbf{y})}G_{\mathbf{y},\mathbf{b}}}\right| = \left|\langle \mathbf{T}^{[\mathbf{a}]}, \mathbf{G}_{*,\mathbf{b}}\rangle\right|,$$

where the second equality is by conjugation, the third equality is by the substitution $\mathbf{x} = \mathbf{y}+\mathbf{a}$, and the fourth equality is because $F_{\mathbf{a},\mathbf{b}}$ is a root of unity. Thus, $A_{(0,\mathbf{u}),(0,\mathbf{v})} = A_{(0,\mathbf{v}),(0,\mathbf{u})}$. The lower-right block can be proved similarly. Hence $\mathbf{A}$ is symmetric.

Next, we further simplify (11.2) using Lemma 11.1:

$$A_{(0,\mathbf{u}),(0,\mathbf{v})} = \frac{m^{4N+4r+6}}{n} \cdot \sum_{i=0}^{n-1} \left|\langle \mathbf{T}^{[\mathbf{v}-\mathbf{u}]}, \mathbf{G}_{*,\mathfrak{b}_i}\rangle\right|^4. \tag{11.3}$$

For the special case of $\mathbf{u} = \mathbf{v}$, since $\mathbf{T}^{[\mathbf{0}]} = \mathbf{1} = \mathbf{G}_{*,\mathfrak{b}_0}$ and $\{\mathbf{G}_{*,\mathfrak{b}_0}, \ldots, \mathbf{G}_{*,\mathfrak{b}_{n-1}}\}$ is an orthogonal basis by Lemma 11.1, we have

$$\sum_{i=0}^{n-1} \left|\langle \mathbf{T}^{[\mathbf{0}]}, \mathbf{G}_{*,\mathfrak{b}_i}\rangle\right|^4 = n^4 \quad \text{and} \quad A_{(0,\mathbf{u}),(0,\mathbf{u})} = L \cdot n^4, \quad \text{where } L \equiv m^{4N+4r+6}/n.$$

Our next goal is to prove for all $\mathbf{a} \in \Lambda_r^{\mathrm{lin}}$ that there exist $\mathbf{b} \in \mathbb{Z}_{\mathcal{Q}}$, $\alpha \in \mathbb{Z}_N$ such that

$$\mathbf{T}^{[\mathbf{a}]} = \omega_N^{\alpha} \cdot \mathbf{G}_{*,\mathbf{b}}. \tag{11.4}$$

If $|\Lambda_r^{\mathrm{lin}}| = 1$, then (11.4) is trivially true. Thus below we assume $|\Lambda_r^{\mathrm{lin}}| > 1$. Because $\mathbf{A}$ is symmetric and nonnegative, we can apply the dichotomy theorem of Bulatov and Grohe. For any pair $\mathbf{u} \neq \mathbf{v}$ such that $\mathbf{u} - \mathbf{v} \in \Lambda_r^{\mathrm{lin}}$, we consider the 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 2.6, 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 (11.3) we get

$$\sum_{i=0}^{n-1} \left|\langle \mathbf{T}^{[\mathbf{v}-\mathbf{u}]}, \mathbf{G}_{*,\mathfrak{b}_i}\rangle\right|^4 \in \{0, n^4\} \quad \text{for all } \mathbf{u}, \mathbf{v} \text{ such that } \mathbf{u} - \mathbf{v} \in \Lambda_r^{\mathrm{lin}}. \tag{11.5}$$

However, the sum in (11.5) cannot be zero, because by Lemma 11.1, $\{\mathbf{G}_{*,\mathfrak{b}_i} : i \in [0 : n-1]\}$ is an orthogonal basis with each $\|\mathbf{G}_{*,\mathfrak{b}_i}\|^2 = n$. Then by Parseval,

$$\sum_{i=0}^{n-1} \left|\langle \mathbf{T}^{[\mathbf{v}-\mathbf{u}]}, \frac{\mathbf{G}_{*,\mathfrak{b}_i}}{\|\mathbf{G}_{*,\mathfrak{b}_i}\|}\rangle\right|^2 = \|\mathbf{T}^{[\mathbf{v}-\mathbf{u}]}\|^2 = n,$$

as 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 $0 \le i < n$, $|\langle \mathbf{T}^{[\mathbf{v}-\mathbf{u}]}, \mathbf{G}_{*,\mathfrak{b}_i}\rangle| \neq 0$, and therefore the sum in (11.5) is nonzero, and thus in fact

$$\sum_{i=0}^{n-1} \left|\langle \mathbf{T}^{[\mathbf{v}-\mathbf{u}]}, \mathbf{G}_{*,\mathbf{b}_i}\rangle\right|^4 = n^4 \quad \text{for all } \mathbf{u},\mathbf{v} \text{ such that } \mathbf{u}-\mathbf{v} \in \Lambda_r^{\text{lin}}.$$

If we temporarily denote $x_i = |\langle \mathbf{T}^{[\mathbf{v}-\mathbf{u}]}, \mathbf{G}_{*,\mathbf{b}_i}\rangle|$ for $0 \le i < n$, then each $x_i \ge 0$. We have both $\sum_{i=0}^{n-1} x_i^2 = n^2$ and $\sum_{i=0}^{n-1} x_i^4 = n^4$. By taking the square, we have

$$n^4 = \left(\sum_{i=0}^{n-1} x_i^2\right)^2 = \sum_{i=0}^{n-1} x_i^4 + \text{ nonnegative cross terms.}$$

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

$$\left|\langle \mathbf{T}^{[\mathbf{v}-\mathbf{u}]}, \mathbf{G}_{*,\mathbf{b}_i}\rangle\right| = n.$$

Applying again the argument that $\langle \mathbf{T}^{[\mathbf{v}-\mathbf{u}]}, \mathbf{G}_{*,\mathbf{b}_i}\rangle$ is a sum of n terms, each of which is a root of unity, (11.4) follows.

Below we use (11.4) to prove $(\mathcal{D}_3)$. Note that if $s = 1$, then $(\mathcal{D}_3)$ follows directly from (11.4). Thus below we assume $s > 1$. First, (11.4) implies the following lemma.

LEMMA 11.2. *Let* $\mathbf{a} \in \Lambda_{r,k}^{\text{lin}}$ *for some* $k \in [s]$. *Then for any* $\ell \neq k$ *and* $\mathbf{c} \in \Lambda_{r,\ell}^{\text{lin}}$,

$$T_{\mathbf{x}+\widetilde{\mathbf{c}}}^{[\widetilde{\mathbf{a}}]} \Big/ T_{\mathbf{x}}^{[\widetilde{\mathbf{a}}]}$$

is a power of ω_{q_ℓ} *for all* $\mathbf{x} \in \Lambda_r$.

Recall that $q_\ell = q_{\ell,1}$. 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, we can divide one by the other.

Proof. By (11.4), 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 $\mathbf{a} \in \Lambda_{r,k}^{\text{lin}}$ and $\mathbf{c} \in \Lambda_{r,\ell}^{\text{lin}}$, $\ell \neq k \in [s]$. By the definition of $T_{\mathbf{x}}^{[\mathbf{h}]}$ in terms of $D_*^{[r]}$,

$$T_{\mathbf{x}+\widetilde{\mathbf{a}}}^{[\widetilde{\mathbf{c}}]} \cdot T_{\mathbf{x}}^{[\widetilde{\mathbf{a}}]} = T_{\mathbf{x}}^{[\widetilde{\mathbf{a}}+\widetilde{\mathbf{c}}]} = T_{\mathbf{x}+\widetilde{\mathbf{c}}}^{[\widetilde{\mathbf{a}}]} \cdot T_{\mathbf{x}}^{[\widetilde{\mathbf{c}}]},$$

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 $k \neq \ell$, $\gcd(q_k, q_\ell) = 1$, so

$$T_{\mathbf{x}+\widetilde{\mathbf{c}}}^{[\widetilde{\mathbf{a}}]} \Big/ T_{\mathbf{x}}^{[\widetilde{\mathbf{a}}]} = 1 \quad \text{for all } \mathbf{c} \in \Lambda_{r,\ell}^{\text{lin}} \text{ such that } \ell \neq k. \tag{11.6}$$

This implies that $T_{\mathbf{x}}^{[\widetilde{\mathbf{a}}]}$, as a function of $\mathbf{x}$, only depends on $\mathbf{x}_k \in \Lambda_{r,k}$. By (11.4),

$$T_{\mathbf{x}}^{[\widetilde{\mathbf{a}}]} = T_{\mathbf{ext}_r(\mathbf{x}_k)}^{[\widetilde{\mathbf{a}}]} = \omega_N^{\alpha} \cdot G_{\mathbf{ext}_r(\mathbf{x}_k),\mathbf{b}} = \omega_N^{\alpha+\beta} \cdot F_{\widetilde{\mathbf{x}_k},\widetilde{\mathbf{b}_k}} = \omega_N^{\alpha+\beta} \cdot F_{\mathbf{x},\widetilde{\mathbf{b}_k}}$$

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 $(\mathcal{D}_3)$. Let $\mathfrak{a}^{[r]} = (\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_s) \in \Lambda_r$. Then

$$\begin{aligned} D^{[r]}_{(0,\mathbf{x})} &= D^{[r]}_{(0,(\mathbf{x}_1,\mathbf{x}_2,\dots,\mathbf{x}_s))}\overline{D^{[r]}_{(0,(\mathbf{a}_1,\mathbf{a}_2,\dots,\mathbf{a}_s))}} \\ &= \left(D^{[r]}_{(0,(\mathbf{x}_1,\mathbf{x}_2,\dots,\mathbf{x}_{s-1},\mathbf{x}_s))}\overline{D^{[r]}_{(0,(\mathbf{x}_1,\mathbf{x}_2,\dots,\mathbf{x}_{s-1},\mathbf{a}_s))}}\right) \\ &\quad \times \left(D^{[r]}_{(0,(\mathbf{x}_1,\mathbf{x}_2,\dots,\mathbf{x}_{s-1},\mathbf{a}_s))}\overline{D^{[r]}_{(0,(\mathbf{x}_1,\dots,\mathbf{x}_{s-2},\mathbf{a}_{s-1},\mathbf{a}_s))}}\right)\cdots \\ &\quad \times \left(D^{[r]}_{(0,(\mathbf{x}_1,\mathbf{a}_2,\dots,\mathbf{a}_s))}\overline{D^{[r]}_{(0,(\mathbf{a}_1,\mathbf{a}_2,\dots,\mathbf{a}_s))}}\right) \quad \text{for any } \mathbf{x} \in \Lambda_r. \end{aligned}$$

We consider the kth factor

$$D^{[r]}_{(0,(\mathbf{x}_1,\dots,\mathbf{x}_{k-1},\mathbf{x}_k,\mathbf{a}_{k+1},\dots,\mathbf{a}_s))}\overline{D^{[r]}_{(0,(\mathbf{x}_1,\dots,\mathbf{x}_{k-1},\mathbf{a}_k,\mathbf{a}_{k+1},\dots,\mathbf{a}_s))}}. \tag{11.7}$$

From (11.6) this factor is independent of all other components in the starting point $(\mathbf{x}_1, \dots, \mathbf{x}_{k-1}, \mathbf{a}_k, \mathbf{a}_{k+1}, \dots, \mathbf{a}_s)$ except the kth 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 (11.7) becomes

$$\begin{aligned} &D^{[r]}_{(0,(\mathbf{a}_1,\dots,\mathbf{a}_{k-1},\mathbf{x}_k,\mathbf{a}_{k+1},\dots,\mathbf{a}_s))}\overline{D^{[r]}_{(0,(\mathbf{a}_1,\dots,\mathbf{a}_{k-1},\mathbf{a}_k,\mathbf{a}_{k+1},\dots,\mathbf{a}_s))}} \\ &= D^{[r]}_{(0,\mathbf{ext}_r(\mathbf{x}_k))}\overline{D^{[r]}_{(0,\mathfrak{a}^{[r]})}} = D^{[r]}_{(0,\mathbf{ext}_r(\mathbf{x}_k))}, \end{aligned}$$

and $(\mathcal{D}_1)$ is now proved.

12. Tractability: Proof of Theorem 5.10. Let $((M,N), \mathbf{C}, \mathfrak{D}, (\mathbf{p}, \mathbf{t}, \mathcal{Q}))$ be a tuple that satisfies $(\mathcal{R}), (\mathcal{L}), (\mathcal{D})$. In this section, we finally show that $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is tractable by reducing it to the following problem. 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 $f(x_1, x_2, \dots, x_n) = \sum_{i,j\in[n]} a_{i,j} x_i x_j$, where $a_{i,j} \in \mathbb{Z}_q$ for all i, j, and the output is

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

We postpone the proof of the following theorem to the end of this section.

THEOREM 12.1. *Let q be a prime power. Then $\mathsf{EVAL}(q)$ 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, where s is the number of primes in the sequence $\mathbf{p}$: $\mathsf{EVAL}(\mathbf{C}^{[1]}, \mathfrak{D}^{[1]}), \dots, \mathsf{EVAL}(\mathbf{C}^{[s]}, \mathfrak{D}^{[s]})$. If each of these s problems is tractable, then so is $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$. Second, we reduce each $\mathsf{EVAL}(\mathbf{C}^{[i]}, \mathfrak{D}^{[i]})$ to $\mathsf{EVAL}(q)$ for some appropriate prime power q that will become clear later. It follows from Theorem 12.1 that all $\mathsf{EVAL}(\mathbf{C}^{[i]}, \mathfrak{D}^{[i]})$'s can be solved in polynomial time.

12.1. Step 1. For each 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 bipartization of the following $m_i \times m_i$ matrix $\mathbf{F}^{[i]}$, where

$$F^{[i]}_{\mathbf{x},\mathbf{y}} = \prod_{j\in[t_i]} \omega_{q_{i,j}}^{x_j y_j} \quad \text{for all } \mathbf{x} = (x_1, \dots, x_{t_i}), \mathbf{y} = (y_1, \dots, y_{t_i}) \in \mathbb{Z}_{\mathbf{q}_i}. \tag{12.1}$$

We index the rows and columns of $\mathbf{F}^{[i]}$ by $\mathbf{x} \in \mathbb{Z}_{\mathbf{q}_i}$ and index the rows and columns of $\mathbf{C}^{[i]}$ by $\{0,1\} \times \mathbb{Z}_{\mathbf{q}_i}$. We let x_j, $j \in [t_i]$, denote the jth entry of $\mathbf{x} \in \mathbb{Z}_{q_{i,j}}$. By $(\mathcal{R}_3)$,

$$F_{\mathbf{x},\mathbf{y}} = F^{[1]}_{\mathbf{x}_1,\mathbf{y}_1} \cdot F^{[2]}_{\mathbf{x}_2,\mathbf{y}_2} \cdots F^{[s]}_{\mathbf{x}_s,\mathbf{y}_s} \quad \text{for all } \mathbf{x}, \mathbf{y} \in \mathbb{Z}_{\mathcal{Q}}. \tag{12.2}$$

For each integer $i \in [s]$, we define a sequence of N $2m_i \times 2m_i$ diagonal matrices

$$\mathfrak{D}^{[i]} = \left(\mathbf{D}^{[i,0]}, \ldots, \mathbf{D}^{[i,N-1]}\right).$$

$\mathbf{D}^{[i,0]}$ is the $2m_i \times 2m_i$ identity matrix; for every $r \in [N-1]$, we set

$$\mathbf{D}^{[i,r]}_{(0,*)} = \mathbf{0} \text{ if } r \notin \mathcal{S} \quad \text{and} \quad D^{[i,r]}_{(0,\mathbf{x})} = D^{[r]}_{(0,\mathbf{ext}_r(\mathbf{x}))} \text{ for all } \mathbf{x} \in \mathbb{Z}_{\mathbf{q}_i} \text{ if } r \in \mathcal{S};$$

$$\mathbf{D}^{[i,r]}_{(1,*)} = \mathbf{0} \text{ if } r \notin \mathcal{T} \quad \text{and} \quad D^{[i,r]}_{(1,\mathbf{x})} = D^{[r]}_{(1,\mathbf{ext}'_r(\mathbf{x}))} \text{ for all } \mathbf{x} \in \mathbb{Z}_{\mathbf{q}_i} \text{ if } r \in \mathcal{T}.$$

By conditions $(\mathcal{D}_1)$ and $(\mathcal{D}_2)$, we have

$$D^{[r]}_{(b,\mathbf{x})} = D^{[1,r]}_{(b,\mathbf{x}_1)} \cdots D^{[s,r]}_{(b,\mathbf{x}_s)} \quad \text{for all } b \in \{0,1\} \text{ and } \mathbf{x} \in \mathbb{Z}_{\mathcal{Q}}. \tag{12.3}$$

Equation (12.3) 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, because there exists an index $i \in [s]$ such that $\mathbf{x}_i \notin \Lambda_{r,i}$ and thus $\mathbf{ext}_r(\mathbf{x}_i) \notin \Lambda_r$. It then follows from (12.1), (12.3), and the following lemma that if $\mathsf{EVAL}(\mathbf{C}^{[i]}, \mathfrak{D}^{[i]})$ is in polynomial time for all $i \in [s]$, then $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is also in polynomial time.

LEMMA 12.2. *Suppose we have the following matrices: for each $i \in \{0,1,2\}$, $\mathbf{C}^{[i]}$ is the bipartization of an $m_i \times m_i$ complex matrix $\mathbf{F}^{[i]}$; $\mathfrak{D}^{[i]} = (\mathbf{D}^{[i,0]}, \ldots, \mathbf{D}^{[i,N-1]})$ is a sequence of N $2m_i \times 2m_i$ diagonal matrices for some $N \geq 1$, where*

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

and $\mathbf{P}^{[i,r]}$ and $\mathbf{Q}^{[i,r]}$ are $m_i \times m_i$ diagonal matrices; $(\mathbf{C}^{[i]}, \mathfrak{D}^{[i]})$ satisfies (Pinning);

$$\mathbf{F}^{[0]} = \mathbf{F}^{[1]} \otimes \mathbf{F}^{[2]}, \quad \mathbf{P}^{[0,r]} = \mathbf{P}^{[1,r]} \otimes \mathbf{P}^{[2,r]} \quad \textit{and} \quad \mathbf{Q}^{[0,r]} = \mathbf{Q}^{[1,r]} \otimes \mathbf{Q}^{[2,r]}$$

for all $r \in [0 : N-1]$ (so $m_0 = m_1 m_2$). If $\mathsf{EVAL}(\mathbf{C}^{[1]}, \mathfrak{D}^{[1]})$ and $\mathsf{EVAL}(\mathbf{C}^{[2]}, \mathfrak{D}^{[2]})$ are tractable, then $\mathsf{EVAL}(\mathbf{C}^{[0]}, \mathfrak{D}^{[0]})$ is also tractable.

Proof. By the second pinning lemma (Lemma 4.3), both functions $Z^{\rightarrow}$ and $Z^{\leftarrow}$ of $(\mathbf{C}^{[i]}, \mathfrak{D}^{[i]})$, for both $i = 1$ and 2, can be computed in polynomial time. The lemma then follows from Lemma 2.4. ∎

We now use condition $(\mathcal{D}_4)$ to prove the following lemma.

LEMMA 12.3. *Given $r \in \mathcal{T}, i \in [s]$, and $\mathbf{a} \in \Delta^{\mathrm{lin}}_{r,i}$, there exist $\mathbf{b} \in \mathbb{Z}_{\mathbf{q}_i}$ and $\alpha \in \mathbb{Z}_N$ such that the following equation holds for all $\mathbf{x} \in \Delta_{r,i}$:*

$$D^{[i,r]}_{(1,\mathbf{x}+\mathbf{a})} \cdot \overline{D^{[i,r]}_{(1,\mathbf{x})}} = \omega_N^{\alpha} \cdot F^{[i]}_{\mathbf{b},\mathbf{x}}.$$

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 $\widetilde{\mathbf{a}}$ is the vector in $\mathbb{Z}_{\mathcal{Q}}$ such that $\widetilde{\mathbf{a}}_i = \mathbf{a}$ and $\widetilde{\mathbf{a}}_j = \mathbf{0}$ 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

$$D^{[i,r]}_{(1,\mathbf{x}+\mathbf{a})} \cdot \overline{D^{[i,r]}_{(1,\mathbf{x})}} = \omega_N^{\alpha} \cdot F^{[i]}_{\widetilde{\mathbf{b}},\mathbf{ext}'_r(\mathbf{x})} = \omega_N^{\alpha} \cdot F^{[i]}_{\mathbf{b},\mathbf{x}} \quad \text{for all } \mathbf{x} \in \Delta_{r,i},$$

and the lemma is proved. ∎

One can also prove a similar lemma for the other block of $\mathbf{D}^{[i,r]}$, using $(\mathcal{D}_3)$.

12.2. Step 2. For convenience, in this step we abuse the notation slightly and use $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ to denote one of the subproblems $\mathsf{EVAL}(\mathbf{C}^{[i]}, \mathfrak{D}^{[i]})$, $i \in [s]$, defined in the last step. Then by using conditions $(\mathcal{R}), (\mathcal{L})$, and $(\mathcal{D})$, we summarize the properties of this new pair $(\mathbf{C}, \mathfrak{D})$ that we need in the reduction as follows:

$(\mathcal{F}_1)$ There is a prime p and a nonincreasing sequence $\boldsymbol{\pi} = (\pi_1, \ldots, \pi_h)$ of powers of the same p. $\mathbf{F}$ is an $m \times m$ complex matrix, where $m = \pi_1 \pi_2 \cdots \pi_h$, and $\mathbf{C}$ is the bipartization of $\mathbf{F}$. We let π denote π_1. We also 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 $\mathbf{F}$ satisfies

$$F_{\mathbf{x},\mathbf{y}} = \prod_{i \in [h]} \omega_{\pi_i}^{x_i y_i} \quad \text{for all } \mathbf{x} = (x_1, \ldots, x_h) \text{ and } \mathbf{y} = (y_1, \ldots, y_h) \in \mathbb{Z}_{\boldsymbol{\pi}},$$

where we use $x_i \in \mathbb{Z}_{\pi_i}$ to denote the ith entry of $\mathbf{x}$, $i \in [h]$.

$(\mathcal{F}_2)$ $\mathfrak{D} = (\mathbf{D}^{[0]}, \ldots, \mathbf{D}^{[N-1]})$ is a sequence of N $2m \times 2m$ diagonal matrices for some $N \geq 1$ 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 use $\{0,1\} \times \mathbb{Z}_{\boldsymbol{\pi}}$ to index the rows and columns of matrices $\mathbf{C}$ and $\mathbf{D}^{[r]}$. (The condition $\pi \mid N$ is from the condition $M \mid N$ 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 use Λ_r and Δ_r to denote

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

We use $\mathcal{S}$ to denote the set of r such that $\Lambda_r \neq \emptyset$ and $\mathcal{T}$ to denote the set of r such that $\Delta_r \neq \emptyset$. Then for every $r \in \mathcal{S}$, Λ_r is a coset in $\mathbb{Z}_{\boldsymbol{\pi}}$; for every $r \in \mathcal{T}$, Δ_r is a coset in $\mathbb{Z}_{\boldsymbol{\pi}}$. For each $r \in \mathcal{S}$ (and $r \in \mathcal{T}$), there is an $\mathfrak{a}^{[r]} \in \Lambda_r$ ($\mathfrak{b}^{[r]} \in \Delta_r$, 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 $\mathbf{a} \in \Lambda_r^{\mathrm{lin}}$, 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 $\mathbf{a} \in \Delta_r^{\mathrm{lin}}$, 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 reduce the computation of $Z_{\mathbf{C},\mathfrak{D}}(G)$ to $\mathsf{EVAL}(\widehat{\pi})$, where $\widehat{\pi} = \pi$ if $p \neq 2$ and $\widehat{\pi} = 2\pi$ if $p = 2$.

Given $a \in \mathbb{Z}_{\pi_i}$ for some $i \in [h]$, let $\widehat{a}$ denote an element in $\mathbb{Z}_{\widehat{\pi}}$ such that $\widehat{a} \equiv a \pmod{\pi_i}$. As $\pi_i \mid \pi_1 = \pi \mid \widehat{\pi}$, 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. From now on we assume $G = (U \cup V, E)$ to be bipartite: every edge 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 reduce $Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}(G, u^*)$ to $\mathsf{EVAL}(\widehat{\pi})$. The $Z^{\leftarrow}$ part can be dealt with 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 use V_ρ to denote the set of vertices in V whose degree is $\rho \pmod N$. We decompose E into $\bigcup_{i,j} E_{i,j}$, where $E_{i,j}$ contains the edges between U_i and V_j.

If $U_r \neq \emptyset$ for some $r \notin \mathcal{S}$ or if $V_\rho \neq \emptyset$ for some $\rho \notin \mathcal{T}$, then $Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}(G) = 0$. Thus, we assume that $U_r = \emptyset$ for all $r \notin \mathcal{S}$ and $V_\rho = \emptyset$ for all $\rho \notin \mathcal{T}$. In this case, we have

(12.4)
$$Z^{\rightarrow}_{\mathbf{C},\mathfrak{D}}(G, u^*) = \sum_{(f,g)} \left[\prod_{r \in \mathcal{S}} \left(\prod_{u \in U_r} D^{[r]}_{(0,\mathbf{x}_u)} \right) \prod_{\rho \in \mathcal{T}} \left(\prod_{v \in V_\rho} D^{[r]}_{(1,\mathbf{y}_v)} \right) \right] \left[\prod_{(r,\rho) \in \mathcal{S} \times \mathcal{T}} \prod_{uv \in E_{r,\rho}} F_{\mathbf{x}_u, \mathbf{y}_v} \right].$$

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 12.4. *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 map $\tau : (\mathbb{Z}_{\widehat{\pi}})^s \to \mathbb{Z}_{\pi_1} \times \cdots \times \mathbb{Z}_{\pi_h}$, where $\tau(\mathbf{x}) = (\tau_1(\mathbf{x}), \ldots, \tau_h(\mathbf{x}))$ and*

$$\tau_j(\mathbf{x}) = \left(\mathbf{x}\mathbf{A}_{*,j} + \widehat{c}_j \pmod{\pi_j} \right) \in \mathbb{Z}_{\pi_j} \quad \text{for all } j \in [h], \tag{12.5}$$

is a uniform *map from $(\mathbb{Z}_{\widehat{\pi}})^s$ onto Φ. This uniformity means that for all $\mathbf{b}, \mathbf{b}' \in \Phi$, the number of $\mathbf{x} \in (\mathbb{Z}_{\widehat{\pi}})^s$ with $\tau(\mathbf{x}) = \mathbf{b}$ is the same as the number of $\mathbf{x}$ with $\tau(\mathbf{x}) = \mathbf{b}'$.*

Proof. Using 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 $\widehat{\pi} \geq \pi = \pi_1 \geq g_1 \geq \cdots \geq g_s$ for some $s \geq 1$. $\mathbb{Z}_{\mathbf{g}} \equiv \mathbb{Z}_{g_1} \times \cdots \times \mathbb{Z}_{g_s}$ 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 ith 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 $\mathbf{a}_i$ componentwise. Similarly let $\widehat{\mathbf{c}}$ be a lifting of $\mathbf{c}$ componentwise. Then we claim that $\mathbf{A} = (\widehat{a}_{i,j})$ and $\widehat{\mathbf{c}}$ together give us the required *uniform* map τ from $(\mathbb{Z}_{\widehat{\pi}})^s$ to Φ.

To show that τ is uniform, we consider the linear part of $\tau' : (\mathbb{Z}_{\widehat{\pi}})^s \to \Phi^{\text{lin}}$,

$$\tau'(\mathbf{x}) = (\tau'_1(\mathbf{x}), \ldots, \tau'_h(\mathbf{x})), \quad \text{where } \tau'_j(\mathbf{x}) = \left(\mathbf{x}\mathbf{A}_{*,j} \pmod{\pi_j} \right) \in \mathbb{Z}_{\pi_j}$$

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 $\mathbb{Z}_{\mathbf{g}}$:

$$\mathbf{x} = (x_1, \ldots, x_s) \mapsto \left(x_1 \pmod{g_1}, \ldots, x_s \pmod{g_s} \right).$$

σ is certainly a uniform map, being a surjective homomorphism. Thus, every vector $\mathbf{b} \in \mathbb{Z}_{\mathbf{g}}$ has $|\ker \sigma| = \widehat{\pi}^s/(g_1 \cdots g_s)$ many preimages. We show that the map τ' factors through σ and f, i.e., $\tau' = f \circ \sigma$. Because f is an isomorphism, this implies that τ' is also a uniform map.

As $g_i \mathbf{e}_i = \mathbf{0}$ in $\mathbb{Z}_{\mathbf{g}}$, the following is a valid expression in the $\mathbb{Z}_{\widehat{\pi}}$-module for $\sigma(\mathbf{x})$:

$$\left(x_1 \pmod{g_1}, \ldots, x_s \pmod{g_s} \right) = \sum_{i=1}^{s} x_i \mathbf{e}_i.$$

Apply f as a $\mathbb{Z}_{\widehat{\pi}}$-module homomorphism $f(\sigma(\mathbf{x})) = \sum_{i=1}^{s} x_i f(\mathbf{e}_i)$ with its jth entry being $\sum_{i=1}^{s} x_i a_{i,j}$. This is an expression in the $\mathbb{Z}_{\widehat{\pi}}$-module $\mathbb{Z}_{\pi_j}$, which is the same as

$$\sum_{i=1}^{s} \left(x_i \pmod{\pi_j}\right) \cdot a_{i,j} = \sum_{i=1}^{s} x_i \widehat{a}_{i,j} \pmod{\pi_j} = \tau'_j(\mathbf{x}).$$

The lemma is proved. □

Applying Lemma 12.4 to Λ_r, 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:

$$\lambda_i^{[r]}(\mathbf{x}) = \left(\mathbf{x}\mathbf{A}_{*,i}^{[r]} + \widehat{\mathfrak{a}}_i^{[r]} \pmod{\pi_i}\right) \quad \text{for all } i \in [h] \text{ and } \mathbf{x} \in \mathbb{Z}_{\widehat{\pi}}^{s_r}. \tag{12.6}$$

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:

$$\delta_i^{[r]}(\mathbf{y}) = \left(\mathbf{y}\mathbf{B}_{*,i}^{[r]} + \widehat{\mathfrak{b}}_i^{[r]} \pmod{\pi_i}\right) \quad \text{for all } i \in [h] \text{ and } \mathbf{y} \in \mathbb{Z}_{\widehat{\pi}}^{t_r}. \tag{12.7}$$

Using $(\mathcal{F}_3)$, we have

$$D^{[r]}_{(0,\lambda^{[r]}(\mathbf{0}))} = 1 \text{ when } r \in \mathcal{S} \quad \text{and} \quad D^{[r]}_{(1,\delta^{[r]}(\mathbf{0}))} = 1 \text{ when } r \in \mathcal{T}. \tag{12.8}$$

Because both $\lambda^{[r]}$ and $\delta^{[r]}$ are uniform, and we know the multiplicity of each map (the cardinality of inverse images), to compute (12.4) it suffices to compute the following:

$$\sum_{(\mathbf{x}_u),(\mathbf{y}_v)} \prod_{r\in\mathcal{S}} \left(\prod_{u\in U_r} D^{[r]}_{(0,\lambda^{[r]}(\mathbf{x}_u))} \right) \prod_{r\in\mathcal{T}} \left(\prod_{v\in V_r} D^{[r]}_{(1,\delta^{[r]}(\mathbf{y}_v))} \right) \prod_{\substack{r_1\in\mathcal{S}, r_2\in\mathcal{T} \\ uv\in E_{r_1,r_2}}} F_{\lambda^{[r_1]}(\mathbf{x}_u),\delta^{[r_2]}(\mathbf{y}_v)}, \tag{12.9}$$

where the sum is over pairs of sequences

$$\left(\mathbf{x}_u; u \in \bigcup_{r\in\mathcal{S}} U_r\right) \in \prod_{r\in\mathcal{S}} \left(\mathbb{Z}_{\widehat{\pi}}^{s_r}\right)^{|U_r|} \quad \text{and} \quad \left(\mathbf{y}_v; v \in \bigcup_{r\in\mathcal{T}} V_r\right) \in \prod_{r\in\mathcal{T}} \left(\mathbb{Z}_{\widehat{\pi}}^{t_r}\right)^{|V_r|}.$$

If (1) for all $r \in \mathcal{S}$, there is a quadratic polynomial $f^{[r]}$ over $\mathbb{Z}_{\widehat{\pi}}$ such that

$$D^{[r]}_{(0,\lambda^{[r]}(\mathbf{x}))} = \omega_{\widehat{\pi}}^{f^{[r]}(\mathbf{x})} \quad \text{for all } \mathbf{x} \in \mathbb{Z}_{\widehat{\pi}}^{s_r}; \tag{12.10}$$

(2) for all $r \in \mathcal{T}$, there is a quadratic polynomial $g^{[r]}$ over $\mathbb{Z}_{\widehat{\pi}}$ such that

$$D^{[r]}_{(1,\delta^{[r]}(\mathbf{y}))} = \omega_{\widehat{\pi}}^{g^{[r]}(\mathbf{y})} \quad \text{for all } \mathbf{y} \in \mathbb{Z}_{\widehat{\pi}}^{t_r}; \tag{12.11}$$

(3) for all $r_1 \in \mathcal{S}, r_2 \in \mathcal{T}$, there is a quadratic polynomial $f^{[r_1,r_2]}$ over $\mathbb{Z}_{\widehat{\pi}}$ such that

$$F_{\lambda^{[r_1]}(\mathbf{x}),\delta^{[r_2]}(\mathbf{y})} = \omega_{\widehat{\pi}}^{f^{[r_1,r_2]}(\mathbf{x},\mathbf{y})} \quad \text{for all } \mathbf{x} \in \mathbb{Z}_{\widehat{\pi}}^{s_{r_1}} \text{ and } \mathbf{y} \in \mathbb{Z}_{\widehat{\pi}}^{t_{r_2}}, \tag{12.12}$$

then we can reduce the computation of the summation in (12.9) to $\mathsf{EVAL}(\widehat{\pi})$.

We start with (3). By $(\mathcal{F}_1)$, the following map $f^{[r_1,r_2]}$ satisfies (12.12):

$$f^{[r_1,r_2]}(\mathbf{x},\mathbf{y}) = \sum_{i\in[h]} \frac{\widehat{\pi}}{\pi_i} \cdot \lambda_i^{[r_1]}(\mathbf{x}) \cdot \delta_i^{[r_2]}(\mathbf{y}) = \sum_{i\in[h]} \frac{\widehat{\pi}}{\pi_i} \left(\mathbf{x}\mathbf{A}_{*,i}^{[r_1]} + \widehat{\mathfrak{a}}_i^{[r_1]}\right) \left(\mathbf{y}\mathbf{B}_{*,i}^{[r_2]} + \widehat{\mathfrak{b}}_i^{[r_2]}\right).$$

Note that the presence of the integer $\widehat{\pi}/\pi_i$ is crucial to be able to substitute the mod π_i expressions in (12.6) and in (12.7), respectively, as if they were mod $\widehat{\pi}$ expressions. It is also clear that $f^{[r_1,r_2]}$ is indeed a quadratic polynomial over $\mathbb{Z}_{\widehat{\pi}}$.

Next we prove (1), which is a little more complicated. The proof of (2) is similar.

Let $r \in S$. Let $\mathbf{e}_i$ denote the vector in $\mathbb{Z}_{\widehat{\pi}}^{s_r}$ whose ith entry is 1 and all other entries are 0. Using $(\mathcal{F}_4)$, 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

$$D^{[r]}_{(0,\lambda^{[r]}(\mathbf{x}+\mathbf{e}_i))} \overline{D^{[r]}_{(0,\lambda^{[r]}(\mathbf{x}))}} = \omega_N^{\alpha_i} \prod_{j\in[h]} \omega_{\pi_j}^{b_{i,j}\cdot\lambda_j^{[r]}(\mathbf{x})} \quad \text{for all } \mathbf{x} \in \mathbb{Z}_{\widehat{\pi}}^{s_r}. \tag{12.13}$$

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, observe that the jth 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 $\mathbf{a} \in \Lambda_r^{\mathrm{lin}}$ 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

$$1 = \prod_{j=0}^{\widehat{\pi}-1} D^{[r]}_{(0,\lambda^{[r]}((j+1)\mathbf{e}_i))} \overline{D^{[r]}_{(0,\lambda^{[r]}(j\mathbf{e}_i))}} = (\omega_N^{\alpha_i})^{\widehat{\pi}} \prod_{k\in[h]} \omega_{\pi_k}^{b_{i,k}[\lambda_k^{[r]}(0\mathbf{e}_i)+\cdots+\lambda_k^{[r]}((\widehat{\pi}-1)\mathbf{e}_i)]}. \tag{12.14}$$

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 sum:

$$\sum_{j=0}^{\widehat{\pi}-1} \lambda_k^{[r]}(j\mathbf{e}_i) = \sum_{j=0}^{\widehat{\pi}-1} \left((j\mathbf{e}_i)\mathbf{A}^{[r]}_{*,k} + \widehat{\mathfrak{a}}_k^{[r]} \pmod{\pi_k} \right) = \left(\sum_{j=1}^{\widehat{\pi}-1} j\mathbf{e}_i \right) \mathbf{A}^{[r]}_{*,k} \pmod{\pi_k} = 0. \tag{12.15}$$

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 $\pi_k \mid \widehat{\pi}$, and when $p = 2$, J is a multiple of $\widehat{\pi}/2$. However, in this case, we have $\widehat{\pi}/2 = \pi_1$ and $\pi_k \mid \pi_1$.

As a result, $(\omega_N^{\alpha_i})^{\widehat{\pi}} = 1$. So there exists $\beta_i \in \mathbb{Z}_{\widehat{\pi}}$ for each $i \in [s_r]$ such that

$$D^{[r]}_{(0,\lambda^{[r]}(\mathbf{x}+\mathbf{e}_i))} \overline{D^{[r]}_{(0,\lambda^{[r]}(\mathbf{x}))}} = \omega_{\widehat{\pi}}^{\beta_i} \prod_{j\in[h]} \omega_{\pi_j}^{b_{i,j}\cdot\lambda_j^{[r]}(\mathbf{x})} \quad \text{for all } \mathbf{x} \in \mathbb{Z}_{\widehat{\pi}}^{s_r}. \tag{12.16}$$

It follows that every nonzero entry of $\mathbf{D}^{[r]}$ is a power of $\omega_{\widehat{\pi}}$. This uses $(\mathcal{F}_3)$, that 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 $f^{[r]} \colon \mathbb{Z}_{\widehat{\pi}}^{s_r} \to \mathbb{Z}_{\widehat{\pi}}$ which satisfies (12.10). We want to show that it is indeed a quadratic polynomial. To see this, by (12.16),

$$f^{[r]}(\mathbf{x}+\mathbf{e}_i) - f^{[r]}(\mathbf{x}) = \beta_i + \sum_{j\in[h]} \frac{\widehat{\pi}}{\pi_j} \cdot b_{i,j} \cdot \lambda_j^{[r]}(\mathbf{x}) = \beta_i + \sum_{j\in[h]} \frac{\widehat{\pi}}{\pi_j} \cdot \widehat{b}_{i,j} \cdot \left(\mathbf{x}\mathbf{A}^{[r]}_{*,j} + \widehat{\mathfrak{a}}_j^{[r]} \right) \tag{12.17}$$

for every $i \in [s_r]$. 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 $\mathbb{Z}_{\widehat{\pi}}$. Moreover,

$$\widehat{b}_{i,j} \equiv b_{i,j} \pmod{\pi_j} \implies \left(\frac{\widehat{\pi}}{\pi_j}\right) \widehat{b}_{i,j} \equiv \left(\frac{\widehat{\pi}}{\pi_j}\right) b_{i,j} \pmod{\widehat{\pi}}.$$

Thus the expression in (12.17) is evaluated in $\mathbb{Z}_{\widehat{\pi}}$, which means that for any $i \in [s_r]$, there exist $c_{i,0}, \ldots, c_{i,s_r} \in \mathbb{Z}_{\widehat{\pi}}$ such that

$$f^{[r]}(\mathbf{x}+\mathbf{e}_i) - f^{[r]}(\mathbf{x}) = c_{i,0} + \sum_{j\in[s_r]} c_{i,j}x_j. \tag{12.18}$$

Since $f^{[r]}(\mathbf{0}) = 0$, the case when p is odd follows from the lemma below.

LEMMA 12.5. *Let π be a power of an odd prime, and let f be a map from $\mathbb{Z}_\pi^s$ to $\mathbb{Z}_\pi$ for some $s \geq 1$. Suppose for every $i \in [s]$, there exist $c_{i,0}, \ldots, c_{i,s} \in \mathbb{Z}_\pi$ such that*

$$f(\mathbf{x}+\mathbf{e}_i) - f(\mathbf{x}) = c_{i,0} + \sum_{j\in[s]} c_{i,j}x_j \quad \textit{for all } \mathbf{x} \in \mathbb{Z}_\pi^s \tag{12.19}$$

and $f(\mathbf{0}) = 0$. Then there exist $a_{i,j}, a_i \in \mathbb{Z}_\pi$ such that

$$f(\mathbf{x}) = \sum_{i\leq j\in[s]} a_{i,j}x_ix_j + \sum_{i\in[s]} a_ix_i \quad \textit{for all } \mathbf{x} \in \mathbb{Z}_\pi^s. \tag{12.20}$$

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, we have

$$f(\mathbf{e}_i+\mathbf{e}_j) = f(\mathbf{e}_i+\mathbf{e}_j) - f(\mathbf{e}_i) + f(\mathbf{e}_i) - f(\mathbf{0}) = c_{j,0} + c_{j,i} + c_{i,0}.$$

It follows that $c_{i,j} = c_{j,i}$.

Finally, we set $a_{i,j} = c_{i,j}$ for all $i < j \in [s]$; $a_{i,i} = c_{i,i}/2$ 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 $i = 1$:

$$g(\mathbf{x}+\mathbf{e}_1) - g(\mathbf{x}) = 2a_{1,1}x_1 + \sum_{j>1} a_{1,j}x_j + (a_{1,1}+a_1) = c_{1,1}x_1 + \sum_{j>1} c_{1,j}x_j + c_{1,0}.$$

Other cases are similar, and the lemma is proved. ∎

When $p = 2$, we first claim that the constants $c_{i,i}$ in (12.18) must be even, since

$$0 = f^{[r]}(\widehat{\pi}\mathbf{e}_i) - f^{[r]}((\widehat{\pi}-1)\mathbf{e}_i) + \cdots + f^{[r]}(\mathbf{e}_i) - f^{[r]}(\mathbf{0}) = \widehat{\pi}c_{i,0} + c_{i,i}(\widehat{\pi} - 1 + \cdots + 1 + 0).$$

This equality happens in $\mathbb{Z}_{\widehat{\pi}}$, so $c_{i,i}(\widehat{\pi}(\widehat{\pi}-1)/2) = 0 \pmod{\widehat{\pi}}$. 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 12.6. *Let π be a power of 2 and let f be a map from $\mathbb{Z}_\pi^s$ to $\mathbb{Z}_\pi$ satisfying $f(\mathbf{0}) = 0$. Suppose for every $i \in [s]$ there exist $c_{i,0}, \ldots, c_{i,s} \in \mathbb{Z}_\pi$, where $2 \,|\, c_{i,i}$, such that* (12.19) *holds. Then there are $a_{i,j}, a_i \in \mathbb{Z}_\pi$ such that f has the form of* (12.20).

Proof. The proof of Lemma 12.6 is essentially the same as that of Lemma 12.5. 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. Finally we turn to the proof of Theorem 12.1, i.e., $\mathsf{EVAL}(q)$ is tractable for any fixed prime power q.

Actually, there is a well-known polynomial-time algorithm for $\mathsf{EVAL}(q)$ when q is a prime [10, 15], [27, Theorem 6.30]. (The algorithm works for any finite field.) Here we present a polynomial-time algorithm that works for any prime power q. We start with the easier case when q is odd.

LEMMA 12.7. *Let p be an odd prime and let $q = p^k$ 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*

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

can be evaluated in polynomial time (in n).

Proof. We assume that $f(x_1, \ldots, x_n)$ has the following form:

$$f(x_1, \ldots, x_n) = \sum_{i \le j \in [n]} c_{i,j} x_i x_j + \sum_{i \in [n]} c_i x_i + c_0, \tag{12.21}$$

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 $k = 1$, i.e., $q = p$ is an odd prime. Note that if f is affine, then the evaluation can be trivially done in polynomial time. In fact, it decouples into a product of n sums,

$$\sum_{x_1,\ldots,x_n \in \mathbb{Z}_q} \omega_q^{f(x_1,\ldots,x_n)} = \sum_{x_1,\ldots,x_n \in \mathbb{Z}_q} \omega_q^{\sum_{i=1}^n c_i x_i + c_0} = \omega_q^{c_0} \times \prod_{i=1}^n \sum_{x_i \in \mathbb{Z}_q} \omega_q^{c_i x_i}.$$

This sum is equal to 0 if any $c_i \in \mathbb{Z}_q$ is nonzero 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 terms.

In the first case, without loss of generality, we assume that $c_{1,1} \neq 0$. There exist an affine function $g \in \mathbb{Z}_q[x_2, \ldots, x_n]$ and a quadratic polynomial $f' \in \mathbb{Z}_q[x_2, \ldots, x_n]$, 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 obtain the expression $c_{1,1}(x_1 + g(x_2, \ldots, x_n))^2$.

For any fixed $x_2, \ldots, x_n$, when x_1 ranges over $\mathbb{Z}_q$, $x_1 + g$ ranges over $\mathbb{Z}_q$. Thus,

$$\sum_{x_1,x_2,\ldots,x_n \in \mathbb{Z}_q} \omega_q^{f(x_1,x_2,\ldots,x_n)} = \sum_{x_2,\ldots,x_n \in \mathbb{Z}_q} \omega_q^{f'} \sum_{x_1 \in \mathbb{Z}_q} \omega_q^{c_{1,1}(x_1+g)^2} = \sum_{x \in \mathbb{Z}_q} \omega_q^{c_{1,1}x^2} \cdot Z_q(f').$$

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 12.8. The claim of $\sum_x \omega_q^{cx^2}$ being "computable in constant time" here 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 following closed formula: If $c \neq 0$,

$$\sum_{x \in \mathbb{Z}_p} \omega_p^{cx^2} = \left(\frac{c}{p}\right) G, \quad \text{where } G = \sum_{x \in \mathbb{Z}_p} \left(\frac{x}{p}\right) \omega_p^x.$$

Here $(\frac{c}{p})$ is the Legendre symbol. It can be computed in polynomial time in the binary length of c and p. G has the closed form $G = +\sqrt{p}$ if $p \equiv 1 \bmod 4$ and $G = +i\sqrt{p}$ if $p \equiv 3 \bmod 4$.[4]

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 nonzero. 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 $\mathbb{Z}_q^2$. Thus,

$$\sum_{x_1,x_2,\ldots,x_n \in \mathbb{Z}_q} \omega_q^{f(x_1,x_2,\ldots,x_n)} = \sum_{x'_1,x'_2,,\ldots,x_n \in \mathbb{Z}_q} \omega_q^{f(x'_1+x'_2,x'_1-x'_2,\ldots,x_n)}.$$

Viewing $f(x'_1 + x'_2, x'_1 - x'_2, \ldots, x_n)$ as a new quadratic polynomial f' of $x'_1, x'_2, \ldots, x_n$ its coefficient of $x_1'^2$ is exactly $c_{1,2} \neq 0$. Thus f' contains at least one square term. This reduces our problem back to the first case. We can use the method described earlier to reduce the number of variables.

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 $q = p^k$.

We can write any nonzero $a \in \mathbb{Z}_q$ as $a = p^t a'$, where t is a unique nonnegative integer, such that $p \nmid a'$. We call t the order of a (with respect to p). 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 nonzero quadratic terms. Let t_0 be the smallest order of all the nonzero 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.

For the first case, without loss of generality, assume $c_{1,1} = p^{t_0} c$ and $p \nmid c$ (so c is invertible in $\mathbb{Z}_q$). By the minimality of t_0, every nonzero 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 $f(x_1, x_2, \ldots, x_n) = c_{1,1}(x_1 + g(x_2, \ldots, x_n))^2 + c_1x_1 +$ a quadratic polynomial in $(x_2, \ldots, x_n)$, where g is a linear function 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 $x_2, \ldots, x_n$, when x_1 ranges over $\mathbb{Z}_q$, $x_1 + g$ also ranges over $\mathbb{Z}_q$. So

$$\sum_{x_1,\ldots,x_n \in \mathbb{Z}_q} \omega_q^f = \left(\sum_{x \in \mathbb{Z}_q} \omega_q^{c_{1,1}x^2 + c_1x}\right)\left(\sum_{x_2,\ldots,x_n \in \mathbb{Z}_q} \omega_q^{f'}\right) = \sum_{x \in \mathbb{Z}_q} \omega_q^{c_{1,1}x^2 + c_1x} \cdot Z_q(f').$$

[4]It had been known to Gauss since 1801 that $G = \pm\sqrt{p}$ 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 plus sign was conjectured by Gauss in his diary in May 1801. He wrote to his friend W. Olbers on September 3, 1805, that seldom had a week passed for four years that he had not tried in vain to prove this very elegant conjecture. Finally, he wrote, "Wie der Blitz einschlägt, hat sich das Räthsel gelöst" (as lightning strikes was the puzzle solved).

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.

For the second case, all square terms of f either are 0 or have orders larger than t_0. 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 $Z_q(f') = Z_q(f)$, and 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 t_0, so we 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 $q = 2^k$, 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.

LEMMA 12.9. *Let $q = 2^k$ for some $k \geq 1$. Let $f \in \mathbb{Z}_q[x_1, \ldots, x_n]$ be a quadratic polynomial over $x_1, \ldots, x_n$. Then $Z_q(f)$ can be evaluated in polynomial time (in n).*

Proof. When $k = 1$, $Z_q(f)$ is computable in polynomial time according to [10], [27, Theorem 6.30] so we assume $k > 1$. We also assume f has the form as in (12.21).

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. build a new quadratic $g \in \mathbb{Z}_{q/2}[x_1, \ldots, x_n]$ and reduce $Z_q(f)$ to $Z_{q/2}(g)$, or
3. build a new quadratic $g \in \mathbb{Z}_q[x_1, \ldots, x_{n-1}]$ and reduce $Z_q(f)$ to $Z_q(g)$.

This gives a polynomial-time algorithm for $\mathsf{EVAL}(q)$, because both base cases, when $k = 1$ or $n = 1$, can be solved 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. Let t be the smallest index in $[n]$ such that one of $\{c_t, c_{t,j} : j > t\}$ is not divisible by 2. Separating out the terms involving x_t, we rewrite f as follows:

$$f = c_{t,t} \cdot x_t^2 + x_t \cdot f_1(x_1, \ldots, \widehat{x_t}, \ldots, x_n) + f_2(x_1, \ldots, \widehat{x_t}, \ldots, x_n), \tag{12.22}$$

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,

$$f_1(x_1, \ldots, \widehat{x_t}, \ldots, x_n) = \sum_{i<t} c_{i,t}x_i + \sum_{j>t} c_{t,j}x_j + c_t. \tag{12.23}$$

From 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

$$Z_q(f) = \sum_{x_1,\ldots,x_n \in \mathbb{Z}_q} \omega_q^{f(x_1,\ldots,x_n)} = \sum_{\substack{x_1,\ldots,x_n \in \mathbb{Z}_q \\ f_1(x_1,\ldots,\widehat{x_t},\ldots,x_n) \equiv 0 \bmod 2}} \omega_q^{f(x_1,\ldots,x_n)}. \tag{12.24}$$

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 $x_1, \ldots, \widehat{x_t}, \ldots, x_n$, we have

$$\sum_{x_t \in \mathbb{Z}_q} \omega_{2^k}^{c_{t,t}x_t^2 + x_t f_1 + f_2} = \omega_{2^k}^{f_2} \sum_{x_t \in [0:2^{k-1}-1]} \omega_{2^k}^{c_{t,t}x_t^2 + x_t f_1} + \omega_{2^k}^{c_{t,t}(x_t + 2^{k-1})^2 + (x_t + 2^{k-1})f_1}$$
$$= \omega_{2^k}^{f_2} \left(1 + (-1)^{f_1}\right) \sum_{x_t \in [0:2^{k-1}-1]} \omega_{2^k}^{c_{t,t}x_t^2 + x_t f_1} = 0,$$

since $f_1 \equiv 1 \bmod 2$. We used $(x + 2^{k-1})^2 \equiv x^2 \pmod{2^k}$ in the first equality.

Recall that f_1 (see (12.23)) is an affine form of $\{x_1, \ldots, \widehat{x_t}, \ldots, x_n\}$, that $c_{i,t}$ is even for all $i < t$, and that one of $\{c_{t,j}, c_t : j > t\}$ is odd. We consider 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 (12.24), $Z_q(f)$ is trivially zero.

In the second case, there exists at least one $j > t$ such that $c_{t,j}$ is odd. We let $\ell > t$ be the smallest of such j. 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 $\mathbb{Z}_q$)

$$x_\ell = c_{t,\ell}^{-1} \left(2x'_\ell - \left(\sum_{i<t} c_{i,t}x_i + \sum_{j>t, j\neq\ell} c_{t,j}x_j + c_t \right) \right). \tag{12.25}$$

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 it, we define a 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 (12.25). 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 and every such tuple has two preimages in $\mathbb{Z}_q^n$. The claim follows.

So to compute $Z_q(f)$, we only need to compute $Z_q(f')$, and 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*) Every cross term and linear term that involves $x_1, \ldots, x_t$ has an even coefficient in f'.

To show this, we partition 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 $s < s', s < t$.

First, we consider the expression (12.22) 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 (12.25); x_t does not appear in the third term, even after the substitution. So (*Even*) holds for x_t.

Second, 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 (12.25) is even since $c_{s,t}$ is even. So, every term in the list above makes an even contribution to c'_s 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):

$$c_{s,s'}x_s x_{s'}, \ c_{\ell,\ell}x_\ell^2, \ c_{s,\ell}x_s x_\ell, \text{ and } \ c_{\ell,s'}x_\ell x_{s'} \ (\text{or } \ c_{s',\ell}x_{s'}x_\ell).$$

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 (12.25) is even. As a result, every term in the list above makes an even contribution to $c'_{s,s'}$ and thus $c'_{s,s'}$ is even.

To summarize, after substituting x_ℓ with x'_ℓ using (12.25) we get a new quadratic polynomial f' such that $Z_q(f') = 2Z_q(f)$, and every cross term and linear term that involves $x_1, \ldots, x_t$ has an even coefficient in f'. We can then repeat this substitution procedure on f': We either show that $Z_q(f') = 0$ or get a quadratic polynomial f'' such that $Z_q(f'') = 2Z_q(f')$ and the parameter t increases by at least one. So given a quadratic polynomial f, we can, in polynomial time, either show that $Z_q(f) = 0$ or get a new quadratic $g \in \mathbb{Z}_q[x_1, \ldots, x_n]$ such that $Z_q(f) = 2^r \cdot Z_q(g)$ for some known integer $r \in [0 : n]$, and every cross term and linear term has an even coefficient in g.

Now it suffices to compute $Z_q(g)$. We 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

$$g = \sum_{i \le j \in [n]} a_{i,j} x_i x_j + \sum_{i \in [n]} a_i x_i + a.$$

We consider 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, $a_{i,j}$ and a_i are even for all $i \le j \in [n]$. Let $a'_{i,j}$ and a'_i denote integers in $[0 : 2^{k-1} - 1]$ that satisfy $a_{i,j} \equiv 2a'_{i,j},\ a_i \equiv 2a'_i \pmod q$, 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' is the quadratic polynomial over $\mathbb{Z}_{q/2} = \mathbb{Z}_{2^{k-1}}$ in the exponent. 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

$$f = a_{1,1}(x_1^2 + 2x_1 g_1) + g_2 = a_{1,1}(x_1 + g_1)^2 + g',$$

where g_1 is an affine 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, $j \ge 2$, are even. Now

$$Z_q(g) = \sum_{x_2,\ldots,x_n \in \mathbb{Z}_q} \omega_q^{g'} \cdot \sum_{x_1 \in \mathbb{Z}_q} \omega_q^{a_{1,1}(x_1+g_1)^2} = Z_q(g') \sum_{x \in \mathbb{Z}_q} \omega_q^{a_{1,1}x^2}.$$

The last equation is because the sum over $x_1 \in \mathbb{Z}_q$ is independent of the value of g_1. This reduces $Z_q(g)$ 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 least one. This gives us a polynomial time algorithm to evaluate $Z_q(f)$. □

This concludes the proof of Theorem 1.1 for the bipartite case.

Remark 12.10. Back in section 1, we mentioned that Holant(Ω) for $\Omega = (G, \mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3)$ are all tractable, and the tractability boils down to the exponential sum

$$\sum_{x_1,x_2,\ldots,x_n \in \{0,1\}} i^{L_1 + L_2 + \cdots + L_s} \tag{12.26}$$

being computable in polynomial time. This can also be derived from Theorem 12.1.

First, each mod 2 sum L_j in (12.26) can be replaced by its square $(L_j)^2$, because $L_j = 0, 1 \pmod 2$ iff $(L_j)^2 = 0, 1 \pmod 4$, respectively. So, (12.26) can be expressed as a sum of the form $i^{Q(x_1,x_2,\ldots,x_n)}$, where Q is an ordinary sum of squares of affine forms with integer coefficients and, in particular, a quadratic polynomial with integer coefficients. For a sum of squares of affine forms Q, if we evaluate each $x_i \in \{0,1,2,3\}$, we may take $x_i \bmod 2$, and this reduces (12.26) to $\mathsf{EVAL}(4)$:

$$\sum_{x_1,x_2,\ldots,x_n \in \mathbb{Z}_4} i^{Q(x_1,x_2\ldots,x_n)} = 2^n \sum_{x_1,x_2,\ldots,x_n \in \{0,1\}} i^{Q(x_1,x_2,\ldots,x_n)}.$$

13. Proof of Theorem 6.3. Let $\mathbf{A}$ be a symmetric, nonbipartite, 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:

$(\mathcal{S}_1')$ $\mathbf{A}$ is an $m \times m$ symmetric matrix. $\boldsymbol{\kappa} = (\kappa_1, \ldots, \kappa_s)$ is a strictly decreasing sequence of positive rational numbers, where $s \geq 1$. $\mathbf{m} = (m_1, \ldots, m_s)$ 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 $\mathbf{x}, \mathbf{y}$, $\mathbf{A}$ satisfies

$$A_{\mathbf{x},\mathbf{y}} = A_{(x_1,x_2),(y_1,y_2)} = \kappa_{x_1}\kappa_{y_1} S_{\mathbf{x},\mathbf{y}},$$

where $\mathbf{S} = \{S_{\mathbf{x},\mathbf{y}}\}$ is a symmetric matrix in which every entry is a power of ω_N:

$$\mathbf{A} = \begin{pmatrix} \kappa_1\mathbf{I}_{m_1} & & & \\ & \kappa_2\mathbf{I}_{m_2} & & \\ & & \ddots & \\ & & & \kappa_s\mathbf{I}_{m_s} \end{pmatrix} \begin{pmatrix} \mathbf{S}_{(1,*),(1,*)} & \mathbf{S}_{(1,*),(2,*)} & \cdots & \mathbf{S}_{(1,*),(s,*)} \\ \mathbf{S}_{(2,*),(1,*)} & \mathbf{S}_{(2,*),(2,*)} & \cdots & \mathbf{S}_{(2,*),(s,*)} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{S}_{(s,*),(1,*)} & \mathbf{S}_{(s,*),(2,*)} & \cdots & \mathbf{S}_{(s,*),(s,*)} \end{pmatrix} \begin{pmatrix} \kappa_1\mathbf{I}_{m_1} & & & \\ & \kappa_2\mathbf{I}_{m_2} & & \\ & & \ddots & \\ & & & \kappa_s\mathbf{I}_{m_s} \end{pmatrix},$$

where $\mathbf{I}_{m_i}$ is the $m_i \times m_i$ identity matrix. We let $I = \{(i,j) : i \in [s], j \in [m_i]\}$.

The proof of Theorem 6.3, just like the one of Theorem 5.3, consists of five steps. All the proofs use the following strategy. We construct from the $m \times m$ matrix $\mathbf{A}$ its bipartization $\mathbf{A}'$, 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 $\mathbf{A}$.

To this end, we need the following lemma.

LEMMA 13.1. *Let $\mathbf{A}$ be a symmetric matrix, and let $\mathbf{A}'$ be its bipartization. Then* $\mathsf{EVAL}(\mathbf{A}') \leq \mathsf{EVAL}(\mathbf{A})$.

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, because $\mathbf{A}'$ is the bipartization of $\mathbf{A}$. Otherwise, assume that $G = (U \cup V, E)$ is bipartite and connected; let $u^* \in U$. Then

$$Z_{\mathbf{A}}(G, u^*, i) = Z_{\mathbf{A}'}(G, u^*, i) = Z_{\mathbf{A}'}(G, u^*, m+i) \quad \text{for any } i \in [m].$$

It then follows that $Z_{\mathbf{A}'}(G) = 2Z_{\mathbf{A}}(G)$ and $\mathsf{EVAL}(\mathbf{A}') \leq \mathsf{EVAL}(\mathbf{A})$. ∎

13.1. Step 2.1.

LEMMA 13.2. *Suppose that $(\mathbf{A}, (N, \boldsymbol{\kappa}, \mathbf{m}))$ 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. Let $\mathbf{A}'$ be the bipartization of $\mathbf{A}$. Suppose that $\mathsf{EVAL}(\mathbf{A})$ is not #P-hard. From Lemma 13.1, $\mathsf{EVAL}(\mathbf{A}') \le \mathsf{EVAL}(\mathbf{A})$ and thus $\mathsf{EVAL}(\mathbf{A}')$ is not #P-hard. Note that the $\mathbf{S}$ matrix in Lemma 8.5 is exactly the same $\mathbf{S}$ here. Also $(\mathbf{A}', (N, \boldsymbol{\kappa}, \boldsymbol{\kappa}, \mathbf{m}, \mathbf{m}))$ satisfies condition $(\mathcal{S}_1)$, so by Lemma 8.5 together with the assumption that $\mathbf{A}'$ is not #P-hard, $\mathbf{S}$ satisfies $(\mathcal{S}_2)$ which is exactly the same as $(\mathcal{S}_2')$ here. (For Lemma 8.5, $\mathbf{S}$ also needs to satisfy $(\mathcal{S}_3)$, but since $\mathbf{S}$ is symmetric here, $(\mathcal{S}_3)$ is the same as $(\mathcal{S}_2)$.) □

We have the following corollary. The proof is the same as that of Corollary 8.6.

COROLLARY 13.3. *For all $i, j \in [s]$, $\mathbf{S}_{(i,*),(j,*)}$ has the same rank as $\mathbf{S}$.*

Next we build a pair $(\mathbf{F}, \mathfrak{D})$ and apply the cyclotomic reduction lemma on $\mathbf{A}$.

Let $h = \operatorname{rank}(\mathbf{S})$. By Corollary 13.3, there exist $1 \le i_1 < \cdots < i_h \le m_1$ 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), assume $i_k = k$ for all $k \in [h]$. Let $\mathbf{H}$ denote this $h \times h$ symmetric matrix: $H_{i,j} = S_{(1,i),(1,j)}$. From Corollary 13.3 and Lemma 13.2, for every index $\mathbf{x} \in I$, there exist two unique integers $j \in [h]$ and $k \in [0 : N-1]$ such that

$$\mathbf{S}_{\mathbf{x},*} = \omega_N^k \cdot \mathbf{S}_{(1,j),*} \quad \text{and} \quad \mathbf{S}_{*,\mathbf{x}} = \omega_N^k \cdot \mathbf{S}_{*,(1,j)}. \tag{13.1}$$

This gives us a partition of the index set I

$$\mathscr{R} = \big\{ R_{(i,j),k} : i \in [s], j \in [h], k \in [0 : N-1] \big\}.$$

For every $\mathbf{x} \in I$, $\mathbf{x} \in R_{(i,j),k}$ iff $i = x_1$ and $\mathbf{x}, j, k$ satisfy (13.1). By Corollary 13.3,

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

Now we define $(\mathbf{F}, \mathfrak{D})$ and use the cyclotomic reduction lemma and $\mathscr{R}$ 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 $I' = [s] \times [h]$ 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,

$$\mathbf{F} = \begin{pmatrix} \kappa_1 \mathbf{I} & & & \\ & \kappa_2 \mathbf{I} & & \\ & & \ddots & \\ & & & \kappa_s \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{H} & \mathbf{H} & \ldots & \mathbf{H} \\ \mathbf{H} & \mathbf{H} & \ldots & \mathbf{H} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{H} & \mathbf{H} & \ldots & \mathbf{H} \end{pmatrix} \begin{pmatrix} \kappa_1 \mathbf{I} & & & \\ & \kappa_2 \mathbf{I} & & \\ & & \ddots & \\ & & & \kappa_s \mathbf{I} \end{pmatrix},$$

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 are

$$D_{\mathbf{x}}^{[r]} = \sum_{k=0}^{N-1} \big| R_{(x_1,x_2),k} \big| \cdot \omega_N^{kr} \quad \text{for all } r \in [0 : N-1], \mathbf{x} \in I'.$$

We use the cyclotomic reduction lemma (Lemma 8.2) to prove the next lemma.

LEMMA 13.4. $\mathsf{EVAL}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$.

Proof. 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'. By (13.1),

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

So $\mathbf{A}$ can be generated from $\mathbf{F}$ using $\mathscr{R}$. The construction of $\mathfrak{D}$ implies that $\mathfrak{D}$ can be generated from $\mathscr{R}$. The lemma follows from the cyclotomic reduction lemma. ∎

13.2. Steps 2.2 and 2.3. Now we have a pair $(\mathbf{F}, \mathfrak{D})$ that satisfies the following condition (*Shape*′):

(*Shape*′$_1$) $\mathbf{F} \in \mathbb{C}^{m\times m}$ is a symmetric $s \times s$ block matrix. (The m here is different from the m used in Step 2.1.) We use $I = [s] \times [h]$ to index its rows and columns.

(*Shape*′$_2$) There are a strictly decreasing sequence $\boldsymbol{\kappa} = (\kappa_1, \ldots, \kappa_s)$ of positive rational numbers together with an $h \times h$ matrix $\mathbf{H}$ of full rank, whose entries are all powers of ω_N, for some $N \geq 1$. 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 for all $r \in [N-1]$ and $\mathbf{x} \in I$, we have

$$D_{\mathbf{x}}^{[r]} = \overline{D_{\mathbf{x}}^{[N-r]}}.$$

Now suppose $\mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ is not #P-hard.

We define $(\mathbf{C}, \mathfrak{D}')$: $\mathbf{C}$ is the bipartization of $\mathbf{F}$; $\mathfrak{D}'$ is a sequence of N copies of

$$\begin{pmatrix} \mathbf{D}^{[r]} & \\ & \mathbf{D}^{[r]} \end{pmatrix}.$$

The proof of the following lemma is the same as that of Lemma 13.1.

LEMMA 13.5. $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D}') \leq \mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$.

By Lemma 13.5, $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D}') \leq \mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ and thus $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D}')$ is not #P-hard. By (*Shape*′$_1$)–(*Shape*′$_3$), $(\mathbf{C}, \mathfrak{D}')$ also satisfies (*Shape*$_1$)–(*Shape*$_3$). It then follows from Lemmas 8.8 and 8.11 that $(\mathbf{C}, \mathfrak{D}')$ also satisfies (*Shape*$_4$)–(*Shape*$_6$). Since $(\mathbf{C}, \mathfrak{D}')$ is built from $(\mathbf{F}, \mathfrak{D})$, the latter must satisfy the following conditions:

(*Shape*′$_4$) $\mathbf{H}/\sqrt{h}$ 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*′$_5$) For all $\mathbf{x} \in I$,

$$D_{\mathbf{x}}^{[0]} = D_{(x_1,1)}^{[0]}.$$

(*Shape*′$_6$) For each $r \in [N-1]$, there are diagonal matrices $\mathbf{K}^{[r]} \in \mathbb{C}^{s\times s}, \mathbf{L}^{[r]} \in \mathbb{C}^{h\times h}$. The norm of every diagonal entry in $\mathbf{L}^{[r]}$ is either 0 or 1. We have

$$\mathbf{D}^{[r]} = \mathbf{K}^{[r]} \otimes \mathbf{L}^{[r]} \quad \text{for all } r \in [N-1].$$

For all $r \in [N-1]$, $\mathbf{K}^{[r]} = \mathbf{0}$ implies $\mathbf{L}^{[r]} = \mathbf{0}$; $\mathbf{L}^{[r]} \neq \mathbf{0}$ implies one of its entries is 1.

In particular, (*Shape*′$_5$) means that by setting

$$K_i^{[0]} = D_{(i,1)}^{[0]} \quad \text{and} \quad L_j^{[0]} = 1 \quad \text{for all } i \in [s] \text{ and } j \in [h],$$

we have $\mathbf{D}^{[0]} = \mathbf{K}^{[0]} \otimes \mathbf{L}^{[0]}$. By $(\mathcal{T}_3)$ in (*Shape*′$_3$), entries of $\mathbf{K}^{[0]}$ are positive integers.

13.3. Step 2.4. Suppose $(\mathbf{F}, \mathfrak{D})$ satisfies $(Shape'_1)$–$(Shape'_6)$. From $(Shape'_2)$ we have $\mathbf{F} = \mathbf{M} \otimes \mathbf{H}$, where $\mathbf{M}$ is an $s \times s$ matrix of rank 1: $M_{i,j} = \kappa_i \kappa_j$ for all $i, j \in [s]$.

We reduce $\mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ to two problems $\mathsf{EVAL}(\mathbf{M}, \mathfrak{K})$ and $\mathsf{EVAL}(\mathbf{H}, \mathfrak{L})$, where

$$\mathfrak{K} = \left(\mathbf{K}^{[0]}, \ldots, \mathbf{K}^{[N-1]}\right) \quad \text{and} \quad \mathfrak{L} = \left(\mathbf{L}^{[0]}, \ldots, \mathbf{L}^{[N-1]}\right).$$

The proof of the following lemma is essentially the same as that of Lemma 8.24.

LEMMA 13.6. $\mathsf{EVAL}(\mathbf{F}, \mathfrak{D}) \equiv \mathsf{EVAL}(\mathbf{H}, \mathcal{L})$.

13.4. Step 2.5. Finally we normalize the matrix $\mathbf{H}$ in the same way we did for the bipartite case and 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 Theorems 6.4 and 6.7. Suppose $((M, N), \mathbf{F}, \mathfrak{D})$ satisfies $(\mathcal{U}'_1)$–$(\mathcal{U}'_4)$. We prove Theorems 6.4 and 6.7 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 bipartization $\mathbf{C}$ of $\mathbf{F}$.

LEMMA 14.1. *Suppose $((M, N), \mathbf{F}, \mathfrak{D})$ 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. Assume $\mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ is not #P-hard. Let $\mathbf{C}$ and $\mathfrak{E} = (\mathbf{E}^{[0]}, \ldots, \mathbf{E}^{[N-1]})$ be

$$\mathbf{C} = \begin{pmatrix} \mathbf{0} & \mathbf{F} \\ \mathbf{F} & \mathbf{0} \end{pmatrix} \quad \text{and} \quad \mathbf{E}^{[r]} = \begin{pmatrix} \mathbf{D}^{[r]} & \mathbf{0} \\ \mathbf{0} & \mathbf{D}^{[r]} \end{pmatrix} \quad \text{for all } r \in [0 : N-1].$$

By $(\mathcal{U}'_1)$–$(\mathcal{U}'_4)$, $((M, N), \mathbf{C}, \mathfrak{E})$ satisfies $(\mathcal{U}_1)$–$(\mathcal{U}_4)$. Furthermore, using Lemma 13.5, we have $\mathsf{EVAL}(\mathbf{C}, \mathfrak{E}) \leq \mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ and thus $\mathsf{EVAL}(\mathbf{C}, \mathfrak{E})$ is also not #P-hard. It follows from Lemma 9.1 that $\mathbf{F}$ satisfies the group condition $(\mathcal{GC})$. ∎

14.1. Proof of Theorem 6.4. We prove Theorem 6.4 again, using $\mathbf{C}$ and $\mathfrak{E}$ again.

Suppose $\mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ is not #P-hard. On the one hand, $\mathsf{EVAL}(\mathbf{C}, \mathfrak{E}) \leq \mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ and $\mathsf{EVAL}(\mathbf{C}, \mathfrak{E})$ is also not #P-hard. On the other hand, $((M, N), \mathbf{C}, \mathfrak{E})$ satisfies conditions $(\mathcal{U}_1)$–$(\mathcal{U}_4)$. Thus, using Theorem 5.4, $\mathfrak{E}$ 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 6.7. In this section we prove Theorem 6.7. However, we cannot simply reduce it, using $(\mathbf{C}, \mathfrak{E})$, to the bipartite case (Theorem 5.6), because in Theorem 6.7, we are only allowed to permute the rows and columns symmetrically, while in Theorem 5.6, 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 9.7, in which we have to bring in the generalized Fourier matrices (see Definitions 5.5 and 6.6).

Suppose $\mathbf{F}$ satisfies $(\mathcal{GC})$. 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 9.2, both F^{R} and F^{C} are finite Abelian groups of order m, under the Hadamard product.

We start by proving a symmetric version of Lemma 9.5, stating that when $M = pq$ and $\gcd(p, q) = 1$ (note that p and q are not necessarily primes), a permutation of $\mathbf{F}$ is the tensor product of two smaller discrete unitary matrices, both of which satisfy the group condition.

LEMMA 14.2. *Suppose $\mathbf{F} \in \mathbb{C}^{m \times m}$ is symmetric and M-discrete unitary and satisfies $(\mathcal{GC})$. Moreover, $M = pq$, $p, q > 1$, and $\gcd(p, q) = 1$. Then there is a*

permutation Π *of* $[0:m-1]$ *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 that of Lemma 9.5. Since $\mathbf{F}$ is symmetric the two bijections f, g that we defined in the proof of Lemma 9.5, from $[0:m-1]$ to $[0:m'-1] \times [0:m''-1]$, are exactly the same. ∎

As a result, we only need to deal with the case when $M = p^\beta$ is a prime power.

LEMMA 14.3. *Suppose* $\mathbf{F} \in \mathbb{C}^{m\times m}$ *is symmetric and* M*-discrete unitary and 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* $p \nmid \alpha_{k,k}$, *where* $F_{k,k} = \omega_M^{\alpha_{k,k}}$.

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, $p \mid \alpha_{k,k}$ for all k. Then because $\mathbf{F}$ 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 $p \nmid \alpha_{2,1} = \alpha_{1,2}$.

By $(\mathcal{GC})$, there exists 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 9.7 showing that when there exists a diagonal entry $F_{k,k}$ such that $p \nmid \alpha_{k,k}$, $\mathbf{F}$ 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 $2 \mid \alpha_{i,i}$ for all $i \in [0:m-1]$.

LEMMA 14.4. *Suppose* $\mathbf{F} \in \mathbb{C}^{m\times m}$ *is symmetric and* M*-discrete unitary and 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 there exists a permutation* Π *such that* $\mathbf{F}_{\Pi,\Pi} = \boldsymbol{\mathcal{F}}_{M,\alpha} \otimes \mathbf{F}'$, *where* $\mathbf{F}'$ *is a symmetric and* M'*-discrete unitary matrix that satisfies condition* $(\mathcal{GC})$ *with* $M' \mid M$.

Proof. The proof is the same as the one of Lemma 9.7 by setting $a = b = k$. The only thing to notice is that since $\mathbf{F}$ is symmetric, the two bijections f and g that we defined in the proof of Lemma 9.7 are the same. Thus, the row permutation and the column permutation applied on $\mathbf{F}$ are the same. Since $F_{k,k} = \omega_M^\alpha$, (9.12) 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 the Fourier matrix $\boldsymbol{\mathcal{F}}_{M,\alpha}$ here. ∎

Finally, we deal with the case when $p = 2$ and $2 \mid \alpha_{i,i}$ for all $i \in [0:m-1]$.

LEMMA 14.5. *Suppose* $\mathbf{F} \in \mathbb{C}^{m\times m}$ *is symmetric and* M*-discrete unitary and satisfies* $(\mathcal{GC})$ *with* $M = 2^\beta$ *and* $2 \mid \alpha_{i,i}$ *for all* $i \in [0:m-1]$. *Then there exist a permutation* Π *and a* 2×2 *symmetric nondegenerate matrix* $\mathbf{W}$ *over* $\mathbb{Z}_M$ (see section 6.3.2 and Definition 6.6), *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 that satisfies* $(\mathcal{GC})$ *with* $M' \mid M$.

Proof. By Property 9.6, there are two integers $a \neq b$ 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 $2 \mid \alpha_a, \alpha_b$.

We let $S^{a,b}$ denote the following subset of F^{R}:

$$S^{a,b} = \{\mathbf{u} \in F^{\mathrm{R}} : u_a = u_b = 1\}.$$

Clearly $S^{a,b}$ 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 let 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 $|S^a| = |S^b| = M$ since $F_{a,b} = \omega_M$. 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 $S^a \times S^b \times S^{a,b}$ to F^{R}. We show that it is surjective.

Toward this end, we first note that

$$\mathbf{W} = \begin{pmatrix} \alpha_a & 1 \\ 1 & \alpha_b \end{pmatrix}$$

is nondegenerate. This follows from Lemma 6.5, 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 $\mathbf{u} \in F^{\mathrm{R}}$, there exist integers k_1 and k_2 such that (since $\mathbf{W}$ is nondegenerate, by Lemma 6.5, $\mathbf{x} \mapsto \mathbf{W}\mathbf{x}$ is a bijection)

$$u_a = F_{a,a}^{k_1} \cdot F_{b,a}^{k_2} = \omega_M^{\alpha_a k_1 + k_2} \quad \text{and} \quad u_b = F_{a,b}^{k_1} \cdot F_{b,b}^{k_2} = \omega_M^{k_1 + \alpha_b k_2}.$$

Thus, $\mathbf{u} \circ \overline{\mathbf{F}_{a,*}^{k_1}} \circ \overline{\mathbf{F}_{b,*}^{k_2}} \in S^{a,b}$. It 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 also injective. Assume this is not the case. 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 $(k_1, k_2, \mathbf{u}) \neq (k_1', k_2', \mathbf{u}')$ 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 $\mathbf{u} = \mathbf{u}'$, contradiction. Therefore, we may assume that

$$\boldsymbol{\ell} = (\ell_1, \ell_2)^{\mathrm{T}} = (k_1 - k_1', k_2 - k_2')^{\mathrm{T}} \neq \mathbf{0}.$$

By restricting on the ath and bth entries, we get $\mathbf{W}\boldsymbol{\ell} = \mathbf{0}$. This contradicts the fact that $\mathbf{W}$ is nondegenerate.

Since $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3) \mapsto \mathbf{u}_1 \circ \mathbf{u}_2 \circ \mathbf{u}_3$ is a group isomorphism, we have $|S^{a,b}| = m/M^2$, which we denote by n. Let $S^{a,b} = \{\mathbf{v}_0 = \mathbf{1}, \mathbf{v}_1, \ldots, \mathbf{v}_{n-1}\}$. There is a bijection f from $[0 : m-1]$ to $[0 : M-1] \times [0 : M-1] \times [0 : n-1]$, $f(i) = (f_1(i), f_2(i), f_3(i))$, with

$$\mathbf{F}_{i,*} = (\mathbf{F}_{a,*})^{f_1(i)} \circ (\mathbf{F}_{b,*})^{f_2(i)} \circ \mathbf{v}_{f_3(i)} \quad \text{for all } i \in [0 : m-1]. \tag{14.1}$$

Since $\mathbf{F}$ is symmetric, this also implies that

$$\mathbf{F}_{*,j} = (\mathbf{F}_{*,a})^{f_1(j)} \circ (\mathbf{F}_{*,b})^{f_2(j)} \circ \mathbf{v}_{f_3(j)} \quad \text{for all } j \in [0 : m-1]. \tag{14.2}$$

Note that $f(a) = (1, 0, 0)$ and $f(b) = (0, 1, 0)$.

Next we permute $\mathbf{F}$ to get a new matrix $\mathbf{G}$. For convenience, we use (x_1, x_2, x_3), where $x_1, x_2 \in [0 : M-1]$ and $x_3 \in [0 : n-1]$, to index the rows and columns of $\mathbf{G}$. We permute $\mathbf{F}$ using $\Pi(x_1, x_2, x_3) = f^{-1}(x_1, x_2, x_3)$:

$$G_{(x_1,x_2,x_3),(y_1,y_2,y_3)} = F_{\Pi(x_1,x_2,x_3),\Pi(y_1,y_2,y_3)}. \tag{14.3}$$

Then by (14.1) and (14.2),

$$\begin{aligned} \mathbf{G}_{(x_1,x_2,x_3),*} &= (\mathbf{G}_{(1,0,0),*})^{x_1} \circ (\mathbf{G}_{(0,1,0),*})^{x_2} \circ \mathbf{G}_{(0,0,x_3),*} \quad \text{and} \\ \mathbf{G}_{*,(y_1,y_2,y_3)} &= (\mathbf{G}_{*,(1,0,0)})^{y_1} \circ (\mathbf{G}_{*,(0,1,0)})^{y_2} \circ \mathbf{G}_{*,(0,0,y_3)}. \end{aligned}$$

As a result,

$$G_{(x_1,x_2,x_3),(y_1,y_2,y_3)} = (G_{(1,0,0),(y_1,y_2,y_3)})^{x_1} (G_{(0,1,0),(y_1,y_2,y_3)})^{x_2}\, G_{(0,0,x_3),(y_1,y_2,y_3)}.$$

We analyze the three factors. First, we have

$$G_{(1,0,0),(y_1,y_2,y_3)} = F_{a,a}^{y_1} \cdot F_{a,b}^{y_2} \cdot v_{y_3,a} = \omega_M^{\alpha_a y_1 + y_2},$$

where $v_{y_3,a}$ is the ath 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,

$$G_{(0,0,x_3),(y_1,y_2,y_3)} = (G_{(0,0,x_3),(1,0,0)})^{y_1} (G_{(0,0,x_3),(0,1,0)})^{y_2}\, G_{(0,0,x_3),(0,0,y_3)}.$$

By (14.3) and (14.2) 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 (14.1), $F_{\Pi(0,0,x),a} = v_{x,a} = 1$. Similarly, $G_{(0,0,x),(0,1,0)} = v_{x,b} = 1$. Therefore,

$$G_{(x_1,x_2,x_3),(y_1,y_2,y_3)} = \omega_M^{\alpha_a x_1 y_1 + x_1 y_2 + x_2 y_1 + \alpha_b x_2 y_2} \cdot G_{(0,0,x_3),(0,0,y_3)}.$$

So $\mathbf{G} = \boldsymbol{\mathcal{F}}_{M,\mathbf{W}} \otimes \mathbf{F}'$; $\mathbf{F}' \equiv (F'_{i,j} = G_{(0,0,i),(0,0,j)})$ is symmetric; $\mathbf{W}$ is nondegenerate.

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 is closed under the Hadamard product. To see that $\mathbf{F}'$ 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 6.7 then follows from Lemmas 14.3, 14.4, and 14.5.

15. Proofs of Theorems 6.8 and 6.9. Suppose $((M,N),\mathbf{F},\mathfrak{D},(\mathbf{d},\mathcal{W},\mathbf{p},\mathbf{t},\mathcal{Q},\mathcal{K}))$ satisfies condition $(\mathcal{R}')$. We prove Theorem 6.8: 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 bipartization of $(\mathbf{F},\mathfrak{D})$. The plan is to show that $(\mathbf{C},\mathfrak{E})$ with appropriate $\mathbf{p}'$, $\mathbf{t}'$, and $\mathcal{Q}'$ satisfies $(\mathcal{R})$.

To see this, 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 $x_{1,i,j} = k_{i,j} \cdot x'_{1,i,j}$ for all $i \in [s], j \in [t_i]$. See $(\mathcal{R}')$ for the definitions 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 nondegenerate 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 $\mathbf{x}'$ 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 we can write $\mathbf{C}_{\Sigma,\Sigma}$ and $\mathfrak{E}_\Sigma = (\mathbf{E}_\Sigma^{[0]}, \ldots, \mathbf{E}_\Sigma^{[N-1]})$ as

$$\mathbf{C}_{\Sigma,\Sigma} = \begin{pmatrix} \mathbf{0} & \mathbf{F}_{\Sigma_0,I} \\ \mathbf{F}_{I,\Sigma_0} & \mathbf{0} \end{pmatrix} \quad \text{and} \quad \mathbf{E}_\Sigma^{[r]} = \begin{pmatrix} \mathbf{D}_{\Sigma_0}^{[r]} & \mathbf{0} \\ \mathbf{0} & \mathbf{D}^{[r]} \end{pmatrix} \tag{15.1}$$

for all $r \in [0 : N-1]$. We make the following two observations: Observation 1: $\mathsf{EVAL}(\mathbf{C}_{\Sigma,\Sigma}, \mathfrak{E}_\Sigma) \equiv \mathsf{EVAL}(\mathbf{C}, \mathfrak{E}) \le \mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ and thus $\mathsf{EVAL}(\mathbf{C}_{\Sigma,\Sigma}, \mathfrak{E}_\Sigma)$ is not #P-hard. Observation 2: $\mathbf{F}_{\Sigma_0,I}$ satisfies

$$\left(\mathbf{F}_{\Sigma_0,I}\right)_{\mathbf{x},\mathbf{y}} = F_{\mathbf{x}',\mathbf{y}} = \prod_{i\in[g]} \omega_{d_i}^{(x'_{0,i,1}\ x'_{0,i,2})\cdot\mathbf{W}^{[i]}\cdot(y_{0,i,1}\ y_{0,i,2})^{\mathrm{T}}} \prod_{i\in[s],j\in[t_i]} \omega_{q_{i,j}}^{k_{i,j}\cdot x'_{1,i,j}y_{1,i,j}}$$
$$= \prod_{i\in[g]} \omega_{d_i}^{x_{0,i,1}y_{0,i,1}+x_{0,i,2}y_{0,i,2}} \prod_{i\in[s],j\in[t_i]} \omega_{q_{i,j}}^{x_{1,i,j}y_{1,i,j}}.$$

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 5.8 and (15.1) that $\mathbf{D}^{[r]}$ satisfy $(\mathcal{L}_2)$ and $(\mathcal{L}_3)$. This proves Theorem 6.8 since $(\mathcal{L}'_1)$ and $(\mathcal{L}'_2)$ follow from $(\mathcal{L}_2)$ and $(\mathcal{L}_3)$, respectively.

We continue to prove Theorem 6.9. 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 5.9 and (15.1), $\mathbf{D}^{[r]}$ satisfies $(\mathcal{D}_2)$ and $(\mathcal{D}_4)$ for all $r \in \mathcal{Z}$. $(\mathcal{D}'_1)$ follows from $(\mathcal{D}_2)$.

To prove $(\mathcal{D}'_2)$, let $\mathbf{F}' = \mathbf{F}_{\Sigma_0,I}$. By $(\mathcal{D}_4)$, for any $r \in \mathcal{Z}$, $k \in [s]$ and $\mathbf{a} \in \Gamma^{\mathrm{lin}}_{r,k}$, there exist $\mathbf{b} \in \tilde{\mathbb{Z}}_{\mathbf{q}_k}$ and $\alpha \in \mathbb{Z}_N$ such that

$$\omega_N^\alpha \cdot F'_{\widetilde{\mathbf{b}},\mathbf{x}} = D^{[r]}_{\mathbf{x}+\widetilde{\mathbf{a}}} \cdot \overline{D^{[r]}_{\mathbf{x}}} \quad \text{for all } \mathbf{x} \in \Gamma_r, \text{ where } \mathbf{F}'_{\widetilde{\mathbf{b}},*} = \mathbf{F}_{\Sigma_0(\widetilde{\mathbf{b}}),*}.$$

Since Σ_0 works within each prime factor, there exists a $\mathbf{b}' \in \tilde{\mathbb{Z}}_{\mathbf{q}_k}$ such that $\Sigma_0(\widetilde{\mathbf{b}}) = \widetilde{\mathbf{b}'}$ and $(\mathcal{D}'_2)$ follows.

16. Tractability: Proof of Theorem 6.10. The proof of Theorem 6.10 is similar to that of Theorem 5.10 for the bipartite case presented in section 12.

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 two steps. First we use $(\mathcal{R}'), (\mathcal{L}'), (\mathcal{D}')$ to decompose $\mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ into s subproblems (recall s is the length of the sequence $\mathbf{p}$), denoted by $\mathsf{EVAL}(\mathbf{F}^{[i]}, \mathfrak{D}^{[i]})$, $i \in [s]$, such that if every $\mathsf{EVAL}(\mathbf{F}^{[i]}, \mathfrak{D}^{[i]})$ is tractable, then so is $\mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$. Second, we reduce each $\mathsf{EVAL}(\mathbf{F}^{[i]}, \mathfrak{D}^{[i]})$ to $\mathsf{EVAL}(\pi)$ for some prime power π.

By Theorem 12.1, $\mathsf{EVAL}(\pi)$ can be solved in polynomial time for any fixed prime power π. Thus, $\mathsf{EVAL}(\mathbf{F}^{[i]}, \mathfrak{D}^{[i]})$ 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 $\mathfrak{D}^{[i]}$. Recall the definition of $\tilde{\mathbb{Z}}_{\mathbf{q}_i}$ from section 6.3.3. For any $\mathbf{x} \in \tilde{\mathbb{Z}}_{\mathbf{q}_i}$, we use $\widetilde{\mathbf{x}} \in \prod_{j=1}^s \tilde{\mathbb{Z}}_{\mathbf{q}_j}$ to denote the vector such that $(\widetilde{\mathbf{x}})_i = \mathbf{x}$ and $(\widetilde{\mathbf{x}})_j = \mathbf{0}$ for all $j \ne i$.

$\mathbf{F}^{[i]}$ is an $m_i \times m_i$ symmetric matrix, where $m_i = |\tilde{\mathbb{Z}}_{\mathbf{q}_i}|$. We use $\tilde{\mathbb{Z}}_{\mathbf{q}_i}$ to index the rows and columns of $\mathbf{F}^{[i]}$. Then

$$F^{[i]}_{\mathbf{x},\mathbf{y}} = F_{\widetilde{\mathbf{x}},\widetilde{\mathbf{y}}} \quad \text{for all } \mathbf{x}, \mathbf{y} \in \tilde{\mathbb{Z}}_{\mathbf{q}_i}.$$

By condition $(\mathcal{R}'_3)$, it is easy to see that

$$\mathbf{F} = \mathbf{F}^{[1]} \otimes \ldots \otimes \mathbf{F}^{[s]}. \tag{16.1}$$

$\mathfrak{D}^{[i]} = (\mathbf{D}^{[i,0]}, \ldots, \mathbf{D}^{[i,N-1]})$ is a sequence of $m_i \times m_i$ diagonal matrices: $\mathbf{D}^{[i,0]}$ is the $m_i \times m_i$ identity matrix; for every $r \in [N-1]$, the $\mathbf{x}$th entry of $\mathbf{D}^{[i,r]}$ is

$$D^{[i,r]}_{\mathbf{x}} = D^{[r]}_{\mathbf{ext}_r(\mathbf{x})} \quad \text{for all } \mathbf{x} \in \tilde{\mathbb{Z}}_{\mathbf{q}_i}.$$

By condition $(\mathcal{D}_1')$, we have

$$\mathbf{D}^{[r]} = \mathbf{D}^{[1,r]} \otimes \ldots \otimes \mathbf{D}^{[s,r]} \quad \text{for all } r \in [0 : N-1]. \tag{16.2}$$

It then follows from (16.1) and (16.2) that

$$Z_{\mathbf{F},\mathfrak{D}}(G) = Z_{\mathbf{F}^{[1]},\mathfrak{D}^{[1]}}(G) \times \ldots \times Z_{\mathbf{F}^{[s]},\mathfrak{D}^{[s]}}(G)$$

for all 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.*

Recall that $\mathcal{Z}$ is the set of $r \in [N-1]$ such that $\mathbf{D}^{[r]} \neq \mathbf{0}$; $\Gamma_{r,i}$ is a coset in $\tilde{\mathbb{Z}}_{\mathbf{q}_i}$ for each $i \in [s]$ such that $\Gamma_r = \Gamma_{r,1} \times \cdots \times \Gamma_{r,s}$. We use $(\mathcal{D}_2')$ to prove the next lemma.

LEMMA 16.2. *Given* $r \in \mathcal{Z}, i \in [s], \mathbf{a} \in \Gamma_{r,i}^{\mathrm{lin}}$*, there are* $\mathbf{b} \in \tilde{\mathbb{Z}}_{\mathbf{q}_i}, \alpha \in \mathbb{Z}_N$ *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

$$D^{[i,r]}_{\mathbf{x}+\mathbf{a}} \cdot \overline{D^{[i,r]}_{\mathbf{x}}} = D^{[r]}_{\mathbf{ext}_r(\mathbf{x}+\mathbf{a})} \cdot \overline{D^{[r]}_{\mathbf{ext}_r(\mathbf{x})}} = D^{[r]}_{\mathbf{ext}_r(\mathbf{x})+\tilde{\mathbf{a}}} \cdot \overline{D^{[r]}_{\mathbf{ext}_r(\mathbf{x})}}.$$

Then by condition $(\mathcal{D}_2')$, we know there exist $\mathbf{b} \in \tilde{\mathbb{Z}}_{\mathbf{q}_i}$ and $\alpha \in \mathbb{Z}_N$ such that

$$D^{[i,r]}_{\mathbf{x}+\mathbf{a}} \cdot \overline{D^{[i,r]}_{\mathbf{x}}} = \omega_N^{\alpha} \cdot F_{\tilde{\mathbf{b}},\mathbf{ext}_r(\mathbf{x})} = \omega_N^{\alpha} \cdot F^{[i]}_{\mathbf{b},\mathbf{x}} \quad \text{for all } \mathbf{x} \in \Gamma_{r,i},$$

and the lemma is proved. ∎

16.2. Step 2. For convenience, we let $\mathsf{EVAL}(\mathbf{F}, \mathfrak{D})$ denote one of the problems $\mathsf{EVAL}(\mathbf{F}^{[i]}, \mathfrak{D}^{[i]})$ 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 is a prime p and a nonincreasing sequence $\boldsymbol{\pi} = (\pi_1, \ldots, \pi_h)$ of powers of p. $\mathbf{F}$ is an $m \times m$ symmetric matrix, where $m = \pi_1 \ldots \pi_h$. We let π denote π_1 and use $\mathbb{Z}_{\boldsymbol{\pi}} \equiv \mathbb{Z}_{\pi_1} \times \cdots \times \mathbb{Z}_{\pi_h}$ to index the rows and columns of $\mathbf{F}$. 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

$$F_{\mathbf{x},\mathbf{y}} = \prod_{(i,j)\in\mathcal{T}} \omega_{\pi_i}^{c_{i,j}x_iy_j} \quad \text{for all } \mathbf{x} = (x_1, \ldots, x_h), \quad \mathbf{y} = (y_1, \ldots, y_h) \in \mathbb{Z}_{\boldsymbol{\pi}},$$

where $x_i \in \mathbb{Z}_{\pi_i}$ denotes the ith entry of $\mathbf{x}$. We express $\mathbf{F}$ in this very general form 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, where $N \geq 1$ and $\pi \mid N$. $\mathbf{D}^{[0]}$ is the identity matrix; 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 $r \in [0 : N-1]$, let Γ_r denote the set of $\mathbf{x} \in \mathbb{Z}_{\boldsymbol{\pi}}$ such that the $\mathbf{x}$th entry of $\mathbf{D}^{[r]}$ is nonzero, 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 is a vector $\mathbf{a}^{[r]} \in \Gamma_r$ such that the $(\mathbf{a}^{[r]})$th entry of $\mathbf{D}^{[r]}$ is 1.

$(\mathcal{F}_4')$ For all $r \in \mathcal{Z}$ and $\mathbf{a} \in \Gamma_r^{\mathrm{lin}}$, there exist $\mathbf{b} \in \mathbb{Z}_{\boldsymbol{\pi}}$ and $\alpha \in \mathbb{Z}_N$ such that

$$D^{[r]}_{\mathbf{x}+\mathbf{a}} \cdot \overline{D^{[r]}_{\mathbf{x}}} = \omega_N^{\alpha} \cdot F_{\mathbf{b},\mathbf{x}} \quad \text{for all } \mathbf{x} \in \Gamma_r.$$

Let G be an undirected graph. Below we reduce the computation of $Z_{\mathbf{F},\mathfrak{D}}(G)$ to $\mathsf{EVAL}(\widehat{\pi})$, where $\widehat{\pi} = \pi$ if $p \neq 2$ and $\widehat{\pi} = 2\pi$ 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 $r \bmod N$. We decompose E into $E_{i,j}$, $i \leq j \in [0 : N-1]$, where $E_{i,j}$ contains the set of edges between V_i and V_j. Clearly, if $V_r \neq \emptyset$ for some $r \notin \mathcal{Z}$, then $Z_{\mathbf{F},\mathfrak{D}}(G)$ is trivially 0. Thus, we assume $V_r = \emptyset$ for all $r \notin \mathcal{Z}$. In this case, we have

$$Z_{\mathbf{F},\mathfrak{D}}(G) = \sum_{\xi} \left[\prod_{r \in \mathcal{Z}} \prod_{v \in V_r} D^{[r]}_{\mathbf{x}_v} \right] \left[\prod_{r \leq r' \in \mathcal{Z}} \prod_{uv \in E_{r,r'}} F_{\mathbf{x}_u, \mathbf{x}_v} \right],$$

where the sum ranges over all assignments $\xi = (\xi_r \colon V_r \to \Gamma_r \,|\, r \in \mathcal{Z})$ with $\xi(v) = \mathbf{x}_v$.

By Lemma 12.4, we know that for every $r \in \mathcal{Z}$, there exist a positive integer s_r and an $s_r \times h$ matrix $\mathbf{A}^{[r]}$ over $\mathbb{Z}_{\widehat{\pi}}$ that give us a *uniform* map $\gamma^{[r]}$ (see Lemma 12.4 for the definition) from $\mathbb{Z}_{\widehat{\pi}}^{s_r}$ to Γ_r:

$$\gamma^{[r]}_i(\mathbf{x}) = \left(\mathbf{x}\mathbf{A}^{[r]}_{*,i} + \widehat{\mathfrak{a}}^{[r]}_i \pmod{\pi_i} \right) \quad \text{for all } i \in [h].$$

For every $r \in \mathcal{Z}$, we have $\gamma^{[r]}(\mathbf{0}) = \mathfrak{a}^{[r]} \in \Gamma_r$. Since $\gamma^{[r]}$ is uniform and we know the multiplicity of this map, in order to compute $Z_{\mathbf{F},\mathfrak{D}}(G)$ it suffices to compute

$$\sum_{(\mathbf{x}_v)} \left[\prod_{r \in \mathcal{Z}} \prod_{v \in V_r} D^{[r]}_{\gamma^{[r]}(\mathbf{x}_v)} \right] \left[\prod_{r \leq r' \in \mathcal{Z}} \prod_{uv \in E_{r,r'}} F_{\gamma^{[r]}(\mathbf{x}_u), \gamma^{[r']}(\mathbf{x}_v)} \right],$$

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 for every $r \in \mathcal{Z}$, there is a quadratic polynomial $f^{[r]}$ over $\mathbb{Z}_{\widehat{\pi}}$ such that

$$D^{[r]}_{\gamma^{[r]}(\mathbf{x})} = \omega_{\widehat{\pi}}^{f^{[r]}(\mathbf{x})} \quad \text{for all } \mathbf{x} \in \mathbb{Z}_{\widehat{\pi}}^{s_r}, \tag{16.3}$$

and for all $r, r' : r \leq r' \in \mathcal{Z}$, there is a quadratic polynomial $f^{[r,r']}$ over $\mathbb{Z}_{\widehat{\pi}}$ such that

$$F_{\gamma^{[r]}(\mathbf{x}), \gamma^{[r']}(\mathbf{y})} = \omega_{\widehat{\pi}}^{f^{[r,r']}(\mathbf{x},\mathbf{y})} \quad \text{for all } \mathbf{x} \in \mathbb{Z}_{\widehat{\pi}}^{s_r} \text{ and } \mathbf{y} \in \mathbb{Z}_{\widehat{\pi}}^{s_{r'}}, \tag{16.4}$$

then we can reduce the computation of $Z_{\mathbf{F},\mathfrak{D}}(G)$ to $\mathsf{EVAL}(\widehat{\pi})$ and finish the proof.

First, we deal with (16.4). By $(\mathcal{F}'_1)$, the following function satisfies (16.4):

$$f^{[r,r']}(\mathbf{x},\mathbf{y}) = \sum_{(i,j) \in \mathcal{T}} c_{i,j} \frac{\widehat{\pi}}{\pi_i} \gamma^{[r]}_i(\mathbf{x}) \gamma^{[r']}_j(\mathbf{y}) = \sum_{(i,j) \in \mathcal{T}} \widehat{c}_{i,j} \frac{\widehat{\pi}}{\pi_i} \left(\mathbf{x}\mathbf{A}^{[r]}_{*,i} + \widehat{\mathfrak{a}}^{[r]}_i \right) \left(\mathbf{y}\mathbf{A}^{[r']}_{*,j} + \widehat{\mathfrak{a}}^{[r']}_j \right).$$

Note that $(i,j) \in \mathcal{T}$ implies that $\pi_i = \pi_j$ and thus

$$\gamma^{[r]}_i(\mathbf{x}),\ \gamma^{[r']}_j(\mathbf{y}) \in \mathbb{Z}_{\pi_i} = \mathbb{Z}_{\pi_j}.$$

To be able to substitute the $(\bmod\ \pi_i)$ expressions for $\gamma^{[r]}_i(\mathbf{x})$ and $\gamma^{[r']}_j(\mathbf{y})$, the presence of $\widehat{\pi}/\pi_i$ is crucial. It is also clear that this 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 $\mathbf{e}_i$ for each $i \in [s_r]$ to denote the unit vector in $\mathbb{Z}_{\widehat{\pi}}^{s_r}$ whose ith entry is 1 and whose other entries are 0. Using $(\mathcal{F}_4')$, we know that for every $i \in [s_r]$, 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

$$D^{[r]}_{\gamma^{[r]}(\mathbf{x}+\mathbf{e}_i)} \cdot \overline{D^{[r]}_{\gamma^{[r]}(\mathbf{x})}} = \omega_N^{\alpha_i} \cdot \prod_{j\in[h]} \omega_{\pi_j}^{b_{i,j}\cdot\gamma_j^{[r]}(\mathbf{x})} \quad \text{for all } \mathbf{x} \in \mathbb{Z}_{\widehat{\pi}}^{s_r},$$

because $\gamma^{[r]}(\mathbf{x}+\mathbf{e}_i) - \gamma^{[r]}(\mathbf{x})$ is a vector in $\mathbb{Z}_{\boldsymbol{\pi}}$ that is independent of $\mathbf{x}$.

With the same argument used in the proof of Theorem 5.10 ((12.14) and (12.15)), $\omega_N^{\alpha_i}$ 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

$$D^{[r]}_{\gamma^{[r]}(\mathbf{x}+\mathbf{e}_i)} \cdot \overline{D^{[r]}_{\gamma^{[r]}(\mathbf{x})}} = \omega_{\widehat{\pi}}^{\beta_i} \cdot \prod_{j\in[h]} \omega_{\pi_j}^{b_{i,j}\cdot\gamma_j^{[r]}(\mathbf{x})} \quad \text{for all } \mathbf{x} \in \mathbb{Z}_{\widehat{\pi}}^{s_r}. \tag{16.5}$$

By the argument used in the proof of Theorem 5.10, every nonzero entry of $\mathbf{D}^{[r]}$ is a power of $\omega_{\widehat{\pi}}$. As a result, there exists a function $f^{[r]}$ from $\mathbb{Z}_{\widehat{\pi}}^{s_r}$ to $\mathbb{Z}_{\widehat{\pi}}$ that satisfies (16.3). To see that $f^{[r]}$ is indeed a quadratic polynomial, by (16.5), we have

$$f^{[r]}(\mathbf{x}+\mathbf{e}_i) - f^{[r]}(\mathbf{x}) = \beta_i + \sum_{j\in[h]} \left(\widehat{b}_{i,j} \frac{\widehat{\pi}}{\pi_j} \left(\mathbf{x}\mathbf{A}^{[r]}_{*,j} + \widehat{\mathfrak{a}}_j^{[r]} \right) \right) \quad \text{for all } i \in [s_r], \mathbf{x} \in \mathbb{Z}_{\widehat{\pi}}^{s_r},$$

which is an affine linear form of $\mathbf{x}$ with all coefficients from $\mathbb{Z}_{\widehat{\pi}}$.

By using Lemmas 12.5 and 12.6, we know 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 $\mathsf{EVAL}(\widehat{\pi})$.

17. Decidability in polynomial time: Proof of Theorem 1.2. Finally, we prove Theorem 1.2, i.e., the following decision problem is computable in polynomial time: Given a symmetric $\mathbf{A} \in \mathbb{C}^{m\times m}$ in which every entry $A_{i,j}$ is algebraic, decide if $\mathsf{EVAL}(\mathbf{A})$ is tractable or is #P-hard.

We follow the model of computation discussed in section 2.2. Let

$$\mathscr{A} = \{A_{i,j} : i, j \in [m]\} = \{a_j : j \in [n]\}$$

for some $n \geq 1$ and let α be a primitive element of $\mathbb{Q}(\mathscr{A})$. Thus, $\mathbb{Q}(\mathscr{A}) = \mathbb{Q}(\alpha)$.

The input of the problem consists of the following three parts:

1. a minimal polynomial $F(x) \in \mathbb{Q}[x]$ of α;
2. a rational approximation $\widehat{\alpha}$ that uniquely determines α as a root of $F(x)$;
3. the standard representation of $A_{i,j}$ with respect to α and $F(x)$, $i, j \in [m]$.

The input size of the decision problem is then the length of the binary string needed to describe all these three parts.

Given $\mathbf{A}$, we follow the proof of Theorem 1.1 as follows. First by Lemma 4.6, we can assume without loss of generality that $\mathbf{A}$ is connected. Then we follow the proof sketch described in sections 5 and 6, depending on whether the matrix $\mathbf{A}$ is bipartite or nonbipartite. We assume that $\mathbf{A}$ is connected and bipartite below. The proof for the nonbipartite case is similar.

17.1. Step 1. We show that either $\mathsf{EVAL}(\mathbf{A})$ is #P-hard or we can construct a purified matrix $\mathbf{A}'$ such that $\mathsf{EVAL}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{A}')$ and then pass $\mathbf{A}'$ down to Step 2. We follow the proof of Theorem 5.2. First, we prove that given $\mathscr{A}$, a generating

set $\mathscr{G} \subset \mathbb{Q}(\mathscr{A})$ of $\mathscr{A}$ can be computed in polynomial time. Recall the definition of a generating set from Definition 7.2. We denote the input size as $\widehat{m}$. Thus, $\widehat{m} \geq m$.

THEOREM 17.1. *Given a finite set of nonzero algebraic numbers* $\mathscr{A}$ (under the model of computation described in section 2.2)*, one can in polynomial time* (*in* $\widehat{m}$) *find* (1) *a generating set* $\mathscr{G} = \{g_1, \ldots, g_d\}$ *of* $\mathscr{A}$ *and* (2) *for every number* $a \in \mathscr{A}$ *the unique tuple* $(k_1, \ldots, k_d) \in \mathbb{Z}^d$ *such that* $a/(g_1^{k_1} \cdots g_d^{k_d})$ *is a root of unity.*

We start the proof with the following lemma.

LEMMA 17.2. *Let*

$$L = \Big\{ \big(x_1, \ldots, x_n\big) \in \mathbb{Z}^n \;\Big|\; a_1^{x_1} \cdots a_n^{x_n} = 1 \Big\}.$$

Let S *be the* $\mathbb{Q}$*-span of* L*, and let* $L' = \mathbb{Z}^n \cap S$*. Then*

$$L' = \Big\{ \big(x_1, \ldots, x_n\big) \in \mathbb{Z}^n \;\Big|\; a_1^{x_1} \cdots a_n^{x_n} \text{ is a root of unity} \Big\}. \tag{17.1}$$

Proof. Clearly L is a lattice, being a discrete subgroup of $\mathbb{Z}^n$. Also L' is a lattice, and $L \subseteq L'$. Suppose $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ is in the lattice in (17.1). Then there exists a nonzero integer ℓ such that $(a_1^{x_1} \cdots a_n^{x_n})^\ell = 1$. As a result, $\ell(x_1, \ldots, x_n) \in L$ and thus $(x_1, \ldots, x_n) \in S$, the $\mathbb{Q}$-span of L.

Conversely, if $\dim(L) = 0$, then $L = \{(0, \ldots, 0)\} = S = L'$. Suppose $\dim(L) > 0$, and we let $\mathbf{b}_1, \ldots, \mathbf{b}_t$ be a basis for L, where $t \in [n]$. Let $(x_1, \ldots, x_n) \in \mathbb{Z}^n \cap S$; then there exist rational numbers $r_1, \ldots, r_t$ such that $(x_1, \ldots, x_n) = \sum_{i=1}^t r_i \mathbf{b}_i$. We have

$$a_1^{x_1} \cdots a_n^{x_n} = \prod_{j=1}^n a_j^{\sum_{i=1}^t r_i b_{i,j}}.$$

Let N be a positive integer such that Nr_i is an integer for $i \in [t]$. Then

$$\big(a_1^{x_1} \cdots a_n^{x_n}\big)^N = \prod_{i=1}^t \left(\prod_{j=1}^n a_j^{b_{i,j}} \right)^{Nr_i} = 1.$$

Thus $a_1^{x_1} \cdots a_n^{x_n}$ is a root of unity and $(x_1, \ldots, x_n)$ is in the lattice in (17.1). ∎

To prove Theorem 17.1, we will also need the following theorem by Ge [19, 20].

THEOREM 17.3 (see [19, 20]). *Given a finite set of nonzero algebraic numbers* $\mathscr{A} = \{a_1, \ldots, a_n\}$ (under the model of computation described in section 2.2)*, one can in polynomial time find a lattice basis for the lattice* L *given by*

$$L = \Big\{ \mathbf{x} = \big(x_1, \ldots, x_n\big) \in \mathbb{Z}^n \;\Big|\; a_1^{x_1} \cdots a_n^{x_n} = 1 \Big\}.$$

Proof of Theorem 17.1. Conceptually this is what we will do: We first use Ge's algorithm to compute a basis for L. Then we show how to compute a basis for L' efficiently. Finally, we compute a basis for $\mathbb{Z}^n/L'$. This basis for $\mathbb{Z}^n/L'$ will define our generating set for $\mathscr{A}$.

More precisely, given the set $\mathscr{A} = \{a_1, \ldots, a_n\}$, we let $\kappa = \{\mathbf{k}_1, \ldots, \mathbf{k}_t\}$ denote the lattice basis for L found by Ge's algorithm [19, 20], where $0 \leq t \leq n$. This basis has polynomially many bits in each integer entry $k_{i,j}$. Here are two easy cases:

1. If $t = 0$, then we can take $g_i = a_i$ as the generators, $1 \leq i \leq n$. There is no nontrivial relation $a_1^{k_1} \cdots a_n^{k_n} =$ a root of unity for any $(k_1, \ldots, k_n) \in \mathbb{Z}^n$ other than $\mathbf{0}$; otherwise a suitable nonzero integer power gives a nontrivial lattice point in L.

2. If $t = n$, then $S = \mathbb{Q}^n$ and $L' = \mathbb{Z}^n$; hence every a_i is a root of unity. In this case, the empty set is a generating set for $\mathscr{A}$.

Assume $0 < t < n$. We will compute from the basis κ a basis β for $L' = \mathbb{Z}^n \cap S$, where S is the $\mathbb{Q}$-span of L; then we compute a basis γ for the quotient lattice $\mathbb{Z}^n/L'$. Both lattice bases γ and β will have polynomially many bits in each integer entry.

Before showing how to compute β and γ, it is clear that $\dim L' = \dim L = t$ and $\dim(\mathbb{Z}^n/L') = n - t$. Let

$$\gamma = \{\mathbf{x}_1, \ldots, \mathbf{x}_{n-t}\} \quad \text{and} \quad \beta = \{\mathbf{y}_1, \ldots, \mathbf{y}_t\}.$$

We define the following set $\{g_1, \ldots, g_{n-t}\}$ from γ as follows:

$$g_j = a_1^{x_{j,1}} a_2^{x_{j,2}} \cdots a_n^{x_{j,n}}, \quad \text{where } \mathbf{x}_j = (x_{j,1}, x_{j,2}, \ldots, x_{j,n}).$$

We check that $\{g_1, \ldots, g_{n-t}\}$ is a generating set of $\mathscr{A}$. Clearly, being exponentials, all $g_j \neq 0$. Suppose for some $(c_1, \ldots, c_{n-t}) \in \mathbb{Z}^{n-t}$, $g_1^{c_1} \cdots g_{n-t}^{c_{n-t}}$ is a root of unity. Since

$$g_1^{c_1} g_2^{c_2} \cdots g_{n-t}^{c_{n-t}} = a_1^{\sum_{j=1}^{n-t} c_j x_{j,1}} a_2^{\sum_{j=1}^{n-t} c_j x_{j,2}} \cdots a_n^{\sum_{j=1}^{n-t} c_j x_{j,n}},$$

we have

$$\left(\sum_{j=1}^{n-t} c_j x_{j,1}, \sum_{j=1}^{n-t} c_j x_{j,2}, \ldots, \sum_{j=1}^{n-t} c_j x_{j,n} \right) = \sum_{j=1}^{n-t} c_j \mathbf{x}_j \in L'.$$

It follows that $c_j = 0$ for all $j \in [n-t]$.

On the other hand, by the definition of $\mathbb{Z}^n/L'$, for every $(k_1, \ldots, k_n) \in \mathbb{Z}^n$, there exists a unique sequence of integers $c_1, \ldots, c_{n-t} \in \mathbb{Z}$ such that

$$(k_1, \ldots, k_n) - \sum_{j=1}^{n-t} c_j \mathbf{x}_j \in L'.$$

In particular, for $\mathbf{e}_i = (0, \ldots, 1, \ldots, 0)$, where there is a single 1 in the ith position, there exist integers $c_{i,j}$, $i \in [n]$ and $j \in [n-t]$, such that

$$\mathbf{e}_i - \sum_{j=1}^{n-t} c_{i,j} \mathbf{x}_j \in L'.$$

As a result, we have

$$\frac{a_i}{a_1^{\sum_{j=1}^{n-t} c_{i,j} x_{j,1}} a_2^{\sum_{j=1}^{n-t} c_{i,j} x_{j,2}} \cdots a_n^{\sum_{j=1}^{n-t} c_{i,j} x_{j,n}}} = \frac{a_i}{g_1^{c_{i,1}} \cdots g_{n-t}^{c_{i,n-t}}}$$

is a root of unity. This completes the construction of a generating set $\mathscr{G}$ for $\mathscr{A}$. In the following, we compute the bases γ and β in polynomial time, given κ.

First, we may change the first vector $\mathbf{k}_1 = (k_{1,1}, \ldots, k_{1,n})$ in κ to be a *primitive* vector, meaning that $\gcd(k_{1,1}, \ldots, k_{1,n}) = 1$, by factoring out the gcd. If the gcd is greater than 1, then this changes the lattice L, but it does not change the $\mathbb{Q}$-span S and thus there is no change to L'.

In addition, there exists a unimodular matrix $\mathbf{M}_1$ such that

$$(k_{1,1}, \ldots, k_{1,n})\, \mathbf{M}_1 = (1, 0, \ldots, 0) \in \mathbb{Z}^n.$$

This is just the extended Euclidean algorithm. (An integer matrix $\mathbf{M}_1$ is *unimodular* iff its determinant is ± 1 or, equivalently, it has an integral inverse matrix.)

Now consider the $t \times n$ matrix

$$\begin{pmatrix} u_{1,1} & \dots & u_{1,n} \\ \vdots & \ddots & \vdots \\ u_{t,1} & \dots & u_{t,n} \end{pmatrix} = \begin{pmatrix} k_{1,1} & \dots & k_{1,n} \\ \vdots & \ddots & \vdots \\ k_{t,1} & \dots & k_{t,n} \end{pmatrix} \mathbf{M}_1.$$

This is also an integral matrix as $\mathbf{M}_1$ is integral. Moreover its first row is $(1, 0, \dots, 0)$. We may perform row transformations to make $u_{2,1} = 0, \dots, u_{t,1} = 0$. Performing the same transformations on the right-hand side replaces the basis κ by another basis for the same lattice, and L' is unchanged. We still use $\kappa = \{\mathbf{k}_1, \dots, \mathbf{k}_t\}$ to denote this new basis.

Next, consider the entries $u_{2,2}, \dots, u_{2,n}$. If $\gcd(u_{2,2}, \dots, u_{2,n}) > 1$ we may divide out this gcd. Since the second row satisfies

$$\big(k_{2,1}, k_{2,2}, \dots, k_{2,n}\big) = \big(0, u_{2,2}, \dots, u_{2,n}\big)\, \mathbf{M}_1^{-1},$$

this gcd must also divide $k_{2,1}, k_{2,2}, \dots, k_{2,n}$. (In fact, this is also the gcd of $(k_{2,1}, k_{2,2}, \dots, k_{2,n})$.) This division updates the basis κ by another basis, which changes the lattice L, but still it does not change the $\mathbb{Q}$-span S and thus the lattice L' remains unchanged. We continue to use the same κ to denote this updated basis.

For the same reason, there exists an $(n-1) \times (n-1)$ unimodular $\mathbf{M}'$ such that

$$\big(u_{2,2}, \dots, u_{2,n}\big)\, \mathbf{M}' = \big(1, 0, \dots, 0\big) \in \mathbb{Z}^{n-1}.$$

Append a 1 at the $(1,1)$ position. This defines a second $n \times n$ unimodular matrix $\mathbf{M}_2$ such that we may update the matrix equation as follows:

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & u_{3,2} & u_{3,3} & \dots & u_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & u_{t,2} & u_{t,3} & \dots & u_{t,n} \end{pmatrix} = \begin{pmatrix} k_{1,1} & \dots & k_{1,n} \\ \vdots & \ddots & \vdots \\ k_{t,1} & \dots & k_{t,n} \end{pmatrix} \mathbf{M}_1 \mathbf{M}_2.$$

Now we may kill off the entries $u_{3,2}, \dots, u_{t,2}$, accomplished by row transformations which do not change L or L'. It follows that we can finally find a unimodular matrix $\mathbf{M}^*$ such that the updated κ satisfies

$$\begin{pmatrix} k_{1,1} & \dots & k_{1,n} \\ \vdots & \ddots & \vdots \\ k_{t,1} & \dots & k_{t,n} \end{pmatrix} \mathbf{M}^* = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & 0 & \dots & 0 \end{pmatrix}. \tag{17.2}$$

The right-hand side is the $t \times t$ identity matrix $\mathbf{I}_t$ with an all-zero $t \times (n-t)$ matrix appended. The updated κ here is a lattice basis for a lattice $\widehat{L}$ which has the same $\mathbb{Q}$-span S as L. It is also a full-dimensional sublattice of (the unchanged) L'.

We claim this updated $\kappa = \{\mathbf{k}_1, \dots, \mathbf{k}_t\}$ is actually a lattice basis for L' and thus $\widehat{L} = L'$. Assume for some rational numbers $r_1, \dots, r_t$ the vector $\sum_{i=1}^{t} r_i \mathbf{k}_i \in \mathbb{Z}^n$. Then multiplying $(r_1, \dots, r_t)$ to the left in (17.2) implies that $r_1, \dots, r_t$ are integers.

This completes the computation of a basis for L'. As the only operations we perform are Gaussian eliminations and gcd computations, this is in polynomial time, and the number of bits in every entry is always polynomially bounded.

Finally we describe the computation of a basis for the quotient lattice $\mathbb{Z}^n/L'$.

We start with a basis κ for L' as computed above and extend it to a basis for $\mathbb{Z}^n$. The extended part will then be a basis for $\mathbb{Z}^n/L'$. Suppose that we are given the basis κ for L' together with a unimodular matrix $\mathbf{M}^*$ satisfying (17.2). Then consider the $n \times n$ matrix $(\mathbf{M}^*)^{-1}$. Since $(\mathbf{M}^*)^{-1} = \mathbf{I}_n(\mathbf{M}^*)^{-1}$, the first t rows of $(\mathbf{M}^*)^{-1}$ are precisely the κ matrix. We define the basis for $\mathbb{Z}^n/L'$ to be the last $n-t$ row vectors of $(\mathbf{M}^*)^{-1}$. It can be easily verified that this is a lattice basis for $\mathbb{Z}^n/L'$. □

With Theorem 17.1, we can now follow the proof of Theorem 5.2. By using the generating set, we construct the matrix $\mathbf{B}$ as in section 7.2. Every entry of $\mathbf{B}$ is the product of a nonnegative integer and a root of unity with $\mathsf{EVAL}(\mathbf{A}) \equiv \mathsf{EVAL}(\mathbf{B})$.

We then check whether $\mathbf{B}'$, where $B'_{i,j} = |B_{i,j}|$ for all i, j, satisfies the conditions imposed by the dichotomy theorem of Bulatov and Grohe. (Note that every entry of $\mathbf{B}'$ is a nonnegative integer.) If $\mathbf{B}'$ does not satisfy, then $\mathsf{EVAL}(\mathbf{B}')$ is #P-hard, and so is $\mathsf{EVAL}(\mathbf{A})$ by Lemma 7.5. Otherwise, $\mathbf{B}$ must be a purified matrix, and we pass it down to the next step.

17.2. Step 2. We follow the proof of Theorem 5.3. After rearranging the rows and columns of the purified matrix $\mathbf{B}$, we check the orthogonality condition imposed by Lemma 8.5. If $\mathbf{B}$ satisfies the orthogonality condition, we can use the cyclotomic reduction to construct efficiently a pair $(\mathbf{C}, \mathfrak{D})$ from $\mathbf{B}$, which satisfies the conditions $(Shape_1)$, $(Shape_2)$, $(Shape_3)$ and satisfies $\mathsf{EVAL}(\mathbf{B}) \equiv \mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$.

Next, we check whether the pair $(\mathbf{C}, \mathfrak{D})$ satisfies $(Shape_4)$ and $(Shape_5)$. If either of these two conditions is not satisfied, $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D})$ is #P-hard, and so is $\mathsf{EVAL}(\mathbf{B})$. Finally we check the rank-1 condition, which implies $(Shape_6)$, as imposed by Lemma 8.12 on $(\mathbf{C}, \mathfrak{D})$. With $(Shape_1)$–$(Shape_6)$, we follow section 8.6 to construct a tuple $((M, 2N), \mathbf{X}, \mathfrak{Y}')$ that satisfies $(\mathcal{U}_1)$–$(\mathcal{U}_4)$, and $\mathsf{EVAL}(\mathbf{C}, \mathfrak{D}) \equiv \mathsf{EVAL}(\mathbf{X}, \mathfrak{Y}')$. We then pass the tuple $((M, 2N), \mathbf{X}, \mathfrak{Y}')$ down to Step 3.

17.3. Step 3. We follow Theorems 5.4, 5.6, 5.8, and 5.9. First, $(\mathcal{U}_5)$ in Theorem 5.4 can be verified efficiently. In Theorem 5.6, we need to check if the matrix $\mathbf{F}$ has a Fourier decomposition, after an appropriate permutation of its rows and columns. This decomposition, if $\mathbf{F}$ has one, can be computed efficiently by first checking the group condition in Lemma 9.1 and then following the proofs of both Lemma 9.5 and Lemma 9.7. Finally, it is easy to see that all the conditions imposed by Theorems 5.8 and 5.9 can be checked in polynomial time.

If $\mathbf{A}$ and other matrices, pairs, or tuples derived from $\mathbf{A}$ satisfy all the conditions in these three steps, then by the tractability part of the dichotomy theorem, $\mathsf{EVAL}(\mathbf{A})$ is solvable in polynomial time. From this, we obtain the polynomial-time decidability of the complexity dichotomy, and Theorem 1.2 is proved.

18. Acknowledgments. We would like to thank Al Aho, Miki Ajtai, Sanjeev Arora, Dick Askey, Paul Beame, Richard Brualdi, Andrei Bulatov, Xiaotie Deng, Alan Frieze, Martin Grohe, Pavol Hell, Lane Hemaspaandra, Kazuo Iwama, Gabor Kun, Dick Lipton, Tal Malkin, Christos Papadimitriou, Mike Paterson, Rocco Servedio, Endre Szemerédi, Shang-Hua Teng, Joe Traub, Osamu Watanabe, Avi Wigderson, and Mihalis Yannakakis for their interest and many comments. We thank especially Martin Dyer, Leslie Goldberg, Mark Jerrum, Marc Thurley, Leslie Valiant, and Mingji Xia for in-depth discussions. We are truly grateful to the reviewers for their dedication

in carefully reading through this long paper; they offered many valuable critiques and suggestions for improvements. We have greatly benefited from their comments.

REFERENCES

[1] A. Bulatov, *The complexity of the counting constraint satisfaction problem*, in Proceedings of the 35th International Colloquium on Automata, Languages and Programming, 2008, pp. 646–661.

[2] A. Bulatov, *The Complexity of the Counting Constraint Satisfaction Problem*, Electronic Colloquium on Computational Complexity, 2009.

[3] A. Bulatov, M. E. Dyer, L. A. Goldberg, M. Jalsenius, M. R Jerrum, and D. M. Richerby, *The complexity of weighted and unweighted #CSP*, J. Comput. System Sci., 78 (2012), pp. 681–688.

[4] A. Bulatov and M. Grohe, *The complexity of partition functions*, Theoret. Comput. Sci., 348 (2005), pp. 148–186.

[5] J.-Y. Cai and X. Chen, *A decidable dichotomy theorem on directed graph homomorphisms with nonnegative weights*, in Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science, 2010, pp. 437–446.

[6] J.-Y. Cai and X. Chen, *Complexity of counting CSP with complex weights*, in Proceedings of the 44th Symposium on Theory of Computing, 2012, pp. 909–920.

[7] J.-Y. Cai, X. Chen, and P. Lu, *Non-negatively weighted #CSPs: An effective complexity dichotomy*, in Proceedings of the 26th Annual IEEE Conference on Computational Complexity, 2011.

[8] J.-Y. Cai and P. Lu, *Holographic algorithms: From art to science*, in Proceedings of the 39th Annual ACM Symposium on Theory of Computing, 2007, pp. 401–410.

[9] J.-Y. Cai, P. Lu, and M. Xia, *Holant problems and counting CSP*, in Proceedings of the 41st ACM Symposium on Theory of Computing, 2009, pp. 715–724.

[10] L. Carlitz, *Kloosterman sums and finite field extensions*, Acta Arithmetica, 16 (1969), pp. 179–193.

[11] N. Creignou, S. Khanna, and M. Sudan, *Complexity Classifications of Boolean Constraint Satisfaction Problems*, SIAM Monogr. Discrete Math. Appl., SIAM, Philadelphia, 2001.

[12] M. E. Dyer, L. A. Goldberg, and M. Paterson, *On counting homomorphisms to directed acyclic graphs*, J. ACM, 54 (2007).

[13] M. E. Dyer and C. Greenhill, *The complexity of counting graph homomorphisms*, Random Structures Algorithms, 17 (2000), pp. 260–289.

[14] M. E. Dyer and D. M. Richerby, *On the complexity of #CSP*, in Proceedings of the 42nd ACM Symposium on Theory of Computing, 2010, pp. 725–734.

[15] A. Ehrenfeucht and M. Karpinski, *The Computational Complexity of (XOR, AND)-Counting Problems*, Tech. report TR-8543, Universität Bonn, 1990.

[16] T. Feder and M. Vardi, *The computational structure of monotone monadic SNP and constraint satisfaction: A study through Datalog and group theory*, SIAM J. Comput., 28 (1999), pp. 57–104.

[17] R. Feynman, R. Leighton, and M. Sands, *The Feynman Lectures on Physics*, Addison-Wesley, Reading, MA, 1970.

[18] M. Freedman, L. Lovász, and A. Schrijver, *Reflection positivity, rank connectivity, and homomorphism of graphs*, J. AMS, 20 (2007), pp. 37–51.

[19] G. Ge, *Algorithms Related to Multiplicative Representations of Algebraic Numbers*, Ph.D. thesis, University of California–Berkeley, 1993.

[20] G. Ge, *Testing equalities of multiplicative representations in polynomial time*, in Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science, 1993, pp. 422–426.

[21] L. A. Goldberg, M. Grohe, M. Jerrum, and M. Thurley, *A complexity dichotomy for partition functions with mixed signs*, SIAM J. Comput., 39 (2010), pp. 3336–3402.

[22] P. Hell and J. Nešetřil, *On the complexity of H-coloring*, J. Combin. Theory Ser. B, 48 (1990), pp. 92–110.

[23] P. Hell and J. Nešetřil, *Graphs and Homomorphisms*, Oxford University Press, New York, 2004.

[24] N. Jacobson, *Basic Algebra* I, W.H. Freeman, New York, 1985.

[25] S. Lang, *Algebra*, 3rd ed., Springer-Verlag, New York, 2002.

[26] H. W. Lenstra, *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc., 26 (1992), pp. 211–244.

[27] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., Cambridge University Press, Cambridge, UK, 1997.
[28] L. Lovász, *Operations with structures*, Acta Math. Hungar., 18 (1967), pp. 321–328.
[29] L. Lovász, *The rank of connection matrices and the dimension of graph algebras*, European J. Combin., 27 (2006), pp. 962–970.
[30] P. Morandi, *Field and Galois Theory*, Grad. Texts in Math. 167, Springer, New York, 1996.
[31] T.J. Schaefer, *The complexity of satisfiability problems*, in Proceedings of the 10th Annual ACM Symposium on Theory of Computing, 1978, pp. 216–226.
[32] A. Schrijver, *Graph invariants in the spin model*, J. Combin. Theory Ser. B, 99 (2009), pp. 502–511.
[33] M. Thurley, *The Complexity of Partition Functions*, Ph.D. thesis, Humboldt Universität zu Berlin, 2009.
[34] M. Thurley, *The Complexity of Partition Functions on Hermitian Matrices*, arXiv:1004.0992, 2010.
[35] L. G. Valiant, *Holographic algorithms (extended abstract)*, in Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science, 2004, pp. 306–315.
[36] L. G. Valiant, *Accidental algorthims*, in Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science, 2006, pp. 509–517.
[37] L. G. Valiant, *Holographic algorithms*, SIAM J. Comput., 37 (2008), pp. 1565–1594.